الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسما لإلكترونيك
Département d'Électronique

Mémoire de Master

Mention Électronique
Spécialité : Systèmes des télécommunications (ST)

Présenté par

BEKHAT RAMZI

&

CHENAIT ABDELKARIM

Simulation de la Supervision d'un réseau informatique par SNMP

Cas université de Blida1

Proposé par : Y.Kabir

Année Universitaire 2020-2021

Remerciement

Nous tenons à remercier, d'abord et avant tout, le bon DIEU de nous avoir donné la force et la volonté nécessaire pour la réalisation de cet humble travail,

Puis, nous adressons nos vifs remerciements et notre pleine gratitude

A :

Notre encadreur M^{r} Y. Kabir. De nous avoir encadré et orienté tout au long de ce projet, et pour ses encouragements, conseils et disponibilité.

Aussi, nous tenons à remercier tous ceux qui nous ont soutenu de près ou de loin pour que ce mémoire puisse voir le jour.

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

DEDICACES

Au nom de Dieu, le Tout Miséricordieux, le Très-Miséricordieux,

Toutes les lettres ne sauraient trouver les mots qu'il faut pour exprimer ma gratitude, mon respect et ma pleine reconnaissance

A mes chers parents qui n'ont épargné aucun effort pour m'épauler, soutenir et me procurer tout ce qu'il faut pour réussir dans la vie afin que je puisse aller toujours de l'avant,

Que Dieu les bénisse,

A mes professeurs particulièrement mon encadreur pour tout ce qu'il m'a appris tout au long de mon cursus universitaire,

Mon frère et mes sœurs, notamment mes neveux Sami et Youcef, sans oublier la princesse Nivine.

Mes grands-parents.

Toute la famille,

Tous mes adorables amis.

Ainsi qu'à tous ceux qui m'ont soutenu par leurs orientations, leurs conseils et leur encouragement pour réaliser ce travail, qu'ils trouvent ici l'expression de ma grande reconnaissance et l'assurance de mes profonds respects.

CHENAIT ABDELKARIM

DEDICACES

Au nom de Dieu, le Tout Miséricordieux, le Très-Miséricordieux,

Toutes les lettres ne sauraient trouver les mots qu'il faut pour exprimer ma gratitude, mon respect et ma pleine reconnaissance

A mes chers parents qui n'ont épargné aucun effort pour m'épauler, soutenir et me procurer tout ce qu'il faut pour réussir dans la vie afin que je puisse aller toujours de l'avant,

Que Dieu les bénisse,

A mes professeurs particulièrement mon encadreur pour tout ce qu'il m'a appris tout au long de mon cursus universitaire,

Mon frère et mes sœurs,

Mes grands-parents.

Toute la famille,

Tous mes adorables amis.

Ainsi qu'à tous ceux qui m'ont soutenu par leurs orientations, leurs conseils et leur encouragement pour réaliser ce travail, qu'ils trouvent ici l'expression de ma grande reconnaissance et l'assurance de mes profonds respects.

BEKHAT RAMZI

Résumé

Le réseau informatique est devenu l'élément essentiel dans tous les domaines de la vie, notamment les services et les sciences, parmi ces exemples nous présentons le réseau LAN universitaire. A cet effet, le protocole SNMP a été produit dans l'optique de surveiller et de gérer un réseau à l'aide de certains logiciels, notamment des logiciels open source et payants.

Pour résumer le projet, nous avons d'abord mis en place le réseau LAN universitaire avec GNS 3 à l'aide d'appareils Cisco (routeurs et switches), puis nous avons installé Nagios avec VMware pour afficher et notifier les changements de réseau et recevoir des alertes et alertes par notre courrier électronique.

Mots clés: LAN, SNMP, GNS 3, Nagios XI, VMware Workstation.

Abstract

The computer network has become the key element in all areas of life, including services and science, among these examples we present the university network called LAN. For this purpose, the SNMP protocol was produced with the aim of monitoring and managing a network with the help of some software, including open source and paid software.

To summarize the project, we first set up the university LAN network with GNS 3 using Cisco devices (routers and switches), then we installed Nagios with VMware to display and notify network changes and receive alerts and alerts through our email.

Keywords: LAN, SNMP, GNS 3, Nagios XI, VMware Workstation.

ملخص:

أصبحت شبكة الكمبيوتر عنصرا أساسيا في جميع مجالات الحياة بما في ذلك الخدمات والعلوم، ومن بين أبرز الأمثلة نذكر شبكة LANالخاصة بالجامعة . لهذا الغرض، تم إنتاج SNMP بغية مراقبة وإدارة الشبكة من خلال استخدام برامج معينة على غرار البرامج مفتوحة المصدر والبرامج المدفوعة. لتلخيص المشروع، قمنا أولاً بإعداد شبكة LANالجامعية مع GNS 3 باستخدام أجهزة Cisco (أجهزة التوجيه والمحولات)، ثم قمنا بتثبيت Nagios مع VMwareلعرض وإخطار تغييرات الشبكة وتلقي التنبيهات والتنبيهات من خلال بريدنا الإلكتروني.

الكلمات المفتاحية: LAN، SNMP، GNS3، Nagios XI، VMware Workstation

Table des Matières

Liste des figures

Liste des tableaux

Liste des acronymes et abréviations

ASN Abstract Sysntax Notation

API Application Programming Interface

CIM Common Information Model

DHCP Dynamic host configuration protocole

DNS Domain Name server

DTMF Distributed Management Task Force

FTP file transport protocole

GNS3 Graphical network simulator

HTTP HyperText Transfer Protocol

HTTPS HyperText Transfer protocole Secure

IP Internet Protocol

IPMI Intelligent Platform Management Interface

ITIL Information Technology Interface

JMX Java Management Interface

MIB Management information base

NAT Network Address Translation

NMS Network Management System

OSPF Open Shortest path first

OID Object Identifiers

PRTG Paessler Router Traffic Grapher

RRD Round-Robin Database

SOAP Simple Object Access Protocol

SSH Secure Shell

SNMP Simple Network Management Protocol

SMS Short Message Service

SBLIM Stanadard Based Linux Instrumentation For Management

SSII Société de Services et d'Ingénierie en Informatique

UDP User Datagram Protocol

USM User-Based Security Model

VLAN Virtuel Local Area Network

VACM View-Based Access Control Model

VTP Vlan Trunking Protocol

WBEM Web Based Entreprise Management

Introduction générale

Nous vivons dans ce siècle à l'ère qu'on appelle « l'ère de l'information » grâce à la diffusion de l'information avec la plus grande facilité, ainsi, le réseau est devenu l'épine dorsale de la vie quotidienne dans tous ses aspects au point que toute interruption ou défaillance du réseau, notamment le réseau interpersonnel, entraînent des pertes colossales aux particuliers, aux entreprises et à bon nombre de secteurs, notamment économiques et financiers. Pour y remédier, il s'avère nécessaire de recourir à la surveillance permanente du réseau à tout moment.

Néanmoins, cette mesure pose le problème suivant : Comment s'assurer que le réseau n'est pas en panne et quelles sont les solutions pour connaître toutes les évolutions du réseau afin d'assurer la continuité des échanges d'information ?

De nombreux programmes de surveillance et de supervision ont été produits et fabriqués pour être en mesure de suivre les divers aspects du réseau et son fonctionnement tels que le trafic, l'utilisation de la bande passante et la disponibilité. Ces systèmes peuvent détecter les appareils et autres éléments composants, se connecter à un réseau, fournir des mises à jour de statut mais aussi nous alerter (par e-mail et SMS) en cas de problème.

Il convient de mentionner que ces programmes se divisent en deux catégories : la première est payante comme PRTG, Tivoli, Atera.... et la seconde est open source comme Cacti, Zabbix, Nagios XI, …etc. Dans notre recherche, nous avons opté pour « Nagios XI » vu qu'il est l'un des meilleurs logiciels libres en termes de qualité, de facilité d'utilisation, et de disponibilité de documentation y afférentes pour apprendre à s'en servir.

Afin de mener à bien notre travail de recherche, nous estimons bénéfique de structurer le présent mémoire en trois chapitres dont deux théoriques et un pratique. Dans le premier, nous faisons une présentation exhaustive de plusieurs concepts de base et généraux des composants d'un réseau informatique et donnons une explication de la surveillance.

Quant au deuxième chapitre, nous expliquons les différents programmes de suivi en termes de classification, définition, fonctionnalité et de leurs avantages et inconvénients dans l'optique de choisir un programme permettant d'atteindre la finalité du projet.

Et enfin, dans le troisième chapitre qui est consacré au volet pratique, le noyau de notre recherche, nous expliquons l'architecture du réseau universitaire, la méthode de sa programmation, sa configuration et sa liaison au logiciel « Nagios XI » afin de pouvoir surveiller et recevoir des messages et des alertes sur l'état du réseau.

Chapitre 1 Réseaux et supervision des réseaux

I.1. INTRODUCTION :

Les réseaux informatiques sont devenus indispensables pratiquement dans tous les domaines en raison de leur rôle important notamment en ce qui concerne l'échange d'information entre les appareils et les personnes tels que les messages, les photos, les vidéos et les fichiers.

Dans ce chapitre, nous allons expliquer en théorie quelques concepts et définitions liés au sujet.

I.2. LE RESEAU INFORMATIQUE :

I.2.1. Définition :

Un réseau est un groupement de deux ou plusieurs appareils électroniques permettant l'échange de données et le partage de ressources communes. Les premiers exemples des réseaux informatiques datent des années 1960, mais ils ont parcouru un long chemin depuis un demi-siècle.

Les réseaux modernes sont un peu plus complexes en général et comportent bien plus que deux ordinateurs. Pour les systèmes à plus de dix participants, on utilise habituellement une configuration de type client/serveur. Dans ce modèle, un ordinateur agissant comme point de commutation central (serveur) met ses ressources à disposition des autres participants au réseau (clients) [1].

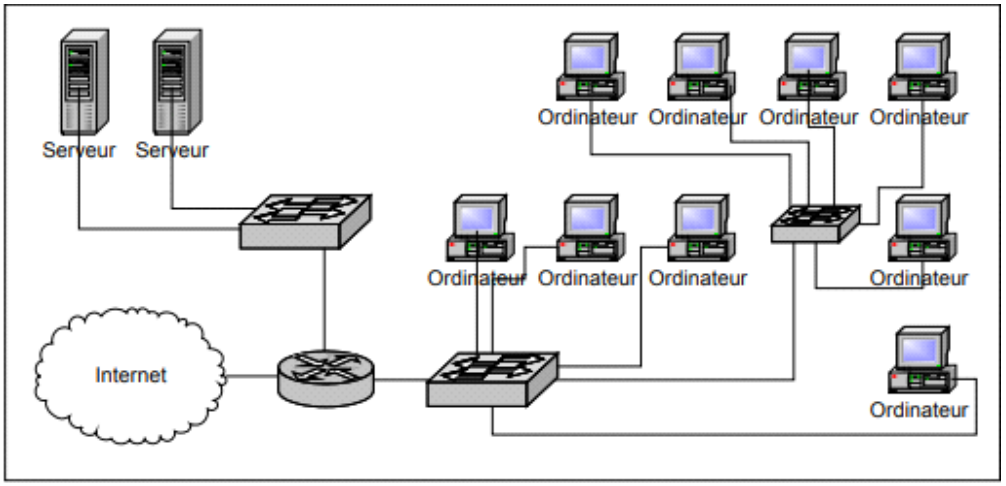

Figure I.1 : Exemple de réseau informatique

I.2.2. Types des réseaux informatiques :

Il existe de nombreux types de réseaux différents, qui peuvent être utilisés à des fins différentes et par différents types de personnes et d'organisations. Voici quelques types de réseaux que vous pourriez rencontrer [2] :

I.2.2.1. Réseaux locaux (LAN) :

Un réseau local ou LAN est un réseau qui connecte des ordinateurs dans une zone limitée. Cela peut être dans une école, un bureau ou même une maison [2].

I.2.2.2. Réseaux personnels (PAN) :

Un réseau personnel est un réseau basé sur l'espace de travail d'un individu. L'appareil de l'individu est le centre du réseau, avec d'autres appareils qui y sont connectés. Il existe également des réseaux personnels sans fi [2].

I.2.2.3. Réseaux étendus (WAN) :

Un réseau étendu est un réseau qui couvre une zone géographique plus étendue, généralement avec un rayon de plus d'un kilomètre.

I.2.2.4. Réseaux de campus :

Un réseau de campus est un réseau local ou un ensemble de réseaux locaux connectés étant utilisé par une agence gouvernementale, une université, une entreprise ou une organisation similaire et qui est généralement un réseau à travers un ensemble de bâtiments proches les uns des autres.

I.2.2.5. Réseaux métropolitains (MAN) :

Les réseaux de zones métropolitaines sont des réseaux qui s'étendent sur une région de la taille d'une zone métropolitaine. Un MAN est une série de LAN connectés dans une ville et qui peuvent également se connecter à un WAN.

I.2.2.6. Réseaux privés d'entreprise :

Un réseau privé d'entreprise est utilisé par une entreprise pour connecter ses différents sites afin que les différents sites puissent partager des ressources.

I.2.2.7. Inter réseaux :

Les inter réseaux connectent différents réseaux entre eux pour construire un réseau plus vaste. L'inter réseautage est souvent utilisé pour décrire la construction d'un grand réseau mondial.

I.2.2.8. Réseaux dorsaux (BBN) :

Une dorsale est une partie d'un réseau qui relie différentes pièces et fournit un chemin pour les informations à échanger.

I.2.2.9. Réseaux mondiaux (GAN) :

Un réseau mondial est un réseau mondial qui connecte des réseaux partout dans le monde, comme Internet.

I.2.3. Conception de réseau :

Les réseaux informatiques peuvent avoir des conceptions différentes, les deux formes de base étant les réseaux client / serveur et Peer-to-Peer. Les réseaux client/serveur ont des serveurs centralisés pour le stockage, auxquels les ordinateurs et périphériques clients accèdent. Les réseaux Peer-to-Peer ont tendance à avoir des périphériques qui prennent en charge les mêmes fonctions. Ils sont plus courants dans les foyers, tandis que les réseaux client/serveur sont plus susceptibles d'être utilisés par les entreprises [2].

I.2.4. Le modèle OSI :

Conçus dans les années 1970, à un moment où les réseaux informatiques prenaient leur essor, deux modèles distincts ont été fusionnés en 1983 et publiés en 1984 pour créer le modèle OSI tel qu'on le connaît aujourd'hui. La plupart des descriptions du modèle OSI partent de haut en bas, les chiffres allant de la couche 7 à la couche 1.

Voici les différentes couches et ce qu'elles représentent :

I.2.4.1. Couche Application :

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie, … etc.

I.2.4.2. Couche de présentation :

Cette couche est principalement responsable de la préparation des données afin qu'elles puissent être utilisées par la couche applicative.

I.2.4.3. Couche Session :

Pour que deux dispositifs, ordinateurs ou serveurs, puissent « parler » entre eux, il faut créer une session, et cela se passe au niveau de la couche du même nom.

I.2.4.4. Couche Transport :

La couche transport s'occupe de la coordination du transfert de données entre les systèmes finaux et les hôtes. Elle gère la quantité de données à envoyer, le rythme, la destination, etc.

I.2.4.5. Couche Réseau :

C'est au niveau de la couche réseau que se trouvent la plupart des fonctionnalités du routeur. Elle est très surveillée par les professionnels des réseaux. Dans son sens le plus élémentaire, cette couche est responsable de la transmission des paquets, y compris le routage par différents routeurs.

I.2.4.6. Couche Liaison de données :

La couche de liaison de données assure le transfert des données de nœud à nœud (entre deux nœuds directement connectés), et gère également la correction des erreurs de la couche physique.

I.2.4.7. Couche Physique :

Au bas de cette liste, la couche physique décrit les caractéristiques électriques, logiques et physiques du système.

I.2.5. Les avantages d'un réseau informatique :

Les principaux avantages des réseaux consistent en ce qui suit [2] :

- Le partage des données,
- Le partage des ressources,
- La gestion centralisée des programmes et des données,
- Le stockage et la sauvegarde centralisés des données,
- Le partage de la puissance de calcul et la capacité de stockage,
- L'administration simple des permissions et responsabilités.

I.3. LA SUPERVISION D'UN RESEAU :

I.3.1. Définition :

La supervision informatique fait référence à la surveillance du bon fonctionnement l'ensemble des outils et ressources déployés pour veiller au bon fonctionnement de votre système d'information qui leur sont reliés. Son objectif est de mettre en place une surveillance pour prévenir les interruptions de service, mais aussi de détecter les failles du réseau informatique afin d'éviter la détérioration des données et contrer les cyberattaques. Cette surveillance intervient dans tous les domaines du système informatique et porte plus spécifiquement sur la qualité (bande passante), sur la sécurité de la connexion internet et, par extension, sur l'état des services et matériels connectés (serveurs, postes de travail, imprimantes…) [3].

I.3.2. Principe :

Les principales solutions de supervision s'intègrent dans l'activité quotidienne informatique et permettent de surveiller, analyser, piloter en agissant directement après avoir reçu des alertes informant de potentielles anomalies pour assurer le bon fonctionnement d'un système. Il peut être appliqué sur plusieurs entités : serveurs, équipements réseaux, firewall, des scripts, des mails, des fax, des appels vocaux ou bien par l'envoi d'un simple SMS d'alerte. Sa mise en place permet d'effectuer des actions proactives et ainsi détecter un éventuel problème avant qu'il survienne. En général, lorsque l'on est en présence d'une grosse infrastructure, on délègue la gestion des alertes à des masters de supervision qui sont chargés de récolter les informations venant des équipements. La mise en place d'une solution de supervision permet d'avoir une vue d'ensemble des équipements supervisés, et ceci en temps-réel. Elle permet de visualiser à tout moment l'état des différents équipements configurés. Les objectifs sont multiples [4] :

- Eviter les arrêts de service,
- Remonter des alertes,
- Détecter et prévenir les pannes,

Pour assurer une bonne supervision, il faut définir clairement le rôle des superviseurs de l'organisation et veiller à ce qu'ils possèdent les compétences nécessaires pour bien s'acquitter de leurs fonctions.

- La fonction de supervision dans l'organisation.
  Exigences inhérentes au rôle de superviseur.
- Habiletés à planifier, organiser, diriger et contrôler.
- Position d'autorité et de responsabilité.
- Comprendre l'environnement de travail dans lequel il évolue : ressources – activités.
- Devoir d'efficacité et de résultats, production, promotion, entraînement, prévention, climat de travail, motivation, etc.
- Prendre conscience de son rôle : bien s'entourer et bien s'organiser [5].

I.3.3. L'intérêt de la supervision d'un réseau :

Via le déploiement de diverses technologies, la supervision informatique est la surveillance, la gestion et le pilotage d'un système, d'une activité, d'une infrastructure ou d'une installation technique donnée. L'intérêt de sa mise en place s'articule essentiellement sur les quatre points suivants [6] :

Surveillance et mesure de performances :

Un système de supervision informatique est avant tout un outil de surveillance qui a l'œil sur tout. Grâce à la collecte de données, il peut surveiller le système ou l'installation donnée et délivre aux administrateurs des informations très utiles : les paramètres clés, les performances, la disponibilité des matériels, l'état physique des machines, les charges des machines, niveau de production, les outils de supervision peuvent aussi faire des déductions et voient à l'avance les éventuelles pannes, surcharges des machines, l'atteinte des objectifs.

Résolution automatique des problèmes :

Tous les dysfonctionnements ne nécessitent pas forcément l'intervention des techniciens. Certains sont dans les cordes des systèmes de supervision. Ils règlent eux-mêmes certains problèmes, sans l'intervention des administrateurs.

Paramétrage automatique du système :

L'outil de supervision informatique se chargera de fournir les paramètres clés qui garantiront le bon fonctionnement des systèmes et activités. Mieux encore, ces paramètres clés sont saisis automatiquement.

Paramétrage d'évènements et gestion d'alarmes : Le paramétrage et gestion d'alarmes est sans aucun doute l'une des

Fonctionnalités les plus importantes en supervision informatique. Elle offre à l'administrateur la possibilité de paramétrer des évènements qui lorsqu'ils se produisent déclencheront aussitôt une procédure.

I.3.4. Type de la supervision d'un réseau :

On distingue différents types de supervision [7] :

La supervision technique (réseau informatique) :
Elle va consister à surveiller le réseau, l'infrastructure et les

Machines du système d'information (Processeur, Mémoire, Stockage).

La supervision Applicative :

Elle permet de superviser l'ensemble des applications telles que les bases de données (Oracle, SQL Server), les serveurs de mails (Exchange, Notes) et autres serveurs Web.

Contrat de service :

Ceci va consister à surveiller le respect des indicateurs, afin de voir si on respecte bien les contraintes que nous impose par exemple un contrat avec un client.

La supervision Métier :

Ceci va consister à surveiller les processus métiers de l'entreprise.

Reporting global :

C'est la raison pour laquelle le rapport de monitoring qui vous est transmis affiche souvent que tous les indicateurs de sécurité de votre système informatique sont au vert.

I.3.5. Les protocoles de supervision d'un réseau :

Les systèmes de supervision utilisent des protocoles, parmi les principaux utilisés, nous relèverons [8] :

- **La supervision des protocoles IPMI : intelligent Platform management interface** :

C'est l'un des plus utilisés que vous pourrez voir à travers ses outils propres IPMITOOLS, il concerne surtout les serveurs et cette interface intelligente de gestion de matériel permet, entre autres, de contrôler à distance certains composants très sensibles comme les sondes et autres ventilateurs.

- **La supervision des protocoles JMX : java management interface :**

C'est l'API qui permet de gérer une application en cours d'exécution. JMX est maintenant complètement intégré dans J2SE à partir de la version V. Certains experts estiment que le JMX est le SNMP de JAVA

- **La supervision des protocoles CIM : Common information model :**

Si l'on se base sur les écrits du DTMF (Distributed Management Task Force), la norme CIM ou Protocole CIM, comprend en plus du méta modèle, une spécification et un schéma. Le méta modèle pour en définir la sémantique. La spécification qui définit les détails pour intégrer avec d'autres modèles de gestion. Le schéma, ensemble de classes avec ses propriétés qui fournit les descriptions des modèles en réel, incluant le cadre conceptuel structuré en couches distinctes ; modèle de base, schémas d'extension et le modèle commun.

- **La supervision protocole SNMP : simple network management Protocol :**

C'est le protocole de communication et de gestion simplifiée du réseau. C'est le SNMP qui permet aux administrateurs de contrôler et de gérer (diagnostiquer) tous les éléments actifs du réseau. En langage SNMP on ne supervise pas, on manage, mais le résultat est similaire. Il est composé de 3 éléments essentiels : le superviseur, les nodes (ou nœuds en français) et les agents. Sans entrer dans les détails, c'est le SNMP qui permet de dialoguer entre le superviseur et les agents pour recueillir les objets dans la MIB.

- **La supervision protocole ITIL : Information Technology Library** : C'est une norme, ensemble de bonnes pratiques diron D'autres, pour la bonne gestion d'un système d'information. Né en Grande Bretagne, et populaire en Europe depuis plus de 35 ans, il tend à s'implanter aux USA grâce à l'impulsion de certaines grandes SSII.
- **La supervision protocole SBLIM : standard based linux instrumentation for manageability :**

SBLIM, Standards Based Linux Instrumentation for Manageability, est nommé par les experts en langage courant SUBLIME. Il s'applique aux machines LINUX et permet entre autres d'avoir accès aux technologies WBEM (Web Based Enterprise Management). Ce standard est exclusivement mis en avant par IBM qui en assure aussi le développement.

- **La supervision protocole WBEM : web based Enterprise management :**

WBEM (Web-Based Enterprise Management), ensemble de standards de base intégrés dans les outils de supervision, pour faciliter l'échange entre plateformes et technologies. WBEM sont des standards Internet de gestion, surtout développés pour unifier les environnements dans l'informatique distribuée.

- **La supervision protocole WS-MANAGEMENT** :

WEB SERVICES FOR MANAGEMENT WS-Management fournit la méthodologie pour échanger des informations d'administrations à travers les infrastructures IT,

spécification fournie par le DTMF. Basé sur les Web Services (SOAP), il est très proche du protocole WBEM.

I.3.6. Les méthodes de supervision :

Avant de voir si les différentes formes de supervision sont plutôt exclusives ou cumulatives, il est important de définir ses formes [9].

- **Supervision active** :

Dans cette forme de supervision, c'est le serveur de supervision qui interroge à intervalles réguliers les composants à surveiller. C'est la forme de supervision la plus communément déployée aujourd'hui. Il existe pléthore d'outils dans le monde Open Source pour effectuer ce type de supervision dont les noms les plus connus sont Nagios, Shinken, Icinga et Zabbix.

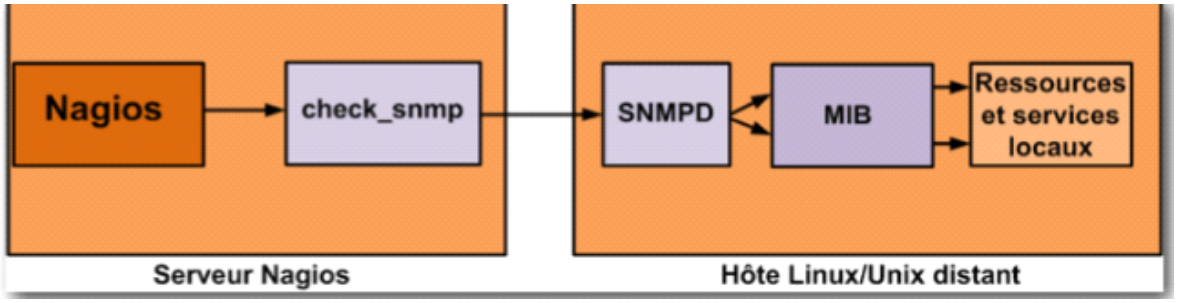

Figure I.2 : Exemple contrôle actif SNMP avec Nagios [9]

- **Supervision passive** :

Fort logiquement, cette forme de supervision est l'exact inverse de la précédente. Ici, ce sont les composants surveillés qui envoient à intervalles réguliers (ou non) métriques et messages vers une instance centrale de supervision.

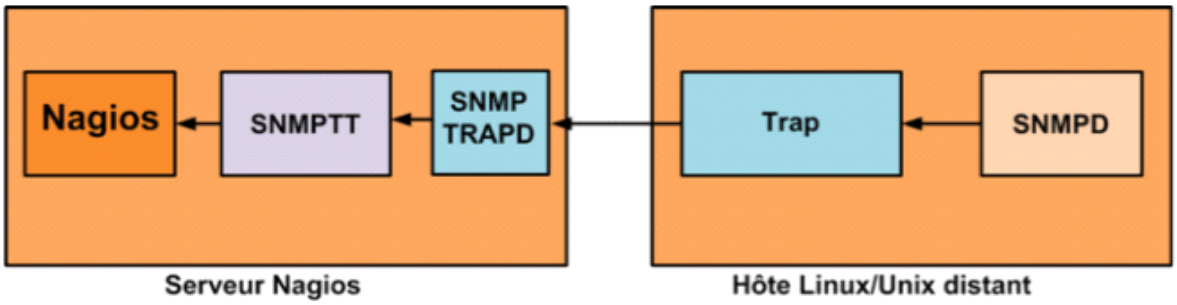

Figure I.3 : Exemple contrôle passif SNMP avec Nagios [9]

- **Supervision externe :**

C’est la forme de supervision qui permet de rendre compte de l’état d’un serveur en se plaçant au plus proche possible de l’utilisateur.

- **Supervision interne :**

Le monitoring interne est fait directement sur l’infrastructure mise en œuvre. Il nécessite un agent de supervision installé sur les serveurs à superviser.

I.4. SNMP :

I.4.1. Introduction

Pour introduire le protocole SNMP, il faut se rappeler que l’informatique est de plus en plus présente dans notre vie de tous les jours. On compte désormais sur les services offerts par les réseaux pour le fonctionnement de l’outil informatique, que ce soit en entreprise, lors de transactions bancaires, lors de téléconférences, etc. Les services offerts sont devenus quasi indispensables. Pour s'assurer que ces services soient convenables, il est nécessaire de surveiller le réseau et d’agir quand une erreur se produit.

I.4.1. Définition :

Le sigle SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau en Français). Il s'agit d'un protocole de couche Application qui permet aux administrateurs réseau de gérer les équipements du réseau, superviser et de diagnostiquer des problèmes réseaux, matériels à distance. L’environnement de gestion SNMP est constitué de plusieurs composantes : la station de supervision, les éléments actifs du réseau, les variables MIB et un protocole [10].

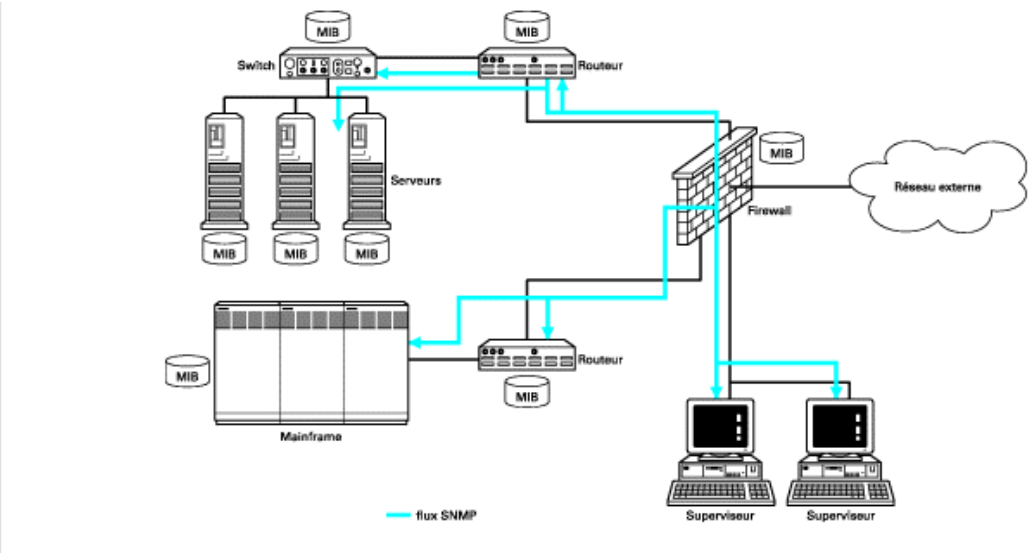

Figure I.4 - Système d'information supervisé par SNMP

I.4.2. Principe de fonctionnement de SNMP :

Le système de gestion de réseau est basé sur deux éléments principaux : un superviseur et des agents. Le superviseur est la console qui permet à l'administrateur réseau d'exécuter des requêtes de management. Les agents sont des entités qui se trouvent au niveau de chaque interface connectant l'équipement managé au réseau et permettant de récupérer des informations sur différents objets. Switchs, hubs, routeurs et serveurs sont des exemples d'équipements contenant des objets manageables. Ces objets manageables peuvent être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont directement liés au comportement en cours de l'équipement en question. Ces objets sont classés dans une sorte de base de données appelée MIB ("Management Information Base").

SNMP permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB.

L'architecture de gestion du réseau proposée par le protocole SNMP est donc basée sur trois principaux éléments :

Les équipements managés (managed devices) sont des éléments du réseau (ponts, hubs, routeurs ou serveurs), contenant des "objets de gestion" (managed objects)

pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques.

Les agents, c'est-à-dire une application de gestion de réseau résidant dans un périphérique est chargée de transmettre les données locales de gestion du périphérique au format SNMP.

Les systèmes de management de réseau (network management systems notés NMS), c'est-à-dire une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration [11].

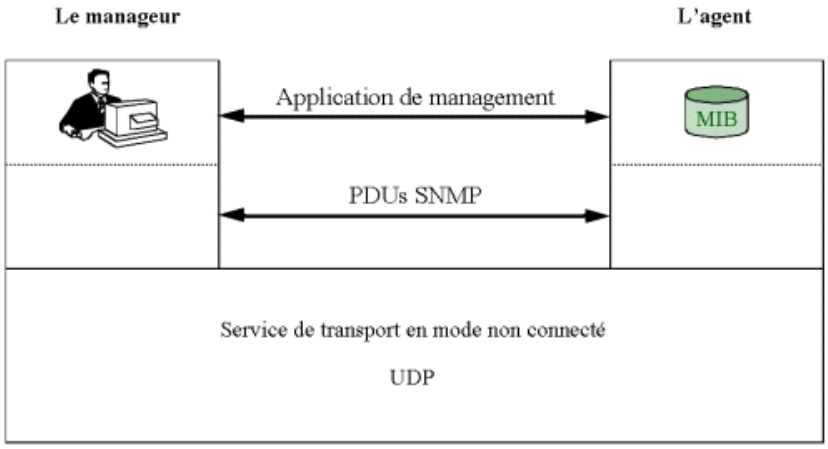

Figure I.5 : Base de SNMP

Le protocole SNMP est basé sur un fonctionnement asymétrique. Il est constitué d'un ensemble de requêtes, de réponses et d'un

Nombre limité d'alertes. Le manager envoie des requêtes à l'agent, lequel retourne des réponses. Lorsqu'un événement anormal surgit sur l'élément réseau, l'agent envoie une alerte (trap) au manager [12].

SNMP utilise le protocole UDP. Le port 161 est utilisé par l'agent pour recevoir les requêtes de la station de gestion. Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents [13].

I.4.2.1. Les requêtes SNMP :

Il existe quatre types de requêtes : Get Request, Get Next Request, Get Bulk, Set Request.

La requête Get Request permet la recherche d'une variable sur un agent. La requête Get Next Request permet la recherche de la variable suivante. La requête Get Bulk permet la recherche d'un ensemble de variables regroupées. La requête Set Request permet de changer la valeur d'une variable sur un agent [14].

I.4.2.2. Les réponses de SNMP :

À la suite de requêtes, l'agent répond toujours par Get Response. Toutefois si la variable demandée n'est pas disponible, le Get Response sera accompagné d'une erreur no Such Object.

I.4.2.3. Les alertes (Traps, Notifications) :

Les alertes sont envoyées quand un événement non attendu se produit sur l'agent. Celui-ci en informe la station de supervision via une trap. Les alertes possibles sont : ColdStart, WarmStart, LinkDown, LinkUp, Authentification Failure [12].

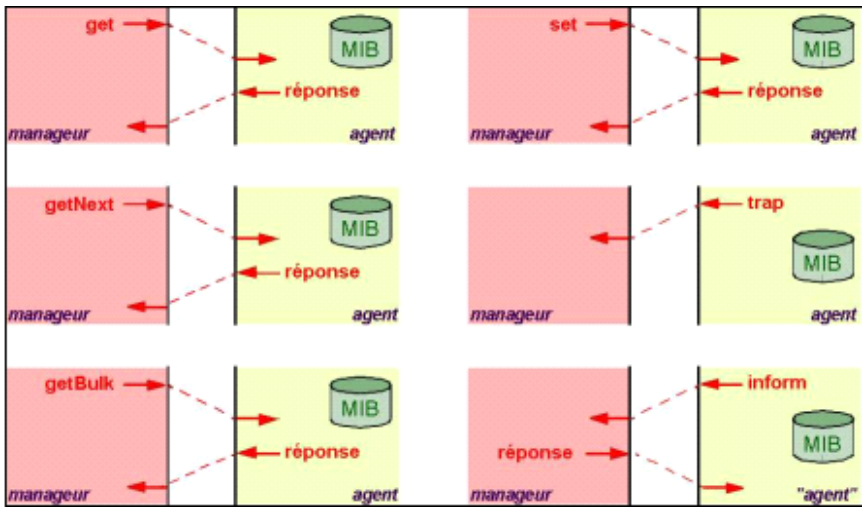

Figure I.6 : La gestion d'un réseau et le protocole SNMP

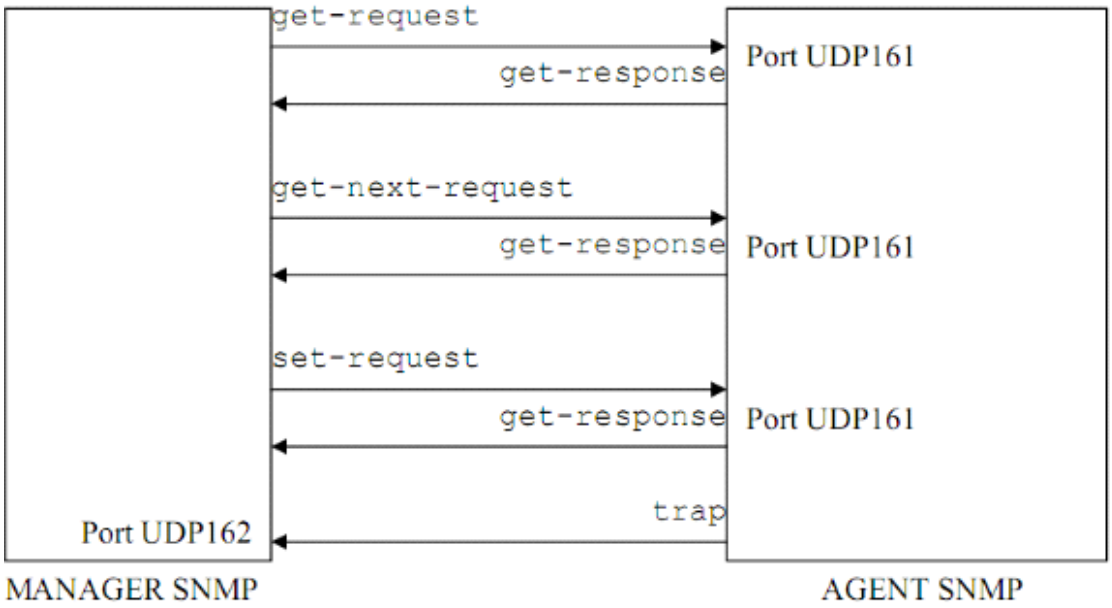

Figure I.7 : Echange entre l'agent et le manager [32].

I.4.3. Les versions de SNMP :

SNMPv1 : Ceci est la première version du protocole, tel que définie dans le RFC1157. La sécurité de cette version est triviale, car la seule vérification qui est faite est basée sur la chaîne de caractères "community ".

SNMPv2c (expérimental) : Cette version du protocole est appelée "community string based SNMPv2 ». Ceci est une amélioration des opérations de protocole et des types d'opérations et utilise la sécurité par chaîne de caractères "community " de SNMPv1.

SNMPv2c a introduit quelques nouveaux types, mais sa nouveauté majeure est l'opération GETBULK, qui permet à une plateforme de gestion, de demander en bloc de plusieurs variables consécutives dans la MIB de l'agent.

Généralement, on demande autant de variables que l'on peut mettre dans un paquet SNMP.

Opération Inform Avec cette Pdu, le manager informe l'agent qu'il a reçu un Trap(acquittement) [12].

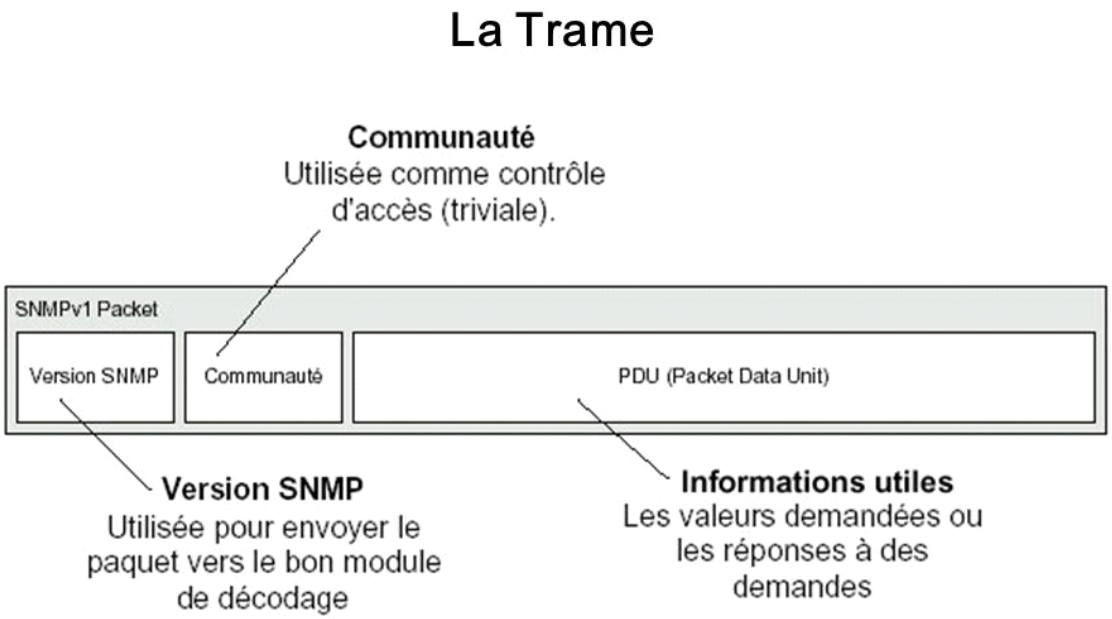

Figure I.8 : La trame de SNMPV1 etV2 [33]

- **SNMPv3 (standard actuel)** : Cette version comprend une combinaison de la sécurité basée sur les usagers et les types et les opérations. Cette nouvelle version du protocole SNMP vise essentiellement à inclure la sécurité des transactions. La sécurité comprend l'identification des parties qui communiquent et l'assurance que la conversation soit privée, même si elle passe par un réseau public.

La sécurité de SNMPv3 est basée sur 2 concepts :

- **USM (User-based Security Model)**

Il y a trois (03) mécanismes sont utilisés, chaque mécanisme permet d'empêcher un type d'attaque.

A. **Authentification** : Empêche quelqu'un de changer le paquet SNMPv3 en cours de route et de valider le Mot de passe de la personne qui transmet la requête.
B. **Chiffrement** :
   Empêche quiconque de lire les informations de gestions contenues dans un paquet SNMPv3.
C. **L'estampillage du temps** :

Empêche la réutilisation d'un paquet SNMPv3 valide a déjà transmis par quelqu'un.

- **VACM** (View- based Access Control Model)

Permet le contrôle d'accès au travers de la MIB. On a la possibilité de restreindre l'accès en lecture et/ou écriture pour un groupe ou par utilisateur.

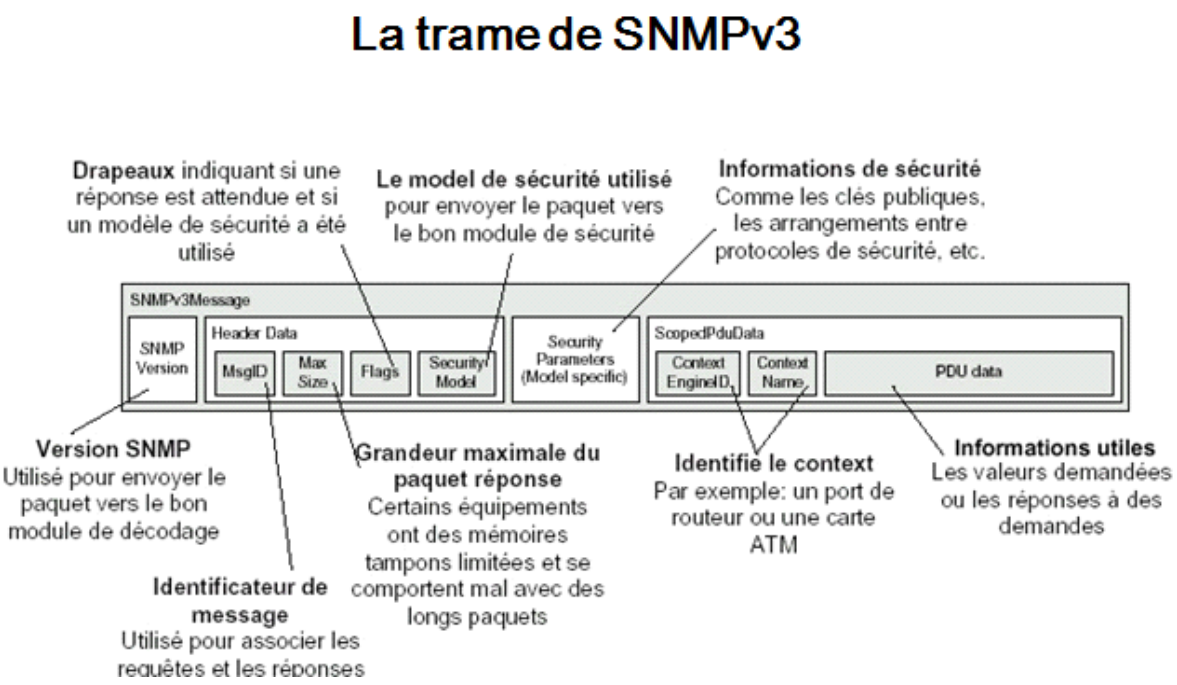

Figure I.9 : La trame de SNMPV3 [4]

I.4.4 MIB :

La MIB (Management Information base) est la base de données des informations de gestion maintenue par l'agent, auprès de laquelle le manager va venir pour s'informer.

Deux MIB publics ont été normalisées : MIB I et MIB II (dite 1 et 2). Un fichier MIB est un document texte écrit en langage ASN.1 (Abstract Syntaxe Notation 1) qui décrit les variables, les tables et les alarmes gérées au sein d'une MIB.

La MIB est une structure arborescente dont chaque nœud est défini par un nombre ou OID (Object Identifier). Elle contient une partie commune à tous les agents SNMP en général, une partie commune à tous les agents SNMP d'un même type de matériel et une partie spécifique à chaque constructeur. Chaque équipement à superviser possède sa propre MIB. Non seulement la structure est normalisée, mais également les appellations des diverses rubriques.

Ces appellations ne sont présentes que dans un souci de lisibilité. En réalité, chaque niveau de la hiérarchie est repéré par un index numérique et SNMP n'utilise que celui-ci pour y accéder [12].

Voici un exemple de structure de table MIB :

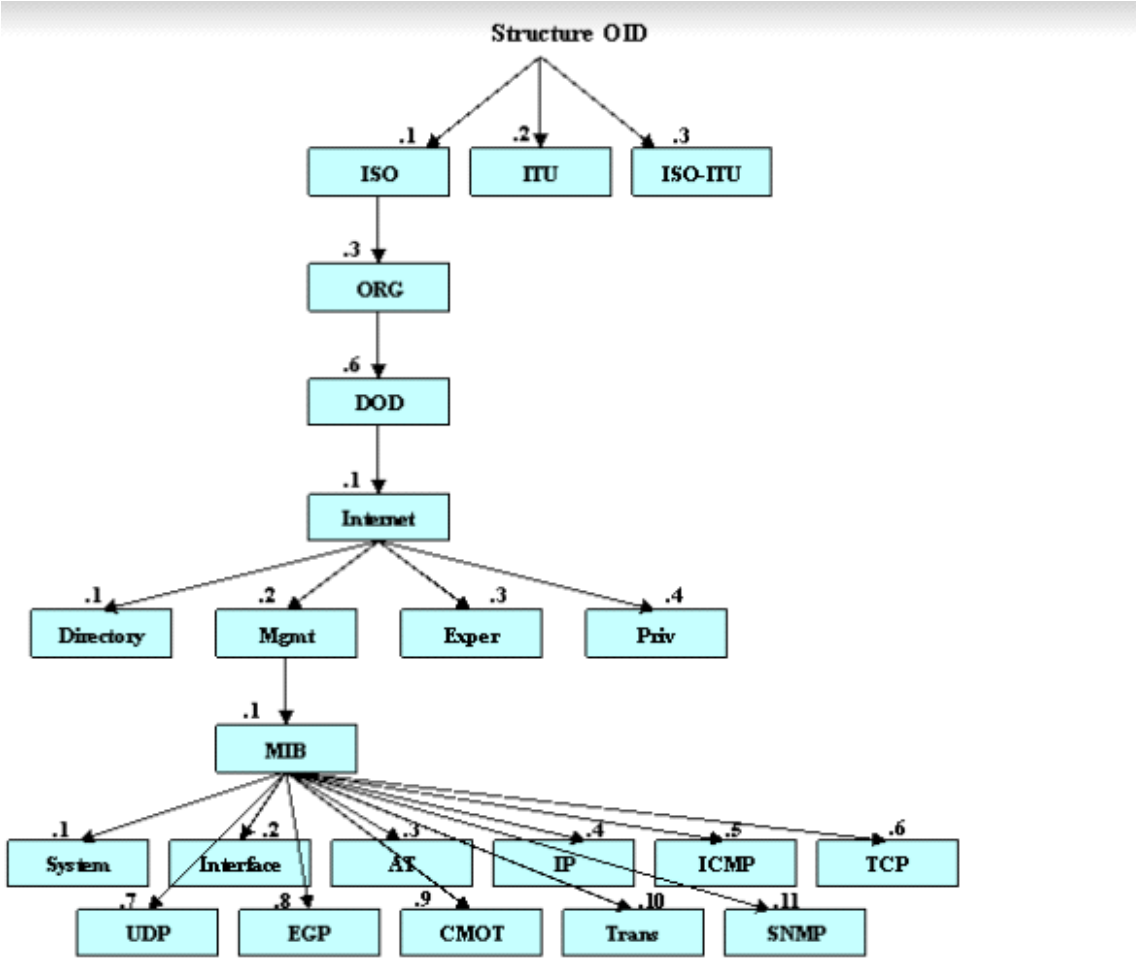

Figure I.10 : Les informations de base de la MIB [12]

I.5. CONCLUSION :

Grâce à l'explication de ce chapitre, nous avons une compréhension détaillée des concepts de base du réseau, de sa gestion et du sens de la surveillance, ce qui nous permettra de réussir plus facilement la finalité pratique du projet.

Chapitre 2 Les outils de supervision

II.1. INTRODUCTION :

La perte de connexion et la survenance de tout dysfonctionnement du réseau entraînent des retards ou la non-livraison des informations. Pour éviter cela, nous devons surveiller le réseau et noter tous ses changements.

Pour y parvenir, nous étudierons dans ce chapitre plusieurs programmes de surveillance au niveau du concept de leur utilisation, de leur qualité et de leurs aspects négatifs.

II.2. LES OUTILS DE SUPERVISIONS PROPRIETAIRES :

À côté des outils de visualisation et de monitoring open source, les solutions propriétaires payantes sous licence comme PRTG (Paessler), OpManager ou Dynatrace sont souvent sollicitées par les entreprises avec des besoins de surveillance réseau plus avancés [15].

II.2.1. PRTG :

II.2.1.1. Définition :

PRTG est un logiciel de surveillance de réseau qui peut s'exécuter sur une machine Windows au sein de votre réseau et qui peut collecter des statistiques à partir d'hôtes désignés tels que des routeurs, des serveurs, des commutateurs et d'autres appareils ou applications importants. L'avantage du logiciel de gestion de réseau est qu'il peut détecter les problèmes avant qu'ils ne se transforment en pannes et qu'en signalant ces problèmes à un administrateur réseau [16].

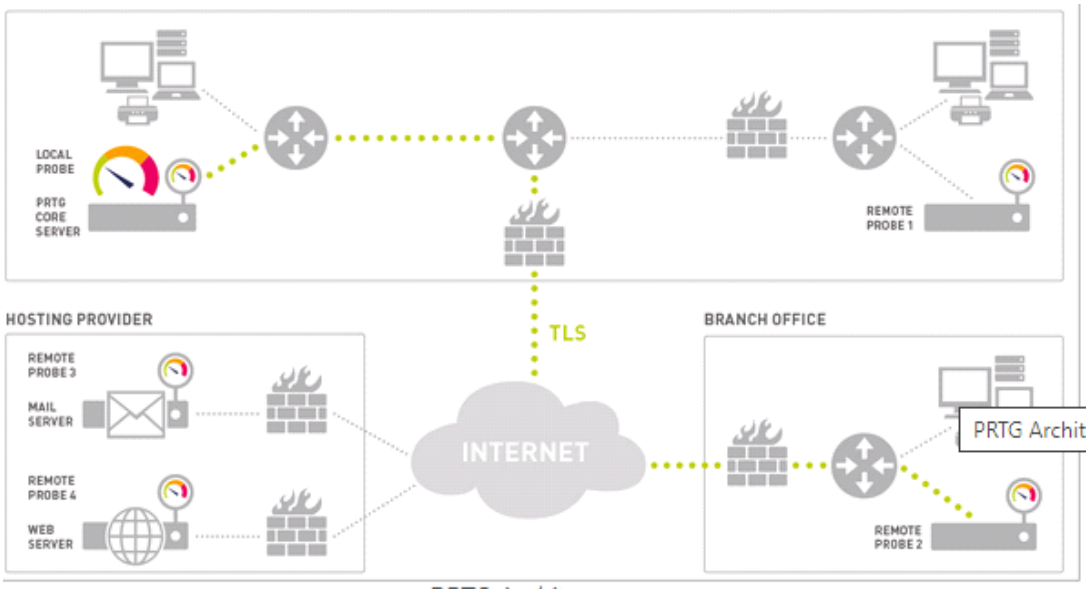

Figure II.1 : PRTG Architecture [17]

II.2.1.2 : la fonctionnalité de PRTG :

Alertes flexibles :

PRTG dispose plus de 10 technologies intégrées telles que le courrier électronique, le push, la lecture de fichiers audio pour les alarmes ou le déclenchement de requêtes HTTP. PRTG sur site prend également en charge les SMS et exécute les fichiers EXE [17].

Cluster de basculement :

Mieux vaut prévenir que guérir. PRTG Network Monitor permet d'assurer un basculement automatique de la supervision.

Traitement automatique du basculement.

Profitez du contrôle des points de présence : les nœuds assurent un contrôle permanent des capteurs, vous pouvez ainsi comparer les temps de réponse sur divers emplacements du réseau (LAN/WAN/VPN).

La version PRTG hébergée par Paessler permet également une surveillance haute disponibilité [17].

Surveillance distribuée :

Contrôlez divers réseaux sur des emplacements ou des réseaux séparés au sein de votre entreprise (par exemple DMZ et LAN) grâce aux sondes distantes PRTG.

Utilisez des sondes distantes pour surveiller votre réseau local avec PRTG hébergé par Paessler.

Surveiller toutes les filiales de votre entreprise à partir de votre PRTG serveur central.

Vous pouvez également utiliser les sondes distantes pour répartir le degré de surveillance [17].

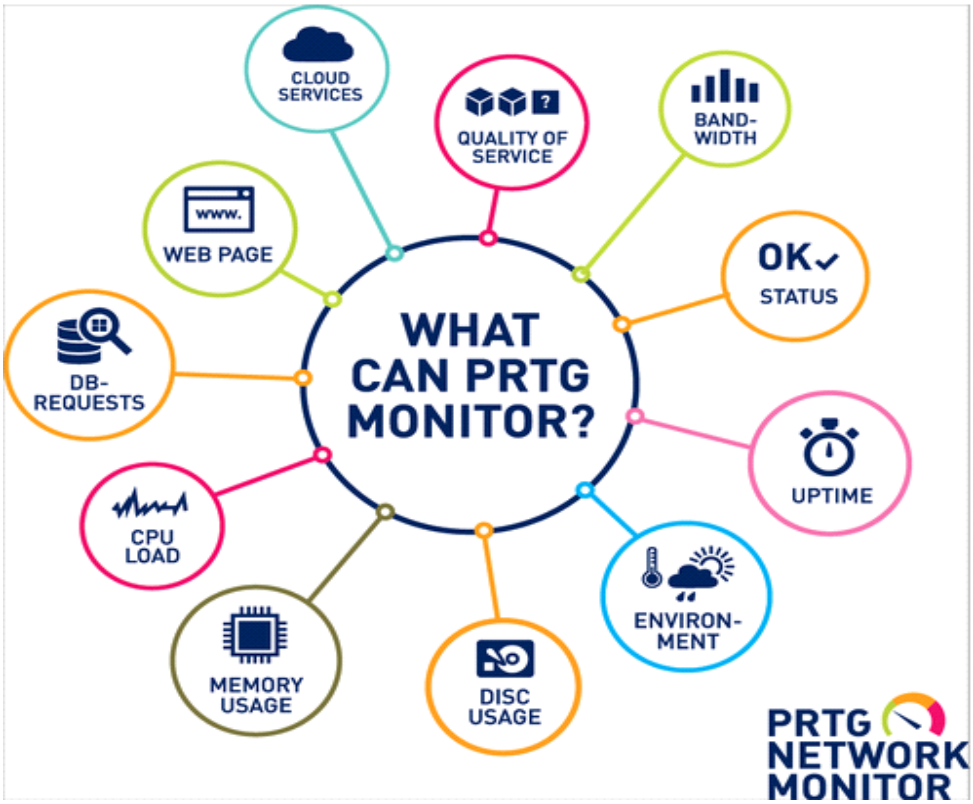

Figure II.2 : PRTG monitoring [17]

II-2-1-3 : Les avantages et les inconvénients :

Les avantages :

- Large palette de fonctionnalités concernant la surveillance,
- Interface utilisateur simple à utiliser et intuitive,
- Technologie de surveillance moderne et performante adaptée aux réseaux de toute taille
- Ensemble des fonctionnalités incluses dans chaque licence, aucune extension ni frais supplémentaires [18].

Les inconvénients :

- Échec des services Windows et blocages du serveur,

- Environnements virtuels avec comportement non fiable,
- Mauvaise qualité audio de VoIP et dysfonctionnement du flux vidéo [19].

II.2.2. ATERA :

II.2.2.1. Définition :

ATERA adapte le processus de surveillance et de gestion à distance aux besoins des MSP (Managed Service Provider ou fournisseur de services managés). En combinant la gestion à distance avec des fonctions de service à la clientèle comme le ticketing et les enquêtes de satisfaction, ATERA vous aide à garder le contrôle de votre réseau et de vos relations avec les clients.

II.2.2.2. La fonctionnalité de ATERA :

ATERA propose la découverte du réseau, les alertes en temps réel, l'accès à distance et des applications mobiles, puis ajoute la gestion des contrats et des SLA, ainsi que la facturation et le support de la facturation (avec des intégrations à QuickBooks, Xero et Freshbooks). Si vous souhaitez développer votre activité de MSP, contrôler les coûts et présenter une image professionnelle, ATERA est un excellent début [20].

II-2.3.1. Les avantages et les inconvénients des outils de supervision propriétaires :

Avantages :

- Solutions plus globales,
- Périmètres techniques et fonctionnels étendus,
- Support présent et réactif [15].

Inconvénients :

- Coûts d'acquisition et de support parfois élevés,
- Incompatibilités entre fournisseurs (plusieurs produits différents),
- Développements additionnels restreints et coûteux [15].

II.3. LES OUTILS DE SUPERVISIONS (OPEN SOURCE) :

Beaucoup d'entreprises au budget informatique limité préfèrent opter pour des logiciels de monitoring open source lorsqu'elles possèdent les compétences nécessaires en interne. Elles se tournent ainsi simplement vers des solutions gratuites ou peu onéreuses comme Nagios, Zenoss, Cacti, Zabbix ou encore Shinken [15].

II.3.1. CACTI :

II.3.1.1. Définition :

Cacti est un logiciel libre de mesure de performances réseau et serveur basé sur RRDTool dédié à la métrologie. Il permet de représenter sous forme de graphiques n'importe quelle donnée quantifiable collectée soit par le biais de protocoles réseaux tels que SNMP ou soit par des scripts personnalisés par l'utilisateur [21].

II.3.1.2. Fonctionnalités générales :

Cacti est un logiciel complet de métrologie de trafic réseau, d'équipements (réseau...) et de services informatiques basé sur RRDTool. Complet dans le sens où il permet de collecter 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 [22].

Collecter des données :

A intervalle donné (5 minutes par défaut) :

Les sources de données stockent des informations sur la composition des archives RRDTools Round Robin (RRA). Les archives Round Robin sont de petites bases de données de séries chronologiques qui stockent et regroupent des informations sur les données qui y sont insérées par les collecteurs de données de Cacti. Ces données peuvent provenir d'hôtes compatibles SNMP ou de scripts/commandes externes exécutés par les collecteurs de données de Cacti. Du fait que Cacti prend en charge la collecte de données à partir de n'importe quel script ou commande externe, fait de Cacti un cadre de gestion des performances très polyvalent.

Des sources de données peuvent également être créées, lesquelles correspondent aux données réelles du graphique. Par exemple, si un utilisateur souhaite représenter graphiquement les temps de Ping vers un hôte, vous pouvez créer une source de données à l'aide d'un script qui envoie une commande Ping à un hôte et renvoie sa valeur en millisecondes. Après avoir défini les options pour RRDTools.

Une fois qu'une ou plusieurs sources de données sont définies et que les collecteurs de données de Cacti commencent à stocker ces données dans les archives Round Robin, les données peuvent ensuite être utilisées pour restituer des graphiques dans Cacti. Par défaut, Cacti utilise la fonction graphique intégrée fournie par RRDTool, mais les

données de RRDTools TSDB peuvent également être utilisées par d'autres outils de visualisation.

Générer des graphes :

Cacti peut créer n'importe quel graphique RRDTool imaginable en utilisant tous les types de graphiques RRDTool standard et les fonctions de consolidation. Une zone de sélection des couleurs et une fonction de remplissage automatique du texte facilitent également la création de graphiques pour faciliter le processus.

Vous pouvez non seulement créer des graphiques basés sur RRDTool dans Cacti, mais il existe de nombreuses façons de les afficher. Outre une “vue liste” standard et un “mode de prévisualisation”, qui ressemble à l’interface RRDToolfrontend 14all, il existe une “vue arborescente” qui vous permet de placer des graphiques dans une arborescence hiérarchique à des fins d’organisation.

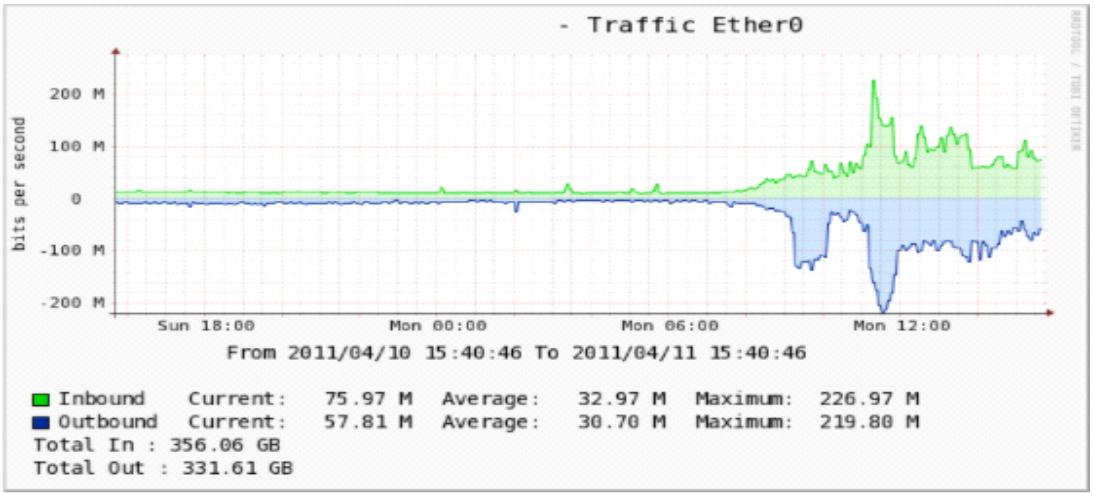

Figure II.3 : Exemples de graphes [34]

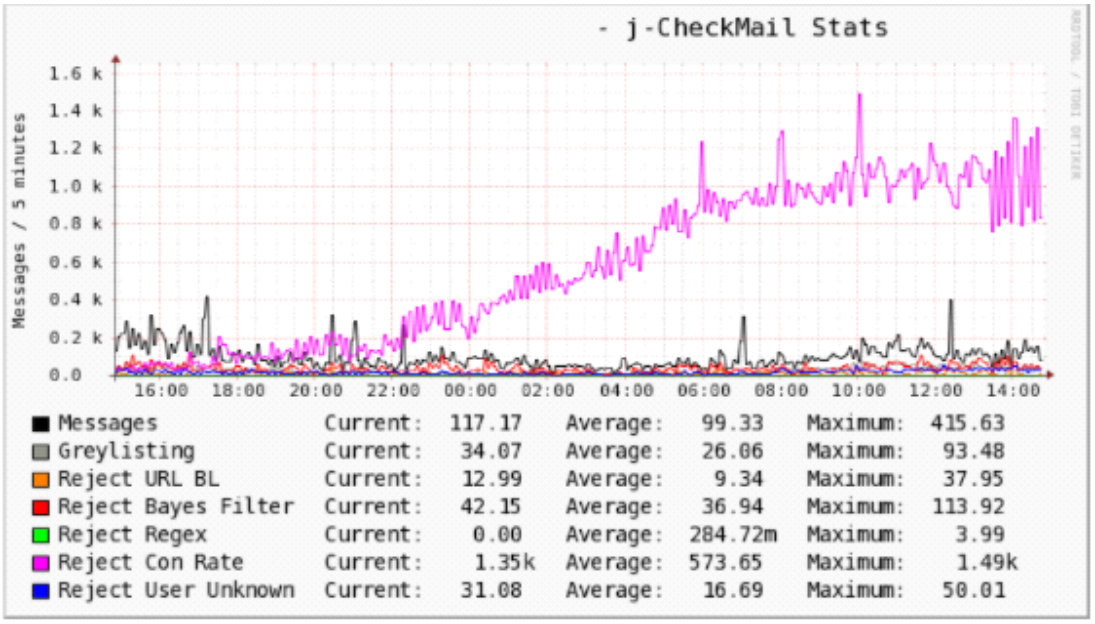

Figure II.4 : Exemples de graphes [34]

Gestion des utilisateurs :

En raison des nombreuses fonctions de Cacti, un outil de gestion basé sur l'utilisateur est intégré afin que vous puissiez ajouter des utilisateurs et leur donner des droits sur certaines zones de Cacti. Cela permettrait à quelqu'un de créer des utilisateurs pouvant modifier les paramètres d'un graphique, tandis que d'autres ne peuvent afficher que des graphiques. Chaque utilisateur conserve également ses propres paramètres lorsqu'il s'agit de visualiser des graphiques.

Cacti fournit trois méthodologies d'authentification et d'autorisation pour donner accès à ses fonctionnalités. Il prend en charge l'authentification locale, LDAP et de base telle que SAML2, TACCS+, etc. De plus, Cacti prend en charge la création de groupes d'utilisateurs et de domaines pour simplifier l'administration globale des utilisateurs. De plus, Cacti prend en charge la gestion de session « Se souvenir de moi » qui permet aux utilisateurs de rester connectés pendant de longues périodes sur des ordinateurs de confiance.

Templating :

Cacti est capable de s'adapter facilement à un grand nombre de sources de données et de graphiques grâce à l'utilisation de modèles et de packages. Les modèles de périphérique permettent aux administrateurs Cacti d'associer des périphériques d'un certain type ou d'une certaine classe à une collection de graphiques pris en charge par cet hôte associé au modèle de périphérique. Tous les modèles de Cacti peuvent être

exportés à partir d'une installation de Cacti, puis importés sur une autre soit en tant que fichiers de modèle, soit plus récemment en tant que fichiers de package [22].

II.3.1.3. Les avantages et les Inconvénients :

Les avantages :

- Facilité d'installation,
- Facilité de configuration,
- Affichage rapide des graphs sur plusieurs périodes,
- Peut-être amélioré grâce à des plugins,
- Grosse communauté.

Les inconvénients :

- Limité de base,
- Peut mettre un certain temps à générer les graphs.

II.3.2. Nagios XI :

II.3.2.1. Définition :

Nagios est un système de surveillance open source pour les systèmes informatiques. Il a été conçu pour fonctionner sur le système d'exploitation Linux et peut surveiller les périphériques exécutant les systèmes d'exploitation (SE) Linux, Windows et Unix.

Le logiciel Nagios effectue des vérifications périodiques des paramètres critiques des ressources applicatives, réseau et serveur. Par exemple, Nagios peut surveiller l'utilisation de la mémoire, l'utilisation du disque, la charge du microprocesseur, le nombre de processus en cours d'exécution et les fichiers journaux. Nagios peut également surveiller des services, tels que Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Hypertext Transfer Protocol (HTTP) et d'autres protocoles réseau courants. Les contrôles actifs sont initiés par Nagios, tandis que les contrôles passifs proviennent d'applications externes connectées à l'outil de surveillance.

Initialement appelé NetSaint et sorti en 1999, Nagios a été développé par Ethan Galstad et ensuite affiné par de nombreux contributeurs en tant que projet open source. Nagios

Entreprises, une société basée sur la technologie Nagios Core, propose plusieurs produits, tels que XI, Log Server, Network Analyzer et Fusion [23].

II.3.2.2. Principe de fonctionnement :

Nagios fait appel aux programmes ou aux scripts exécutables à travers des commandes afin de contrôler la disponibilité des applications et services du réseau. Ces plugins seront exécutés localement sur le serveur Nagios ou en utilisant des agents installés sur les machines contrôlées.

Nagios offre un ensemble de plugins officiels prêts à être utilisés pour contrôler les applications et les services réseau, à savoir :

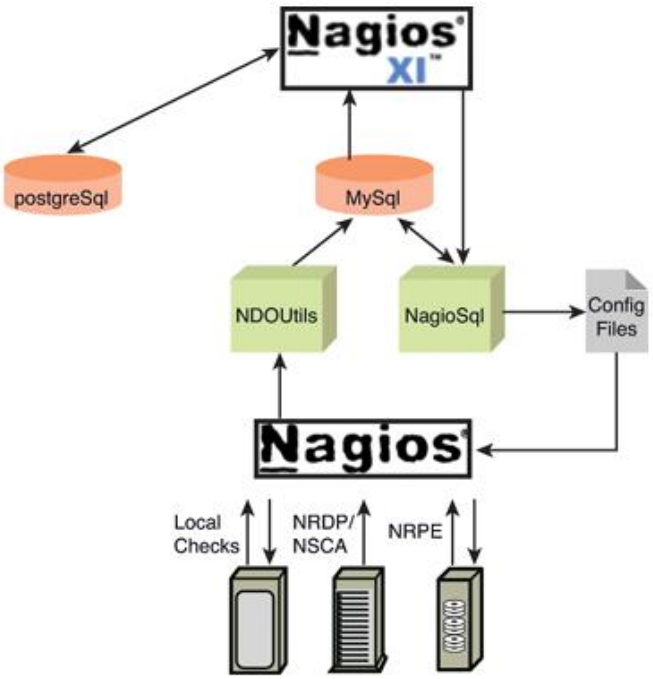

Figure II.5 : Principe de fonctionnement [23]

Code de retour du plugin	Etat du service	Etat de l'hôte
0	OK (tout va bien)	UP
1	WARNING (le seuil d'alerte est dépassé)	UP ou DOWN/UNREACHABLE (2)
2	CRITICAL (le service a un problème)	DOWN/UNREACHABLE
3	UNKNOWN (impossible de connaître l'état du service)	DOWN/UNREACHABLE

Figure II.6 : Principe de fonctionnement (suite)[35]

La plupart de ces plugins sont basés sur le plugin générique check tcp permettant de vérifier l'état d'un port et sa disponibilité sur le réseau. Tous ces plugins suivent des

règles communes pour les contrôles d'hôtes et les contrôles de service. Nagios exige que chaque commande renvoie des codes de résultat spécifiques, qui sont présentés ci-dessous :

0 OK : ce retour indique que l'hôte et le service fonctionnent correctement.

1 WARNING : ce retour indique que l'hôte et le service ne fonctionnent pas. NRPE est l'agent le plus utilisé pour superviser les serveurs Linux mais il peut être utilisé aussi avec les machines Windows. Son principe de fonctionnement ressemble beaucoup à Nagios. Il permet d'exécuter les plugins localement dans la machine distante et de renvoyer le résultat à Nagios.

Nagios fait appel à NRPE en utilisant le plugin check_nrpe pour lancer la commande et exécuter le plugin. À la fin de l'exécution de la commande, NRPE renvoie les informations à check_nrpe. Ces informations correspondent à un code de résultat (0= OK, 1=WARRING, 2=CRITICAL et 3=UNKNOWN) et d'autres informations utiles comme les données de performance.

La communication entre Nagios et le daemon NRPE se fait par le flux SSL et par défaut NRPE utilise le port TCP 5666 pour assurer cette communication.

L'intérêt d'utiliser NRPE par rapport à SSH est de minimiser l'utilisation des ressources sur l'hôte distante et sur le serveur Nagios. Par contre NRPE est moins sécurisé que SSH puisqu'il utilise un mécanisme d'authentification auprès de l'hôte basé sur l'adresse IP ou la plage d'adresses IP du demandeur. Le diagramme suivant résume ce principe de fonctionnement [23].

II.3.2.3. Comment fonctionne Nagios :

Surveillance des infrastructures :

Les utilisateurs peuvent configurer Nagios XI pour surveiller tout Composants d'infrastructure critiques et les processus métier dès l'interface Web. Les assistants de configuration font il est facile de surveiller à peu près n'importe quoi.

Surveillance active et passive :

Que vos périphériques réseau soient derrière un pare-feu ou directement accessibles, Nagios XI peut les surveiller avec des contrôles actifs et passifs.

Escalades d’alerte :

Les pannes et les pannes non résolues peuvent être transmises au personnel de garde et aux autres parties prenantes de l'entreprise pour garantir que les problèmes ne passent pas inaperçus.

Planification de la capacité :

Les rapports de planification de la capacité fournissent des projections graphiques de l'utilisation future en fonction des performances historiques, permettant aux parties prenantes de mettre à niveau les ressources système avant qu'elles ne soient surchargées.

Détection et résolution des incidents :

Résolvez rapidement les pannes de réseau et minimisez les temps d'arrêt de l'infrastructure. Nagios XI identifie la cause des pannes de réseau afin que les utilisateurs puissent passer moins de temps à trouver le problème et plus de temps à le résoudre.

Notifications :

Nagios XI envoie des notifications au personnel informatique, aux parties prenantes et aux utilisateurs finaux par e-mail et SMS, leur fournissant les détails de la panne afin qu'ils puissent commencer à résoudre les problèmes immédiatement.

Rapports historiques :

Affichez un historique des pannes, des événements, des notifications et des réponses aux alertes pour un examen ultérieur. Les rapports de disponibilité et de SLA permettent de garantir que vous respectez vos engagements de disponibilité.

Temps d'arrêt programmé :

Le personnel informatique peut planifier des temps d'arrêt pour éviter les notifications pendant les fenêtres de maintenance et de mise à niveau programmées. Les temps d'arrêt programmés peuvent également être filtrés à partir des rapports [24].

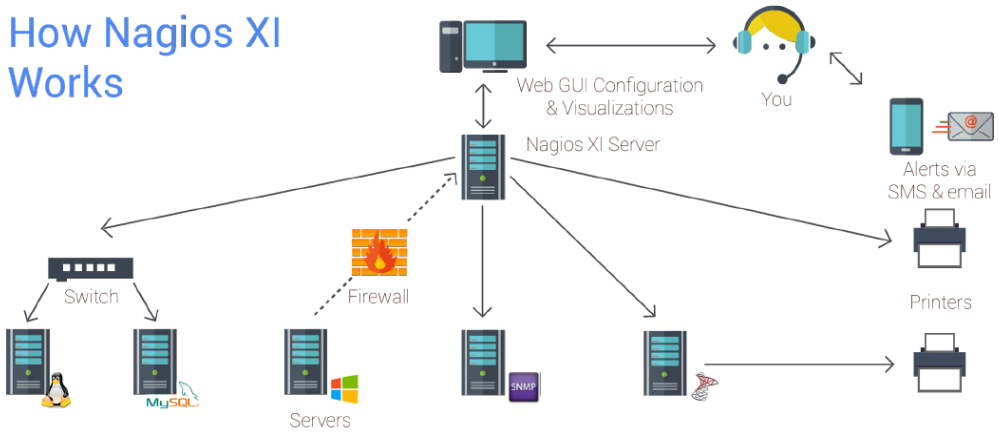

Figure II.7 : La fonctionnalité de Nagios Xi [24]

II.3.2.4. Les avantages et les inconvénients de Nagios :

Les avantages :

Surveillance complète de l'infrastructure informatique :

Assure la surveillance de tous les composants d'infrastructure critiques, y compris les applications, les services, les systèmes d'exploitation, les protocoles réseau, les métriques des systèmes et l'infrastructure réseau. Des centaines de modules complémentaires tiers permettent de surveiller pratiquement toutes les applications, services et systèmes internes.

Performance :

Le puissant moteur de surveillance Nagios Core 4 offre aux utilisateurs le plus haut degré de performance du serveur de surveillance. Les processus de travail à haute efficacité permettent une évolutivité et une efficacité de surveillance presque illimitées.

Visibilité :

Fournit une vue centrale de l'ensemble de votre réseau d'exploitation informatique et de vos processus métier. De puissants tableaux de bord offrent un accès rapide à de puissantes informations de surveillance et à des données tierces. Les vues offrent aux utilisateurs un accès rapide aux informations qu'ils trouvent les plus utiles.

Planification proactive et sensibilisation :

Des graphiques automatisés et intégrés de tendances et de planification des capacités permettent aux entreprises de planifier les mises à niveau de l'infrastructure avant que les systèmes obsolètes ne les surprennent. Des alertes sont envoyées au personnel informatique, aux parties prenantes de l'entreprise et aux utilisateurs finaux

par e-mail ou SMS, leur fournissant les détails de la panne afin qu'ils puissent commencer à résoudre les problèmes immédiatement.

Personnalisation :

Une interface graphique puissante permet de personnaliser la mise en page, la conception et les préférences pour chaque utilisateur, offrant à vos clients et aux membres de votre équipe la flexibilité qu'ils souhaitent.

Facilité d'utilisation :

L'interface de configuration Web intégrée permet aux administrateurs de confier facilement le contrôle de la gestion de la configuration de surveillance, des paramètres système et plus encore aux utilisateurs finaux et aux membres de l'équipe. Les assistants de configuration guident les utilisateurs tout au long du processus de surveillance de nouveaux appareils, services et applications, le tout sans avoir à comprendre des concepts de surveillance complexes.

Capacités multi-locataires :

L'accès multi-utilisateurs à l'interface Web permet aux parties prenantes de visualiser l'état de l'infrastructure pertinente. Les vues spécifiques à l'utilisateur garantissent que les clients ne voient que les composants d'infrastructure pour lesquels ils sont autorisés. La gestion avancée des utilisateurs simplifie l'administration en vous permettant de gérer facilement les comptes d'utilisateurs. Provisionnez de nouveaux comptes d'utilisateurs en quelques clics et les utilisateurs reçoivent automatiquement un e-mail avec leurs identifiants de connexion.

Architecture extensible :

Plusieurs API permettent une intégration simple avec des applications internes et tierces. Des milliers de modules complémentaires développés par la communauté étendent les fonctionnalités de surveillance et d'alerte natives. Des développements d'interfaces et d'addons personnalisés sont disponibles pour adapter Nagios XI aux besoins exacts de votre organisation [25].

Les inconvénients :

Les rapports de planification sont limités à l'entreprise, mais dans le cas de l'édition standard, nous devons configurer les tâches pour générer les rapports de planification. Les rapports avancés devraient avoir des options de serveur en masse. La surveillance des données sensibles comme l'expiration du certificat devrait avoir des

assistants simples car la configuration du service Web, puis la surveillance du certificat est un long processus qui doit être simplifié [26].

II.3.3. Les avantages et les inconvénients des outils de supervision open source :

II.3.3.1. Avantages :

- Coûts d'acquisition limités ou gratuits.
- Indépendance des fournisseurs.
- Respect des standards.
- Développements additionnels peu coûteux et riches.
- Communauté active derrière le produit

II.3.3.2. Inconvénients :

- Efforts d'implémentation et de configuration plus intenses que la moyenne.
- Gamme souvent limitée des fonctionnalités proposées.
- Support payants [15].

II.4. CONCLUSION :

Ce chapitre permet d'identifier et de sélectionner le programme de surveillance approprié au besoin, car de nombreux programmes open source et payants ont été traités.

Il convient de citer que nous avons opté pour un programme open source pour mener à bien le projet.

Chapitre 3 III-Implémentation et supervision du réseau LAN

III.1 Introduction :

Après une étude approfondie de l'aspect technique du sujet, dans le but de créer le réseau et de réussir à en assurer le suivi, nous avons choisi les programmes suivants :

- GNS3 : Pour créer un réseau virtuel similaire au réseau LAN de l'université,
- VMware : pour exécuter le logiciel Nagios Xi et le serveur Ubuntu,
- Nagios XI : Pour surveiller et envoyer des messages et des alertes sur l'état du réseau.

III.2. Supervision d'un réseau informatique :

III.2.1. Définition :

La supervision réseau fait référence à la surveillance du bon fonctionnement des réseaux informatiques et des services informatiques connectés sur ces réseaux.

- La surveillance du réseau porte plus spécifiquement sur :
- La qualité (bande passante),
- La sécurité de la connexion Internet,

Mais aussi, par extension, l'état des services et matériels connectés : serveurs, imprimantes, postes de travail, …

III.2.2. Objectif de supervision :

Obtenir un point de centralisation pour la gestion de l'ensemble du système informatique en trois points :

- Entre réactif.
- Entre proactif.
- Entre pertinent.

III.3. Les outils utilisent :

III.3.1. GNS3 :

GNS3 (Graphical Network Simulator) est un simulateur de réseau graphique qui permet l'émulation des réseaux complexes. Vous connaissez peut-être avec VMWare ou Virtual Box qui sont utilisées pour émuler les différents systèmes d'exploitation dans un

environnement virtuel. Ces programmes vous permettent d'exécuter plusieurs systèmes d'exploitation

Tels que Windows ou Linux dans un environnement virtuel. GNS3 permet le même type d'émulation à l'aide de Cisco Internetwork Operating Systems [27].

III.3.2. VMware :

VMware est une entreprise américaine spécialisée dans Lan Virtualisation et le Cloud Computing. Les différentes machines virtuelles se partagent les ressources du serveur physique, telles que le networking et la RAM, mais Chacune d'entre elles peut tourner sur un système d'exploitation différent. La virtualisation est particulièrement utile pour les entreprises, puisqu'elle leur permet d'exécuter plusieurs systèmes serveur sans avoir à investir dans une infrastructure physique pour chacun d'entre eux.

II.4. Implémentation du réseau LAN de l'université :

Afin de s'assurer que le réseau est contrôlé et surveillé, le réseau virtuel universitaire doit être établi sous le simulateur gns3 et ajuster les configurations.

II.4.1. Partie théorique

II.4.1.1. VLAN :

Le VLAN (Virtual Local Area Network) regroupe, de façon logique et indépendante, un ensemble de machines informatiques. On peut en retrouver plusieurs coexistant simultanément sur un même Commutateur réseau.

Eu regard de l'architecture de l'université, et pour une meilleure organisation du réseau, nous avons opté pour le regroupement de toutes les machines d'un pavillon dans un seul et même VLAN, le tableau le montre comme suit :

Nom VLAN	VLAN ID	Adresse	Description
Serveur	10	10.10.10.0/24	VLAN pour le serveur de supervision
MATH	13	172.16.13.0/24	VLAN des poste de pavions math
SCIENCE	14	172.16.14.0/24	VLAN des poste de pavions science

ELCTRONIQUE	16	172.16.19.0/24	VLAN des poste de pavions électronique
MECHANIQUE	19	172.16.19.0/24	VLAN des poste de pavions MECHANIQUE
AUDITORUM	20	172.16.20.0/24	VLAN des poste de AUDITORUIM
RECTORAT	30	172.16.30.0/24	VLAN des poste de RECTORAT
MANAGMENT	90	192.168.90.0/24	VLAN pour management des équipements

Table III.1 : Nom de Vlan

II.4.1.2. VTP (Vlan Trunking Protocol)

Le protocole VTP est un protocole de couche 2 propriétaire de la compagnie Cisco. En général, son avantage principal c'est sa capacité de propager automatiquement des vlan configures sur un commutateur en mode 'server' vers les autres commutateurs configures en mode 'client'.

Dans notre déploiement sur la base du concept VTP, nous avons choisi le switch CORE en mode VTP server alors que les switches seront des VTP client [28].

II.4.1.3. SSH (Secure Shell) :

SSH est une méthode de communication sécurisée avec un autre ordinateur. La partie "sécurisée" du nom signifie que toutes les données envoyées via une connexion SSH sont cryptées. Cela signifie que si une tierce tente d'intercepter les informations en cours de transfert, celles-ci semblent brouillées et illisibles [29].

II.4.1.4. SNMP :

« Protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance [30].

II.4.1.5. Routage dynamique

Le routage dynamique est une technique de mise en réseau qui permet un routage optimal des données. Le routage dynamique permet aux routeurs de

sélectionner des chemins en fonction des changements de disposition du réseau logique en temps réel.

Le routage dynamique utilise plusieurs algorithmes et protocoles. Le plus populaires est OSPF (Open Shortest Path First) [31].

II.4.1.6. Administration des équipements :

Dans l'administration des équipements, nous avons créé le vlan 90 comme un vlan de management.

II.4.2. Partie Pratique :

Après avoir étudié le sujet et afin de réaliser le projet, nous avons choisi un simulateur Gns3 et l'outil de supervision Nagios xi qui vont être détaillés comme suit :

II.4.2.1. Simulateur GNS3 (Graphique network simulator)

Grâce au simulateur Gns3, nous avons ajouté les dispositifs suivants : les switches et les routeurs à partir de l'interface graphique, dans le but de réaliser la topologie de l'université.

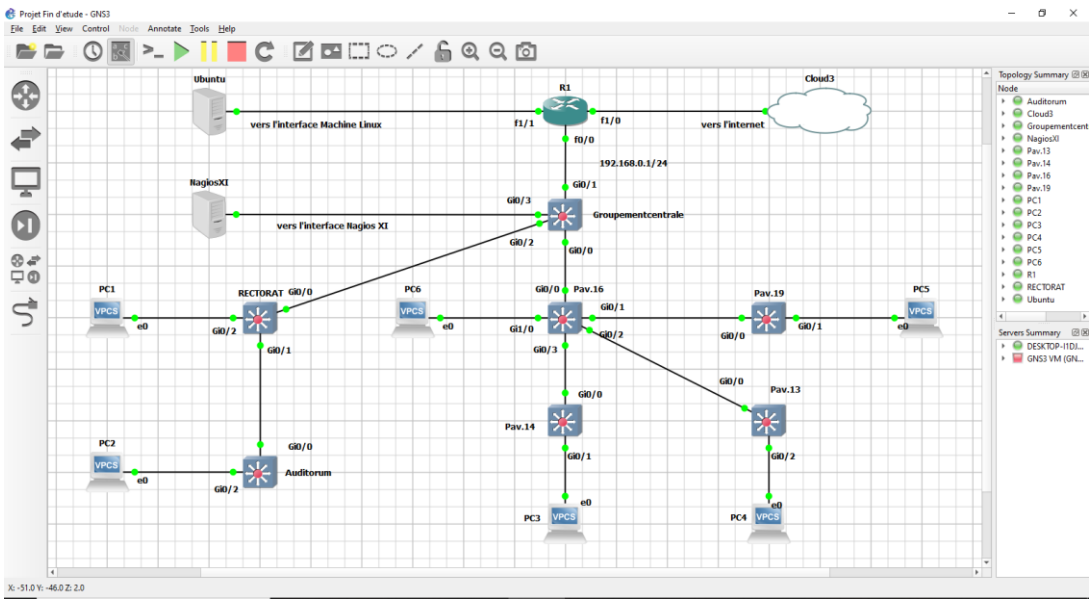

Figure III.1 : Architecture du réseau LAN de l'université sous Gns3

II.4.2.2. Configuration des équipements :

Pour configurer les équipements, nous avons utilisé l'application solar-putty.

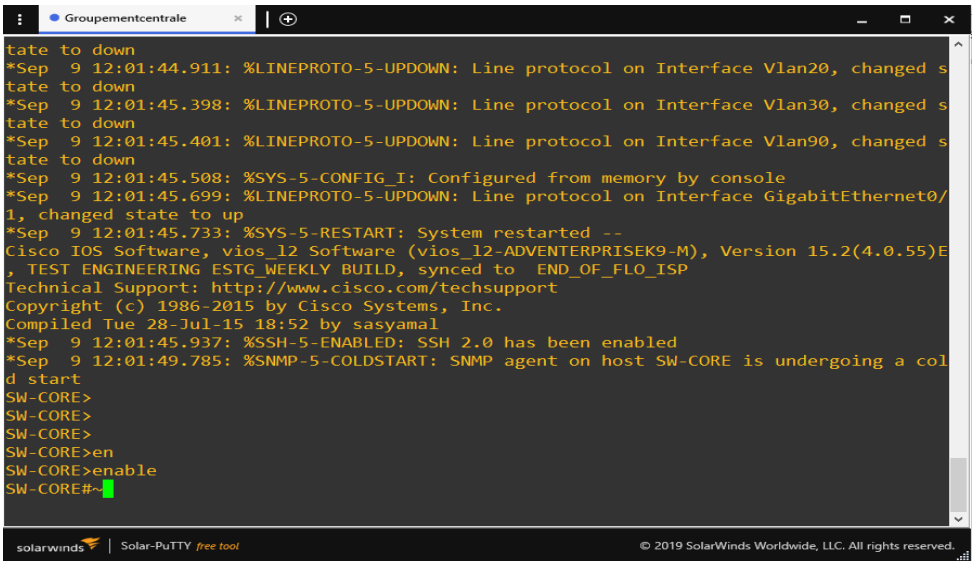

Figure III.2 : L'interface de solar-putty

II.4.2.3. Configuration des équipements :

Pour créer un réseau et se connecter entre les appareils, vous devez configurer tous les équipements avec un exemple configuré (Regroupement Centrale).

II.4.2.4. Configuration des switches :

Pour obtenir un bon réseau et une bonne configuration, il faut suivre les étapes suivantes :

- Configuration de hostname
- Configuration de mots de passe pour la ligne console
- Configuration de SSH
- Configuration de VTP
- Configuration de Vlan
- Configuration de l'interface
- Configuration de DHCP et DNS
- Configuration de routage inter-vlan.
- Configuration SNMP

Exemple de Configuration le switches Regroupement centrale :

1. **Configuration de Hostname:** la configuration de hostname dans SW-CORE.

Figure III.3 : Configuration de Hostname

2. **Configuration de mots de passe :** la figure la configuration de mot de passe dans SW-CORE.

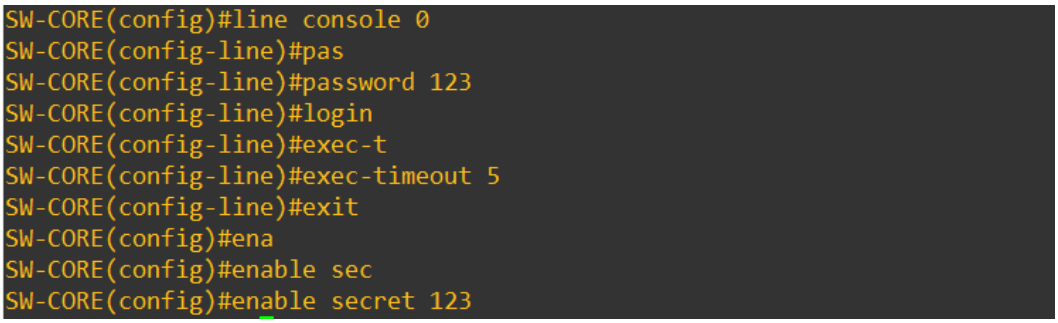

Figure III.4 : Configuration de mot de passe

3. **Configuration de VTP** : la figure montre la configuration de VTP dans le SW-CORE.

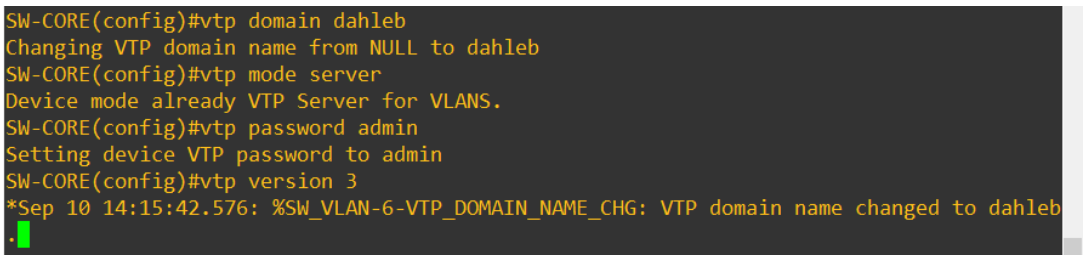

Figure III .5 : Configuration de VTP

4. **Démonstration de l'implémentation de VTP :** la configuration de VTP dans le SW-CORE.

```
SW-CORE#show vtp sta
SW-CORE#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : dahleb
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Enabled
Device ID                       : 0c77.5cca.e600

Feature VLAN:
--------------
VTP Operating Mode                : Server
Number of existing VLANs          : 13
Number of existing extended VLANs : 0
Maximum VLANs supported locally   : 4096
Configuration Revision            : 2
Primary ID                        : 0c77.5cca.e600
Primary Description               : SW-CORE
MD5 digest                        : 0xDD 0x69 0x09 0x64 0x91 0x65 0xC5 0x0F
                                    0x07 0xF2 0x66 0x3E 0xAE 0x19 0x7C 0xCC
```

Figure III .6 : **Démonstration de l'implémentation de VTP**

5. **Configuration de Vlan :** la figure III.7 Montre la configuration de Vlan dans le SW-CORE

```
SW-CORE(config)#Vlan 10
SW-CORE(config-vlan)#name server
SW-CORE(config-vlan)#Vlan 13
SW-CORE(config-vlan)#name MATH
SW-CORE(config-vlan)#Vlan 14
SW-CORE(config-vlan)#name SCIENCE
SW-CORE(config-vlan)#Vlan 16
SW-CORE(config-vlan)#name ELCT
SW-CORE(config-vlan)#Vlan 19
SW-CORE(config-vlan)#name MECHANIQUE
SW-CORE(config-vlan)#Vlan 20
SW-CORE(config-vlan)#name AUDITORUM
SW-CORE(config-vlan)#Vlan 30
SW-CORE(config-vlan)#name RECTORAT
SW-CORE(config-vlan)#Vlan 90
SW-CORE(config-vlan)#name MANAGMENT
```

Figure III.7 : Configuration des Vlan

6. **Démonstration de l'implémentation de Vlan :** la figure suivant montre la démonstration de l'implémentation de Vlan

```
SW-CORE#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/3, Gi1/0, Gi1/1, Gi1/2
                                                 Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                 Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                 Gi3/3
10   server                            active
13   MATH                              active
14   SCIENCE                           active
16   ELCT                              active
19   MECHANIQUE                        active
20   AUDITORUM                         active
30   RECTORAT                          active
90   MANAGMENT                         active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

Figure III.8 : Démonstration de l'implémentation de Vlan

7. **Configuration des interfaces Vlan :** la figure…. Montre la configuration de Vlan

```
SW-CORE(config)#interface Vlan10
SW-CORE(config-if)# ip address 10.10.10.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan13
SW-CORE(config-if)# ip address 172.16.13.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan14
SW-CORE(config-if)# ip address 172.16.14.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan16
SW-CORE(config-if)# ip address 172.16.16.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan19
SW-CORE(config-if)# ip address 172.16.19.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan20
SW-CORE(config-if)# ip address 172.16.20.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan30
SW-CORE(config-if)# ip address 172.16.30.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan90
SW-CORE(config-if)# ip address 192.168.90.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
```

Figure III.9 : Configuration interface Vlan

8. **Configuration des interfaces Vlan en mode Access : L**a configuration de l'interface Vlan en mode Access de vlan 10 qui reliée avec le serveur Nagios XI**.**

```
SW-CORE(config)#interface g0/3
SW-CORE(config-if)#switchport mode access
SW-CORE(config-if)#switchport access vlan 10
```

Figure III.10 : Configuration de l'interface avec les serveurs Nagios Xi

9. **Configuration des interfaces Vlan en mode trunk :** La configuration des interfaces en mode trunk avec les autres switches.

```
SW-CORE(config)#interface range g0/2,g0/0
SW-CORE(config-if-range)#$trunk allowed vlan 10,13,14,16,19,20,30,90,99
SW-CORE(config-if-range)# switchport trunk encapsulation dot1q
SW-CORE(config-if-range)# switchport trunk native vlan 99
SW-CORE(config-if-range)# switchport mode trunk
SW-CORE(config-if-range)# switchport nonegotiate
SW-CORE(config-if-range)#
```

Figure III.11** : **Configuration des interfaces Vlan en mode trunk

10. Configuration de SSH : Par défaut, on ne peut pas activer le SSH car il faut configurer certains paramètres pour que cela fonctionne, premièrement nous avons défini le nom de Domain-Name et après on génère une clé de chiffrement RSA utilisée par le processus SSH pour générer la clé de session. La variable "modulus 1024" définit la taille de votre clé, on définit un utilisateur nommé "*admin*" dont le mot de passe associé est "*admin*" puis on active le SSH pour savoir combien d'utilisateur peuvent accéder dans le switch au même temps, enfin il faut activer le SSH version 2 :

```
SW-CORE(config)#ip domain-name dahleb.dz
SW-CORE(config)#crypto key generate rsa modulus 1024
The name for the keys will be: SW-CORE.dahleb.dz

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

SW-CORE(config)#username admin priv 15 secret admin
SW-CORE(config)#line vty 0 4
SW-CORE(config-line)# logging synchronous
SW-CORE(config-line)# login local
SW-CORE(config-line)# transport input ssh
SW-CORE(config-line)#exit
SW-CORE(config)#ip ssh version 2
*Sep 10 15:38:06.190: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-CORE(config)#
```

Figure III.12 : Configuration de SSH

11. Configuration de DHCP et DNS : la Configuration de DHCP se fait dans 4 étape : tout d'abord, la création d'un pool DHCP math, ensuite le réseau à écouter 172.16.16.0/24, puis la passerelle par défaut 172.16.16.254 et enfin on termine par le DNS 8.8.8.8 :

```
SW-CORE(config)#ip dhcp pool MATH
SW-CORE(dhcp-config)#network 172.16.13.0 255.255.255.0
SW-CORE(dhcp-config)#default-router 192.16.13.254
SW-CORE(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
SW-CORE(dhcp-config)#!!!!!!!!!!!!!!!!
SW-CORE(dhcp-config)#ip dhcp pool SCIENCE
SW-CORE(dhcp-config)#network 172.16.14.0 255.255.255.0
SW-CORE(dhcp-config)#default-router 192.16.14.254
SW-CORE(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
SW-CORE(dhcp-config)#!!!!!!!!!!!!!!!!
SW-CORE(dhcp-config)#ip dhcp pool ELCTRONIQUE
SW-CORE(dhcp-config)#network 172.16.16.0 255.255.255.0
SW-CORE(dhcp-config)#default-router 192.16.16.254
SW-CORE(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
SW-CORE(dhcp-config)#!!!!!!!!!!!!!!!!
SW-CORE(dhcp-config)#ip dhcp pool MECHANIQUE
SW-CORE(dhcp-config)#network 172.16.19.0 255.255.255.0
SW-CORE(dhcp-config)#default-router 192.16.19.254
SW-CORE(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
SW-CORE(dhcp-config)#!!!!!!!!!!!!!!!!
SW-CORE(dhcp-config)#ip dhcp pool AUDITORUM
SW-CORE(dhcp-config)#network 172.16.20.0 255.255.255.0
SW-CORE(dhcp-config)#default-router 192.16.20.254
SW-CORE(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
SW-CORE(dhcp-config)#!!!!!!!!!!!!!!!!
SW-CORE(dhcp-config)#ip dhcp pool RECORAT
SW-CORE(dhcp-config)#network 172.16.30.0 255.255.255.0
SW-CORE(dhcp-config)#default-router 192.16.30.254
SW-CORE(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
SW-CORE(dhcp-config)#!!!!!!!!!!!!!!!!
SW-CORE(dhcp-config)#
```

Figure III.13 : Configuration de DHCP.

12. Démonstration de l'implémentation de DHCP : la figure suivant montre la Démonstration de l'implémentation de DHCP

```
Pool MATH :
 Utilization mark (high/low)     : 100 / 0
 Subnet size (first/next)        : 0 / 0
 Total addresses                 : 254
 Leased addresses                : 0
 Excluded addresses              : 0
 Pending event                   : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 172.16.13.1          172.16.13.1      - 172.16.13.254     0      / 0      / 254

Pool SCIENCE :
 Utilization mark (high/low)     : 100 / 0
 Subnet size (first/next)        : 0 / 0
 Total addresses                 : 254
 Leased addresses                : 0
 Excluded addresses              : 0
 Pending event                   : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 172.16.14.1          172.16.14.1      - 172.16.14.254     0      / 0      / 254

Pool ELCTRONIQUE :
 Utilization mark (high/low)     : 100 / 0
 Subnet size (first/next)        : 0 / 0
 Total addresses                 : 254
 Leased addresses                : 0
 Excluded addresses              : 0
 Pending event                   : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased/Excluded/Total
 172.16.16.1          172.16.16.1      - 172.16.16.254     0      / 0      / 254
```

Figure III.14 : Démonstration de l'implémentation DHCP

13. Configuration de routage inter-vlan : Tout d'abord le routage doit s'activer dans le switch, par la suite, on procède à l'implémentation des Vlan et leur interface avec l'adresse de chaque VLAN. Concernant les autres switches, ils doivent être connectés avec le lien trunk:

```
SW-CORE(config)#interface Vlan10
SW-CORE(config-if)# ip address 10.10.10.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan13
SW-CORE(config-if)# ip address 172.16.13.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan14
SW-CORE(config-if)# ip address 172.16.14.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan16
SW-CORE(config-if)# ip address 172.16.16.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan19
SW-CORE(config-if)# ip address 172.16.19.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan20
SW-CORE(config-if)# ip address 172.16.20.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan30
SW-CORE(config-if)# ip address 172.16.30.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
SW-CORE(config-if)#interface Vlan90
SW-CORE(config-if)# ip address 192.168.90.254 255.255.255.0
SW-CORE(config-if)#no sh
SW-CORE(config-if)#!!!
```

Figure III.15 : Démonstration de l'implémentation des interfaces vlan

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Vlan10
L        10.10.10.254/32 is directly connected, Vlan10
      172.16.0.0/16 is variably subnetted, 12 subnets, 2 masks
C        172.16.13.0/24 is directly connected, Vlan13
L        172.16.13.254/32 is directly connected, Vlan13
C        172.16.14.0/24 is directly connected, Vlan14
L        172.16.14.254/32 is directly connected, Vlan14
C        172.16.16.0/24 is directly connected, Vlan16
L        172.16.16.254/32 is directly connected, Vlan16
C        172.16.19.0/24 is directly connected, Vlan19
L        172.16.19.254/32 is directly connected, Vlan19
C        172.16.20.0/24 is directly connected, Vlan20
L        172.16.20.254/32 is directly connected, Vlan20
C        172.16.30.0/24 is directly connected, Vlan30
L        172.16.30.254/32 is directly connected, Vlan30
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/1
L        192.168.0.1/32 is directly connected, GigabitEthernet0/1
      192.168.90.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.90.0/24 is directly connected, Vlan90
L        192.168.90.254/32 is directly connected, Vlan90
```

Figure III.16 : Commande d'affichage de table de routage

14. Configuration SNMP : dans cette configuration, nous avons lié l'accès de notre switch à un serveur de supervision basé sur le protocole SNMP. Tout d'abord on définit l'Access-List pour autoriser la connexion du serveur de management SNMP, puis on crée le nom de la communauté SNMP ainsi que les droits associés (RO/RW) :

```
SW-CORE(config)#snmp-server community karim RW
SW-CORE(config)#snmp-server host 10.10.10.136 version 2c karim
SW-CORE(config)#snmp-server enable traps
SW-CORE(config)#!!!!!!!!!!
SW-CORE(config)#
```

Figure III.17 : Configuration de SNMP

II.4.2.5. Configuration routeur :

Pour obtenir un bon réseau et une bonne configuration, il faut suivre ces étapes :

- Configuration des interfaces,
- Configuration routage dynamique,
- Configuration NAT.

1) **Configuration interfaces :** les configurations des interfaces dans le routeur R1 :

```
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#interface f1/0
R1(config-if)#ip address dhcp
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#interface f1/1
R1(config-if)#ip address 192.168.100.1 255.255.255.0
R1(config-if)#
```

Figure III.18 : Configuration des interfaces

2) **Configuration routage dynamique** : L'activation d'un protocole de routage OSPF consiste à déclarer une interface dans le processus de routage dynamique, le numéro du processus OSPF est 1. L'adresse IP de l'interface connectée à un autre switch layer 3 est 192.168.0.1/24 et le numéro de l'aire est 0.

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 0.0.0.0 0.0.0.0 area 0
R1(config-router)#passive-interface f1/0
R1(config-router)#
```

Figure III.19 : Configuration routage dynamique

3) **Configuration NAT** : Les interfaces sont configurées du NAT entrant et sortant. La commande Access-List définit les IP autorisées et le NAT est configuré pour translaté les adresses internes vers l'interface externe.

```
R1(config-if)#access-list 1 permit any
R1(config)#interface f1/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface f0/0
R1(config-if)#ip nat inside
R1(config-if)#
R1(config-if)#exit
R1(config)#interface f1/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat inside source list 1 interface f1/0 overload
R1(config)#
```

Figure III.20 : Configuration NAT

II.5. La gestion de surveillance des équipements :

Après avoir étudié de nombreux logiciels, nous avons adopté l'interface graphique de Nagios xi dans le but de réaliser le projet et suivre les dispositifs suivants.

II.5.1. Ajouter les équipements dans Nagios XI :

Pour ajouter des appareils dans Nagios xi, vous devez passer par les étapes suivantes :

Premièrement, ouvrez l'interface Nagios xi et dirigez-vous vers configure puis configuration Wizards (voir la figure)

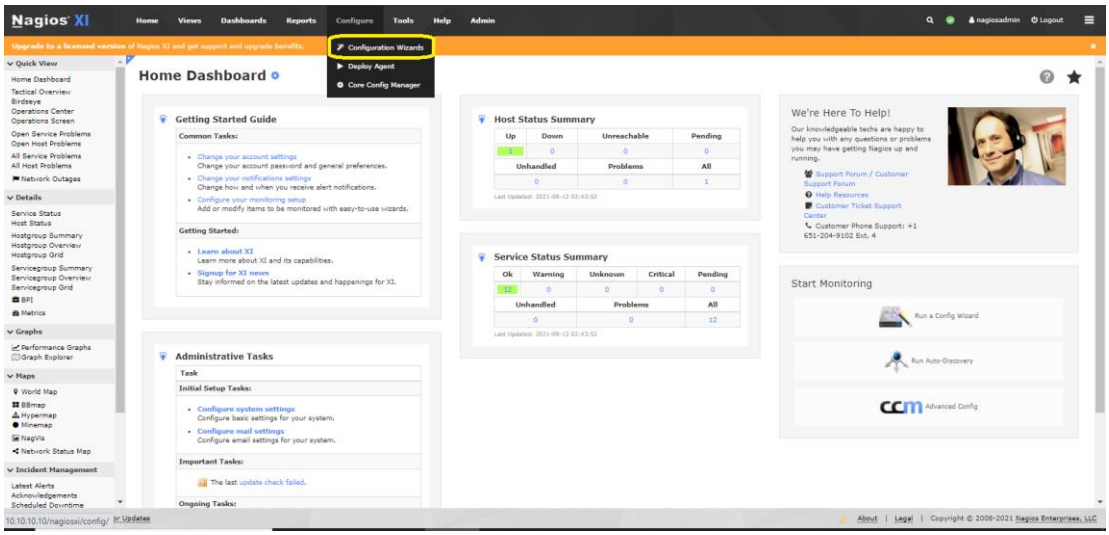

Figure III.21 : Interface graphique Nagios XI

Recherchez ensuite network switch /router et cliquez dessus (voir figure III.22)

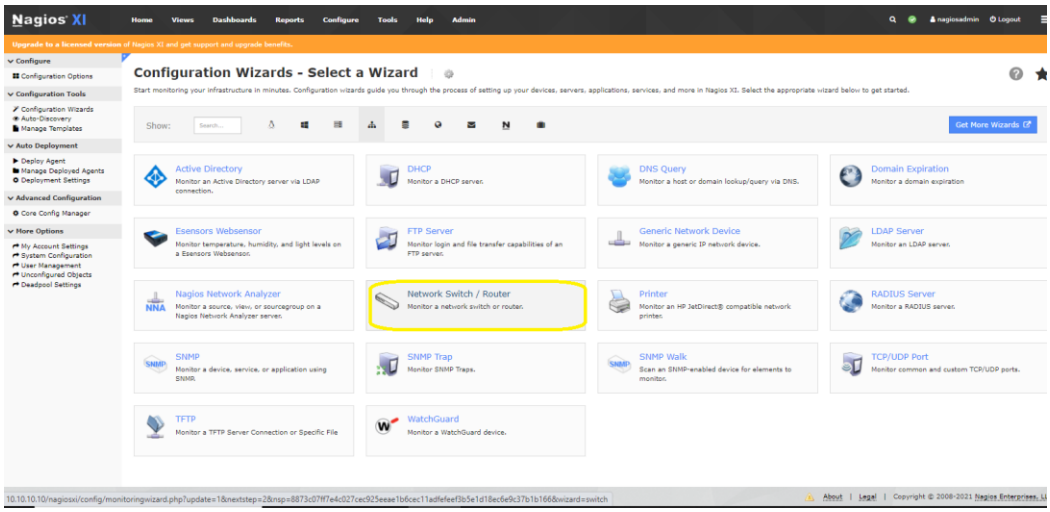

Figure III.22 : Assistant de configuration

Après qu'une interface s'ouvre, nous ajoutons l'adresse IP de l'équipement (SW-CORE) et le nom de SNMP communauté (community) :(voir figure *III.23*)

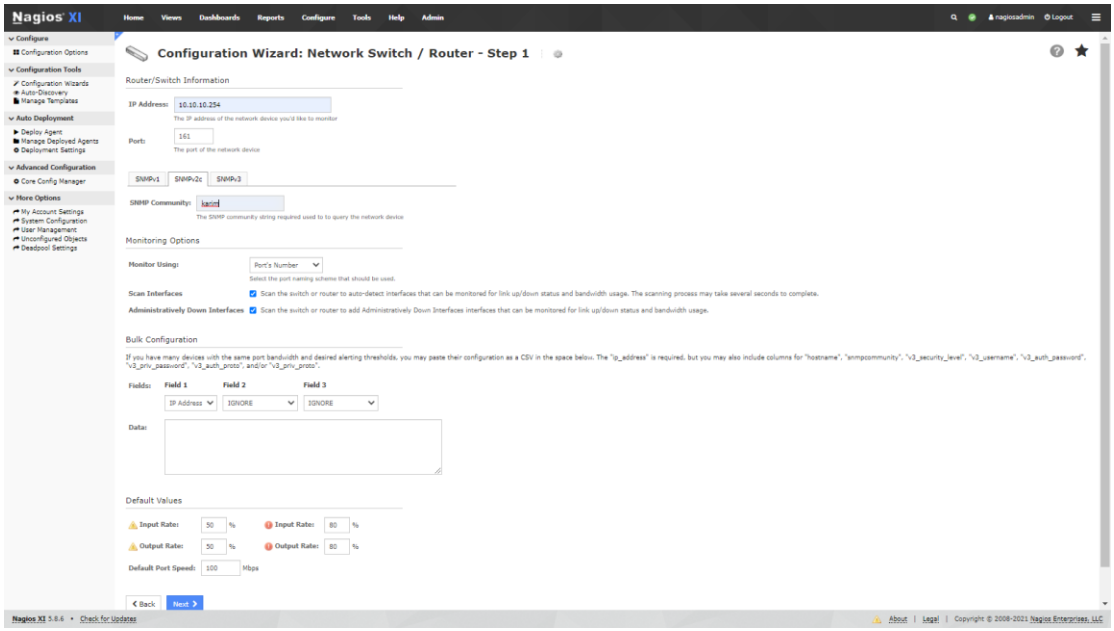

Figure III.23 : Joindre une adresse IP

A partir de l'adresse IP introduite, Nagios XI lance ainsi une découverte des interfaces :

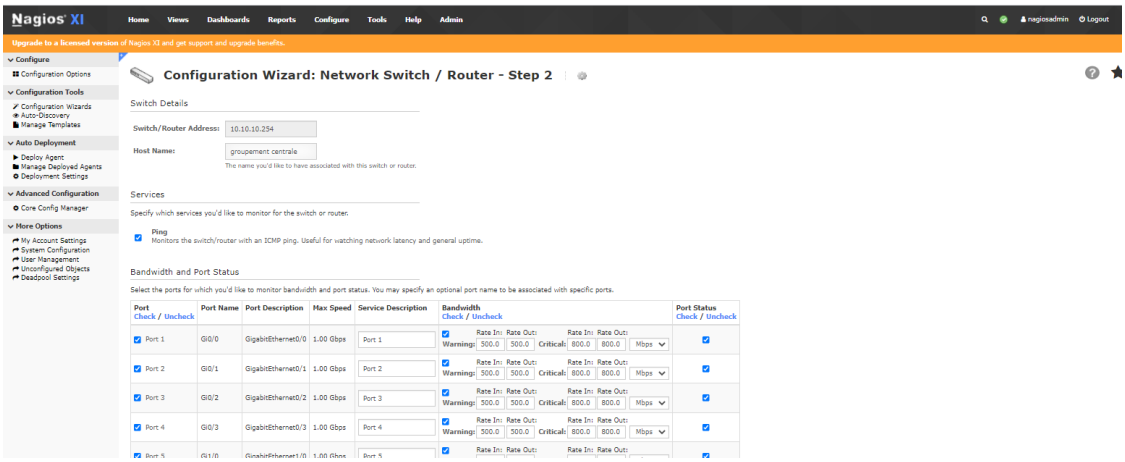

Figure III.24 : Détail du commutateur

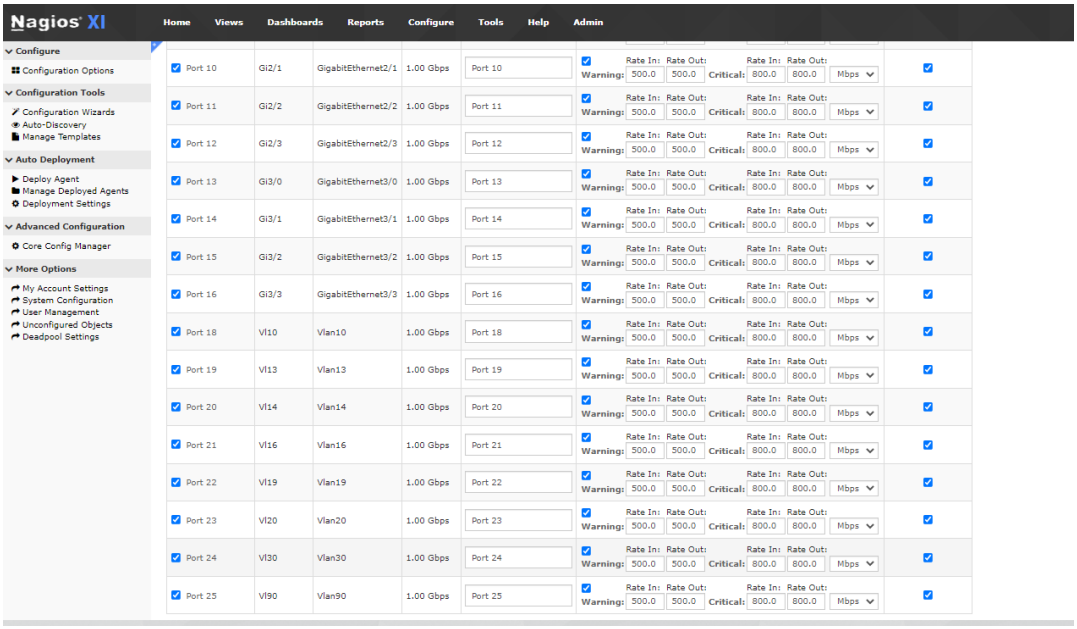

Figure III.25 : Détail du commutateur (suite)

Après avoir appuyé sur **Next**, un message annonce la configuration appliquée avec succès (voir figure III.26)

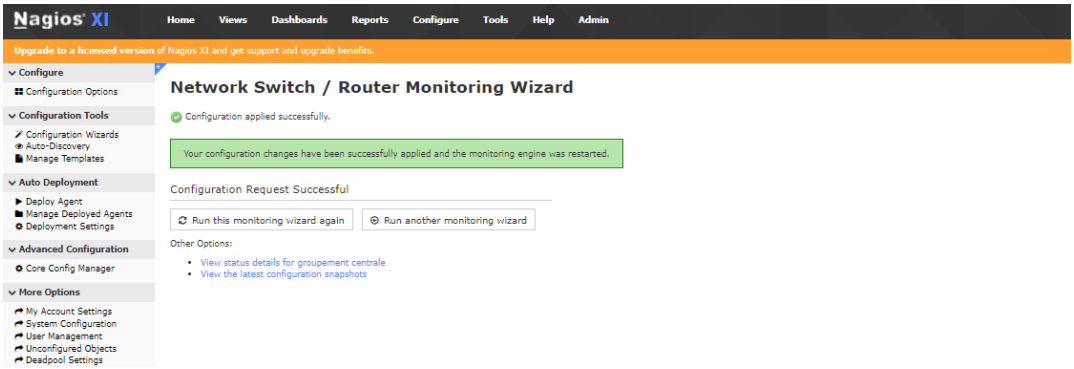

Figure III.26 : Demande de configuration réussie

En cliquant sur l'option "Viewstatusdetail for GroupementCentrale " Le résultat apparaît dans la figure III.27

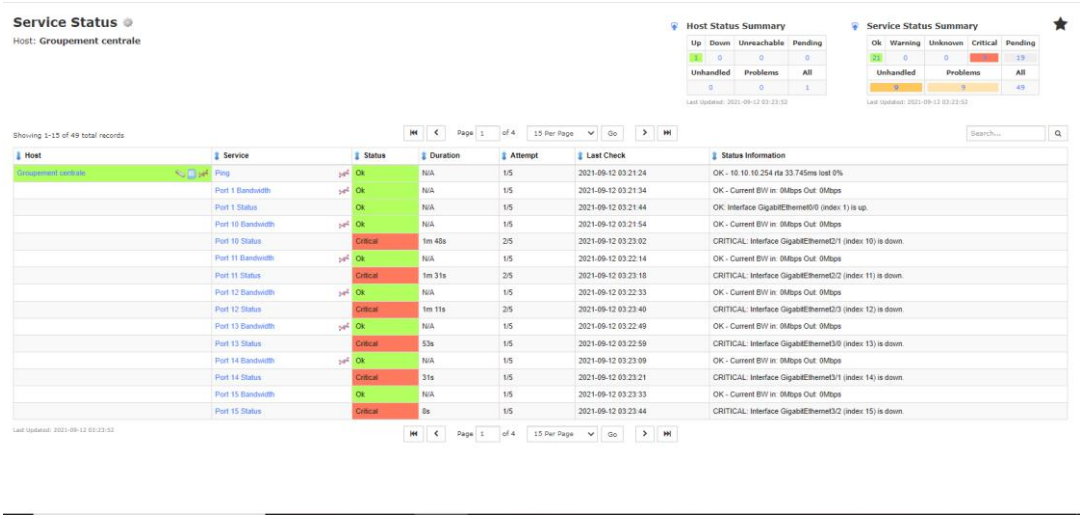

Figure III.27 : Résultat et l'état de service

II.5.2. Ajouter machine linux dans Nagios XI :

Pour ajouter un serveur Linux dans Nagios XI, cliquez sur l'option "Linux SNMP"

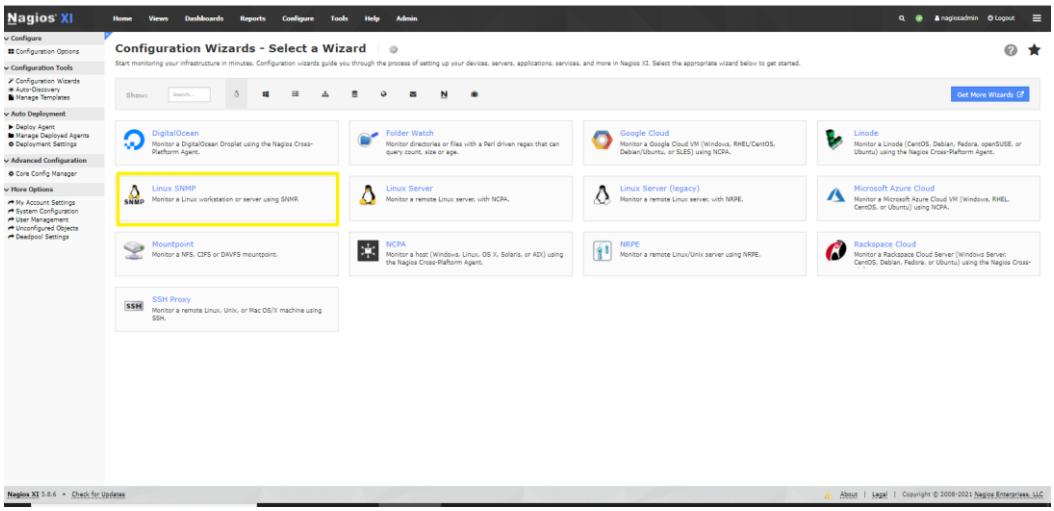

Figure III.28 : Assistant de configuration

Après avoir ouvert la fenêtre "LINUX SNMP", nous ajoutons l'adresse IP de Linux, la version de SNMP(2C) et le nom de SNMP communauté :

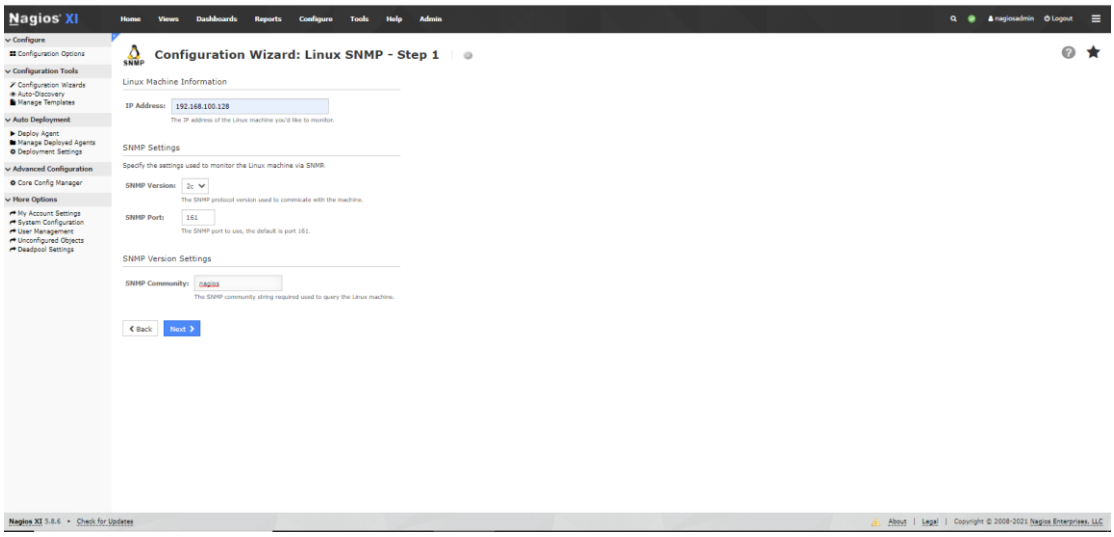

Figure III.29 : Joindre adresse IP du serveur Linux

Après avoir appuyé sur "**Next**", l'interface de sélection des options de surveillance apparaît. Nous choisissons tout ce que nous souhaitons superviser.

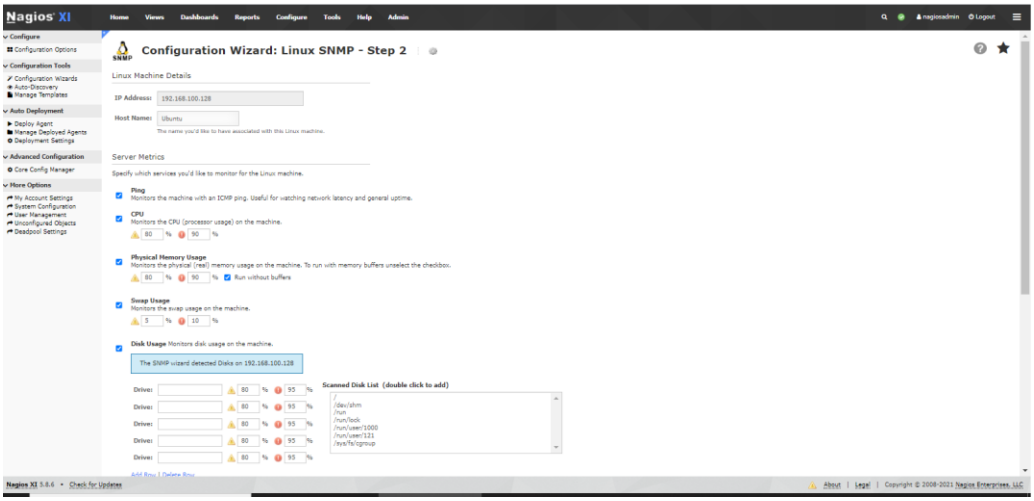

Figure III.30 : Les Choix de supervision

Apres avoir appuyé sur Next, une fentre de Modification de temps de Rê-surveillance et de vérification de l'hôte et du service entre le serveur linux et Nagios XI apparait.

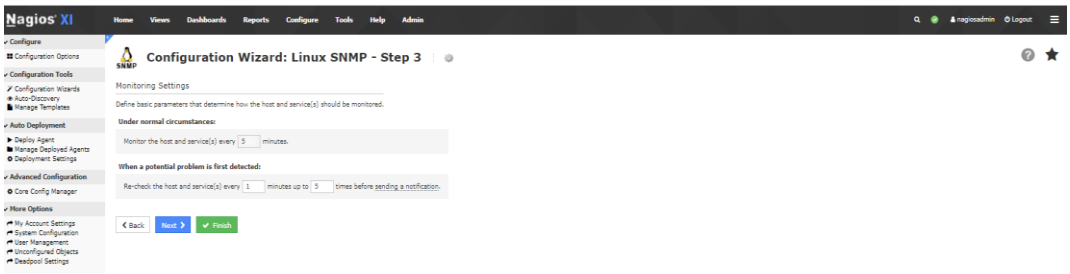

Figure III.31 : Indiquer le temps de Rê-surveillance de l'hôte et du service

Après avoir appuyé sur **Next**, un message annonce la configuration appliquée avec succès (voir figure III.32)

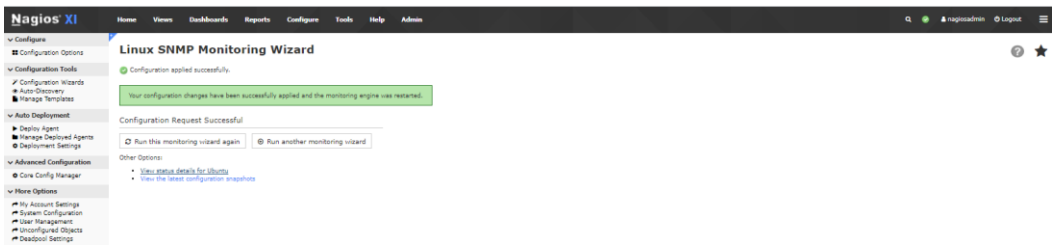

Figure III.32 : Demande de configuration réussie (serveur linux)

Voir le resultat suivant sur la figure III.33

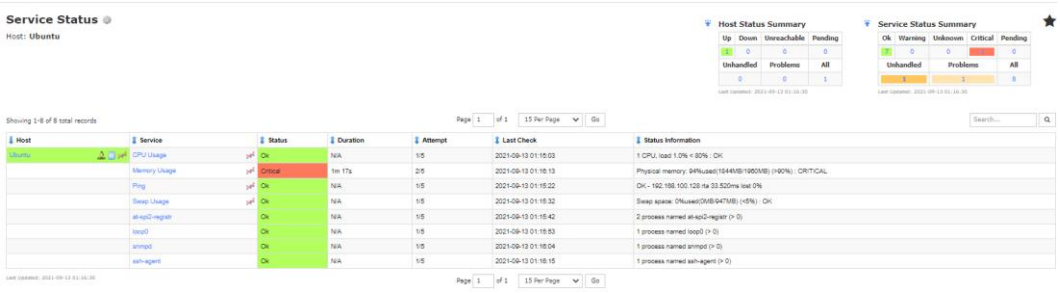

Figure III.33 : Résultat et l'état de service (serveur Ubuntu)

Afin de traiter tous les equipements, nous avons reussie à superviser tout le reseau de l'universite (figure III.34).

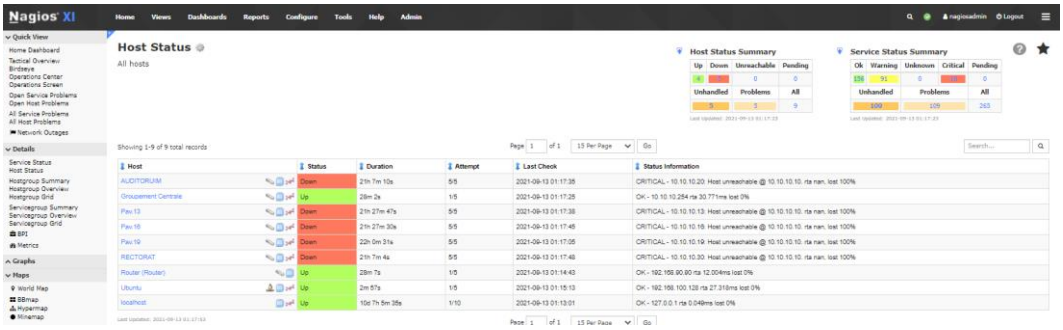

Figure III.34 : L'état des équipements

II.5.3. Configuration de courrier électronique :

Pour créer un projet de surveillance professionnelle et remarquer les changements dans le réseau, grâce à Nagios, une page a été créée pour permettre la communication par e-mail, pour recevoir des messages et des alertes de réseaux.

Les étapes suivantes nous permettent de comprendre en détail comment les e-mails sont envoyés par Nagios XI :

- Configuration SMTP pour les notifications Nagios XI
- Recevoir les alertes Nagios par e-mail Nagios XI

1. **Configuration SMTP :**

   L'utilisation de SMTP comme méthode d'envoi d'e-mails, vous permet de configurer Nagios XI via l'utilisation d'un serveur de messagerie pour la livraison du courrier.

   Les paramètres de messagerie dans Nagios XI se trouvent dans **Admin > System Config > Email Settings.**

   Nous choisissons, d'abord, la méthode SMTP, ensuite nous ajoutons l'email dans le nom d'utilisateur, le mot de passe de notre mail qui autorise les connexions depuis le serveur Nagios XI puis le numéro de port de SMTP et nous sélectionnons TLS pour que les e-mails soient envoyés cryptés.

   Pour assurer les informations, il faut cliquer sur **Update setting**

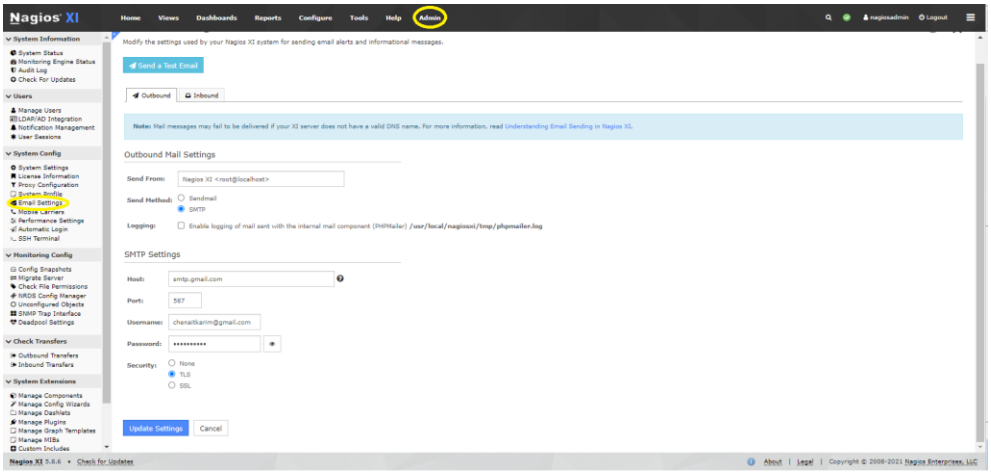

Figure III.35 : Paramétrage de la messagerie

Pour vérifier la réception des messages et notifications, nous appuyons sur « **Send Test Email »**

Figure III.36 : Tester les paramètres de messagerie

La figure III.37 Montre que le message a été bien envoyé

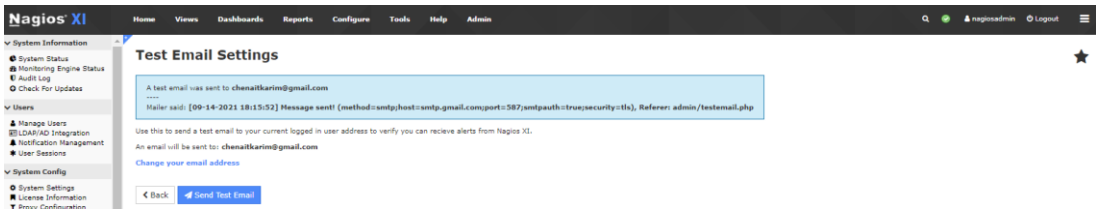

Figure III.37 : Tester les paramètres de messagerie (suite)

La figure III.38 Signifie que le message a été bien reçu

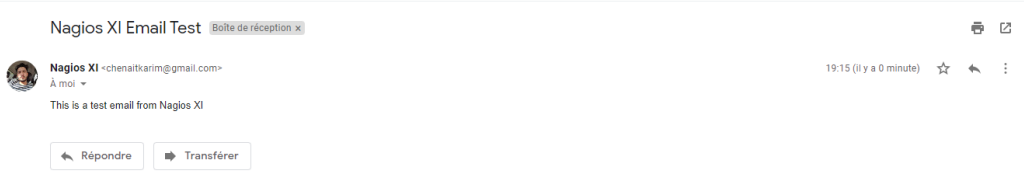

Figure III.38 : Recevoir le test mail par Nagios XI

III.5.4. Recevoir les alertes Nagios par e-mail :

Les notifications peuvent être des e-mails envoyés aux utilisateurs lorsque les hôtes et les services changent les états, cela permet aux utilisateurs de rester informés de la santé de leur environnement de surveillance.

Pour modifier comment, quand et pourquoi un utilisateur reçoit des notifications, cliquez sur **Admin > Notification Preferences.**

Sélectionnez le type d'alerte que vous souhaitez recevoir et cliquez par la suite sur **Update Settings**

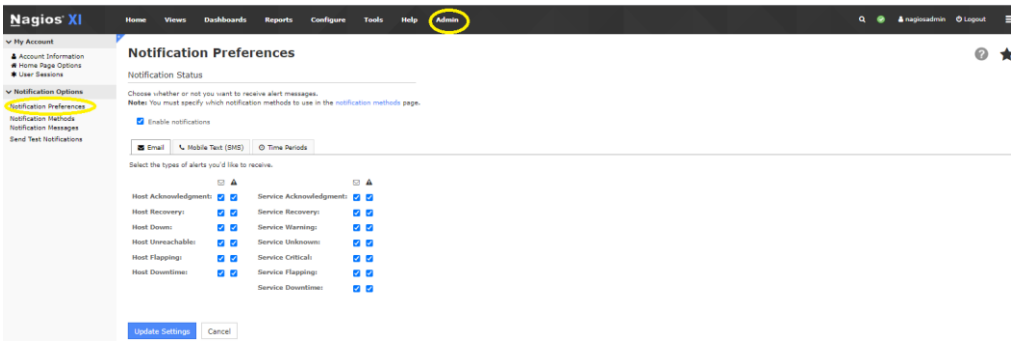

Figure III.39 : Type d'alerte

Ensuite on va sélectionner l'option **« Notification method »** et cliquer sur **« Receive alerts via email »** puis sur **« Update settings » :**

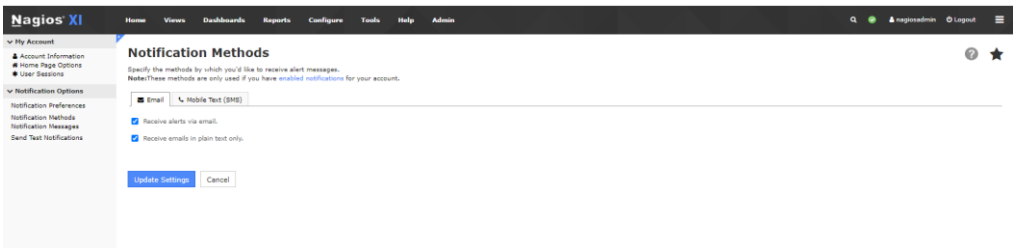

Figure III.40 : Méthode de notification

Et au final, pour verifier l'arrivée des notifications, on se dirige vers l'option **« Send test notification »**

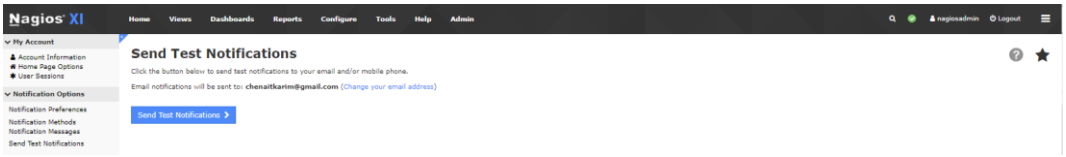

Figure III.41 : Envoyer une notification de test

La figure montre que le message a été bien envoyé.

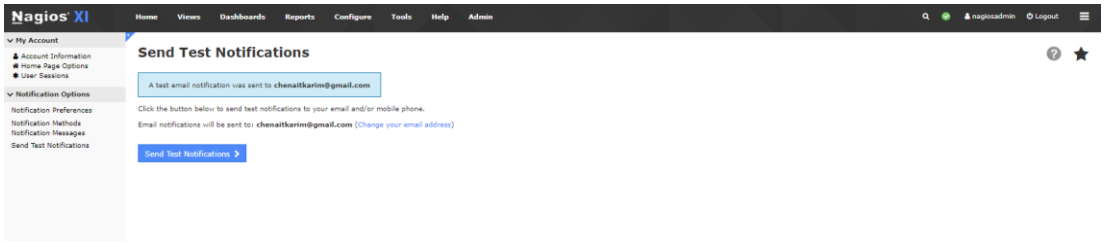

Figure III.42 : Envoyer une notification de test (suite)

Les messages de Nagios XI sont reçus dans notre adresse mail

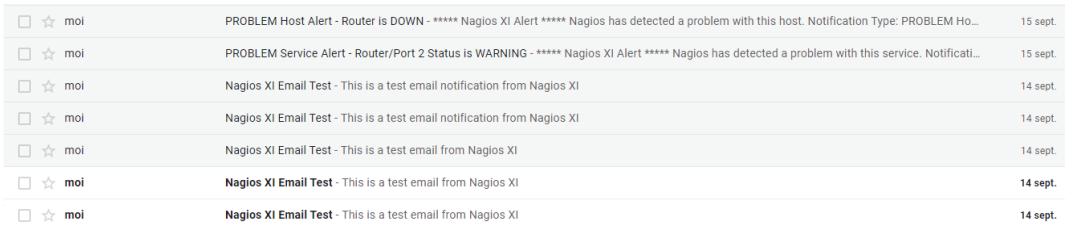

Figure III.43 : Les messages reçus de Nagios XI

III.6. CONCLUSION :

Dans ce chapitre, le projet a été présenté en détail dans son volet pratique, où un réseau a été créé pour l'université grâce à GNS3, et tous ses détails et modifications ont été surveillés à distance en recevant des notifications et des alertes à l'aide du Nagios XI.

Conclusion générale

Suite à un travail acharné et à l'acquisition de nombreux concepts scientifiques et appliqués se rapportant au sujet de notre mémoire d'étude, nous avons réussi à atteindre l'objectif de notre recherche dans laquelle nous avons créé et surveillé tous les appareils, Switches, routeurs et serveur Ubuntu et le statut de chacun d'eux a été examiné à distance, ce qui a permis de recevoir des alertes et des notifications sur l'ensemble des changements survenus en temps réel sur le réseau.

Ceci est dû à notre choix du programme approprié en termes de coût et de qualité, soit « Nagios XI » qui est l'un des meilleurs programmes open source car il présente les avantages de surveiller l'état des services réseau, de surveiller les ressources de l'hôte et de déterminer le niveau de l'hôte du réseau, entre autres atouts.

A travers notre traitement du sujet et les paramètres réseau de base, nous concluons qu'il est indispensable de développer et de créer un réseau performant respectant tous les critères nécessaires à son succès/bon fonctionnement, et parmi ces critères nous proposons brièvement les suivants :

- Etude détaillée de l'aspect scientifique.
- Étude du schéma du réseau en termes de quantité et de position des appareils.
- Choix des meilleurs équipements et câbles.
- S'assurer que les configurations sont correctes et précises (Vlan VTP SSH OSPF NAT SNMP.....).
- Protection du réseau en ajoutant des outils de sécurité.
- Ajout des programmes de surveillance pour vous assurer que les changements sont remarqués.

Pour conclure, il sied de dire que grâce au logiciel « Nagios XI », nous avons pu surveiller et recevoir des messages et des alertes sur l'état du réseau en temps réel, ce qui permet, en finalité, d'assurer la protection du réseau et la pérennité du service, et donc un gain de temps et d'argent.

A. Installation de GNS3 :

Cette partie explique comment installer GNS3 en utilisant un environnement Windows.

A.1 Etape 1 : téléchargement Gns3

Suivez ces étapes pour télécharger GNS3 sur votre PC. À l'aide d'un navigateur Web, accédez à https://gns3.com et cliquez sur le lien de téléchargement gratuit :

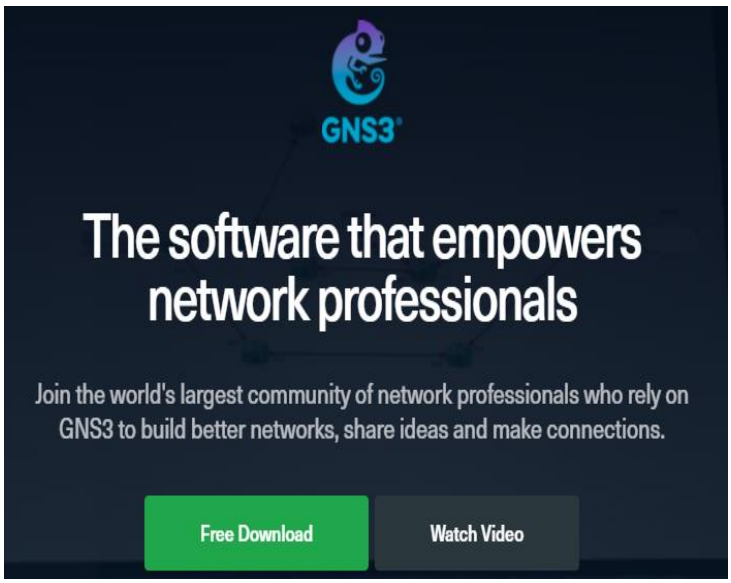

Figure A.1- Lien de téléchargement

Si vous n'êtes pas déjà inscrit sur le site GNS3, créez un compte puis cliquez sur Créer un compte & Continuer :

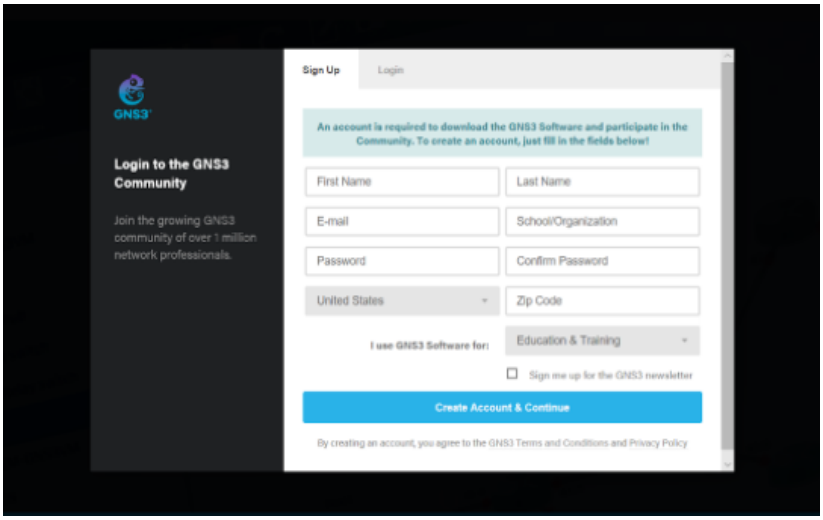

Figure A.2 : Crée un compte GNS3

Après la connexion, nous sélectionnerons l'installation de Windows. Cliquez sur le bouton Télécharger pour télécharger le GNS3 :

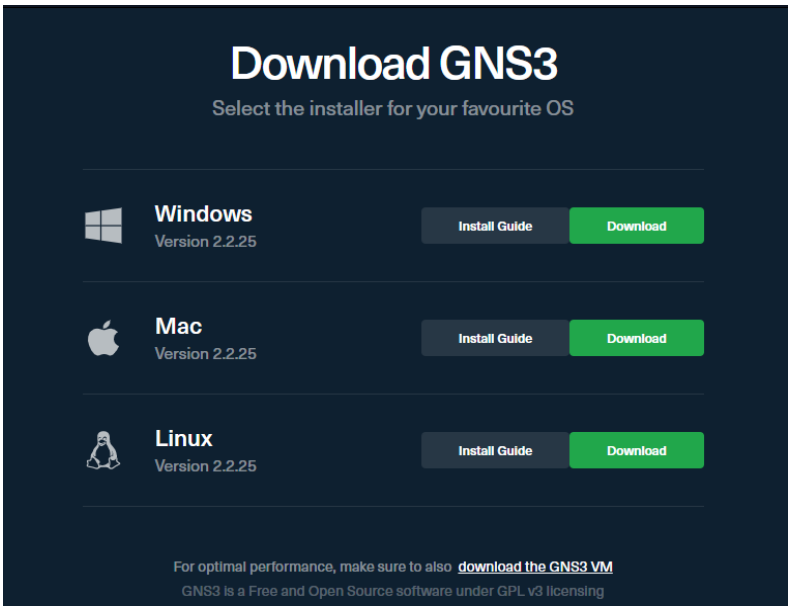

Figure A.3 : ***Sélectionner la version de GNS3 à télécharger***

Le package GNS3 sera automatiquement téléchargé sur votre PC :

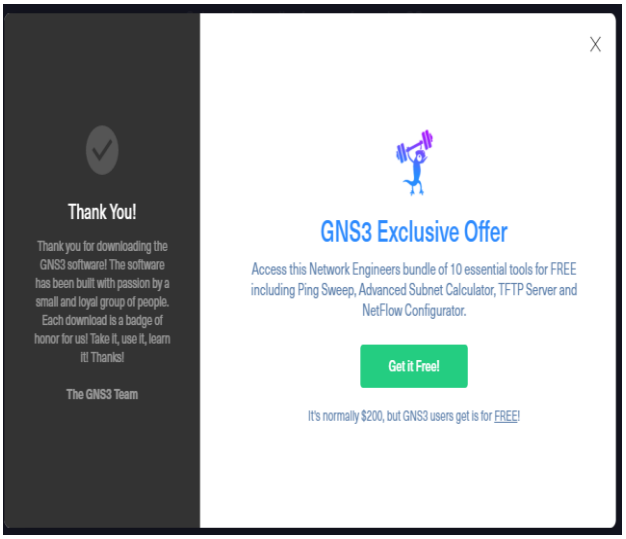

Figure A.4 : GNS3 a été télécharger

A.2 Etape 2 : installation le Package GNS3

La configuration GNS3 s'affiche. Cliquez sur Suivant > pour démarrer l'installation :

Figure A.5 : Configuration GNS3

Cliquez sur le bouton **« I Agree »** pour continuer l'installation :

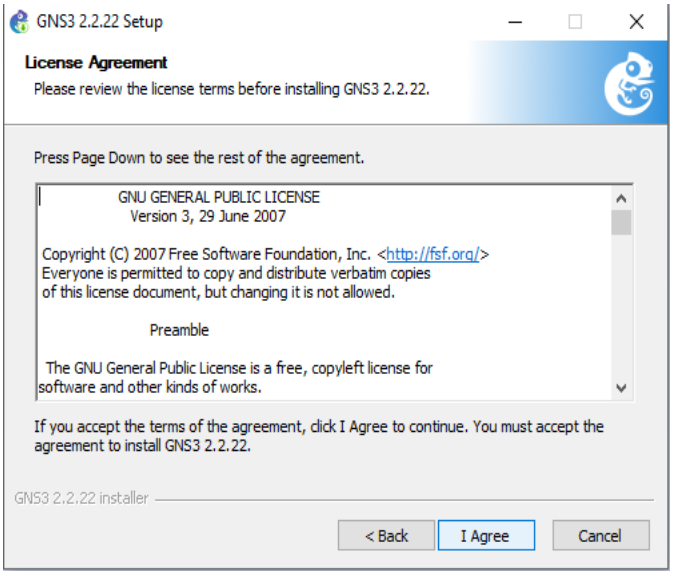

Figure A.6 : Accord de licence

Sélectionnez le dossier du menu Démarrer pour le raccourci GNS3. Cliquez sur Suivant > pour continuer l'installation :

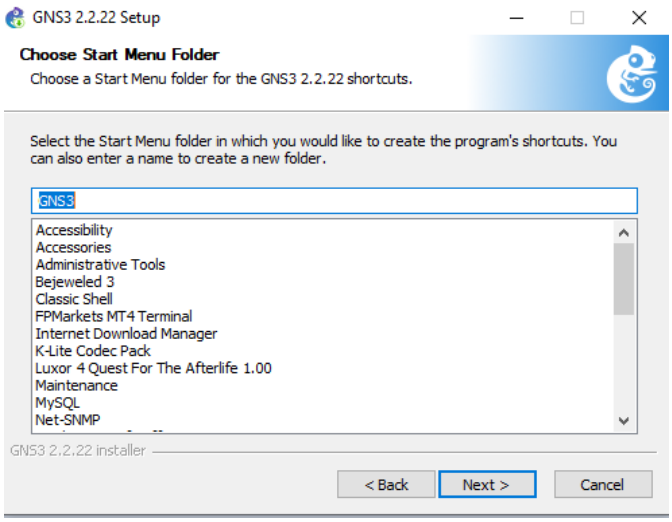

Figure A.7 : Choisir le dossier de raccourci

Choisir la fonctionnalité de Gns3 que vous souhaitez installer et cliquez sur suivant pour Continuer :

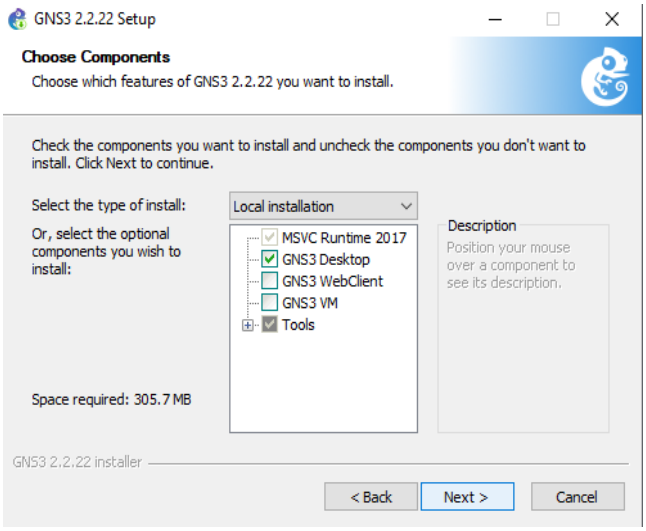

Figure A.8 : Sélectionner les composant

Choisir l'emplacement d'installation, cliquez sur suivant pour Continuer :

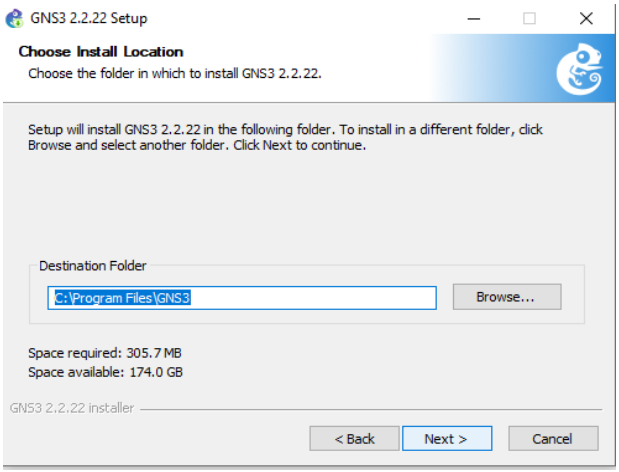

Figure A.9 : L'emplacement d'installation

Attendre pendant que Gns3 soit installé et cliquer sur suivant pour Continuer :

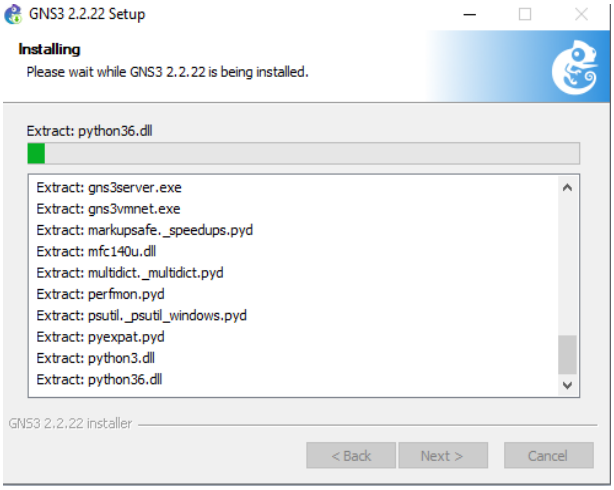

Figure A.10 : Commence l'installation

La figure montre que le GNS3 a été installé sur PC, il faut alors cliquer sur **« Finish » :**

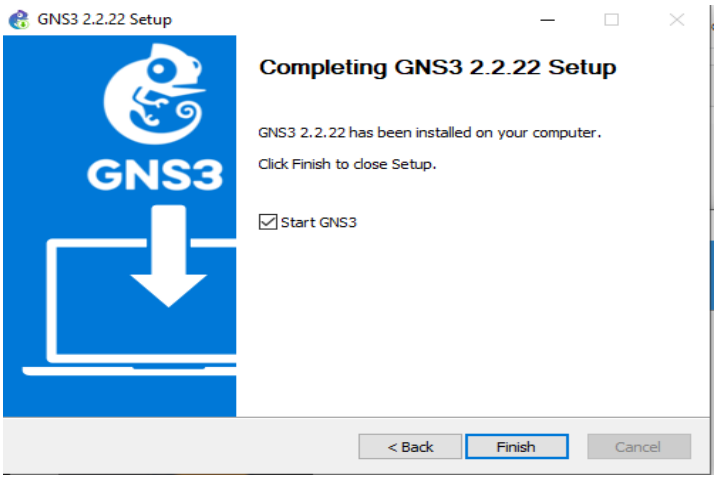

Figure A.11 : Installation termini

B. Installation Ubuntu in VMware Workstation:

Cette partie explique comment installer Ubuntu en utilisant un environnement VMware :

1. Télécharger l'image ISO de l'Ubuntu à partir de site officiel d'Ubuntu **https://ubuntu.com/#download.**
2. Une fois le fichier ISO Ubuntu téléchargé, ouvrir VMware Workstation et ajouter l'image ISO dans la VMware
3. Les Etapes d'installation d'Ubuntu sur VMware :

Pour commencer l'installation d'Ubuntu, il faut allumer la machine virtuelle.

La figure montre que Ubuntu a démarré :

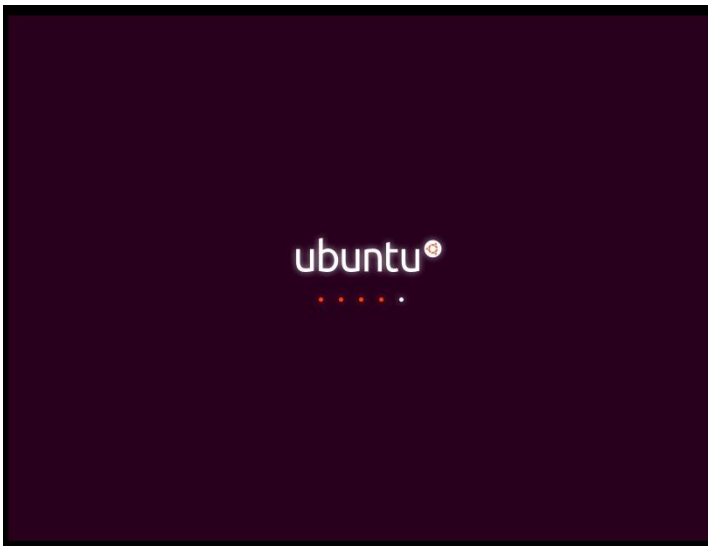

Figure B.1 : Ubuntu allumer

Pour installer Ubuntu, cliquer sur Installer Ubuntu.

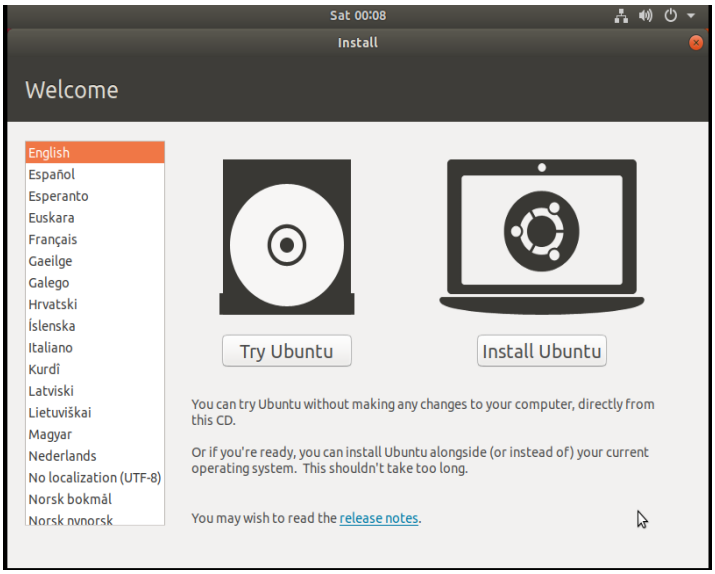

Figure B.2 : Installation Ubuntu

Sélectionner le mode de clavier et cliquer sur Continuer :

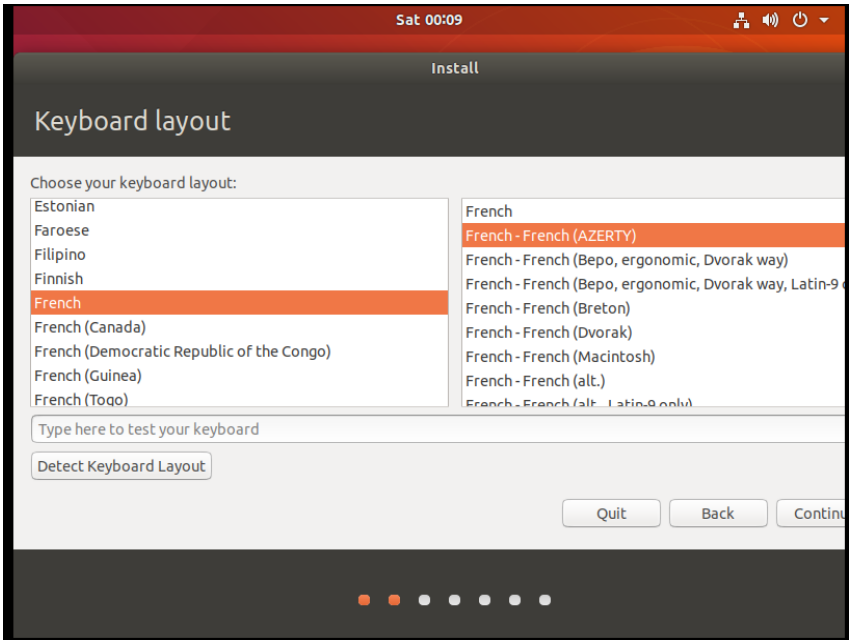

Figure B.3 : Choix du clavier

On Clique sur Continuer :

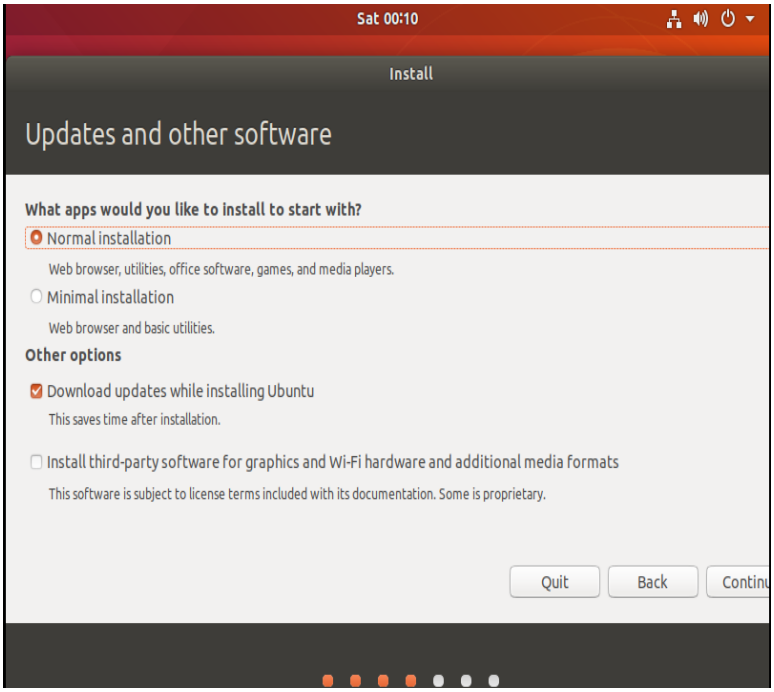

Figure B.4 : Sélectionner les options pour continuer l'installation

Sélectionner **« Erase Disk and Install Ubuntu »**, cliquer sur Installer maintenant :

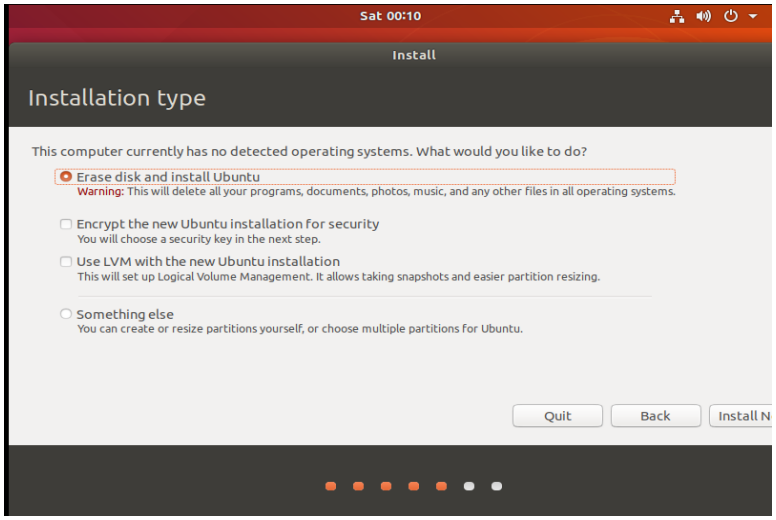

Figure B.5 : Choisir le type d'installation

Cliquer sur Continuer :

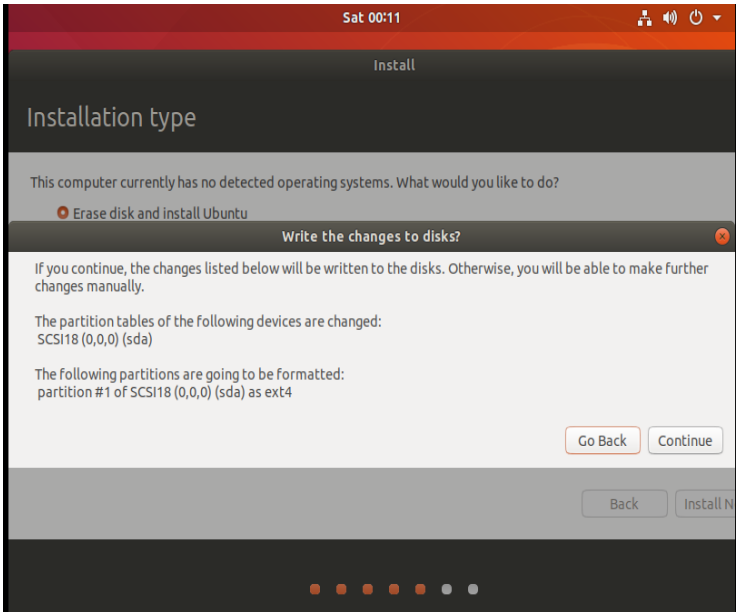

Figure B.6 : Choisir le type d'installation (suite)

Sélectionner la zone horaire et cliquer sur Continuer :

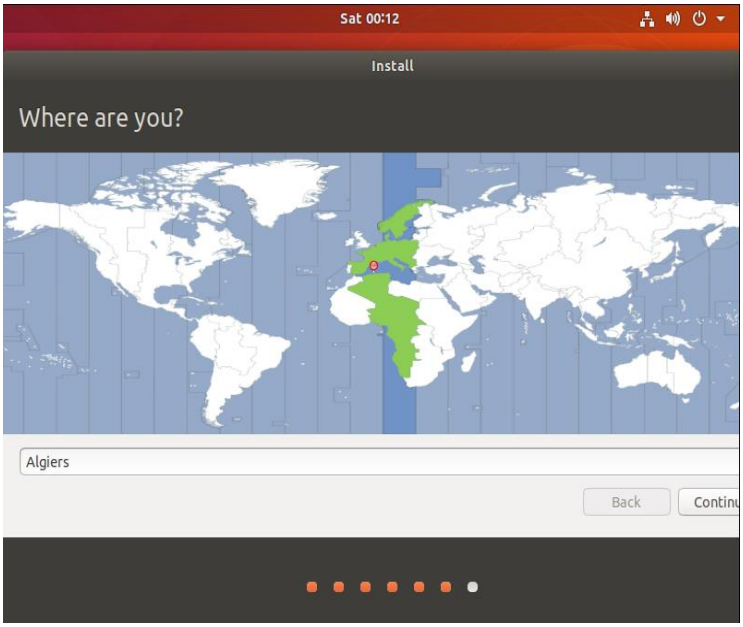

Figure B.7 : Zone horaire

Renseigner les informations personnelles puis cliquer sur continuer :

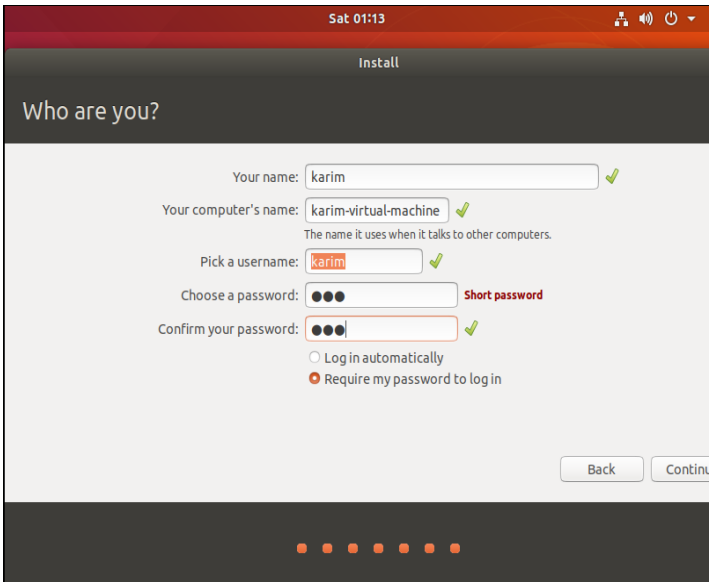

Figure B.8 : Saisie des informations personnelles

La mise en place du programme a commencé et cela peut prendre quelques temps :

Figure B.9 : Installation en cours

L'installation du l'Ubuntu a été effectuée avec succès :

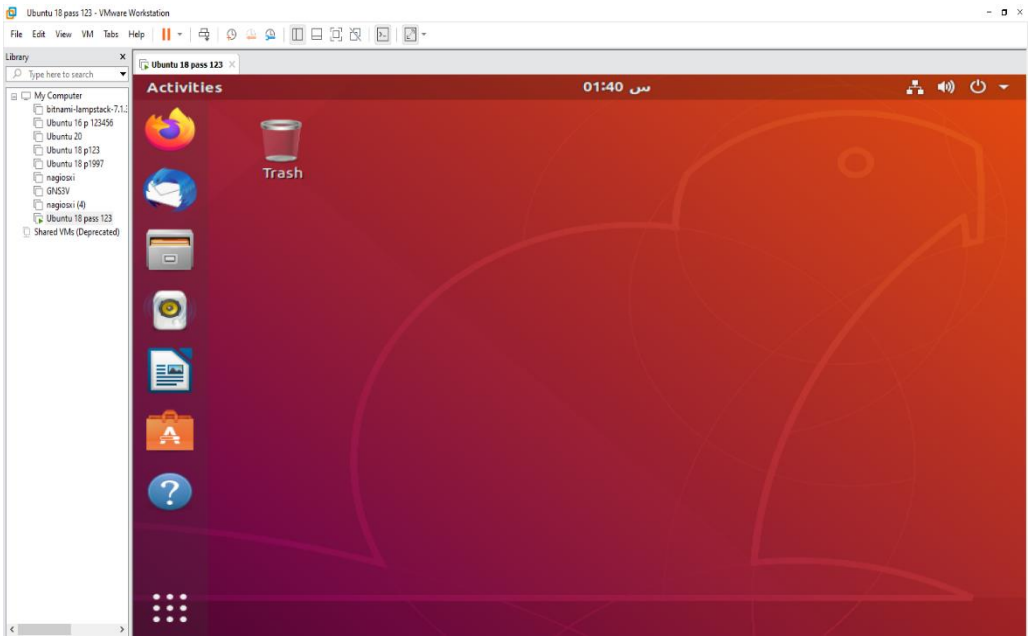

Figure B.10 : Installation complète

C. Installation Nagios XI :

Les étapes requises pour installer Nagios XI dans VMware Workstation Player :

- Télécharger le fichier OVA de Nagios XI à partir du site officiel de Nagios https://www.nagios.com/downloads/nagios-xi/microsoft.
- Lorsque le téléchargement est terminé, il faut importer le fichier OVA de Nagios XI dans la VMware et allumer Nagios Xi.
- Les étapes d'installation Nagios XI :

Quand on allume Nagios XI dans VMware, on aperçoit l'apparition de l'interface suivante :

Figure C.1 : Interface Nagios XI dans VMware

Ouvrir le navigateur web et taper l'adresse IP de Nagios XI (Trouvé dans VMware) dans la barre de recherche puis appuyer sur Entrer :

Figure C.2 : Accès à Nagios XI

En cliquant sur **Access Nagios XI** pour configurer les paramètres de programme :

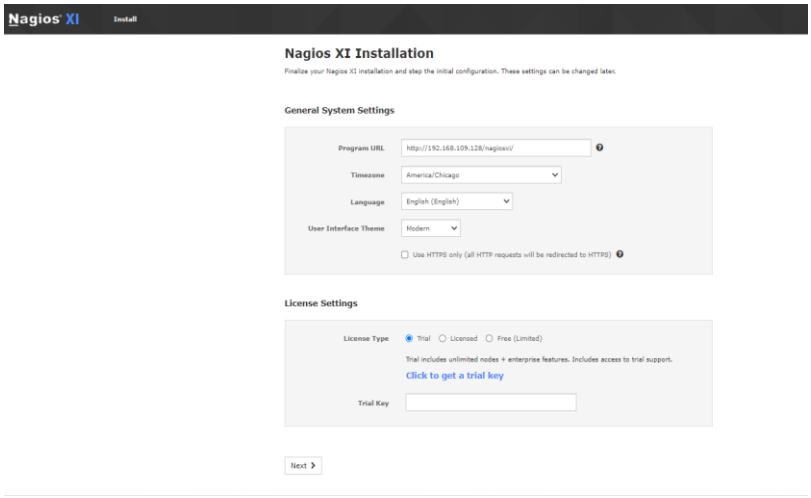

Figure C.3 : Configuration de réglage de Nagios XI

Après avoir cliqué sur **Next,** on configure le nom, mot de passe une fois le changement fait, cliquez sur Install :

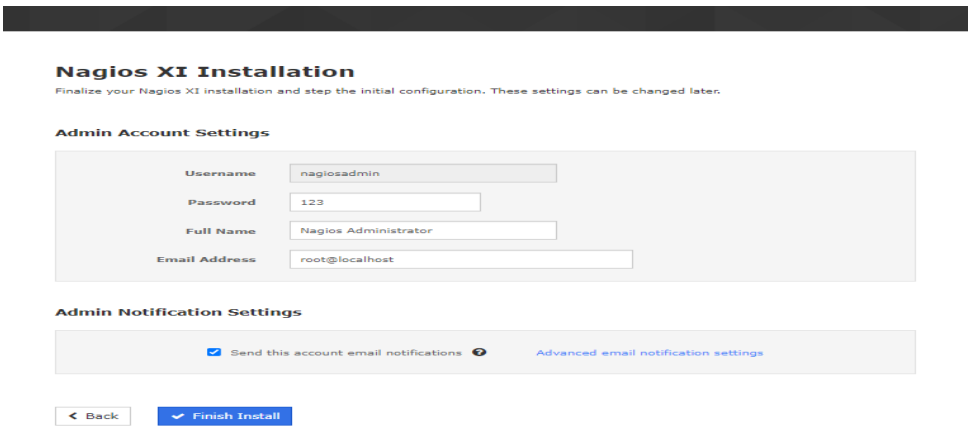

Figure C.4 : Configuration du mot de passe

La figure C.5 montre que l'installation est terminée.

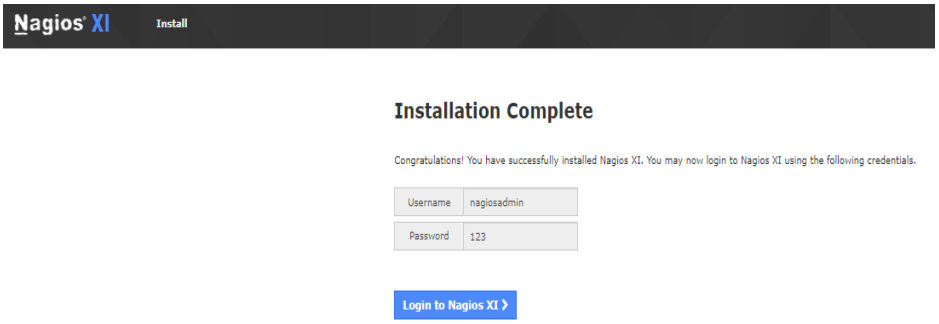

Figure C.5 : Installation complète

Insérer les informations à partir de la page précédente et cliquer sur **Login :**

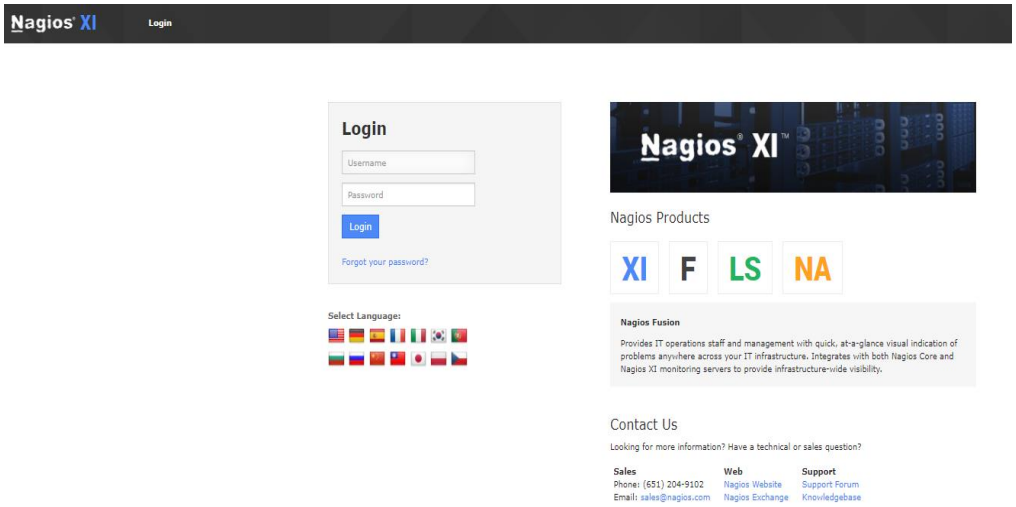

Figure C.6 : Page de connexion

Pour accéder au tableau de bord de Nagios XI, il suffit de cliquer sur **Submit**

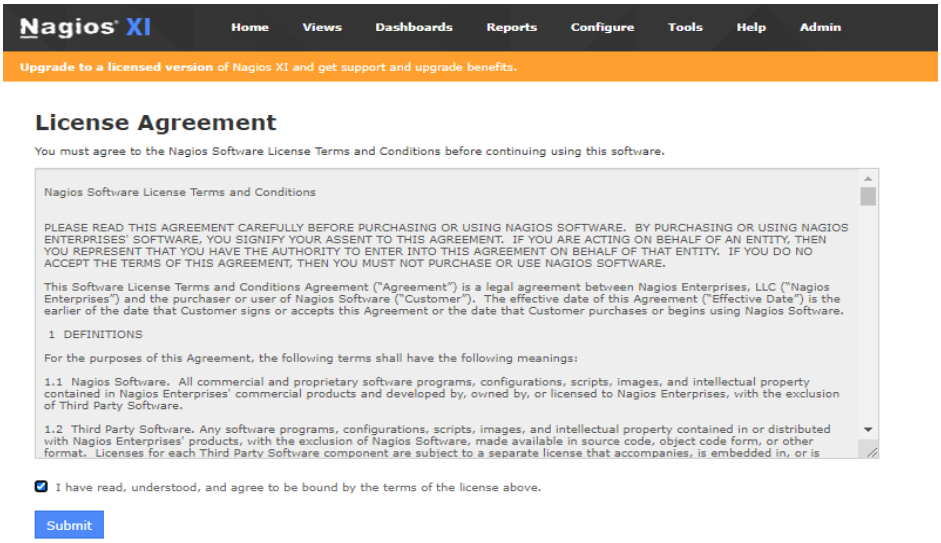

Figure C.7 : Accord de licence

Voici le tableau de bord de Nagios XI :

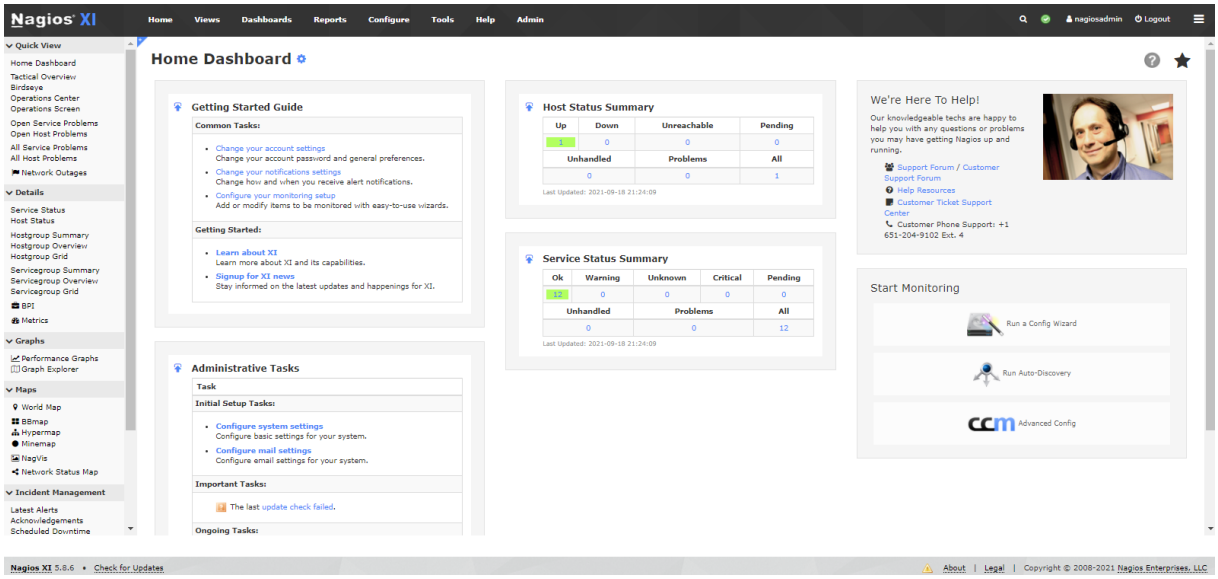

Figure C.8 : Tableau de Bord de Nagios XI

[1] :https://www.ionos.fr/digitalguide/serveur/know-how/reseau-informatique-definition/ , site consulté le 20 mai 2021

[2] :https://ciscoblog.fr/index.php/2020/12/02/quest-ce-quun-reseau-informatique/ , site consulté le 20 mai 2021

[3] :https://www.digital-marketing-66.fr/quel-est-le-role-de-la-supervision-dun-reseau-informatique/ , site consulté le 21 mai 2021

[4] :http://igm.univ-mlv.fr/~dr/XPOSE2010/supervision/#:~:text=La%20mise%20en%20place%20d,Eviter%20les%20arr%C3%AAts%20de%20service , site consulté le 21 mai 2021

[5] :https://www.centresurmescompetences.com/show.php?id=308/role_et_responsabilite_du_superviseur , site consulté le 21 mai 2021

[6] :https://supervision-informatique.solutions/avantage-interet-supervision/ , site consulté le 21 mai 2021

[7] :http://www-igm.univ-mlv.fr/~dr/XPOSE2007/dmichau_supervision/supervision.html , site consulté le 25 mai 2021

[8] :https://supervision-clever.fr/monitoring-protocoles-reseaux/ , site consulté le 25 mai 2021

[9] :https://wooster.checkmy.ws/2014/05/monitoring-interne-externe-actif-passif/#:~:text=Monitoring%20actif,r%C3%A9guliers%20les%20composants%20%C3%A0%20surveiller.&text=Il%20existe%20pl%C3%A9thore%20d'outils,%2C%20Shinken%2C%20Icinga%20et%20Zabbix. , site consulté le 30 mai 2021

[10] :https://www.commentcamarche.net/contents/537-le-protocole-snmp , site consulté le 30 mai 2021

[11] https://www.techno-science.net/definition/1465.html, site consulté le 02 juin 2021

[12] https://www.frameip.com/snmp/ ,site consulté le 02 juin 2021

[13] https://philpetitpa.pagesperso orange.fr/adminsupervis/SNMP.pdf, site consulté le 03 juin 2021

[14] http://igm.univ-mlv.fr/~dr/XPOSE2013/administration_reseau_SNMP_LDAP/architecture.html , site consulté le 05 juin 2021

[15] https://www.appvizer.fr/magazine/services-informatiques/supervision-reseau/monitoring-reseau-4-outils-pour-detecter-les-anomalies , site consulté le 06 juin 2021

[16] https://www.virtualhostedpbx.net/what-is-prtg/ ,site consulté le 08 juin 2021

[17] https://www.paessler.com/fr/prtg/features , site consulté le 10 juin 2021

[18] https://www.monreseau-it.fr/produit/reseaux/cris-reseaux-supervision-reseau-prtgpaessler-1095850.htm ,site consulté le 11 juin 2021

[19] https://docplayer.fr/1715139-10-problemes-de-reseau-courants-que-prtg-network-monitor-vous-aide-a-resoudre.html ,site consulté le 11 juin 2021

[20] https://www.zdnet.fr/guide-achat/les-meilleurs-outils-de-surveillance-reseaux-en-2020-atera-connectwise-automate-datadog-et-autres-39908617.html ,site consulté le 15 juin 2021

[21] https://open-source-guide.com/Solutions/Infrastructure/Supervision-et-la-metrologie/Cacti ,site consulté le 02 juillet 2021

[22] https://www.cacti.net/info/cacti ,site consulté le 02 juillet 2021

[23] Anis MAJDOUB, Nagios La clé de la supervision informatique, ENI ,14 septembre 2016

[24] https://assets.nagios.com/handouts/nagiosxi/Nagios-XI-How-It-Works.pdf ,site consulté le 05 juillet 2021

[25] https://www.nagios.com/products/nagios-xi/ ,site consulté le 05 juillet 2021

[26] https://www.capterra.fr/reviews/152793/nagios-fusion ,site consulté le 07 juillet 2021

[27] http://network-informatique.blogspot.com/2013/02/gns3-installation.html ,site consulté le 02 septembre 2021

[28] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203415-vlan-virtual-local-area-network-definition-traduction/, site consulté le 02 septembre 2021

[29] https://techlib.fr/definition/ssh.html , site consulté le 03 septembre 2021

[30] https://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol, site consulté le 05 septembre 2021

[31] https://waytolearnx.com/2018/07/difference-entre-routage-statique-et-dynamique.html ,site consulté le 08 septembre 2021

[32] https://www.memoireonline.com/12/13/8126/m_Mise-sur-pied-d-une-solution-de-supervision-reseaux9.html, site consulté le 08 septembre 2021

[33] -https://slideplayer.fr/slide/4807521/, site consulté le 08 septembre 2021

[34] *https://www.projet-plume.org/fiche/cacti* , site consulté le 08 septembre 2021

[35] *https://djibril.developpez.com/tutoriels/perl/ecrire-facilement-plugin-nagios-perl/* , site consulté le 10 septembre 2021