République Algérienne Démocratique et Populaire
Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER

En

Informatique

Option

Administration et Sécurité des Réseaux

Thème

Supervision des réseaux informatiques. Cas d'étude : Centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance de l'Université de Béjaia

Présenté par :

MEDJBER Kenza
KHRAMSIA Halima

Soutenu le 2 juillet 2024 devant le jury composé de :

Président	**Mme HAMZA Lamia**	**U. A/Mira Béjaia.**
Examinateur	**Mme BOUADEM Nassima**	**U. A/Mira Béjaia.**
Encadrant	**Mme BACHIRI Lina**	**U. A/Mira Béjaia.**

Béjaïa, juillet 2024.

⁂ Remerciements ⁂

Nous remercions le dieu le tout puissant de nous avoir donné la force ,la volonté de donner le meilleur de nous-même et le courage de mener ce travail.

Tout d'abord, nous tenons à exprimer notre profonde gratitude à toutes les personnes qui ont contribué à l'élaboration de ce mémoire et qui ont rendu cette expérience enrichissante et mémorable.

Un grand merci pour nos familles, surtout nos parents qui nous ont soutenus tout au long de ce projet.

Nous remercions chaleureusement notre encadrante de mémoire, BACHIRI Lina, pour sa guidance précieuse, ses conseils avisés et son soutien constant tout au long de ce projet. Son expertise et son engagement ont été essentiels à la réalisation de ce travail.

Nous souhaitons également exprimer notre reconnaissance à l'ensemble de l'équipe du Centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance de l'Université de Béjaïa. Leur accueil, leur disponibilité et leur collaboration ont grandement facilité la conduite de cette étude de cas.

Nous remercions, enfin, les membres du jury qui ont accepté d'évaluer ce mémoire.

⁕ *Dédicaces* ⁕

Je remercie en premier lieu le grand DIEU de m'avoir donnée
les moyens,l'énergie mais surtout la volonté nécessaire
pour la réalisation de ce modeste travail.

Que je dédie :

À mes parents pour leur soutien moral et leur encouragement Leur
présence a été une source de motivation constante.

je tiens à exprimer ma gratitude à mes sœurs, dont l'amour, la patience
et le soutien inconditionnel m'ont permis de mener à bien
ce mémoire. Merci de croire en moi et de m'encourager
à chaque étape de mon parcours.

Kenza

⁂ *Dédicaces* ⁂

C'est avec l'aide et la grâce de Dieu qu'on a achevé ce travail

Que je dédie :

À mes parents pour l'éducation qu'ils m'ont prodiguée et pour leur soutien, leur confiance ainsi que leurs prières tout au long de mes études. Sans eux je ne serais jamais arrivée à ce stade de ma vie. Que Dieu vous accorde santé, longue vie et vous garde à mes côtés.

À mes chèrs frères et sœurs .

À toute la famille KHRAMSIA et la famille HADDAD.

À tous les professeurs et enseignants qui ont collaboré à ma formation depuis mon premier cycle d'études jusqu'à la fin de mes études universitaires.

Halima

Table des matières

Table des figures

Liste des tableaux

Notations et symboles

ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BNC	Bayonet Neill–Concelman
CAN	Campus Area Network
CDDI	Copper Distributed Data Interface
CPU	Central Processing Unit
CSRICTED	Centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
FAN	Fully Automated Nagios
FTP	File Transfer Protocol
GNS3	Graphical Network Simulator
GPL	GNU General Public License
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IrDA	Infrared Data Association
LAN	Local Area Network
MAC	Media Access Control (Contrôle d'accès au support physique)
MAN	Metropolitan Area Network
MD5	Message Digest 5
MIB	Base d'informations de gestion
NMA	Network Management Application

NME	Network Management Entity
NMS	Network Management Station
NNM	Network Node Manager
NRPE	Nagios Remote Plugin Executor
OID	Object Identifier
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PHP	Hypertext Preprocessor
PING	Packet Internet Groper
POP3	Post Office Protocol version 3
Prise SC	Simplex préchargés
RJ45	Registered Jack
RRDtool	Round-Robin Database Tool
SI	Système d'Information
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STP	Signal Mode Fibre
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TELNET	Telnet Network Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

Introduction générale

Dans un monde de plus en plus connecté, la gestion et la supervision des réseaux informatiques sont devenues des enjeux cruciaux pour garantir la disponibilité, la performance et la sécurité des infrastructures technologiques. Les réseaux informatiques, qui permettent le partage des ressources et la communication entre divers dispositifs, sont au cœur des opérations des entreprises modernes.

Ce mémoire se penche sur l'importance de la supervision des réseaux informatiques en utilisant l'outil Nagios, avec un focus sur une étude de cas réalisée au Centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance de l'Université de Béjaïa.

Dans le cadre des établissements universitaires, les centres de calcul jouent un rôle crucial en fournissant des ressources informatiques essentielles pour les activités académiques et de recherche. La complexité et la diversité des infrastructures informatiques dans ces centres, comprenant des pare-feu, des serveurs, des commutateurs, et divers services réseau, nécessitent une supervision constante pour garantir leur disponibilité, leur performance, et leur sécurité.

Cependant, l'absence d'un système de supervision efficace peut entraîner des interruptions de service, des performances dégradées, et des risques de sécurité non détectés, impactant directement les utilisateurs et les opérations académiques. La question se pose alors : comment peut-on implémenter une solution de supervision centralisée et automatisée capable de surveiller l'intégralité de l'infrastructure d'un centre de calcul universitaire et de fournir des alertes en temps réel en cas de défaillance ou d'anomalie ? Pour répondre à cette problématique, les objectifs du projet incluent la simulation d'un réseau de centres de calcul, la configuration des équipements pour la supervision, la définition des paramètres de supervision, le test de l'efficacité de Nagios et l'analyse des résultats de la simulation.

Dans ce cadre, nous avons utilisé Graphical Network Simulator(GNS3) pour simuler les réseaux du Centre des Systèmes et Réseaux, permettant de configurer et tester les équipements en environnement virtuel avant de les déployer sur le réseau réel.

Le premier chapitre de ce mémoire introduit les concepts fondamentaux des réseaux informatiques, en détaillant les types de réseaux, leurs topologies, les équipements utilisés ainsi que les

modèles de communication OSI et TCP/IP, fournissant une base théorique solide pour comprendre les aspects techniques abordés dans les chapitres suivants.

Le deuxième chapitre se concentre sur la supervision des réseaux, ses objectifs, les types et les architectures de supervision, les méthodes anisi que les modes de surveillance,,mettant également en lumière le protocole SNMP, fondamental pour la gestion des réseaux dans le modèle TCP/IP.

Le troisième chapitre présente une revue des principaux outils de supervision des réseaux, en mettant en lumière leurs caractéristiques, avantages et inconvénients, avec une attention particulière accordée à Nagios ainsi qu'à d'autres solutionspropriétaires et open source telles que Zabbix, Centreon et Prometheus.

Le quatrième chapitre offre une description détaillée de l'organisme d'accueil, le Centre des Systèmes et Réseaux de l'Université de Béjaïa, décrivant l'infrastructure existante, les ressources matérielles et logicielles, et les défis rencontrés dans la gestion du réseau.

Le dernier chapitre décrit le contexte de travail et les étapes d'implémentation de la solution de supervision avec Nagios, couvrant, le matériel et le logiciel utilisé, l'architecture proposée, et les résultats obtenus.

En conclusion, ce mémoire vise à démontrer l'importance de la supervision proactive des réseaux informatiques pour maintenir leur performance, en mettant en pratique les connaissances théoriques acquises à travers une étude de cas concrète.

Chapitre 1

Généralités sur les réseaux informatiques

1.1 Introduction

Les réseaux informatiques représentent des éléments cruciaux de l'infrastructure technologique moderne, permettant de connecter les systèmes d'information et de faciliter la transmission de données entre différents sites informatiques. Les organisations et les entreprises s'appuient largement sur les services fournis par ces réseaux, les considérant comme indispensables à leur fonctionnement. En effet, ces réseaux offrent un moyen efficace de promouvoir le travail collaboratif, de partager des données, d'imprimer à distance, d'échanger des messages et d'accéder à des bases de données, qu'elles soient localisées ou délocalisées.

Dans ce chapitre nous allons présenter les réseaux informatiques leurs significations, objectifs, classifications, ses équipements ainsi le modèle OSI les protocoles réseau les plus utilisé. Pour l'objectif de bien identifier le domaine dans lequel nous souhaitons travailler.

1.2 Réseaux informatiques

Dans cette section, nous allons présenter la signification des réseaux informatiques, leurs objectifs de déploiement, ainsi que leur classification selon l'étendue géographique, l'intention de l'organisation et la topologie. Nous aborderons également les équipements des réseaux informatiques, leurs architectures, les modèles de communication OSI et TCP/IP, ainsi que les différents types de protocoles.

1.2.1 Que signifie un réseau

Un réseau informatique est un système qui relie deux ou plusieurs appareils informatiques pour transmettre et partager des informations. Ces réseaux peuvent aller de petites installations, comme

la connexion de deux ordinateurs portables avec un câble Ethernet, à des systèmes complexes comme l'internet, qui connecte des milliards d'appareils dans le monde entier [1].

1.2.2 Objectifs du déploiement d'un réseau informatique

• **Partage des ressources :** optimiser l'utilisation des ressources en permettant aux appareils connectés de partager le matériel, les logiciels et les ressources de données, mais aussi l'accès aux données et aux équipements critiques à travers les différents départements.

• **Assurer la disponibilité et la fiabilité des ressources :** grâce à une gestion diversifiée de l'approvisionnement et des sauvegardes.

• **Améliorer les performances du système :** en ajoutant des processeurs et en organisant efficacement les données.

• **Réduire les coûts opérationnels :** en optimisant l'utilisation des ressources et en centralisant la gestion du réseau.

• **Accroître la capacité de stockage :** pour répondre à l'afflux croissant de données clients.

• **Simplifier la collaboration et la communication interne :** grâce au partage de fichiers et aux plateformes de messagerie.

• **Minimiser les erreurs :** en garantissant l'unicité des sources d'information et en effectuant des sauvegardes régulières.

• **Assurer un accès distant sécurisé aux données sensibles :** même en période d'incertitude, grâce à des protocoles d'authentification multiples.

1.2.3 Classification des réseaux informatiques selon l'étendue géographique

Les réseaux informatiques peuvent être classifiés en fonction de leur étendue géographique, ce qui permet de distinguer les différents types de réseaux selon leur taille, leur portée et leur usage spécifique. Cette classification est essentielle pour comprendre les caractéristiques de chaque type de réseau. Du réseau personnel limité à une seule personne jusqu'aux réseaux mondiaux qui connectent des ordinateurs sur de vastes distances, voici une classification détaillée des principaux types de réseaux informatiques selon leur étendue géographique.

♦ **Personal Area Network (PAN) :** Le PAN est le type de réseau informatique le plus basique. Ce réseau est limité à une seule personne, il offre une portée de réseau de 1 à 100 mètres d'une personne à l'autre pour la communication. Sa vitesse de transmission est très élevée, son entretien très facile et son coût très faible. Il utilise les technologies Bluetooth, IrDA et Zigbee.. [2].

♦ **Local Area Network (LAN) :** est le réseau le plus fréquemment utilisé. Il s'agit d'un réseau informatique qui relie des ordinateurs par une voie de communication commune, à l'intérieur d'une zone limitée. La portée du réseau peut atteindre 2 km et la vitesse de transmission est très élevée, la maintenance est aisée et le coût est faible [2].

♦ **Campus Area Network (CAN) :** Le CAN est plus grand qu'un LAN mais plus petit qu'un MAN. Il s'agit d'un type de réseau informatique généralement utilisé dans des lieux tels que les écoles ou les collèges. Ce réseau couvre une zone géographique limitée, c'est-à-dire qu'il s'étend sur plusieurs bâtiments du campus. Le CAN utilise principalement la technologie Ethernet avec une portée de 1km à 5km. Sa vitesse de transmission est très élevée, avec un coût de maintenance modéré et un coût modéré [2] .

♦ **Métropolitain Area Network (MAN) :** Un MAN est plus grand qu'un LAN mais plus petit qu'un WAN. Il s'agit d'un type de réseau informatique qui connecte des ordinateurs sur une zone métropolitaine comme une ville. Ce réseau utilise principalement les technologies FDDI, CDDI et ATM sur une distance de 5 à 50 km. Sa vitesse de transmission est moyenne. Il est difficile à entretenir et son coût est élevé [2].

♦ **Wide Area Network (WAN) :**Le WAN est un type de réseau informatique qui connecte des ordinateurs sur une grande distance géographique. Il n'est pas limité à un seul endroit mais s'étend sur de nombreux sites. Le WAN peut également être défini comme un groupe de réseaux locaux qui communiquent entre eux sur une distance supérieure à 50 km. Sa vitesse de transmission est très faible et elle s'accompagne d'une maintenance et d'un coût très élevés. L'exemple le plus courant de WAN est l'Internet [2] .

1.2.4 Classification des réseaux informatiques selon l'intention de l'organisation

Les réseaux informatiques peuvent également être classifiés selon l'intention de l'organisation qui les utilise. Cette classification permet de comprendre comment les réseaux sont gérés, qui y a accès et pour quels usages spécifiques ils sont conçus. Qu'il s'agisse de réseaux internes limités à une seule organisation ou de réseaux mondiaux ouverts à un large public, chaque type de réseau sert des objectifs distincts et possède des caractéristiques uniques. Voici une classification détaillée des principaux types de réseaux informatiques selon l'intention de l'organisation :

♦ **Intranet :** l'intranet est un ensemble de réseaux gérés et contrôlés par une seule entité. Dont l'accès est réservé aux utilisateurs autorisés seuls. Un intranet se trouve généralement derrière le routeur d'un réseau local [1].

♦ **Internet :** L'internet (ou l'inter réseau) est un ensemble de réseaux multiples reliés par des routeurs et des logiciels de mise en réseau. Il s'agit d'un système mondial qui gouvernements, les chercheurs, les entreprises, le public et les réseaux informatiques individuels. Réseaux informatiques individuels [1].

♦ **Extranet :** Un extranet est similaire à l'intranet, mais avec des connexions à des réseaux externes particuliers. Il est généralement utilisé pour partager des ressources avec des partenaires, des clients ou des employés éloignés [1].

♦ **Darknet :** Le darknet est un réseau superposé qui fonctionne sur l'internet et auquel on ne peut accéder qu'au moyen d'un logiciel spécialisé. Accessible qu'au moyen d'un logiciel spécialisé. Il utilise des protocoles de communication uniques et personnalisés. De communication uniques et personnalisés [1].

1.2.5 Classification des réseaux informatiques selon la topologie

La topologie réseau décrit la manière dont les différents nœuds d'un réseau sont connectés et comment les données circulent entre eux. Elle détermine la disposition physique et logique des connexions réseau. Chaque topologie a ses propres avantages, inconvénients et cas d'utilisation appropriés [3].

♦ **Topologie en bus :**

• **Description :** La connexion des matériels est assurée par un bus partagé par tous les utilisateurs. Telle que chaque message est reçu par tous les nœuds. La figure suivante montre la topologie en bus :

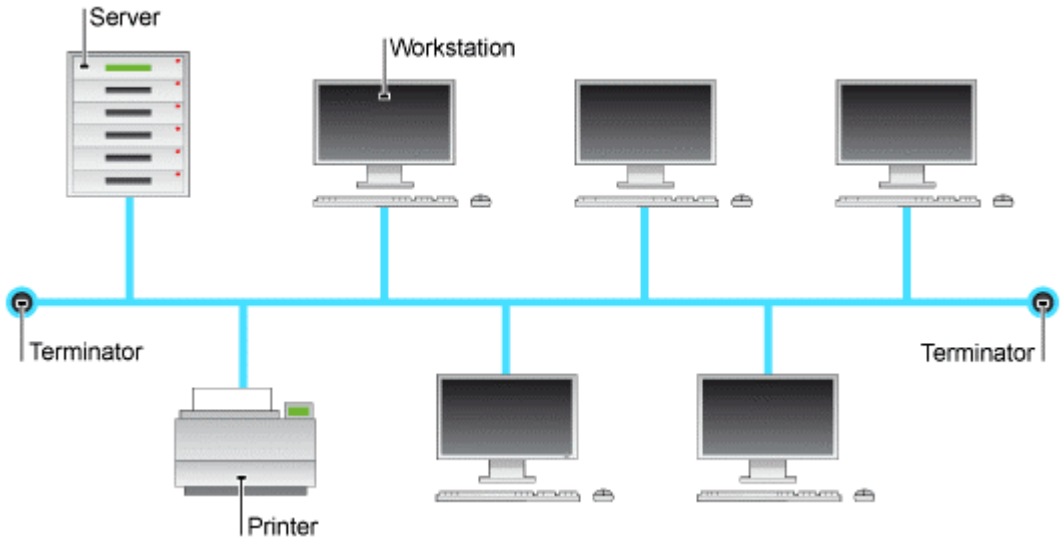

FIGURE 1.1 – Topologie en bus [3]

• **Avantages :**

- Présente l'un des coûts de mise en réseau les plus bas.

- Facile à mettre en œuvre et à étendre.

• **Inconvénients :**

- Longueur du câble et nombre de stations limités.

- Faible sécurité des données transitant sur le réseau.

- N'est plus adaptée aux réseaux importants.

♦ **Topologie en anneau :**

• **Description :** Toutes les machines sont reliées entre elles dans une boucle fermée. Les données circulent dans une direction unique. La figure suivante montre la topologie en anneau :

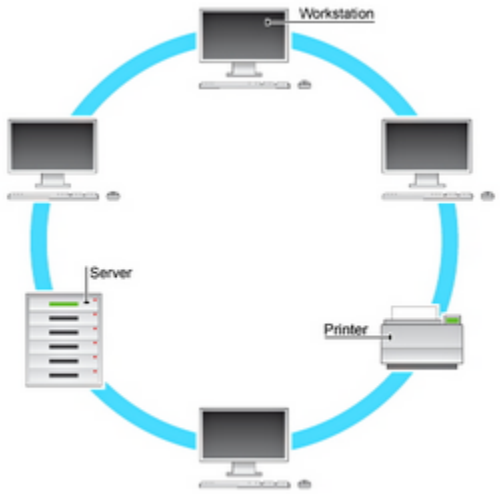

FIGURE 1.2 – Topologie en anneau [3]

• **Avantages :**

- Taux d'utilisation de la bande passante optimum.

- Le protocole est simple, il évite la gestion des collisions.

• **Inconvénients :**

- Le retrait ou la panne d'une entité active paralyse le trafic du réseau.

- L'ajout et la modification de machines connectées peuvent affecter le réseau.

♦ **Topologie Maillée :**

• **Description :** Chaque nœud est connecté à tous les autres nœuds. La figure suivante montre la topologie maillée :

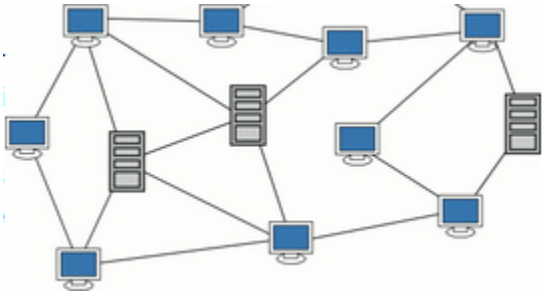

FIGURE 1.3 – Topologie Maillée [3]

• **Avantages :**

- Détection facile des pannes.

- Offre une redondance élevée et une grande fiabilité.

• **Inconvénients :**

- Le coût de câblage est plus élevé.

- Complexité technique.

⧫ **Topologie en arbre :**

• **Description :** Une topologie arborescente divisée en niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur.La figure suivante montre la topologie en arbre :

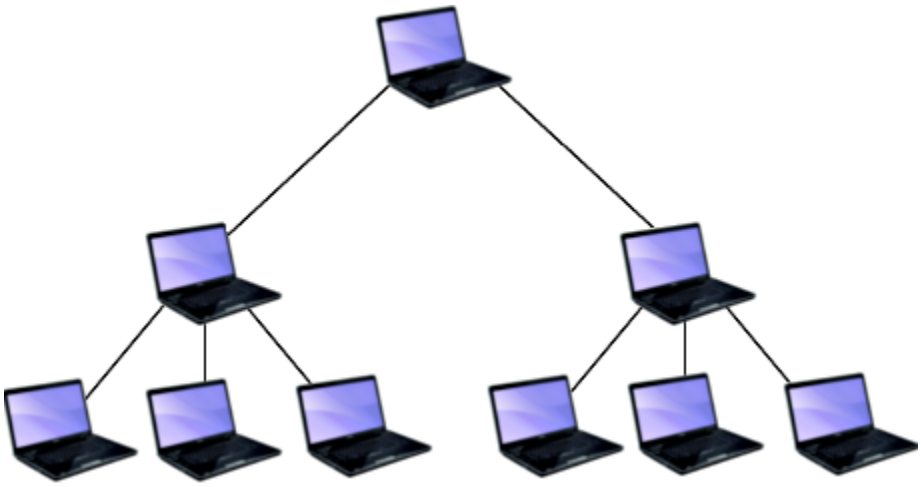

FIGURE 1.4 – Topologie en arbre [3]

• **Avantages :**

- Permet une gestion claire des nœuds.

- Facilité d'ajout des nœuds sans perturber l'ensemble du système.

• **Inconvénients :**

- Complexité en cas de panne, surtout dans les réseaux avec plusieurs niveaux hiérarchiques.

♦ **Topologie en étoile :**

• **Description :** Les équipements du réseau sont reliés à un système matériel central (switch). Celui-ci a pour rôle d'assurer la communication entre les différents équipements du réseau. La figure suivante montre la topologie étoile :

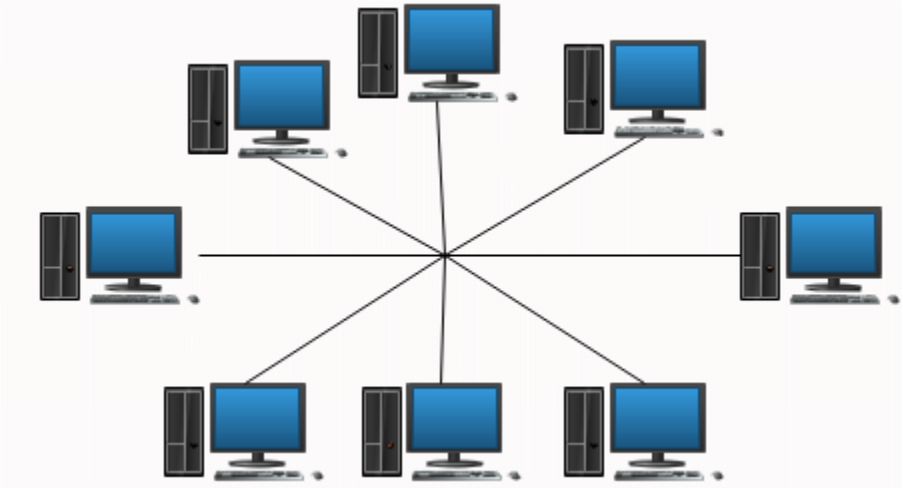

FIGURE 1.5 – Topologie en étoile [3]

• **Avantages :**

- Localisation facile des pannes.

- Le débranchement d'une connexion ne paralyse pas le reste du réseau.

- Ajout facile de postes.

• **Inconvénients :**

- Si le concentrateur est défectueux, tout le réseau est en panne.

- Utilisation de multiples routeurs ou switches afin de pouvoir communiquer entre différents réseaux ou ordinateurs

1.2.6 Équipements d'un réseau informatique

Les équipements d'un réseau informatique sont essentiels pour établir, gérer et maintenir les communications entre différents appareils au sein d'un réseau. Ces équipements permettent la transmission de données, garantissent la sécurité des communications, et assurent la disponibilité et la performance du réseau. Voici une présentaion aux principaux équipements d'un réseau informatique :

1.2.6.1 Equipements d'interconnexion

Répéteur (repeater) : Le répéteur est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau. Agit exclusivement sur les aspects physiques du signal réseau. En d'autres termes, il se contente de prendre le signal entrant, de l'amplifier et de le transmettre à nouveau sans altérer son contenu ou effectuer des opérations de traitement plus avancées [4].

FIGURE 1.6 – Répéteur (Repeater)

Concentrateur (Hub) : C'est un appareil électronique qui permet de relier plusieurs équipements au réseau Son rôle est de prendre les données reçues sur un port et de les diffuser bêtement sur l'ensemble des ports ce qui ralentit considérablement le réseau si un nombre important d'ordinateurs sont connectés. Opère dans la couche physique [4].

FIGURE 1.7 – Concentrateur (Hub)

Pont (bridge) : C'est équipement qui permet d'interconnecter deux réseaux de liaison différente, Il examinant et décryptant les adresses mac pour décider la suite des paquets Il base sur principe de ne pas transmettre les trames dont l'émetteur et le destinataire se trouvent sur le même segment du réseau local. Il fonctionne au niveau 2 de modèle OSI [4].

FIGURE 1.8 – Pont (bridge)

Commutateur (switch) : Un boitier contenant une multitude de ports, pour connecter les prises RJ45 des câbles réseau agissant au niveau 2 de modèle OSI Contrairement au concentrateur qui envoie l'information à l'ensemble des ordinateurs connectés au réseau, le commutateur va établir une liaison seulement entre les ordinateurs intéressés par l'information [4].

FIGURE 1.9 – commutateur (switch)

Routeur : Est un équipement qui permet l'interconnexion des réseaux. Et L'échange des informations entre deux réseaux. Il dispose d'un CPU, la carte mère, RAM, ROM. Les routeurs peuvent avoir les deux types de ponts console pour la connexion d'un terminal utilisé pour la gestion et d'un réseau différents ports de média LAN ou WAN [4].

FIGURE 1.10 – Routeur

1.2.6.2 Système de câblage

La communication d'information à travers un réseau s'effectue sur un support qui fournit le canal via lequel le message se déplace de la source à la destination. Chaque nature de support correspond une forme particulière du signal qui s' y propage. .

♦ **Types de câbles :**

Le câble à fibre optique, le câble à paire torsadée et le câble coaxial sont les trois types principaux de câbles réseau utilisés dans les systèmes de communication.

• **Paire torsadée :** C'est le moyen de transmission le plus simple. Composé de deux fils de cuivre torsadés recouverts d'une gaine isolante, ce câblage se présente en version blindée STP (STP : Signal Mode Fibre) et non blindée UTP (UTP : Unshieldtwinted Pair)

• **Câble coaxial :** c'est un câble à deux conducteurs permet de transmettre des signaux hautes fréquences, son débit peut atteindre 10 Mb /s sur une distance de 1 Km, toute en limitant les interférences.

• **Fibre optique :** Les réseaux de fibre optique utilisent des signaux optiques pour conduire l'information, ils sont chargés de transporter les signaux au travers de fibre de verre ou de plastique.

♦ **Types de prises :**

• **RJ45 (Registered Jack) :** Elle est utilisée pour les câbles à paires torsadées, ce qui permet de connecter divers appareils de communication entre eux. RJ45 existe principalement dans la connexion Ethernet [5].

• **Prise SC (simplex préchargés) :** Elle est conçue pour amener la fibre optique dans les bureaux et est déployé dans les immeubles de grande hauteur. Ces prises peuvent fournir jusqu'à 4 ports d'adaptateurs LC, SC, ST, FC, ces adaptateurs sont préinstallés dans la prise murale [5].

• **BNC (Bayonet Neill–Concelman) :** Utilisé pour la terminaison de câbles coaxiaux, en particulier dans le domaine des radiofréquences. Facile à utiliser et rapide à installer. Pour plus de simplicité, le même type de prises est installé dans le bureau et le local technique [5].

1.2.7 Architectures des réseaux informatiques

L'architecture de réseau fait référence à la conception d'un réseau, englobant à la fois ses composants physiques et logiques. Elle implique la sélection et l'agencement des dispositifs, des protocoles et des technologies de réseau pour répondre à des exigences spécifiques.

◦ **Architecture poste à poste (Peer to Peer) :**

Dans cette architecture les dispositifs individuels reliés directement entre eux, ayant des responsabilités et des pouvoirs égaux sans la présence d'une autorité centrale Chaque ordinateur dispose de droits spéciaux pour le partage des ressources, Utile dans les environnements plus petits avec un nombre réduit d'ordinateurs.

♦ **Avantages du réseau pair à pair :**

• aucun appareil n'est client ou serveur, les tâches et les responsabilités des serveurs sont réparties entre tous les appareils, qui agissent également en tant que clients.

• Il est très peu coûteux à mettre en place, car il n'est pas nécessaire de disposer d'un serveur

centralisé, ce qui garantit également qu'en cas de défaillance du réseau, tous les appareils non affectés continuent à fonctionner normalement.

• Il est simple à mettre en place et à entretenir car chaque ordinateur fonctionne de manière indépendante.

♦ **Inconvénients du réseau pair à pair :**

• Il n'y a pas de système centralisé et il est donc difficile de conserver une copie de sauvegarde des données en cas de défaillance.

• Il présente une faille de sécurité car les ordinateurs sont autogérés.

• Avec l'augmentation du nombre de machines sur ce réseau, les performances, la sécurité et l'accès peuvent devenir des problèmes majeurs

◦ **Architecture Client-Serveur :**

Cette architecture est également connue sous le nom d'architecture centralisée, car un ordinateur central puissant est chargé de répondre à toutes les demandes des ordinateurs clients. Cet ordinateur central est un serveur. Les ordinateurs clients se connectent au serveur lorsqu'ils ont besoin d'utiliser des ressources ou des données partagées. Toutes les données partagées sont stockées uniquement sur le serveur, et non sur un autre ordinateur. Le serveur s'occupe de toutes les tâches essentielles, telles que la sécurité et l'administration du réseau. Tous les clients interagissent entre eux par l'intermédiaire d'un serveur.

♦ **Avantages de l'architecture client-serveur :**

• Ce type d'architecture est beaucoup plus facile à faire évoluer car il est beaucoup plus pratique d'ajouter des ordinateurs serveurs que de configurer le réseau sur chaque ordinateur (comme c'est le cas dans l'architecture poste-à poste).

• Les vitesses de réseau sont beaucoup plus rapides.

• Comme un seul serveur gère les ressources partagées dans un réseau client/serveur, la sécurité est améliorée.

• La sauvegarde des données est facile grâce au système centralisé.

♦ **Inconvénients de l'architecture client-serveur :**

• Elle est plus sujette aux pannes, car si le serveur tombe en panne, aucune des machines clientes n'est en mesure de répondre à ses demandes.

• Nécessité d'un administrateur de réseau dédié pour gérer toutes les ressources

FIGURE 1.11 – Architecture poste à poste Vs Architecture Client-Serveur

1.2.8 Modèles de communication OSI et TCP/IP

Les modèles de communication OSI et TCP/IP sont essentiels pour comprendre le fonctionnement des réseaux informatiques. Le modèle OSI, élaboré par l'Organisation internationale de normalisation (ISO), fournit un cadre théorique en sept couches distinctes, chacune ayant des responsabilités spécifiques pour faciliter l'interopérabilité entre différents systèmes informatiques. Le modèle TCP/IP, quant à lui, est plus pragmatique et se compose de quatre couches. Il a été développé pour répondre aux besoins d'Internet et est largement utilisé en raison de sa simplicité et de son efficacité. Ces deux modèles offrent une structure hiérarchique pour analyser et concevoir des réseaux informatiques, et bien que différents dans leur approche, ils se complètent mutuellement pour offrir une compréhension complète des processus de communication en réseau.

1.2.8.1 Modèle OSI (Open System Interconnection)

Le modèle OSI (Open Systems Interconnection) : est un cadre conceptuel utilisé pour décrire les fonctions d'un système de réseau. Il a été créé par l'Organisation internationale de normalisation (ISO) pour faciliter l'interopérabilité entre différents systèmes informatiques [6].

L'objectif principal du modèle OSI est de fournir une structure hiérarchique pour comprendre le fonctionnement des réseaux informatiques en décomposant le processus de communication en différentes couches distinctes, chacune ayant des responsabilités spécifiques [7].

♦ **La Couche Application :** La couche la plus élevée interagit directement avec les applications logicielles et les utilisateurs finaux. Elle fournit des services de réseau aux applications et permet aux interfaces utilisateur d'accéder aux ressources du réseau.

♦ **Couche de présentation :** Responsable de la traduction, du cryptage et de la compression des données, cette couche garantit que les données sont présentées dans un format lisible que les applications peuvent interpréter.

♦ **Couche session :** La couche session établit, maintient et termine les connexions entre les applications. Elle gère les sessions, ce qui permet la synchronisation et le contrôle du dialogue entre les appareils.

♦ **Couche transport :** Cette couche gère la communication de bout en bout et garantit l'intégrité des données elle fournit des mécanismes de vérification des erreurs et des contrôles du flux de données. Elle détermine la quantité de données à envoyer, l'endroit où elles sont envoyées et le débit. Le protocole TCP est le plus connu de cette couche .

♦ **Couche réseau :** La couche réseau se concentre sur l'acheminement des paquets de données de la source à la destination à travers plusieurs réseaux. Elle traite de l'adressage logique et des protocoles de routage.

♦ **Couche liaison de données :** d'un programme gère l'entrée et la sortie des données d'une liaison physique dans un réseau. Cette couche gère les problèmes résultant des erreurs de transmission de bits. Elle veille à ce que le rythme du flux de données ne surcharge pas les dispositifs d'envoi et de réception. Cette couche permet également la transmission des données à la couche 3, la couche réseau, où elles sont adressées et acheminées elle est divisée en deux sous couche LLC et MAC.

♦ **Couche physique :** Cette couche traite de la connexion physique entre les appareils. Elle transporte les données à l'aide d'interfaces électriques, mécaniques ou procédurales. Elle est responsable de l'envoi des bits informatiques d'un appareil à l'autre le long du réseau. Elle détermine comment les connexions physiques au réseau sont établies et comment les bits sont représentés en signaux prévisibles.

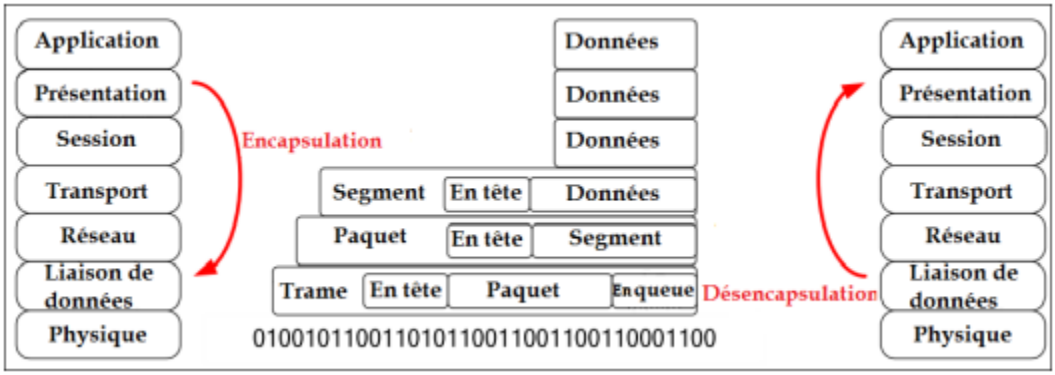

FIGURE 1.12 – Modèle OSI [8]

1.2.8.2 Modèle TCP/IP

Contrairement au modèle OSI qui est plus théorique et complexe, Le modèle TCP/IP est plus simple et plus facile à mettre en œuvre développer spécialement pour répondre aux besoins

d'Internet, Ce modèle est plus compatible avec les réseaux existants et a permis une transition plus fluide vers les nouvelles technologies de communication.

♦ **Couche Application :** est la couche la plus élevée du modèle TCP/IP. Elle fournit des interfaces pour les applications utilisateur afin d'accéder au réseau. Cette couche est responsable de la présentation des données à l'utilisateur et de la communication avec les services réseau. Elle comprend des protocoles tels que HTTP, SMTP, FTP et DNS.

♦ **Couche Transport :** est responsable de l'établissement, du maintien et de la terminaison des connexions entre les applications sur des machines différentes. Elle fournit des services de communication fiables (TCP) et non fiables (UDP) aux applications. Elle garantit également le contrôle de flux et de congestion. Les protocoles les plus couramment utilisés dans cette couche sont TCP et UDP .

♦ **Couche Internet :** est responsable de l'acheminement des paquets de données à travers le réseau. Elle utilise des adresses IP pour identifier les hôtes et les réseaux, ainsi que des protocoles de routage pour diriger les paquets vers leur destination. Cette couche comprend le protocole IP (Internet Protocol) et des protocoles de routage tels que BGP (Border Gateway Protocol) et OSPF (Open Shortest Path First).

♦ **Couche Accès Réseau :** est responsable de l'encapsulation des données en trames et de la gestion de l'accès au support physique du réseau. Elle garantit la fiabilité de la transmission des données sur des liaisons physiques spécifiques. Cette couche comprend des protocoles tels qu'Ethernet, PPP et Wi-Fi .

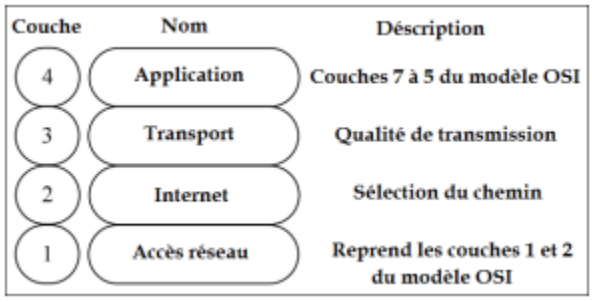

FIGURE 1.13 – Modèle TCP/IP [8]

1.2.9 Différents types de protocoles

Les protocoles de communication sont essentiels pour permettre l'échange de données entre différents dispositifs au sein d'un réseau. Ils définissent un ensemble de règles, de conventions et de normes pour assurer une communication efficace et fiable. Chaque protocole remplit une fonction spécifique, allant de la résolution d'adresses, à la transmission de données, en passant par le diagnostic et la gestion des réseaux. Dans cette section, nous allons explorer les principaux protocoles

utilisés dans les réseaux informatiques, en mettant en lumière leurs rôles et leurs caractéristiques distinctives.

♦ **Le Protocole ARP (Adress Resolution Protocol) :** est un protocole de couche 2 utilisé pour faire la correspondance entre une adresse de niveau réseau et une adresse physique. Lors d'une demande de ARP, l'adresse de destination et l'adresse de diffusion (broadcast) font de sorte à ce que tout le réseau reçoit la demande, En revanche seule la machine possède l'adresse IP précise dans la demande, répond en fournissant son adresse MAC. Cela est utilisé par exemple lorsqu'une machine cherche une adresse IP devant serveur DHCP.

♦ **Le protocole IP(internet Protocol)** : est un protocole de communication utilisé pour la transmission de données sur Internet. Il est conçu pour permettre l'adressage unique et l'acheminement des paquets de données entre les ordinateurs sur le réseau Internet. Le protocole IP fait partie de la couche Internet de la suite de protocoles TCP/IP. Il n'est pas orienté connexion, c'est à dire qu'il n'est pas fiable, cela signifie qu'il n'offre aucune garantie que les paquets envoyés arrive à la destination avec aucune perte. Mais cette fiabilité dépend de la couche de transport.

♦ **Protocole ICMP (Internet Control Message Protocol) :** est un protocole de la couche réseau utilisé pour diagnostiquer les problèmes et échanger des informations opérationnelles entre les appareils du réseau, tels que les routeurs. Il est utilisé pour envoyer des messages d'erreur et des informations indiquant le succès ou l'échec de la communication avec une autre adresse IP. Contrairement aux protocoles de transport comme TCP et UDP, ICMP n'est généralement pas utilisé pour échanger des données entre les systèmes, mais plutôt pour des fonctions de contrôle et de diagnostic.

♦ **Protocole UDP (User Datagram Protocol) :** est un protocole de couche transport simple sans connexion, utilisé pour l'échange des données entre deux processus. L'UDP est idéal pour des applications où la rapidité est primordiale et où la perte occasionnelle de données est acceptable mais il n'offre aucune garantie de livraison des paquets à leur destination.

♦ **Le Protocole TCP (Transmission Control Protocol) :** est un protocole de couche transport fonctionne en mode connecté .il offre une communication fiable en garantissant que toutes les données reçues sont identiques et dans le même ordre. Il utilise un mécanisme d'acquittement positif avec retransmission pour assurer la transmission sans erreur des données.

♦ **Protocole DHCP (Dynamic Host Configuration Protocol) :** est protocole de couche application qui permet d'attribuer les adresse IP d'une façon automatique dans un réseau ce qui permet à l'utilisateur de ce réseau de communiquer avec n'importe quel autre utilisateur d'internet .

♦ **DNS (Domaine Name System) :** est system qui permet de faire la correspondance entre le nom de domaine et une adresse IP Le DNS utilise un réseau de serveurs pour faire ces traductions et rendre la navigation sur Internet plus simple.

♦ **Protocole HTTP (HyperText Transfer Protocol) :** est un protocole de couche application permet d'établir un dialogue entre le client web et le serveur web, en envoyant des requêtes http. Ce protocole est indépendant du média cela veut dire qu'il est utilisable avec n'importe quel type de données.

♦ **FTP (File Transfer Protocol) :** est un protocole de couche application qui permet le transfert des fichiers, il établit deux connexions entre client et serveur, l'une pour les informations de contrôle et l'autre pour les données à transférer. L'authentification doit d'abord être effectuée au moyen de la validation du nom d'utilisateur et du mot de passe.

♦ **Protocole POP3 (Post Office Protocol version 3) :** est un protocole Internet standard de couche d'application utilisé pour la récupération du courrier électronique. POP3 permet aux utilisateurs de se connecter à un serveur TCP/IP pour collecter des courriels, en utilisant le port 110. Il permet aux utilisateurs de consulter les courriels reçus lorsqu'ils ne sont pas en ligne, en s'authentifiant à l'aide d'un identifiant et d'un mot de passe.

♦ **TELNET (Telnet Network Protocol) :** est un protocole de couche application qui permet à un utilisateur de communiquer avec un périphérique distant.il est connu pour être vulnérable à des attaques en raison de son manque d'authentification et de sécurité. Les données transmises via Telnet ne sont pas cryptées,

♦ **SSH (Secure Shell) :** est un protocole qui joue le même rôle que Telnet. La principale différence entre SSH (Secure Shell) et Telnet sont la sécurité et la manière dont ils transmettent les données. SSH utilise un cryptage de bout en bout pour protéger les données transmises, ce qui rend les communications entre un client et un serveur très difficile à intercepter et à lire.

1.3 Conclusion

Dans ce chapitre nous avons présenté le réseau informatique d'une façon générale, nous avons cité les critères basiques qui montrent le rôle d'un réseau informatique, pour l'objectif de bien définir le concept de supervision d'un réseau. Le chapitre suivant sera consacré pour la présentation générale de la supervision des réseaux informatique .

Chapitre 2

Supervision des réseaux informatiques

2.1 Introduction

La complexité croissante des réseaux informatique, associée à la diversité des appareils et des protocoles, a rendu leur gestion et leur surveillance indispensables. La supervision des réseaux informatiques est donc devenue un aspect crucial de la gestion informatique, visant à garantir la disponibilité, la performance et la sécurité des infrastructures réseau .

Ce chapitre explorera les principes fondamentaux de la supervision des réseaux informatiques, en mettant en lumière ses objectifs et ses concept fondamentaux .

2.2 Administration des réseaux informatiques

L'administration de réseau a trait à l'ensemble des activités permettant d'assurer le bon fonctionnement du réseau à distance afin qu'il livre les services attendus. Elle englobe la configuration, la surveillance et la gestion des performances du réseau, la collecte de données à partir des dispositifs du réseau et la fourniture d'un contrôle fin sur les opérations des dispositifs. : le protocole SNMP(Simple Network Management Protocol) est actuellement la technologie de base qui permet d'administrer un réseau TCP/IP.

2.2.1 Architecture d'administration et principe général

Une architecture classique d'administration se repose sur le modèle Gérant/Agent (Manager/Agent). Le système se compose [8] :

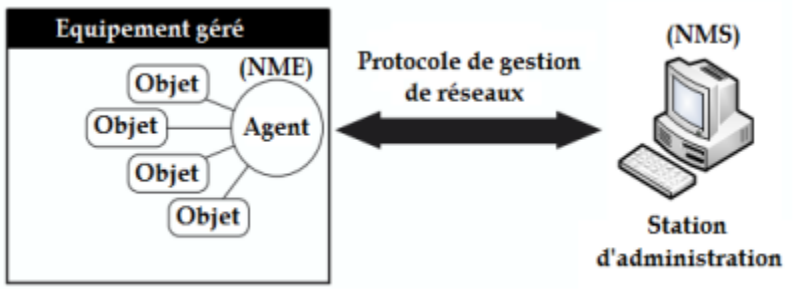

FIGURE 2.1 – Composants du système de gestion réseau

• D'une entité d'administration NMS (Network Management System) qui est le gérant. Constitué d'un ensemble de logiciels et d'outils conçus pour faciliter la gestion du réseau.

• Des entités de gestion NME (Network Management Entity) appelés agents qui sont gérées par le NMS.

• Un protocole pour la gestion.

♦ **Principe général :**

Un système de réseau informatique se compose d'un ensemble d'objets (ces objets et les informations relatives sont stockés dans des bases de données MIB) qu'un système d'administration surveille et contrôle (via un protocole de gestion reposant sur UDP) grâce à un processus appelé manager ou gérant. Pour ce faire, chaque objet est géré localement par un processus appelé agent qui en effet transmet régulièrement ou sur sollicitation les informations de gestion relatives à son état et aux événements qui le concernent au manager.

Le principe se repose donc sur les échanges :

- D'une part : entre une MIB (Management Information Base) et l'ensemble des éléments administrés.

-D'autre part : entre les éléments administrés et le système d'administration.

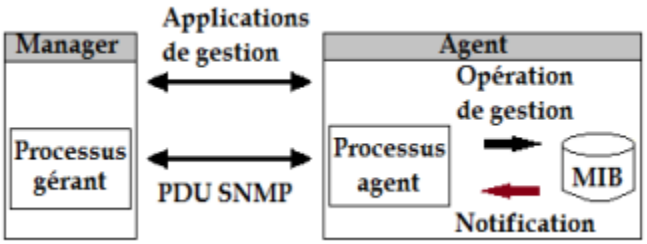

FIGURE 2.2 – Structure fonctionnelle d'administration

De ce fait, on peut modéliser l'architecture d'un système d'administration par :

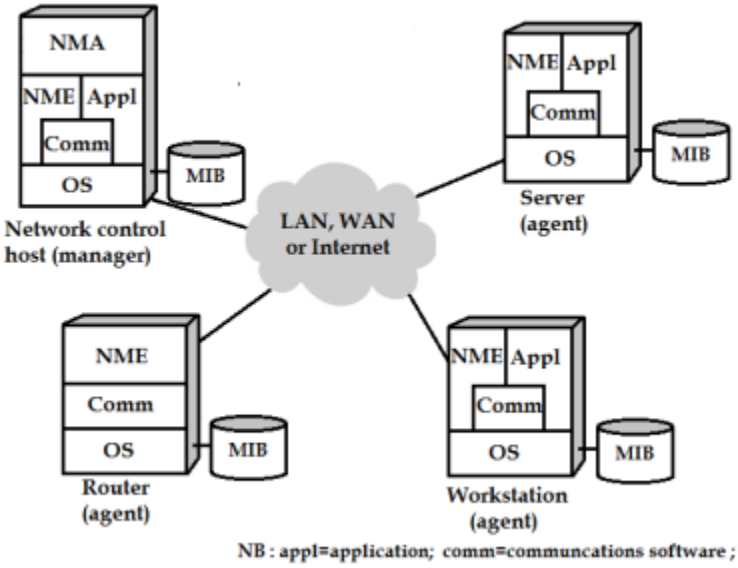

FIGURE 2.3 – Architecture de système de gestion réseau

Remarque : L'entité d'administration a sa propre entité de gestion NME (Network Management Entity) et aussi un logiciel pour gérer le réseau appelé NMA (Network Management Application) contenant une interface via laquelle les activités d'administration sont effectuées.

2.2.2 Activités d'administration des réseaux

L'ISO (International Standard Organizations) a regroupé les activités d'administration de réseaux en cinq domaines fonctionnels [9].

♦ **Gestion de configuration :** permet de designer et de paramétrer différents objets, la collecte d'informations, le contrôle de l'état du système, et la sauvegarde de l'état dans un historique.

♦ **Gestion des anomalies :** des techniques et processus visant à détecter, réparer et corriger les problèmes réseaux et de conserver un enregistrement du processus de résolution dans une base de données.

♦ **Gestion de performances :** elle consiste à collecter régulièrement des statistiques sur la qualité du service réseau et puis les analyser afin d'atteindre les objectifs de performance souhaités.

♦ **Gestion de comptabilité :**vise à recueillir des informations sur l'utilisation du réseau pour la refacturation ou le suivi de la consommation des différents services ou secteurs d'activité.

♦ **Gestion de sécurité :** combine plusieurs couches de défense, des politiques strictes d'accès aux ressources, une surveillance proactive et des outils avancés pour protéger les réseaux contre les menaces croissantes et garantir l'intégrité des données et des systèmes.

Ces activités sont communément classées selon la façon suivante :

• **Supervision :** consiste à surveiller, et collecter toutes sortes d'informations.

• **Gestion :** consiste à gérer le réseau (gestion configurations, ressources, sécurité, dysfonctionnement, les remontées d'alarmes et leurs rapports...).

• **Exploitation :** consiste à traiter les problèmes opérationnels sur le réseau (maintenance, assistance technique...).

2.3 Supervision des réseaux informatiques

Ensembles de moyens consistant à surveiller et visualiser les systèmes et à récupérer des informations sur leur état et leur comportement pour détecter des problèmes tels que la lenteur du trafic ou la défaillance d'un composant. Ce processus est essentiel pour maintenir l'intégrité du réseau et prévenir les temps d'arrêt en identifiant les anomalies de manière proactive.

2.3.1 Objectifs de la supervision

Pour que la supervision du réseau soit efficace, différentes orientations doivent être décrites.

• Assurer la disponibilité des continu des services.

• Prévenir les pannes en détectent les anomalies .

• Optimiser les performances des réseaux.

• Assurer le bon fonctionnement du système .

• Améliorer la gestion de système.

• Renforcer la sécurité de réseau.

• Réduction des couts de maintenance.

2.3.2 Types de la supervision

♦ **Supervision system :** La supervision des systèmes informatiques se concentre principalement sur trois types principaux de ressources matérielles : le processeur, la mémoire et d'autres composants essentiels. Elle vise à garantir le bon fonctionnement, la disponibilité et la sécurité de ces ressources [10].

♦ **Supervision réseau** : elle porte sur la surveillance de manière continue de la disponibilité des services en ligne du fonctionnement, des débits, de la sécurité mais également du contrôle des flux [10].

♦ **Supervision des applications :** Porte sur la vérification de l'accessibilité, du bon fonctionnement et de la réactivité des applications utilisées dans l'entreprise [10].

2.3.3 Architectures de la supervision

En fonction de la topologie du réseau sur laquelle SNMP (Simple Network Management Protocol) est implémenté, plusieurs types d'architectures peuvent être définis pour superviser les agents.

♦ **Architecture centralisée :** Dans cette architecture, toutes les opérations de supervision sont gérées par un seul serveur de gestion centralisé (station d'administration (NMS)). Les agents SNMP sont configurés pour envoyer des informations de gestion à ce serveur central. Cela simplifie la configuration et la gestion, mais peut entraîner des goulets d'étranglement en cas de trafic réseau important ou de défaillance du serveur central.

♦ **Architecture hiérarchisée :** Cette architecture divise le réseau en domaines de gestion plus petits, chaque domaine ayant son propre serveur de gestion. Les informations de gestion peuvent être remontées à des niveaux supérieurs de la hiérarchie pour une vue d'ensemble du réseau. Cela permet une gestion plus distribuée et évolutive, mais nécessite une planification soignée pour éviter les problèmes de cohérence et de gestion des données.

♦ **Architecture distribuée :** c'est un type de d'architecture ou il existe plusieurs stations d'administration autonomes et ayant une responsabilité égale. Chaque station d'administration possède sa propre base MIB qu'elle gère et met à jour.

2.3.4 Modes de la supervision

il existe deux modes de supervison , en temps réel et en temps différé :

Caractéristiques	**Supervision en Temps Réel**	**Supervision en Temps Différé**
Définition	Données collectées et analysées instantanément.	Données collectées et analysées après coup.
Fonctionnement	Surveillance continue avec alertes immédiates en cas de problème.	Données enregistrées pour analyse à intervalles définis ou sur demande.
Avantages	- Une intervention rapide et efficace. - Prise de décision rapide. - Prévention des pannes avant qu'un problème ne devienne critique.	- Moins de charge réseau. - Analyse approfondie. - Moins de fausses alertes.
Limitations	- Charge réseau supplémentaire. - Complexité de gestion. - Nécessite des investissements importants en termes de matériel.	- Délai de réaction. - Risque de manquer des problèmes critiques. - Moins adapté aux environnements dynamiques.

Tableau 2.1 – Modes de la supervision

2.3.5 Méthodes de la supervision

Les principales méthodes de supervision sont les suivantes [8] :

♦ **Les fichiers log :** sont des enregistrements détaillés d'événements qui se produisent au sein d'un système informatique. Ils peuvent contenir des informations sur les erreurs, les alertes, les transactions et les activités des utilisateurs.

L'analyse des fichiers log peut se faire de deux manières :

• Consultation manuelle : Les administrateurs système consultent les fichiers log pour identifier les problèmes en utilisant des outils comme tail, grep ou des éditeurs de texte.

• Remontée automatique : Des outils de surveillance analysent automatiquement les fichiers log , en utilisant des solutions comme Splunk, et Graylog.

♦ **Récupération des résultats de commandes et de scripts locaux ou distants :** Cette méthode implique l'exécution de commandes et de scripts pour collecter des informations sur l'état du système ou du réseau. Les scripts peuvent être exécutés localement pour collecter des métriques telles que l'utilisation du CPU, la mémoire, l'espace disque, etc. . ou à distance via des protocoles comme SSH ou telnet.

♦ **Le protocole SNMP (Simple Network Management Protocol) :** standard pour la gestion des dispositifs réseau, permet de superviser et contrôler divers équipements grâce à une communication entre un manager SNMP et des agents SNMP sur les dispositifs.

Remarque : En fonction des besoins spécifiques de l'organisation, des ressources disponibles et de la criticité du réseau, l'une ou l'autre méthode de supervision peut être préférable. Une combinaison des deux approches peut également être utilisée pour obtenir une vue complète et équilibrée de la santé du réseau.

2.4 Protocole de gestion de réseau dans le modèle TCP/IP : SNMP

SNMP (Simple Network Management Protocol) est un protocole de communication de la couche d'application de modèle OSI. Il s'appuie sur le protocole de télécommunication UDP. Le paquet UDP est encapsulé dans un paquet IP et permet de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseau et matériels à distance. C'est l'un des protocoles les plus utilisés pour la gestion (management, monitorage) des réseaux [8].

SNMP (Simple Network Management Protocol) est utilisé pour [8] :

• Administrer les équipements et échanger des éléments de configuration.

• Surveiller le comportement des équipements et les performances réseaux.

• Modifier le paramétrage de certains composants.

SNMP fonctionne sur un modèle client-serveur. Le client correspond à le Manager. Les serveurs correspondent aux agents SNMP qui enregistrent en permanence des informations les concernant dans leur MIB. La station interroge les MIB des différents agents pour récupérer les informations qu'elle souhaite.

Toutefois, il y'a deux modes de fonctionnement [8] :

Le polling : C'est un processus par lequel le gestionnaire SNMP envoie périodiquement des requêtes aux agents SNMP pour obtenir des informations sur l'état et les performances des périphériques réseau.

Les traps SNMP : où l'équipement remonte lui-même une alarme afin de signaler une anomalie au superviseur.

2.4.1 Concepts fondamentaux de protocole SNMP

Le protocole SNMP (Simple Network Management Protocol) est un élément clé de la gestion des réseaux informatiques, offrant un cadre standardisé pour la surveillance et le contrôle des équipements réseau. Les principaux composants de SNMP comprennent les stations d'administration (NMS), les agents de gestion, les communautés, les alarmes, les objets, les MIB et les proxies. Ces éléments interagissent pour permettre la collecte d'informations sur les performances, la configuration et les événements des équipements réseau, ainsi que la gestion proactive de ces ressources.

2.4.1.1 Station d'administration (NMS-Network Management Station)

Une station de gestion de réseau (NMS) est l'entité principale utilisée par l'administrateur réseau pour surveiller et gérer son infrastructure. Elle dispose généralement d'une entité logicielle appelé "manager", qui agit en tant que client. Le rôle du manager est d'envoyer des requêtes aux agents SNMP présents sur les équipements du réseau afin de collecter des informations sur leur état et leur performance.

Le manager SNMP doit également agir en tant que serveur, car il doit être capable de recevoir des alertes émises par les agents SNMP en cas de problèmes ou d'événements importants sur le réseau. Ces alertes sont envoyées par les agents vers le manager sur le port UDP 162, et le manager doit donc rester à l'écoute de ce port pour les recevoir. Une NMS doit obligatoirement posséder [11] :

- Un ensemble de logiciels appelés l'application d'administration réseau (NMA).
- La NMA comporte une interface utilisateur permettant aux administrateurs autorisés de gérer le réseau.
- La capacité à récupérer des informations des éléments administrés .

- La NMA comporte une interface utilisateur permettant aux administrateurs .
- Une base de données obtenue à partir des MIB des éléments administrés :

2.4.1.2 Agent de gestion

Chaque équipement que l'on voudra "manager" à distance devra disposer d'un agent SNMP, C'est-à-dire une application de gestion résidant dans un périphérique et chargée de transmettre les données locales de gestion de celui-ci au format SNMP. Cet agent est un serveur, qui reste à l'écoute du port UDP 161 pour des requêtes provenant de l'administrateur. L'agent devra éventuellement pouvoir agir sur l'environnement local, si l'administrateur souhaite modifier un paramètre. Par ailleurs, l'agent SNMP pourra émettre des alertes de sa propre initiative, s'il a été configuré pour ça. Un agent assume ainsi les travaux ci-dessous [11] :

- Collecter des informations statistiques concernant la communication, et les opérations de réseau.
- Stocker les informations localement dans les MIB.
- Répondre aux commandes de la station d'administration, inclus : Transmet des informations statistiques à l'entité d'administration, modifie les paramètres...[11].

2.4.1.3 Communautés

Sont des chaines de texte utilisé pour l'authentification et l'autorisation entre manager et les agents SNMP [11].

La sécurité de SNMPv1 est basée sur des noms de communautés qui sont utilisés comme des mots de passe pour accéder à une arborescence de données de l'équipement appelée MIB. Cette version n'étant pas sécurisée car le nom de la communauté transmis en clair dans le message SNMP le protocole SNMP a ainsi évolué en une deuxième, SNMPv2. La sécurité de cette version est encore faible car elle utilise l'algorithme MD5 (message Digest5) pour hacher les noms de communautés La sécurité a été étudier plus en avant avec SNMP v3, qui intègre des mécanismes de vérification d'intégrité des messages et d'authentification avec des algorithmes de hachage et de chiffrement [11].

2.4.1.4 Alarmes

Il est possible de demander (en configurant) aux stations d'émettre de temps en temps un rapport, cela fait par les alarmes qui ce sont des notifications ou des alertes générées par les équipements réseau ou les systèmes de supervision pour signaler des événements importants, des anomalies ou des problèmes qui se produisent dans le réseau[11].

2.4.1.5 Objets

Dans SNMP, un objet peut être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres variables qui sont directement liés au comportement en cours de l'équipement. Les objets sont classés dans une sorte de base de données appelée MIB. Chaque objet est identifié par un OID (Object IDentifier) qui est une séquence numérique qui définit son emplacement unique dans la MIB [11].

2.4.1.6 MIB (base d'informations de gestion)

La MIB se présente comme une base de données normalisée d'objets, qui permettra de lire et d'écrire sur les équipements distants. Chaque MIB est propre à l'agent. Il Ya donc une MIB pour chaque équipement supervisé [11].

♦ **Structure d'une MIB :**

Est une base de données organisée de manière hiérarchique, suivant une structure d'arbre.

• Chaque nœud de l'arbre représente un objet de gestion spécifique. Cet objet est défini avec un OID.

• La racine de l'arbre MIB est le point de départ de la hiérarchie. Elle est désigné par OID nœud unique avec un l'OID « iso.org.dod.internet » (ou « 1.3.6.1 »).

• A partir de nœud racine, la MIB se divise en plusieurs branches principales, chacune représente une catégorie spécifique d'objet telle que « system », « interface » ...

• Chaque branche de la MIB se divise en sous-branches et enfin en nœuds feuilles, qui représente les objets de gestion réels telle que le nom d'hôte.

• Une MIB contient un ensemble d'informations standards, c'est la MIB standard. Or pour la plupart des éléments réseaux, on rajoute un certain nombre d'objet propre à un agent pour en exploité les possibilités : c'est la MIB privée.

• La MIB est un fichier texte écrit en langage ASN 1(Abstract Syntaxe Notation 1).

Remarque :

SMI (Structure of Management Information) est une syntaxe qui spécifie comment les données (objets SNMP) sont représentées via ASN.1 (décrit pour chaque objet (avec un OID, une syntaxe, un encodage) [11].

♦ **Représentation d'une MIB (Structure et représentation d'objets) :**

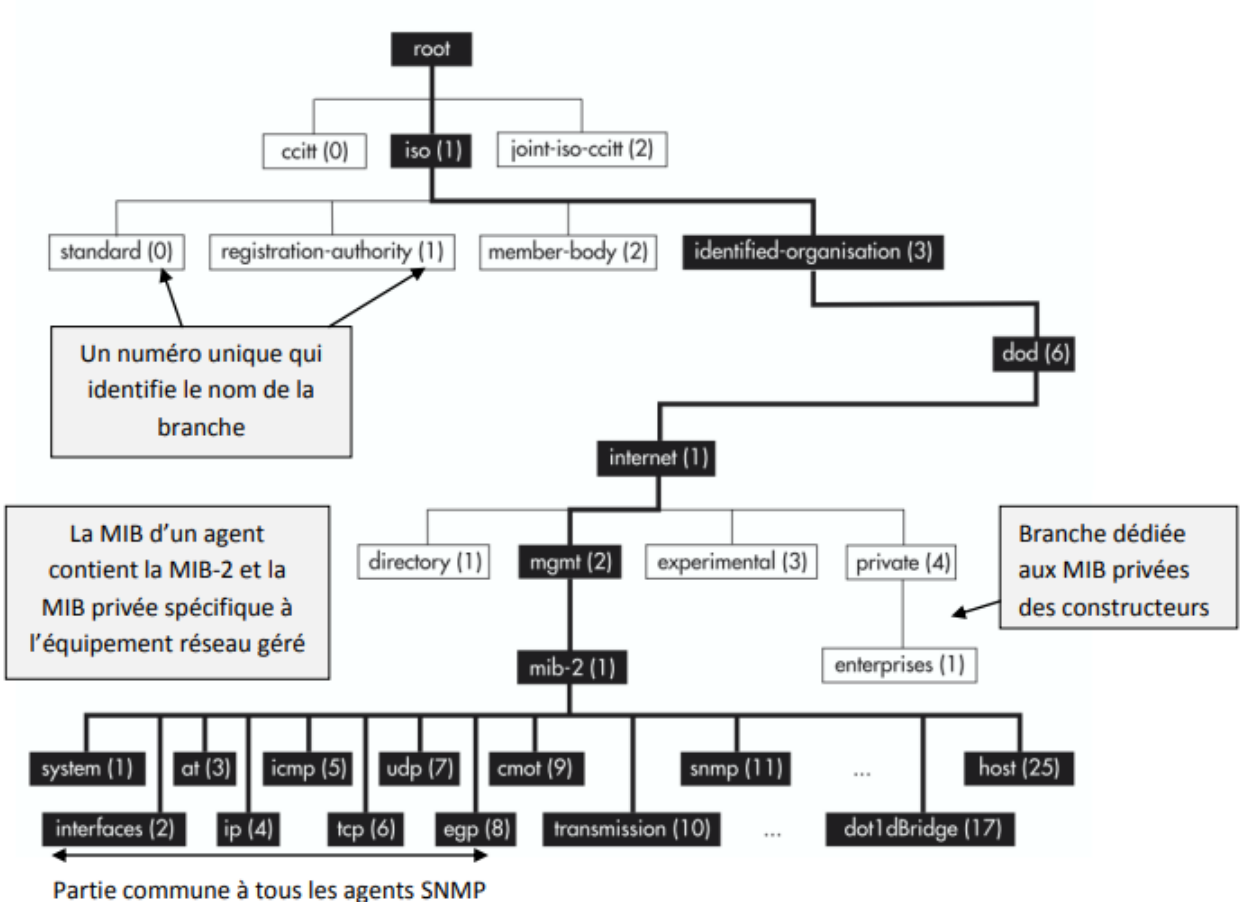

FIGURE 2.4 – Structure de MIB [11]

♦ **Description :** [11]

- **iso(1)** : branche qui définit La gestion de réseau. Dans cette branche on trouve un certain nombre de définitions d'organisations subordonnées. La gestion de réseau entre dans le nœud **identified-organisation(3)**.

- Sous le nœud **dod(6)** se trouvent un certain nombre de réseaux subordonnés. La gestion de réseau entre dans le nœud **internet(1)**.

- Sous le nœud internet(1) se trouvent un certain nombre de nœuds subordonnés représentant différents services et tentatives de normalisation. La gestion de réseau standardisée se trouve dans le réseau **mgmt(2)**.

- Sous le nœud mgmt(2) se trouvent un certain nombre de nœuds subordonnés représentant différents services et tentatives de normalisation. La gestion de réseau standardisée se trouve dans le nœud **mib-2(1)**.

- Sous le nœud mib-2(1) se trouvent un certain nombre de nœud subordonnés représentant différents groupement de variables MIB, Ce sont des tables contenant les informations de l'élément du réseau. Ce qu'on appel Les tables MIB, on y trouve :

• Groupe « System » : Informations génériques de configuration.

• Groupe « Interfaces » : Informations concernant les interfaces (type, adresse, nombre d'octets in/out, statut,) .

• at (adress translation) ou Groupe « ARP » : Liaison Adresse Physique – Adresse logique.

• Groupe « IP » : Informations sur le niveau IP (TTL, forwarding ?, tables de routage, nombre de paquets, d'octets, de "forward"...) .

• Groupe « ICMP » : Informations statistiques sur les messages ICMP (Nombre de messages, de messages Echo, ...).

• Groupe « TCP » : Informations sur les connexions TCP (connexions en cours, nombre de messages, de circuits ouverts, TTL, ...) .

• Groupe « UDP », « EGP », « SNMP » ... Remarque : mib-2 est une base d'objets commune à tous les équipements. Correspond à des informations TCP/IP.

2.4.1.7 Proxies SNMP

L'utilisation de SNMP est basée sur le principe que tous les agents réseau prennent en charge un protocole commun, tel que UDP et IP Cependant, dans certaines situations, il peut être nécessaire de surveiller des équipements qui ne prennent pas en charge TCP/IP ou qui n'ont pas d'agent SNMP. Pour répondre à ce besoin, des proxies SNMP peuvent être utilisés pour traduire les données entre le format utilisé par l'agent de supervision privée de l'équipement et le format SNMP compréhensible par le superviseur SNMP. L'utilisation de ces proxies permet ainsi à SNMP

de s'adapter facilement à des réseaux très hétérogènes et prouve la grande flexibilité de ce protocole [11].

2.4.1.8 Messages SNMP

Pour interroger une MIB, le superviseur (NMS) dispose des commandes suivantes, ces commandes sont envoyées via SNMP Il existe trois messages SNMP différents les requêtes, les réponses et les alarmes (trapes).

♦ Les requêtes SNMP sont les suivantes [11] :

- GetRequest : recherche d'une variable sur un agent.

- GetNextRequest : recherche la variable suivante.

- GetBulk Request : recherche un ensemble de variables regroupées.

- SetRequest : change la valeur d'une variable sur un agent.

♦ L'agent répond aux requêtes par un message GetResponse. En cas d'erreur, le message sera accompagné d'un des codes d'erreurs suivants [11] :

✓ :NoAccess : accès non autorisé.

✓WrongLength : erreur de longueur.

✓WrongValue : erreur de valeur.

✓WrongType : erreur de type.

✓WrongEncoding : erreur d'encodage.

✓NoCreation : objet inexistant.

✓ReadOnly : seule la lecture est autorisée.

✓NoWritable : interdiction d'écrire.

✓AutorisationError : erreur d'autorisation.

♦ Les alarmes sont envoyées par l'agent lorsqu'un événement survient sur la ressource monitorée. Ce dernier informe le manager via une « trap ». Pour chaque envoi de messages, une réponse est retournée à l'exception de la commande « trap ». Les réponses sont du type suivant [11] :

✓ColdStart (0) : redémarrage du système à froid.

✓WarmStart (1) : redémarrage du système à chaud.

✓LinkDown (2) : le lien n'est plus opérationnel.

✓LinkUp (3) : le lien est à nouveau opérationnel.

✓AuthentificationFailure (4) : Tentative d'accès à l'agent avec un mauvais nom de communauté.

✓EgpNeighborLoss (5) : la passerelle adjacente ne répond plus.

✓EntrepriseSpecific (6) : alarme spécifique aux entreprises.

2.5 Solution de supervision

Les solutions de supervision informatique jouent un rôle essentiel dans la gestion efficace des infrastructures technologiques modernes. Elles offrent aux organisations la capacité de surveiller en temps réel les performances, la disponibilité et la sécurité de leurs réseaux, serveurs, applications et services. En fournissant une visibilité complète sur l'état de l'environnement informatique, ces solutions permettent aux équipes informatiques de détecter rapidement les problèmes potentiels, de diagnostiquer les causes sous-jacentes et d'y remédier avant qu'ils n'affectent leur opération. Qu'il s'agisse de solutions open-source telles que Nagios, Zabbix ou commerciales telles que Splunk, Orion Platform. Les organisations peuvent choisir parmi une gamme diversifiée d'outils de supervision pour répondre à leurs besoins spécifiques en matière de surveillance et de gestion des performances informatiques. En fin de compte, ces solutions contribuent à améliorer l'efficacité opérationnelle, à réduire les temps d'arrêt non planifiés et à optimiser les performances des systèmes informatiques.

2.6 Conclusion

La supervision des réseaux informatiques est un aspect crucial de l'administration et de la gestion des infrastructures réseau dans le contexte actuel. Ce chapitre a exploré en détail les différents aspects de la supervision, en mettant en lumière ses objectifs, ses types, ses architectures et les méthodes utilisées.

Le protocole SNMP a été présenté comme une solution standard largement utilisée pour la supervision des réseaux, offrant un cadre robuste pour la collecte d'informations et la gestion des équipements réseau.

Nous allons présenter dans la chapitre suivant les outils les plus utilisés dans le milieu professionnel pour superviser les réseaux informatiques.

Chapitre 3

Outils de la supervision

3.1 Introduction

La supervision informatique est un pilier essentiel de la gestion efficace des infrastructures numériques. Dans un environnement en constante évolution, où la disponibilité et la performance des systèmes sont primordiales, le choix de l'outil de supervision adéquat revêt une importance cruciale. Cette introduction vise à présenter un aperçu des outils de supervision disponibles, en mettant particulièrement l'accent sur les solutions open source et leurs avantages par rapport aux solutions propriétaires.

3.2 Outils de la supervision propriétaires

Les logiciels de supervision dits « propriétaires » sont des logiciels caractérisés par l'appartenance à une personne ou à une société en particulier. Ce sont des logiciels qui ne sont pas des standards à l'origine et ne sont pas compatibles avec d'autres logiciels comparables de la concurrence. Nous allons présenter trois logicielles les plus utiliser [9].

3.2.1 HP OpenView

HP OpenView, une suite logicielle développée par Hewlett-Packard (HP), était dédiée à la gestion et à la supervision des systèmes informatiques, notamment des réseaux d'entreprise. Elle proposait diverses applications conçues pour surveiller, administrer et améliorer les performances des infrastructures informatiques. Le produit principal de cette suite, HP OpenView Network Node Manager (NNM), fournissait des fonctionnalités pour superviser les réseaux, gérer les événements, analyser les performances et configurer les équipements réseau. Fonctionnant sur le protocole SNMP (Simple Network Management Protocol), HP OpenView collectait des données détaillées sur l'état et le fonctionnement des périphériques réseau. Dotée d'une interface graphique conviviale, elle permettait de visualiser facilement l'état du réseau, de générer des rapports et d'envoyer des alertes en cas de problèmes [9].

3.2.2 WhatsUp Gold

WhatsUp Gold est un logiciel de supervision réseau développé par Ipswitch Il offre une solution complète pour la surveillance et la gestion des réseaux informatiques, permettant aux administrateurs réseau de surveiller en temps réel les performances, la disponibilité et la sécurité de leurs infrastructures réseau.

Les principales fonctionnalités de WhatsUp Gold comprennent la découverte automatique des périphériques réseau, la surveillance des performances des équipements, la gestion des événements et des alertes, ainsi que la génération de rapports détaillés sur l'état du réseau. Il prend également en charge la surveillance du réseau sans fil, des applications, des serveurs, des commutateurs, des routeurs et d'autres périphériques réseau.

WhatsUp Gold offre une interface conviviale qui permet aux utilisateurs de visualiser facilement l'état du réseau, d'identifier les problèmes potentiels et de prendre des mesures correctives rapidement. Il est largement utilisé dans les environnements informatiques d'entreprise pour assurer la disponibilité et les performances optimales des réseaux.

3.2.3 PRTG Network Monitor

PRTG Network Monitor est un logiciel qui fonctionne sous Windows développée par Paessler AG .est un logiciel complet et efficace pour surveiller un réseau et les services qu'il propose. L'outil s'adresse aux administrateurs réseau qui souhaitent disposer d'un outil performant pour s'assurer du bon fonctionnement de l'infrastructure et de ses serveurs [9].

PRTG Network Monitor mesure l'usage de la bande passante et la disponibilité des serveurs. Il prend en charge un grand nombre de capteurs et de protocoles tels qu'IMAP, FTP, DNS, Ping, POP3 et SNMP. Il propose également de nombreux tableaux de bord et des rapports détaillés sous la forme de graphiques, de tableaux et pour chacun des éléments qu'il surveille.il offre une surveillance complète. En outre, il se distingue par ses interfaces multiples, dont une interface web compatible avec la plupart des navigateurs et des applications mobiles iOS et Android [9].

3.3 Outils de supervision open source

les logiciels dits « Open Source » sont définis particulièrement comme des « logiciels libres », c'est-à-dire que ce sont des logiciels qui rassemblent les applications livrées dont le code source est accessible au public, cela signifie que n'importe qui peut consulter, modifier et distribuer le code selon ses besoins. Ce modèle de développement est collaboratif et décentralisé souvent géré par une communauté plutôt qu'une seule entreprise ou individu [9].

3.3.1 Nagios

En 1996, Ethan Galstad a créé Nagios comme un petit programme pour effectuer des pings sous MS-DOS. Deux ans plus tard, il a migré son application vers Linux. En 1999, Galstad a décidé de la rendre accessible à la communauté open source sous le nom de NetSaint. Cependant, en raison de problèmes de propriété intellectuelle concernant ce nom, il a été renommé Nagios. Nagios est une application conçue pour surveiller les systèmes et réseaux. Elle garde un œil sur les hôtes et les services spécifiques, alertant en cas de dysfonctionnement et signalant leur retour à un fonctionnement normal [12].

Bien que Nagios ait été initialement développé pour fonctionner dans un environnement Linux, il est parfaitement adapté pour superviser divers systèmes d'exploitation, tels que Windows XP, Windows 2000, Windows 2003 Server, ainsi que les équipements réseau grâce au protocole SNMP. Cette adaptabilité lui permet d'être utilisé dans une variété d'entreprises, indépendamment de la topologie de leur réseau et des systèmes d'exploitation utilisés en interne [12].

3.3.1.1 Architecture de Nagios

L'architecture globale de Nagios est composée principalement de 3 parties :

♦ **L'ordonnanceur :** L'ordonnanceur est le cœur du programme. Il s'agit d'un processus qui se lance en tant que service système. Son mode de fonctionnement est simple mais très efficace : il paramètre des objets host et service, qui seront supervisés par l'intermédiaire d'un objet command. Celui-ci lancera, à intervalles réguliers et paramétrables, des sondes sous la forme de programmes exécutables. Les résultats de ces actions de supervision sont stockés dans des fichiers au format texte ,configurer des objets permet de [12] :

✓observer le temps entre chaque exécution de la sonde.

✓définir des seuils permettant de juger les résultats (aussi appelés « statuts », OK,WARNING ou CRITICAL, par exemple pour les objets de type service) .

✓gérer efficacement les notifications vers les acteurs responsables de la maintenance de ces objets .

✓indiquer un minimum de topologie concernant le schéma d'architecture réseau .

✓déclencher des actions particulières sur certains statuts.

♦ **Plugins :** (aussi appelés « sondes ») sont des programmes qui fonctionnent de manière autonome et servent à superviser les caractéristiques des objets configurés. Parmi ces caractéristiques, on peut notamment citer la charge CPU, l'occupation de la mémoire ou du disque, les services HTTP, SSH, FTP, POP3, et beaucoup d'autres encore. Les plugins Nagios étant normalisés et très bien documentés, il est possible de coder soi-même un plugin spécifique à son besoin .

♦ **Interface Web d'administration :** Ce composant très pratique, codé en CGI/PHP, va lire les informations stockées dans les fichiers résultat de Nagios afin d'afficher ces données sur des pages Web. Il est possible de générer des rapports ou de gérer un minimum de droit utilisateur. Un système de pipe, Unix, permet à l'utilisateur de donner des ordres au moteur Nagios (forcer le lancement d'une sonde à l'instant T, redémarrer le service, modifier la configuration d'un objet, etc.) [12].

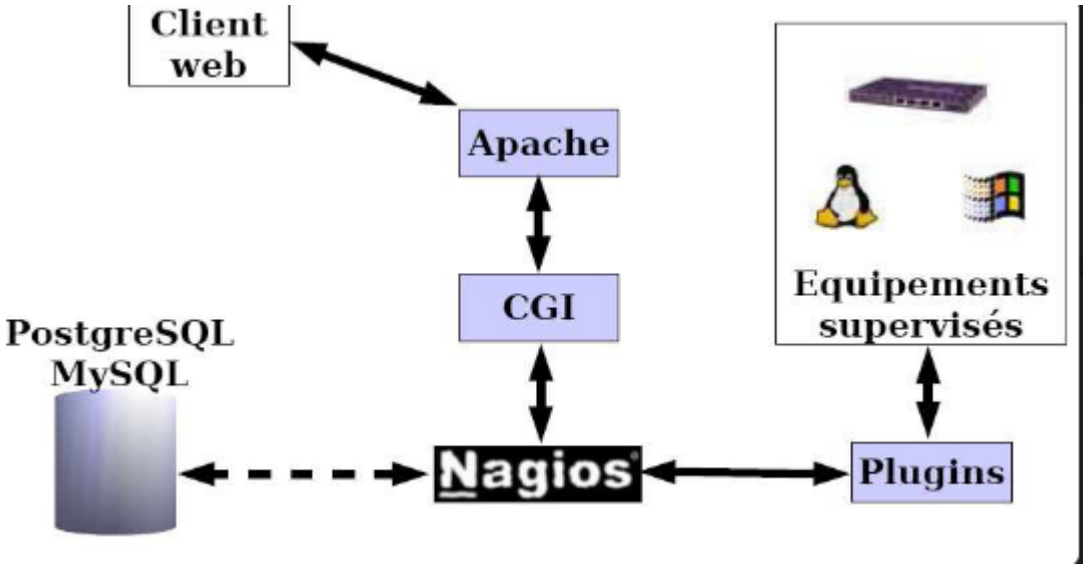

FIGURE 3.1 – Architecture de nagios

il existe deux versions différentes de Nagios :

• **Nagios Core**, la solution historique, diffusée librement sous licence GPL.

• **Nagios XI**, diffusée sous licence commerciale à partir de 2009, qui apporte notamment une nette amélioration du composant interface Web.

3.3.1.2 Exemple de fonctionnement de nagios

Nagios fonctionne en suivant un processus organisé, débutant par la configuration des éléments à surveiller. Imaginons que vous ayez un serveur web que vous souhaitez surveiller. Vous configurez Nagios en ajoutant cet hôte à sa configuration, spécifiant les services à surveiller, comme la disponibilité du service HTTP et l'utilisation du CPU, ainsi que la fréquence des vérifications, par exemple toutes les 5 minutes.

Une fois configuré, l'ordonnanceur de Nagios entre en jeu, planifiant les vérifications pour chaque service sur le serveur web selon les intervalles spécifiés. Par exemple, à midi, il planifie une vérification de la disponibilité du service HTTP. À chaque intervalle planifié, Nagios exécute les vérifications à l'aide des sondes correspondantes, collectant les données de réponse telles que le temps de réponse du serveur.

Les résultats des vérifications sont ensuite envoyés à l'ordonnanceur pour analyse. Celui-ci les compare avec les seuils de tolérance définis dans la configuration. Si le seuil est dépassé, une alerte est déclenchée, notifiant les administrateurs système via des moyens configurés comme l'e-mail.

Enfin, les administrateurs peuvent accéder à l'interface web de Nagios pour visualiser l'état de surveillance de leur infrastructure. Ils peuvent vérifier la disponibilité des services, consulter les tendances de performance et l'historique des alertes. En fonction des alertes reçues, ils peuvent prendre des mesures correctives telles que redémarrer le serveur web ou augmenter ses ressources. Ainsi, Nagios assure une surveillance proactive des systèmes informatiques, aidant à maintenir la disponibilité et les performances des services critiques.

3.3.1.3 Intégration et utilisation de modules tiers supplémentaires

Nagios Core offre un ensemble de fonctionnalités de base pour la surveillance, mais il peut également être étendu grâce à l'utilisation de modules tiers supplémentaires. Ces modules permettent d'enrichir les capacités de Nagios Core en ajoutant de nouvelles fonctionnalités et en améliorant sa flexibilité et son adaptabilité.

• **Brokers dialoguant avec une base de données :** Ces modules agissent comme des interfaces entre Nagios Core et d'autres systèmes, tels que les bases de données. Ils permettent à Nagios de stocker les données de surveillance dans une base de données externe et d'interagir avec d'autres systèmes de gestion [12].

• **Add-ons générant des vues logiques, des graphes :** Ces modules fournissent des fonctionnalités supplémentaires telles que la génération de vues logiques des données de surveillance et la création de graphiques pour visualiser les tendances et les performances du système surveillé [12].

• **Cartographie dynamique des objets supervisés :** Il s'agit d'un type d'add-on qui permet de créer des cartes dynamiques des composants surveillés. Cela aide les administrateurs système à visualiser les relations entre les différents éléments surveillés et à mieux comprendre la topologie de leur infrastructure [12].

3.3.1.4 Avantages et inconvénients

Avantages :

• La possibilité de créer des plugins personnalisés selon des besoins spécifiques, dans différents langages de programmation, rend le système flexible et facile à étendre.

• Nagios offre une surveillance complète des ressources des serveurs, des services et des réseaux, ce qui permet une gestion proactive.

• Les possibilités de tests deviennent donc infinies, il suffit d'écrire tout plugin qui n'existerait pas déjà sur les sites spécialisés.

• Les notifications sont envoyées aux contacts en cas de problème sur un hôte ou un service, et également lorsque le problème est résolu, via email, pager, ou toute autre méthode définie par l'utilisateur.

• Il est possible de définir des gestionnaires d'évènements qui s'exécutent pour des évènements sur des hôtes ou des services, pour une résolution des problèmes.

• Nagios garantit un haut niveau de sécurité pour la surveillance des systèmes et des réseaux, assurant ainsi la protection des données et des informations critiques.

Inconvénients :

• La configuration de Nagios peut être complexe et nécessite une bonne connaissance du logiciel.

• Les graphiques fournis ne sont pas toujours suffisamment clairs pour une interprétation facile.

• L'administration de Nagios est complexe et son utilisation est limitée à Linux ou une variante Unix.

3.3.2 Zabbix

Zabbix, créé en 2005 par Alexei Vladishev, est une plateforme de supervision professionnelle open-source offrant une réponse rapide aux problèmes serveurs grâce à un mécanisme de notification flexible. Cette solution complète de monitoring inclut des vues graphiques générées par RRDtool, des alertes sur seuil, et prend en charge la surveillance SNMP, IPMI et la découverte de réseau. Avec un front-end web, des serveurs distribués et des agents multiplateformes précompilés, Zabbix permet de superviser divers éléments tels que les serveurs, les applications, les bases de données, etc. Son architecture reposant sur du C/C++, PHP et des bases de données telles que MySQL, PostgreSQL ou Oracle assure une gestion efficace de la capacité. Zabbix est activement développé et maintenu par ZABBIX SIA, et sa licence GPL garantit sa gratuité et son accessibilité à tous [13].

3.3.2.1 Architecture de Zabbix

Zabbix se compose de plusieurs composants logiciels majeurs, dont les responsabilités et leurs fonctionnements sont décrites ci-dessous.

♦ **Serveur Zabbix :** Le cœur de Zabbix réside dans son serveur, qui agit comme le pivot central pour la supervision et la gestion des services en réseau. Ce composant crucial permet la surveillance à distance des serveurs web, de messagerie, FTP, etc., tout en recevant les informations vitales des agents. En tant que référentiel central, il stocke toutes les données de configuration, les statistiques et les opérations dans une base de données dédiée. En cas de dysfonctionnement dans les systèmes surveillés, le serveur Zabbix alerte activement les administrateurs via des notifications

par e-mail et peut également utiliser le protocole SNMP pour surveiller les hôtes. Bien qu'il puisse opérer sans les agents, cela se traduirait par une collecte limitée d'informations [13].

♦ **Agents Zabbix :** des programmes légers installés sur les systèmes à surveiller, collectent des données de performance telles que l'utilisation du processeur, de la mémoire et les statistiques réseau. Ces informations sont ensuite transmises au serveur Zabbix pour analyse et stockage. Bien que le serveur puisse fonctionner indépendamment des agents, leur utilisation permet une surveillance plus détaillée et précise. Les agents sont déployés sur les cibles pour surveiller activement les ressources et les applications locales, assurant ainsi une supervision accrue. Leur efficacité est renforcée par l'utilisation d'appels système natifs pour la collecte d'informations statistiques. En bref, l'installation d'un agent Zabbix offre une surveillance active des ressources locales et des applications, renforçant la capacité de supervision de Zabbix [13].

♦ **Le proxy Zabbix :** optionnel dans le déploiement de Zabbix, joue un rôle crucial dans la collecte des données de performance et de disponibilité pour le compte du serveur Zabbix. En agissant comme une sonde intermédiaire, il recueille les informations sur les hôtes avant de les transmettre au serveur, ce qui permet de réduire la charge sur ce dernier. Cette solution est particulièrement utile pour la surveillance centralisée des sites distants, des succursales et des réseaux sans administrateurs locaux. De plus, les proxies peuvent également être utilisés pour distribuer la charge d'un seul serveur Zabbix, en traitant localement les données collectées avant leur transmission, ce qui allège la charge en CPU et en E/S disque sur le serveur principal [13].

♦ **L'interface Zabbix :** aussi connue sous le nom de Zabbix frontend, est la passerelle principale pour visualiser les événements et administrer Zabbix. Basée sur une plateforme web PHP, elle offre la commodité d'être accessible depuis n'importe quelle plateforme disposant d'un navigateur internet. Cette interface permet aux utilisateurs de visualiser les données de surveillance, de configurer les paramètres de Zabbix, de gérer les alertes et les rapports. Généralement exécutée sur la même machine physique que le serveur Zabbix, l'interface Web assure un accès aisé aux données et à la configuration, même si elle peut être déployée séparément dans certaines configurations notamment lorsque SQLite est utilisé [13].

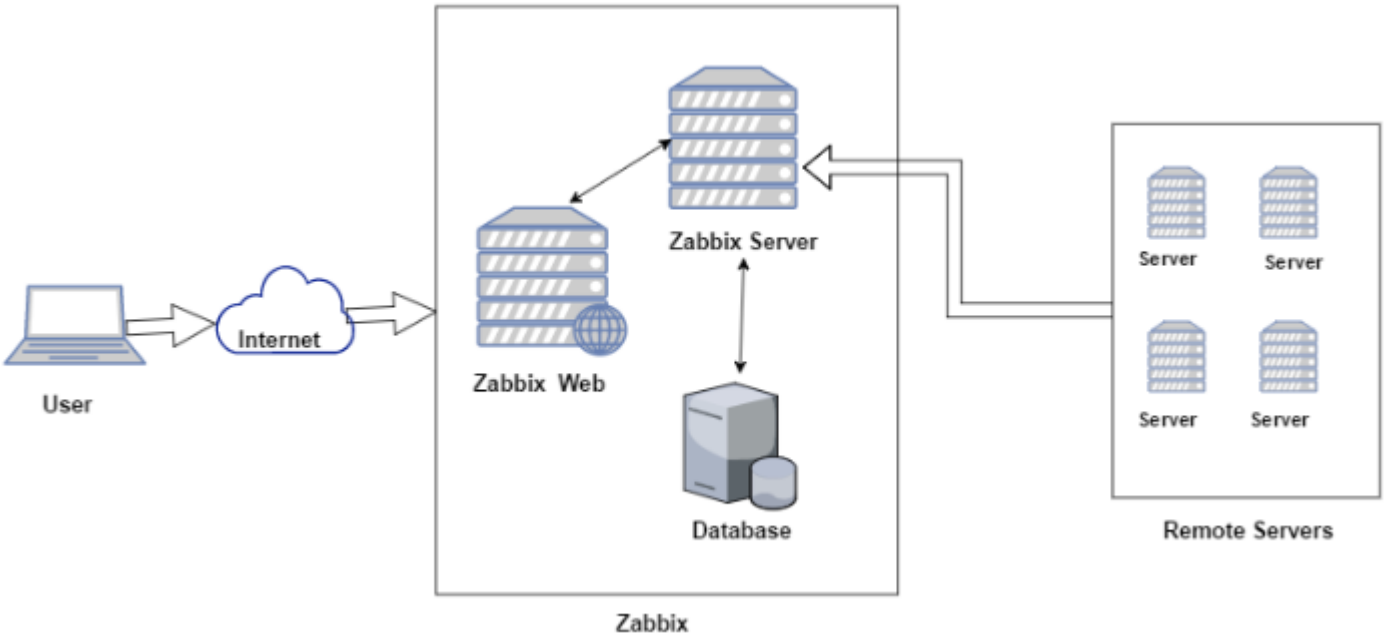

FIGURE 3.2 – Architecture de zabbix

3.3.2.2 Exemple de fonctionnement de zabbix

Le fonctionnement de Zabbix repose sur une configuration initiale où les administrateurs définissent les éléments à surveiller, tels que les serveurs, postes de travail et équipements réseau, via son interface web. Ensuite, des agents Zabbix sont installés sur chaque élément cible pour collecter en continu des données de performance telles que l'utilisation du CPU, de la mémoire et le trafic réseau. Ces données sont ensuite transmises au serveur Zabbix qui les analyse, les stocke et les compare à des seuils prédéfinis pour détecter toute anomalie. En cas de dépassement de seuil, des alertes sont envoyées aux administrateurs, leur permettant de prendre des mesures correctives. Les données collectées peuvent être visualisées et analysées à travers l'interface utilisateur web, fournissant ainsi une vue détaillée de la santé et des performances de l'infrastructure informatique de l'entreprise. En résumé, Zabbix offre une solution complète de surveillance et de gestion proactive de l'infrastructure informatique, permettant une détection précoce des problèmes et une optimisation des performances.

3.3.2.3 Avantages et inconvénients

Les avantages :

- offre une interface utilisateur Web moderne et conviviale.
- Facilité de consultation et Génération des graphs en fonction du temps.
- Zabbix découvre automatiquement les ressources sur le réseau, y compris les périphériques,

les applications et les services, ce qui simplifie le processus d'installation sur des environnements multiplateformes.

Les inconvénients :

• Chaque machine à superviser doit disposer du client Zabbix.

• la complexité de configuration initiale.

• L'interface est un peu vaste, la mise en place des templates n'est pas évidente au début : Un petit temps de formation nécessaire.

• L'agent zabbix communique par défaut en clair les informations d'où la nécessité de sécuriser ces données (via VPN par exemple).

3.3.3 Centreon

Centreon, en tant qu'outil de surveillance informatique robuste et open source, offre une palette étendue de fonctionnalités au-delà de la simple surveillance. À l'origine nommé Oreon, Centreon était conçu pour simplifier l'expérience d'utilisation du moteur de collecte de données Nagios grâce à une interface graphique conviviale. Depuis 2011, Centreon a évolué en développant son propre moteur de collecte et de distribution des données. Bien qu'il puisse être utilisé de manière autonome, sa fusion avec Nagios peut fournir une solution de surveillance plus complète. Cependant, cette intégration ajoute une complexité supplémentaire, nécessitant des ressources et une maintenance accrues. Centreon propose une solution intégrale de surveillance informatique, couvrant la disponibilité et la performance des applications jusqu'aux ressources matérielles. Parmi ses fonctionnalités avancées, on trouve la surveillance de l'état des services et des machines, la métrologie, le reporting et la gestion des utilisateurs. En outre, des modules supplémentaires, tels que des outils de Business Intelligence et de cartographie, ainsi que des API pour l'automatisation, enrichissent son potentiel. Toutefois, il est à noter que Centreon n'est compatible qu'avec les systèmes Linux ou Solaris [14].

3.3.3.1 Architecture de centeron

L'architecture de Centreon est basée sur plusieurs composants qui fonctionnent ensemble pour fournir une solution complète de surveillance et de supervision des systèmes informatiques.

♦ **Centreon Web :** est l'interface web qui permet aux utilisateurs d'interagir avec le système, de visualiser les données de surveillance et de configurer les paramètres. Elle fonctionne sous Apache et fournit une interface conviviale pour la gestion du système [14].

♦ **Centreon Engine :** est le moteur central qui exécute les tâches de surveillance et de supervision proprement dites. Il est responsable de l'exécution des contrôles, de la collecte des données et de la génération des alertes. Centreon Engine est basé sur Nagios et utilise des plugins pour effectuer différents contrôles [14].

♦ **Centreon Broker :** est un courtier de données qui gère la communication entre Centreon Engine et la base de données. Il reçoit les données de Centreon Engine et les stocke dans la base de données, et il récupère également les données de la base de données et les envoie à Centreon Web [14].

♦ **La base de données :** est utilisée pour stocker toutes les données de surveillance, y compris les paramètres de configuration, les données historiques et les données en temps réel. Centreon utilise MariaDB comme base de données par défaut et stocke les données dans deux bases de données : centreon et centreon-storage. La base de données centreon contient les données de configuration, tandis que la base de données centreon-storage contient les données en temps réel, les journaux et les données de performance [14].

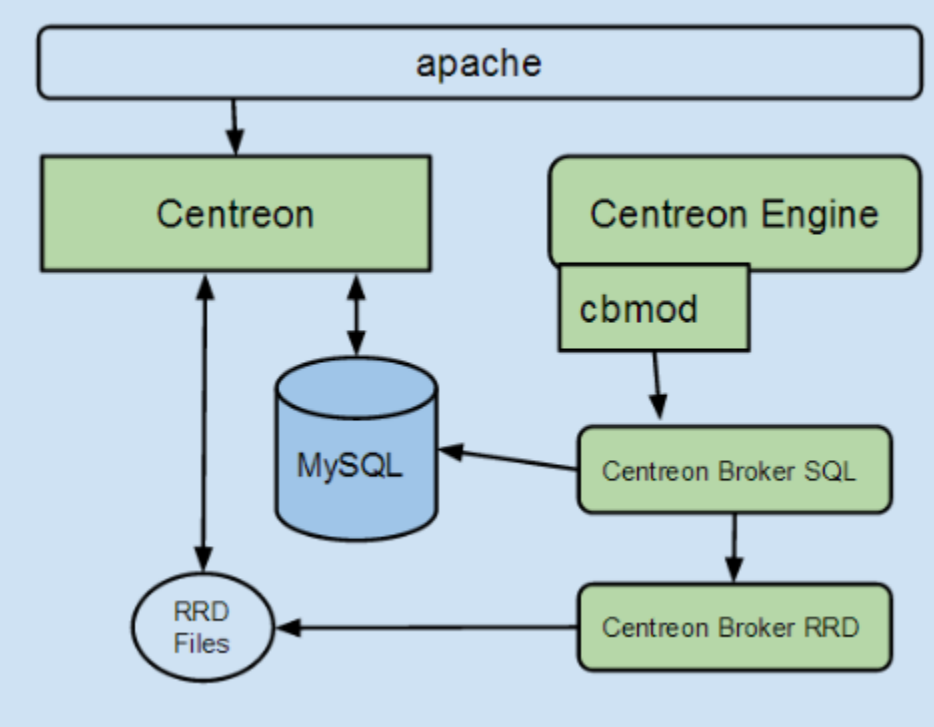

FIGURE 3.3 – Architecture de centreon [14]

3.3.3.2 Exemple de fonctionnent de centeron

Dans un environnement de surveillance avec Centreon, imaginons que nous souhaitons monitorer un serveur web. Nous commençons par configurer Centreon sur un serveur dédié, installant Centreon Web comme interface utilisateur principale, Centreon Engine pour la collecte des données, et Centreon Broker pour la communication entre Engine et la base de données. Ensuite, nous ajoutons le serveur web à surveiller dans Centreon Web, spécifiant ses détails comme son adresse IP et ses services à surveiller tels que la disponibilité du ping ou la charge CPU. Nous configurons les plugins nécessaires pour collecter les données, comme un plugin HTTP pour la disponibilité

du site et un plugin SNMP pour la charge CPU. Centreon Engine collecte ensuite régulièrement ces données, les stockant dans la base de données. Les utilisateurs accèdent à Centreon Web pour visualiser les données, recevant des alertes en temps réel en cas de problèmes détectés, comme une charge CPU élevée. Les administrateurs peuvent alors analyser les données historiques pour optimiser les performances du serveur web et assurer sa disponibilité.

3.3.3.3 Avantages et inconvénients

Les avantages :

- Basé sur Nagios, offrant une excellentes capacités d'intégration.
- Interface qui permet une configuration facile.
- Peut fonctionner indépendamment du serveur Nagios.
- Solution complète comprenant des fonctionnalités de reporting, de gestion des alarmes et la cartographie du réseau.

Les inconvénients :

- Une interface peut être complexe en raison des nombreuses options et vues disponibles.
- Un peu plus lourd par rapport à Nagios.
- Peut nécessiter une courbe d'apprentissage abrupte pour les nouveaux utilisateurs.
- La difficulté de maintenance.

3.3.4 Cacti

Cacti est une solution de surveillance réseau open source qui permet de visualiser les performances des réseaux et des systèmes à travers des graphiques. Il est largement utilisé pour sa capacité à tracer des graphiques sur toutes les métriques numériques possibles d'un équipement [9].

Cacti fonctionne grâce à un serveur web équipé d'une base de données et du langage PHP. Il utilise RRDTool pour la gestion des données temporelles et la génération de graphiques. Cacti est capable d'effectuer des mesures complexes en utilisant des scripts personnalisés (Bash, PHP, Perl, VBs...) [9].

Cacti n'est pas directement une solution de supervision, car elle ne possède pas de système de gestion d'alertes basé sur des seuils, à la manière des plugins. En revanche, elle permet de stocker des informations diverses et variées dans une base de données de type RRDTool (Round Robin Database), ce qui rend possible des sauvegardes cycliques de données et garantit une taille d'occupation fixe sur le périphérique de stockage [9].

Cette solution est très souvent employée pour stocker des éléments de données concernant les

flux réseau, et inclut des outils capables de générer des graphes variés. Elle permet aussi de gérer les profils utilisateurs [9].

3.3.4.1 Architecture de Cacti

Cacti fonctionne en collectant des données de performances sur les différents équipements surveillés, stocker ces données dans des bases, générer des graphes et les visualiser grâce à une interface web.

♦ **Collecter des données :** A intervalle donné (5 minutes par défaut), Cacti va collecter des valeurs ou mesurer des temps de réponse grâce à son ordonnanceur intégré. Il existe plusieurs types d'ordonnanceurs, du plus simple écrit en PHP au plus performant écrit en C. Cacti interroge les hôtes principalement par l'intermédiaire du protocole SNMP. Une majorité d'équipements réseaux et informatiques proposent cette fonctionnalité mais si ce n'est pas le cas, Cacti peut aussi interroger via des scripts étendant grandement les possibilités [9].

♦ **Stocker les données :** Le grand principe de RRDTool est de stocker les valeurs dans des bases de données tournantes à taille fixe, appelées RRD (Round Robin Database). On ne conserve que les dernières valeurs, ensuite ces valeurs sont moyennées pour fournir une autre base sur une période plus longue, et ainsi de suite [9].

♦ **Générer des graphes :** S'appuyant sur RRDTool, Cacti fournit une représentation graphique de ces valeurs et de leur évolution dans le temps. Les graphes sont générés en temps réel et l'on peut zoomer ou changer l'échelle de temps [9].

♦ **Une interface de visualisation :** Cacti permet aux utilisateurs de consulter les graphes à travers une interface web écrite en PHP. Mais elle permet aussi d'effectuer très simplement toute la configuration de l'outil [9].

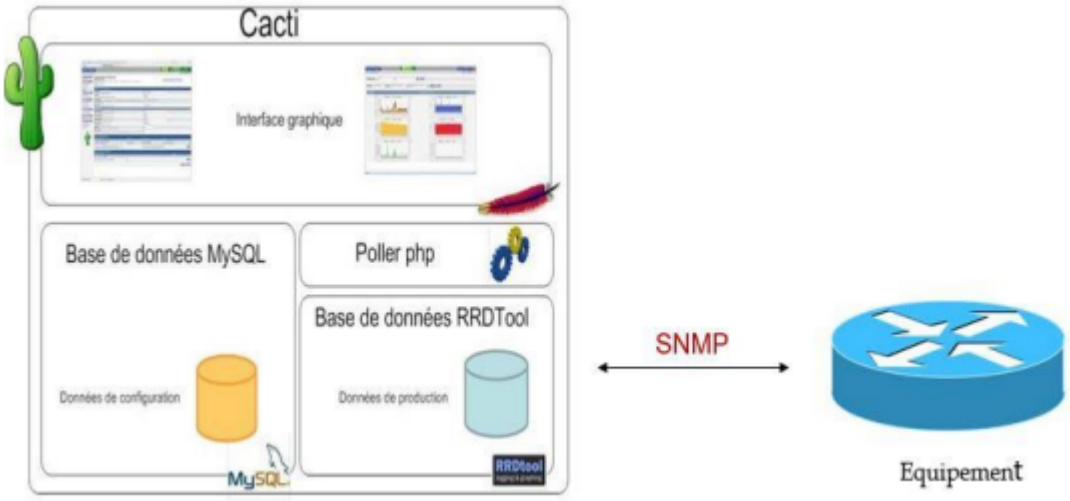

FIGURE 3.4 – Architecture de cacti

3.3.4.2 Avantages et Inconvénients

Avantages :

• Simplicité d'installation .

• Il peut détecter automatiquement les différentes points de contrôle comme les partitions et les interfaces réseaux .

• L'intégration poussée de RRDTool permet de modifier les aspects des graphiques générés.

Inconvénients :

• Manque d'évolutions : Le développement de Cacti semble se ralentir ces dernières années, ce qui peut soulever des questions sur sa capacité à s'adapter aux nouvelles technologies et pratiques.

• Absence d'héritage multiple : Cacti ne supporte pas la notion d'héritage multiple, ce qui est considéré comme essentiel dans la supervision moderne. Être limité à un seul type d'équipement lors de la définition de l'équipement est restrictif.

• Absence de gestion d'alarmes sauf avec un plugin nommé Thold.

• Absence de gestion de panne et d'une cartographie de réseau.

3.3.5 Prometheus

Prometheus. C'est un système open-source de surveillance et d'alerte, conçu initialement par SoundCloud. Prometheus est spécialement conçu pour les environnements dynamiques et distribués, offrant une collecte de données flexible, des requêtes puissantes en langage de requête PromQL, ainsi qu'une intégration étroite avec Grafana pour la visualisation des données. Vous pourriez explorer ses fonctionnalités de découverte automatique des services, de gestion des alertes et de scalabilité horizontale pour compléter votre mémoire sur les outils de supervision informatique.

3.3.5.1 Architecture de Prometheus

L'architecture de Prometheus est conçue pour être à la fois simple et puissante, permettant une surveillance efficace et flexible des systèmes informatiques. Voici les éléments clés de son architecture :

♦ **Serveur Prometheus :** Le cœur de Prometheus est son serveur central, qui collecte et stocke les données. Le serveur exécute des tâches essentielles telles que :

• **Extraction des métriques :** Il récupère régulièrement les métriques des cibles configurées via des scrapes HTTP.

• **Stockage des données :** Les métriques collectées sont stockées dans une base de données de séries temporelles.

• **Exécution des requêtes :** Il permet d'interroger les données stockées en utilisant le langage de requête PromQL.

♦ **Exporters et Intégrations :**Pour collecter les métriques, Prometheus utilise des exporters. Ce sont des agents ou des bibliothèques qui sont installés sur les serveurs surveillés et qui transforment les métriques de ces systèmes en un format compréhensible par Prometheus. Il existe des exporters pour une multitude de services et de systèmes d'exploitation.Pushgateway Pour les tâches ou les processus qui ne peuvent pas être scrapés directement, Prometheus offre le Pushgateway. C'est un intermédiaire qui permet de pousser les métriques vers le serveur Prometheus.

♦ **Alertmanager :** L'Alertmanager gère les alertes générées par le serveur Prometheus. Il s'occupe de la déduplication, du groupement et de la transmission des alertes aux systèmes de notification appropriés.

♦ **Service Discovery :** Prometheus est équipé d'un système de découverte de services qui lui permet de trouver automatiquement les cibles à surveiller dans des environnements dynamiques comme les clusters Kubernetes.

♦ **Interface Utilisateur :** Prometheus propose une interface utilisateur web pour l'exécution des requêtes, la visualisation des métriques et le débogage. Il fournit également une API HTTP pour l'intégration avec d'autres applications.

3.3.5.2 Avantages et inconvénients

Les avantages :

• offre une collecte de données en temps réel.

• Grâce à son langage de requête PromQL, Prometheus permet des analyses approfondies des métriques système et d'application.

• L'intégration transparente avec Grafana rend la visualisation des données intuitive et captivante.

• Son architecture modulaire et sa communauté active font de Prometheus un choix fiable pour les organisations de toutes tailles.

Les inconvénients :

• La gestion du stockage local des données peut poser des défis de rétention à long terme pour les grandes infrastructures.

• La configuration initiale et la définition des règles d'alerte peuvent nécessiter une expertise technique, ce qui peut être intimidant pour les nouveaux utilisateurs.

• Bien que Prometheus excelle dans la surveillance en temps réel, son support pour le traitement des données historiques peut être limité par rapport à d'autres solutions.

• La surveillance de services distribués peut poser des défis de configuration et de coordination, en particulier dans les environnements dynamiques.

3.4 Comparaison des outils de supervision

Pour évaluer les différentes solutions de supervision disponibles, nous avons comparé Nagios avec Zabbix, Centreon, Cacti et Prometheus en fonction des besoins spécifiques d'un centre de calcul informatique universitaire. Ces besoins incluent la surveillance des serveurs et des applications académiques, la gestion des alertes et des notifications , Reporting et analyse pour les administrateurs ainsi que robustesse et fiabilité .

Le tableau ci-dessous illustre comment chaque outil répond à ces besoins, mettant en évidence pourquoi Nagios s'est révélé être la solution la plus complète et adaptée à notre environnement.

Besoins	**Nagios**	**Zabbix**	**Centron**	**Cacti**	**Prometheus**
Surveillance des serveurs et applications académiques	Excellente Large gamme de plugins disponibles.	Très bonne Prise en charge étendue.	Très bonne Utilise les plugins de Nagios.	Moyenne Limité aux performances réseau.	Très bonne Idéal pour les applications cloud-native.
Gestion des alertes et notifications	Excellente Système d'alerte configurable.	Très bonne Système d'alerte avancé.	Très bonne Basé sur Nagios.	Moyenne Notification basique.	Bonne Notifications configurables.
Reporting et analyse pour les administrateurs	Bonne Rapports de base, extensibles.	Très bonne Rapports détaillés.	Très bonne Rapports améliorés.	Très bonne Excellents graphiques réseau.	Excellente Utilisé avec Grafana.
Robustesse et fiabilité	Excellente Historique de stabilité éprouvée.	Très bonne Fiable mais plus complexe à configurer pour une grande infrastructure.	Très bonne Fiable avec l'ajout de Centreon pour l'interface.	Bonne Fiable mais limité aux performances réseau.	Très bonne Haute fiabilité pour les environnements cloud.

Tableau 3.1 – Comparaison des outils de supervision

Dans le cadre de notre études sur la supervision des réseaux informatiques, on a schoisi de travailler avec Nagios, une solution déjà en place au centre de calcul de notre université. Nagios s'est révélé être une solution complète, répondant parfaitement à tous les besoins de supervision du centre grâce à sa flexibilité, son extensibilité et sa robustesse. Ce choix stratégique nous a permis

de tirer parti de ses nombreuses fonctionnalités pour surveiller une grande diversité de systèmes et d'applications de manière efficace et fiable.

Dans la partie pratique de ce mémoire, nous avons réalisé une simulation détaillée du réseau informatique du centre, intégrant les différents équipements et services critiques. Nous avons également approfondi notre apprentissage de Nagios, en explorant ses capacités de configuration et de personnalisation. Cette approche pratique nous a permis de démontrer concrètement comment Nagios peut être utilisé pour optimiser la performance, détecter les anomalies rapidement, et assurer une surveillance continue des infrastructures.

Après l'analyse approfondie que nous avons réalisée et les résultats obtenus on confirme que Nagios est une solution idéale pour les environnements complexes et variés tels que notre centre de calcul universitaire. Non seulement il répond aux exigences actuelles de supervision, mais il offre également une base solide pour future croissance et adaptation aux nouveaux besoins technologiques.

3.5 Conclusion

En conclusion, le paysage de la supervision informatique offre une multitude d'options, des logiciels propriétaires bien établis aux solutions open source en constante évolution. Alors que les outils propriétaires offrent souvent une intégration étroite avec les environnements d'entreprise, les solutions open source comme Nagios, Zabbix, Centreon, Cacti et Prometheus apportent une flexibilité, une personnalisation et une évolutivité sans pareilles. Bien que chaque outil présente ses propres avantages et inconvénients, le choix final dépendra des besoins spécifiques de l'organisation en matière de supervision et de gestion des infrastructures informatiques. En définitive, que ce soit par le biais de solutions propriétaires ou open source, l'objectif ultime reste le même : assurer la disponibilité, la performance et la fiabilité des systèmes pour répondre aux exigences croissantes du monde numérique moderne.

Le chapitre suivant sera consacré à la présentation de l'organisme d'accueil et à l'étude approfondie des notions de supervision d'un réseau.

Chapitre 4

Présentation de l'organisme d'accueil

4.1 Introduction

Pour améliorer nos compétences dans le domaine des réseaux, il est essentiel de développer nos aptitudes professionnelles. Dans cette optique, nous avons suivi un stage pratique au sein du Centre des Systèmes et Réseaux d'Information, de Communication, de Télé-enseignement et d'Enseignement à Distance (CSRICTED) de l'université de Béjaia, que nous allons présenter dans ce chapitre.

Ce chapitre se concentre sur la présentation du CSRICTED, permettant ainsi une analyse du réseau de l'organisation. L'objectif est de comprendre l'état actuel du réseau afin de proposer des solutions efficaces pour sa supervision.

4.2 Présentation du service d'accueil

Le centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance (CSRICTED) est l'un des services communs de l'université de Bejaïa, il se charge de la gestion de toutes les ressources informatiques de l'université ainsi que de l'assurance de la continuité des services informatiques et de leurs maintenances, tels que le service pédagogique, la disponibilité de la connexion aux réseaux intranet et internet et l'exploitation des différents services offerts, et enfin la maintenance du parc informatique de l'université [15].

4.2.0.1 Organisation

Le CSRICTED se constitue de quatre sections : la section système d'information, la section réseau, la section e-learning et la section maintenance comme c'est montré dans la Figure suivante :

FIGURE 4.1 – Organigramme du CSRICTED [15]

4.2.1 Description et rôles de chaque section

1. **Section Système d'Information :**

La Section Système d'Information (SI), a pour mission de mettre en œuvre la politique des systèmes d'information et des technologies de l'information et de la communication, la gestion d'une manière plus générale à tout ce qui touche au traitement automatique de l'information. La section se compose de trois cellules qui sont : cellule de développement, cellule pédagogique et cellule système [15].

2. **Section Réseau :**

La section réseau a pour missions de maintenir le fonctionnement normal du réseau intranet de l'université, d'assurer la sécurité des équipements réseaux et des services offerts par le réseau au système d'information et aux applications et enfin de fournir des services de connexion internet, de messagerie électronique, de support utilisateur d'étude et de suivi des projets réseau de l'université de Béjaia [15].

3. **Section chargée du Télé-enseignement (e-learning) :**

Cette section a pour mission de prendre en charge toutes les opérations liées au e-sslearning à l'université de Bejaia. Son champ d'intervention concerne au moins deux domaines : le domaine pédagogique et le domaine technique.

- Le domaine pédagogique englobe la formation des enseignants, des responsables et du personnel ATS de l'université sur l'usage des technologies de l'information et de la communication [15].

- Le domaine technique englobe la mise en place d'une solution e-learning répondant à la fois aux besoins et aux ambitions de cette université. Il s'agit notamment de l'installation, de l'administration et de la maintenance des plates formes de e-learning. En plus de cela, cette cellule gère une salle de visioconférence [15].

4. **Section Maintenance :** Comme son nom l'indique, cette section assure le maintient en bon état des équipements informatiques des différents services de l'université [15].

4.3 Étude de l'existant

Dans cette section nous incluons une analyse approfondie du réseau de l'université de Bejaia. Nous avons eu l'opportunité de réaliser un stage à l'université qui s'est déroulé sous la forme de visites au centre des système et réseau (CSRICTED) précisément dans la section réseau. Ces visites nous ont permis d'interagir avec des professionnels du secteur et de recueillir des informations précieuses pour notre projet.

4.3.1 Présentation du réseau de centre des système et réseau (CSRICTED)

Le réseau du Centre Système et Réseau de l'Université de Bejaia débute avec la connexion Internet fournie par Algérie Télécom. Cette connexion transite par l'Université de Bejaia et le CSRICTED (centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance) avant d'être acheminée vers un routeur Cisco. Le routeur gère le trafic réseau en le dirigeant vers un pare-feu Fortinet qui assure la sécurité avant son accès au réseau interne en contrôlant et filtrant les données. Le réseau est ensuite distribué par un switch Cisco du Centre de Calcul vers différents VLANs (Virtual Local Area Networks) : VLAN1, VLAN2 ,. . ..permettant une segmentation logique du réseau pour améliorer la gestion et la sécurité. Parallèlement, une zone DMZ (Demilitarized Zone) héberge les services accessibles de l'extérieur, tels que les serveurs web,le serveur dns , tout en les isolant du reste du réseau pour renforcer la sécurité.

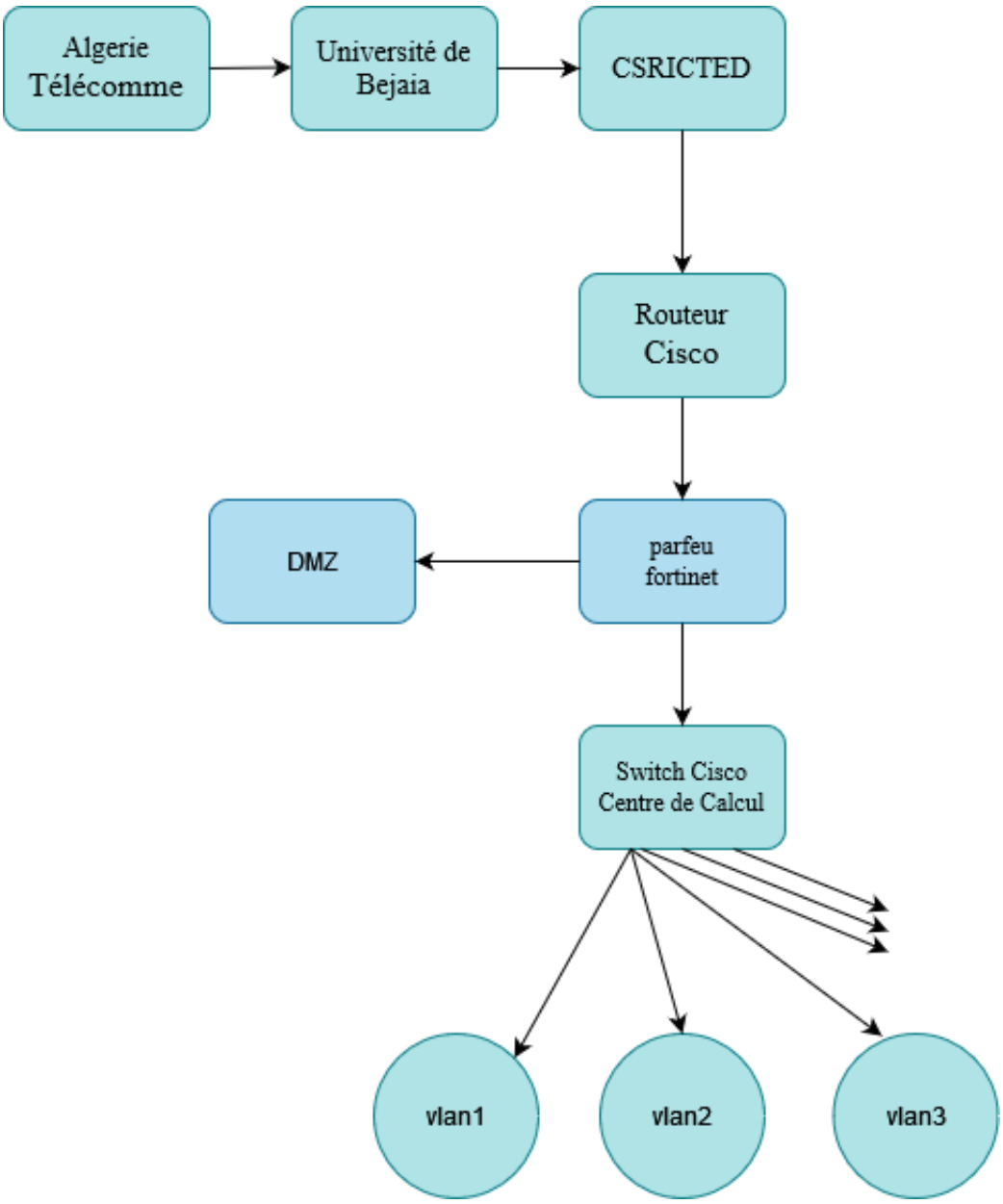

FIGURE 4.2 – Architecture du réseau de CSRICTED

.

4.3.2 Analyse du parc informatique

Dans le cadre de notre étude approfondie, nous entreprenons une analyse complète du parc informatique afin de mieux comprendre sa configuration, son efficacité et ses besoins.

4.3.2.1 Caractéristiques des équipements de raccordement

Le tableau suivant décrit les switches distribués sur chaque bloc dans le centre de Calcul , tout en présentant également l'état actuel du matériel en utilisation ainsi que les recommandations émises par l'équipe chargée de l'évaluation.

	Etat actuel	**Recommandations**
Salle machines CSRICTED (data center)	3 switchs 2950 24 ports 3 switchs 2960 24 ports	3 switchs 9200 48 ports
Salle 12 CSRICTED	4 switchs 2950 24 ports 1 switch 2960 24 ports	2 switchs 9200 48 ports
Bureau 2 CSRICTED	5 switchs 2950 24 ports 1 switch 2960 24 ports	3 switchs 9200 48 ports
Bloc 1 département ST	1 switch 9200 48 ports 1 switch 2960 24 ports	RAS
Bureau comptable (centrale)	1 switch 2960X 48 ports	Ras
Faculté Technologie	1 switch 2960X 48 ports 1 switch 2950 24 ports	1 switch 9200 24 ports
Bloc 11	1 switch 2960S 48 ports 1 switch 2950G 24 ports	1 switch 9200 24 ports
UFC	2 switchs 2950 24 ports	1 switch 9200 48 ports

Tableau 4.1 – Dispositifs matériels (switches) dans centre de Calcul

4.3.2.2 Description des ressources matérielles et logicielles du centre des système et réseau (CSRICTED)

♦ **Les ressources logicielles :**

Les ressources logicielles de CSRICTED sont les suivantes :

• Des systèmes d'exploitation constitués de : Linux, Windows ,..

• Des différents services installés sur les serveurs sont : la messagerie, le DNS, DHCP,.

♦ **Les ressources matérielles :**

Les éléments qui composent les ressources matérielles de la structure se présentent comme suit dans le tableau :

Équipement	Rôle
Serveurs dans la DMZ	Hébergement des services accessibles depuis Internet.
Routeur	Gestion des flux entre le réseau interne, la DMZ et Internet.
Pare-feu Fortigate	Sécurité du réseau, filtrage des paquets et protection.
Commutateur de distribution	Distribution du réseau vers les commutateurs d'accès.
Commutateurs d'accès	Connexion des postes de travail au réseau.
Postes de travail	Utilisateurs finaux connectés au réseau.

Tableau 4.2 – Ressources matérielles

4.3.2.3 Serveurs de centre des système et réseau (CSRICTED)

♦ **Serveur DNS :**Le DNS (Domain Name System) est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements. Il permet aux utilisateurs d'accéder à des sites web en utilisant des noms de domaine compréhensibles (comme www.example.com) plutôt que des adresses IP numériques. Concrètement, le DNS fait correspondre les noms de domaine aux adresses IP des serveurs web, permettant ainsi aux navigateurs d'accéder aux sites web. Lorsqu'un utilisateur tape un nom de domaine dans son navigateur, le serveur DNS traduit ce nom en une adresse IP compréhensible par les ordinateurs, renvoyant ainsi le contenu du site web demandé. Le DNS est organisé de manière hiérarchique, avec des serveurs DNS de différents niveaux qui se transmettent les requêtes jusqu'à trouver l'adresse IP correspondante. Cette architecture distribuée permet une grande évolutivité et fiabilité du système.

4.4 Conclusion

Dans ce chapitre, consacré à la présentation du projet et de l'organisme d'accueil de notre stage, nous avons effectué une analyse approfondie du réseau. Cette étude nous a permis d'identifier les caractéristiques de l'organisme d'accueil. Forts de ces constats, nous avons été motivés à proposer des solutions visant à renforcer et améliorer le réseau du CSRICTED de l'université de Béjaia.

Le chapitre suivant sera consacré à la conception de notre travail étudié dans les chapitres précédents.

Chapitre 5

Contexte de travail et implementation

5.1 Introduction

L'intégration efficace d'une solution de supervision est essentielle pour garantir le bon fonctionnement du réseau. Ce chapitre se consacre à la mise en œuvre pratique de Nagios comme outil de supervision au sein du Centre des Systèmes et Réseaux de l'Université de Béjaïa. Après avoir exploré les concepts théoriques et comparé divers outils de supervision dans les chapitres précédents, nous aborderons ici les étapes concrètes de déploiement de fully automated Nagios (FAN), de la configuration initiale à l'analyse des résultats.

Dans ce contexte, nous décrirons d'abord le processus de simulation du réseau à l'aide de GNS3, ce qui nous a permis de tester et de valider les configurations avant leur application en environnement réel. Nous expliquerons ensuite la configuration des équipements et la définition des paramètres de supervision spécifiques à notre infrastructure. Cette section détaillera les différentes étapes de mise en place et les solutions apportées.

5.2 Environnement du travail

Cette section décrit les outils et les technologies utilisés pour réaliser notre projet au sein de centre de calcul(CSRICTED).

5.2.1 Pc utilisé

Pour pouvoir configurer l'architecture souhaitée dont la nécessité de mettre en place une gestion de superviseur nagios nous avons travaillé avec un pc de marque HP avec une RAM de 8Go et pour assurer la compatibilité des environnements on a choisi de travailler avec le système d'exploitation Windows 10.

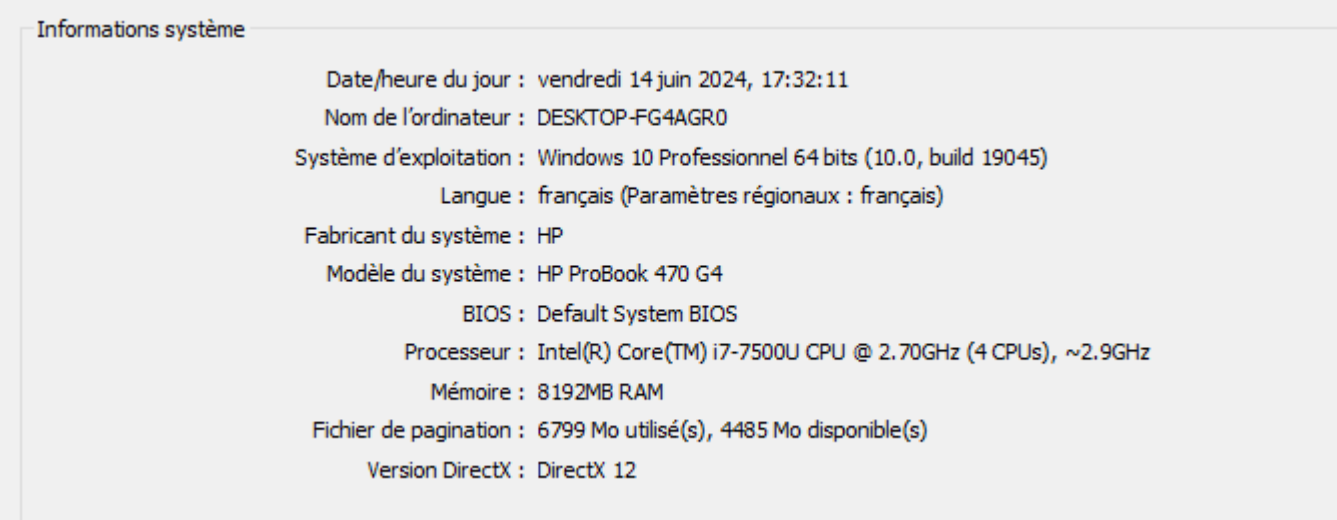

FIGURE 5.1 – Pc utilisé

5.2.2 Logiciels utilisés

5.2.2.1 VMware Workstation

est un logiciel de virtualisation de système d'exploitation qui permet de créer un ou plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités), et de faire fonctionner Plus d'un système d'exploitation en même temps en toute sécurité [16].

5.2.2.2 GNS3 (Graphical Network Simulator)

GNS3 est un outil open source de simulation de réseaux informatiques utilisé dans les environnements éducatifs et professionnels qui permet d'émuler des équipements informatiques (routeur, switch, PC...) et qui permet de simuler leurs fonctionnements. Cet outil est très utile pour maquetter avant une mise en production, Avec GNS3, les utilisateurs peuvent créer, tester et résoudre des problèmes sur des réseaux virtuels complexes, en utilisant une variété de périphériques virtuels tels que des routeurs, des commutateurs et des pare-feu [17].

L'objectif de GNS3 est d'apporter aux étudiants et professionnels des nouvelles technologies de communication travaillant dans le domaine de l'administration systèmes et réseaux une solution pour virtualiser et modéliser fidèlement des réseaux.

Le principal avantage de GNS3 réside dans l'émulation matérielle, en lieu et place de l'utilisation de simulateurs qui souvent est une manière limitée de virtualiser du matériel. Grâce à GNS3, les utilisateurs peuvent tester et estimer, dans des conditions quasi réelles et sans avoir à financer le matériel, leurs configurations et réseaux avant de les mettre en place physiquement.GNS3 nous permet : [18]

- Le design de topologies réseaux de haute qualité et complexes.
- Emulation de plusieurs plate-forme de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA.
- Simulation de switches Ethernet, ATM et frame Relay.
- Connexion de réseaux simulés au monde réel.
- Capture de paquets grâce à Wireshark.

5.3 Architecture Simulée

Dans cette section, nous décrirons l'architecture réseau simulée pour le centre de calcul universitaire ainsi que les configurations nécessaires pour chaque composant afin d'assurer une supervision efficace avec nagios. L'architecture proposée comprend des équipements critiques tels que les pare-feu Fortigate, les commutateurs Cisco, les serveurs DNS et web, et plusieurs VLANs. Chaque composant sera configuré pour permettre une surveillance optimale via SNMP, garantissant ainsi que FAN puisse collecter les données de supervision et générer des alertes en cas de défaillance ou d'anomalie. La mise en place détaillée de chaque élément sera également expliquée pour assurer une compréhension complète du processus de simulation et de configuration.La figure ci-dessous représente l'architecture de réseau.

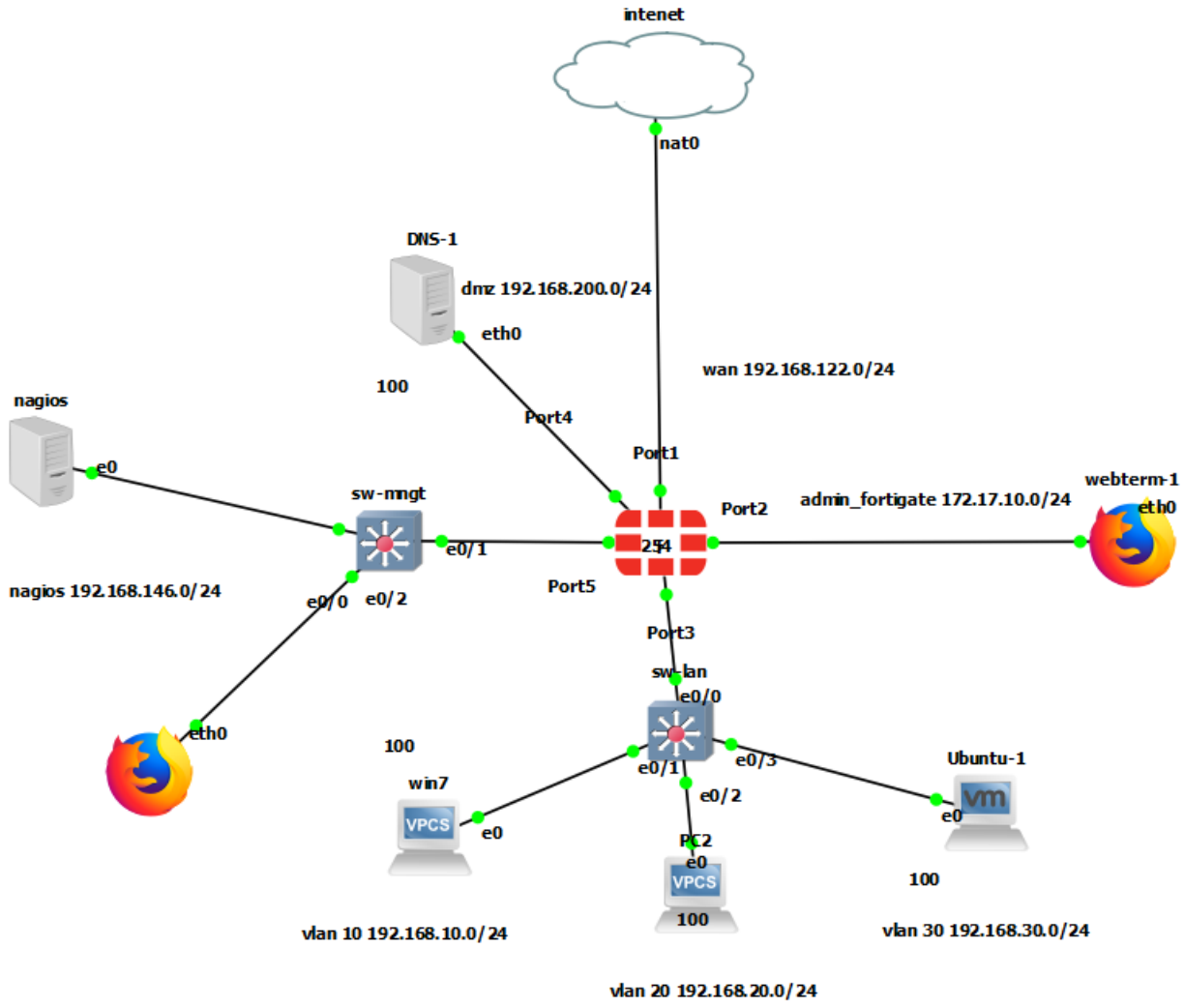

FIGURE 5.2 – Architecture proposée

5.3.1 Description de l'Architecture

Le pare-feu Fortigate est au cœur de notre architecture réseau. Il dispose de cinq ports configurés comme suit :

- **Port 1 : Connexion à l'Internet :** Ce port assure la connectivité du réseau interne vers l'extérieur, permettant l'accès aux ressources et services en ligne.
- **Port 2 : Administration :** Un navigateur web est connecté à ce port pour administrer le pare-feu via son interface web. Cela permet aux administrateurs réseau de gérer et configurer les règles de sécurité et les paramètres du pare-feu.
- **Port 3 : Connexion au Switch VLAN :** Ce port est connecté à un switch qui segmente

le réseau interne en plusieurs VLANs. Cela permet de séparer les différents segments du réseau pour des raisons de performance et de sécurité.

• **Port 4 : Zone DMZ :** Ce port est dédié à la zone démilitarisée (DMZ), où est placé un serveur web. La DMZ permet de sécuriser le serveur web en le plaçant dans une zone tampon entre le réseau interne et l'Internet.

• **Port 5 : Connexion à Nagios :** Ce port connecte directement le pare-feu au serveur Nagios, permettant la supervision directe de l'état et des performances du pare-feu.

5.3.1.1 Tableaux d'adressage

Les tableaux ci-dessous représentent l'adressage utilisé pour les différents équipements.

♦ Le tableau 5.1 représente l'adressage des équipements.

Nom de l'équipement	**Interfaces**	**Adresse IP**
Pare-feu Fortigate	Port 1 (WAN)	192.168.122.254/24
	Port 2 (parfeau_access)	172.17.10.254/24
	Port 3 (LAN)	/
	Port 4 (DMZ)	192.168.200.254/24
	Port 5 (management_nagios)	192.168.146.254/24

Tableau 5.1 – Tableau d'adressages de l'équipement : pare-feu Fortigate

♦ Le tableau 5.2 est le tableau d'adressage des VLANs :

Nom	**ID**	**Adresse sous-réseau**	**La passerelle**
Section réseau	10	192.168.10.0 /24	192.168.10.254
Section sécurité	20	192.168.20.0 /24	192.168.20.254
Section SI	30	192.168.30.0 /24	192.168.30.254

Tableau 5.2 – Tableau d'adressage des VLANs

♦ Le tableau 5.3 est le tableau d'adressage des serveurs de la DMZ :

Nom de l'équipement	**Adresse IP**
DNS	192.168.200.100 /24

Tableau 5.3 – Tableau d'adressage des serveurs de la DMZ.

♦ Le tableau 5.4 est le tableau d'adressage des équipements de superviseur nagios :

Nom de l'équipement	**Adresse IP**
Nagios	192.168.146.132/24
Nagios_access	192.168.146.131/24

TABLEAU 5.4 – Tableau d'adressage des équipements de superviseur Nagios

5.3.2 Simulation

Dans cette section nous allons présenter les différentes configurations effectuées.

5.3.2.1 Configuration des VLANs

La segmentation en VLANs (Virtual Local Area Networks) améliore la gestion et la sécurité du réseau en isolant les différentes parties selon leur fonction ou niveau de sécurité. Avant de superviser ces segments avec nagios, il est crucial de configurer correctement les VLANs sur les équipements réseau. Cette section détaille les étapes nécessaires pour cette configuration.

♦ **Configuration des Noms des VLANs :**

La figure suivant montre les noms attribués à chaque VLAN. Chaque VLAN est identifié par un numéro.

FIGURE 5.3 – Création des VLANs

♦ Après la création des VLANS , nous allons ensuite vérifier leurs créations avec la commande « **show vlan** » comme le montre la figure suivante :

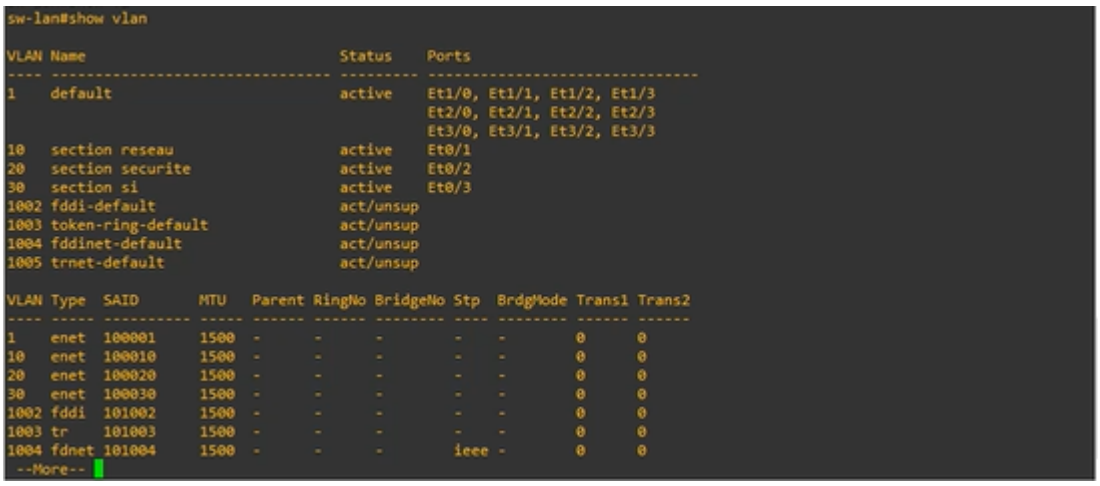

FIGURE 5.4 – Vérification de la création des VLANs

♦ Configuration des vlans en mode Access :

La figure 5.5 montre les interfaces configurées en mode access pour des VLANs spécifiques.

FIGURE 5.5 – Configuration des interfaces VLANs en mode access

♦ Configuration des vlans en mode trunk :

La figure 5.6 montre la configuration des interfaces VLANs en mode trunk.

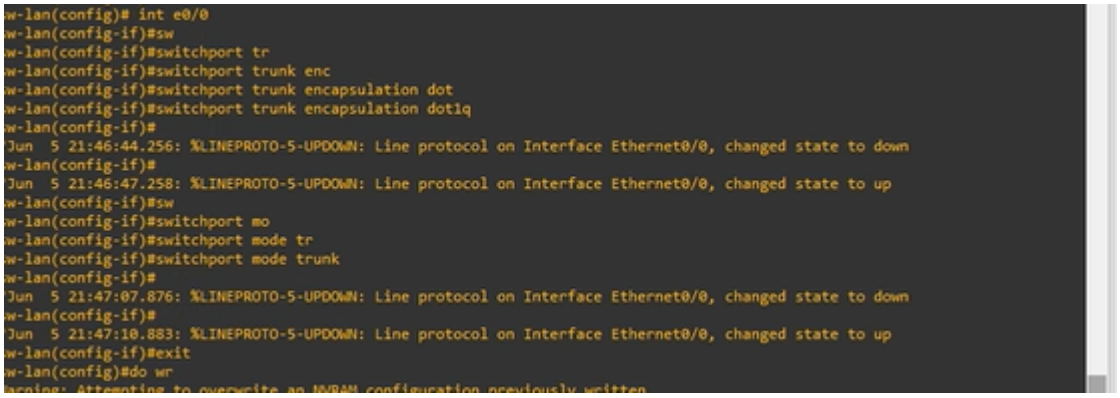

FIGURE 5.6 – Configuration des interfaces VLANs en mode trunk

5.3.2.2 Configuration de parfeu

La configuration du pare-feu est une étape cruciale pour assurer la sécurité et le bon fonctionnement de votre réseau. Le pare-feu contrôle le trafic entre les différents segments du réseau, appliquant des règles strictes pour autoriser ou bloquer les communications. Dans cette section, nous détaillerons la configuration des ports et des règles de filtrage sur le pare-feu FortiGate, afin de garantir une communication sécurisée et efficace entre les VLANs, la zone DMZ, et l'accès à internet.

♦ **Configuration du DHCP pour un VLAN :**

Dans cette capture, nous configurerons le service DHCP pour un VLAN spécifique sur le pare-feu. Cette configuration comprendra :

A. le nom de de vlan et la passerelle :

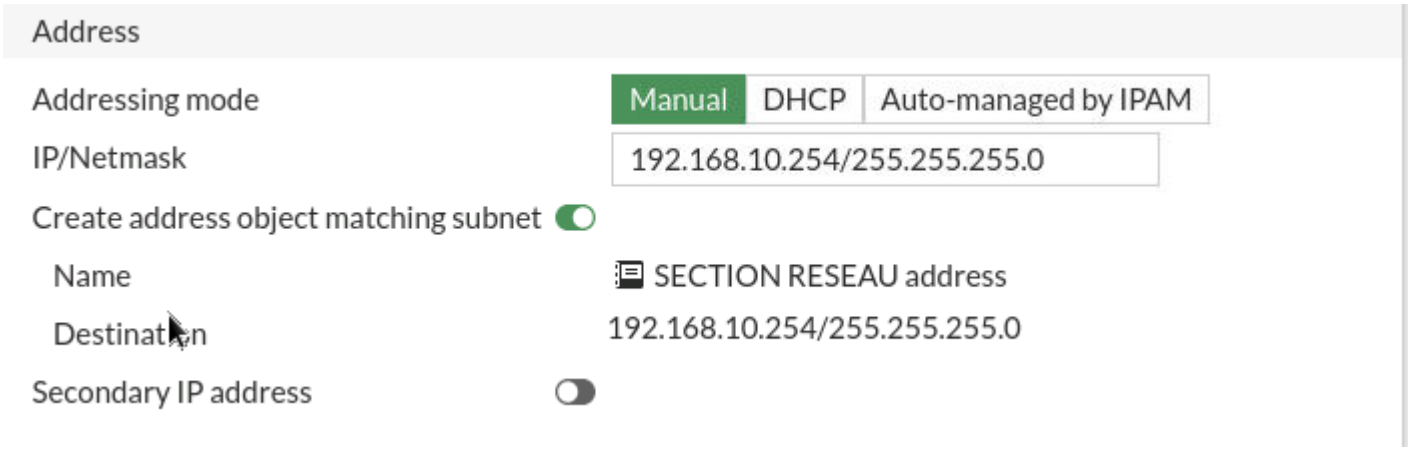

FIGURE 5.7 – Passerelle de VLan 10

B. la définition de la plage d'adresses IP :

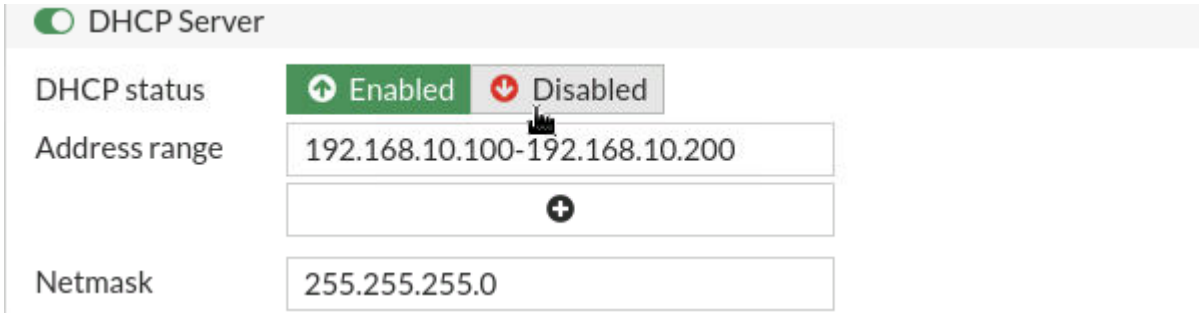

FIGURE 5.8 – Plage dhcp de Vlan 10

C. Et les protocoles autorisée vers cette interface :

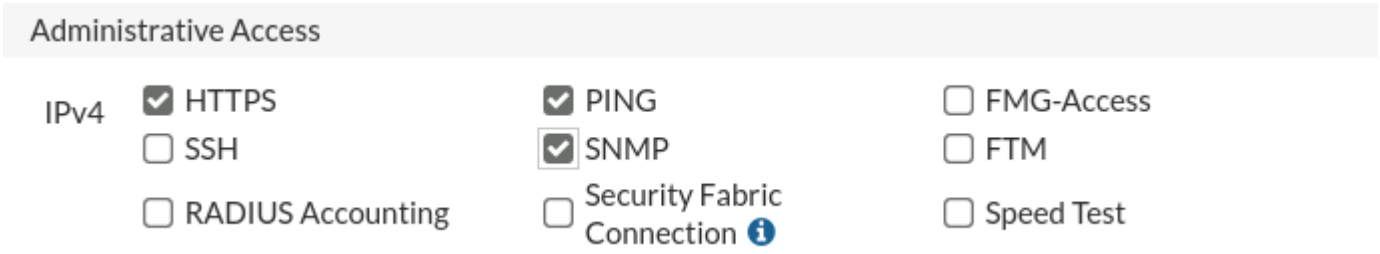

FIGURE 5.9 – Protocoles autorisés vers Vlan 10

Nous allons répéter cette opération pour tous les vlan et tous les ports connecter de fortigate chacun avec son adresse IP et ces paramètres spécifiques.

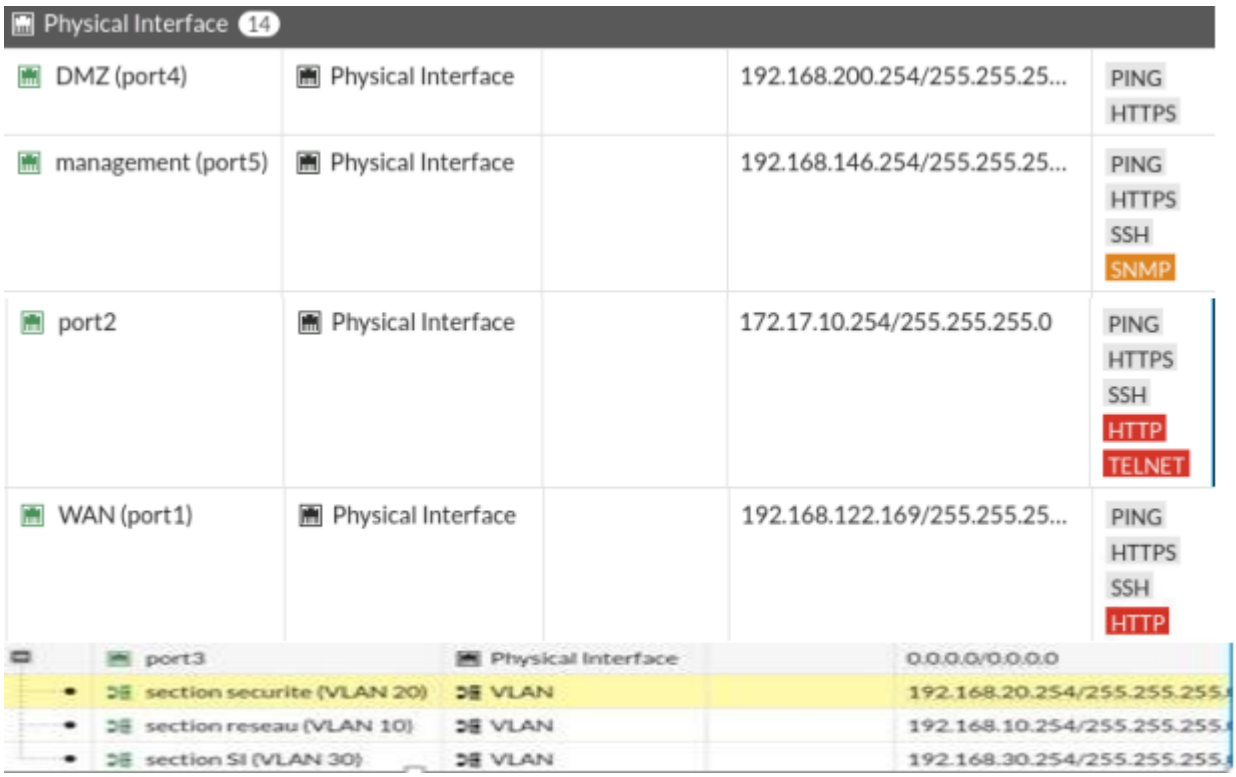

FIGURE 5.10 – Configuration des ports de parfeu

♦ Création de la zone locale :

Dans cette section nous allons créer une zone locale pour assurer une communication sécurisé et efficace entre ces VLANS .

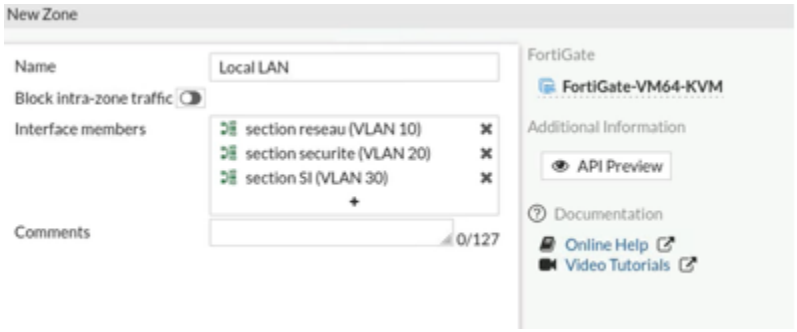

FIGURE 5.11 – Création de la zone locale Lan

♦ Configuration des Règles et Politiques sur le Pare-feu FortiGate :

Le pare-feu FortiGate est configuré par défaut pour bloquer tout le trafic, assurant ainsi une première ligne de défense robuste pour le réseau. Cependant, pour permettre un flux de données sécurisé et contrôlé, des règles spécifiques sont définies et appliquées. Comme suite :

✓le trafic du réseau interne vers le réseau externe est autorisé.

✓le trafic du réseau interne vers la DMZ est autorisé.

✓le trafic du serveur nagios vers tout le réseau est autorisé.

5.3.2.3 Installation et configuration de fully automated nagios

fully Automated Nagios (FAN) est une distribution Linux basée sur CentOS, conçue pour simplifier la mise en place rapide d'un serveur de supervision complet. Elle intègre Nagios pour la surveillance proactive de l'infrastructure informatique, avec une configuration facilitée grâce à Centreon pour la gestion avancée des données de surveillance et à NagVis pour la visualisation graphique interactive de l'état du réseau.

fully Automated Nagios (FAN) se distingue par sa capacité à installer Nagios et ses plugins, Centreon et NagVis sans nécessiter une configuration détaillée, offrant ainsi une solution prête à l'emploi pour lesa dministrateurs système. Cette distribution utilise NDOutils pour assurer la communication efficace entre Nagios et Centreon, facilitant le transfert des données de surveillance.

L'installation traditionnelle de ces outils peut souvent être complexe et décourager les utilisateurs. FAN résout ce problème en fournissant une image ISO prête à l'emploi, permettant une installation rapide et simplifiée de tous les logiciels nécessaires à une supervision informatique complète.

Nous allons voir les étapes de son installation :

1. Interface initial de fan :

FIGURE 5.12 – Interface initial de fan

2. Le choix de la langue :

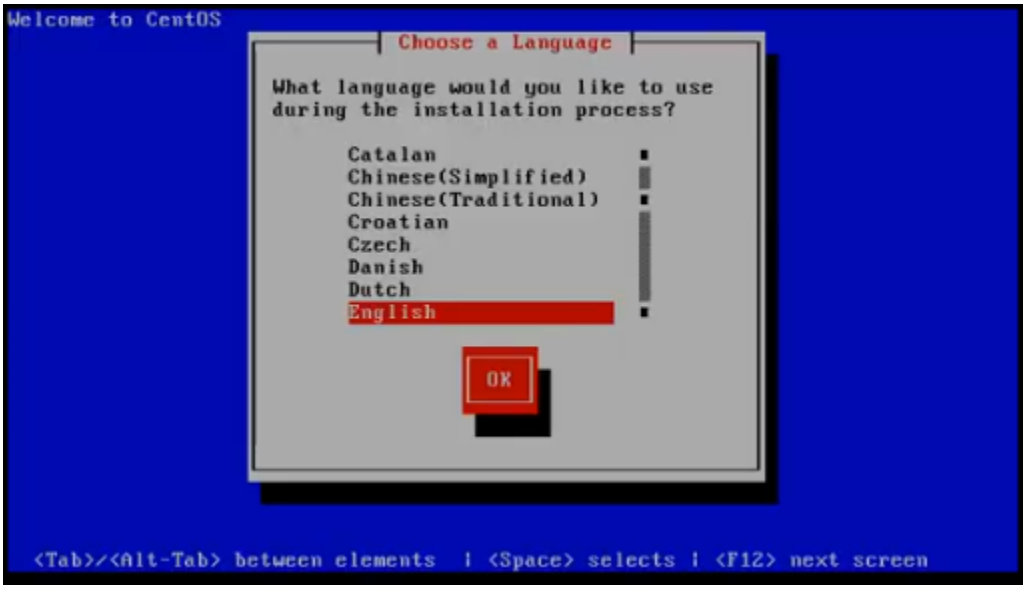

FIGURE 5.13 – Choix de la langue

3. L'installation des outils :

FIGURE 5.14 – Installation des outils

4. Définition de mot de passe :

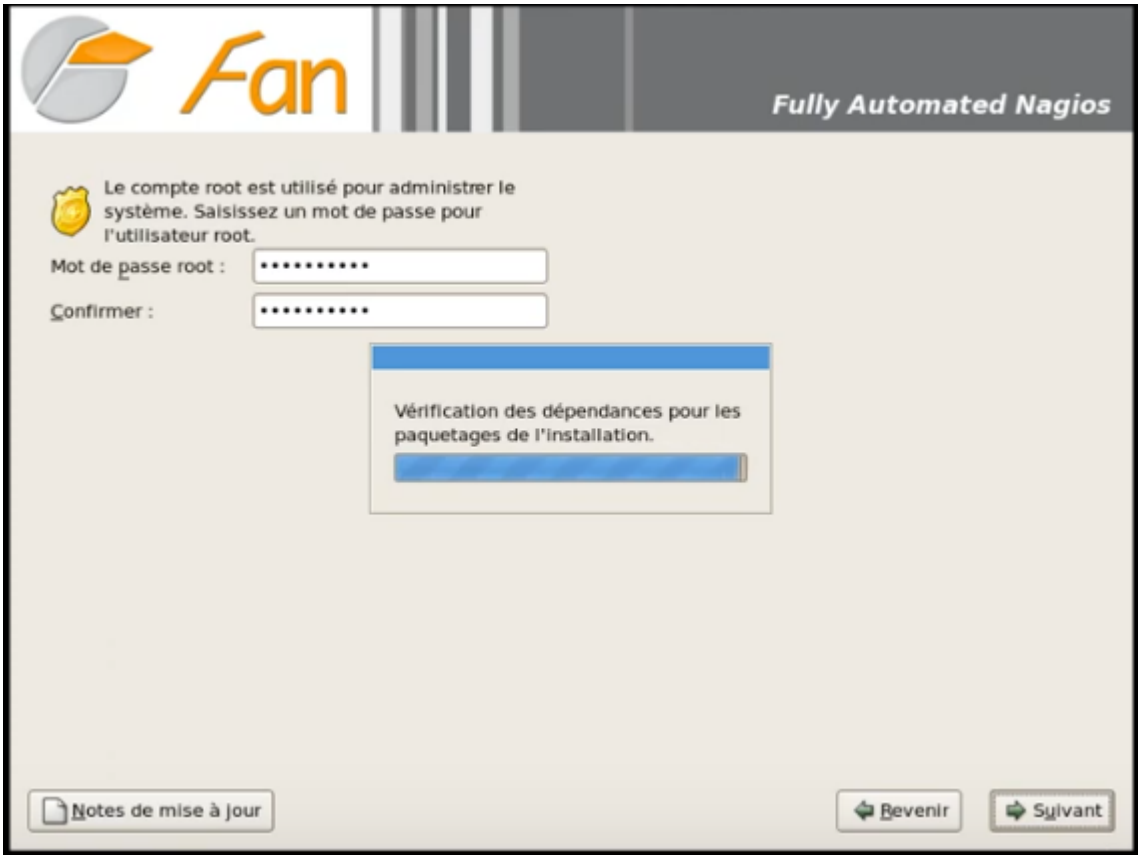

FIGURE 5.15 – Définition de mot de passe

5. Apres avoir installer on passe a la configuration de l'adresse ip de l'interface eth0 avec la commande ifconfig :

```
System      : FAN 2.4

localhost login: root
Password:
Last login: Mon Jun 10 22:17:48 on tty1
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:2C:0D:E1
          inet addr:192.168.146.132  Bcast:192.168.146.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe2c:de1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:1980 (1.9 KiB)
```

FIGURE 5.16 – Configuration de l'adresse IP de FAN

6. Connecter a l'interface web de fan :

FIGURE 5.17 – Interface web de FAN

5.3.2.4 Configuration des hôtes et des services

5.3.2.4.1 Configuration d'une machine Ubuntu :

• Initialement pour l'ajout d'un hôte, nous devons nous connecter à l'interface web Centreon ensuite se rendre dans le menu **Configuration** > **Hosts** > **Hosts** et cliquer sur le bouton **Add**

• Accéder à un formulaire permettant de définir notre équipement. En remplissant les champs du premier formulaire indiqué dans la figure suivante :

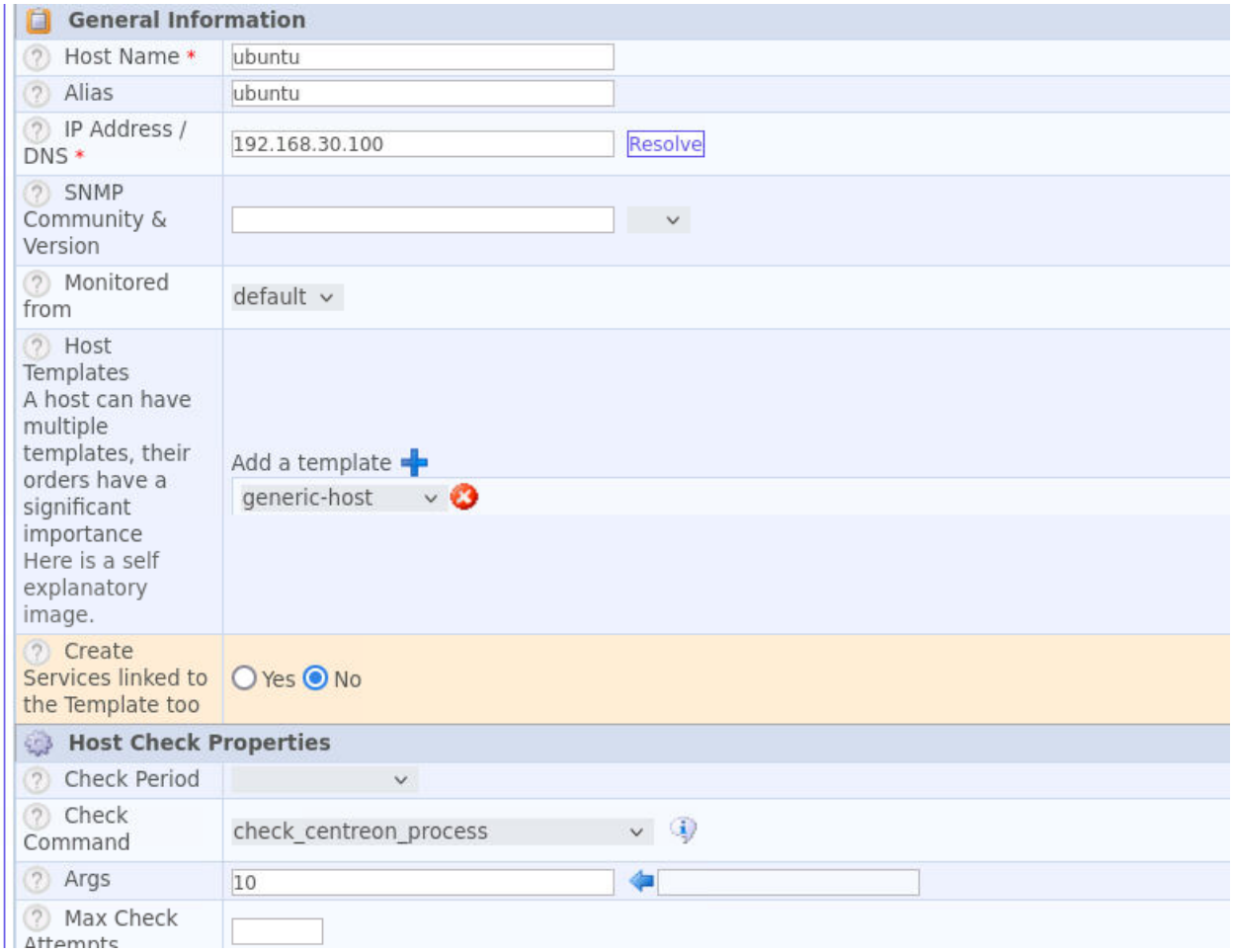

FIGURE 5.18 – Ajout de l'hôte ubuntu

Pour démarrer on remplit les champs suivants :

• Le champ Host Name définit le nom d'hôte qui sera utilisé par le moteur de supervision ubuntu .

• Le champ Alias indique l'alias de l'hôte. l'hôte ubuntu .

• Le champ IP address / DNS Adresse IP ou nom DNS de l'hôte.@ip 192.168.30.100.

• Les champs SNMP Community & Version contiennent respectivement le nom de la communauté ainsi que la version SNMP.

• Le champ Monitored from indique quel est le serveur de supervision chargé de superviser cet hôte.

• Le champ Host Templates permet d'associer un ou plusieurs modèles d'hôtes à cet objet.

Après remplissage des champs on clique sur bouton Save pour sauvegarder les modifications.

• charger le fichier de configuration de mchine ubuntu

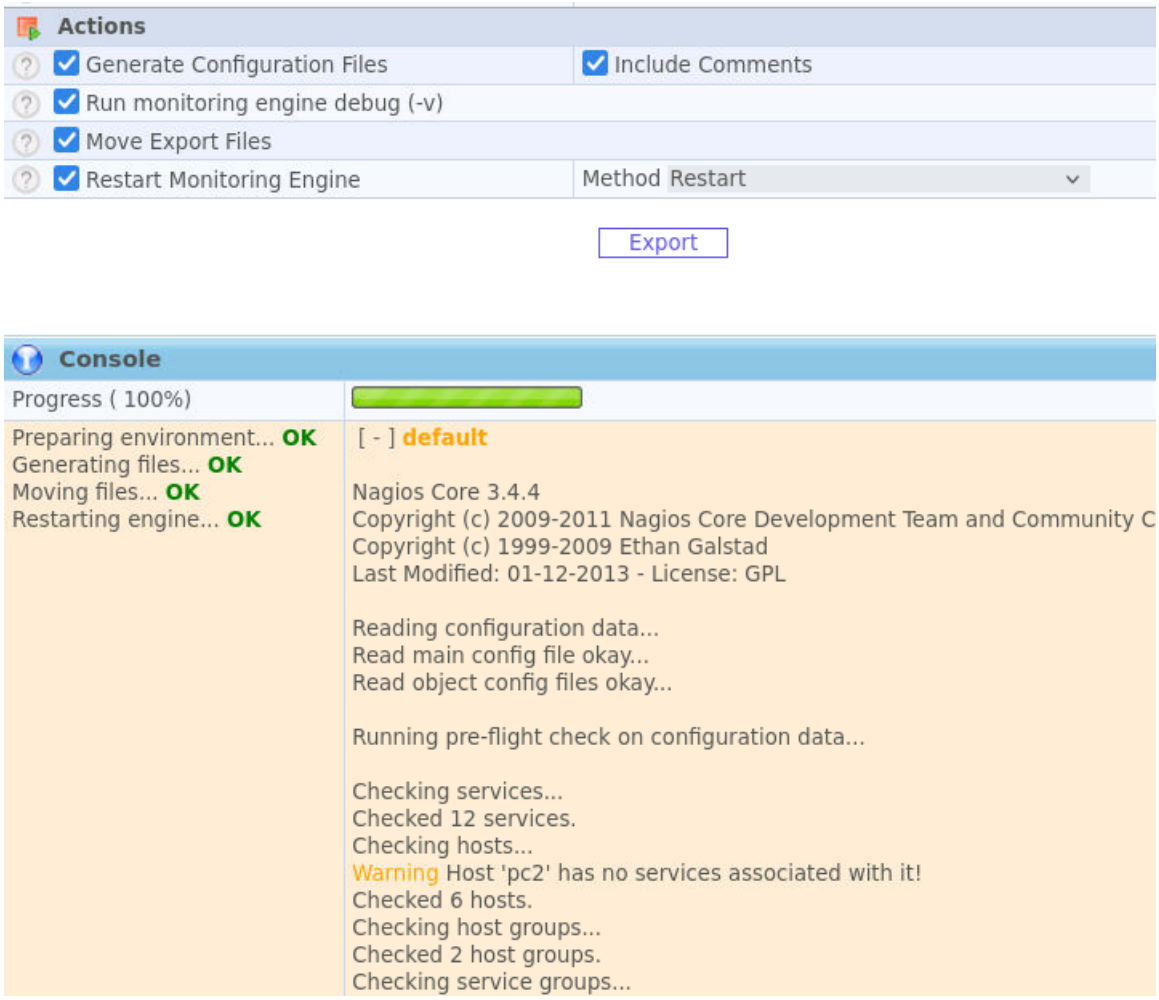

FIGURE 5.19 – Chargement le fichier de configuration de mchine ubuntu

5.3.2.4.2 Configuration des services :

Pour superviser l'utilisation de la mémoire et l'utilisation de cpu d'une machine Ubuntu et générer des alertes via FAN , on doit :

A. installer les plugins NRPE (Nagios Remote Plugin Executor) necessaire sur la machine ubuntu avec la commande .

```
sudo apt update
sudo apt install nagios-nrpe-server nagios-plugins
```

FIGURE 5.20 – Installation des plugins

B. Éditez le fichier de configuration NRPE pour Autoriser les connexions depuis le serveur nagios :

```
sudo nano /etc/nagios/nrpe.cfg
```

FIGURE 5.21 – Fichier plugins

```
allowed_hosts=127.0.0.1,192.168.146.132
```

FIGURE 5.22 – Autorisation de connexions de serveur nagios

C. Ajouter une commande Pour superviser la charge CPU du machine ubuntu et générer une alerte CRITICAL si la charge CPU et l'utilisation de la mémoire est égale à 90ou plus ou une alerte WARNING si la charge CPU et l'utilisation de la mémoire est égale à 80 % ou plus.

```
command[check_mem]=usr/lib/nagios/plugins/check_nrpe -H localhost -c check_mem
command[check_cpu]= usr/lib/nagios/plugins/check_cpu -w 80 -c 90
```

FIGURE 5.23 – Commandes de la verification

D. pour l'ajout d'une commande de verification nous devons nous connecter à l'interface web Centreon puis la section **Services** >**Commands** et ajoutez une nouvelle commande de vérification pour l'utilisation de la mémoire et utilisation cpu.

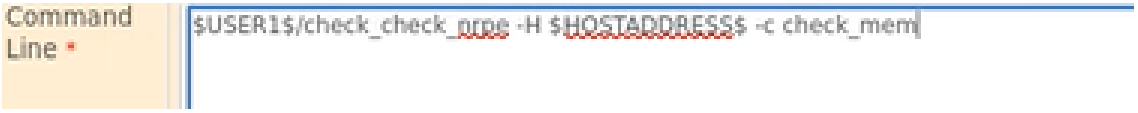

FIGURE 5.24 – Check_memory

E. ajouter un nouveau service de vérification de mémoire avec la commande configurer et definir les parametttre de l'alarte .

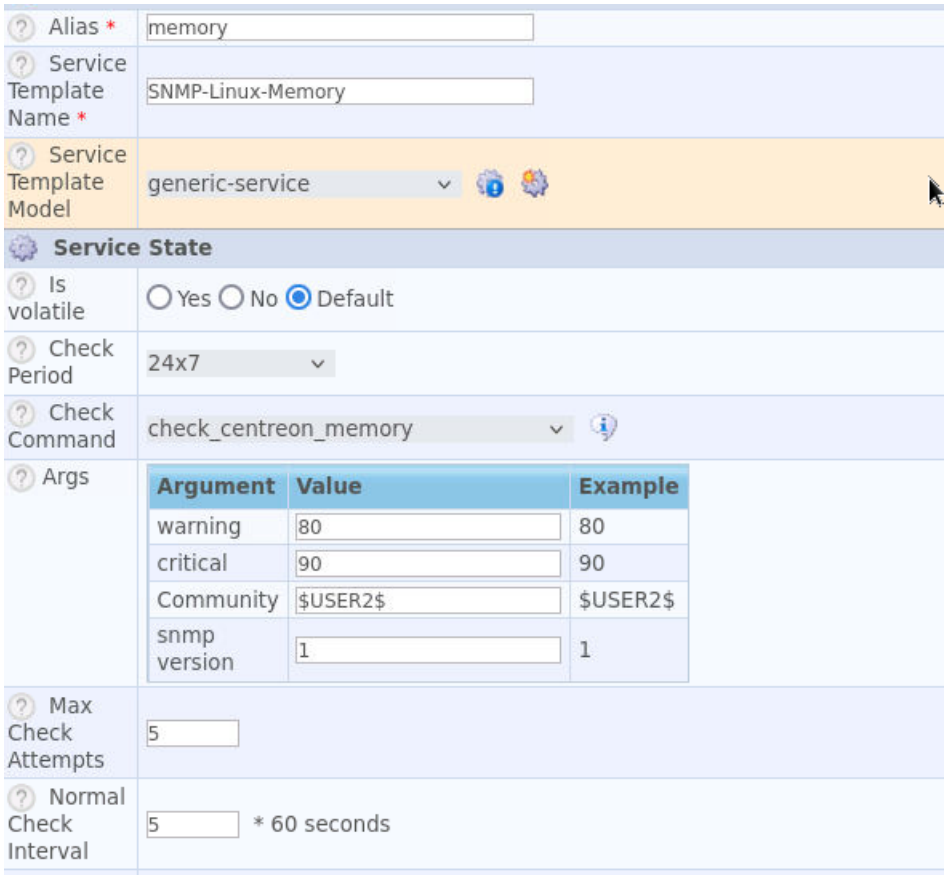

FIGURE 5.25 – Configuration des paramètres de service memory

F. Activer le protocole snmp sur la machine ubuntu .

```
sudo apt update
sudo apt install snmpd snmp

sudo nano /etc/snmp/snmpd.conf

 agentAddress  udp:161,udp6:[::1]:161

rocommunity public default
```

FIGURE 5.26 – Commandes d'activation de protocole SNMP sur ubuntu

5.3.2.4.3 Configuration d'un switch :

A. Pour superviser un switch de niveau 2 il faut créer un vlan de gestion et attribuer un addreess ip :

```
sw-mgmt(config)#int vlan 1
sw-mgmt(config-if)#ip add 192.168.146.1 255.255.255.0
sw-mgmt(config-if)#no sh
sw-mgmt(config-if)#
*Jun 12 16:42:35.713: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jun 12 16:42:36.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
sw-mgmt(config-if)#ex
```

FIGURE 5.27 – Création des vlans et attribution d'adresses ip

B. Activer le service snmp :

```
sw-mgmt(config)#snmp-server community public RO
sw-mgmt(config)#snmp-server host 192.168.146.132 mycommunity
```

FIGURE 5.28 – Activation de snmp dans switch de niveau 2

5.3.2.4.4 Configuration de parfeu :

Pour superviser le parfeu il faut

A. Ajouter le parfeu à le serveur nagios :

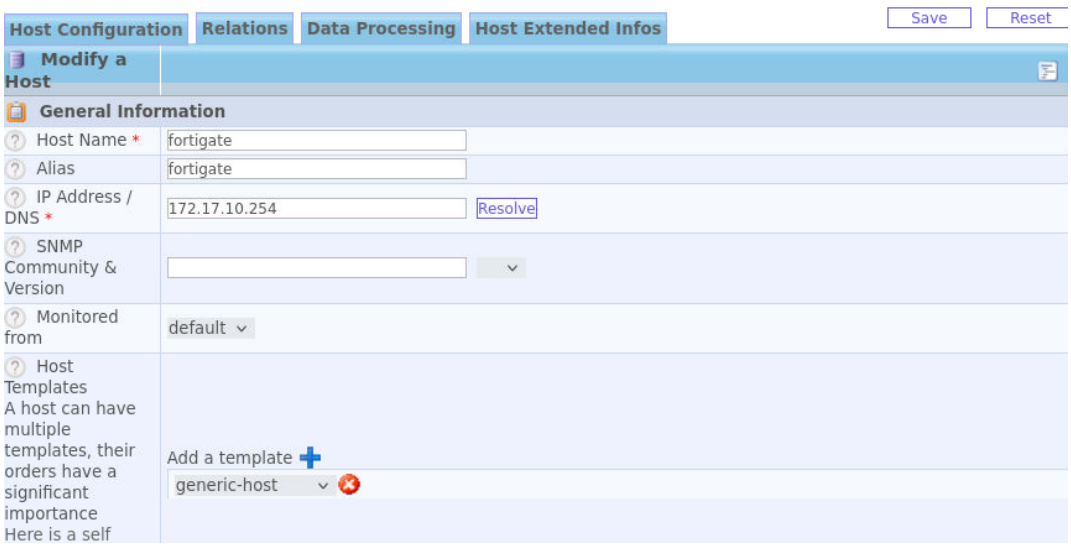

FIGURE 5.29 – Ajout de parfeu

B. Autoriser le prtocole snmp à collecter des informations sur le parfeu :

FIGURE 5.30 – Autorisation de protocole snmp

C. Difinir le service à superviser par exemple nous allons surveillons le service dhcp sur le port 3 avec la commande prédéfinie check_dhcp

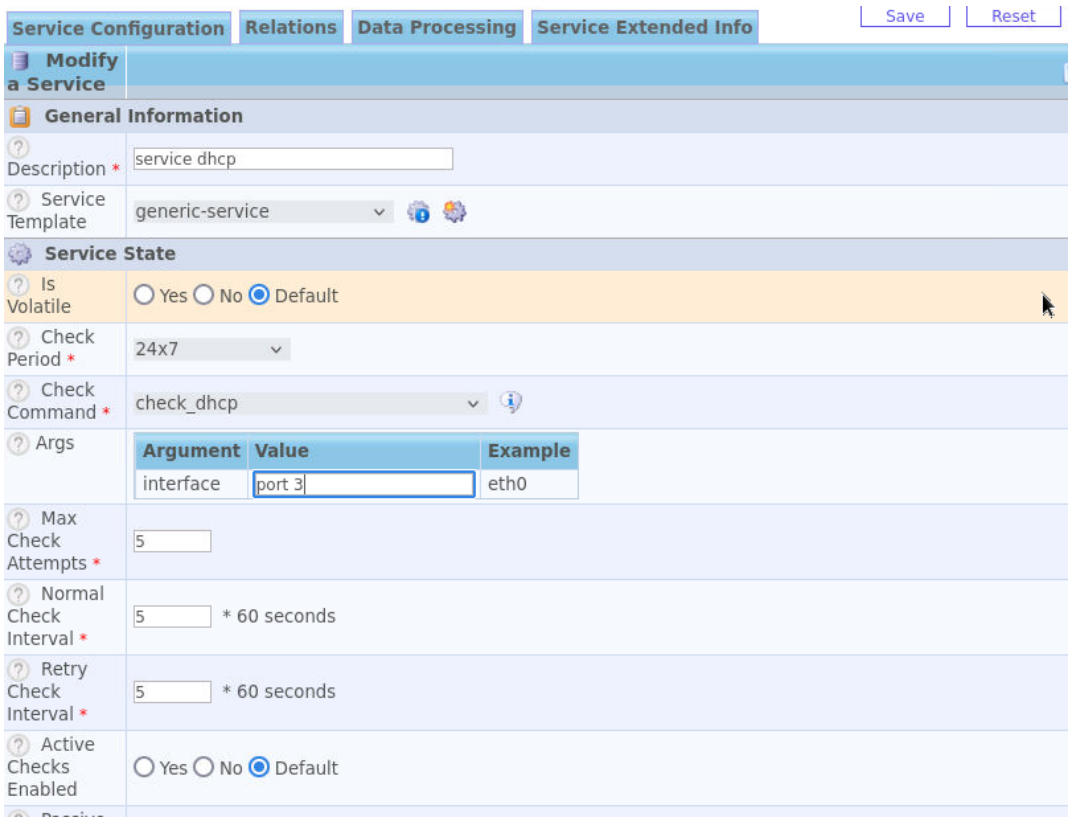

FIGURE 5.31 – Difinir le service dhcp

5.3.2.4.5 Configuration de serveur DNS

Pour superviser le serveur dns il faut

A.Ajout de serveur DNS :

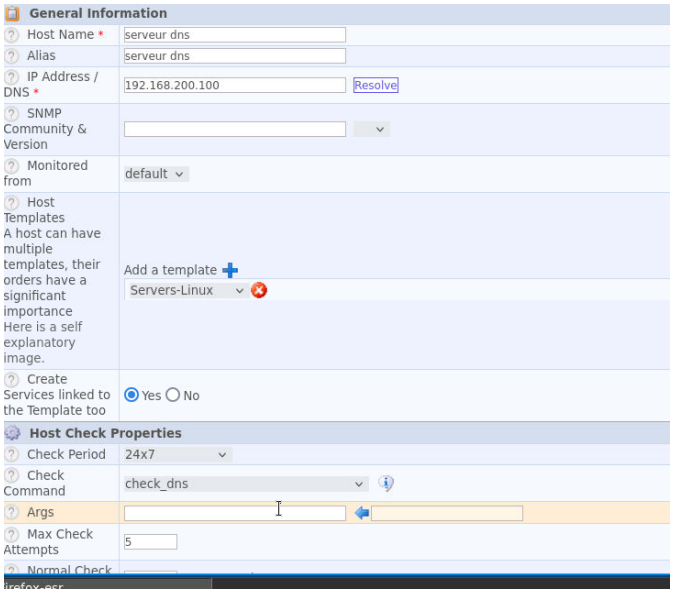

FIGURE 5.32 – Ajout de service DNS

B.Definir le service DNS avec la commande check_dns :

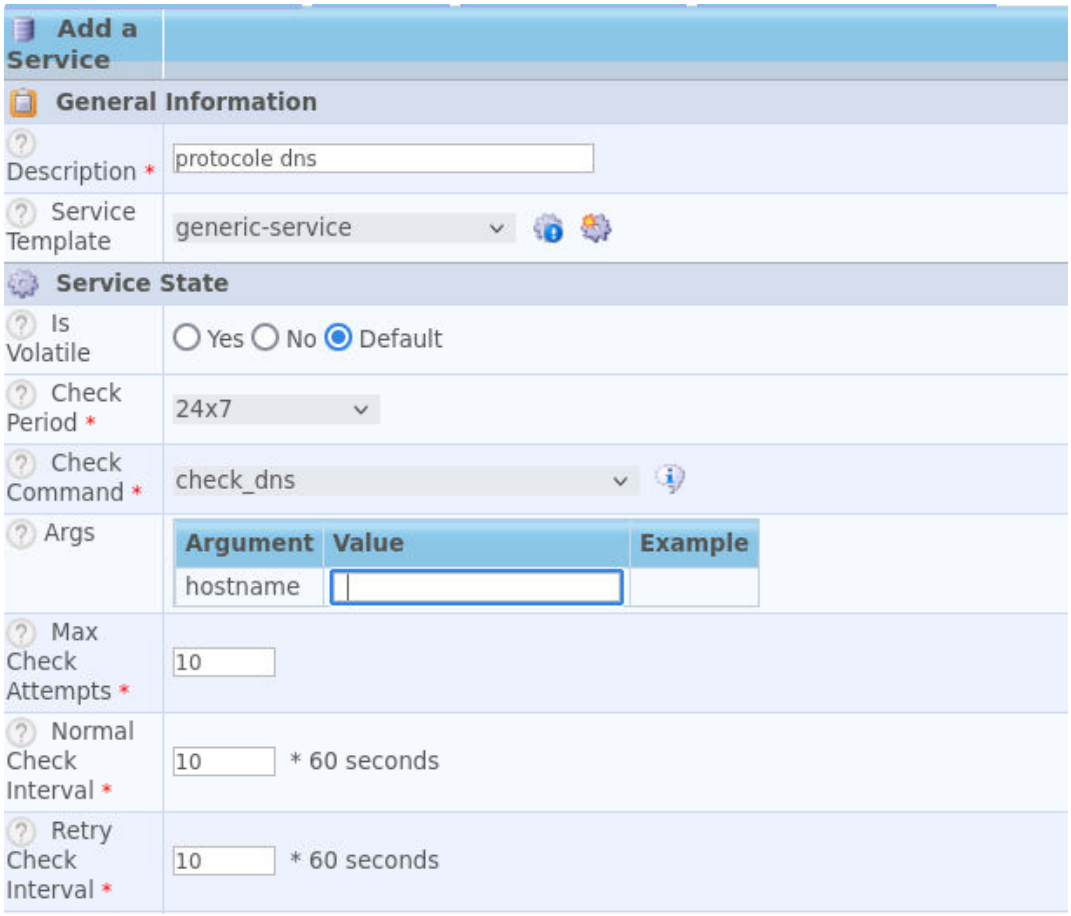

FIGURE 5.33 – Definir le service dns

C.Associer le serveur avec service dns :

FIGURE 5.34 – Associer le serveur avec service dns

5.3.2.5 Résultat de la supervision de tous les services

• Les resultat de supervision des services :

Hosts	Services	Status	Duration	Last Check	Tries
Centreon-Server	/	OK	3w 1d 5h 18m 37s	27/06/2024 01:23:25	1/3 (H)
	ping	OK	3w 1d 5h 17m 37s	27/06/2024 01:23:48	1/3 (H)
fortigate	ping	OK	1h 14m 8s	27/06/2024 01:21:30	1/3 (H)
	service dhcp	UNKNOWN	1w 6d 21h 4m 19s	27/06/2024 01:24:11	5/5 (H)
sw-mgmt	etat de interface	UNKNOWN	2w 3h 51m 16s	27/06/2024 01:17:16	10/10 (H)
	ping	OK	1h 15m 41s	27/06/2024 01:24:57	1/3 (H)
ubuntu	ping	OK	17m 59s	27/06/2024 01:22:39	1/3 (H)
	utilisation de memory	OK		N/A	1/5 (H)

FIGURE 5.35 – Résultat de supervision des services

• Des alertes si l'utilisation de mémoire et cpu dépasse 90% :

	utilisation cpu	CRITICAL	14h 45m 56s	13/06/2024 07:30:28	4/4
	utilisation_de_memoire	CRITICAL	10h 41m 4s	13/06/2024 07:34:11	3/3

FIGURE 5.36 – Alertes

• Creation des rapports sur l'etat de reseau nagios donne a les administrateurs la possibilite de créer des rapports sur l'etat de leurs réseaux :

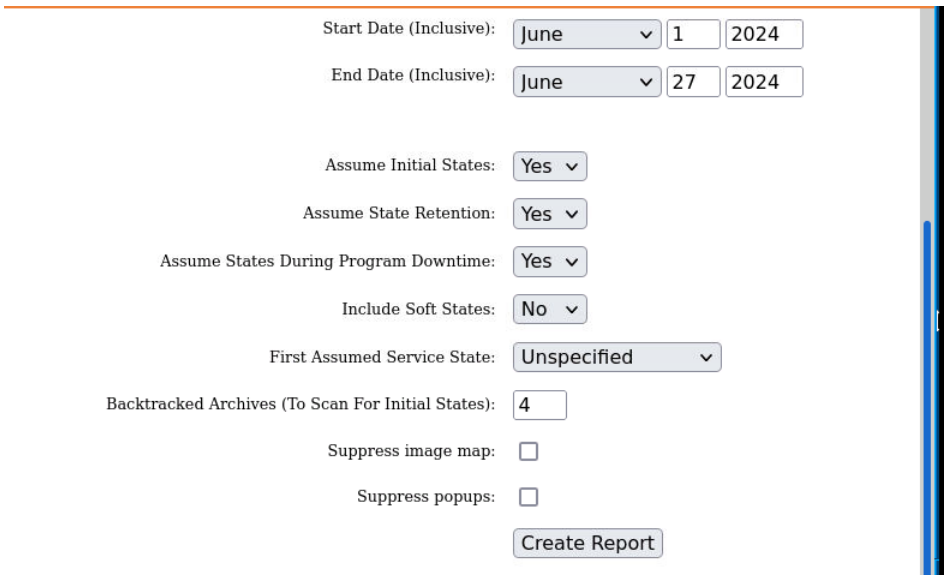

FIGURE 5.37 – parametttres de création des rapports

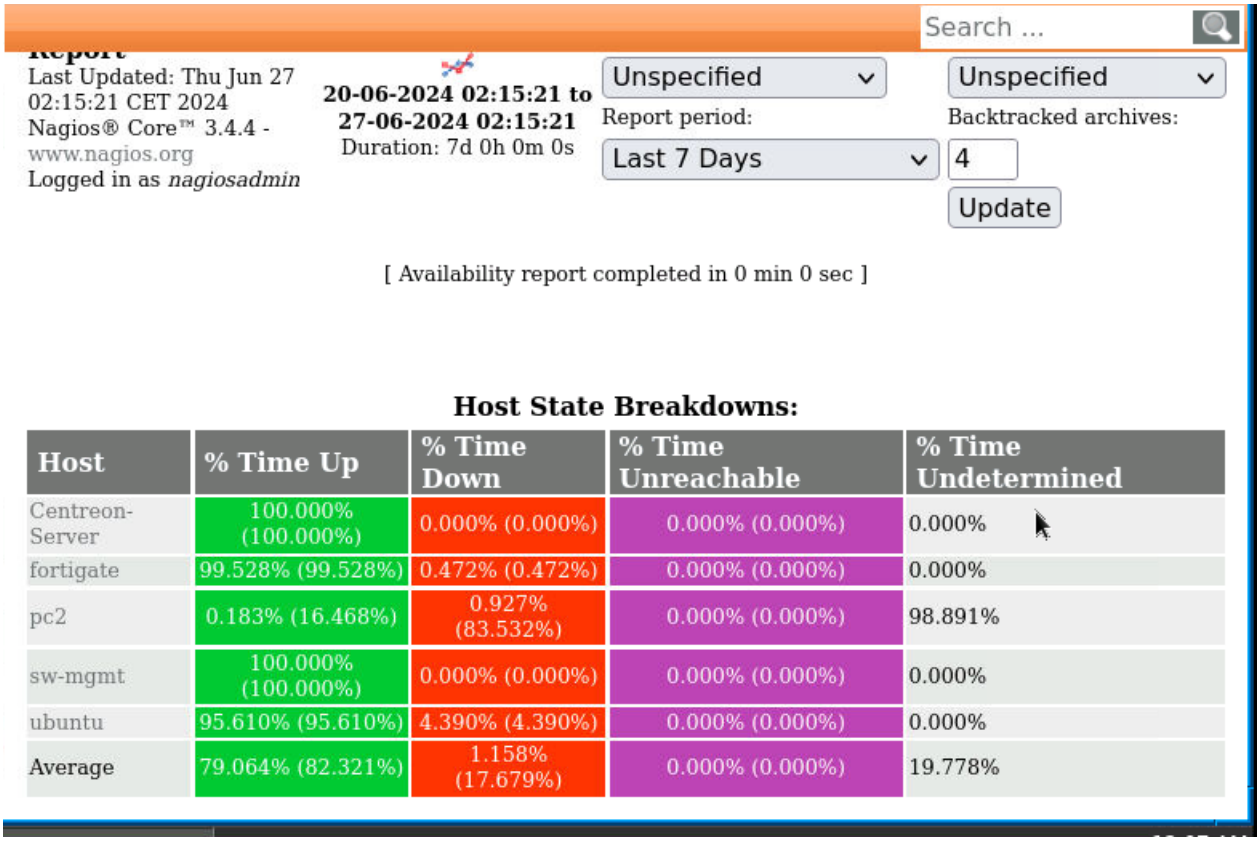

FIGURE 5.38 – Creation des rapports sur l'etat de reseau

- La sauvegarde des alertes :

FIGURE 5.39 – Sauvegarde des alertes

5.4 Conclusion

Dans ce chapitre, nous avons décrit l'aspect pratique de notre projet, où nous avons expliqué les étapes configuration de notre réseau et comment installer et superviser avec la solution fully automated nagios et tester cette solution sur quelques équipement de centre de calcul de l'université de bejaia .

Conclusion générale

L'administration et la supervision des réseaux informatiques sont des composantes essentielles pour assurer la disponibilité, la performance et la sécurité des systèmes d'information. Ce mémoire a exploré de manière approfondie les différents aspects de la gestion des réseaux, en mettant particulièrement l'accent sur l'importance de la supervision proactive pour prévenir et résoudre les problèmes potentiels.

Notre étude a été concrétisée par un stage pratique au Centre des Systèmes et Réseaux de l'Université de Béjaïa. Cette expérience nous a permis de mettre en application les concepts théoriques appris, en utilisant Nagios. Nous avons pu constater les avantages significatifs de Nagios en termes de détection rapide des anomalies, de diagnostic précis et de notification en temps réel, ce qui en fait une solution robuste pour la surveillance des infrastructures réseau.

Les résultats obtenus montrent que, malgré la complexité de configuration et la nécessité de compétences techniques spécialisées, Nagios offre une flexibilité et une efficacité supérieures pour la supervision des réseaux. Sa capacité à intégrer divers plugins et à fournir des alertes détaillées en fait un choix idéal pour les environnements nécessitant une surveillance continue et proactive.

En conclusion, la supervision des réseaux informatiques est un domaine complexe mais essentiel pour le maintien de l'intégrité, de la performance et de la sécurité des systèmes d'information. À travers l'étude de cas du Centre des Systèmes et Réseaux de l'Université de Béjaïa, ce mémoire a démontré que l'utilisation de Nagios constitue une solution robuste et flexible pour la surveillance proactive des infrastructures réseau. Les compétences et les connaissances acquises durant ce projet nous ont non seulement permis de mieux comprendre les défis de l'administration des réseaux, mais également d'appréhender les meilleures pratiques pour garantir un fonctionnement optimal des systèmes d'information.

Bibliographie

[1] R.Mohanakrishnan. What is a computer network ? definition, objectives, components, types, and best practices, 2024.

[2] https://www.geeksforgeeks.org/types-of-computer-networks/, Consulté le 1/03/2024.

[3] https://sti2d.ecolelamache.org/ii_rseaux_informatiques___7_topologie_des_rseaux.html, Consulté le 4 mars 2024.

[4] https://fad.umi.ac.ma/Support_de_Cours_reseau_FST_chap3.pdf, Consulté le 14 mai 2024.

[5] J.-L. Montagnier. *Réseaux d'entreprises par la pratique*. Éditions Eyrolles, 2010.

[6] https://www.cloudflare.com/fr-fr/learning/ddos/glossary/open-systems-interconnection-model-osi/, Consulté le 6 mars 2024.

[7] https://en.wikipedia.org/wiki/OSI_model, Consulter le 06/03/2024.

[8] N.Belhadj. Etude et conception d'une plateforme de réseau informatique couplant entre sécurité et supervision pour l'entreprise eniem, 2024.

[9] R.G.Yende. *Cours d'administration des réseaux informatique*. 2019.

[10] https://fr.wikipedia.org/wiki/Supervision_%28informatique%29, Consulter le 10 mars 2024.

[11] S. Nataf, V. Bel, and F. Veysset. « techniqe de supervision de la sécurité des réseaux ip ». 2010.

[12] S.Vacore. Mettez en place un outil de supervision de production avec nagios, 2024.

[13] https://www.zabbix.com.

[14] L.Guillaume. Gestion du déploiement d'une solution de supervision réseau multi-sites. *Systèmes et contrôle*, 2017.

[15] http://www.univ-bejaia.dz, Consulté le 15 mai 2024.

[16] T. Nejiba and S. Djebbi. Sécurisation des routeurs cisco. Rapport de stage de perfectionnement, Université Virtuelle de Tunis, 2010-2011.

[17] https://all-it-network.com/gns3/, Consulté le 10/06/2024.

[18] http://eip.epitech.eu/2013/gns3/fr/project.html/, Consulter le 10/06/2024.

RÉSUMÉ

Notre projet concerne la **supervision des réseaux** au sein d'un Centre des Systèmes et Réseaux d'Information, de Communication de Téléenseignement et de l'Enseignement à Distance de l'université de Béjaia (**CSRICTED**). Le travail vise à montrer comment une supervision efficace peut être mise en œuvre pour garantir la performance et la sécurité des réseaux. Les objectifs principaux de cette étude étaient d'analyser les différentes techniques de supervision des réseaux, d'identifier les outils les plus adaptés pour cette tâche, et de mettre en place une solution de supervision. L'étude s'est concentrée sur l'utilisation de **fully Automated Nagios (FAN)** comme **outil de supervision** à base de protocole SNMP.

Les résultats obtenus montrent que l'intégration de cet outil permet de créer une infrastructure robuste et réactive pour la surveillance de réseau. La mise en œuvre de **Nagios** a permis de détecter et de résoudre proactivement les problèmes réseau, améliorant ainsi la performance globale du centre de calcul. Ce projet montre l'importance de la supervision proactive des réseaux informatiques pour maintenir leur performance et leur sécurité.

Mots clés : Supervision des réseaux informatiques, CSRICTED, Outils de la supervision, GNS3,VMware, Nagios et Fully Automated Nagios.

ABSTRACT

Our project concerns the **supervision of networks** at the Centre des Systèmes et Réseaux d'Information, de Communication de Téléenseignement et de l'Enseignement à Distance at the University of Béjaia (**CSRICTED**). The aim of the work is to show how effective supervision can be implemented to guarantee network performance and security. The main objectives of this study were to analyse the various network supervision techniques, identify the most suitable tools for this task, and implement a supervision solution. The study focused on the use of **Fully Automated Nagios (FAN)** as a **monitoring tool** based on the SNMP protocol.

The results obtained show that the integration of this tool makes it possible to create a robust and responsive infrastructure for network monitoring. The implementation of **Nagios** has enabled network problems to be detected and resolved proactively, thereby improving the overall performance of the computer centre. This project demonstrates the importance of proactively monitoring IT networks to maintain their performance and security.

Key words : supervision of networks, CSRICTED, monitoring tool, GNS3,VMware, Nagios and Fully Automated Nagios.