

REPUBLIQUE DU SENEGAL



UN PEUPLE-UN BUT-UNE FOI

Ministère de l'Enseignement Supérieur, de la Recherche et de l'innovation

**Direction Générale de l'Enseignement Supérieur**

**Direction de l'Enseignement Supérieur Privé**

**Ecole Supérieure de Technologie et de Management**



MEMOIRE DE FIN DE CYCLE

Pour l'obtention de la licence en TELEINFORMATIQUE

Option : Télécommunications et réseaux

INTITULE

**ETUDE ET MISE EN PLACE D'UN SYSTEME DE SUPERVISION  
DES EQUIPEMENTS INFORMATIQUES AU SEIN D'UNE  
ENTREPRISE.**

Présenté et soutenu par :

M. Madou SALL

Sous la direction de :

Dr. Sosthène Cyr Rufin YAMALE

**Année académique :2019-2020**

## IN MEMORIUM

A la mémoire de tous ceux qui ont contribué à mon éducation et à ma formation mais qui ne sont plus là malheureusement :

- A ma cousine KHADY NDAO.
- Mon Papa El hadji Ousmane Sall.

Paix à leur âme et que Dieu les accueille dans son paradis céleste éternel.

## DEDICACES

### **A MA TRES CHERE MERE Banna SALL :**

Autant de phrases aussi expressives soient-elles ne sauraient montrer le degré d'amour et d'affection que j'éprouve pour vous. Vous m'avez comblé avec la tendresse et d'affection tout le long de mon parcours. Vous n'avez cessé de me soutenir et m'encourager durant toutes les années de mes études, vous avez été présent à mes cotes pour me consoler quand il fallait. En ce mémorable jour pour moi ainsi que pour vous, reçoit ce travail en signe de ma vive reconnaissance et ma profonde estime. Puis Dieu vous accorder la santé, le bonheur et une longue vie afin que nous puissions un jour combler de joie vos vieux jours.

### **A MON TRES CHER PAPA Boubouring SALL:**

Autant d'expressions ne sauraient montrer le degré d'amour et d'affection que j'éprouve pour vous.

### **A MON TRES CHER PAPA MON HOMONYME Madou SALL**

Qui a beaucoup contribuer et qui a financé la presque totalité de mes études

## REMERCIEMENTS

Après avoir rendu grâce à Dieu et prié au nom du prophète Mohamed (PSL), nous tenons à remercier

Tous ceux qui ont participé à l'élaboration de ce mémoire :

A mon ami, mon papa, mon homonyme pour son encouragement, ses conseils, son soutien affectif et financier ;

A mon directeur de recherche Dr. Sosthène Cyr Rufin YAMALE pour sa disponibilité et ses conseils en m'offrant avec patience et dévouement une aide constante ;

A tout le corps professoral de l'ESTM.

Nous exprimons notre gratitude à tous les amis étudiants qui nous ont aidés de manière bénévole pour la réalisation de ce travail.

Je tiens également à remercier tous ceux qui ont de près ou de loin contribué à ma réussite.

## AVANT PROPOS

L'ESTM (Ecole Supérieure de Technologie et de Management) est une école d'ingénieurs et de management privée créée en 2001. ESTM a pour but de former les techniciens supérieurs et des ingénieurs dans les domaines des télécommunications, des téléinformatiques et de gestions. Elle est une école « haut de gamme » où la qualité de l'enseignement repose sur des effectifs à taille humaine, une pédagogie active, des ressources humaines, compétences et une équipe pédagogique de très grande qualité. La formation se basant aussi bien sur des cours théoriques et sur des travaux pratiques pour une très bonne compréhension pour la réalisation des projets.

L'école, dans son projet initial, a défini un large éventail de filières en rapport avec les besoins de la société afin de proposer une offre de formation de qualité. Elle s'est positionnée dès sa création dans le domaine des STEM, qui vient d'être érigé en priorité par le gouvernement du Sénégal à la suite des conclusions de la concertation Nationale sur l'Enseignement Supérieure. Après une étude d'opportunités et en fonction des ressources de l'institution, l'ESTM a effectivement lancé les filières : Téléinformatique, Télécommunications, Gestion énergies renouvelables, Génie logiciel et Multimédia. La mise en place des filières est décidée par les instances habilitées de l'ESTM notamment le conseil d'orientation scientifique, dans lequel sont représentés les acteurs du monde professionnel.

En effet, dans sa préoccupation de formateur de futurs cadres, dans le souci de nous préparer à d'éventuelles situations dans notre carrière informatique, et de nous permettre d'acquérir de nouvelles connaissances dans le domaine de la télécommunication, à la fin de chaque cycle un mémoire ou rapport doit être présenté et défendu devant un jury. C'est dans cet optique que nous avons élaboré ce mémoire qui s'intitule : « **ETUDE ET MISE EN PLACE D'UN SYSTEME DE SUPERVISION DES EQUIPEMENTS INFORMATIQUES AU SEIN D'UNE ENTREPRISE** ».

Ce document représente notre premier travail de recherche. En effet, nous tenons à remercier les membres du jury qui ont bien voulu accepter l'évaluation de ce travail et nous sollicitons aussi beaucoup d'indulgence de leur part quant à l'évaluation.

# SOMMAIRE

INTRODUCTION GENERALE.....	15
PARTIE I: CADRE METHODOLOGIQUE ET THEORIQUE.....	Erreur ! Signet non défini.
CHAPITRE I : CADRE METHODOLOGIQUE ET THEORIQUE .....	17
1.1. PRESENTATION DE L'ESTM .....	17
1.2. CONTEXT DU SUJET .....	21
1.3. OBJECTIFS DU TRAVAIL.....	21
1.4. LA METHODOLOGIE DU TRAVAIL .....	22
1.5. PERTINENCE DU SUJET ET DELIMITATION DU CHAMP DE RECHERCHE .....	22
1.6. DELIMITATION DU CHAMP D'ETUDE.....	22
1.7. CRITIQUE DE L'EXISTANT .....	22
1.8. SOLUTION PROPOSEE .....	23
CHAPITRE II : PRESENTATION DE RESEAUX INFORMATIQUES .....	24
2.1. GENERALITE SUR LES RESEAUX .....	24
2.2. CATEGORIES DES RESEAUX .....	24
PARTIE II : GENERALITES SUR LA SUPERVISION.....	Erreur ! Signet non défini.
CHAPITRE I : PRESENTATION DE LA SUPERVISION RESEAU .....	44
1.1. PRINCIPE DE FONCTIONNEMENT DE LA SUPERVISION.....	44
1.2. LES PROTOCOLES DE SUPERVISION.....	45
1.3. LES OUTILS DE SUPERVISIONS .....	48
1.4. ETUDE COMPARATIVE DES OUTILS DE SUPERVISION .....	50
1.5. SOLUTION RETENUE .....	51
PARTIE III : PRESENTATION DE LA SOLUTION RETENUE.....	Erreur ! Signet non défini.
CHAPITRE I : PRESENTATION DE LA SOLUTION RETENUE .....	53
1.1. PRESENTATION DE NAGIOS.....	53
1.2. LE FONCTIONNEMENT DE NAGIOS .....	53
1.3. ARCHITECTURE DE LA SOLUTION.....	53
1.4. LES FONCTIONNALITES DE NAGIOS .....	55
1.5. LES PLUGINS .....	55
1.6. LES FICHIERS DE CONFIGURATION.....	58
CHAPITRE II : MISE EN ŒUVRE DE NAGIOS .....	59
2.1. Environnement de travail.....	59
2.2. Mise en place de la solution.....	59
CONCLUSION GENERALE .....	74

WEBOGRAPHIE .....	75
TABLE DES MATIERES.....	76

## LISTE DES FIGURES

Figure 1:Organigramme de l'ESTM.....	19
Figure 2:Architecture réseau de l'ESTM.....	20
Figure 2 : Figure 3:Réseau LAN : .....	25
Figure 4:MAN.....	25
Figure 5:Réseau MAN .....	26
Figure 6:FHSS.....	29
Figure 7:DSSS.....	30
Figure 8:OFDM .....	30
Figure 9:MIMO .....	31
Figure 10:Infrarouge.....	32
Figure 11:Réseau WIFI en mode Adhoc .....	32
Figure 12:Réseau Wi-Fi en mode infrastructure .....	33
Figure 13:Topologie en bus .....	34
Figure 14:Topologie en anneau .....	35
Figure 15:Topologie en étoile.....	36
Figure 16:Topologie hiérarchique .....	37
Figure 17:Topologie arborescente .....	38
Figure 18:Topologie maillée .....	38
Figure 19:modèle OSI .....	40
Figure 20:modèle TCP/IP .....	42
Figure 21:Structure OID.....	47
Figure 22:traps SNMP.....	48
Figure 23:Architecture de Nagios.....	54
Figure 24:Fonctionnalité de Nagios.....	55
Figure 25:Les plugins de Nagios .....	56
Figure 26:Installation de Nagios.....	60
Figure 27:Creation des utilisateurs .....	60



Figure 28: Téléchargement de Nagios.....	60
Figure 29:le contenu de Nagios.....	61
Figure 30:Installation de Nagios Core .....	61
Figure 31:Installation de l'interface web de Nagios Core .....	61
Figure 32:Creation d'un acces administrateur .....	62
Figure 33:le nom d'utilisateur et le mot de passe.....	63
Figure 34:saisir le nom d'utilisateur et le mot de passe.....	63
Figure 35:Interface de Nagios Core.....	64
Figure 36:Installation des plugins de Nagios .....	64
Figure 37:Installation des plugins de Nagios1.....	64
Figure 38:Installation de NSclirnt .....	65
Figure 39:Installation de NSclirnt1 .....	66
Figure 40:Installation NSClient2 .....	66
Figure 41:Installation de NSClient3 .....	67
Figure 42:Installation de NSClient4 .....	67
Figure 43:Le fichier NSClient.....	68
Figure 44:Redemarage des services .....	69
Figure 45:L'etat du serveur Nagios et du serveur Windows en mode Up .....	71
Figure 46:Les status du service de serveur Nagios.....	72
Figure 47:L'interface Map de Nagios.....	73

## LISTE DES TABLEAUX

Tableau 1: Les normes de wifi .....	28
-------------------------------------	----

## GLOSSAIRE

**BSSID** : Basic Service Set Identifier.

**CAMES** : Comités Africaine et Malagas pour l'Enseignement Supérieure.

**CGI**: Common Gateway Interface.

**DSSS**: Direct Sequence Spread Spectrum.

**FHSS**: Frequency Hopping Spread Spectrum.

**IP**: Internet Protocol.

**LAN**: Local Area Network

**ICMP**: Internet Control Message Protocol.

**MAU**: Medium Access Unit.

**MIMO**: Multiple-Input Multiple-Output.

**MIB**: Management Information Base.

**OFDM**: Orthogonal Frequency-Division Multiplexing.

**OID**: Object Identifier.

**SISO**: Single-Input Single-Output.

**SNMP** : Simple Network Management Protocol.

**TCP** : Transmission Control Protocol.

**VDI** : Voix-Données-Informatique.

**VPN**: Virtual Private Network.

**WLAN**: Wireless Local Area Network.

## RESUME

L'objectif de ce mémoire est la mise en place d'un outil de supervision système et réseau au sein d'une entreprise.

En effet, aujourd'hui la taille des réseaux ne cessant de grandir de jour en jour et l'importance des réseaux dans le monde de l'entreprise prenant une place importante, le besoin de contrôler en temps réel leur qualité et leur état est rapidement devenu une priorité. C'est dans ce but qu'est apparu, le concept de supervision de réseaux.

L'étude comparative effectuée dans ce travail nous a permis de choisir la solution Open Source adaptée pour notre Structure qui est Nagios. L'installation et le déploiement de la solution nous a permis de mettre en place une solution de supervision système et réseau qui va permettre à l'administrateur de l'entreprise de mieux superviser les équipements et les services de son réseau.



## ABSTRACT

The objective of this thesis is the implementation of a system and network monitoring tool within a company. Indeed , today the size of networks continues to grow day by day and the importance of networks in the business world taking an important place, the need to control in real time their quality and their state is quickly become a priority. It is for this purpose that the concept of network supervision arose. The comparative study carried out in this work allowed us to choose the Open Source solution suitable for our Structure which is Nagios. The installation and deployment of the solution allowed us to set up a system and network monitoring solution that will allow the company administrator to better supervise the equipment and services of his network.

# INTRODUCTION GENERALE

Avec la naissance des nouvelles technologies, l'informatique s'est imposée plus que jamais comme un outil incontournable dont toute entreprise a besoin. Ainsi, au niveau des entreprises, un des rôles des administrateurs est de gérer les systèmes d'information qui sont tous différents par leur taille et leur nature.

En effet, toutes les entreprises sont équipées d'un réseau local. Les administrateurs ont un objectif clair qui est de maintenir la production du système d'information. Leurs parcs informatiques englobent plusieurs terminaux. Cependant, tous ces éléments peuvent ne pas être dans le même réseau.

Afin de minimiser la perte dans l'exploitation et les anomalies de fonctionnement qui provoquent des conséquences variables en degrés pour le fonctionnement au niveau du système d'entreprise, l'outil de supervision peut ainsi mettre des priorités sur les interventions des administrateurs et leur permettre de se concentrer sur l'essentiel.

Vu que le système informatique est au cœur des activités de l'entreprise, il est nécessaire d'améliorer le fonctionnement de son réseau en se dotant d'une solution de surveillance pour garantir la fiabilité et l'efficacité d'une part et d'autre part les défaillances, les pannes, les coupures et les différents problèmes techniques.

C'est pourquoi les administrateurs réseaux et systèmes font appels à des logiciels de supervision réseaux pour vérifier l'état de cette dernière en temps réel et s'informer au plutôt de tous incidents réseaux par différents moyens.

Notre document s'articulera autour de trois parties. Dans la première partie qui comprend deux chapitres, nous allons faire une présentation du Cadre Méthodologique et Théorique. La deuxième partie comprend aussi deux chapitres : Etude détaillée du système informatique et Généralité sur la supervision. Et enfin, une troisième partie comprenant deux chapitres : Etude de la technologie choisie et Implémentation. Et nous terminerons par une conclusion.



## PARTIE I: CADRE METHODOLOGIQUE ET THEORIQUE



# CHAPITRE I : CADRE METHODOLOGIQUE ET THEORIQUE

## 1.1 PRESENTATION DE L'ESTM

### 1.1.1 HISTORIQUE

ESTM (Ecole Supérieure de Technologie et de Management) de Dakar, est une école privée d'enseignement supérieur, universitaire et professionnel. Elle a été créée en 2001 par les professionnels des secteurs des technologies de l'information, de la communication et de la gestion.

Les enseignements dispensés s'inspirent des normes exigées par le CAMES (Comité Africain et Malagas pour l'enseignement Supérieur) et sont donc superposables à ceux dispensés dans des meilleures écoles tant sur le continent africain que sur le reste du monde.

L'école compte toujours rester à la pointe de la technologie dans un environnement qui se veut compétitif. Ses principaux atouts résident dans : le conseil pédagogique, la qualité des enseignements et dans la rigueur. Ce conseil pédagogique consultatif élabore programmes qui sont constamment mise à jour, dans l'optique de les adapter à la réalité toujours suivant les besoins de l'entreprise. C'est ce qui lui a d'ailleurs donné la pleine reconnaissance de ses diplômes par le CAMES.

### 1.1.2 FORMATIONS

Le programme de l'ESTM est élaboré en fonction des besoins du monde professionnel et adapté à l'évolution de la technologie de manière à donner à l'étudiant des compétences aussi bien théorique que pratiques.

Pour la licence à l'issue du cycle de formation, les étudiants sont titulaires d'un diplôme de licence en Télécom et Réseau, avec les spécialités suivantes :

- Télécommunication et réseaux
- Réseau sans fils et sécurité
- Electronique des télécommunications

Ce diplôme leur permet d'exercer entre autres les fonctions suivantes : Administrateur système et réseaux, Assistant en planification des réseaux fixes et mobiles, Responsable de l'administration, de la sécurité et de la qualité de services dans les réseaux, Architecte réseaux, Développeur d'applications client/serveur.

Pour le master à l'issue du cycle de formation, les étudiants titulaires d'un diplôme de Licence en Télécom et Réseau, avec une spécialisation en Electronique des Télécoms.

Ce diplôme les permet d'exercer entre autres les fonctions suivantes :

- Ingénieur Conseil,
- Ingénieur Support et Développement,
- Chef de Projet,
- Chargé d'Etudes et de Conception,

- Directeur Technique

L'ESTM a pour vocation de former des cadres compétents dans les domaines des téléinformatiques, des télécommunications et de la gestion, les enseignements dispensés sont comparables à ceux dispensés dans les meilleures écoles et sont faites par des universitaires et des professionnels des secteurs concernés. En parallèle l'école propose des stages aux seins même de ses locaux à certains étudiants dans le but de développer leur capacité à travailler dans des situations d'autonomie, de conduire des projets et d'exploiter des équipements dans le domaine des réseaux informatiques et télécommunications.

Pour l'obtention de la licence en télécommunications et réseaux, l'ESTM exige de ses étudiants la rédaction d'un mémoire de fin de cycle.

### **1.1.3 MISSION**

L'ESTM assure des formations dans deux départements qui la composent. Ces formations sont en cours du jour, comme en cours du soir, aussi bien en formation initiale qu'en formation continue pour le compte des entreprises, sociétés et particuliers.

Ces départements sont :

- Le Département de l'informatique et des télécommunications ;
- Le Département de science de la gestion ;  
L'accès aux formations peut se faire sur :
  - Dossier pour la formation initiale ;
  - Contrat dans le cadre des formations continue.

L'école vise à ce que les étudiants, sortant de ses cycles de formation, soient capables de participer à la conception, la réalisation et la mise en œuvre des systèmes correspondant au besoin des utilisateurs. Ainsi l'école forme des techniciens supérieurs en informatique de gestion, maintenance informatique, réseaux télécommunications, réseaux informatiques en trois ans et des licences professionnelles en réseaux et génie logiciel, en réseaux télécommunication, en réseaux téléinformatique.

Le second cycle des ingénieurs technologues en : réseaux et télécommunications réseaux téléinformatique, génie logiciel et système de gestion de base des données dans son département des sciences de l'informatique et télécommunication, des diplômes de premier cycle en Marketing, Comptabilité, Tourisme et Gestion.

### 1.1.4 ORGANIGRAMME

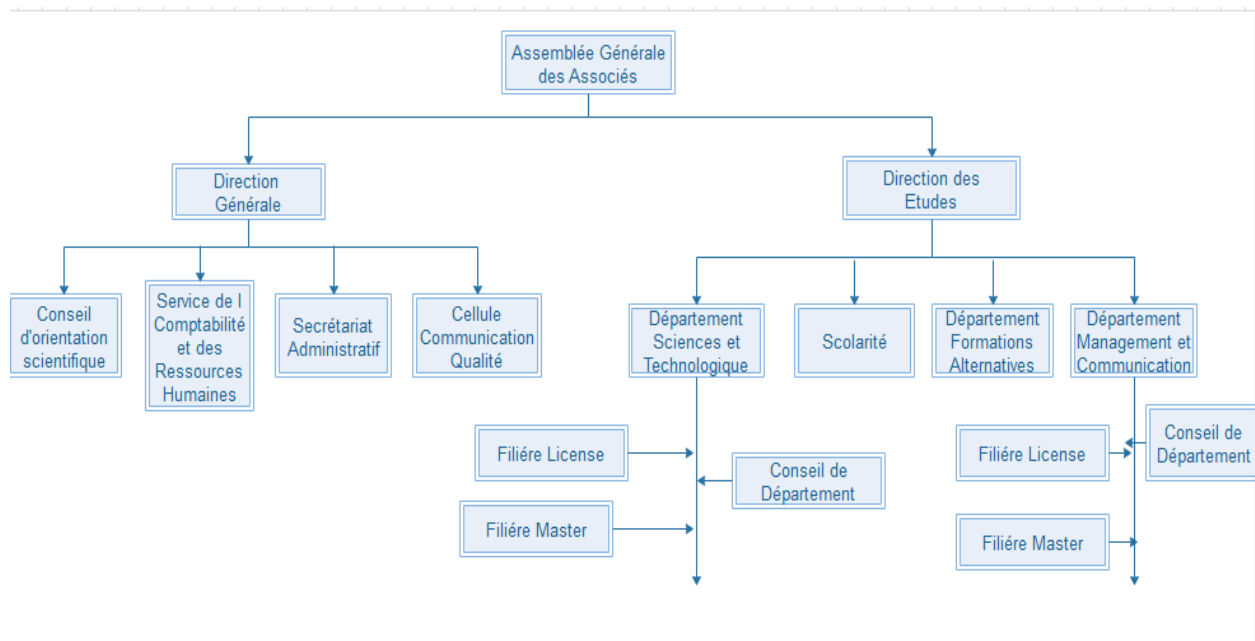


Figure 1: Organigramme de l'ESTM

### 1.1.5 Présentation de Réseaux Informatique de l'ESTM.

Le réseau de l'ESTM est composé d'une infrastructure réseaux et du cloud.

- La partie réseau est composée du réseau IP et du réseau téléphonique.
- Pour le cloud, les différents serveurs sont hébergés sur Internet pour assurer un accès permanent aux applications métiers (gestion pédagogiques) et au services (mailing, drive, tchat etc.)
- Le câblage est conventionnel en VDI (Voix-Données-Informatique) sur du câble UTP 6 E
- Le réseau d'accès est essentiellement constitué de liaison WIFI avec une couverture globale.
- Au niveau distribution, une combinaison de Routeur Switch (Physique et Applicatif) nous permet d'assurer la stabilité et la sécurité du réseaux. Il existe une organisation en VLAN qui segmente le réseau des étudiants de celui du personnel administratif et enseignant.

Les deux sites (2) sont reliés via une connexion VPN (Virtual Privat Network) permettant de créer un lien direct entre eux.

Au niveau de chaque site nous avons :

- Un XEN-Server pour virtualiser le serveur DNS, le serveur de fichier, le serveur de messenger, le serveur de portail captif et le serveur DHCP ;

- Un stock des serveurs virtuels primaire au niveau de l'ESTM Cheikh Anta et un stockage des serveurs virtuels secondaire au niveau de l'ESTM Bourguiba ;
- Une subdivision du réseau de l'ESTM en 4 (quatre) sous réseaux tel que : le réseau « management », le réseau « personnel », le réseau « étudiant » et le réseau « visiteur » ;
- Le réseau comprend : un firewall, des points d'accès sans fils, des commutateurs, des routes d'accès à l'intérieur, des salles informatiques, des étudiants et des invités ;
- Les utilisateurs ont un accès filaire et sans fil au réseau interne leurs permettant d'utiliser le réseau ;
- Une disposition de switch qui est directement connecté au XEN-Server.

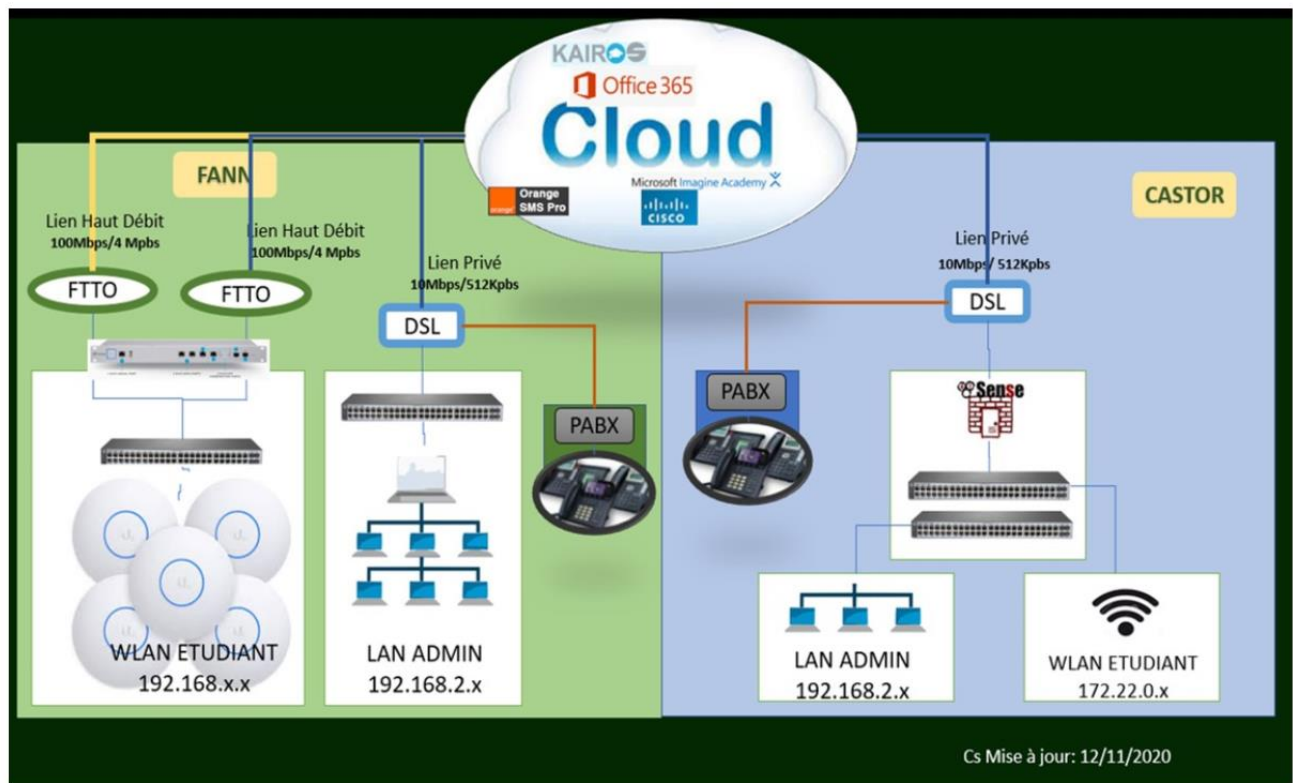


Figure 2:Architecture réseau de l'ESTM

## **1.2. CONTEXT DU SUJET**

Toute application de supervision réseau est destinée avant tout à simplifier la tâche de l'administrateur qui est tenu d'intervenir en cas de panne. Celle que nous devons mettre en place doit assurer aussi cette mission. Elle se charge de détecter tout d'abord la faille, de la localiser, avec la possibilité d'envoyer un mail à l'administrateur ou bien au groupe d'utilisateur et ensuite d'essayer de la réparer afin d'assurer la continuité de fonctionnement du réseau dans les meilleures conditions de performance possibles. Cette solution doit permettre de localiser les nœuds administrés, d'envoyer les informations sur les équipements défectueux vers le nœud de supervision. Notre application de supervision doit offrir donc plus de simplicité d'utilisation, plus d'efficacité mais également être capable d'évoluer facilement et efficacement du rythme des besoins. A la fin de notre travail, nous devons pouvoir :

- Surveiller la disponibilité des équipements et Service.
- Surveiller la connexion Internet.
- Surveiller l'usage du CPU, de la RAM, du Disque Dur et/ou de quelques processus.
- Être alerter en cas de problème (CPU et/ou RAM sur utilisé, hôtes et/ou services inaccessible.....)
- Ressortir le comportement des ressources surveillées sur une période déterminée
- Ressortir une carte du réseau
- Tracer des graphes de performances

## **1.3. OBJECTIFS DU TRAVAIL**

L'objectif principal de notre travail repose sur la mise en place d'un système de supervision des équipements informatiques au sein d'une entreprise.

Nos objectifs spécifiques reposent précisément sur :

- Passer en revue la littérature sur le réseau informatique et sur la supervision réseau ;
- Faire une étude comparative des solutions existantes ;
- La mise en place de la solution retenue ;
- Présenter l'ensemble des services offerts par la solution.

## 1.4. LA METHODOLOGIE DU TRAVAIL

La méthodologie de travail est basée sur l'approche participative. La collecte des données s'effectuera à travers des interviews et réunions au près des administrateurs réseaux de l'ESTM et par le biais de l'internet et des revues documentaires.

Nous procéderons ensuite par une étude comparative des solutions existantes sur le marché, et nous choisirons la solution appropriée à nos attentes et puis nous procéderons à sa mise en œuvre et aux tests de configuration.

## 1.5. PERTINENCE DU SUJET ET DELIMITATION DU CHAMP DE RECHERCHE

Nagios nous permet de savoir quel système ou quel processeur doit être surveillé. Tout cela s'articule autour des quatre composants ou objets suivants :

- **Hôte** : en tant que hôte vous définissez les serveurs, bases de données et appareils, etc. Du réseau que vous souhaitez surveiller l'indicateur le plus important un hôte est l'adresse IP respective
- **Service** : Avec cet composant vous pouvez définir quelles caractéristiques de l'hôte Nagios doit vérifier. Cela peut aussi être les services en cours d'exécution sur l'hôte (http, FTP, etc), des attributs internes comme l'espace disque disponible mais aussi des caractéristiques physiques comme la température de votre matériel.
- **Commandes** : avec ce volet vous contrôlez la séquence de monitoring. Vous pouvez configurer la façon dont la surveillance des hôtes et des services doit être conçue et quand Nagios doit vous avertir quand un événement se produit.
- **Contacts** : avec la définition des contacts, Nagios peut alors envoyer des notifications à des contacts administratifs via un email, un message texte ou encore un message vocal

## 1.6. DELIMITATION DU CHAMP D'ETUDE

N'ayant pas eu la possibilité d'effectuer notre travail dans une entreprise, notre champ d'étude se limitera à l'ESTM. La mise en œuvre de la solution retenue se fera dans un environnement virtuel.

## 1.7. CRITIQUE DE L'EXISTANT

Nous avons constaté après l'analyse de l'existant du réseau de l'ESTM les points faibles suivants :

- Aucun outil de supervision système et réseau n'est en place au sein de l'ESTM
- Un taux important de temps est gaspillé lors du diagnostic des pannes ce qui influe sur la qualité du service et donc le bon fonctionnement.

- Plus le nombre des équipements et des services augmente plus les tâches de l'administrateur deviennent trop compliquées et il n'arrive pas à les assurer convenablement
- Vu l'absence d'un outil de supervision, l'administrateur n'est pas alerté en cas de problèmes de fonctionnements anormaux.

## **1.8. SOLUTION PROPOSEE**

La gestion et la supervision des serveurs et des équipements réseaux distants représentent un souci important pour l'administrateur. De ce fait, nous avons jugé nécessaire de mettre en place un outil pour contrôler le fonctionnement du réseau, d'étudier les données collectées et de définir les mécanismes déclenchant des alertes lors de détection des problèmes. Il s'agit donc et sans doute d'une mise en place d'un système de supervision qui pourra grâce aux différentes fonctionnalités qu'il offre, anticiper les pannes en suivant méticuleusement le fonctionnement du système et en surveillant le statut des serveurs, des divers services réseaux et d'offrir des renseignements supplémentaires voir la charge CPU, l'espace disque, la mémoire disponible, face aux pannes qui peuvent intervenir afin d'éviter un arrêt de production de trop longue durée.

# CHAPITRE II : PRESENTATION DE RESEAUX INFORMATIQUES

## 2.1. GENERALITE SUR LES RESEAUX

Un réseau en général, est le résultat de la convention de plusieurs équipements informatiques entre elles afin que les utilisateurs et les applications qui fonctionnent puissent échanger des informations.

Le terme réseau en plus de son contexte peut designer plusieurs choses. Il peut designer l'ensemble des machines ou infrastructures informatique une organisation avec les protocoles qui sont utilisées : réseau Ethernet, Token Ring, en étoile, en bus, anneau, etc. Il est défini comme un réseau destiné à relier des équipements informatique (serveurs, ordinateur imprimante, etc...) pour rendre possible l'échange de donnée binaires issus d'application ou processus informatiques tels que les traitements de textes, les bases de données, ou les navigateurs internet. Ils permettent aussi le partage de ressources informatiques (imprimantes, Disque durs, etc..).

## 2.2. CATEGORIES DES RESEAUX

On distingue plusieurs types de réseaux qui se différencient entre eux en fonction de la distance entre les systèmes informatiques ou encore en fonction de la technologie qui permet de les mettre œuvre.

### 2.2.1. LES RESEAUX LOCAUX (LAN)

Ce sont des réseaux de taille plus ou moins modestes, complexes, qui permettent l'échange de données informatiques et le partage de ressources (données, disques durs, périphériques divers, etc..). Ce type de catégorie regroupe les réseaux adaptés à la taille d'entreprise et dont les deux points les plus éloignés ne dépassent pas quelques kilomètres.



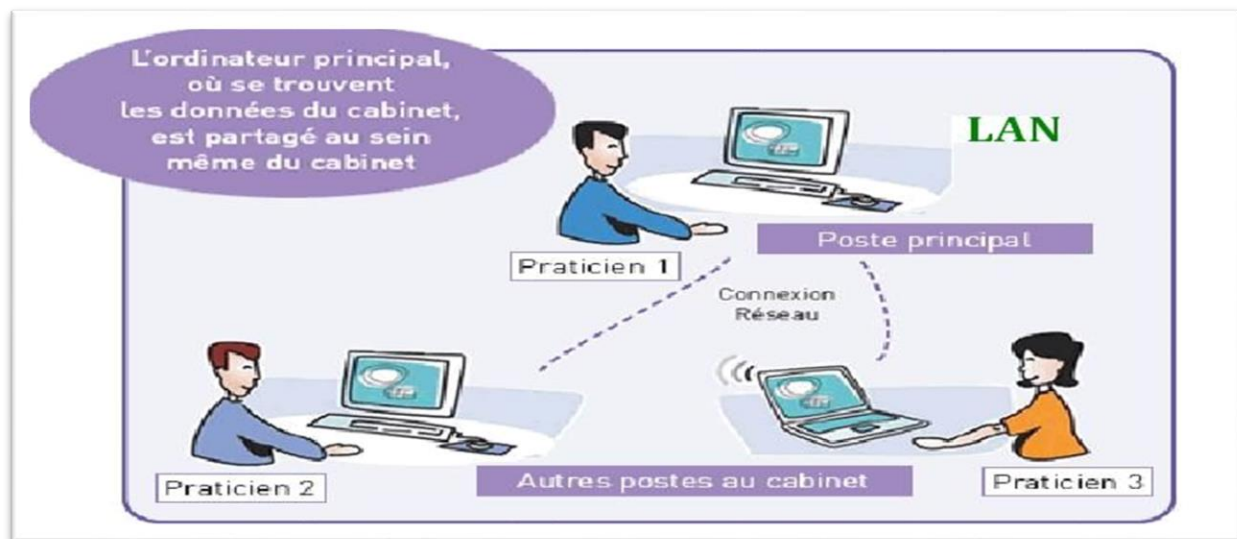


Figure 2 : Figure 3:Réseau LAN :

### 2.2.2. LES RESEAUX METROPOLITAINS (MAN).

Ils sont d'une étendue de l'ordre d'une centaine de kilomètres, les MAN sont généralement utilisés pour fédérer les réseaux locaux ou assurer la desserte informatique de circonscriptions géographiques importantes (réseau de campus). Ces réseaux peuvent être privés ou publics.



Figure 4:MAN

### 2.2.3. LES RESEAUX ETENDUS (WAN)

Appelés aussi réseaux longue distance ou réseaux étendus se situent à l'échelle nationale et internationale. Ces réseaux assurent généralement le transport d'information sur de grandes distances. Lorsque ces réseaux appartiennent à des opérateurs, les services sont offerts à des abonnés contre une redevance et la plupart de ces réseaux sont publics. Les débits offerts sont très variables, de quelques Kbits/s à quelques Mbit/s.

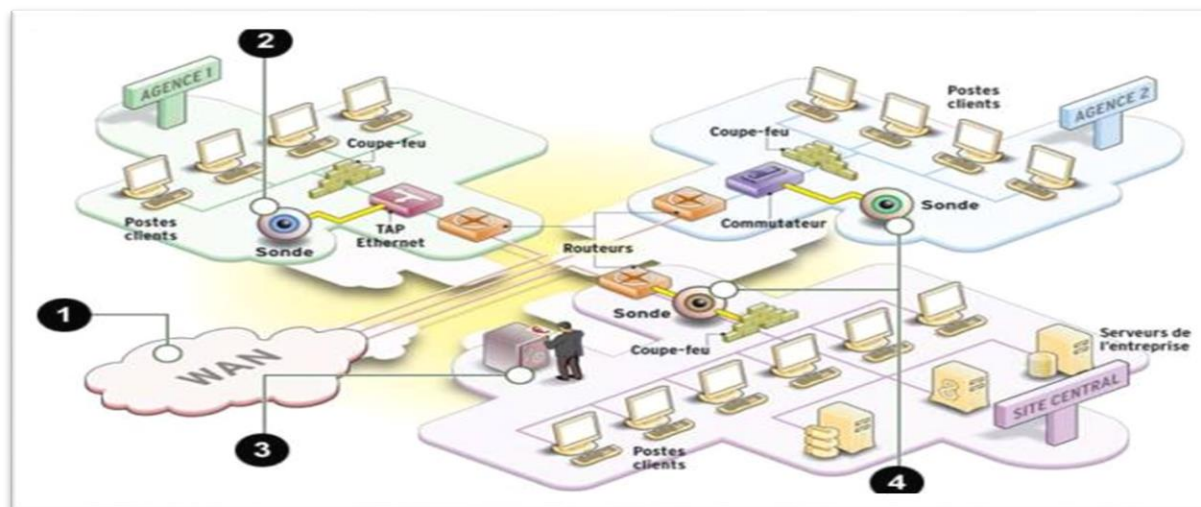


Figure 5:Réseau MAN

### 2.2.4. LES RESEAUX LOCAUX SANS FIL (Wireless, LAN ou WLAN)

#### 2.2.4.1.PRESENTATION

Ce sont des réseaux sans connexions physiques visibles. Ces réseaux utilisent les ondes (radios, infrarouge, etc.) comme support de communication. Les ordinateurs mobiles ou les assistants personnels (Palm pilot, etc....) constituent le secteur informatique en plus forte progression. Beaucoup de possesseurs de ce type d'ordinateurs ont également un ordinateur relié à des LAN ou des WAN, chez eux ou au bureau, auxquels ils sont reliés à tout instant.

Il permet de relier les terminaux présents dans la zone de couverture. Il existe plusieurs techniques concurrentes :

Le Wifi (ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

#### 2.2.4.2. LES NORMES ET LES BANDES DE FREQUENCES

IEEE 802.11 fait partie d'un ensemble de normes édictées sous l'égide du comité de standardisation IEEE 802 à partir de 1997. Celui-ci constitue un tout cohérent servant de base de travail aux constructeurs développant des équipements et les services chargés de l'implémentation des infrastructures réseaux à liaison filaire et sans fil.

Le schéma ci-dessous est une adaptation du synopsis du standard IEEE 802 consigné dans la section « introduction » dans la plupart des normes publiées sous ce standard.

Celui-ci est articulé autour de la norme IEEE 802.11 qui définit les spécifications relatives à l'implémentation de la couche **Physique** et de la sous-couche **MAC** (Couche liaison de données du modèle OSI) pour les réseaux locaux sans fil (WLAN) ;

Norme	Nom	Description
802.11a	Wi-Fi 5	Wi-Fi La norme 802.11a est la norme la plus répandue actuellement. Elle propose un débit théorique de 11Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2,4GHz, avec 3 canaux radio disponibles
802.11b	Wi-Fi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mb (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles
802.11c		La 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.11d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données)
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale Des réseaux locaux 802.11 Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de manière à

		permettre notamment une meilleure transmission de la voix et de la vidéo
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des valeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming Protocol permettant à un utilisateur itinérant de changer de point d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming en anglais)
802.11g		La norme 802.11g offrira un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2,4GHz. Cette norme n'a pas encore été validée, le matériel disponible avant la finalisation de la norme risque ainsi de devenir obsolète si celle-ci est modifiée ou amendée. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui se signifie que des matériels conformes à la norme 802.11g pourront fonctionner en 802.11b
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryptions Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g
802.11j		La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

Tableau 1: Les normes de wifi

Ensemble articulé autour de la norme IEEE 802.11 se décompose en éléments identifiés comme suit :

802 : standard général de base pour le déploiement de réseaux numériques locaux ou métropolitains à liaison filaire ou sans fil ;

802.1 : gestion des réseaux ;

802.10 : sécurisation des échanges pour les systèmes à liaison filaire ou sans fil (Token Ring, Ethernet, Wi-Fi, WiMax) ;

802.11 : spécification pour l'implémentation de réseau numérique locaux à liaison sans fil ;

802.2 : description générale de la sous-couche Logical Link Control.

### 2.2.4.3. LES TECHNIQUES DE TRANSMISSIONS

#### a) Le FHSS (Frequency Hopping Spread Spectrum)

Le FHSS est une technique qui utilise le saut de fréquence. Elle consiste à diviser la bande passante disponible en 79 sous-canaux de 1 Mhz de largeur de bande offrant, chacun un débit allant au moins 1MB/s avec codage binaire.

L'émetteur et le récepteur s'entendent sur une séquence de sauts de fréquence porteuse pour envoyer les données successivement sur les différents sous-canaux, ce qui sert à ne pas utiliser (temporairement) les sous-canaux fortement perturbés. La séquence de sauts est calculée pour minimiser la probabilité que deux émissions utilisent le même sous-canal.

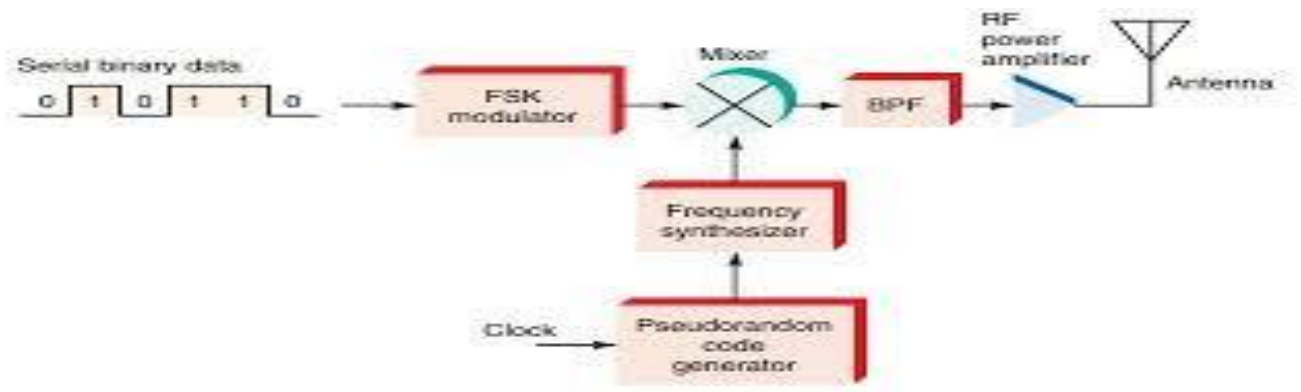


Figure 6: FHSS

#### b) LE DSSS

DSSS est la deuxième couche physique qui utilise une technique radio. Pour cela, la bande de fréquence est divisée en 14 sous-canaux de 22 Mhz. Ces canaux fournissent des signaux bruités

cette phénomène est dû au fait que les signaux adjacents ont des bandes passantes dont le recouvrement est partiel. Ils peuvent par conséquent se perturber mutuellement.

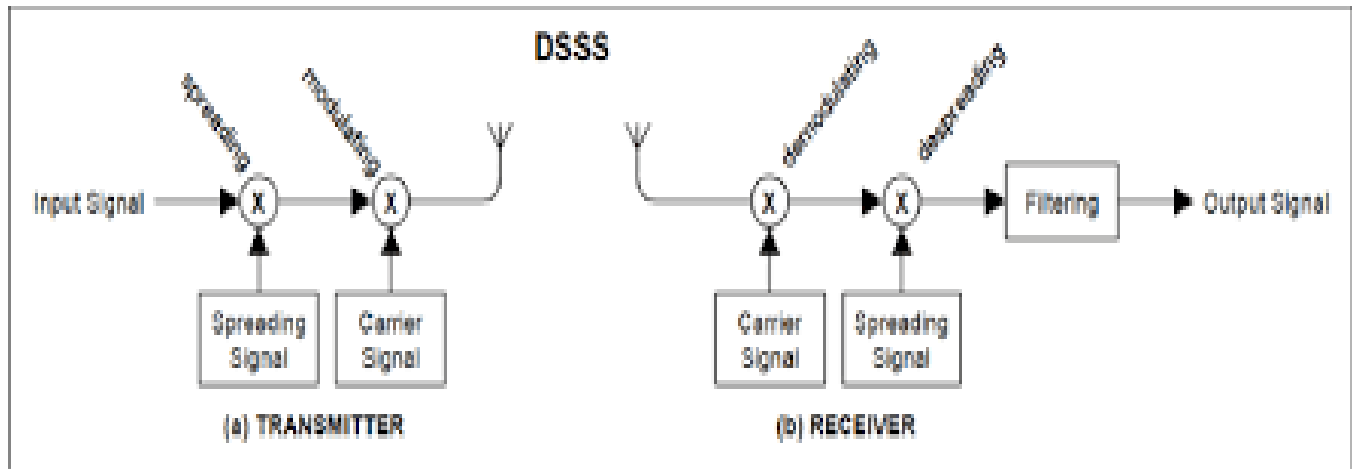


Figure 7:DSSS

### c) L'OFDM

Cette technique fait appel au multiplexage par la répartition des fréquences sur des porteuses orthogonales. Cette orthogonalité permet de séparer les canaux afin d'éviter les interférences du canal. Dans la technique OFDM, la bande de fréquence est divisée en porteuses. L'utilisation de ces porteuses peut être simultanée, en y multiplexant les données. Un canal se compose de 52 porteuses de 300 KHz de largeur. Le transport de l'information utilise 48 porteuses et la correction d'erreur utilise 4 porteuses appelées porteuses pilotes. L'OFDM supporte une série de modulation et de codages permettant d'offrir l'ensemble des débits. Dans la bande (de 5,15 à 5,35 GHz), huit canaux de 20 Mhz sont définis. Il est possible d'avoir une colocalisation de huit réseaux au sein du même espace et d'avoir un débit maximal de 432 Mbits/s

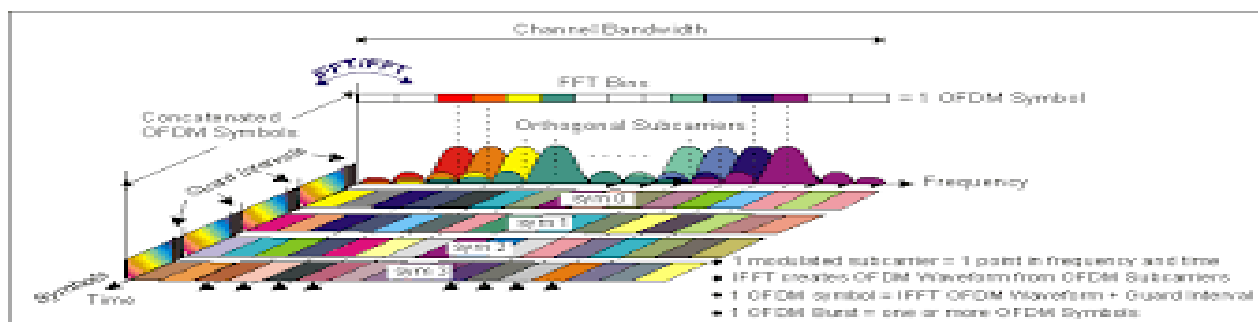


Figure 8:OFDM

#### d) LE MIMO

Multiple-Input Multiple-output ou MIMO (« entrées multiples, sorties multiples » en français) est une technique de multiplexage utilisée dans les réseaux mobiles permettant des transferts de données à plus longue portée et avec un débit plus élevé qu'avec des antennes utilisant la technique SISO (Single-input Single-output).

Alors que les anciens réseaux Wi-Fi ou les réseaux GSM standards utilisent une seule antenne au niveau de l'émetteur et du récepteur, MIMO utilise plusieurs antennes tant au niveau de l'émetteur (par exemple un routeur) que du récepteur (par exemple un PC portable ou un smartphone)



Figure 9:MIMO

#### e) L 'INFRAROUGE

Les infrarouges sont utilisés pour le transport des données. Cette méthode impose que les distances entre émetteurs/récepteurs soient limitées. Elle offre un débit de 1 Mbps.

Le support infrarouge fait partie de la norme IEEE 802.11. Il utilise une longueur d'onde de 850nm à 950nm pour le signal. Cette longueur d'onde est proche de la bande du visible par l'homme. C'est une lumière infrarouge diffusée.

Le seul inconvénient de ce support, est qu'il ne traverse aucun mur et difficilement une fenêtre. Son utilisation en extérieur n'est non plus à son avantage aussi, car, s'il n'y a aucune surface de réflexion, la portée est énormément réduite. Le signal reçu est assez faible. Donc, les LAN IEEE 802.11 utilisant un support physique à infrarouge se limitent à une pièce

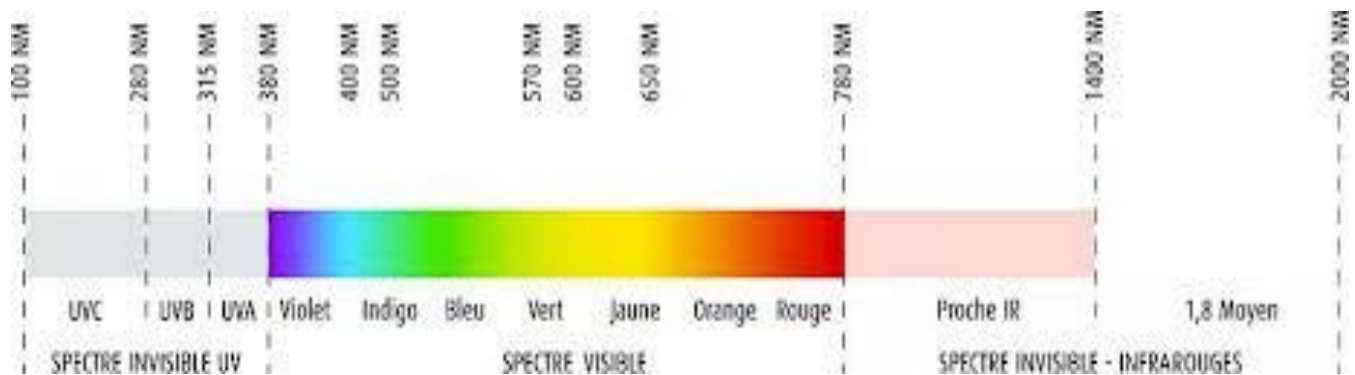


Figure 10: Infrarouge

## 2.2.4.4. FONCTIONNEMENT D'UN RESEAU Wi-Fi

### a) LE MODE ADHOC

En mode Adhoc les machines sans fil clientes se connectent les unes aux autres afin de constituer un réseau point à point, c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès comme illustré

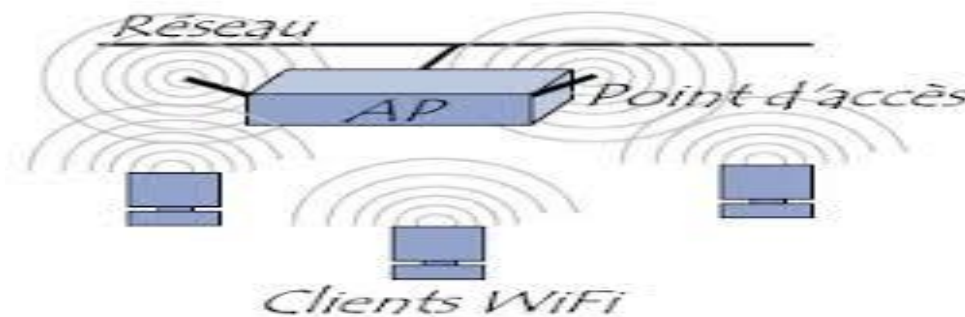


Figure 11: Réseau WIFI en mode Adhoc

L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (en anglais Indépendant Basic Service Set, abrégé en IBSS). Un IBSS est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un

SSID (Service Set Identifier), comme l'est un ESS en mode infrastructure. Dans un réseau Adhoc, la portée du BSS est déterminée par la portée de chaque station. Cela signifie que si deux des stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles voient d'autres stations. En effet, contrairement au mode infrastructure, le mode Ad hoc ne



propose pas de système de distribution capable de transmettre les trames d'une station à une. Ainsi un IBSS est par définition un réseau sans fil restreint.

### b) LE MODE INFRASTRUCTURE

En mode infrastructure les ordinateurs station se connectent en un point d'accès via une liaison sans fil. L'ensemble formé par une point d'accès les stations situées dans sa zone de couverture est appelés l'ensemble des services de base (BSS) et constitue une cellule. Chaque BSS est identifié par une BSSID (Basic Service Set Identifier), un identifiant de 6octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès.

Il est possible de relier plusieurs points d'accès entre eux (ou plusieurs BSS) par une liaison appelée système de distribution (noté DS pour Distribution System) afin de constituer un ensemble de service étendu (Extendeds Service Set ou ESS). Le système de distribution (DS) peut être aussi bien un réseau filaire : un câble entre deux points d'accès ou bien même un réseau sans fil.

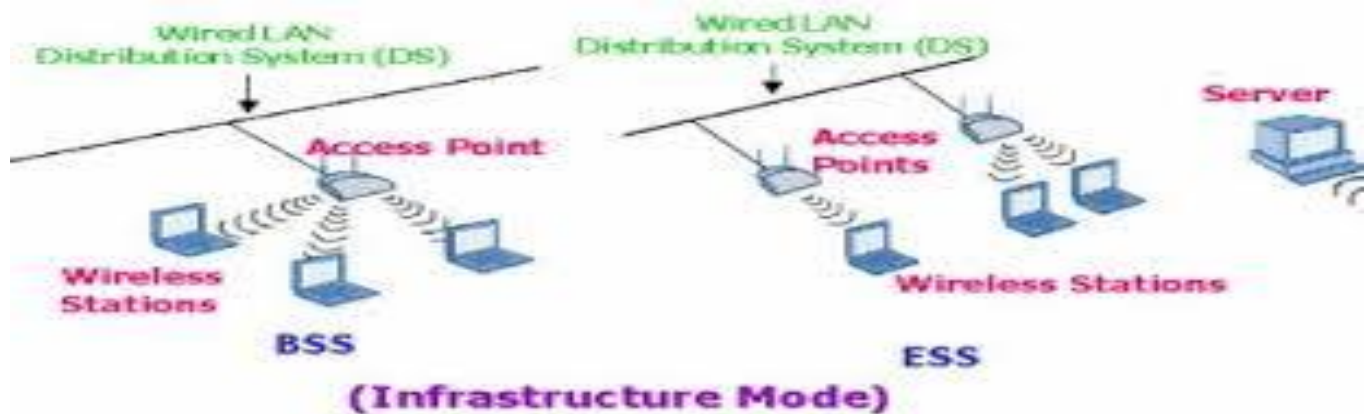


Figure 12: Réseau Wi-Fi en mode infrastructure

Lorsqu'un utilisateur nomade passe d'un BSS à une autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès.

Les points d'accès communiquent entre eux craque au système de distribution afin d'échanger des informations sur les stations et permettre dans le cas échéant de transmettre les données des stations mobiles. Cette caractéristique permet aux stations de « passer de façon transparente » d'un point d'accès à un autre est appelé itinérance (en anglais roaming).

Les cellules d'un réseau ESS peuvent être disjointes ou recouvertes. Le recouvrement permet d'avoir un réseau plus dense que dans le cas de cellules disjointes ceci offre à l'utilisateur une possibilité sans perte de connexion. Le recouvrement permet aussi de connecter un grand nombre d'utilisateurs puisqu'il permet d'augmenter l'étendue du réseau.

### 2.2.5. Les réseaux privés virtuels (VPN)

Les réseaux privés virtuels consistent en l'interconnexion de LAN à l'échelle nationale ou internationale. Ces réseaux restent privés et sont transparents pour l'utilisateur. Ils permettent en fait, par exemple pour une entreprise de s'affranchir de certaines, telles que la localisation géographique. Ils rendent possible une transmission plus sécurisée des données sur un réseau public, en particulier sur internet.

### 2.2.6. LES TOPOLOGIES DE RESEAUX

Il existe deux types de topologie :

- **La topologie logique** qui désigne le mode de circulation des données sur le média et donc le mode d'échange des messages sur le réseau.
- **La topologie physique** qui désigne le mode d'interconnexion physique des différents éléments du réseau.

**NB** : un réseau ayant une topologie physique en étoile peut très bien avoir une topologie logique en bus.

#### 2.2.6.1. LES TOPOLOGIES LOGIQUE

##### a) LA TOPOLOGIE EN BUS

Une topologie en bus désigne le fait que lors d'une émission de données sur le bus par une station de travail, l'ensemble des stations de travail connecté sur le bus la reçoivent. Seule la station de travail à qui le message est destiné la recopie.

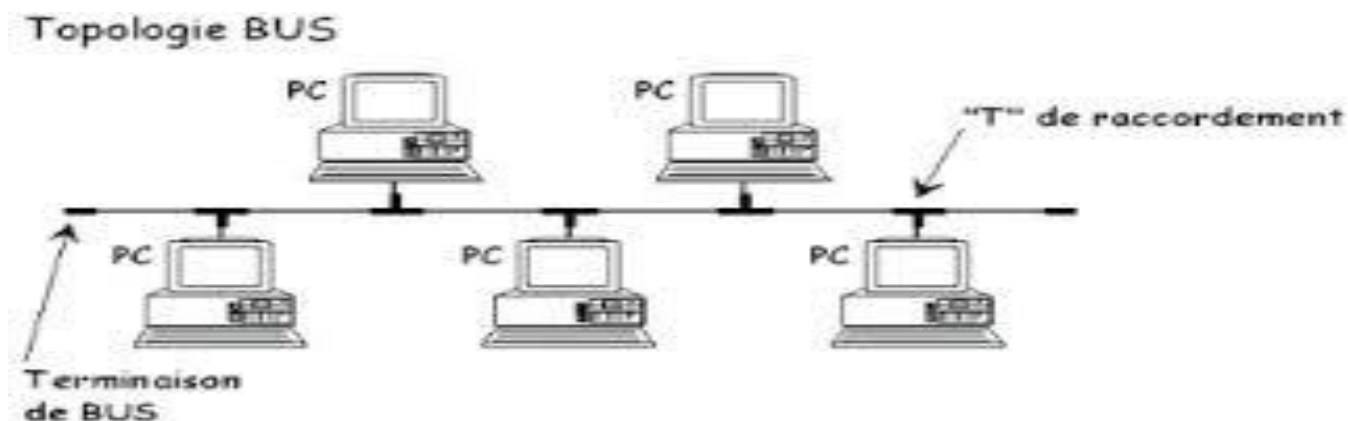


Figure 13: Topologie en bus

- **La topologie en bus unidirectionnelle**

C'est une topologie qui nécessite deux bus séparés, il en existe deux :

Les stations émettent et reçoivent dans un sens sur un des deux bus et dans l'autre sur le second bus

Les stations émettent et reçoivent les données sur les deux bus grâce à deux fréquences séparées, une par bus

- **La topologie en bus bidirectionnel**

L'émission et la réception se fait sur un bus unique, mais non simultanément. Lorsqu'une station émet le signal se propage dans les deux sens.

### b) LA TOPOLOGIE EN ANNEAU

L'information circule le long de l'anneau dans un seul sens. A chaque passage d'un message au niveau d'une station de travail, celle-ci regarde si le message lui est destiné, si c'est le cas elle le recopie.

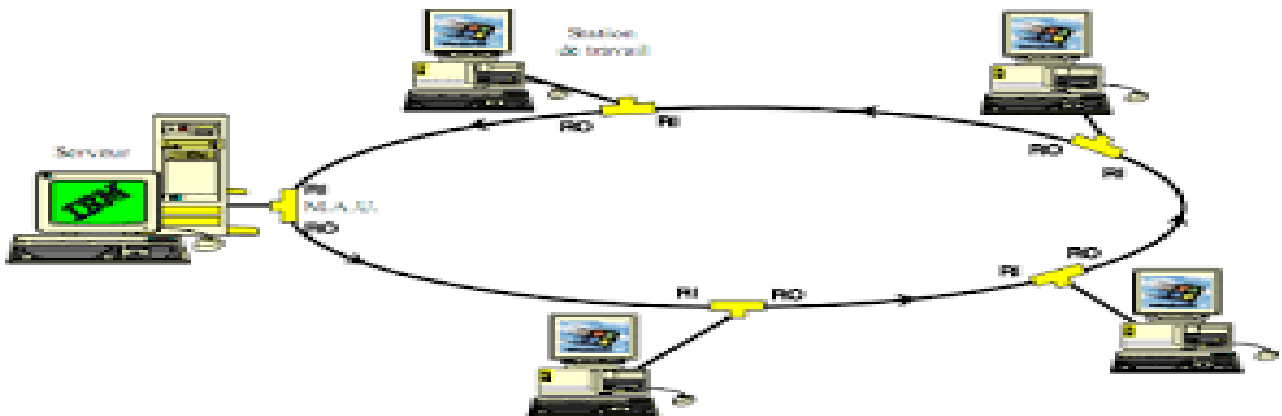
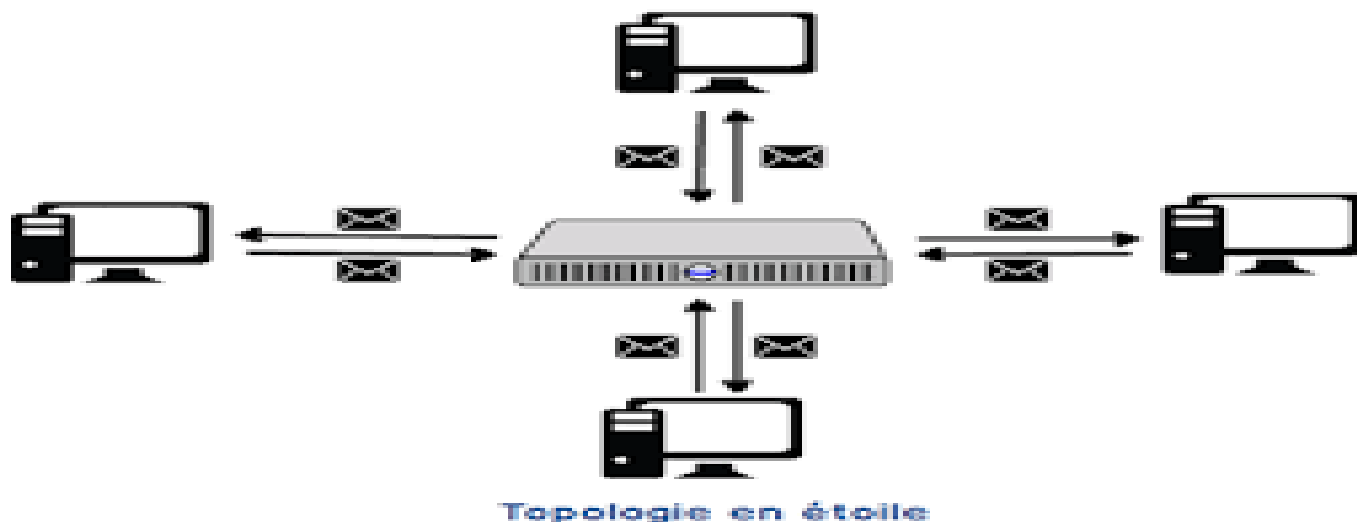


Figure 14:Topologie en anneau

### c) LA TOPOLOGIE EN ETOILE

L'ensemble des stations de travail est connecté à un concentrateur qui examine le contenu du message, qui le régénère et le transmet qu'à son destinataire. C'est en réalité un réseau de plusieurs liaisons point par point, car il établit un circuit entre deux utilisateurs.



*Figure 15:Topologie en étoile*

### 2.2.6.2. LA TOPOLOGIE PHYSIQUE

#### a) La liaison avec les stations

Afin de connecter les stations de travail entre elles et avec le serveur, il est nécessaire d'utiliser différents équipements qui les relient aux médias via un contrôleur de communication (une carte réseau).

#### b) Les nœuds

Ils désignent toutes les ressources constituant un carrefour de lignes de communication dans un réseau.

- **Les M.A.U (Medium Access Unit)**

C'est l'équipement de connexion concentrant plusieurs voies, huit généralement, dans un réseau local de type Token Ring. Ils s'agissent d'un équipement passif ne modifiant pas le signal, mais assurant une connexion en refermant automatiquement l'anneau lorsqu'une prise est enfoncée ou retirée.

- **Les transceiver (transmetteur)**

C'est un équipement diffusant une source de signaux vers plusieurs destinataires, et ceci de manière passive. Il est principalement utilisé dans les réseaux locaux Ethernet sous la forme d'un composant situé à l'interconnexion du câble desservant une station de câble coaxial matérialisant le bus.

#### c) La topologie en bus

La liaison des stations est effectuée à l'aide d'un câble coaxial qui est commun à l'ensemble des stations de travail. Les connexions des stations sur les câbles sont de types passifs. C'est-à-dire

que le signal n'est pas modifié ni régénéré à chaque station, ce qui limite l'étendu de ce genre de réseau. Par contre l'insertion d'une nouvelle station ne perturbe pas la communication au sein du réseau et peut donc être effectué sans l'arrêt de celui-ci.

#### d) La topologie en anneau

Chaque équipement est relié à l'équipement voisin de telle sorte que l'ensemble forme une boucle fermée. Les nœuds ou MAU sont actifs, ils reçoivent et régénèrent le message. Mais en cas de coupure de l'anneau le réseau est interrompu, ce qui est le cas lors de l'installation d'une nouvelle station de travail.

On peut résoudre cette sensibilité aux coupures en doublant l'anneau.

- **Double anneau unidirectionnel** : si les informations circulent dans le même sens sur les deux anneaux, le fonctionnement du réseau est assuré en cas de rupture de l'un des câbles.

- **Double anneau bidirectionnel** : si les informations circulent en sens inverse sur les deux anneaux est assuré en cas de rupture des deux câbles.

#### e) Topologie en étoile

Dans une topologie en étoile tous les MAU du réseau sont connectés à un nœud central : le concentrateur. L'ensemble des messages transitent par ce nœud.

Le câblage du réseau est plus couteux que celui de la topologie en bus. Il est effectué à l'aide de câble en paire torsadées. Une topologie physique étoile peut supporter les trois topologies électriques.

#### f) La topologie hiérarchique

Dérivée des réseaux en étoile, les réseaux hiérarchiques sont constitués d'un ensemble de réseaux étoiles reliées entre eux par des concentrateurs jusqu'à un nœud unique. Cette topologie est essentiellement mise en œuvre dans les réseaux locaux, 10 bases T, Starlan.

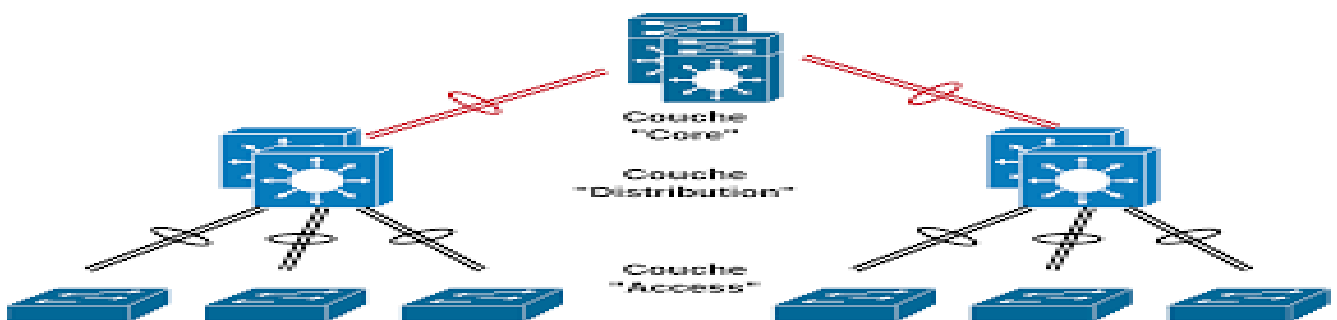


Figure 16: Topologie hiérarchique

### g) La topologie arborescente

C'est une topologie en bus sur laquelle un des nœuds est connecté en un répéteur, qui donne naissance à un nouveau bus. Elle est souvent utilisée pour les extensions de réseaux et permet ainsi de les étendre au-delà des recommandations du constructeur.

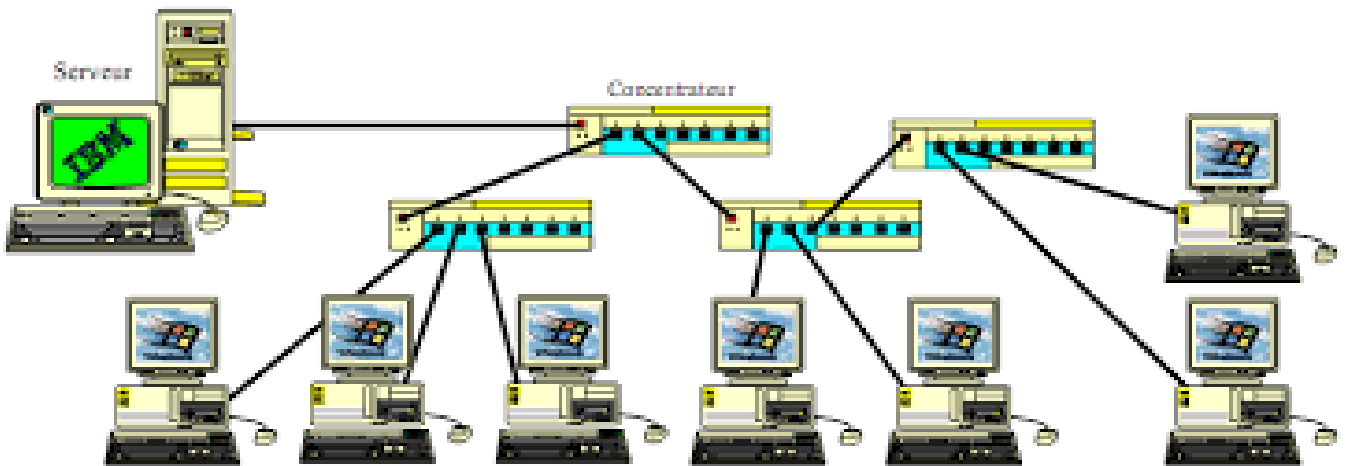


Figure 17:Topologie arborescente

### h) La topologie maillée

Le réseau maillé est un réseau dans le quelles deux stations de travail peuvent être mises en relation par différents chemins. La connexion est effectuée à l'aide de commutateurs, par exemple les autocommutateurs PABX.

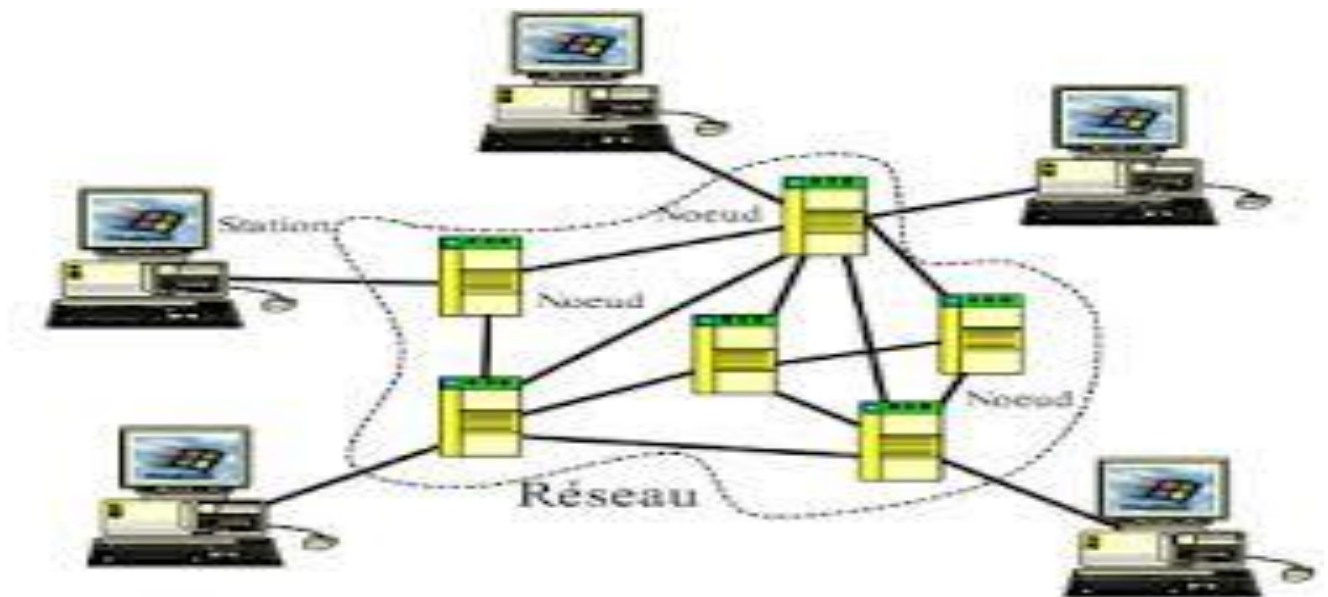


Figure 18:Topologie maillée

## **2.2.7. LES MODELES DE RESEAUX**

### **2.2.7.1. LE MODELE OSI :**

Le développement rapide des moyens de calcul et l'importance croissante des systèmes d'information ont engendré la multiplication des techniques de réseaux. La complexité croissante des besoins de communication et la diversité de solutions adoptées ont très vite fait apparaître la nécessité de définir un modèle complet de communication ou architecture protocolaire réseau.

Historiquement, les deux architectures : SNA d'IBM, DSA de BULL propriétaires incompatibles entre elles ne permettent pas l'interopérabilité des systèmes. La nécessité est de définir des techniques de mises en relation en spécifiant une architecture normalisée. C'est qu'entreprit l'ISO (modèle OSI).

Le modèle OSI est architecturé en sept (7) couches permettant la transmission de données de façons méthodiques.

#### **➤ La couche physique**

Elle décrit les caractéristiques physiques et électriques du support de transmission.

La couche physique ne s'intéresse en aucune façon aux données transportées par le réseau. Elle convertit les signaux électriques en bits constituant une trame complète de couche de liaison données (PDU) de la couche physique est appelée « bit ».

#### **➤ La couche liaison des données**

Elle définit les règles d'émission et de réception des données à travers les médias entre les deux systèmes. La normalisation ne concerne que la couche liaison dans le modèle OSI l'unité de données de la couche liaison est appelée « trame ».

#### **➤ La couche réseau**

Elle assure l'acheminement des données de nœuds, les opérations d'adressage et de routage de paquets de données vers la destination. L'unité de données de la couche réseau est appelée « paquets ».

#### **➤ La couche transport**

Elle gère le transport de paquets de bout en bout à travers du réseau. Elle assure les fonctions d'adressage, de découpage et réassemblage des informations. Le rôle principal de la couche transport est de contrôler les flux d'informations de la source vers la destination. L'unité de donnée de la couche transport est appelée « message ou segment ».

#### **➤ La couche session**

Première couche orientée traitement, son rôle est d'assurer l'ouverture et la fermeture de session entre deux systèmes distants. Son rôle principal est de mettre en place le contrôle de dialogue entre les entités communicantes : connexion, gestion des entrées/sorties, la synchronisation.

### ➤ La couche présentation

Elle convertit les données informatiques par l'application et les utilisateurs ; cryptage, graphique, format de fichier. C'est-à-dire elle permet de compresser les données pour qu'il puisse être décompressé par le destinataire.

### ➤ La couche application

Cette couche rend utilisable le système par le biais des applications (navigateurs) et des protocoles (FTP, SNMP, etc.). Cela couvre des éléments tels que les programmes de messagerie électronique, qui utilisent le réseau de manière significative pour les utilisateurs humains et les objectifs qu'ils tentent d'atteindre.

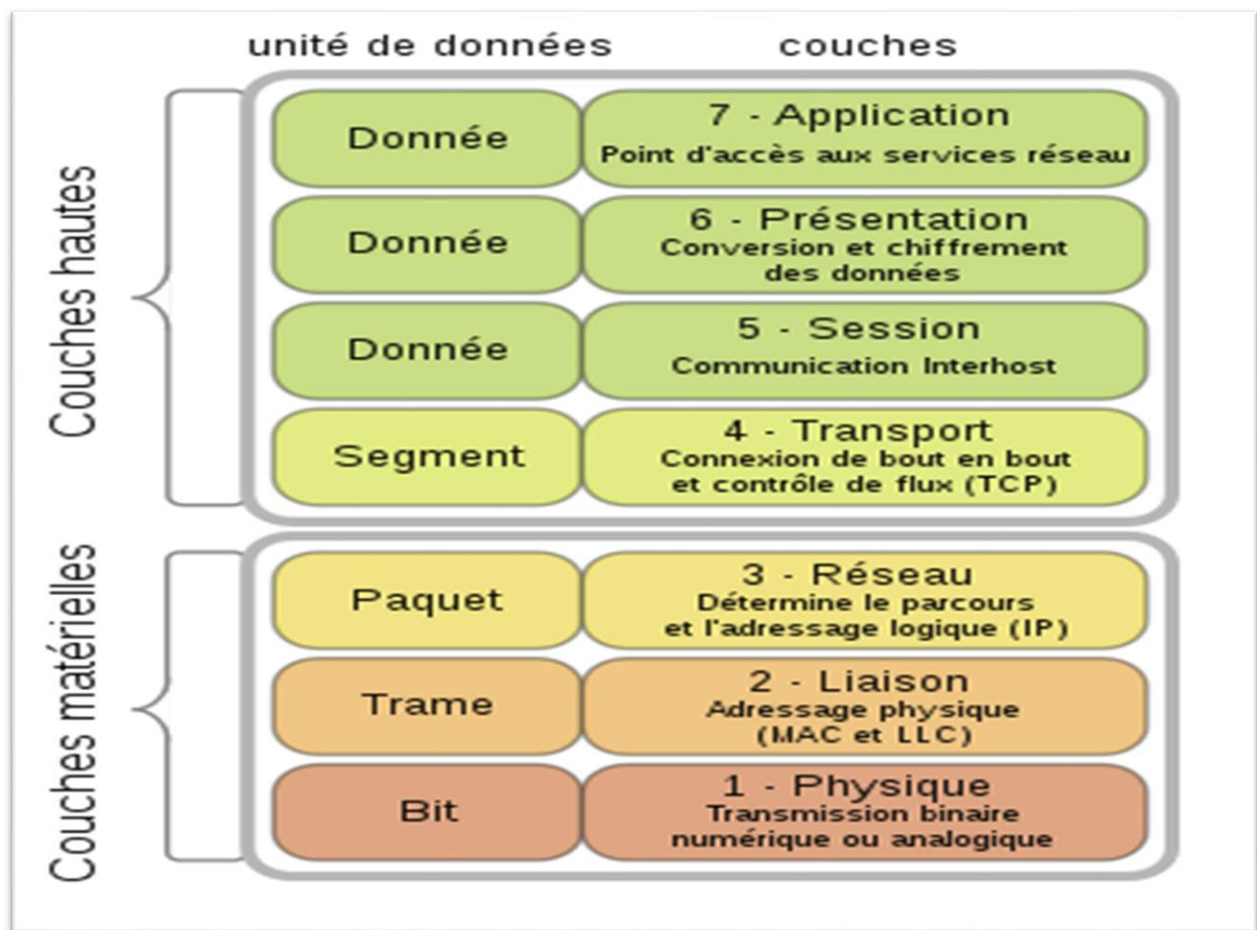


Figure 19:modèle OSI



### 2.2.7.2. LE MODELE TCP/IP

Le modèle TCP/IP a été inventé bien avant le modèle OSI. Les deux systèmes de réseau dont est basé l'internet pour permettre les ordinateurs de connecter via des réseaux engendrant l'échange des informations en paquets est appelé TCP et IP. Le rôle de chacun de ces dernières est énuméré comme suit :

#### ➤ **TCP (Transmission Control Protocol)**

Il se charge de la sécurité du transport des paquets en récupérant tous paquets perdus par le réseau lors de leur transmission jusqu'à l'aboutissement complété, sécurité et fiable de celui-ci. C'est un protocole IP non seulement de niveau supérieur mais aussi orienté connexion, fiable sur l'IP. Pour une connexion TCP entre deux machines du réseau, les messages sont libérés et délivrés en séquence.

#### ➤ **IP (Internet Protocol)**

L'acheminement des paquets est assuré par ce Protocol IP. Mais celui-ci ne garantit pas que le destinataire recevra le message dans l'ordre, ou même s'il le recevra ; c'est plutôt le TCP qui le gère. L'IP est en mode non connecté et ne garantit pas la remise.

Le modèle TCP/IP est une proposition plus simple, plus facile à comprendre et plus pratique. Le TCP/IP utilisant quatre couches légèrement et simples qui sont :

- **L'accès au réseau** (parfois appelée couche d'interface réseau) : elle représente le matériel réseau de base et correspond aux couches de liaison physique et de donnée du modèle OSI.
- **L'internet** (parfois appelé couche réseau) : indique comment les données sont envoyées sur le réseau et elle est équivalente à la couche réseau du modèle OSI.
- **Transport** : correspond à la couche de transport dans le modèle OSI. TCP (Transmission Control Protocol) fonctionne au niveau de cette couche. TCP convertit les données transmises en paquets (et inversement à la réception) et veille à ce que ces paquets soient distribués et réassemblés de manière fiable dans l'ordre ou ils ont été envoyés.
- **Application** : équivalent aux couches Session, Présentation et Application du modèle OSI. Des protocoles Internet bien connus tels que HTTP, FTP, et SMTP travaillent tous au niveau de cette couche.



Figure 20:modèle TCP/IP

## 2.2.8. LES EQUIPEMENTS RESEAUX

### 2.2.8.1.REPETEURS

Ils permettent de raccorder deux réseaux identiques ou deux stations de travail ou une station et un serveur, lorsque la liaison ne peut pas être effectuée, en raison de la distance, par un seul câble. Ils n'ont aucune fonction de routage, de traitement des données, d'accès au support

### 2.2.8.2. LES CONCENTRATEURS

Ils autorisent aussi le partage d'une voie composite. Ils analysent le contenu des blocs d'informations, provenant généralement d'un ordinateur gérant les stations de travail, le serveur, et les redirigent vers la seule station de travail concernée. Ils possèdent une logique programme

### 2.2.8.3. LE ROUTEUR

Le routeur est un équipement qui intervient au niveau 3 du modèle OSI, il intervient surtout dans la régulation du trafic dans les grands réseaux. Il analyse et peut prendre des décisions (c'est un équipement intelligent). SON rôle principal consiste à examiner les paquets entrants, à choisir le meilleur chemin pour le transporter vers la machine destinataire. On peut relier un routeur à un ordinateur afin de permettre sa configuration (mot de passe, type de réseau). Le routeur est intelligent par ce qu'il est doté :

D'une mémoire, d'un programme(algorithme), de logiciel d'exploitation.

## PARTIE II : GENERALITES SUR LA SUPERVISION

# CHAPITRE I : PRESENTATION DE LA SUPERVISION RESEAU

## 1.1. PRINCIPE DE FONCTIONNEMENT DE LA SUPERVISION

### 1.1.1. INTRODUCTION

La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l'état des réseaux et de leurs composants. Ces données seront ensuite traitées et affichées afin de mettre la lumière sur d'éventuels problèmes. La supervision peut résoudre les problèmes automatiquement ou dans les cas contraires via un système d'alerte (email ou SMS par exemple) les administrateurs. Cette définition de la supervision est décrite plus en détail dans la norme ISO7498/4.

Plusieurs actions sont ainsi réalisées :

- Acquisition de données, analyse, puis visualisation et réaction. Un tel processus est réalisé à plusieurs niveaux d'un parc de machine : Au niveau interconnexion (Réseau), au niveau de la machine elle-même (Système) et au niveau des services offerts par cette machine (Applications).
- **Supervision réseau** : Par le terme réseau on entend ici l'aspect communication entre les machines. Le rôle est de s'assurer du bon fonctionnement des communications et de la performance des liens (débit, latence, taux d'erreurs). C'est dans ce cadre que l'on va vérifier par exemple si une adresse IP est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau.
- **Supervision système** : La surveillance se cantonne dans ce cas à la machine elle-même et en particulier ses ressources. Si l'on souhaite par exemple contrôler la mémoire utilisée ou la charge processeur sur le serveur voire analyser les fichiers de logs système.
- **Supervision applicative** : Cette technique est plus subtile, c'est elle qui va nous permettre de vérifier le fonctionnement d'une application lancée sur une machine. Cela peut être par exemple une tentative de connexion sur le port de l'application pour voir si elle retourne ou demande bien les bonnes informations, mais aussi de l'analyse de logs applicatifs

### 1.1.2. LE ROLE DE LA SUPERVISION

Deux phases sont importantes pour que les administrateurs soient capables d'atteindre l'objectif voulu par la supervision, à savoir, surveiller le système et garantir sa disponibilité même en cas d'anomalie. Tenter de prévenir en cas de problème et garantir une remontée d'information rapide ; Automatiser les tâches de récupération des applications et des services en des mécanismes de redondance en une durée d'intervention minimale (par exemple : le redémarrage des services interrompus, l'arrêt de la machine en cas de la surcharge de CPU, la sauvegarde des données en cas de risque de perte d'un disque dur en mémoire...etc.).

### **1.1.3. TYPES DE SURVEILLANCE**

Pour la supervision informatique il existe 3 principaux types qui sont :

#### **1.1.3.1. SUPERVISION RÉSEAU**

Par le terme réseau on entend ici l'aspect communication entre les machines. Le rôle est de s'assurer du bon fonctionnement des communications et de la performance des liens (débit, latence, taux d'erreurs). C'est dans ce cadre que l'on va vérifier, par exemple, si une adresse IP est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau ;

#### **1.1.3.2. SUPERVISION SYSTÈME**

La surveillance se limite dans cas, à la machine elle-même et en particulier ses ressources comme :

- Le contrôle de la mémoire utilisée
- La charge processeur sur le serveur voir analyser les fichiers de logs système ;
- Le stockage de données ;
- Serveur : utilisateur des ressources ;

#### **1.1.3.3. SUPERVISION DES APPLICATIONS**

Cette technique est plus subtile, c'est elle qui va nous permettre de vérifier le fonctionnement d'une application lancée sur une machine. Cela peut être, par exemple, une tentative de connexion sur le port de l'application pour voir si elle retourne ou demande bien les bonnes informations. En effet, rien ne garantit qu'un port X ouvert veut dire que l'application qui tourne derrière, n'est pas « plantée ».

## **1.2. LES PROTOCOLES DE SUPERVISION**

### **1.2.1. LE PROTOCOLE ICMP**

Le protocole ICMP (Internet Contrôle message protocole) permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des datagrammes en erreurs. Chaque pile IP, que ce soit des routeurs ou des stations de travail, gèrent l'entête ICMP par défaut.

Ce protocole est considéré comme étant une partie de l'ensemble des protocoles TCP/IP. Cependant, contrairement à TCP et UDP, il se situe en couche 3 et donc, il est encapsulé dans un

paquet IP. Le mot « Encapsulation » relate clairement la confusion du placement d'ICMP dans les 7 couches OSI.

Les messages d'erreur ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi, les messages d'erreurs peuvent eux même être sujets aux erreurs. Toutefois, en cas d'erreur sur un message ICMP, aucune trame d'erreur n'est délivrée pour éviter un effet « boule de neige ».

### **1.2.2. LE PROTOCOLE SNMP**

SNMP (Simple Network Management Protocol) est le protocole de gestion de réseaux proposé par l'IETF. Il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux. SNMP est un protocole relativement simple. Pourtant l'ensemble de ses fonctionnalités est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications : les bases de données, les serveurs, les logiciels, etc. Les buts du protocole SNMP sont de :

- Connaître l'état global d'un équipement (actif, inactif, partiellement opérationnel...)
- Gérer les événements exceptionnels (perte d'un lien réseau, arrêt brutal d'un équipement...);
- Analyser différentes métriques afin d'anticiper les problèmes futurs (engorgement réseau...);
- Agir sur certains éléments de la configuration des équipements.

#### **1.2.2.1. LA MIBS**

Chaque agent SNMP maintient une base de données décrivant les paramètres de l'appareil géré. Le Manager SNMP utilise cette base de données pour demander à l'agent des renseignements spécifiques. Cette base de données commune partagée entre l'agent et le manager est appelée Management Information Base (MIB). Généralement ces MIB contiennent l'ensemble des valeurs statiques et de contrôle définis pour les éléments actifs du réseau. SNMP permet également l'extension de ces valeurs standards avec des valeurs spécifiques à chaque agent, grâce à l'utilisation de MIB privées. Un fichier MIB est écrit en utilisant une syntaxe particulière, cette syntaxe s'appelle SMI 3, basée sur ASN.1 tout comme SNMP lui-même. En résumé, l'agent collecte ces données localement et les stocke, tel que défini dans la MIB. Ainsi le Manager doit être conscient de la structure (que celle-ci soit de type standard ou privée) de la MIB afin d'interroger l'agent au bon endroit.

La structure d'une MIB est une arborescence hiérarchique dont chaque nœud est défini par un nombre ou un Object IDentifier (OID). Chaque identifiant est unique et représente les caractéristiques spécifiques du périphérique géré. Lorsqu'un OID est donc une séquence de chiffres séparés par des points. Une MIB est un arbre très dense, il peut y avoir des milliers d'OID dans la MIB.



Figure 21:Structure OID

Ainsi pour interroger les différentes variables d'activités sur un appareil, il faudra explorer son arborescence MIB. Celle-ci est généralement fournie par le constructeur mais il est aussi possible d'utiliser un explorateur de MIB tel que « Gétif MIB Browser ». Ensuite, pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne l'emplacement de la variable à consulter dans la MIB. On aura par exemple sur un commutateur Nortel Passport l'OID .1.3.6.1.4.1.2272.1.1.20 désignant le taux de charge du PCU.

### 1.2.2.2. LES TRAPS SNMP

Les traps SNMP sont des informations envoyer en utilisant le protocole SNMP depuis un équipement superviser vers un serveur de supervision. Les traps consistent à faire une vérification passive ; en gros, on configure l'agent SNMP pour qu'il contact un autre agent SNMP en cas de problèmes ou lors de certains évènements.

Ces informations contiennent plusieurs attributs dont :

- Adresse de l'équipement qui a envoyé l'information.
- L'OID racine (Object Identifier) correspond à l'identifiant du message reçu.
- Le message envoyer à travers du traps SNMP qui correspond à un ensemble de paramètres. Afin de pouvoir interpréter l'évènement reçu, le serveur de supervision doit posséder dans sa configuration le nécessaire, pour traduire l'évènement. Pour cela il doit disposer d'une base de données contenant les OID ainsi que leurs descriptions, c'est ce qu'on appelle les fichiers MIB. Il deux types de MIB :
  - Les MIB standards qui utilisent des standardisés et qui sont implémentés par de nombreux constructeurs sur leurs équipements.
  - Les MIB constructeurs qui sont propres à chacun et souvent à chaque modèle d'équipement, ils sont récupérés auprès des constructeurs de matériels.

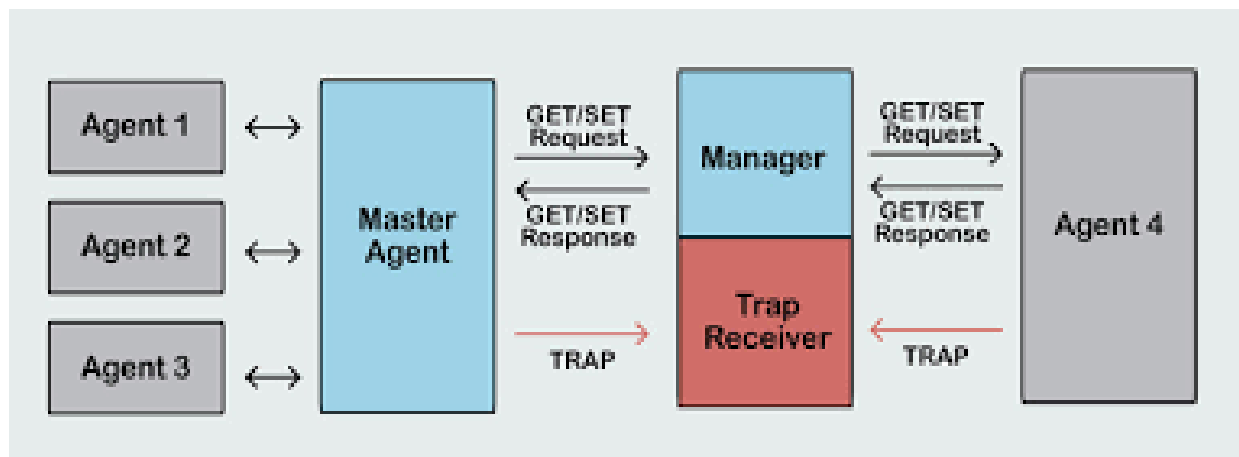


Figure 22:traps SNMP

### 1.3. LES OUTILS DE SUPERVISIONS

#### 1.3.1. NAGIOS

NAGIOS est une application écrite en C permettant la surveillance des systèmes, Créée en 1999 sous le nom de Net Saint. C'est aussi un logiciel de supervision de réseau libre sous licence GPL, qui fonctionne sous Linux et d'autres variantes Unix.

Il a pour fonction de surveiller les hôtes et services spécifiés, alternant l'administrateur des états des machines et équipements présents sur le réseau.

Bien qu'il fonctionne dans un environnement Linux, ce logiciel est capable de superviser toutes sortes de systèmes d'exploitation (Windows, Linux, Mac OS) est également des équipements réseaux grâce aux protocoles SNMP. Cette polyvalence permet d'utiliser NAGIOS dans toutes sortes d'entreprises, quel que soit la pédagogie du réseau et les systèmes d'exploitation utilisés au sein de l'entreprise. La modularité et la forte communauté qui gravite autour de Nagios offrent

Des possibilités en termes de supervision qui permettent aujourd'hui de pouvoir superviser pratiquement n'importe quelle ressource. Parmi ces fonctionnalités on y retrouve :

- La supervision réseau ;
- La supervision des ressources systèmes ;
- La supervision applicative ;
- La notification par différents moyens de communication ;
- La représentation des états des ressources supervisées, par coloration ;
- La cartographie du système d'informations supervisé ;
- La surveillance des services ;
- La journalisation des événements ;



- La gestion des graphiques à l'aide de centreon ;

Néanmoins, Nagios est un outil difficile à installer et à configurer et dispose d'une interface austère.

### **1.3.2. ZABIX**

Zabbix est un logiciel open source qui permet de surveiller le statut de divers services réseau, serveurs et autres matériels réseau. Distribué sous licence GPL v2, Zabbix fait partie des solutions majeurs de supervision libre.

Ses principales fonctionnalités sont les suivantes :

- Une supervision répartie avec une administration web centralisée, afin que la récolte des données ne soit pas interrompue en cas de problème réseau ;
- Génération et consultation facile des graphes en fonction du temps ;
- Une supervision de site web avec recherche de motif et scénarios de navigation ;
- Une interface web pour une visualisation efficace de l'état des éléments réseaux et des données récoltées ;
- La notification par e-mail, les messageries instantanées, les SMS, et pratiquement n'importe quel autre moyen, pour être informé rapidement lors qu'un problème apparaît.
- Une supervision sans agent, par SNMP, par SSH ou encore par IPMI, pour les serveur ou éléments réseaux ne permet pas l'installation de l'agent Zabbix
- Une supervision proactive, pour une interaction forte avec vos équipement (relance de services, extinction, redémarrage etc.) ;

La découverte automatique des serveurs et périphériques réseaux, pour surveiller les nouveaux serveurs dès que ceux-ci sont présent sur le réseau. Zabbix est facile à installer mais on rencontre souvent des problèmes lors de la configuration du switch et chaque machine à supervision doit disposer du client Zabbix.

### **1.3.3. CACTI**

Cacti est un outil purement de monitoring basé sur RRDtool permettant de surveiller l'activité de son architecture informatique à partir de graphiques quotidiens, hebdomadaires, mensuels et annuels. Il permet de représenter graphiquement divers états de périphériques et équipements réseaux utilisant SNMP pour connaître la charge processeur. Il est facile à installer et à configurer mais il est limité de base et peut mettre un certain temps à générer les graphes.

### **1.3.4. CENTREON**

C'est un outil qui vous permet de superviser l'ensemble de vos infrastructures matériels et logiciels composant votre système d'information. Aujourd'hui c'est une plateforme de supervision à la fois conviviale et puissante reposant sur Centreon Engine, Centreon Broker et Centreon Web.

Centreon offre :

- La possibilité d’avoir une vue synthétique de la supervision de son système d’informations
- La visualisation de graphiques de performances
- Des rapports de disponibilités des ressources supervisées
- Une interface de configuration intuitive pour les différents objets et fichiers de configurations des ordonnanceurs
- La possibilité d’administrer chaque paramètre de l’interface web
- La possibilité de construire un Dashboard à l’aide de widgets graphiques
- La possibilité de développer des modules additionnels pour étendre les fonctionnalités de la solution. Par contre il requiert plus de ressources matérielles que Nagios.

#### 1.4. ETUDE COMPARATIVE DES OUTILS DE SUPERVISION

La comparaison de ces différents outils de supervision est basée sur plusieurs critères. Nous allons donner plus de détails à l’aide du tableau suivant :

**Tableau 2 : Tableau comparatif**

<b>Solution</b>	<b>Avantage</b>	<b>Inconvénient</b>
Cacti	-Outil de métrologie complet -Multitude de fonctionnalités grâce aux plugins	-Création complexe des Template -Insuffisant pour une supervision d’un grand parc matériel
-Centreon	-IHM agréable et intuitive -Basé sur le cœur de Nagios	-L’aspect Métrologie est des plus simples -Pas de graphes corrélant les performances (utilisation d’un Apache par exemple)
Zabbix	-Outil complet -Prise en main complexe -Polyvalent (supervision métrologie)	-manque de lisibilité sur certains écrans -Prise en main complexe
Nagios	-Outil de supervision par excellence -Automatisation (Template-Mesure des ressources)	-Pas d’exploitation graphique des mesures -IHM à améliorer -Configuration par fichier

- Zabbix propose une interface unifiée, avec des fonctions avancées, la partie métrologie présente vraiment des notions intéressantes (graphes complexes de mesures...) sa prise en main n'est pas assez intuitive pour compenser son IHM qui est moins agréable que Centreon par exemple.
- Cacti est un outil de métrologie avancé, même s'il présente un aspect de supervision, pas assez développé malheureusement pour conduire son choix.
- Nagios semble parfait pour l'automatisation des configurations et la gestion centralisée d'infrastructure, son gros désavantage est et restera son interface graphique qui repoussera tous les débutants dans le domaine de la supervision

## 1.5. SOLUTION RETENUE

Le monde informatique retiendra que c'est la recherche de fiabilité et de la réduction des coûts qui dessinent l'avenir du système informatique en entreprise. La mise en place d'un tel outil doit être réfléchie et repose aussi sur les besoins exprimés par le décisionnel de l'entreprise.

Après avoir fait la comparaison de ces différents outils, on constate que, d'après les résultats du tableau, NAGIOS semble être la solution appropriée pour la supervision réseau.

En effet, Nagios, couplé à centreon, est une solution très performante, il est initiateur dans le monitoring possédant une large communauté qui met à disposition, un libre accès, des plugins SNMP préconfigurés.

A blue graphic element resembling a scroll, with a vertical strip on the left and a horizontal strip on the right, both with rounded ends and a slight 3D effect.

## PARTIE III : PRESENTATION DE LA SOLUTION RETENUE

# CHAPITRE I : PRESENTATION DE LA SOLUTION RETENUE

## 1.1. PRESENTATION DE NAGIOS

Nagios est un logiciel de supervision de réseau libre sous licence GPL qui fonctionne sous Linux. Il a pour fonction de surveiller les hôtes et les services spécifiés, alertant l'administrateur des états des machines et équipements présent sur le réseau. Bien qu'il fonctionne dans un environnement Linux, ce logiciel est capable de surveiller toutes sorte de systèmes d'exploitation (Windows XP, Windows 2000, Windows 2003 Server, Linux, Mac OS Entre autres) et également des équipements réseaux grâce au protocole SNMP

Cette polyvalence permet d'utiliser Nagios dans toutes sortes d'entreprises, quel soit la Topologie du réseau et les systèmes d'exploitation utilisés au sein de l'entreprise. Ce logiciel est composé de trois parties :

- Le moteur de l'application, qui gère et ordonnance la supervisons des différents équipements.
- Les plugins qui servent d'intermédiaire entre les ressources que l'on souhaite superviser et le Moteur de NAGIOS. Il faut bien noter que pour accéder à une certaine ressource sur un hôte, il faut un plugin coté NAGIOS et un autre coté hôte administré.
- L'interface web qui permet d'avoir une vue d'ensemble des états de chaque machine du parc informatique supervisé et ainsi pouvoir le plus rapidement possible en ciblant la bonne panne.

## 1.2. LE FONCTIONNEMENT DE NAGIOS

Le principe de supervision de NAGIOS repose sur l'utilisation de plugins, l'un installé sur la machine qui supporte NAGIOS, et l'autre sur la machine que l'on souhaite superviser. Un plugin est un programme modifiable, qui peut être écrit dans plusieurs langages possibles, selon les besoins, et qui servent à récupérer les informations souhaitées. NAGIOS, par l'intermédiaire de son plugin, contact l'hôte souhaité et l'informe des informations qu'il souhaite. Le plugin correspondant installé sur la machine concernée reçoit la requête envoyer par NAGIOS et ensuite vas chercher dans le système de sa machine les informations demandées. Il existe deux types de récupération d'informations : La récupération ACTIVE et la récupération PASSIVE. Alors que lors d'une récupération PASSIVE, l'envoi d'information est planifié en local, soit à partir d'une date, soit en réaction à un événement qui se déroule sur la machine administrée.

## 1.3. ARCHITECTURE DE LA SOLUTION

L'architecture de Nagios se base sur le paradigme serveur-agent. D'une manière spécifique, un serveur faisant office de point centrale de collecte des informations au serveur.

L'architecture globale de Nagios peut être décomposée en 3 parties coopératives entre elles :

- Un noyau qui est cœur du serveur Nagios, lancé sous forme de démon et responsable de la collecte et l'analyse des informations, la réaction, la prévention, la réparation et l'ordonnancement des vérifications (quand et dans quel ordre). C'est le principe de répartition des contrôles au mieux dans le temps qui nous évite la surcharge du serveur et des machines à surveiller.



Figure 23: Architecture de Nagios

- **Des exécutants :** ce sont les plugins dont un grand nombre est fourni de base, responsables de l'exécution des contrôles et tests sur des machines distantes ou locales et du renvoi des résultats au noyau du serveur Nagios
- Une IHM : C'est une interface graphique accessible par le web conçu pour rendre plus exploitable les résultats. Elle est basée sur les CGI (Common Gateway Interface) fournis par défaut lors de l'installation de Nagios qui interprètent les réponses des plugins pour les présenter dans l'interface. Cette interface sert à afficher de manière claire et concise une vue d'ensemble du système d'information et d'état des services surveillés, de générer des rapports et de visualiser l'historique. D'une manière générale avoir la possibilité de détecter en un simple coup d'oeil, les services ou hôtes ayant besoin d'une intervention de leur administrateur.

#### ➤ Les avantages de Nagios

- Des plugins qui étendent les possibilités de Nagios ;
- Une très grande communauté qui participe activement au développement
- Un moteur performant ;  
Solution complète permettant le reporting, la gestion des pannes et d'alarmes, gestion des utilisateurs... ;
- Des plugins permettent aux utilisateurs de développer facilement ces propres

Vérifications de leurs services ;

- Possibilité de répartir la supervision entre plusieurs administrateurs ;
- Offre la possibilité de développer ses propres modules

➤ **Les Inconvénients de Nagios**

- Configuration complexe mais peut s'améliorer en ajoutant
- Interface peu ergonomique et intuitive.

## 1.4. LES FONCTIONNALITES DE NAGIOS

Nagios fonctionne sur linux et dans le cas général pour la plupart des systèmes Unix. Nagios offre les possibilités suivantes :

- La supervision des services réseaux (SNMP, http...), des hôtes et des ressources systèmes (CPU, charge mémoire...) Mise en place d'un système de supervision Nagios Open source
- Présentation de l'outil de Supervision « Nagios »
- La détermination à distance et de manière automatique l'état des objets et les ressources nécessaires au bon fonctionnement du système grâce à ses plugins.
- Représentation colorisée des états des services et hôtes définis
- Génération de rapports.
- Cartographie du réseau.
- Gestion des alertes.
- Surveillance des processus (sous Windows, Unix...).
- Superviser des services réseaux :(SMTP, POP3, http, ICMP, SNMP, DAP, etc.)
- Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche (Bash, C++, Python, Perl, PHP, etc.)



Figure 24:Fonctionnalité de Nagios

## 1.5. LES PLUGINS

Les plugins qui sont des minis programmes que l'on peut compiler en fonction des besoins de supervision. Nagios exécute un plugin dès qu'il a besoin de connaître l'état d'un service ou d'un hôte et évalue le code de retour de ce plugin.

L'avantage de cette architecture est qu'on peut contrôler tout ce que l'on veut à travers les plugins.

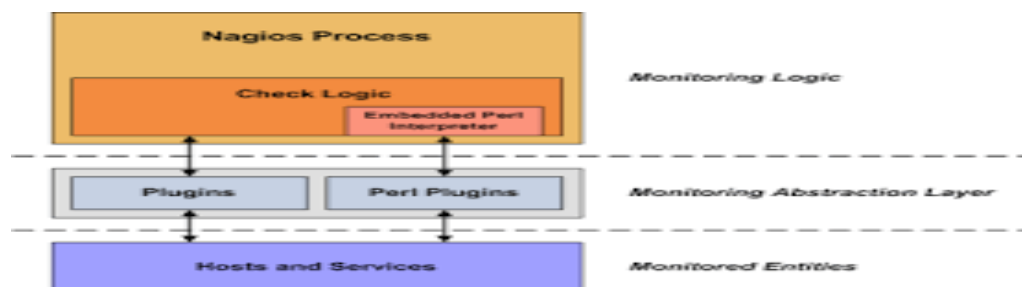


Figure 25: Les plugins de Nagios

Il existe de nombreux plugins pour Nagios et nous allons présenter quelques-uns dans ce rapport :

Pour la supervision des ressources systèmes locales nous disposons des plugins suivants :  
 Check\_Joad : pour vérifier la charge moyenne (load average) sur les systèmes Unix ;

- Check\_Idem : pour vérifier l'état des espaces mémoire pour sur les systèmes Unix
- Check\_disk : pour vérifier les espaces disques disponible pour les systèmes Unix ;
- Check\_file\_age : pour vérifier qu'un fichier a été mise à jour et qu'il a une taille minimale.
- Check\_otp-peer : pour vérifier le temps du système par rapport au serveur de temps NTP. On a aussi des plugins pour superviser l'état physique de la machine ;
- Check\_ide\_smart : pour analyser des informaion SMART des et detecter cieux qui sont défectueux ;
- Check\_seosors : pour vérifier les informations que les systèmes unix exportent sur l'etat de la machine. Il y a des plugins pour superviser les applications locales ;
- Check-procs : pour surveiller l'etat des processus et leur priorité sur les systèmes unix ;
- Check\_mail : pour connaître l'etat des mails en attant d'envoi par sendmail ou mail ;
- Check\_log2 : pour vérifier les nouvelles entrées dans un fichier log. Pour la supervision des services distants nous disposons des plugins suivants :
- Check\_tcp : pour vérifier l'ouverture d'un port tcp ;
- Check\_udp : pour verifier l'ouverture d'un port tcp ;
- Check\_dhcp : pour verifier qu'un serveur dhcp répond bien à la demande d'adresse IP ;
- Check\_dos et check\_dig : pour interroger un serveur DNS et verifier les enregistrements
- Check\_flexlm : pour verifier le bon etat d'un serveur de licence de type flexm HIEN K
- Check\_smtp : pour verifier le bon fonctionnement du serveur SMTP ;



- Check http : pour permettre la vérification simple de l'accès à la page web ;
- Check\_oracle : pour vérifier diverses informations sur l'état d'une base de données Oracle : connexion au listener, état des caches, remplissages des tablespaces, etc. ce plugin a besoin d'un client Oracle pour fonctionner ;
- Check MySQL check-f) gsql : pour tester des connexions à des bases de données MySQL et PostgreSQL. Pour la supervision des systèmes distants nous pouvons utiliser les plugins suivants :
- Check\_icmp, check\_fping, check-f) ing : pour vérifier qu'une machine est connectée au réseau. Ces trois plugins effectuent ce test mais le plus léger est check\_icmp ;
- Check\_hpjd : pour superviser les imprimantes à distance par SNMP ;
- Check\_centreon\_snmp\_traffic : permet de suivre le trafic d'un élément réseau et vérifier qu'il est en bon état ;
- Check\_snmp : pour interroger une ou plusieurs OID et de comparer et comparer les résultats obtenus avec des seuils définis par l'administrateur ;
- Check\_disk\_smb : pour vérifier l'état de partage des fichiers Windows et également vérifier que l'espace alloué n'est pas plein ;
- Check\_ups : pour vérifier l'état de fonctionnement des onduleurs de type UPS ;
- Check\_snmp\_load, checksnmp\_mem, check\_snmp\_storage : pour vérifier la charge du système, l'espace mémoire occupé, l'espace disque utilisé des serveurs distants via SNMP ;
- Check\_snmp\_win : pour superviser l'état d'un ou de plusieurs services sous Windows.

Il existe des plugins utilitaires pour superviser l'état du processus Nagios

- Check\_oagios : lorsque l'on met en place une architecture distribuée ou hautement disponible, ce plugin est nécessaire pour vérifier qu'au moins un des processus Nagios fonctionne toujours correctement ;
- Check\_dummy : pour vérifier l'état d'un élément dans le cas d'une supervision passive. Ce plugin renvoie comme résultat l'état de l'élément et le texte passé en argument ;
- Check\_orpe, check\_by\_ssh, check\_ot : pour vérifier le bon fonctionnement des agents nrpe, ssh et nsclient++, situés sur les hôtes ;
- Check\_cluster : pour faire une agrégation d'états au sein de Nagios.

## 1.6. LES FICHIERS DE CONFIGURATION

Nagios s'appuie sur différents fichiers textes de configuration pour construire son infrastructure de supervision. Nous allons à présent citer et définir ceux qui sont les plus importants :

- Nagios.cfg est le fichier de configuration principal de Nagios. Il contient la liste des autres fichiers de configuration et comprend l'ensemble des directives globale de fonctionnement.
- Cgi.cfg contient un certain nombre de directives qui affectent le mode de fonctionnement des CGI. Il peut être intéressant pour définir les préférences concernant l'interface web de Nagios.
- Resource.cfg permet de définir des variables globales réutilisables dans les autres fichiers. Etant inaccessible depuis le CGI qui génèrent l'interface, ce fichier peut être utilisé pour stocker des informations sensibles de configuration
- Commands.cfg contient les définitions des commandes externes, telles que celles qui seront utiles pour la remonté d'alerte.
- Checkcommands.cfg contient les définitions des commandes de vérification prédéfinies et celles définies par l'utilisateur.
- Hosts.cfg définies par l'utilisateur.
- Hosts.cfg définit les différents hôtes du réseau à superviser. A chaque hôte est associe son nom son adresse IP, le teste est effectuer par défaut pour caractériser l'état de l'hôte, etc.
- Services.cfg associe à chaque hôte ou à chaque groupe d'hôtes l'ensemble des services qui doit être vérifiés.
- Hostgroups.cfg définit des groupes d'hôtes pour regrouper des hôtes selon des caractéristiques communes. Un hôte peut appartenir à plusieurs groupes.
- Contacts.cfg déclare les contacts à prévenir en cas d'incident et de définir les paramètres des alertes (fréquences des notifications, moyens pour contacter ces personnes, plages horaires d'envoi des alertes...)

## CHAPITRE II : MISE EN ŒUVRE DE NAGIOS

### 2.1. Environnement de travail.

#### 2.1.1. Besoins matériels.

La supervision nécessite un réseau informatique opérationnel. Dans notre cas, la mise en réseau a été faite entre une machine virtuelle équipée de système Ubuntu qui recevra notre serveur Nagios et une machine virtuelle Windows qui sera supervisée par notre serveur Nagios. La machine physique est de marque DELL (de processeur Intel Core <sup>TM</sup> i3-7300U, de RAM 8GB et de disque dur 300 GB) ayant un système d'exploitation Windows 10 équipée de logiciel VirtualHost qui accueillera les machines virtuelles.

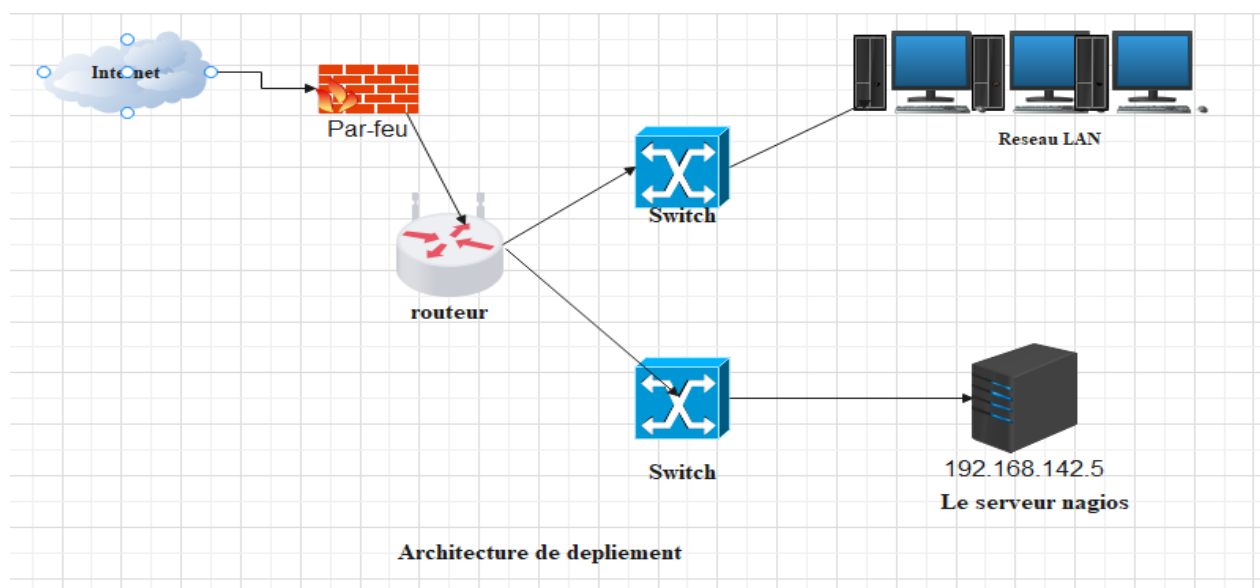
Un réseau /20 avec une Passerelle à 192.168.1.1, pas de serveur DHCP sur le réseau et le serveur hébergeant le serveur Nagios n'aura pas d'adresse IP dynamique, pour simplifier l'installation.

### 2.2. Mise en place de la solution.

La mise en place de la solution reposera sur le déploiement d'un environnement comportant trois éléments :

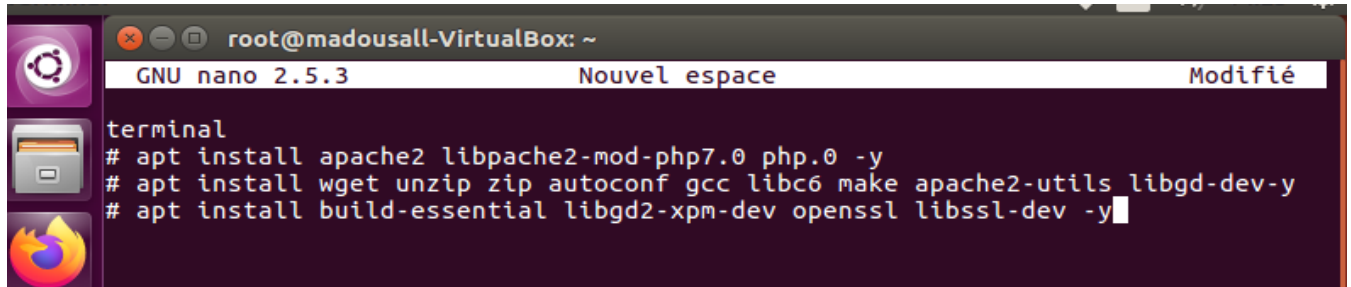
- La mise en place de Nagios ;
- L'installation de la machine Windows ;
- Tests de la solution.

#### 2.2.1. Architecture de mise en œuvre



### 2.2.2. Installation de Nagios

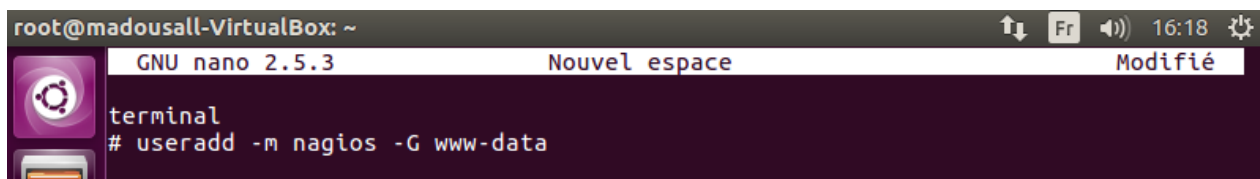
Maintenant que le réseau a été configuré, nous pouvons procéder à l'installation des dépendances de Nagios comme nous montre la figure suivante.



```
root@madousall-VirtualBox: ~  
GNU nano 2.5.3          Nouvel espace          Modifié  
terminal  
# apt install apache2 libapache2-mod-php7.0 php.0 -y  
# apt install wget unzip zip autoconf gcc libc6 make apache2-utils libgd-dev-y  
# apt install build-essential libgd2-xpm-dev openssl libssl-dev -y
```

Figure 26: Installation de Nagios

Il faut ensuite créer un utilisateur Nagios et l'ajouter au groupe apache qui est www-data.



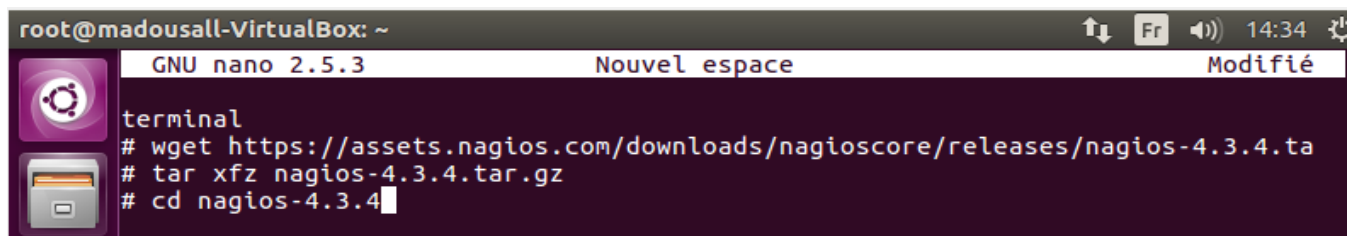
```
root@madousall-VirtualBox: ~  
GNU nano 2.5.3          Nouvel espace          Modifié  
terminal  
# useradd -m nagios -G www-data
```

Figure 27: Creation des utilisateurs

Les dépôts pour Nagios sont accessibles sur le site

<https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.3.4.tar.gz>

Les dépôts contiennent les paquets sources de nagios core qu'il faut télécharger, puis décompresser et désarchiver comme nous montre la figure ci-dessous.



```
root@madousall-VirtualBox: ~  
GNU nano 2.5.3          Nouvel espace          Modifié  
terminal  
# wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.3.4.ta  
# tar xzf nagios-4.3.4.tar.gz  
# cd nagios-4.3.4
```

Figure 28: Téléchargement de Nagos

```

root@madousall-VirtualBox: ~
root@madousall-VirtualBox:~# cd nagios-4.3.4/
root@madousall-VirtualBox:~/nagios-4.3.4# ls
base          daemon-init.in  Makefile        sample-config
cgi           docs            Makefile.in     subst
Changelog     doxy.conf       make-tarball    subst.in
common        functions       mkpackage       t
config.guess  html           module          tap
config.log    include        nagios.spec     test
config.status indent-all.sh  nagios.sysconfig THANKS
config.sub    indent.sh      openrc-init     t-tap
configure     INSTALLING    openrc-init.in  update-version
configure.ac  install-sh    pkginfo         UPGRADING
contrib       LEGAL         pkginfo.in      worker
CONTRIBUTING.md lib           README          xdata
daemon-init   LICENSE       README.asciidoc

```

Figure 29:le contenu de Nagios

Ensuite il faut lancer le script **configure** puis la commande **make** pour effectuer l'installation.

```

root@madousall-VirtualBox: ~
GNU nano 2.5.3          Nouvel espace          Modifié
terminal
# ./configure
# make all
# make install
# make install-init
# make install-commandmode
# make install-config
# systemctl enable nagios-service

```

Figure 30:Installation de Nagios Core

Il faut à présent configurer le serveur web pour fonctionner avec l'interface web nagios. Ceci est réalisé assez facilement grâce aux commandes ci-après :

```

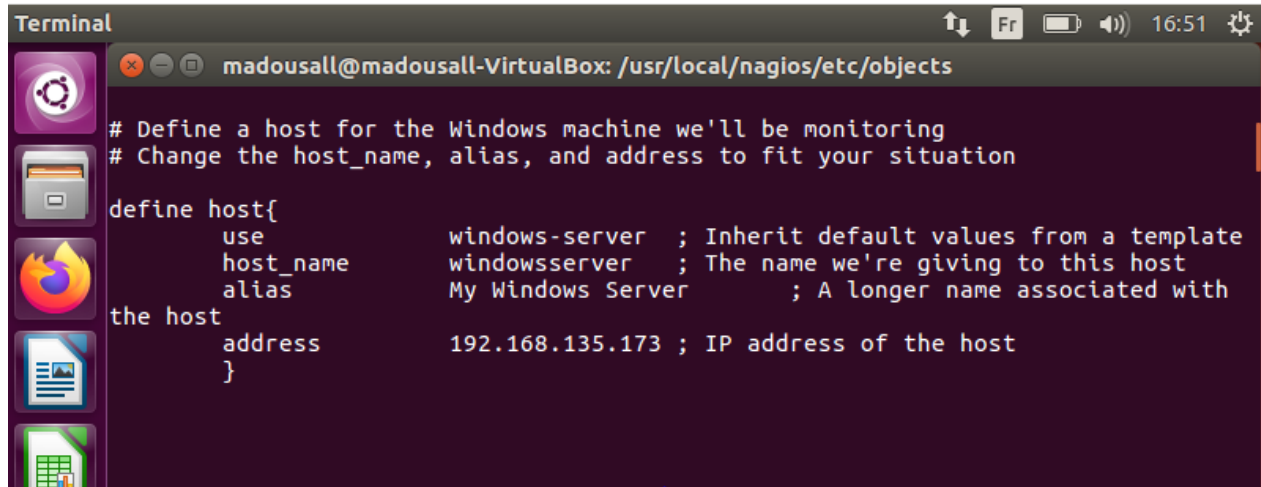
root@madousall-VirtualBox: ~
GNU nano 2.5.3          Nouvel espace          Modifié
terminal
# mkdir -p /etc/httpd/conf.d/nagios.conf
# make install-webconf
# cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/
# chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
# /usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-enabled
# a2enmod cgi
# service apache2 restart
# systemctl start nagios.service

```

Figure 31:Installation de l'interface web de Nagios Core

Une fois les deux paquets installés, nous pouvons vérifier s'il y a un problème de localisation des fichiers ou une redondance de définition dans les fichiers de configuration en utilisant la commande suivante.

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

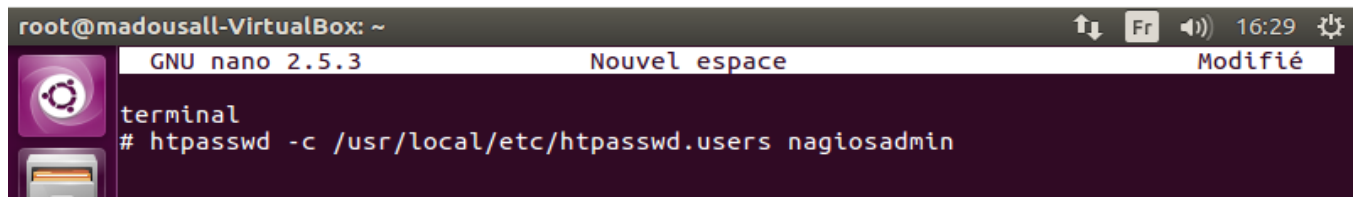
A terminal window titled 'Terminal' with a dark background. The prompt is 'madousall@madousall-VirtualBox: /usr/local/nagios/etc/objects'. The text shows the configuration for a host named 'windows-server'.

```
# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

define host{
    use             windows-server ; Inherit default values from a template
    host_name       windowsserver  ; The name we're giving to this host
    alias           My Windows Server ; A longer name associated with
the host
    address         192.168.135.173 ; IP address of the host
}
```

Figure 32: la configuration de nagios

Il faut ensuite attribuer un mot de passe à l'administrateur nagiosadmin pour sécuriser l'accès à l'interface web de Nagios. Le mot de passe sera stocker dans le fichier htpasswd.users.

A terminal window titled 'root@madousall-VirtualBox: ~' with a dark background. The prompt is 'root@madousall-VirtualBox: ~'. The text shows the command to create a user named 'nagiosadmin' in the file 'htpasswd.users'.

```
GNU nano 2.5.3          Nouvel espace          Modifié
terminal
# htpasswd -c /usr/local/etc/htpasswd.users nagiosadmin
```

Figure 33: Creation d'un acces administrateur

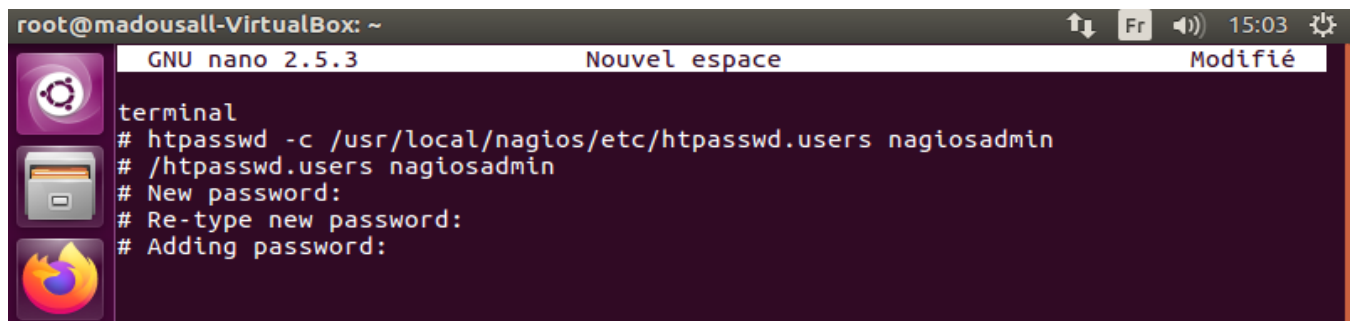


Figure 34:le nom d'utilisateur et le mot de passe

Il est encore nécessaire de configurer les différents services de Nagios, mais cela sera fait dans le tableau de bord de Nagios après connexion au serveur dans un navigateur à l'adresse suivante : <http://localhost/nagios>

Un identifiant sera demander et pour notre cas, c'est « nagiosadmin » et le mot de passe saisi lors de la création « admin »

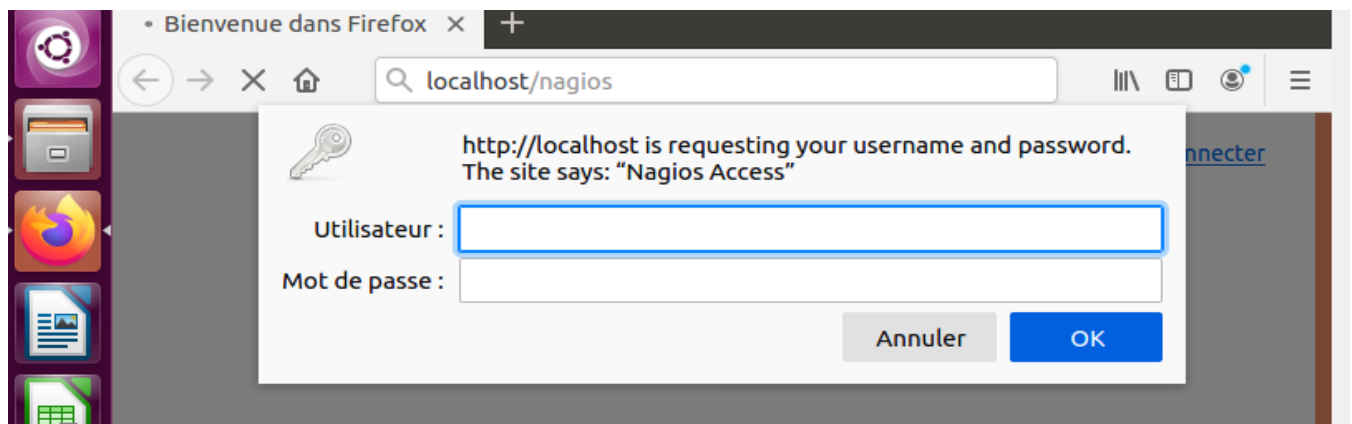


Figure 35:saisir le nom d'utilisateur et le mot de passe

L'interface de Nagios Core

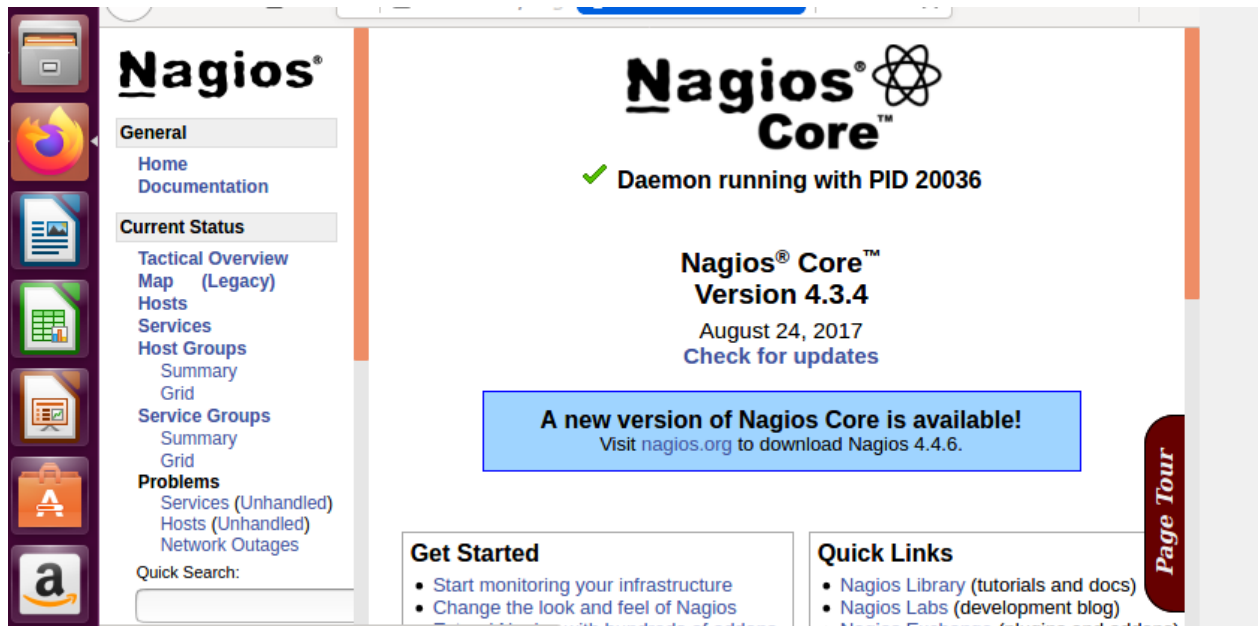


Figure 36: Interface de Nagios Core

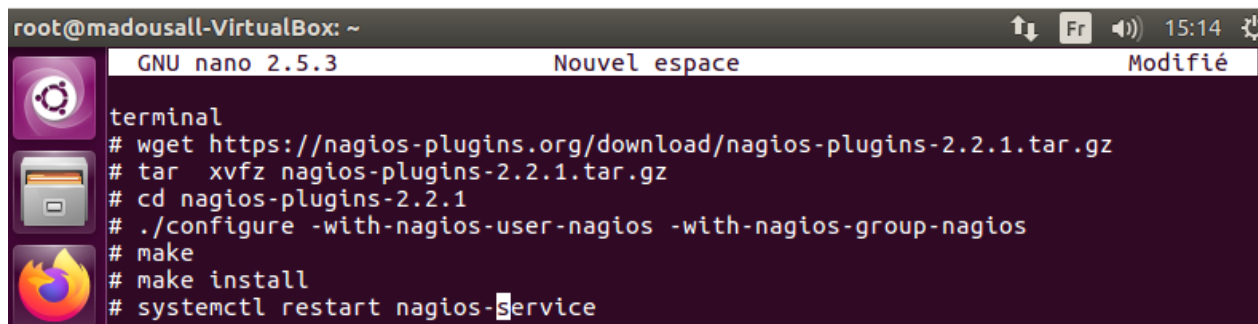


Figure 37: Installation des plugins de Nagios

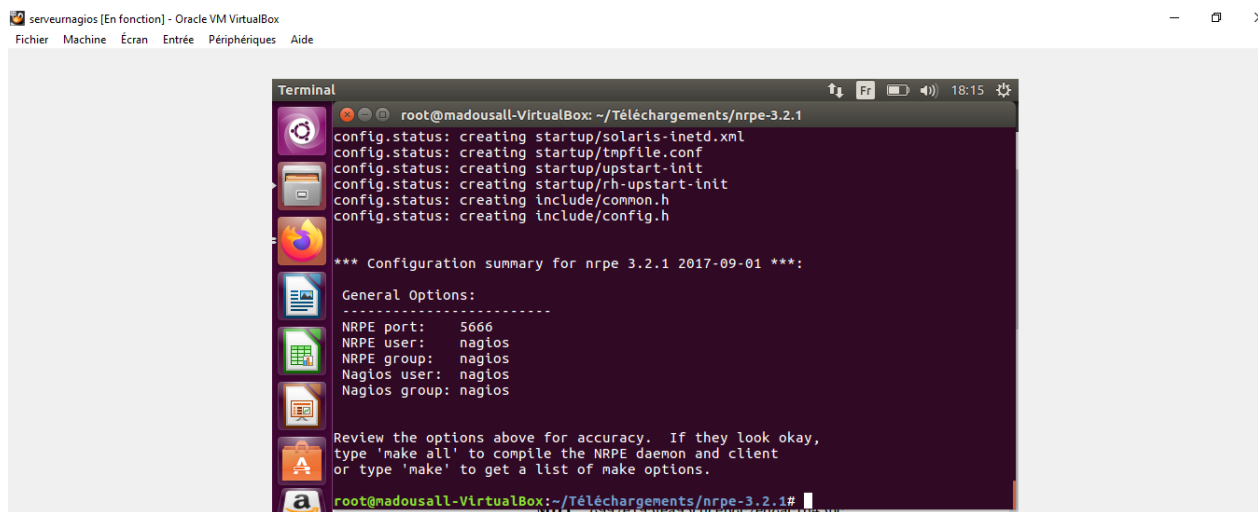


Figure 38: Installation des plugins de Nagios1



### 2.2.3. Machine Windows :

Pour surveiller les machines fonctionnant sous le système d'exploitation Windows nous avons besoin d'un daemon (responsable d'une tâche exécutée en arrière-plan) sous le nom de NSClient++.

#### 2.2.3.1.Installation et Configuration :

L'agent possède un exécutable d'installation. Il s'installe par défaut dans le répertoire

C:\Program Files\NSClient++. Nous avons téléchargé et installer la dernière version 64 bit de NSClient. Ensuite faire double clic sur l'exécutable pour lancer l'installation de NSClient++.

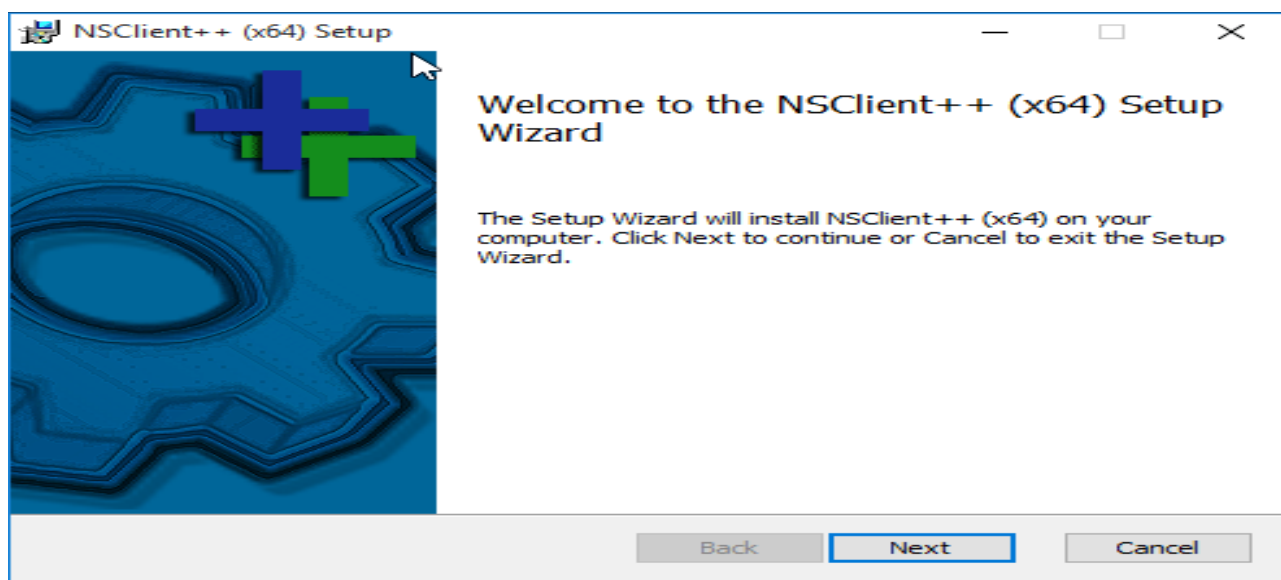


Figure 39:Installation de NSClient

Après avoir cliqué sur suivant, il faut ensuite saisir l'adresse IP du serveur et le mot de passe de l'administrateur Nagiosadmin et suivre les étapes jusqu'à la fin de l'installation comme indiqué dans sur les écrans suivants :

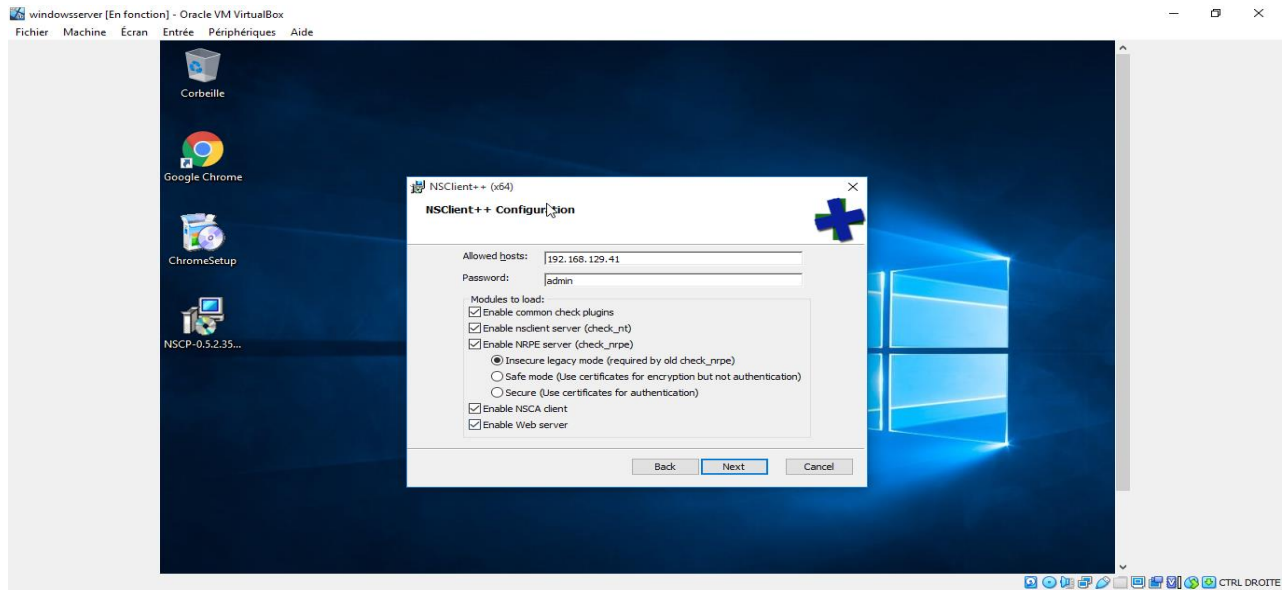


Figure 40:Installation de NSclint1

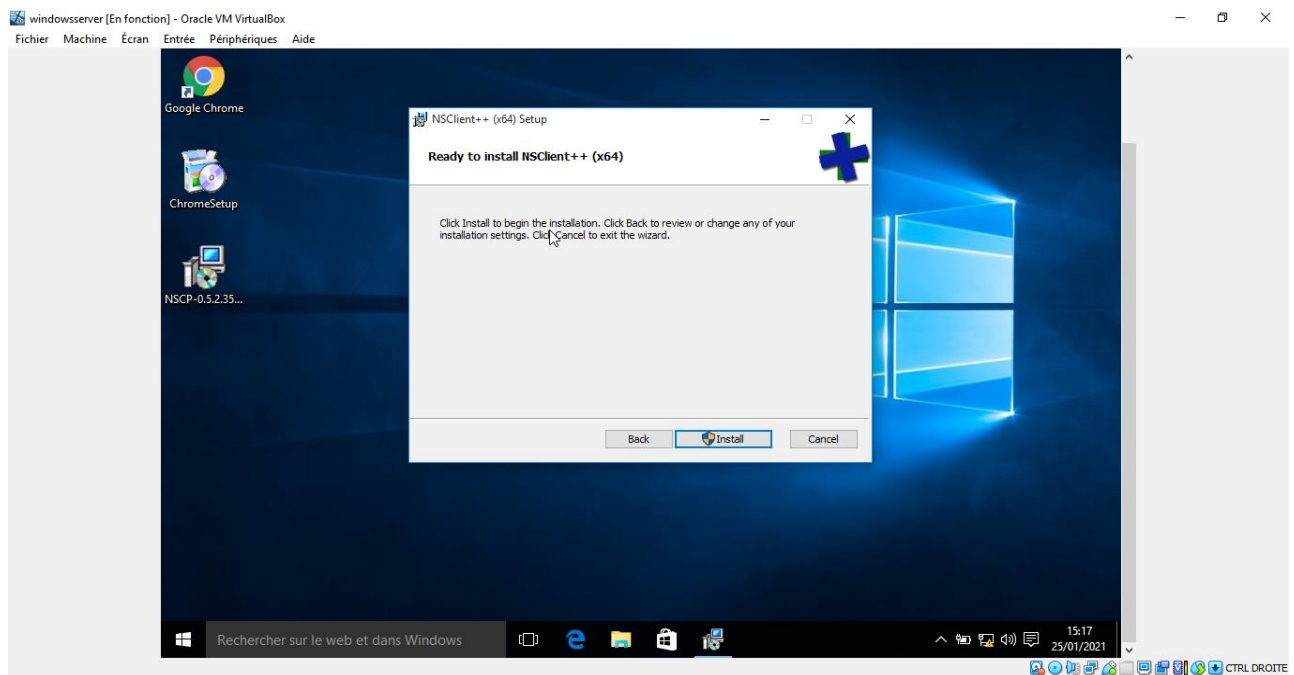


Figure 41:Installation NSClient2

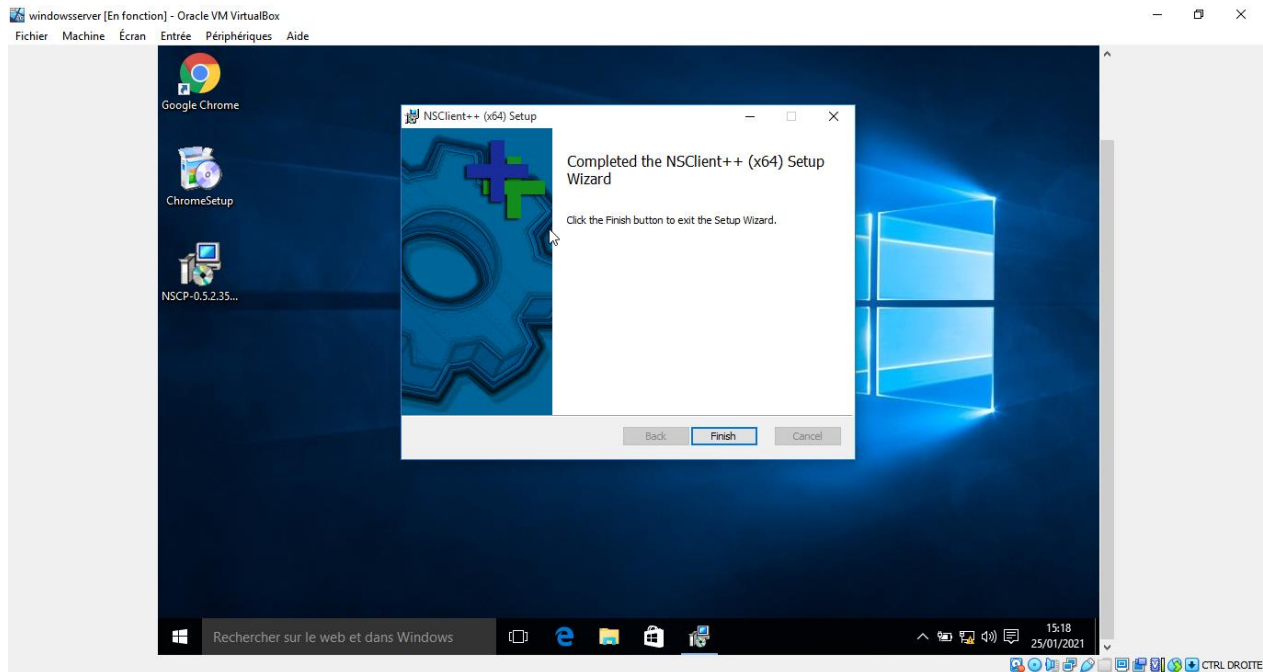


Figure 42: Installation de NSClient3

A la fin de l'installation, il faut modifier les droits de l'administrateur de pouvoir modifier les fichiers de NSClient++ en faisant un clic droit sur le sous repertoire NSClient dans C:\Programme Files\ NSClient++

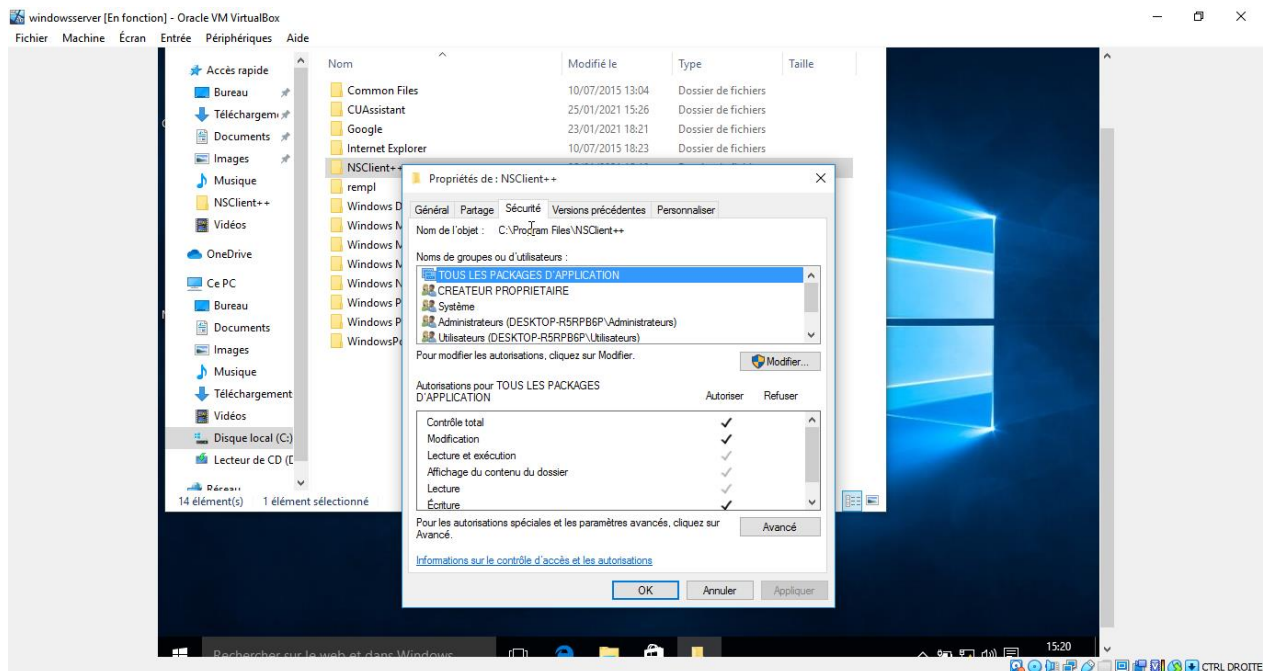


Figure 43: Installation de NSClient4

Dans A présent le fichier nsclient il faut activer les paramètres en les mettant à enabled de la section modules puis cliquer sur enregistrer pour sauvegarder les modifications.

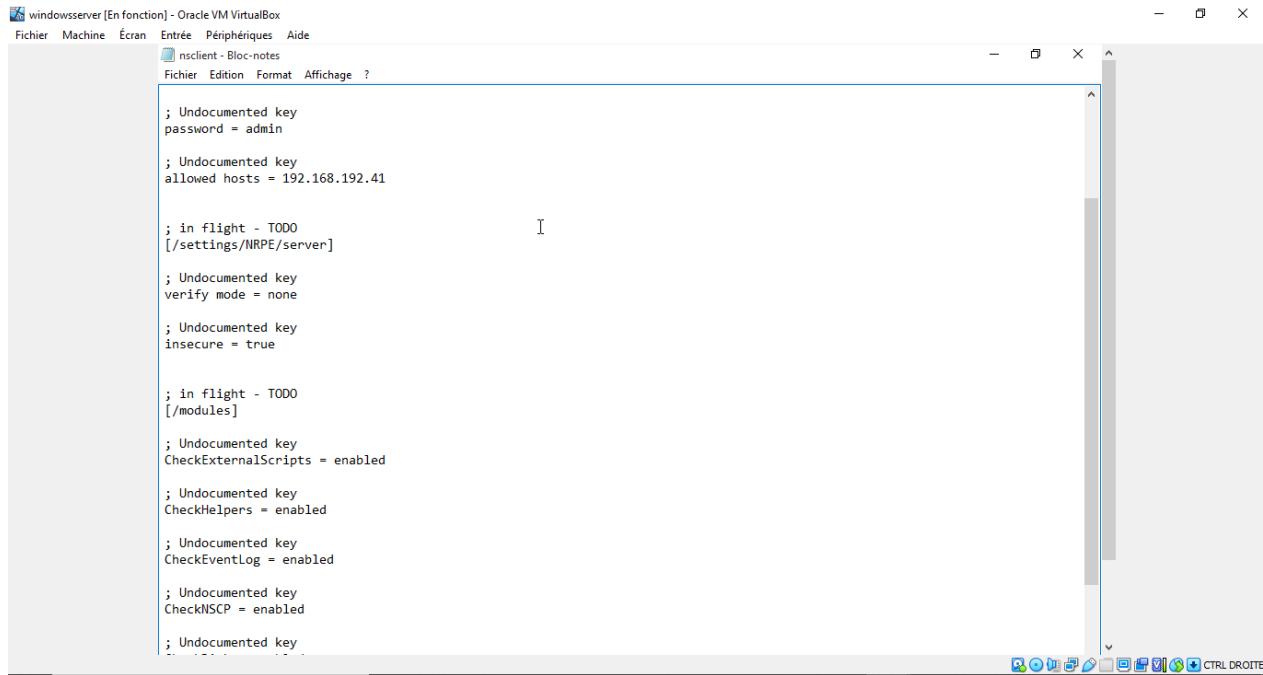


Figure 44:Le fichier NSCLient

Avant de lancer le service, il faut modifier le fichier de configuration nsclient.ini avec l'éditeur de texte classique de Windows. Il faut plus précisément dé-commenter quelques lignes nécessaires à son fonctionnement. Il faut aussi définir le mot de passe de la connexion entre les deux machines (password = nagios) et les utilisateurs aptes à accéder aux informations retournées (allowed hosts = 192.168.128.45/24, qui est l'adresse de notre serveur de supervision Nagios).

Et enfin il faut relancer le service pour prendre en compte les modifications.

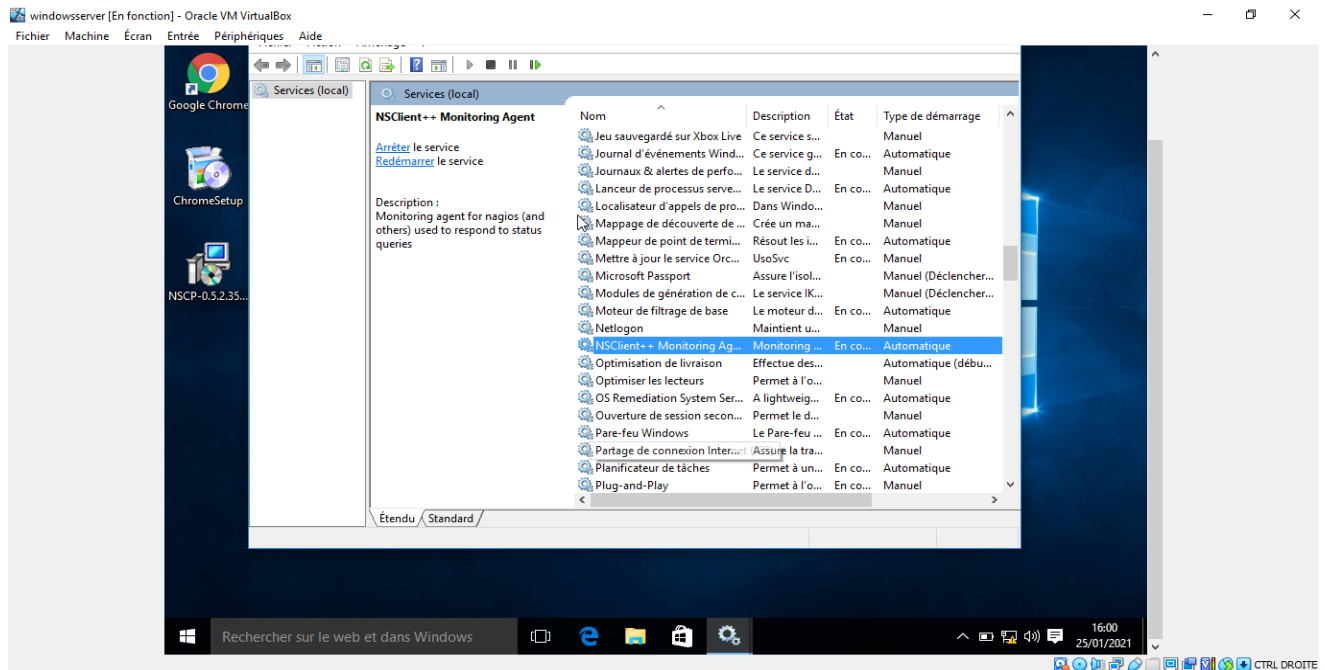


Figure 45: Redémarrage des services

## 2.2.4. Configuration et utilisation de Nagios

### 2.2.4.1. Accès à l'interface utilisateur

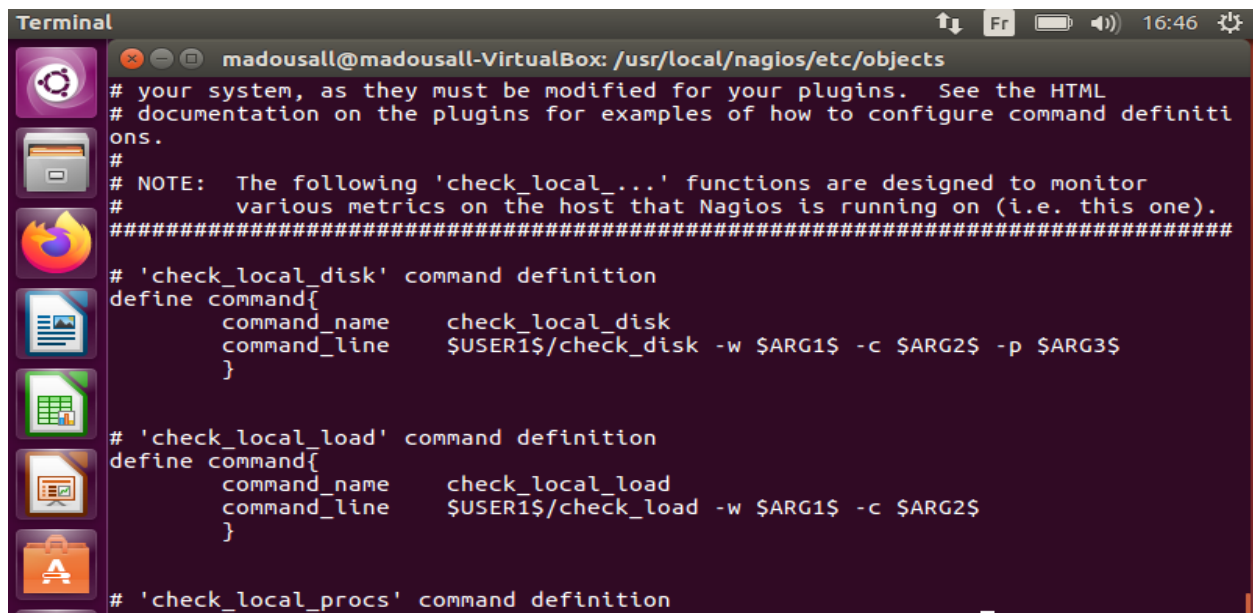
Pour accéder à l'interface web de Nagios, il suffit de visiter <http://localhost/nagios> à l'aide d'un navigateur.

L'utilisateur par défaut est 'nagiosadmin' et le mot de passe par défaut est 'admin'.

Un écran d'accueil permet alors de choisir entre différentes options pour configurer Nagios.

### 2.2.4.2. Configurer des machines ou hosts

Il faut maintenant déclarer la machine à travers son nom et son adresse IP dans le fichier de configuration `/usr/local/nagios/etc/objects/windows.cfg`

A terminal window titled 'Terminal' with a dark background and light text. The window shows the configuration of Nagios objects in the file /usr/local/nagios/etc/objects. The configuration includes comments about system modifications, a note about local monitoring functions, and three command definitions: 'check\_local\_disk', 'check\_local\_load', and 'check\_local\_procs'. The 'check\_local\_disk' command uses 'check\_disk' with arguments for warning, critical, and performance thresholds. The 'check\_local\_load' command uses 'check\_load' with arguments for warning and critical thresholds. The 'check\_local\_procs' command is partially visible at the bottom.

```
Terminal
madousall@madousall-VirtualBox: /usr/local/nagios/etc/objects
# your system, as they must be modified for your plugins. See the HTML
# documentation on the plugins for examples of how to configure command definitions.
#
# NOTE: The following 'check_local_...' functions are designed to monitor
# various metrics on the host that Nagios is running on (i.e. this one).
#####
# 'check_local_disk' command definition
define command{
    command_name    check_local_disk
    command_line     $USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$
}
# 'check_local_load' command definition
define command{
    command_name    check_local_load
    command_line     $USER1$/check_load -w $ARG1$ -c $ARG2$
}
# 'check_local_procs' command definition
```

Figure 46: la configuration de windowsserver

La figure ci-dessous présente les détails sur l'état des machines sur la page d'accueil de Nagios.

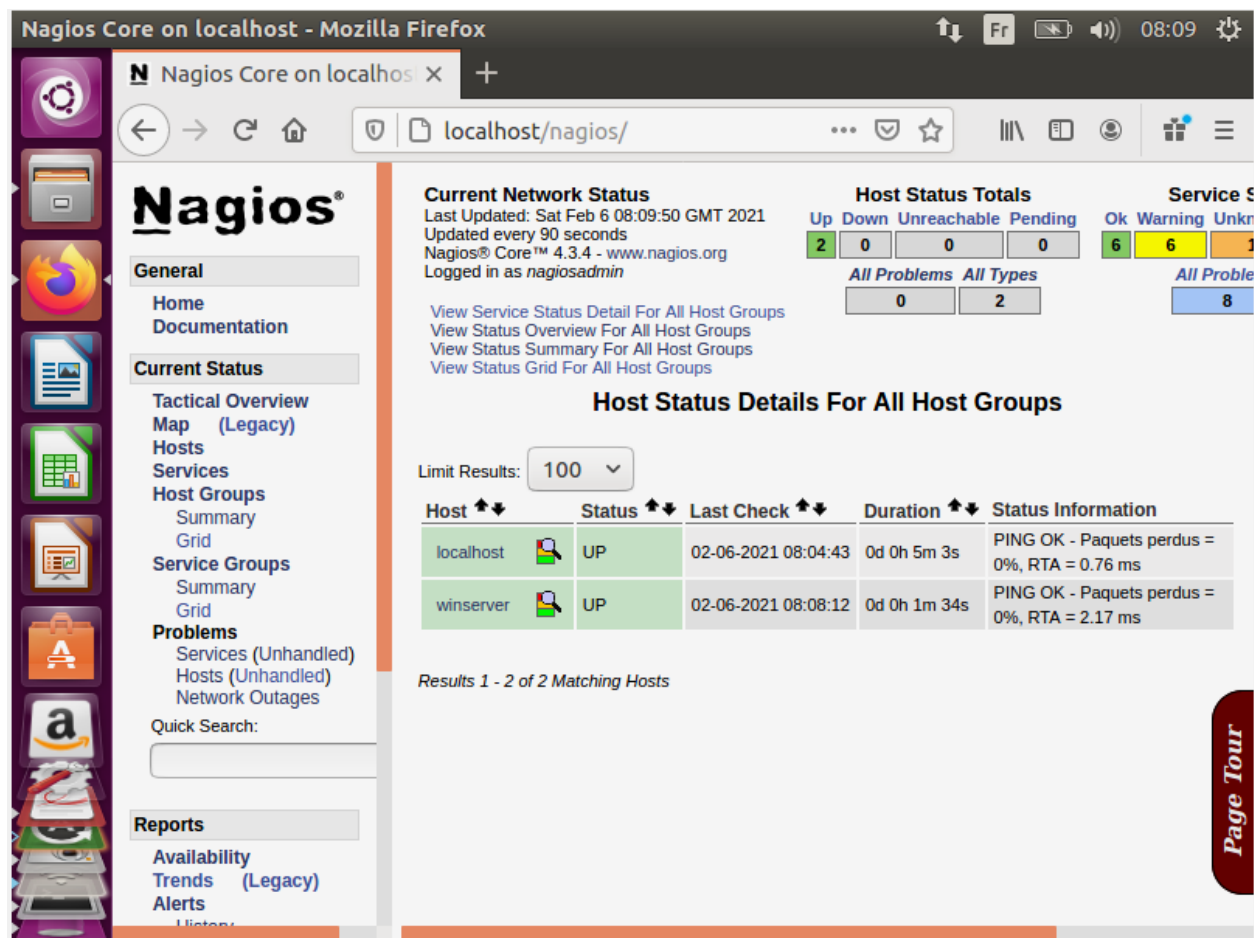


Figure 47: L'état du serveur Nagios et du serveur Windows en mode Up

Nous avons également configuré quelques services tels que PING, http, etc. sur le serveur et sur le client qui seront superviser par le serveur nagios. L'écran ci-dessous affiche l'état de ses services en cours d'exécution.

### 2.2.5. Tests de Nagios

Nous laissons le programme faire la collecte et le traitement des données pendant quelques minutes avant d'actualiser l'interface de Nagios.



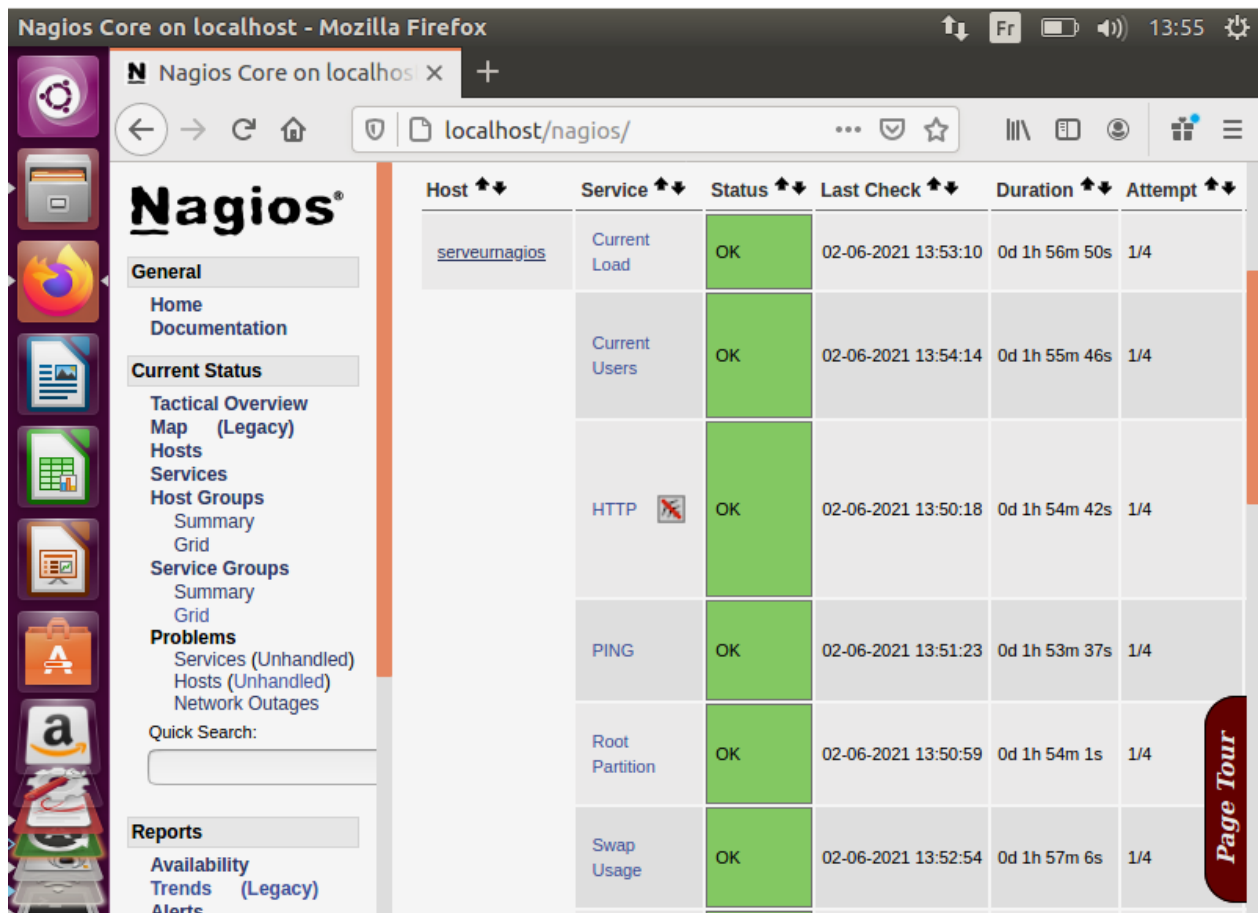


Figure 48: Les status du service de serveur Nagios

L'administrateur possède à une heure précise à travers Nagios quelques informations additionnelles l'aidant à mieux anticiper les pannes :

Pour le serveur Nagios, nous constatons comme illustré dans la figure précédente que :

- L'état de l'espace disque est : OK.
- L'état du service des utilisateurs courants est : OK.
- L'Etat du service HTTP est : OK
- L'état de l'utilisation de la mémoire virtuelle swap est : ok.
- L'état du service PING est OK.

Nous pouvons afficher la carte graphique du réseau à partir de menus **Map** de Nagios comme nous montre la figure suivante.



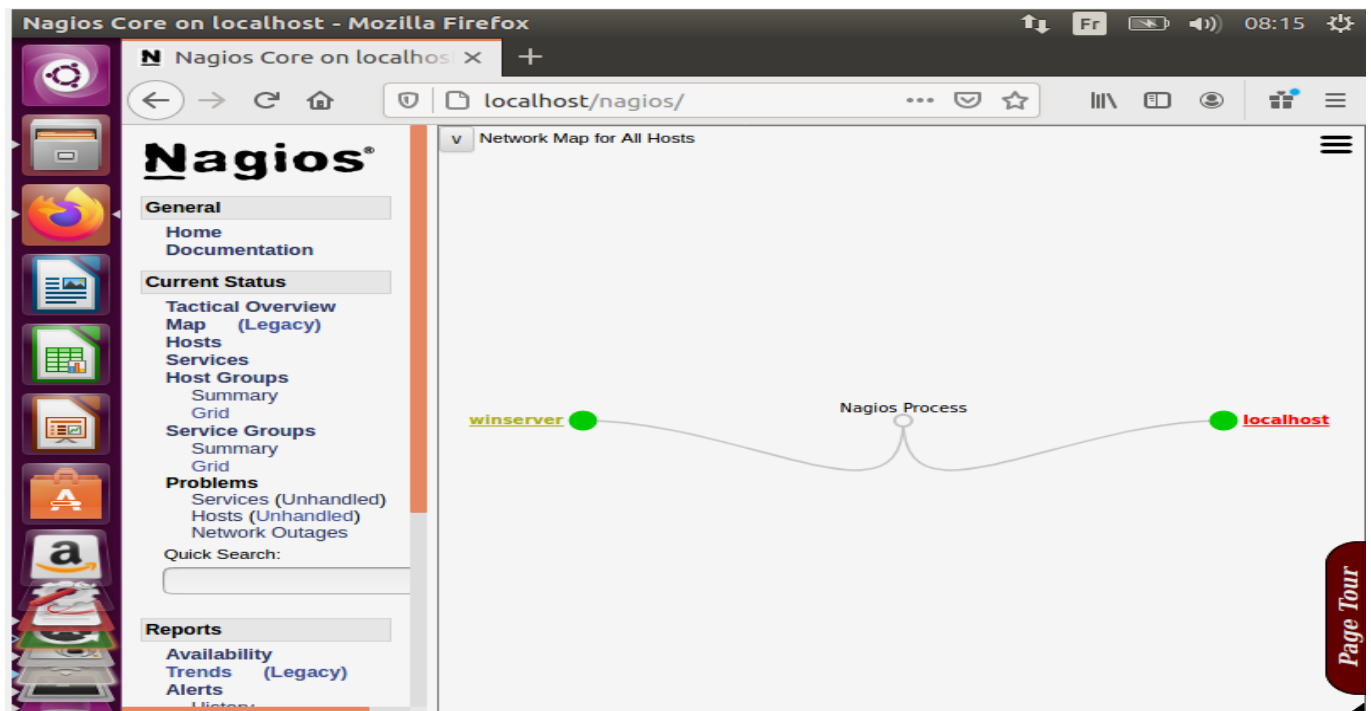


Figure 49: L'interface Map de Nagios

## CONCLUSION GENERALE

Au cours de ce mémoire, nous avons effectué une étude pour la mise en place d'une solution de supervision des équipements informatiques au sein de l'ESTM. Nous avons consacré la première partie du mémoire aux notions de base sur les réseaux informatiques et la supervision des réseaux, ensuite nous avons présenté et détaillé les différentes solutions permettant de mettre en place une supervision des réseaux en faisant une étude comparative entre ces différentes solutions, ce qui nous a permis d'avoir une idée précise et complète sur les solutions disponibles de la supervision et surtout de choisir celle qui nous convient le mieux. Puis nous avons procédé à sa mise en œuvre du système de supervision par le biais de la solution retenue qui est Nagios.

Ce projet étant très ambitieux, nous nous sommes vite heurtés à de nombreuses difficultés, tant sur le plan matériel que sur le plan réseau. Ces difficultés ont occupé en grande partie le travail de ce mémoire mais nous ont amené aussi à expérimenter le mode « investigation », primordial pour tout informaticien en devenir et qui se doit de trouver de solution à tout problème quelques soit sa complexité.

Ce projet a été pour nous une chance et une formidable opportunité de découvrir un environnement informatique nouveau, complexe et vaste, ce qui nous a permis d'acquérir de l'expérience en administration systèmes et réseaux Linux et d'approfondir nos connaissances dans le domaine de la supervision.

## WEBOGRAPHIE

1. <https://homputersecurity.com/25/01/2021/guide-dinstallation-dun-serveur-nagios-sur-ubuntu-16.04/> Consulté le 02/02/2021 à 12 :17
2. <https://fr.slideshare.net/christedykeihouad/projet-technique-licence-christedy> Consulté le 03/02/2021 à 13 :11
3. <https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/monitoring-windows.html> Consulté le 06/02/2021 à 10 :21
4. <https://wiki.monitoring-fr.org/nagios/nagios-nsclient-host> Consulté 03/02/2021 à 17:34
5. <https://web.univ-pau.fr/~cpham/MASIR/BIBLIO/DOC04-05/Nagios.pdf> Consulté le 07/02/2021 à 11 :26
6. <http://ditwww.epfl.ch/SIC/SA/SPIP/Publications/spip.php?article1450> Consulté le 08/02/2021 à 09 :21
7. <https://www.nsclient.org/download/> Consulté le 12/02/2021/ à 13 :09

# TABLE DES MATIERES

IN MEMORIUM.....	2
DEDICACES.....	3
REMERCIEMENTS .....	4
AVANT PROPOS .....	5
SOMMAIRE.....	6
GLOSSAIRE .....	11
RESUME .....	12
ABSTRACT .....	14
INTRODUCTION GENERALE.....	15
PARTIE I: CADRE METHODOLOGIQUE ET THEORIQUE.....	16
CHAPITRE I : CADRE METHODOLOGIQUE ET THEORIQUE .....	17
1.1    PRESENTATION DE L'ESTM .....	17
1.1.1    HISTORIQUE.....	17
1.1.2    FORMATIONS.....	17
1.1.3    MISSION.....	18
1.1.4    ORGANIGRAMME .....	19
1.1.5    Présentation de Réseaux Informatique de l'ESTM.....	19
1.2.    CONTEXT DU SUJET .....	21
1.3.    OBJECTIFS DU TRAVAIL.....	21
1.4.    LA METHODOLOGIE DU TRAVAIL .....	22
1.5.    PERTINENCE DU SUJET ET DELIMITATION DU CHAMP DE RECHERCHE .....	22
1.6.    DELIMITATION DU CHAMP D'ETUDE.....	22
1.7.    CRITIQUE DE L'EXISTANT .....	22
1.8.    SOLUTION PROPOSEE .....	23
CHAPITRE II : PRESENTATION DE RESEAUX INFORMATIQUES .....	24
2.1.    GENERALITE SUR LES RESEAUX .....	24
2.2.    CATEGORIES DES RESEAUX .....	24
2.2.1.    LES RESEAUX LOCAUX (LAN).....	24
2.2.2.    LES RESEAUX METROPOLITAINS (MAN). .....	25
2.2.3.    LES RESEAUX ETENDUS (WAN).....	26
2.2.4.    LES RESEAUX LOCAUX SANS FIL (Wireless, LAN ou WLAN) .....	26
2.2.5.    Les réseaux privés virtuels (VPN) .....	34
2.2.6.    LES TOPOLOGIES DE RESEAUX.....	34
2.2.7.    LES MODELES DE RESEAUX.....	39
2.2.8.    LES EQUIPEMENTS RESEAUX .....	42
PARTIE II : GENERALITES SUR LA SUPERVISION.....	43

CHAPITRE I : PRESENTATION DE LA SUPERVISION RESEAU .....	44
<b>1.1. PRINCIPE DE FONCTIONNEMENT DE LA SUPERVISION.....</b>	<b>44</b>
1.1.1. INTRODUCTION .....	44
1.1.2. LE ROLE DE LA SUPERVISION .....	44
1.1.3. TYPES DE SURVEILLANCE .....	45
<b>1.2. LES PROTOCOLES DE SUPERVISION.....</b>	<b>45</b>
1.2.1. LE PROTOCOLE ICMP .....	45
1.2.2. LE PROTOCOLE SNMP .....	46
<b>1.3. LES OUTILS DE SUPERVISIONS .....</b>	<b>48</b>
1.3.1. NAGIOS .....	48
1.3.2. ZABIX.....	49
1.3.3. CACTI .....	49
1.3.4. CENTREON .....	49
<b>1.4. ETUDE COMPARATIVE DES OUTILS DE SUPERVISION .....</b>	<b>50</b>
<b>1.5. SOLUTION RETENUE .....</b>	<b>51</b>
PARTIE III : PRESENTATION DE LA SOLUTION RETENUE.....	52
CHAPITRE I : PRESENTATION DE LA SOLUTION RETENUE .....	53
<b>1.1. PRESENTATION DE NAGIOS.....</b>	<b>53</b>
<b>1.2. LE FONCTIONNEMENT DE NAGIOS .....</b>	<b>53</b>
<b>1.3. ARCHITECTURE DE LA SOLUTION.....</b>	<b>53</b>
<b>1.4. LES FONCTIONNALITES DE NAGIOS .....</b>	<b>55</b>
<b>1.5. LES PLUGINS .....</b>	<b>55</b>
<b>1.6. LES FICHIERS DE CONFIGURATION.....</b>	<b>58</b>
CHAPITRE II : MISE EN ŒUVRE DE NAGIOS .....	59
<b>2.1. Environnement de travail.....</b>	<b>59</b>
2.1.1. Besoins matériels. ....	59
<b>2.2. Mise en place de la solution. ....</b>	<b>59</b>
2.2.1. Architecture de mise en œuvre.....	59
2.2.2. Installation de Nagios .....	60
2.2.3. Machine Windows : .....	65
2.2.4. Configuration et utilisation de Nagios.....	69
2.2.4.1. Accès à l'interface utilisateur .....	69
2.2.4.2. Configurer des machines ou hosts .....	69
2.2.5. Tests de Nagios.....	71
CONCLUSION GENERALE .....	74
WEBOGRAPHIE .....	75