

UNIVERSITE AUBE NOUVELLE



**INSTITUT SUPERIEUR D'INFORMATIQUE ET DE GESTION  
DEPARTEMENT HIGH-TECH**

**MÉMOIRE EN VUE DE L'OBTENTION DE LA LICENCE**

**DOMAINE : Sciences et Technologie**

**OPTION : Technologie des réseaux et systèmes**

**TITRE : ETUDE ET MISE EN PLACE D'UNE SUPERVISION  
INFORMATIQUE AVEC NAGIOS XI : cas de DANON'S GROUP**

Présenté le 22 Décembre 2021

Par : NEDUMLUBA-ANG Merveille

Jury

Président : Dr SAVADOGO Mahamadi

Membres :

**M. Mamadou SANGARE**, Enseignant à U-AUBEN

**M. YE Ange Prosper**, Ingénieur Informaticien à DANON'S GROUP

Année académique 2020 - 2021

Université AUBE NOUVELLE

Rectorat

OUAGADOUGOU

BURKINA FASO



### ATTESTATION DE CORRECTION

Par la présente attestation, le Président du jury et le rapporteur confirment que :

MEDUMLUBA -ANG..... Merveille..... Matricule : 1012308

qui a soutenu son mémoire de fin de cycle de licence en  
Technologies des réseaux et Systèmes.....

Le ....22.... Décembre..... 2021.....

sur thème : « Etude..... et..... mise..... en..... place..... d'une.....  
Supervision..... informatique..... avec..... Nagios..... XI..... Les..... de..... Dawn's..... Group»

a effectué les différentes corrections exigées par les membres du jury lors de la soutenance, conformément aux normes académiques en vigueur.

En foi de quoi, la présente attestation lui est délivrée pour servir et valoir ce que de droit.

Le Président du jury

(Titre, nom et prénom)

Dr SAVADOGO Rahamadi  
MA / UJKZ

Le rapporteur/Professeur de suivi

(Titre, nom et prénom)

SANGARÉ Namadou

Ouagadougou le ..12/01/2022.....TF

## SOMMAIRE

SOMMAIRE .....	
DEDICACE.....	II
REMERCIEMENT .....	III
AVANT - PROPOS .....	IV
LISTE DES SIGLES ET ABREVIATIONS .....	V
LISTE DES FIGURES .....	VI
LISTE DES TABLEAUX .....	VIII
RESUME.....	IX
ABSTRACT .....	X
INTRODUCTION GENERALE.....	1
PROBLEMATIQUE .....	2
CHAPITRE I : Présentation de la structure de formation et de la structure d'accueil .....	3
CHAPITRE 2 : Étude théorique et l'état de l'art et choix de l'outil .....	14
CHAPITRE 3 : Mise en place de la solution de supervision adoptée .....	38
CONCLUSION GENERALE .....	62
BIBLIOGRAPHIE .....	XII
WEBOGRAPHIE.....	XIII
TABLE DES MATIERES .....	XIV

## DEDICACE

*Je dédie ce mémoire*

*A mes chers parents, c'est principalement grâce à eux que je suis arrivé à ce niveau aujourd'hui. Ils m'ont donné la vie, ils m'ont éduqué et ils m'ont appris à poursuivre mes objectifs et à les atteindre. Ils ont toujours cru en moi, en ce que j'allais accomplir même si des fois, je n'y croyais plus.*

*A ma mère NODJIGOTO DATOLUOMBAYE qui m'a toujours encouragé dans mes études, et m'a toujours apporté son amour et son soutien infaillible.*

*A la mémoire de mon père, que la terre lui soit légère et que son âme repose en paix.*

*A mon tuteur Bantar KOROUNAI qui m'a soutenu dans mes études dès mon enfance.*

*A mon oncle DJIMADOUM Jean-Pierre qui m'a toujours soutenu malgré ses occupations.*

*A ma tante MELOM Rejeanne LE DATOLOUMBAYE grâce à ses précieux conseils et appuis, j'ai pu exceller dans le domaine de l'informatique.*

*A mon petit frère GHISLAIN et à ma petite sœur JUVANIE qui ont été présents pour moi, je ne vous souhaite que du meilleur et je vous garderai toujours dans mon cœur.*

*A mon encadreur, mon maître de stage et mon professeur de suivi.*

*A tous mes amis.*

## REMERCIEMENT

Le présent document n'aurait pas vu le jour sans la contribution de certaines personnes que nous tenons à remercier :

- ✚ Je rends grâce à Dieu pour tout et pour sa présence dans ma vie, qui m'a permis de maintenir le cap et de ne jamais abandonné ;
- ✚ Monsieur Mamadou SANGARE, qui a accepté de nous encadrer et pour les nombreuses et systématiques corrections, ses orientations, ses conseils, ses remarques et sa disponibilité ;
- ✚ Monsieur YE Ange Prosper, pour ses précieux conseils, remarques et recommandations ;
- ✚ Monsieur DANON Narcisse, Directeur Général de DANON'S GROUP et tout le personnel pour leur accueil chaleureux, leur sympathie et leur encouragement ;
- ✚ A tout le corps professoral de l'université U-AUBEN pour toutes les connaissances et pratiques qu'ils m'ont transmises durant mes trois années de formation.
- ✚ A toute ma famille, qui m'a donné tout le nécessaire pour la réussite de ma formation ; elle a su me motiver lorsque le besoin se faisait ressentir et elle a toujours cru en moi ;

## AVANT - PROPOS

D'après les exigences du système de formation de l'Université Aube Nouvelle, tout étudiant en année de licence doit passer un stage de formation en entreprise dans le but de mettre en pratique les connaissances théoriques acquises durant sa formation universitaire et de rédiger un rapport de stage qui fera l'objet d'une soutenance publique devant un jury. C'est ainsi que nous avons eu à passer trois (3) mois de stage à DANON'S GROUP, qui a bien voulu nous accueillir en son sein et nous aider à parfaire ce projet.

Nous étions appelés à mener des recherches sur un thème retenu par nos différents maîtres de mémoire afin de pouvoir résoudre un problème concret.

Ce travail nous a permis d'appréhender et d'étudier l'un des domaines de l'informatique, la supervision informatique. La revue de littérature nous a permis d'élargir nos connaissances sur le sujet de notre thème.

Nous espérons pouvoir apporter un point de vue différent qui pourra être utile lors de l'établissement d'un projet dans ce domaine.

Nous retirons de ce travail, la satisfaction d'avoir beaucoup appris sur ce sujet et d'avoir participé à la recherche dans un domaine dont l'utilité est incontestable.

## LISTE DES SIGLES ET ABREVIATIONS

<b>ACL</b>	Access Control List
<b>ALC</b>	Americain Language Center
<b>ADSL</b>	Asymmetric Digital Subscriber Line
<b>API</b>	Interface de programmation
<b>BDD</b>	Base De Données
<b>CAMES</b>	Conseil Africain et Malgaches pour l'Enseignement Supérieur
<b>CCI</b>	Centre de Carrière et de l'Innovation
<b>CMBD</b>	Configuration Management DataBase
<b>CPU</b>	Central Processing Unit
<b>D'G</b>	Danon's Group
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DNS</b>	Domaine Name System
<b>GLPI</b>	Gestion Libre de Parc Informatique
<b>GPL</b>	General Public License
<b>HDD</b>	Hard Disk Drive
<b>HTTP</b>	HyperText Transfer Protocol
<b>ICMP</b>	Internet Control Message Protocol
<b>ISO</b>	International Organization for Standardization
<b>ISIG</b>	Institut Supérieur de l'Informatique et de Gestion
<b>IT</b>	Infrastructure Informatique
<b>ITIL</b>	Information Technology Infrastructure Library
<b>ITRI-GEC</b>	Institut de Technologie et de Recherche Industrielle et Génie Civil
<b>J2SE</b>	Java 2 Platform Standard Edition
<b>JMX</b>	Java Management Extentions
<b>MIB</b>	Management Information Base
<b>MRTG</b>	Multi Router Traffic Grapher
<b>NMAP</b>	Network Mapper
<b>NMS</b>	Network Management Station
<b>NRPE</b>	Nagios Remote Plugin Executor
<b>NSCA</b>	Nagios Service Check Acceptor
<b>PDU</b>	Protocol Data Unit
<b>SMI</b>	Structure of Management Information
<b>SMS</b>	Short Message Service
<b>SNMP</b>	Simple Network Management Protocol
<b>SSH</b>	Secure Shell
<b>SSL</b>	Secure Sockets Layer
<b>U-AUBEN</b>	Université Aube Nouvelle
<b>UDP</b>	User Datagram Protocol
<b>UFR</b>	Unité de Formation et de Recherche
<b>WBEM</b>	Web Based Entreprise Management
<b>WMI</b>	Windows Management Instrumentation

## LISTE DES FIGURES

<b>Figure 1 :</b> récapitulatif graphique de l'organigramme de DANON'S GROUP .....	9
<b>Figure 2 :</b> Equipements terminaux .....	11
<b>Figure 3 :</b> Équipements intermédiaires .....	12
<b>Figure 4 :</b> Supports de communications.....	12
<b>Figure 5 :</b> Architecture du réseau informatique de DANON'S GROUP .....	13
<b>Figure 6 :</b> Supervision active.....	18
<b>Figure 7 :</b> Supervision passive .....	19
<b>Figure 8 :</b> Architecture SNMP .....	23
<b>Figure 9 :</b> fonctionnement SNMP .....	24
<b>Figure 10 :</b> Interface web de Nagios XI .....	32
<b>Figure 11 :</b> Supervision active avec NRPE .....	34
<b>Figure 12 :</b> Supervision active avec NSCA.....	35
<b>Figure 13 :</b> Schéma comparatif NRPE-NSCA .....	36
<b>Figure 14 :</b> Importation de Nagios XI .....	40
<b>Figure 15 :</b> Nom de la machine et vérification des prérequis.....	40
<b>Figure 16 :</b> Importation de la machine .....	41
<b>Figure 17 :</b> Interface du serveur Nagios XI.....	41
<b>Figure 18 :</b> Connexion à Nagios XI .....	42
<b>Figure 19 :</b> Configuration de Nagios XI (Setup 1).....	42
<b>Figure 20 :</b> Configuration de Nagios XI (Setup 2).....	43
<b>Figure 21 :</b> Fin de l'installation .....	43
<b>Figure 22 :</b> Connexion au portail .....	44
<b>Figure 23 :</b> Contrat de licence .....	44
<b>Figure 24 :</b> Page d'accueil de Nagios XI .....	45
<b>Figure 25 :</b> Vérification de l'adresse IP .....	46
<b>Figure 26 :</b> configuration de l'adresse .....	46
<b>Figure 27 :</b> configuration de l'interface <i>enp0s17</i> .....	47
<b>Figure 28 :</b> Choix de la configuration IPv4.....	47
<b>Figure 29 :</b> Fixation de l'adresse IP .....	48
<b>Figure 30 :</b> Mise à jour de l'adresse IP .....	48
<b>Figure 31 :</b> Test vers Google .....	49
<b>Figure 32 :</b> Démarrage de l'installation de NCPA .....	50
<b>Figure 33 :</b> Insertion de l'API .....	50

<b>Figure 34 :</b> Démarrage de l'installation .....	51
<b>Figure 35 :</b> Fin de l'installation.....	51
<b>Figure 36 :</b> Configuration de Windows.....	52
<b>Figure 37 :</b> Les seuils d'alertes.....	52
<b>Figure 38 :</b> Paramètre de base pour pouvoir superviser .....	53
<b>Figure 39 :</b> Configuration terminée.....	53
<b>Figure 40 :</b> Connexion au routeur .....	55
<b>Figure 41 :</b> accès à l'onglet SNMP .....	55
<b>Figure 42 :</b> activation du protocole SNMP .....	56
<b>Figure 43 :</b> choix du type d'équipement à superviser .....	57
<b>Figure 44 :</b> Renseignement de l'adresse IP .....	57
<b>Figure 45 :</b> Nom du routeur.....	58
<b>Figure 46 :</b> Fin de la configuration.....	58
<b>Figure 47 :</b> Configuration du paramètre de messagerie .....	59
<b>Figure 48 :</b> Envoi de message de test .....	60
<b>Figure 49 :</b> Vérification de la réception du mail de test.....	60

## LISTE DES TABLEAUX

<b>Tableau 1:</b> Comparaison des outils de supervision.....	28
<b>Tableau 2:</b> Correspondance de retour-état .....	31
<b>Tableau 3 :</b> Prérequis installation de Nagios XI .....	39
<b>Tableau 4 :</b> Caractéristiques du Mikrotik.....	54
<b>Tableau 5 :</b> Devis estimatif du matériel .....	61

## RESUME

Pour assurer la disponibilité permanente de leur infrastructure informatique, les entreprises ont rapidement compris que la supervision était devenue une ressource clef. Reçues en Avril 2021, DANON'S GROUP nous a confié la mise en place d'un outil de supervision de son système d'information à travers un stage de 03 mois, c'est une solution qui va permettre la supervision complète de son parc informatique. Ainsi la solution NAGIOS XI a été retenue. Nous l'avons choisi après une étude comparative des outils de supervision qu'on trouve sur internet. Certains critères qui ont considérés sont : logiciel libre, grandes performances, adaptabilité et fonctionnalités. L'outil déployé permet de contrôler tout type de système d'information. En somme, l'objectif de ce stage est d'éviter les arrêts de service, détecter et prévenir les pannes.

**Mots clés :** Réseau, supervision, SNMP, Nagios XI

## ABSTRACT

To ensure the permanent availability of their IT infrastructure, companies quickly realized that supervision had become a key resource. Received in April 2021, DANON'S GROUP entrusted us with the implementation of a monitoring tool for its information system through a 03-month internship, it is a solution that will allow the complete supervision of its IT equipment. The NAGIOS XI solution was therefore chosen. We chose it after a comparative study of the supervision tools found on the internet. Some criteria that have been retained are: free software, high performance, adaptability and functionalities. The deployed tool makes it possible to control any type of information system. In short, the objective of this internship is to avoid downtime, detect and prevent breakdowns.

**Key words :** Network, monitoring, SNMP, Nagios XI

## INTRODUCTION GENERALE

Les entreprises quel que soit leur domaine veulent toujours à être dans le centre de la concurrence économique et à garder leur bonne réputation. Pour cela elles donnent beaucoup d'importance à leur système informatique avec toutes ses composantes, puisque le système d'information et de communication est actuellement la clef de voute de l'entreprise. Il permet de collecter, de traiter, de communiquer toute les informations stockées, archivées et générées par l'entreprise. Toutes ces informations sont capitales pour sa survie et représentent son histoire et son savoir-faire.

Vu que le système informatique est au cœur des activités d'entreprise, sa maîtrise devient primordiale, puisque, il doit fonctionner pleinement et en permanence pour garantir la fiabilité et l'efficacité exigées. D'autre part, les problèmes liés au système informatique tels que les défaillances, les pannes, les coupures et les différents techniques doivent être réduits, du fait qu'une indisponibilité du système ou du réseau peut causer des pertes considérables.

Afin de minimiser le nombre de ces pertes, une sorte de surveillance et de contrôle s'avère obligatoire ; c'est ainsi que la notion de la « *supervision informatique* » a vu le jour et est devenue une tâche vitale pour tout système informatique.

Notre travail consiste à la mise en œuvre et la configuration d'un outil de supervision réseau. Pour bien comprendre le travail et bien cerner les problèmes techniques, nous avons réalisé un stage de trois (03) mois au niveau de DANON'S GROUP, une structure de prestation de service spécialisée dans le numérique. Ceci nous a permis d'établir la problématique qui consiste en la détection de pannes et éviter la perte du temps et proposer une solution de supervision réseau à base de l'outil Nagios XI.

Pour bien présenter notre travail, notre mémoire sera structuré sur trois (03) chapitres, comme suit :

Dans le premier chapitre, nous procéderons à la présentation de la structure de formation et celle de l'accueil ainsi que le réseau informatique de l'entreprise; par la suite, l'étude théorique et l'état de l'art, ainsi que le choix de l'outil feront l'objet du deuxième chapitre. En troisième lieu, nous mettrons en place notre solution.

Finalement, nous terminerons notre mémoire par une conclusion générale qui récapitulera les principales observations concernant l'évolution du travail et nous indiquons également comment les travaux réalisés tout au long de ce mémoire pourraient être améliorés.

## PROBLEMATIQUE

DANON'S GROUP est une structure de prestation de service fondée en 2015, ayant son siège à Ouagadougou au Burkina Faso, spécialisée dans le numérique, offrant des services telles que réseaux et télécommunications, développement numérique, BTP, mines et carrières ...

DANON'S GROUP dans sa volonté d'améliorer le fonctionnement de ses équipements, s'est dotée de la solution de supervision CACTI qui surveille actuellement les links vers les différentes entreprises. Cependant étant donné le nombre important de ces abonnés, DANON'S GROUP veut s'assurer que l'outil actuel est celui qui répond au mieux à son infrastructure informatique. C'est dans ce contexte que nous avons effectué notre stage d'ingénieur de travaux à DANON'S GROUP. Notre intérêt vers la supervision et notre volonté de découvrir le monde de l'entreprise nous ont conduit à ce choix. Le travail au cours de notre stage s'est porté essentiellement sur l'étude de la solution mise en place au sein de l'entreprise (le Dude), afin d'optimiser le système de surveillance au sein de l'entreprise.

Cependant il est important de s'interroger sur quelques points suivants :

- Quelle solution afin d'optimiser la solution déjà mise en place ?
- Avoir une vue globale sur le fonctionnement et les problèmes pouvant survenir sur le réseau ?
- Comment disposer des indicateurs sur les performances de son architecture ?
- Comment être informé lorsqu'un client n'a pas la connexion ? Ou lorsqu'un problème survient sur les équipements ?
- Comment avoir une vue sur l'ensemble des équipements interconnectés ?

Tant de questions auxquels il faudra apporter des réponses afin de mener à bien notre projet.

# CHAPITRE I : Présentation de la structure de formation et de la structure d'accueil

## Introduction

Dans ce premier chapitre, nous présenterons les différentes structures qui nous ont permis de réaliser ce projet. Il s'agit de présenter brièvement la structure de formation (U-AUBEN) et les moyens mis en place pour assurer la formation des apprenants ; ensuite, nous présenterons la structure d'accueil (DANON'S GROUP, entreprise dans laquelle nous avons mis en pratiques nos connaissances théoriques) et les différentes missions qu'elle s'est fixée, enfin, présenter l'architecture du réseau informatique de l'entreprise.

### I. Structure de formation (Université Aube Nouvelle)

#### I.1. présentation générale

L’Institut Supérieur d’Information et de Gestion (ISIG) est un grand établissement privé d’enseignement supérieur à caractère professionnel. Créé en octobre 1992 par M. Isidore Gnaton KINI agréé par l’état par arrêté 2010-335/MSSERS/ETFP/CAB de l’octobre 2010 portant modification des statuts de l’ISIG INTERNATIONAL et arrêté 2010-356/MESSERS/ETFP/CAB du 11 octobre 2010 portant d’ouverture de cycles de filière d’étude et délivrance de diplômes à l’ISIG INTERTIONAL. C’est au 17 février 2012 qu’ISIG INTERNATIONAL devient université AUBEN NOUVELLE (U-AUBEN) par autorisation № 2010-0000344/MESSERS/SG/DERSR/DIEPER.

Avec plus de cinq milles étudiants de dix-huit nationalités différentes, U-AUBEN est une référence dans le domaine de l’enseignement supérieur et de la recherche scientifique. Elle compte deux (02) campus dont l’un à Ouagadougou et l’autre à Bobo-Dioulasso au Burkina Faso.

#### I.2. Objectifs

Dans le souci de mettre sur le marché de l’emploi des travailleurs bien formés et très compétents, l’université Aube Nouvelle propose des formations pluridisciplinaires de haut niveau dans les domaines suivants :

- Science économiques de gestion ;
- Environnement et développement durable ;
- Science juridiques et politiques ;
- Science des techniques comptables et financières ;

- Science et technologie.

Aussi dans la même optique de formation, Aube Nouvelle a signé de nombreux partenariats avec des université et institutions d'enseignement supérieur, scientifiques et de recherche, aussi bien en Amérique, en Europe, en Asie qu'en Afrique. Ainsi, chaque année, plus de vingt (20) missions d'enseignement sont programmées à Aube Nouvelle. Cela lui permet d'avoir les chiffres clés suivants :

- Plus de 4000 étudiants ;
- Plus de 28 nationalités ;
- 25 diplômes homologués par le CAMES ;
- Plus de 5000 diplômés sur le marché.

Pour la formation des étudiants de l'Université AUBE NOUVELLE dispose des trois instituts à savoir :

- L'Institut Supérieur d'Informatique et de Gestion (ISIG International);
- L'Institut de Technologie et de Recherche Industrielle et Génie Civil (ITRI-GEC) ;
- L'institut des métiers.

Quatre unités de formation et de recherche (UFR) à savoir :

- L'UFR Sciences et Technique ;
- L'UFR Sciences Économiques et de Gestion ;
- L'UFR Sciences Juridiques et Politique ;
- L'UFR des Langues, Lettre, Sciences Humaines et Sociales.

Quatre centres à savoir :

- The Americain Language Center (ALC) ;
- Le laboratoire de langue (TOEIC) ;
- L'académie CISCO ;
- Le centre CCI.

Et enfin l'école doctorale. Il compte deux campus, Ouagadougou et Bobo Dioulasso, tous deux délivrant le DUT, la Licence, le Master et le Doctorat. Le siège de l'U-AUBEN est situé à Ouagadougou la capitale du Burkina Faso au cœur du quartier 1200 logements.

### I.3. Formations

L’U-AUBEN offre les formations suivantes :

- HIGH TECH
  - 1. Technologie des réseaux et systèmes ;
  - 2. Technologie du génie Informatiques ;
  - 3. Génie Électrique.
- BUSINESS SCHOOL
  - 1. Marketing et Gestion Commercial ;
  - 2. Transport et Logistique ;
  - 3. Gestion de Projet ;
  - 4. Gestion des Ressources Humaines ;
  - 5. Finance-Comptabilité ;
  - 6. Assistant de Direction Bilingue ;
  - 7. Assurance-Banque ;
  - 8. Finance Banque.
- ITRI-GEC
  - 1. Électricité et Énergie Renouvelable ;
  - 2. Génie Civil : Construction ;
  - 3. Génie Civil : Architecture et Urbanisme.
- UFR/SEG
  - 1. Analyse Économique ;
  - 2. Management International.
- UFR/SJP
  - 1. Droit Public ;
  - 2. Droit Privé.
- UFR/ST
  - 1. Géologie Appliquée et Amines ;
  - 2. Bio Analyse et Contrôle Qualité ;
  - 3. Industrie Agroalimentaire ;
  - 4. Agronomie ;
  - 5. Eau, Hygiène et Assainissement (EHA).

- UFR/LLSHS
  - 1. Traduction et Interprétariat : Anglais
  - 2. Sociologie Urbaine et Rurale.
- SCIENCE ET TECHNIQUE DE L'INFORMATION ET DE LA COMMUNICATION
  - 1. Communication pour le Développement ;
  - 2. Communication des Organisations ;
  - 3. Journalisme.
- FORMATION A DISTANCE (E-LEARNING)
  - 1. Licence en Finance Comptabilité ;
  - 2. Licence en Gestion de projet (GP) ;
  - 3. Licence en GRH ;
  - 4. Licence en Communication ;
  - 5. Licence en Marketing ;
  - 6. Ingénierat.
- ADRESSES UTILES
  - Direction Générale : [auben.direction@u-auben.org](mailto:auben.direction@u-auben.org), +226 25 36 24 99
  - Direction de la Scolarité : [auben.ds@u-auben.org](mailto:auben.ds@u-auben.org), +226 25 36 24 99
  - École Doctorale : [ecoledoctorale@u-auben.org](mailto:ecoledoctorale@u-auben.org), +226 25 36 39 77
  - [e-learning@u-auben.org](mailto:e-learning@u-auben.org), +226 25 36 24 99
  - Centre Americain de langue : [alc-ouaga@u-auben.org](mailto:alc-ouaga@u-auben.org), +226 25 36 39 34
  - [alc-bobo@u-auben.org](mailto:alc-bobo@u-auben.org), +226 20 98 04 42

#### I.4. La filière Technologie des réseaux et systèmes

La filière Technologie des réseaux et systèmes est l'une des premières filières à U-AUBEN. Elle offre une formation de qualité allant dans le sens des systèmes de réseaux et des télécommunications. Elle forme des ingénieurs de travaux et des ingénieurs de conception (Master I et II). C'est l'une des filières à posséder un laboratoire pour des pratiques comme les TP en électronique analogique, numérique et construction électronique. Nous avons été formés dans cette prestigieuse université dans un cadre studieux et accueillant.

## II. Structure d'accueil (DANON'S GROUP)

### II.1. Présentation générale

Structure relativement jeune, DANON'S GROUP est le cadre dans lequel la présente étude a été conduite, ainsi nous nous faisons un devoir de la présenter dans cette partie.

Fondée en 2015 par un groupe de jeunes passionnés de l'informatique, par Arrêté N°BFA2018M8975, DANON'S GROUP est une structure de prestation de services, spécialisée dans le numérique. Jeunes, dynamiques et enthousiastes, les promoteurs de cette entreprise partagent la même vision d'une Afrique qui bouge grâce aux solutions numériques. Ayant son siège à Ouagadougou au Burkina Faso, cette entreprise dispose d'un réseau de partenaires dans plusieurs pays du continent (Bénin, Togo, Côte d'Ivoire, Tchad, Guinée Équatoriale, etc.) afin de rapprocher au mieux ses services de ses clients. En termes de ressources humaines, cette société met au service de ses partenaires et/ou clients des ingénieurs hautement qualifiés et expérimentés dans les domaines d'activités suivants :

- Télécommunication ;
- BTP, mines et carrières ;
- Énergies ;
- Immobiliers ;
- Développement numérique.

DANON'S GROUP est un regroupement des entreprises évoluant dans des secteurs d'activités divers. Elle est composée de jeunes dynamiques et motivés issus de grandes écoles de formation. Pour faire face aux problèmes du sous-développement qui fait des ravages dans le continent africain, DANON'S GROUP met au cœur de son métier, la transformation de l'économie à travers le numérique.

#### II.1.1. Visions

DANON'S GROUP veut se positionner comme la première unité industrielle de référence au Burkina Faso et dans la sous-région en proposant des produits de qualité à des prix compétitifs.

A court terme, elle entend conforter ses parts dans le marché domestique et les étendre progressivement dans la sous-région sous sa propre marque.

#### II.1.2. Missions

DANON'S GROUP se veut être un acteur majeur dans le développement du continent en apportant un service de qualité pour accompagner ses partenaires et collaborateurs à renforcer et développer leurs structures dans le domaine des communications et télécommunication. A

long terme, cette entreprise envisage de se positionner comme un leader du développement en Afrique.

A travers les différents domaines où elle opère, elle accompagne des structures privées et des institutions de l'État vers un développement sûre et accès sur le numérique et les différentes techniques d'informations et de communications.

Le challenge que se lance aujourd'hui cette structure est d'apporter son expertise et ses compétences dans le domaine des BTP, mines et carrières car elle reste convaincue que le développement passe d'abord par des voies de communication sûres et fiables. Pour les promoteurs de DANON'S GROUP, il n'est pas question pour eux de demeurer en marge de l'édification de leur continent. Pour eux, apporter leur modeste contribution en mettant à la disposition de leurs partenaires des BTP des matières premières de qualité répondant aux exigences requises du point de vue qualité/prix.

Ainsi, les missions que s'est assignées DANON'S GROUP peut se résumer en ces points suivants :

- Procurer un service de qualité ;
- Répondre aux besoins changeants du marché ;
- Créer des valeurs sociales additionnées au maintien d'un haut niveau de qualité ;
- Construire un confort pour la qualité et maintenir une relation de longue durée.

#### **II.1.3. Valeurs**

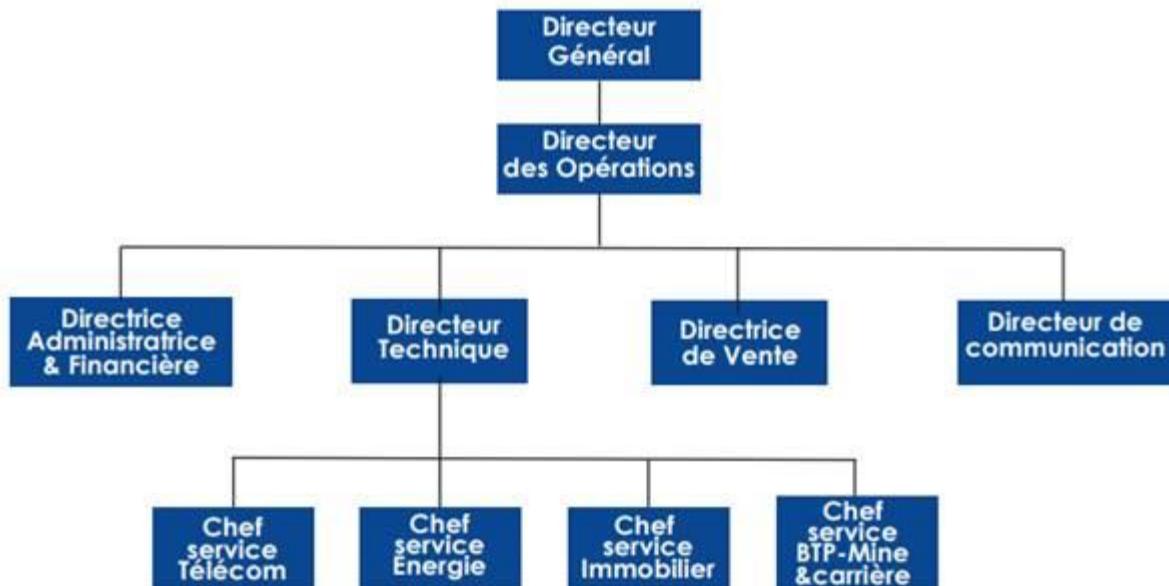
Les valeurs éthiques prônées par DANON'S GROUP sont :

- Le respect de la personne humaine ;
- La transparence à tous les niveaux dans le travail ;
- La culture de la bonne performance ;
- La rigueur dans le travail ;
- La culture du travail bien fait ;
- Le sens de l'innovation et du partage.

#### **II.1.4. Organisation et fonctionnement**

La société DANON'S GROUP dispose d'une structure organisationnelle qui permet de mener ses activités en fonction des ressources qui lui sont alloués en vue d'atteindre les objectifs qu'elle s'est fixée. Cette structure organisationnelle se compose d'une Direction Générale (DG), d'un Directeur Opérationnel (DO), d'une Direction Administrative et Financière (DAF),

d'une Direction Commerciale (DC), d'une Direction de Vente (DV), et d'une Direction Technique (DT).



**Figure 1** : récapitulatif graphique de l'organigramme de DANON'S GROUP

Pour un fonctionnement harmonisé de l'entreprise, chaque employé s'est vu définir son poste. Ainsi chaque poste a des attributs suivants :

- **Président Directeur Général** : il est le premier responsable de la société. A ce titre, il a pour mission de fixer les objectifs généraux de l'entreprise et les axes de développement, de coordonner et de superviser l'ensemble des activités de l'entreprise ;
- **Directeur des Opérations** : deuxième personnalité de l'entreprise, il s'occupe de toutes les affaires courantes de l'organisation en cas de nécessité, consulte le Directeur Général pour savoir les directives à donner et à la conduite à tenir face à une situation donnée ;
- **Directrice Administratif et Financier** : a pour rôle de superviser toutes les transactions financières effectuées au sein de l'entreprise, de faire les analyses financières des résultats comptables obtenus après un exercice ;
- **Directeur Commercial et communication** : a pour mission d'établir les prévisions de ventes et d'élaborer des stratégies lui permettant d'atteindre ses objectifs ;
- **Community Manager** : en charge des situations délicates, il est la personne en charge de gérer aussi bien les conflits internes entre le personnel que ceux de l'entreprise avec

les clients, partenaires et les autorités étatiques. Par ailleurs, il officie comme le fournisseur de la société en consommables et ressources humaines ;

- **Informaticiens** : a pour mission de garantir l'intégrité, la sécurité, l'assistance, le développement et la sauvegarde de toutes les données informatiques de l'entreprise ; d'apporter un entretien et une maintenance du parc informatique ; de faire des propositions et des choix techniques sur l'achat du matériel informatique.

En somme, il a pour rôle de pérenniser tout le système informatique de l'entreprise ;

- **Secrétaire** : a en charge l'accueil des visiteurs de l'entreprise ; la gestion des correspondances téléphoniques et des courriers ;
- **Livreur** : assure la livraison des commandes des clients ; sert d'agent de liaison ; etc.

#### **II.1.5. Produits et services de DANON'S GROUP**

Ayant constaté un vide numérique pour solliciter des services à distance, les premiers responsables de DANON'S GROUP ont eu à cœur de combler ce vide en concevant la plateforme RESERVERTOUT. Cet outil digital permet de faire des réservations en ligne. En effet, cette plateforme permet de faire des réservations de chambre d'hôtel, de réserver des résidences d'hôtes, de réserver des tables et de passer des commandes dans un restaurant et d'être livré au lieu indiqué, et de louer de voitures. Cet outil est particulièrement utile à un touriste qui débarque pour la première fois à Ouagadougou ou qui envisage de s'y rendre. La plateforme est disponible gratuitement sur Smartphone et tablette sous forme d'application et constitue un outil très pratique pour un professionnel, un homme d'affaire ou un touriste amoureux du Burkina Faso.

En dehors de la plateforme **RESERVERTOUT**, DANON'S GROUP a mis en place **Allo Lavage**, un dispositif numérique qui offre des services de lavage des véhicules à domicile, dans un lieu de travail ou dans d'autres endroits.

Le service **Envoi Rapid** est une application permettant l'envoi de colis à travers le monde de manière sécurisée et fiable. Elle vous fait gagner en argent et en temps. C'est un service qui offre la possibilité d'envoyer votre colis via un particulier, tout en permettant de suivre sa mobilité.

## II.2. Présentation du réseau informatique de DANON'S GROUP

Le thème intitulé « Étude et mise en place d'une supervision informatique avec Nagios XI : cas de DANON'S GROUP » s'inscrit dans un contexte de mise en place d'une solution de supervision du réseau de DANON'S GROUP.

Le réseau IP de DANON'S GROUP abrite différents services tels que les services web, DNS, DHCP, de messagerie, etc. De ce fait DANON'S GROUP souhaite ajouter à ces différentes plateformes, un service pour superviser son réseau. Le projet consiste à faire une étude pour une mise en place d'une supervision de son réseau.

### ➤ Constituant du réseau informatique de DANON'S GROUP

Le réseau informatique de DANON'S GROUP est constitué :

- **D'équipements terminaux :**

Comme équipements terminaux qui existent à DANON'S GROUP, nous avons : des postes de travail (ordinateur de bureau, ordinateurs portables), des serveurs.



PC bureau

Laptop

Serveur

**Figure 2 :** Equipements terminaux

- **D'équipements intermédiaires :**

Parmi les équipements intermédiaires de DANON'S GROUP, on a : des routeurs, des switchs et des points d'accès.



Routeur



Switch



Point d'accès

**Figure 3 :** Équipements intermédiaires

- **Des supports de communications :**

Les supports de communications au sein de l'entreprise sont :

- Des câbles UTP Catégorie 6 (câble Ethernet RJ45) ;
- Des antennes Cambium et UniFi.



Antenne Cambium



Antenne UniFi



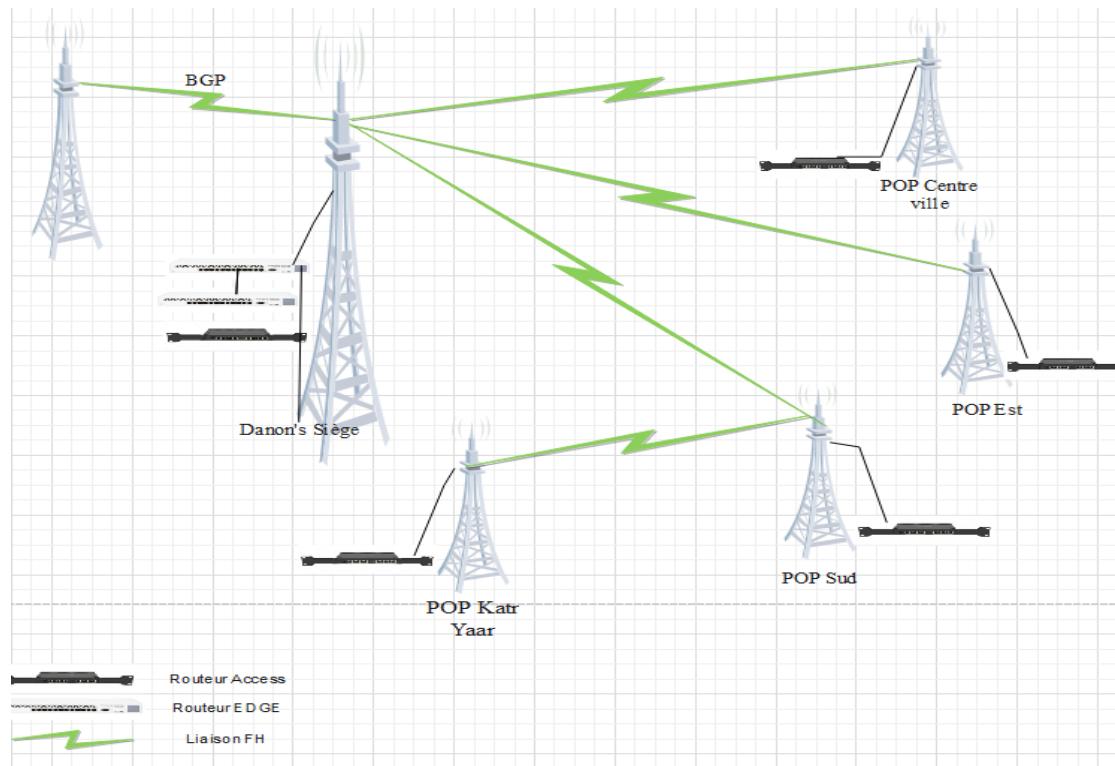
Câble Ethernet

**Figure 4 :** Supports de communications

## ➤ Architecture du réseau de DANON'S GROUP

Le réseau internet de DANON'S GROUP est un réseau de type BLR. C'est est une technologie éprouvée utilisée par de nombreux fournisseurs d'accès internet dans le monde pour offrir une connexion internet très haut débit aux clients finaux.

A DANON'S GROUP, la BLR se compose à ce jour de quatorze (14) stations de base (BS) utilisant les bandes de fréquences hertziennes de 5 GHz. Ces stations de bases sont connectées au backbone de transport permettant de distribuer le réseau internet aux CPEs (Customer Premise Equipment) des utilisateurs finaux.



**Figure 5 :** Architecture du réseau informatique de DANON'S GROUP

## CHAPITRE 2 : Étude théorique et l'état de l'art et choix de l'outil

### Introduction

Pour pouvoir garantir une activité ainsi qu'une bonne notoriété de son entreprise, il est primordial de réduire au maximum les problèmes informatiques. C'est pour cela que les entreprises ont désormais recours à des sociétés de supervision informatique au travers de contrat de maintenance informatique.

Dans ce chapitre, nous allons présenter le concept de la supervision informatique et la manière dont il a été normalisé par l'ISO 7498/4, les aspects de la supervision, ensuite présenter l'outil Nagios XI.

### I. La supervision informatique

#### I.1. Définition

La supervision informatique est une technique de surveillance, d'analyses et d'alertes permettant de pallier les problèmes liés à tous les niveaux de fonctionnement informatique d'une entreprise.

L'utilisation de la supervision informatique a un but bien précis : rendre l'entreprise plus performante et surtout proactive.

La surveillance des équipements informatiques permet de détecter toute anomalie en temps réel, et de pouvoir ainsi la traiter dans les meilleurs délais. Selon le type d'anomalie relevée, le traitement se fera en maintenance locale ou à distance.

La supervision informatique peut concerner tout l'existant informatique et téléphonique de l'entreprise, le courant électrique, les disponibilités réseaux (fibres, ADSL (Asymmetric Digital Subscriber Line), les serveurs, les imprimantes et les autres éléments actifs constituant le réseau (hubs, switchs, routeurs, etc.).

Elle doit répondre aux préoccupations suivantes :

- Technique : surveillance du réseau informatique, de l'infrastructure de l'entreprise ;
- Fonctionnelle : surveillance des machines informatiques et de production ;
- Applications : suivi des applications dans le cadre d'un processus métier.

## I.2. Rôle de la supervision

Deux phases sont importantes pour que les administrateurs soient capables d'atteindre l'objectif visé par la supervision, à savoir, surveiller le système et garantir sa disponibilité même en cas d'anomalie. Nous pouvons citer les rôles suivants :

- ❖ Tenter de prévenir en cas de problème (défaillances matérielles ou interruption des services) et garantir une remontée d'information rapide ;
- ❖ Automatiser les tâches de récupération des applications et des services en assurant des mécanismes de redondance en une durée d'intervention minimale (par exemple : le redémarrage des services interrompus, l'arrêt de la machine en cas du surcharge du CPU (Central Process Unit), la sauvegarde des données en cas du risque de perte d'un disque dur en mémoire, etc.).

## I.3. La supervision des réseaux

### I.3.1. Définition

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

La surveillance du réseau porte plus spécifiquement sur la qualité (bande passante) et la sécurité de la connexion Internet mais aussi, par extension, à l'état des services et matériels connectés : serveurs, routeurs, switch imprimantes, postes de travail, etc.

La supervision réseau est un des 3 types de supervision informatique avec la supervision système (bas niveau) et la supervision applicative.

## I.4. Principe de la supervision

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 le cas contraire prévenir via un système d'alerte (E-mail 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 machines : Au niveau interconnexions (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, latency, 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 latency 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 analysé 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.

### I.5. La norme ISO 7498/4

Le concept de la supervision a été normalisé par l'ISO (International Organization for Standardization). Voici les différentes fonctions qui ont été défini par l'ISO :

#### I.5.1. Gestion des performances

Elle doit pouvoir évaluer les performances des ressources du système et leur efficacité. Elle comprend les procédures de collecte de données et de statistiques. Elle doit aboutir à l'établissement de tableaux de bord. Les informations recueillies doivent aussi permettre de planifier les évolutions du réseau.

Les performances du réseau sont évaluées à partir de quatre paramètres :

- Le temps de réponse ;
- Le débit ;
- Le taux d'erreur par bit ;
- La disponibilité.

### I.5.2. Gestion des configurations

La gestion de configuration permet d'identifier, de paramétriser et de contrôler les différents objets du réseau. Les procédures requises pour gérer une configuration sont :

- La collecte d'information ;
- Le contrôle d'état ;
- La sauvegarde historique de configuration de l'état du système.

### I.5.3. Gestion de la comptabilité

Son rôle est de connaître les charges des objets gérés ainsi que leurs coûts de communication. Des quotas d'utilisation peuvent être fixés temporairement ou non sur chacune des ressources réseaux. De plus, la gestion de la comptabilité autorise la mise en place de systèmes de facturation en fonction de l'utilisation pour chaque utilisateur.

### I.5.4. Gestion des anomalies

La gestion des fautes permet la détection, la localisation et la correction d'anomalies passagères ou persistantes. Elle doit également permettre le rétablissement du service à une situation normale.

### I.5.5. Gestion de la sécurité

La gestion de la sécurité contrôle l'accès aux ressources en fonction des politiques de droits d'utilisation établies. Elle veille à ce que les utilisateurs non autorisés ne puissent accéder à certaines ressources protégées.

Elle a également pour rôle de mettre en application les politiques de sécurité.

## II. Les aspects de la supervision

### II.1. Fonctionnement d'une plateforme de supervision

Le fonctionnement d'une telle plateforme se fait à l'aide des tests qui sont envoyées vers les stations à surveiller dans un réseau, puis les réponses à ces tests sont analysées afin de voir leurs états.

Le superviseur peut être alors informé d'une panne ou bien d'une défaillance qui survient sur le réseau à l'aide d'un message qui lui est transmis sur son mail ou bien par SMS.

### II.2. Les méthodes de la supervision

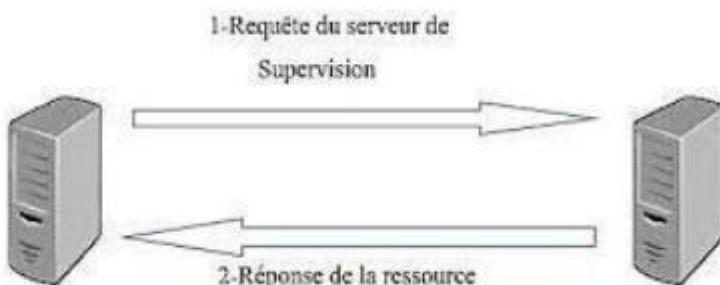
Deux grandes méthodes de supervision sont utilisées avec plusieurs variantes : les méthodes active et passive, détaillées dans les paragraphes suivants :

#### ➤ Supervision active

La supervision active est la plus classique et la plus utilisée. Elle consiste en l'envoi de requêtes d'interrogation et de mesure par la plateforme de supervision. Elle a l'avantage d'être fiable : les vérifications se font de manière régulière et en mode question-réponse.

Cette méthode est composée de trois étapes :

- Le serveur envoie une requête vers la ressource supervisée ;
- La ressource répond à la requête du serveur ;
- Le serveur analyse l'information et détermine un état pour la ressource.



**Figure 6 :** Supervision active

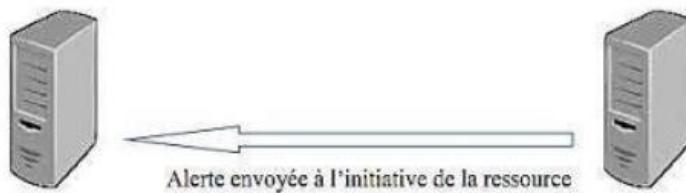
Les deux principaux protocoles de supervision active sont SNMP et WMI, ces deux protocoles sont à privilégier car non intrusifs : les agents sont natifs aux systèmes supervisés.

Certains protocoles d'administration peuvent également être utilisés pour la supervision: IPMI et JMX, les protocoles systèmes SSH et Telnet sont également très utilisés.

➤ **Supervision passive :**

La supervision passive l'est du point de vue du serveur de supervision : ce sont les ressources supervisées qui transmettent des alertes au serveur de supervision :

- La ressource supervisée vérifie son état et transmet de manière autonome le résultat au serveur de supervision ;
- Le serveur de supervision reçoit l'alerte et la traite.



**Figure 7 :** Supervision passive

Le protocole standardisé et privilégié pour la supervision passive est SNMP avec le mécanisme de trappes. La communauté Nagios propose également un module passif dédié appelé NSCA (Nagios Service Check Acceptor).

### II.3. Les standards de la supervision

Surveiller les systèmes d'information, permet de s'assurer d'une bonne disponibilité des services (Ex : l'arrêt d'un système de paiement par carte bancaire), ou la disponibilité d'un site de vente de billets en ligne (l'impact pour l'entreprise peut être très conséquent).

En détectant toutes les anomalies, on peut alerter par tout moyen à disposition (mail, SMS, autres) et prévenir ainsi les défaillances. Une automatisation des tâches permettra de relancer les serveurs et d'intervenir à distance si nécessaire en toute sécurité, en relançant ainsi le service concerné.

Les systèmes de supervision utilisent des protocoles, très réglementés par la DMTF depuis 2005, parmi les principaux utilisés, nous relèverons 10 principaux protocoles dans la supervision :

#### II.3.1. Intelligent Platform Management Interface (IPMI)

C'est l'un des standards les plus utilisés, il concerne surtout les serveurs et cette interface intelligente de gestion de matériel permet, entre autres, de contrôler à distance certains composants très sensibles comme les sondes et autres ventilateurs.

### **II.3.2. Java Management Interface (JMX)**

C'est l'API, qui permet de gérer une application en cours d'exécution. JMX est maintenant complètement intégré dans J2SE à partir de la version V. Certains experts estiment que le JMX est le SNMP de JAVA puisqu'il agit dynamiquement sur son comportement, génère des statistiques en temps réel sur son fonctionnement et notifie des dysfonctionnements.

### **II.3.3. Common Information Model (CIM)**

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

### **II.3.4. Information Technology Infrastructure Library (ITIL)**

C'est une norme, ensemble de bonnes pratiques diront d'autres, pour la bonne gestion d'un système d'information. Né en Grande Bretagne, et populaire en Europe depuis plus de 35 ans, il tend à s'implanter aux USA grâce à l'impulsion de certaines grandes SSII.

Basé sur la CMDB (Configuration Management DataBase), c'est une BDD (*Base De Données*) qui unifie les composants d'un système d'information et qui en plus, permet de comprendre l'organisation et de modifier la configuration si nécessaire. C'est la base même du système ITIL., en positionnant des blocs organisationnels et des flux d'informations, les recommandations ITIL, abordent des sujets aussi variés que :

- Les productions informatiques ;
- Les réductions des risques ;
- L'augmentation de la qualité du service ;
- L'efficacité globale du système d'information.

### **II.3.5. Standard Based Linux Instrumentation for Manageability (SBLIM)**

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

### **II.3.6. Web Based Enterprise Management (WBEM)**

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

### **II.3.7. Web Services for Management (WS-MANAGEMENT)**

WS-Management fournit la méthodologie pour échanger des informations d'administrations à travers les infrastructures IT, spécification fournie par le DMTF. Basé sur les Web Services (SOAP), il est très proche du protocole WBEM.

### **II.3.8. Windows Management Instrumentation**

C'est le protocole pour les plateformes Windows, il étend le modèle du CIM, pour représenter les objets, dans cet environnement. Son interface cohérente et orientée objet, utilise les normes de l'industrie et permet aux informaticiens une utilisation simplifiée des tâches de gestion. L'accès aux données sous WMI, que ce soit en local ou à distance, est totalement transparent.

Tous ces protocoles sont normalisés et gérés par la DMTF : c'est un organisme mondial, où sont regroupés tous les grands constructeurs et donneurs d'ordre, qui met en place et gère les standards de la technologie. La DMTF simplifie la gérabilité de tous ces standards, grâce à la collaboration et à la participation des grandes sociétés mondiales de technologie, ainsi que des principaux constructeurs.

### **II.3.9. Simple Network Management Protocol (SNMP)**

#### **II.3.9.1. Présentation**

Le protocole SNMP (Simple Network Management Protocol), conçu à l'initiative de CISCO, HP et Sun, puis normalisé par l'IETF et l'OSI, permet de contrôler à distance l'état des principaux constituants du réseau.

Les buts du protocole SNMP sont de :

- Connaitre 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 différents métriques afin d'anticiper les problèmes futurs (engorgement réseau...) ;
- Agir sur certains éléments de la configuration des équipements.

### II.3.9.2. Les différentes versions du SNMP

Ce protocole d'administration, très répandu dans les réseaux locaux, est basé sur l'échange de messages entre les périphériques administrables et une station d'administration. Il existe 3 versions du protocole : SNMP v1, SNMP v2c et SNMP v3.

- **SNMP v1** : qui reste la version la plus utilisée car la plus « légère ». La sécurité de cette version est minimale car elle basée uniquement sur la chaîne de caractère appelée "communauté" ;
- **SNMP v2c** : est une version délaissée car trop complexe. Elle assure un niveau plus élevé de sécurité (authentification, cryptage...), des messages d'erreurs plus précis, autorise l'usage d'un Manager central. Cependant ce protocole utilise la structure d'administration de SNMP V1 (à savoir "communauté") d'où le terme SNMP V2C ;
- **SNMP v3** : permet de disposer des avantages de la version 2 sans en présenter les inconvénients. Elle définit un nouveau modèle de sécurité USM (User-based Security Model) évitant le décryptage des messages de commande qui transitent sur le réseau et autorise des droits différents en fonction des utilisateurs.

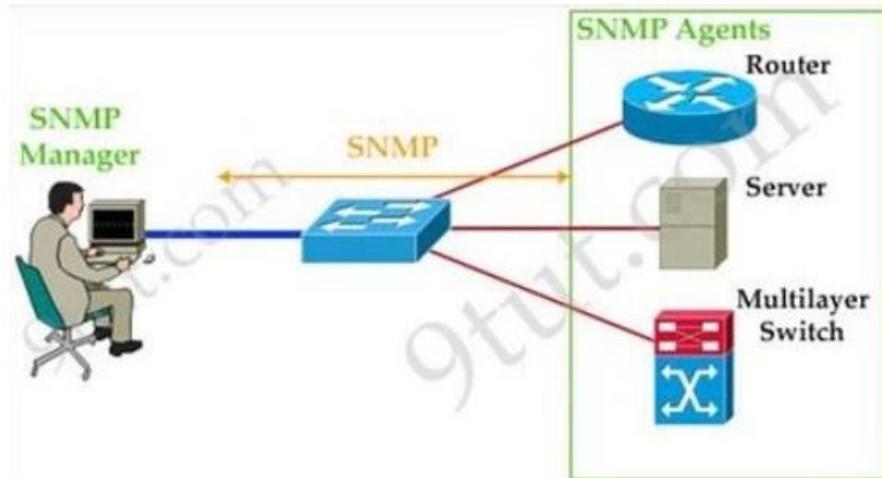
Malgré tout la version SNMP v1 persiste encore sur les périphériques, plusieurs facteurs expliquent ce phénomène :

- Les infrastructures déployées en V1 ne sont plus modifiées, tout simplement car cela fonctionnait suffisamment à l'époque, du coup aucune modification n'y est appliquée ;
- Les autres versions de SNMP ont été implémentées tardivement par les différents constructeurs ;
- SNMP V1 demande très peu de ressources sur des petits équipements tels qu'une imprimante.

### II.3.9.3. Architecture

Les différents éléments que l'on peut identifier avec le protocole SNMP sont :

- Les agents SNMP : ce sont les équipements (réseau ou serveur) qu'il faut superviser.
- Le superviseur SNMP : c'est une machine centrale à partir de laquelle un opérateur humain peut superviser en temps réel toute son infrastructure, diagnostiquer les problèmes et finalement faire intervenir un technicien pour les résoudre.
- La MIB : ce sont les informations dynamiques instanciées par les différents agents SNMP et remontées en temps réel au superviseur.



*SNMP is the protocol running between SNMP Manager & Agent*

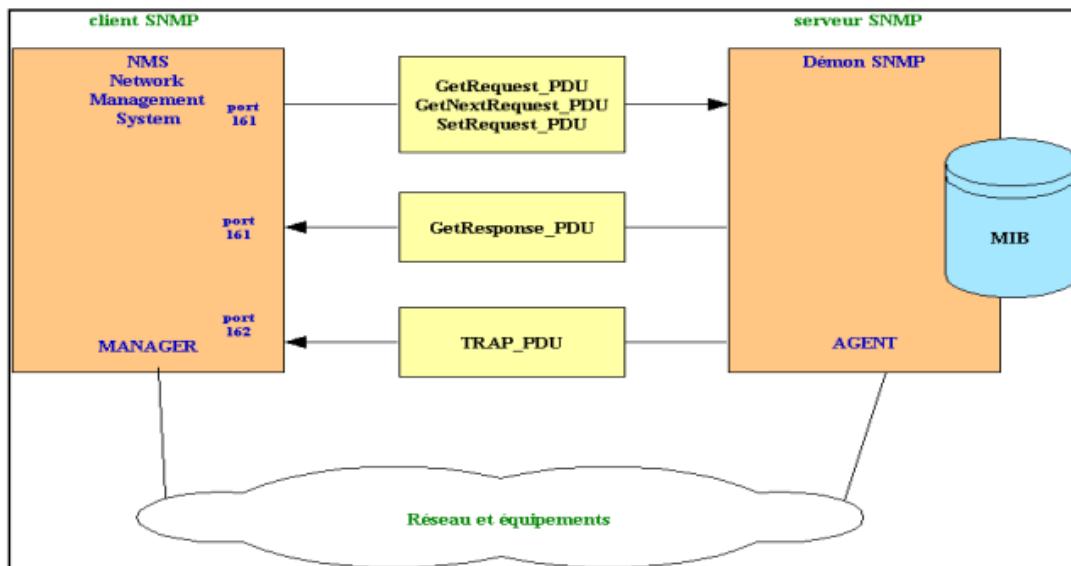
**Figure 8 :** Architecture SNMP

#### II.3.9.4. Principe de fonctionnement

SNMP fonctionne avec les technologies utilisant les protocoles TCP/IP et s'appuie sur le protocole UDP.

SNMP est basé sur trois éléments :

- un équipement à superviser qui contient des objets à gérer : informations de configuration, sur le matériel, statistiques... ;
- il exécute un agent, c'est-à-dire un logiciel qui agrège les données locales ;
- une console de supervision qui permet d'interroger les agents accessibles par le réseau ou de recevoir des alertes émises par les agents.



**Figure 9 :** fonctionnement SNMP

Chaque équipement sur lequel intervient l'administrateur via SNMP doit disposer d'un agent SNMP qui y soit installé. L'interrogation d'un agent se fait en lui envoyant des messages sur le port UDP 161. L'agent envoie des alertes à la console sur le port UDP 162. Les objets collectés sont des informations matérielles, des paramètres de configuration, des statistiques de performance ou bien d'autres sont regrouper dans la base de données MIB.

#### II.3.9.5. La MIB

La MIB (Management Information Base) est la base de données utilisée par le protocole SNMP pour stocker des informations de gestion maintenue par l'agent. Elle est utilisée par la plate-forme comme source d'information sur le réseau.

#### II.3.9.6. L'agent SNMP

L'agent est un programme qui fait partie de l'élément actif du réseau. L'activation de cet agent permet de recueillir la base de données d'informations et la rend disponible aux interrogations.

Les principales fonctions d'un agent SNMP :

- Collecter des informations de gestion sur son environnement local ;
- Récupérer des informations de gestion telle que déni dans la MIB propriétaire ;
- Signaler un évènement au gestionnaire.

Par ailleurs même si la principale fonction de l'agent est de rester à l'écoute des éventuelles requêtes du Manager et y répondre s'il y est autorisé, il doit également être capable d'agir de sa propre initiative, s'il a été configuré.

### **II.3.10. Internet Control Message Protocol (ICMP)**

ICMP (*Internet Control Message Protocol*) est un protocole de gestion des informations concernant les erreurs des hôtes qui lui sont connectées. ICMP crée et envoie des messages à l'adresse IP source, indiquant qu'une passerelle vers l'Internet tel qu'un routeur, un service ou une hôte ne peuvent pas être atteints pour la livraison de paquets. Tout dispositif de réseau IP a la capacité d'envoyer, recevoir ou traiter des messages ICMP. ICMP n'est pas utilisé régulièrement dans les applications de l'utilisateur final, il est utilisé par les administrateurs réseau pour contrôler les connexions Internet dans les utilitaires de diagnostic, y compris ping et traceroute.

## **II.4. Étude comparative des outils de supervision open source**

Nous allons présenter les principaux outils de supervision réseau open source que nous avons choisi vu la diversité de ces outils tout en dégageant leurs avantages et inconvénients :

### **II.4.1. Cacti**

- **Présentation de l'outil :**

C'est un logiciel de supervision réseau basé sur RRDTool. Il peut être considéré comme un successeur à MRTG et également comme une interface à RRDTool. Cacti permet de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP ou encore grâce à des scripts (Bash, PHP, Perl, VBs...) pour avoir par exemple l'espace disque restant ou bien la mémoire utilisée, la charge processeur ou le ping d'un élément actif. Les données sont récoltées auprès des différents agents SNMP (ou auprès des scripts locaux) grâce à un script php. Pour de meilleures performances un exécutable, nommé cactid, peut également effectuer les interrogations.

- **Avantages :**

- Configuration : Avec l'utilisation des templates pour les machines, les graphiques, et la récupération des données tout se configure aisément et entièrement via l'interface web. Import/ Export très simple des templates au format XML. On peut aussi très facilement utiliser des options poussées de RRDTOOL ;

- Performance : Avec le choix du moteur de récolte des données, On peut opter pour la performance ou la simplicité ;
  - Gestion des utilisateurs ;
  - Communauté sur le web, présence d'une dizaine de plugins permettant d'étendre les fonctionnalités.
- **Inconvénients :**
    - ✓ Pas de gestion d'alarmes, sauf avec un plugin nommé Thold ;
    - ✓ Pas de gestion de panne et absence d'une cartographie de réseau ;
    - ✓ Un développement lent tout comme NztMRG.

#### II.4.2. Zabbix

- **Présentation de l'outil :**

Zabbix est un outil de supervision, ambitionnant de concurrencer Nagios et MRTG. Il permet de superviser réseau, systèmes (processeur, disque, mémoire, processus,...). Zabbix offre des vues graphiques (générés par RRDtool) et des alertes sur seuil. Le « serveur ZABBIX » peut être décomposé en 3 parties séparées: Le serveur de données, l'interface de gestion et le serveur de traitement. Chacune d'elles peut être disposée sur une machine différente pour répartir la charge et optimiser les performances. Un agent ZABBIX peut aussi être installé sur les hôtes Linux, UNIX et Windows afin d'obtenir des statistiques comme la charge CPU, l'utilisation du réseau, l'espace disque... Le logiciel peut réaliser le monitoring via SNMP. Il est possible de configurer des « proxy Zabbix » afin de répartir la charge ou d'assurer une meilleure disponibilité de service.

- **Avantages :**

- ✓ Une solution très complète : cartographie de réseaux, gestion poussée d'alarmes via SMS, Jabber ou Email, gestion des utilisateurs, gestion de pannes, statiques et reporting ;
- ✓ Une entreprise qui pousse le développement, et une communauté croissante ;
- ✓ Une interface vaste mais claire ;
- ✓ Une gestion des templates poussée, avec import/export xml, modifications via l'interface ;
- ✓ Des performances au rendez-vous : l'application a été testée avec succès avec 10000 équipements supervisés ;

- ✓ Compatible avec MySQL, PostgreSQL, Oracle, SQLite.

- **Inconvénients :**

- ✓ Interface est un peu vaste, la mise en place des templates n'est pas évidente au début : petit temps de formation nécessaire ;
- ✓ L'agent zabbix communique par défaut en clair les informations d'où la nécessité de sécuriser ces données (via VPN par exemple) ;
- ✓ Commence à être connu, mais pas encore auprès des entreprises : peu d'interfaçage avec d'autres solutions commerciales.

### II.4.3. Nagios

- **Présentation de l'outil :**

Nagios (anciennement Netsaint) est un logiciel qui permet de superviser un système d'information. Nagios est, avant toute chose, un moteur gérant l'ordonnancement des vérifications, ainsi que les actions à prendre sur incidents (alertes, escalades, prise d'action corrective). L'interface web est la partie graphique visible, via un serveur web tel que Apache, et qui va permettre à l'administrateur d'avoir une vue d'ensemble de son réseau, de visualiser la supervision des équipements et de produire des rapports d'activité.

- **Avantages :**

- ✓ Reconnu auprès des entreprises, grande communauté ;
- ✓ Très puissant et modulaire ;
- ✓ Plétoire de plugins qui permettent d'étendre les possibilités (agents comme zabbix, reporting amélioré, etc...)
- ✓ Une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau ;
- ✓ Beaucoup de documentaires sur le web ;
- ✓ Performances du moteur.

- **Inconvénients :**

- ✓ Interface non ergonomique et peu intuitive ;
- ✓ Configuration fastidieuse via beaucoup de fichiers ;
- ✓ Pour avoir toutes les fonctionnalités il faut installer des plugins, de base c'est assez limité.

## II.5. Tableau comparatif des outils de supervision

Ci-dessous représente un récapitulatif des outils de supervision open source :

**Tableau 1:** Comparaison des outils de supervision

Outils	Licence	OS	Installation	Protocole	Alerte
<b>Cacti</b>	Gratuit (GPL)	Unix/Windows	Facile sur Unix	SNMP	-
<b>Nagios XI</b>	Gratuit (GPL)	Unix	Difficile	SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP	E-mail et/ou SMS
<b>Zabbix</b>	Gratuit (GPLv2)	Unix	Difficile	SNMP TCP UDP JSON	E-mail et/ou SMS

### III. Étude technique détaillée de Nagios XI

#### Introduction

Dans cette partie, nous commençons par présenter l'outil Nagios, son architecture et son principe de fonctionnement, ensuite nous présentons les compléments de notre solution qui sont les agents spécialisés en supervision à distance NSClient et NRPE ainsi que ses fichiers de configurations.

#### III.1. Présentation de Nagios

Nagios (anciennement appelé Netsaint) est un logiciel libre sous licence GPL permettant principalement la surveillance système et réseau mais reste évolutif et assez flexible. Il se base sur la collecte déclenchée et personnalisée des informations que nous cherchons à analyser, il permet la surveillance d'un grand nombre de paramètres sur les machines du réseau. La principale particularité de cet outil est sa grande modularité qui lui permet de s'adapter aux besoins des utilisateurs. L'utilisateur pourra donc affiner les tests à effectuer selon ce qu'il veut surveiller.

A la différence de beaucoup d'autres outils de supervision, Nagios ne possède pas un mécanisme interne qui vérifie l'état d'une application, d'un hôte... A la place, il utilise des programmes externes appelés plugins.

#### III.2. Choix de l'outil

Pour la supervision informatique au sein de la société, nous avons choisi Nagios XI comme un outil de supervision à mettre en place.

Notre choix s'est basé sur les points forts de cet outil notamment sa modularité complète et sa capacité à gérer un parc important de machines.

- **Sa modularité :** Nagios laisse la supervision à des plug-ins, ou sondes, que va lui fournir l'utilisateur. Il se contente de les lancer et de gérer les informations recueillies par ce biais. Il permet également de définir des plug-ins qui vont alerter les utilisateurs en cas de problème, ce qui permet d'être inventif en matière d'avertissement. Lorsque quelque chose se passe mal, d'autres plug-ins peuvent tenter de corriger le problème. Il n'est pas possible de prévoir tous les cas de réparations possibles. Nagios laisse le soin de définir lui-même les commandes pour résoudre le problème sur son environnement.
- **Sa capacité à gérer un parc important de machines :** sur ce point, trois critères principaux entrent en jeu :

- ✓ Les performances : En matière de performances, Nagios n'a rien à envier aux outils de supervision propriétaires. Il permet, avec un serveur modeste, de surveiller près de 10 000 éléments. Nagios propose des options pouvant sensiblement augmenter cette valeur ;
- ✓ La gestion de la configuration : Plus on a de points à surveiller, plus la configuration ne devient lourde, avec les risques, si elle devient trop dure à gérer, d'être laissée de côté. Nagios propose diverses solutions pour faciliter la gestion d'un nombre élevé de points surveillés, et c'est même une de ses grandes forces ;
- ✓ Les pertes massives : Dans le cas des grandes architectures, de petits problèmes peuvent vite devenir un véritable cauchemar. Partant d'une simple erreur, on atteint au final un nombre impressionnant d'alertes. Si l'outil de supervision ne gère pas ce genre de cas, les utilisateurs auront toutes les peines du monde à trouver, parmi toutes ces alertes, la cause initiale du problème. Nagios gère ces cas grâce aux relations dépendances. Ces relations peuvent être physiques (par exemple pour les liens réseau) ou bien virtuelles (comme c'est le cas entre une application et sa base de données). Il permet de filtrer les alertes pour avoir uniquement celles qui apportent des informations sur la résolution du problème.

### III.3. Architecture de Nagios

C'est un programme modulaire qui se décompose en trois parties : un ordonnanceur, une IHM (Interface Home Machine) Et les sondes.

- **L'ordonnanceur** est le moteur de l'application qui vient ordonner et gérer les tâches, les vérifications, et les actions à prendre en cas d'incidents (alertes, types d'analyse et d'action corrective) ;
- **IHM (Interface Home Machine)** représente la partie graphique, visible à travers un simple serveur Web tel Apache, permettant d'avoir une vue d'ensemble du système d'information et des possibles anomalies afin de faciliter la communication entre l'administrateur réseau et l'ordonnanceur ;
- **Les sondes (un greffon/plugin)** est un petit programme qui assure une ou plusieurs tâches particulières. Pour les plugins dédiés à Nagios. Il existe déjà plusieurs disponibles gratuitement sur internet, notamment sur le site [10]. Chaque utilisateur pourra

compléter et modifier en fonction de ses besoins pour superviser chaque service ou ressource disponible de la manière qu'il souhaite. C'est cette troisième composante de Nagios qui fait « sa force ». En effet les plugins peuvent être développés à l'aide de langages de programmations communs comme le C++, Perl ou PHP en fonction des aptitudes de l'utilisateur et suivant ses critères personnels de supervision afin d'appliquer les solutions adéquates à chaque situation.

#### **III.4. Principe de fonctionnement de Nagios**

Nagios est un moteur d'ordonnancement de vérifications diverses et variées. Ces dernières, dont le développement est séparé du noyau moteur, sont assurées par des plugins. La relation entre le moteur et les plugins est assurée d'une part par la configuration de Nagios afin que Nagios sache quelles vérifications lancer et sur quelles machines. D'autre part, cette relation est garantie par la sortie renvoyée du plugin sous la forme d'un code retour. Ce code sera accompagné éventuellement d'un petit message décrivant le déroulement de l'exécution (dans le but d'aider l'utilisateur à faire le bon diagnostic en cas de problème). Ce sont donc ces états qui seront ensuite remontés au moteur qui prendra les décisions et lancera les actions adéquates et préalablement programmées. Le code retour fourni par l'exécution du plugin est décrit dans le tableau ci-dessous.

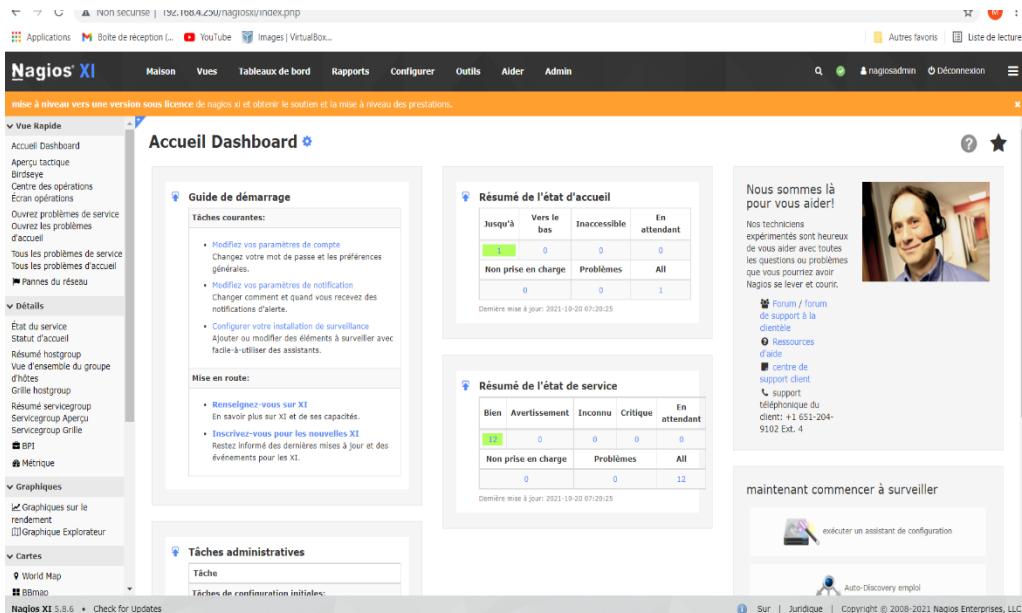
**Tableau 2:** Correspondance de retour-état

Valeur Numérique	Statut du service	Description du statut
0	OK	Le plugin a été en mesure de vérifier le service et fonctionne correctement
1	WARNING	Le plugin a été en mesure de vérifier le service, mais ne semble pas fonctionner correctement
2	CRITICAL	Le plugin n'a même pas pu être vérifié
3	UNKNOWN	Arguments invalides dans la ligne de commande du plugin ou bien ce dernier a été incapable de vérifier l'état de l'hôte donné ou le service

Le processus standard se déroule comme suit : Nagios exécutera un plugin dès qu'il a besoin de tester un service ou un hôte. Les plugins feront ce qu'il faudra pour exécuter le contrôle choisi et envoyer ensuite le résultat à la machine serveur de supervision. Nagios analysera le

résultat reçu du plugin et prendra les mesures nécessaires prévus au préalable (informer l'administrateur via e-mail, SMS...).

Ces greffons fonctionnent soit à distances (tests sur des protocoles réseaux tels que SMTP, FTP ou l'exécution à distance via SSH ou autre), soit en local sur la machine supervisée (par exemple vérification sur les disques).



**Figure 10 :** Interface web de Nagios XI

### III.5. Les plugins

Les plugins sont des programmes externes permettent de contrôler une ressource ou un service local ou distant en effectuant des tests de toutes sortes (fonctionnement de services, espace disque, charge, ...) sur la machine Nagios, ainsi que des tests simples (par exemple ping) sur une machine distante.

Nagios possède une importante communauté sur Internet. Grâce à celle-ci, de nombreux utilisateurs ont créés des plugins permettant à Nagios d'aller récupérer des informations sur des équipements du réseau (PC, routeurs, serveurs, ...).

Les plugins n'utilisent pas tous le même protocole pour échanger les informations. Le protocole utilisé est dans la plupart des cas un facteur décisif sur le choix des plugins à utiliser.

Un seul plugin Nagios ne peut pas aller chercher toutes les informations sur les équipements du réseau: En effet, chaque plugin n'a accès qu'à certaines informations (exemple: un plugin peut aller chercher l'occupation du disque dur, et un autre l'occupation du processeur d'un PC).

Pour superviser un parc informatique, il est donc nécessaire de mettre en place plusieurs plugins. De plus, certains plugins peuvent aller chercher des informations sur des clients uniquement sur certains systèmes d'exploitation (c'est le cas du plugin `check_nt` qui peut chercher des informations uniquement sur des équipements Windows).

### III.5.1. Les plugins locaux

En standard, SNMP ne remonte que des informations systèmes basiques. Pour aller plus loin et surveiller des processus plus complexe, Nagios a mis en place un système de type plugins locaux. Un plugin local est un script localisé sur le serveur Nagios (`/usr/lib/nagios/plugins` sous Linux, c'est pour cela que l'on dit qu'il est local). Ce script, lancé à la demande de Nagios, doit retourner un code dont la signification est la suivante :

- Code 0 : OK – tout va bien
- Code 1 : WARNING – alerte
- Code 2 : CRITICAL – alerte critique
- Code 3 : UNKNOWN – problème lors de l'exécution du plugin

En plus de ces codes, un plugin peut fournir d'autres informations (sous la forme d'une chaîne de caractères) qui seront affichées à côté du statut de la machine.

### III.5.2. Les principaux plugins

- `check_disk` : Vérifie l'espace occupé d'un disque dur ;
- `check_http` : Vérifie le service « http » d'un hôte ;
- `check_ftp` : Vérifie le service « ftp » d'un hôte ;
- `check_mysql` : Vérifie l'état d'une base de données MySQL ;
- `check_nt` : Vérifie différentes informations (disque sur, processeur...) sur un système d'exploitation Windows ;
- `check_nrpe` : Permet de récupérer différentes informations sur les hôtes ;
- `check_ping` : Vérifie la présence d'un équipement, ainsi que sa durée de réponse ;
- `check_pop` : Vérifie l'état d'un service POP (serveur mail) ;
- `check_snmp` : Récupère diverses informations sur un équipement grâce au protocole SNMP (Simple Network Management Protocol) ;

Il est possible de créer son propre plugin. Dans ce cas, il faudra les créer de la sorte que celui renvoie à Nagios :

- L'état du résultat (OK, CRITICAL, DOWN, UP, ...);
- Une chaîne de caractères (pour donner le détail du résultat).

### III.6. Supervision passive et active

Nagios peut utiliser différentes méthodes dans le but de récolter les informations sur les machines du réseau. Une méthode dite active, et une autre passive. Les deux se basent sur l'exécution d'un daemon sur la machine à surveiller. Ces deux méthodes se combinent généralement pour une efficacité optimale de la supervision.

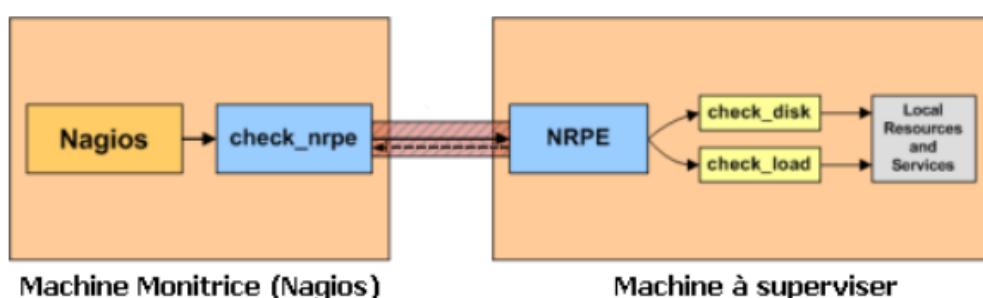
Nous rappelons que dans tout système d'exploitation multitâche, un démon est un programme informatique qui s'exécute en arrière-plan, et non sous le contrôle direct d'un utilisateur.

#### III.6.1. Les plugins actifs avec NRPE

A la différence des plugins locaux (ceux qui s'exécute sur la machine serveur, localhost, concernant ses propres ressources), le module/démon NRPE (Nagios Remote Plugin Executor) permet l'exécution de plugins dit actifs directement sur les machines à surveiller. Dans ce cas, la demande d'exécution du greffon actif est faite à l'initiative de la machine serveur Nagios.

La procédure interne est la suivante: Le serveur Nagios demande, via le client NRPE, l'exécution du plugin P sur la machine M. Le daemon NRPE hébergé sur la machine M, reçoit la requête d'exécution du plugin P. Ensuite l'exécution de ce plugin sur la machine M. Le daemon NRPE de la machine M récolte les informations suivant à l'exécution du greffon P et envoie le résultat au serveur Nagios. Enfin le serveur Nagios interprète les résultats et lance le traitement adéquat.

Ce type de procédure permet d'assurer une surveillance distante .Il faudra toutefois ouvrir un port de communication pour permettre au NRPE de communiquer avec son client et récupérer les informations d'état concernant les machines déportées.



**Figure 11 :** Supervision active avec NRPE

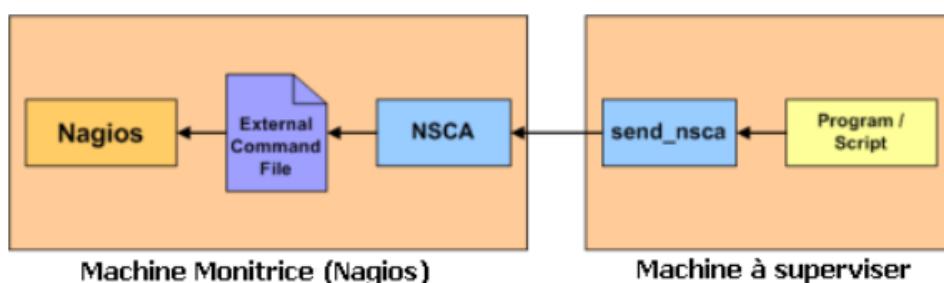
Comme nous venons de le voir, NRPE est déclenché à l'initiative du serveur Nagios. Ce mode de fonctionnement présente des limites. Par exemple dans le cas où les machines à surveiller sont derrière un réseau sécurisé, NRPE ne permet que les connexions sortantes de celui-ci, ou encore si le processus à surveiller demande une fréquence d'exécution très courte. L'échange des informations n'est plus assuré. Dans ce cas nous avons recours aux greffons dits passifs.

### III.6.2. Les plugins passifs avec NSCA

Le module NSCA propose l'exécution de plugins passifs sur les machines à surveiller. Leur exécution est déclenchée suite à des critères préalablement définis sur les machines distantes. Par exemple, le dépassement de 75% de la capacité de stockage, la détection d'une activité réseau anormale ou simplement des checks périodiques sous forme de mises à jour autodéclenchées.

La procédure interne est la suivante : Le daemon NSCA sur une machine M lance l'exécution du plugin P suite à un critère de déclenchement vérifié. En effet le plugin P est exécuté sur la machine M. Le daemon NSCA de la machine M récolte les informations suite à l'exécution du greffon P et envoie le résultat au serveur Nagios. Enfin le serveur Nagios interprète les résultats et lance le traitement adéquat.

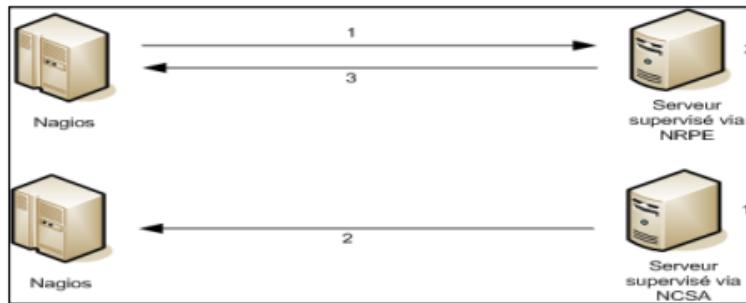
Nous remarquons bien que dans ce cas, la demande d'exécution du greffon est faite non pas par l'initiative de la machine serveur Nagios mais à celle de la machine distante elle-même.



**Figure 12 :** Supervision passive avec NSCA

La figure 12 présente la supervision passive avec NSCA. Nous remarquons que la demande d'exécution du greffon est faite non pas par l'initiative de la machine serveur Nagios, mais par l'initiative de la machine distante elle-même (la machine à superviser) suite à un critère de déclenchement vérifié.

Dans la pratique, les vérifications sont rarement passives, nous avons eu recours à cette méthode dans certains cas où la sécurité impose d'interdire une connexion dans un sens, ou encore dans le cas de supervision hiérarchique, mais le plus souvent les vérifications sont actives.



**Figure 13 :** Schéma comparatif NRPE-NSCA

La figure 13 présente un schéma comparatif entre les plugins actifs NRPE et les plugins passifs NSCA.

Dans ce projet, nous nous limiterons au cas de la supervision active.

### III.7. Les fichiers de configurations

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 globales de fonctionnement ;
- **Cgi.cfg** contient un certain nombre de directives qui affectent le mode de fonctionnement des CGI. Il peut être intéressant pour définir des préférences concernant l'interface web de Nagios ;
- **Ressource.cfg** permet de définir des variables globales réutilisables dans les autres fichiers. Étant inaccessible depuis les 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 remontée d'alerte ;
- **Checkcommands.cfg** contient les définitions des commandes de vérification prédéfinies et celles définies par l'utilisateur ;

- **Hosts.cfg** définit les différents hôtes du réseau à superviser. A chaque hôte est associé son nom, son adresse IP, le test à 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 doivent être vérifiés ;
- **Hostsgroups.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 définit les paramètres des alertes (fréquences des notifications, moyens pour contacter ces personnes, plages horaires d'envoi des alertes...).

### Conclusion

Après avoir bien étudié l'outil de supervision open source choisi, nous allons passer dans le chapitre suivant à sa mise en place au sein de l'entreprise.

## CHAPITRE 3 : Mise en place de la solution de supervision adoptée

### Introduction

À travers ce chapitre, nous allons décrire la phase de réalisation de notre application. Nous allons commencer par la spécification des différents environnements de développement, matériels et logiciels. Ensuite nous décrirons les points les plus intéressants de l'application, tout en donnant un aperçu sur les différentes parties développées au cours de ce projet.

### I. Environnement de travail

#### I.1. Environnement matériel

Tout au long de notre projet, nous avons eu à notre disposition un ordinateur portable avec la configuration suivante :

- Intel® Core i5 (2.50 GHz)
- 8 Go de RAM
- Disque dur de capacité 1 To
- Système d'exploitation Windows 10 professionnel.

#### I.2. Environnement logiciel

Après avoir présenté l'environnement matériel de développement de notre projet, nous allons rappeler et justifier brièvement les choix techniques que nous avons adoptés.

##### I.2.1. Oracle VM VirtualBox

Oracle VM VirtualBox est un logiciel de virtualisation créé par InnoTek et publié par Oracle Corporation. Ce logiciel permet de créer des machines virtuelles et d'installer sur chacune un système invité, indépendant du système hôte. Vous pourrez donc, par exemple, travailler sous Mac OS X (votre système d'exploitation principal, le système hôte) tout en utilisant une machine virtuelle sous Linux ou Windows (système invité), sous la forme d'une fenêtre.

##### I.2.2. Système d'exploitation

Les systèmes d'exploitation « Entreprise » (orientés vers le marché commercial) doivent répondre à certains critères essentiels. En effet, il est par exemple crucial que le logiciel d'administration système approprié soit lié à une offre de support complète des développeurs ou du fournisseur. C'est en effet la seule façon de s'assurer que les améliorations et les corrections de bugs régulières du logiciel ainsi que les mises à jour de sécurité soient garanties de manière permanente afin de se protéger contre les nouveaux logiciels malveillants et pour combler les failles de sécurité récemment découvertes. De plus il est aussi important de garantir un fonctionnement constant des applications commerciales ainsi que la stabilité des

interfaces entre le système d'exploitation et les programmes utilisés (rétrocompatibilité). La distribution Linux CentOS est une solution « Entreprise » particulièrement populaire dans le secteur du Web, elle est de plus open source.

### I.2.3. Navigateur

Un navigateur web est un logiciel conçu pour consulter et afficher le World Wide Web. Techniquement, c'est au minimum un client http.

Les plus utilisés sont Google Chrome, Mozilla Firefox, Internet Explorer/Edge, Safari, Opera.

## II. Installation et configuration de Nagios XI

### II.1. Prérequis

Pour l'installation de notre serveur, ces chiffres dans le tableau ci-dessous représentent les exigences minimales pour exécuter Nagios XI.

**Tableau 3 : Prérequis installation de Nagios XI**

Disque dur	Mémoire	CPU	SE
20 GO	2 GO	Double cœur, 2.4 GHz	CentOS ou Redhat Entreprise Linux, Ubuntu ou Debian

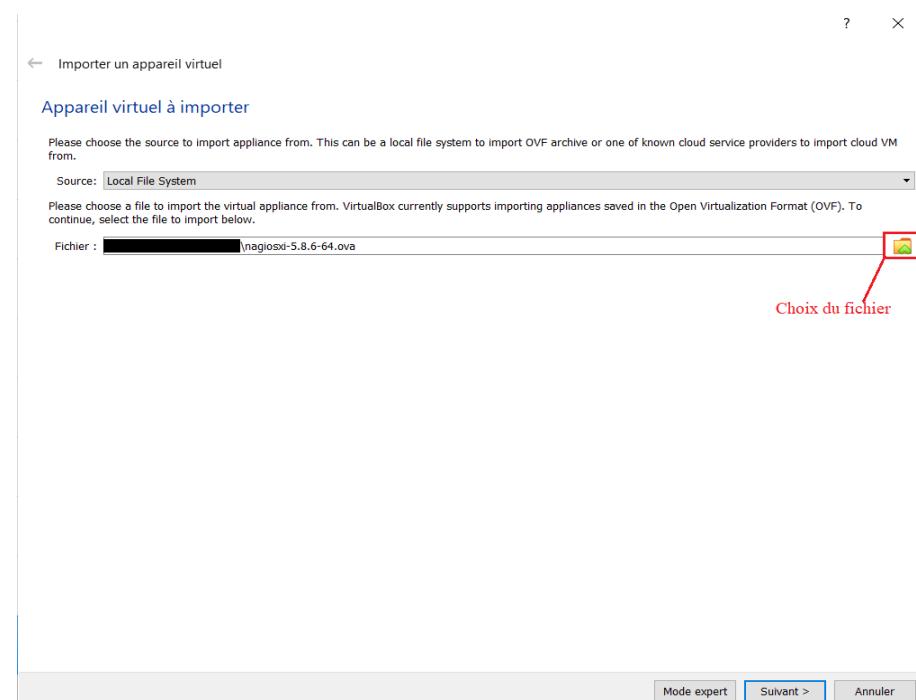
### II.2. Installation de Nagios XI

Afin d'installer Nagios XI sur notre machine, nous avons téléchargé le logiciel Nagios XI depuis le site web de Nagios sur notre machine physique, c'est le moyen le plus rapide d'être opérationnel.

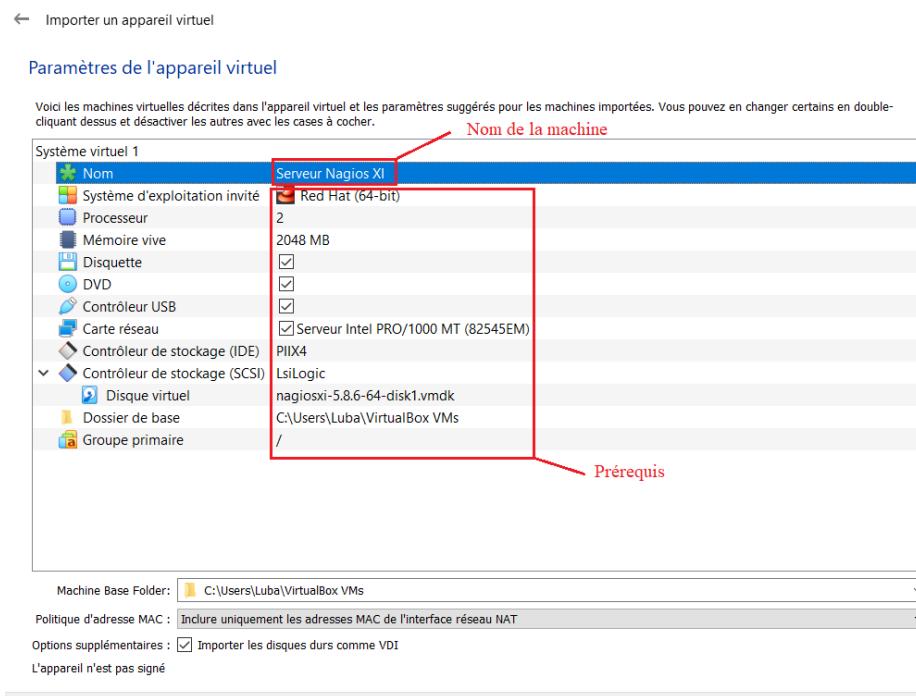
#### Étape 1 :

Avant l'installation, comme nous allons utiliser VirtualBox pour créer notre machine virtuelle, il faut qu'on converti l'image (.ova) qu'on a téléchargé en (.vdi) pour pouvoir installer sur VirtualBox.

Depuis l'onglet fichier de VirtualBox, on import le fichier téléchargé dans le répertoire la machine physique.

**Figure 14 :** Importation de Nagios XI**Étape 2 :**

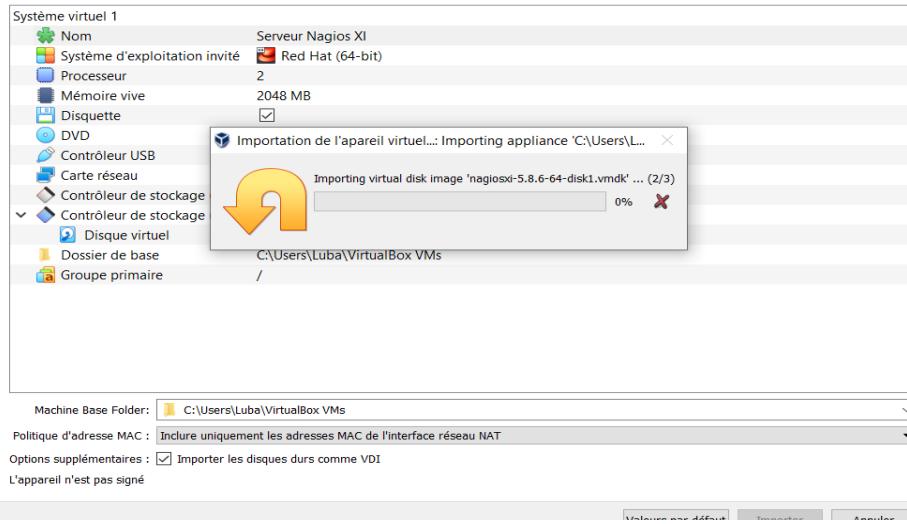
Ensuite on fait suivant puis on change le nom de notre machine, et on vérifie si on respecte les prérequis minimales pour le bon fonctionnement de notre serveur Nagios XI.

**Figure 15 :** Nom de la machine et vérification des prérequis

← Importer un appareil virtuel

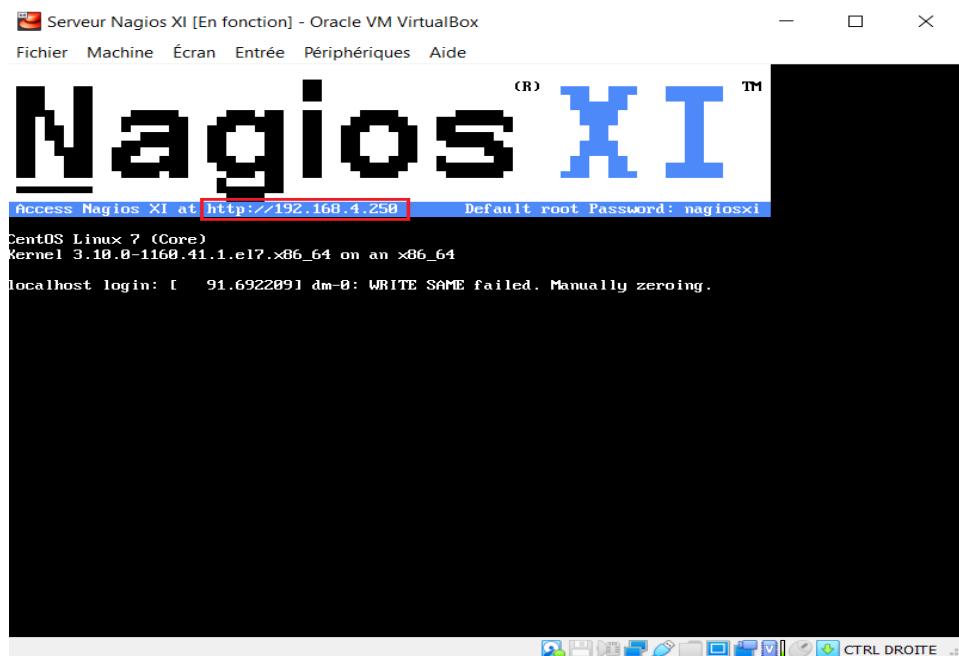
#### Paramètres de l'appareil virtuel

Voici les machines virtuelles décrites dans l'appareil virtuel et les paramètres suggérés pour les machines importées. Vous pouvez en changer certains en double-cliquant dessus et désactiver les autres avec les cases à cocher.



**Figure 16 :** Importation de la machine

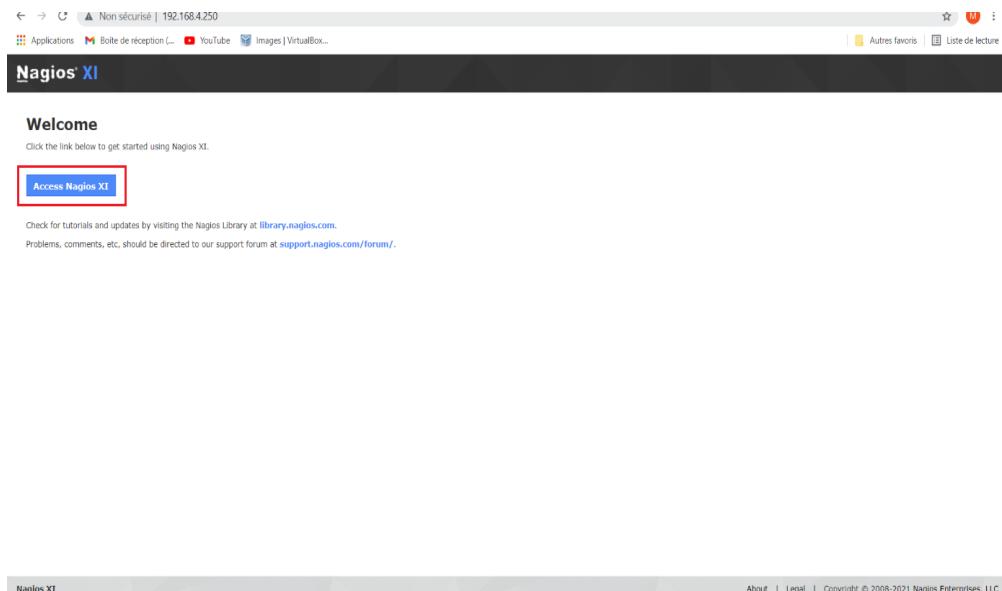
Une fois l'importation finie, nous allons voir notre machine dans VirtualBox au niveau de l'onglet Gestionnaires de machines puis on démarre.



**Figure 17 :** Interface du serveur Nagios XI

### Étape 3 :

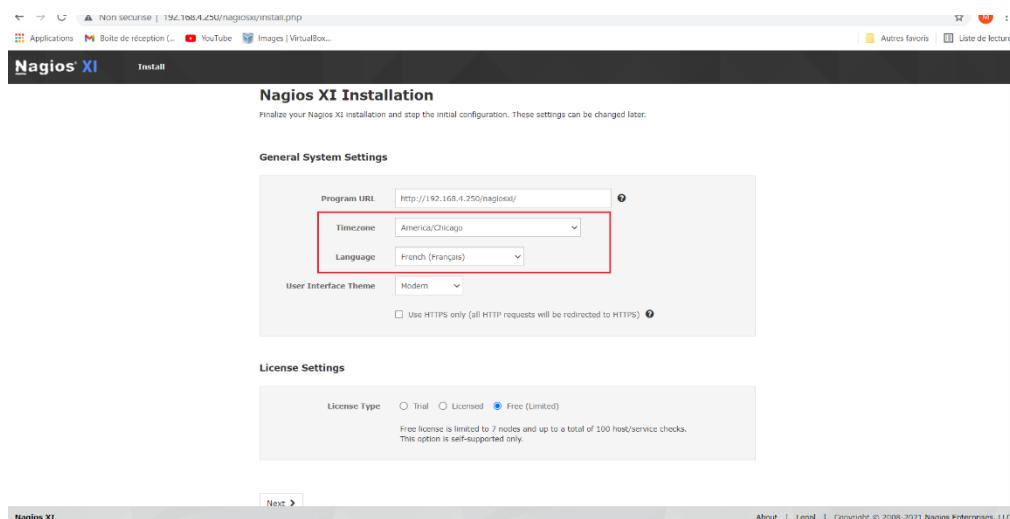
Nous utiliserons ici le navigateur Google Chrome ; pour accéder à l'interface web de notre serveur, on tape l'adresse IP du serveur Nagios XI au niveau de la barre de recherche, ensuite clic sur Access Nagios XI, afin de finaliser la configuration.



**Figure 18 :** Connexion à Nagios XI

### Étape 4 :

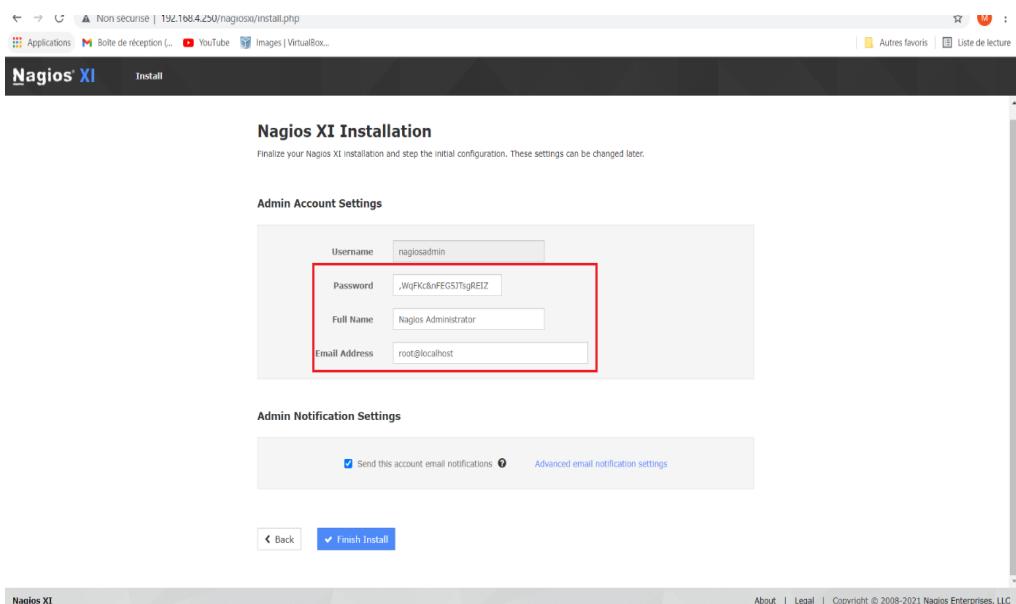
Ensuite, on renseigne les informations (Timezone & Language) puis on fait suivant.



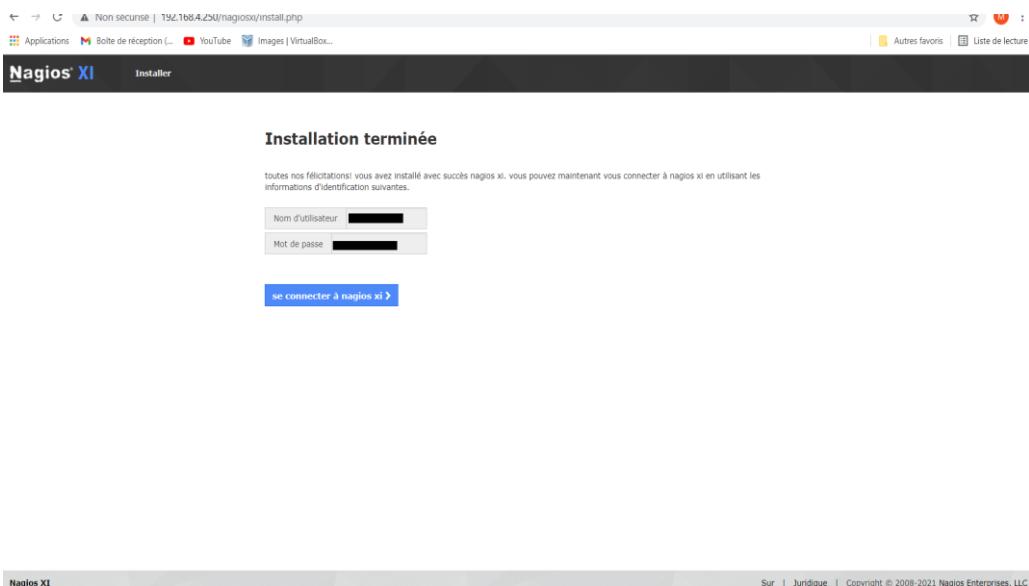
**Figure 19 :** Configuration de Nagios XI (Setup 1)

## Étape 5 :

Puis, on met un mot de passe et une adresse mail de l'administrateur.

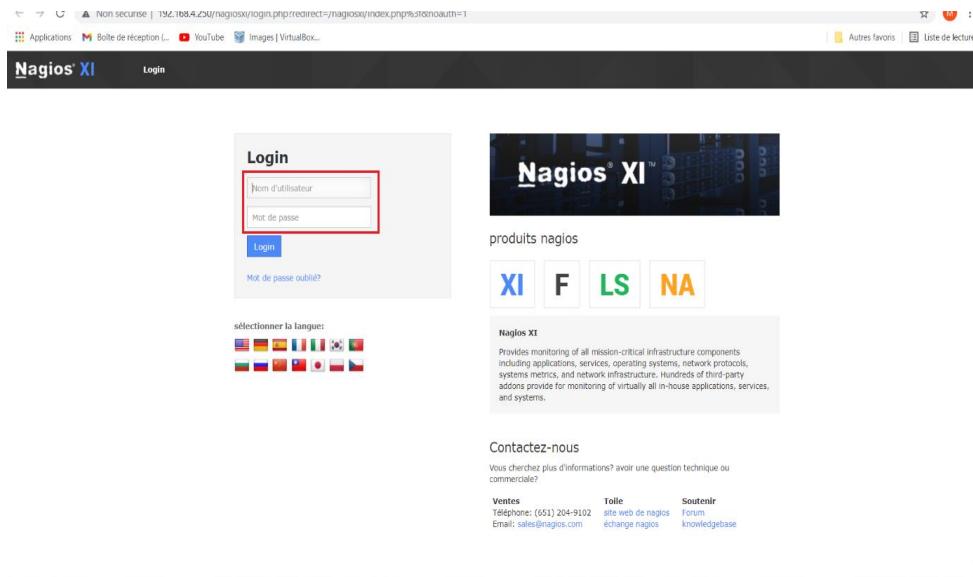


**Figure 20 :** Configuration de Nagios XI (Setup 2)



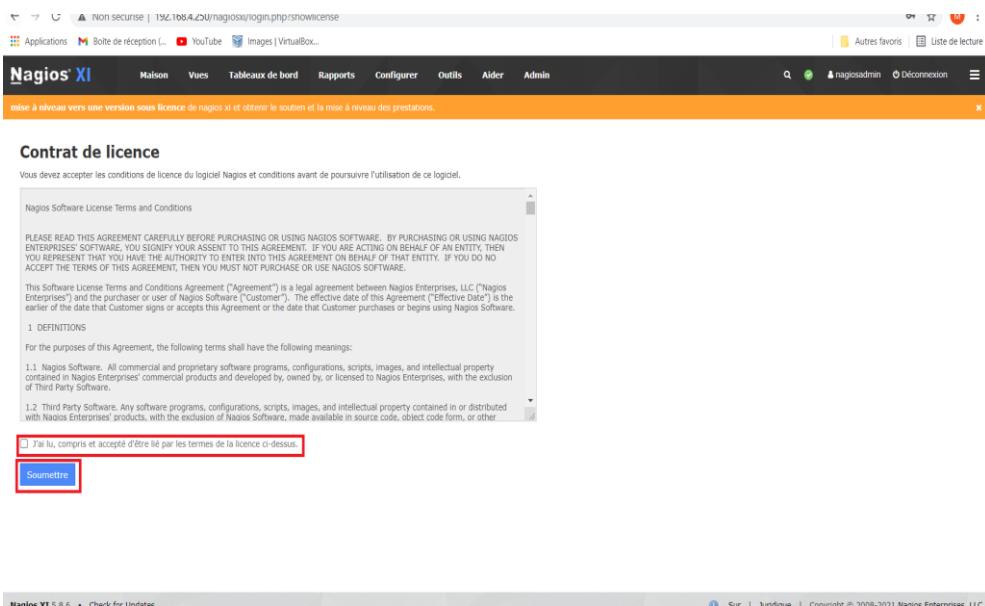
**Figure 21 :** Fin de l'installation

Une fois l'installation terminée, on met les accès pour pouvoir se connecter sur le serveur grâce au navigateur.



**Figure 22 :** Connexion au portail

On lit le contrat de licence, on coche la case puis on soumet.



**Figure 23 :** Contrat de licence

Ci-dessous l'interface web de notre serveur Nagios XI.

The screenshot shows the Nagios XI dashboard. On the left, there's a sidebar with 'Vue Rapide' (Quick View) containing links like Accueil Dashboard, Aperçu tactique, Birdseye, Centre des opérations, Écran opérations, Ouvrez problèmes de service, Ouvrez les problèmes d'accueil, Tous les problèmes de service, Tous les problèmes d'accueil, Panier du réseau, Détails (État du service, Résumé hostgroup, Vue d'ensemble du groupe d'hôtes, Grille hostgroup, Résumé servicehostgroup, Servicegroup/Aperçu Servicegroup Grille, BPI, Métrique), Graphiques (Graphiques sur le rendement, Graphique Explorateur), and Cartes (World Map, Bâton). The main area has three main sections: 'Guide de démarrage' with tasks like 'Modifier vos paramètres de compte', 'Modifier vos paramètres de notification', and 'Configurer votre installation de surveillance'; 'Résumé de l'état d'accueil' with a table showing 1 up, 0 down, 0 inaccessible, and 0 pending; and 'Résumé de l'état de service' with a table showing 12 up, 0 warning, 0 unknown, 0 critical, and 12 pending. There's also a sidebar with 'Nous sommes là pour vous aider!' featuring a photo of a support agent, and a footer with links like Forum, Ressources d'aide, Centre de support client, Support technique du client, and Auto-Discoveryemploi.

**Figure 24 :** Page d'accueil de Nagios XI

### II.2.1. Configuration de l'adresse IP du serveur

De nos jours, la plupart des dispositifs réseau tels que les routeurs ou commutateurs de réseau utilisent le protocole IP comme norme de communication sur le réseau. Dans le protocole IP, chaque dispositif du réseau possède un identifiant unique appelé IP. La méthode la plus simple pour l'obtenir était de configurer une adresse IP fixe ou une adresse IP statique. Comme il existe des limites aux IP statiques, certains administrateurs utilisent plutôt des IP dynamiques. DHCP (Dynamic Host Configuration Protocol) est un protocole permettant d'attribuer des adresses IP dynamiques aux appareils connectés au réseau.

Une adresse IP statique est une adresse qui est attribuée en permanence à vos appareils réseau par votre fournisseur d'accès Internet et qui ne change pas même si votre appareil est redémarré. Une adresse IP statique est généralement attribuée à un serveur qui héberge des sites web et fournit des services de courrier électronique, VPN et de FTP. [12]

Dans notre cas ici, nous allons utiliser Nagios comme serveur de supervision, nous allons mettre cette machine en statique. Ci-dessous les étapes de la configuration.

## Étape 1 :

Nous allons vérifier l'adresse IP que notre machine a reçu et en suite vérifier le port en tapant

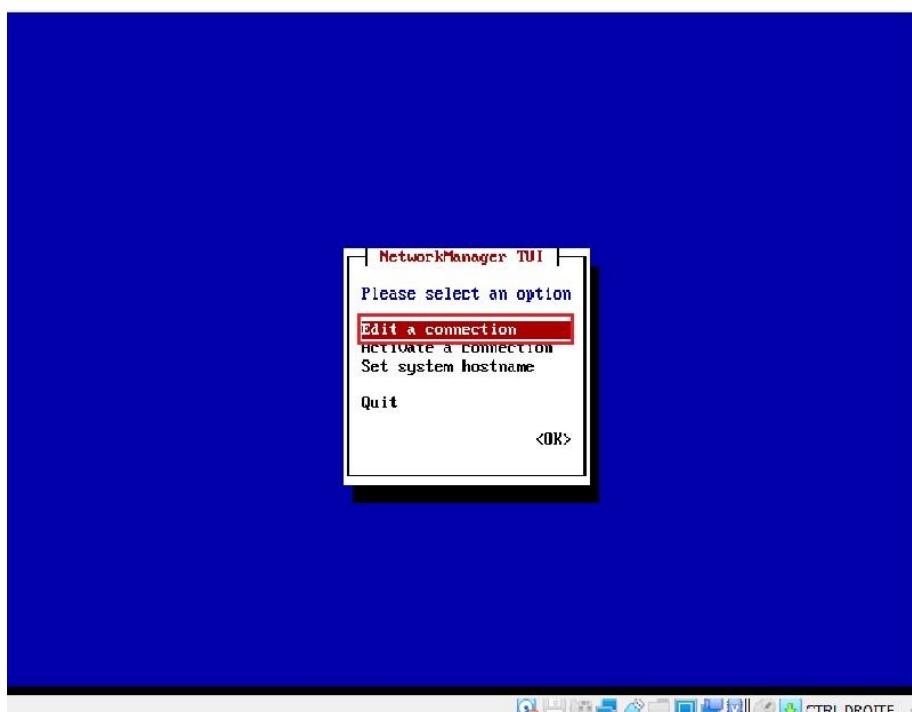
La commande **ip addr show**.

```
[root@localhost ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ad:aa:c2 brd ff:ff:ff:ff:ff:ff
        inet 192.168.4.2/24 brd 192.168.4.255 scope global nopref ixroute dynamic enp0s17
            valid_lft 388sec preferred_lft 388sec
        inet6 fe80::6871:fe14:8a87:1545/64 scope link nopref ixroute
            valid_lft forever preferred_lft forever
[root@localhost ~]#
```

**Figure 25 :** Vérification de l'adresse IP

## Étape 2 :

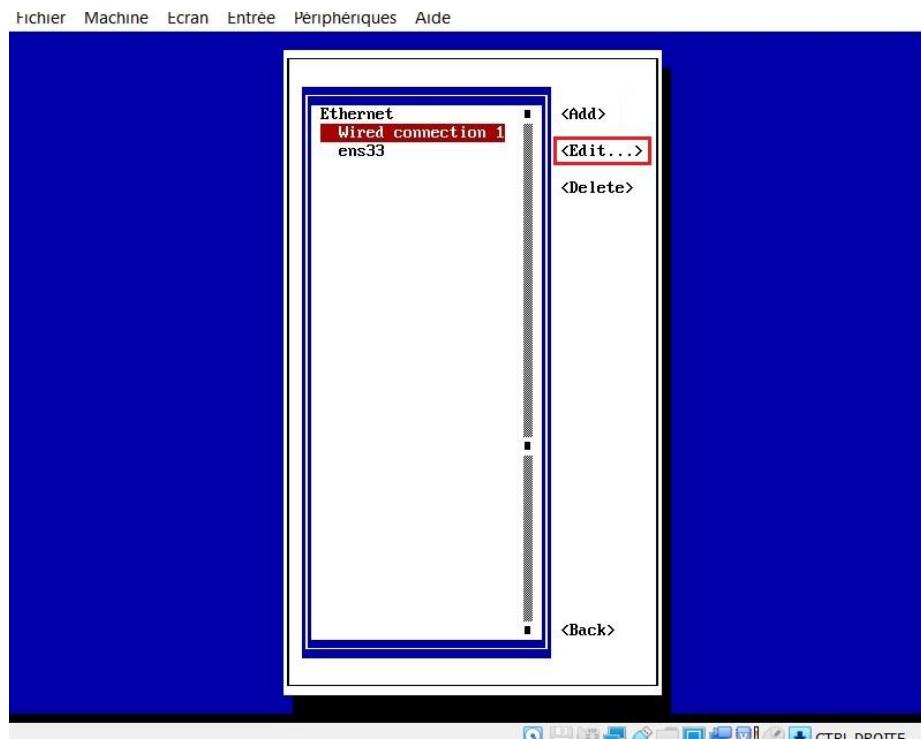
Nous allons taper la commande **nmtui** pour pouvoir accéder au port de la machine afin de changer l'adresse.



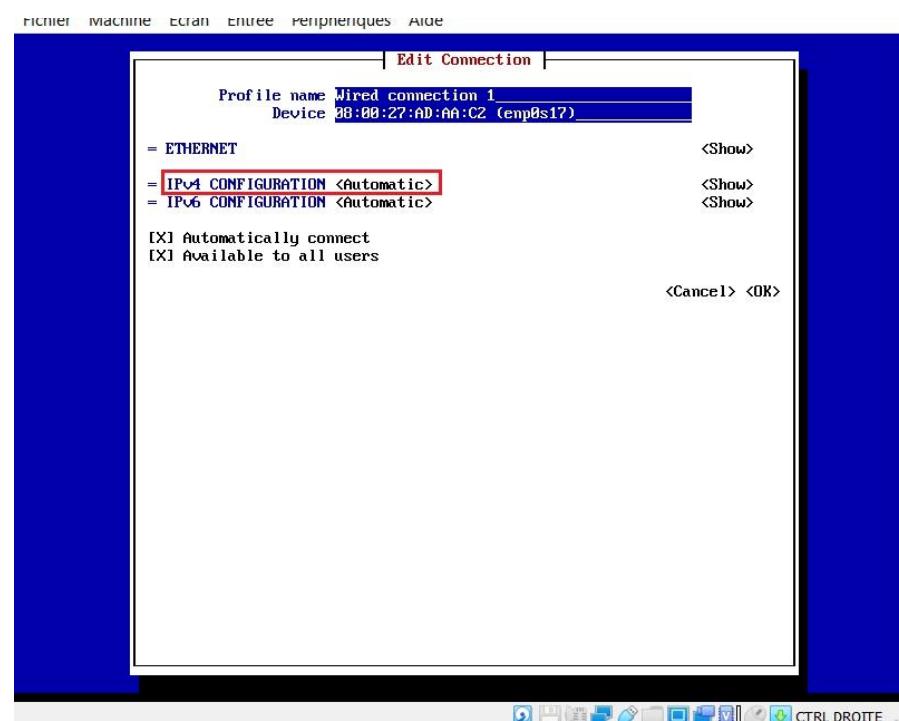
**Figure 26 :** configuration de l'adresse

### Étape 3 :

Nous allons taper sur Enter pour pouvoir éditer l'interface.



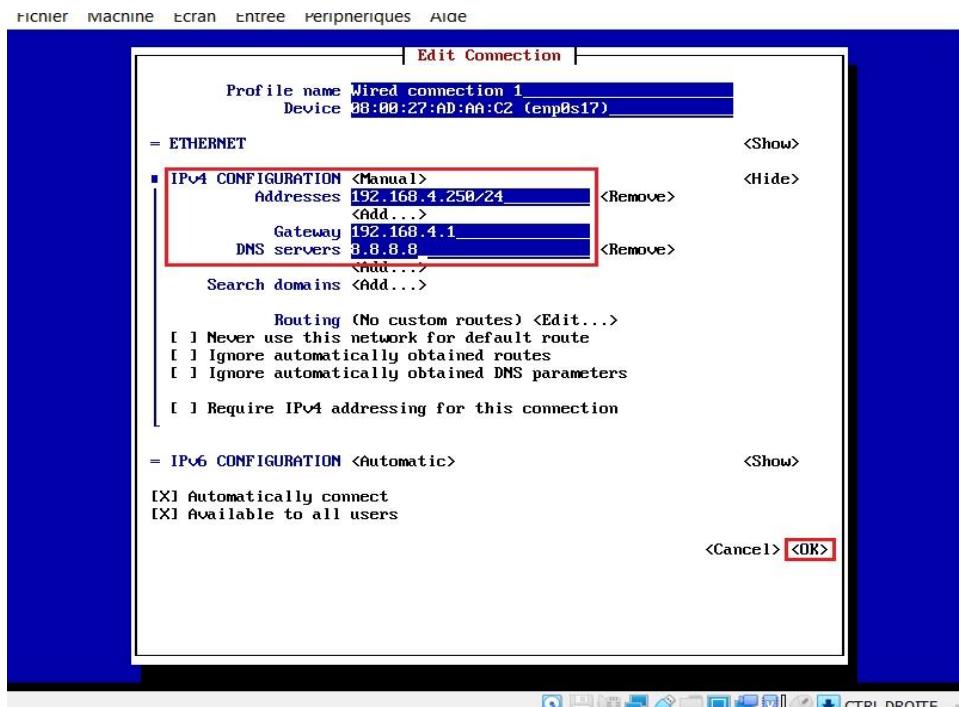
**Figure 27 :** configuration de l'interface *enp0s17*



**Figure 28 :** Choix de la configuration IPv4

## Étape 4 :

Une fois arrivé sur l'interface ci-dessus, nous allons mettre l'**IPv4 CONFIGURATION** en manuel puis clic sur show ; ensuite on renseigne les informations puis on fait OK.



**Figure 29 :** Fixation de l'adresse IP

## Étape 5 :

On désactive le port après on réactive pour pouvoir mettre à jour l'adresse qu'on a fixé en faisant **ifdown nom du port** pour désactiver, et **ifup nom du port** pour activer.

```
[root@localhost ~]# ifdown enp0s17
Device 'enp0s17' successfully disconnected.
[root@localhost ~]# ifup enp0s17
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)
[root@localhost ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ad:aa:c2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.250/24 brd 192.168.4.255 scope global noprefixroute enp0s17
        valid_lft forever preferred_lft forever
        inet6 fe80::6871:fe14:8a87:1545/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
[root@localhost ~]#
```

**Figure 30 :** Mise à jour de l'adresse IP

```
[root@localhost ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=25.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=26.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=25.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=26.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=34.7 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=114 time=26.5 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=114 time=26.3 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=114 time=30.5 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=114 time=26.7 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=114 time=32.9 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=114 time=31.4 ms
```

**Figure 31 :** Test vers Google

### II.3. Supervision d'une machine Windows

Pour pouvoir superviser une machine Windows, nous avons commencé par installer le module NCPA sur la machine à superviser, ensuite nous allons configurer Nagios XI.

#### II.3.1. Installation de l'agent NCPA

Avant de pouvoir superviser les attributs et services privés de la machine Windows, nous allons devoir installer un agent sur cette machine. [13]

NCPA est en fait deux services distincts qui constituent un seul agent de surveillance. Cette séparation permet à l'agent d'exécuter des vérifications passives sans avoir besoin d'autoriser les connexions à l'interface graphique Web ou d'autoriser les appels externes à l'API. Il permet également de désactiver la partie passive de l'agent si elle n'est pas utilisée pour économiser des ressources, même si la partie passive nécessite très peu de ressources lors de son exécution en arrière-plan.

Les étapes de l'installation de NCPA ci-dessous :

##### Étape 1 :

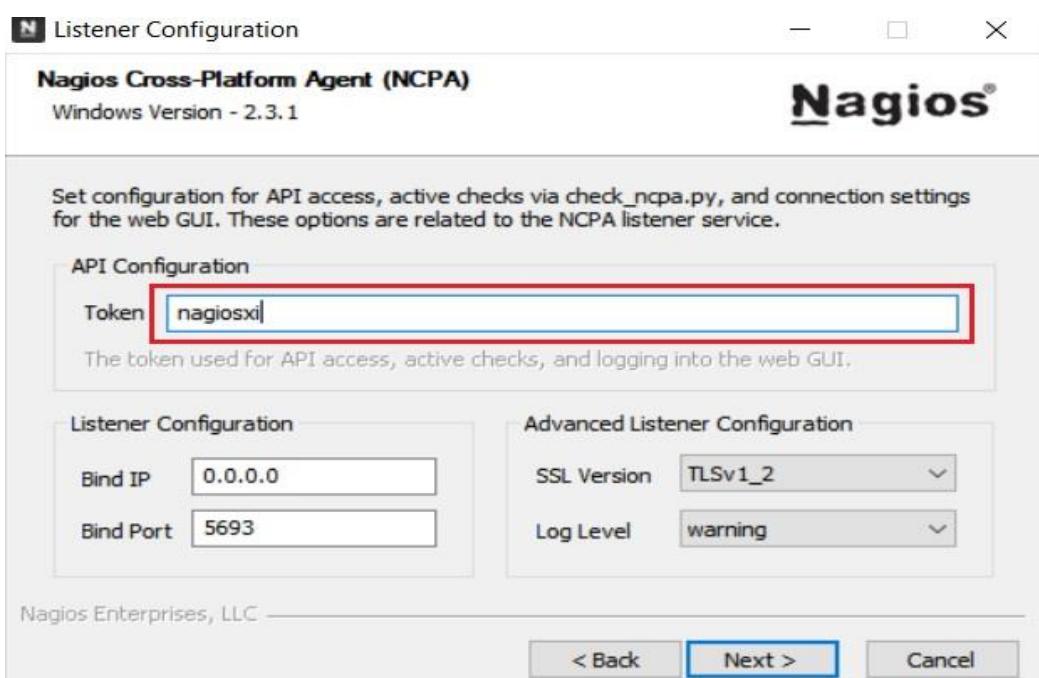
Dans un premier, nous allons faire un double clic sur le fichier NCPA qu'on a téléchargé depuis le répertoire de notre machine.



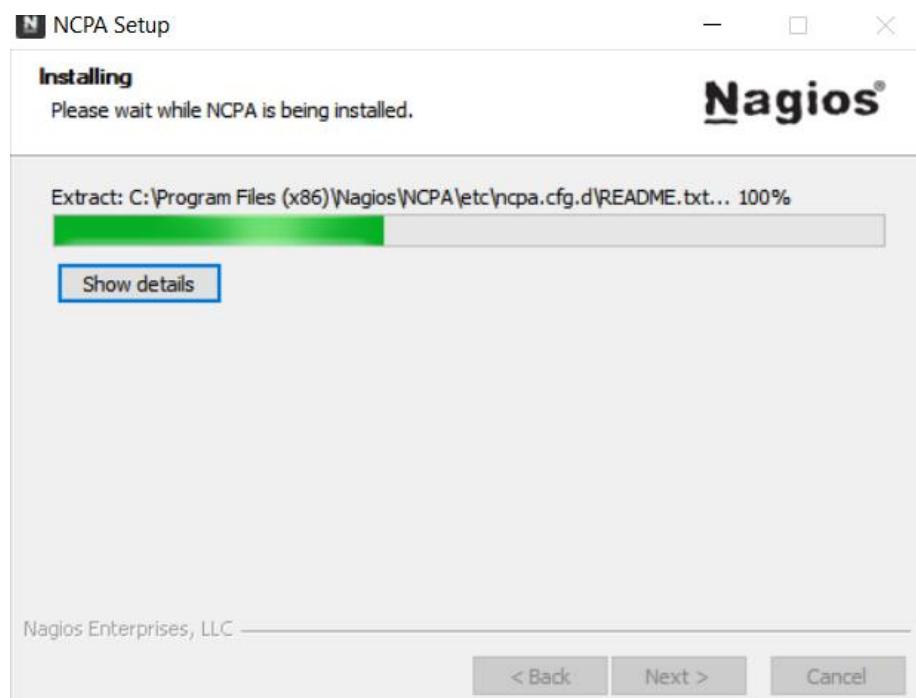
**Figure 32 :** Démarrage de l'installation de NCPA

## Étape 2 :

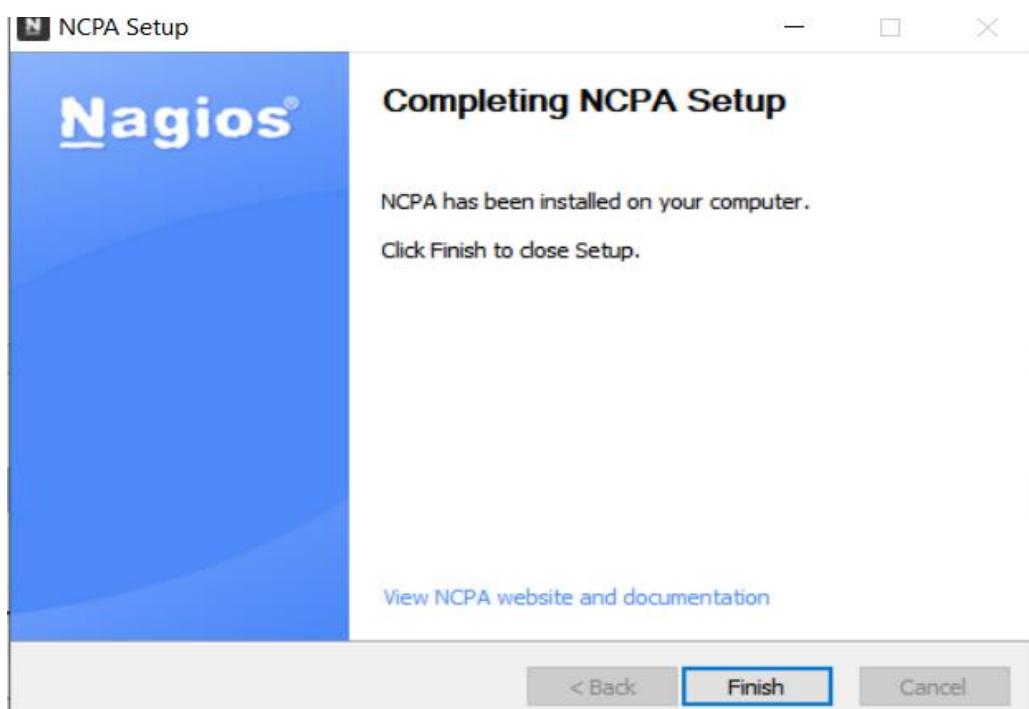
Ensuite, on met la clef API



**Figure 33 :** Insertion de l'API



**Figure 34 :** Démarrage de l'installation



**Figure 35 :** Fin de l'installation

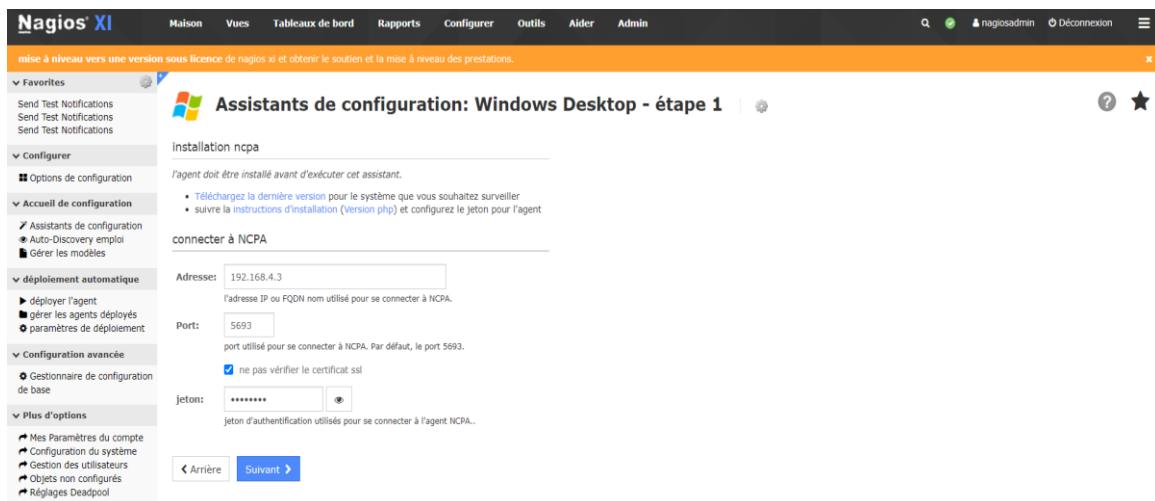
### II.3.2. Configuration de Windows dans Nagios XI

Une fois qu'on a terminé l'installation de l'agent sur la machine à superviser, nous terminer la configuration sur le serveur Nagios XI.

Ci-dessous, les étapes de la configuration :

#### Étape 1 :

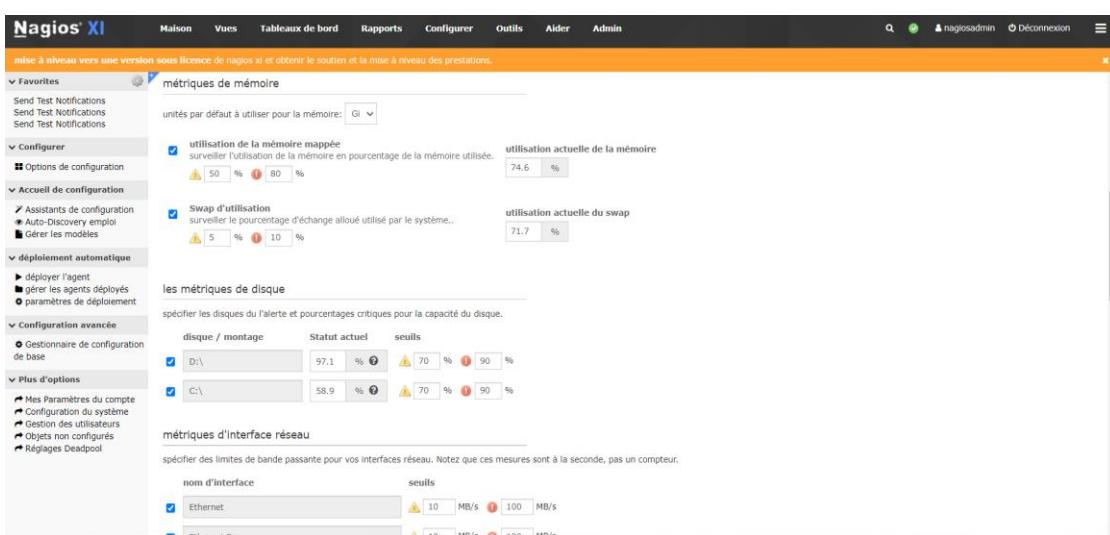
On ajout l'adresse IP de la machine et la clef API.



**Figure 36 :** Configuration de Windows

#### Étape 2 :

Dans cette étape, nous allons d'abord mettre le nom de la machine, ensuite mettre les seuils de l'utilisation du CPU, de la mémoire, le disque dur, l'interface réseau,... puis on fait suivant.



**Figure 37 :** Les seuils d'alertes

## Étape 3 :

Dans cette étape, nous allons définir les paramètres de base qui déterminent la façon dont la machine et les services doivent être surveillés.

The screenshot shows the Nagios XI configuration interface for a Windows Desktop host. The main title is "Assistants de configuration: Windows Desktop - étape 3". The left sidebar has sections like Favorites, Configurer (selected), Accueil de configuration, déploiement automatique, Configuration avancée, and Plus d'options. The main content area is titled "Paramètres de surveillance des" and includes fields for "Surveiller l'hôte et de service (s) à chaque [3] minutes." Below it is a section for "Lorsqu'un problème potentiel est détecté pour la première:" with a field "Vérifiez à nouveau l'hôte et de service (s) à chaque [1] minutes jusqu'à [5] fois avant envoyer une notification." At the bottom are buttons: "Arrière", "Suivant >" (highlighted in blue), and "Terminer". The footer shows "Nagios XI 5.8.6 • Check for Updates" and copyright information.

**Figure 38 :** Paramètre de base pour pouvoir superviser

The screenshot shows the Nagios XI configuration interface after step 3. The main title is "Windows Desktop Assistant de surveillance". The left sidebar is identical to Figure 38. The main content area shows a green success message: "Configuration appliquée avec succès" and "Vos modifications de configuration ont été appliquées avec succès à la surveillance du moteur." Below this is a "Demande Configuration réussie" section with two radio buttons: "Exécuter cet Assistant à nouveau suivant" (selected) and "Exécute un autre assistant de surveillance". There are also "Autres Options:" with links to "Voir détails sur l'état de Serveur" and "Voir les photos récentes de configuration". The footer is identical to Figure 38.

**Figure 39 :** Configuration terminée

## II.4. Supervision d'un équipement réseau (routeur Mikrotik)

Au sein de DANON'S GROUP, la plupart des clients de cette entreprise sont connectés à Internet par le MikroTik RB951Ui-2HnD.

### II.4.1. Description du routeur Mikrotik

Le Mikrotik RB951Ui-2HnD est un routeur sans fil proposant 5 ports Ethernet dont 1 en PoE Out (permet d'alimenter par exemple une NanoStation), 1 port USB 2.0 et un point d'accès 2.4 GHz avec antennes intégrées. Il est également possible de remplacer une antenne par de votre choix (connecteur MMCX). Le design compact et discret du RB951Ui-2HnD le rend idéal pour le bureau comme pour la maison. Il intègre des trous fixation murale. [14]

**Tableau 4 :** Caractéristiques du Mikrotik

Vitesse CPU	600 GHz
RAM	128 Mo
Ports LAN	5
Gigabit	Oui
USB	1
Alimentation	8 - 30V DC
PoE	8 - 30V sur Eth1 et 1 en Out sur Eth5
Poids	230g
Micrologiciel	RouterOS
Température de fonctionnement	-20° C to +50° C
Consommation	7W

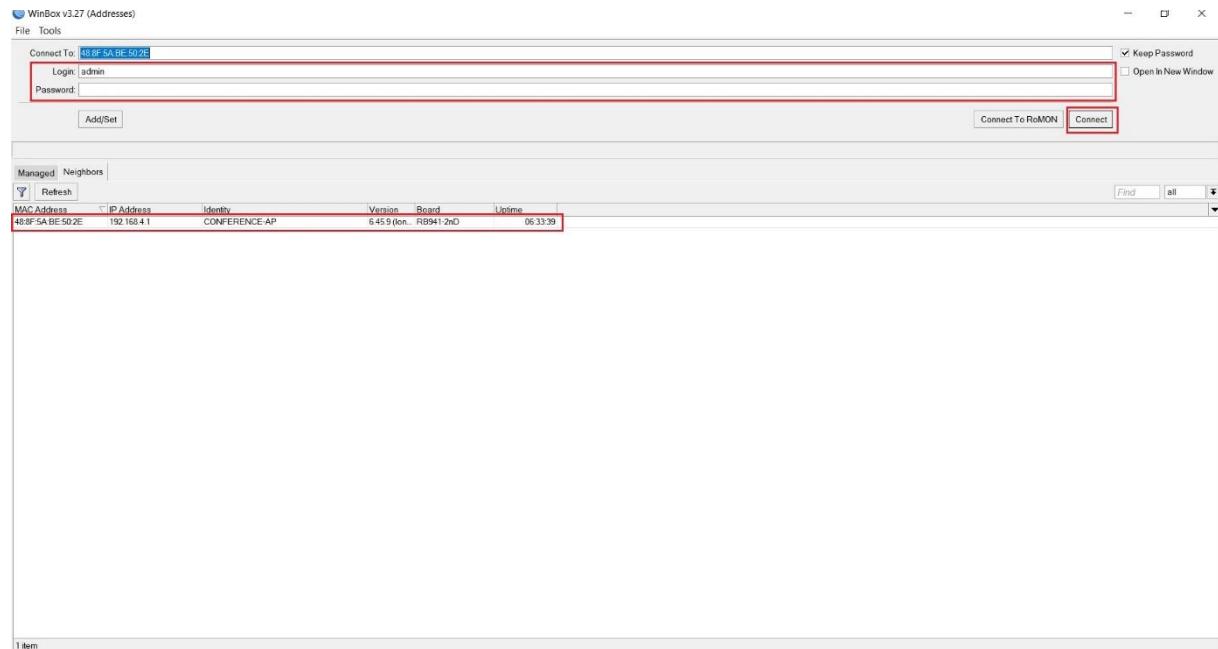
### II.4.2. Configuration du protocole SNMP sur le Mikrotik

Afin de pouvoir superviser le routeur Mikrotik, nous devons configurer le protocole SNMP sur le routeur Mikrotik, ci-dessous les étapes de la configuration :

#### **Étape 1 :**

On se connecte à l'interface du routeur Mikrotik grâce à l'application WinBox ; on peut se connecter soit par l'adresse mac ou l'adresse IP du routeur.

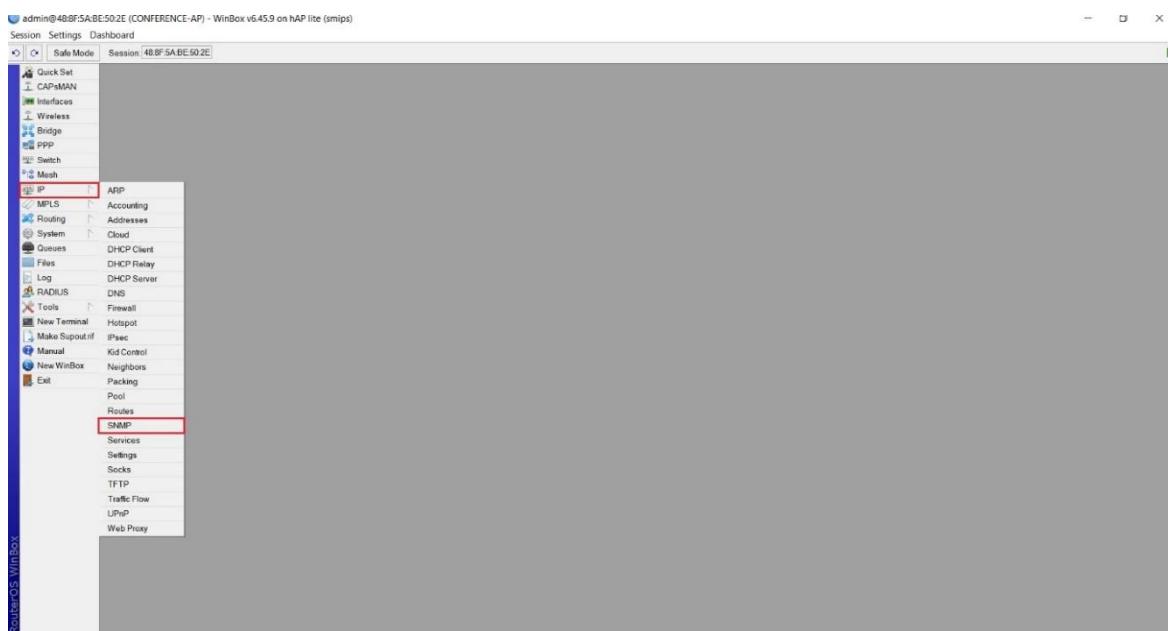
On renseigne le login et le password après avoir choisi le routeur qu'on veut attaquer puis on clique sur **connect**.



**Figure 40 :** Connexion au routeur

## Étape 2 :

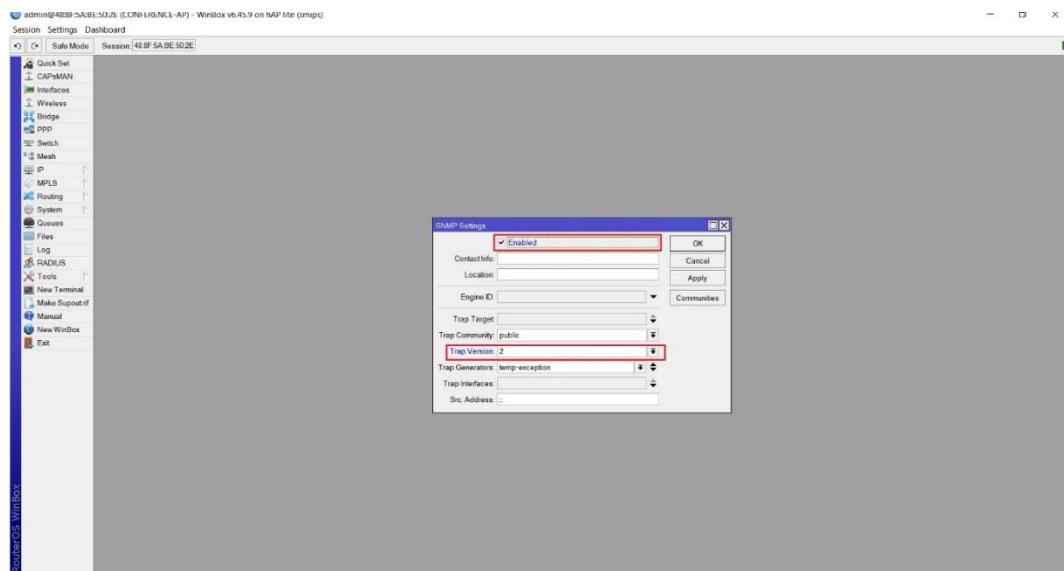
Après avoir accéder à l'interface de WinBox, on clique sur IP puis SNMP.



**Figure 41 :** accès à l'onglet SNMP

### Étape 3 :

Une fois accéder à l'onglet SNMP Settings, on coche la case **Enabled** pour pouvoir activer le protocole et met **Trap version 2.**



**Figure 42 :** activation du protocole SNMP

#### II.4.3. Ajout du Mikrotik sur le serveur Nagios XI

Pour ajouter le routeur Mikrotik sur le serveur, nous suivre les trois étapes ci-dessous :

## Étape 1 :

Nous allons cliquer sur **configurer** puis **assistants de configuration** choisir l'onglet **réseau** puis prendre **commutateur réseau / routeur**.

The screenshot shows the Nagios XI 5.8.6 interface. In the top navigation bar, 'Configurer' is selected. On the left sidebar, 'Configurer' is expanded, showing 'Assistants de configuration'. The 'Commutateur réseau / routeur' option is highlighted with a red border. Other options shown include Active Directory, DHCP, DNS Query, FTP, Imprimeur, Port TCP / UDP, Périphérique réseau générique, and SNMP.

**Figure 43 :** choix du type d'équipement à superviser

## Étape 2 :

Après avoir choisi **routeur**, nous allons renseigner l'adresse de l'équipement puis vérifier la version du protocole, puis on fait suivant.

The screenshot shows the 'Assists de configuration: Commutateur réseau / routeur - étape 1' configuration page. The 'Adresse IP' field is highlighted with a red border. Other fields shown include 'Port' (161), 'SNMPv2c' selected in the 'SNMPv1 / SNMPv2c / SNMPv3' dropdown, and 'public' in the 'Communauté SNMP' field. Below these, there are sections for 'Démons de surveillance' and 'Appliquer la configuration'.

**Figure 44 :** Renseignement de l'adresse IP

### Étape 3 :

Ensuite, on met le nom du routeur et on vérifie les services ainsi que les ports qu'on veut superviser, suivant.

The screenshot shows the Nagios XI configuration interface for a network switch/router. The main title is "Assistants de configuration: Commutateur réseau / routeur - étape 2". On the left, a sidebar lists various configuration options like Favorites, Configurer, Accueil de configuration, déploiement automatique, Configuration avancée, and Plus d'options. The main panel has sections for "Détails de commutation" (Address/routeur and host name), "Services" (Ping selected), and "La bande passante et l'état du port" (Ports Port1 and Port2 selected). A table shows port details and bandwidth monitoring thresholds. At the bottom, there are navigation buttons: « Arrière », « Suivant > », and a red-bordered "Terminer" (Finish) button.

**Figure 45 :** Nom du routeur

### Étape 4 :

On définit les paramètres de base qui déterminent la façon dont l'hôte et des services doivent être surveillés.

The screenshot shows the Nagios XI configuration interface for a network switch/router. The main title is "Assistants de configuration: Commutateur réseau / routeur - étape 3". The sidebar and table structure are similar to Figure 45. The main panel includes sections for "Paramètres de surveillance des" (normal circumstances: check every 3 minutes) and "Lorsqu'un problème potentiel est détecté pour la première:" (check again after 1 minute, up to 5 times before sending a notification). At the bottom, there are navigation buttons: « Arrière », "Suivant >", and a red-bordered "Terminer" (Finish) button.

**Figure 46 :** Fin de la configuration

## II.5. Notification par mail

Malgré l'existence d'une interface web permettant de voir l'état d'un hôte ou service en temps réel, la notification des contacts reste toujours obligatoire. Pour envoyer les notifications par mail depuis Nagios XI.

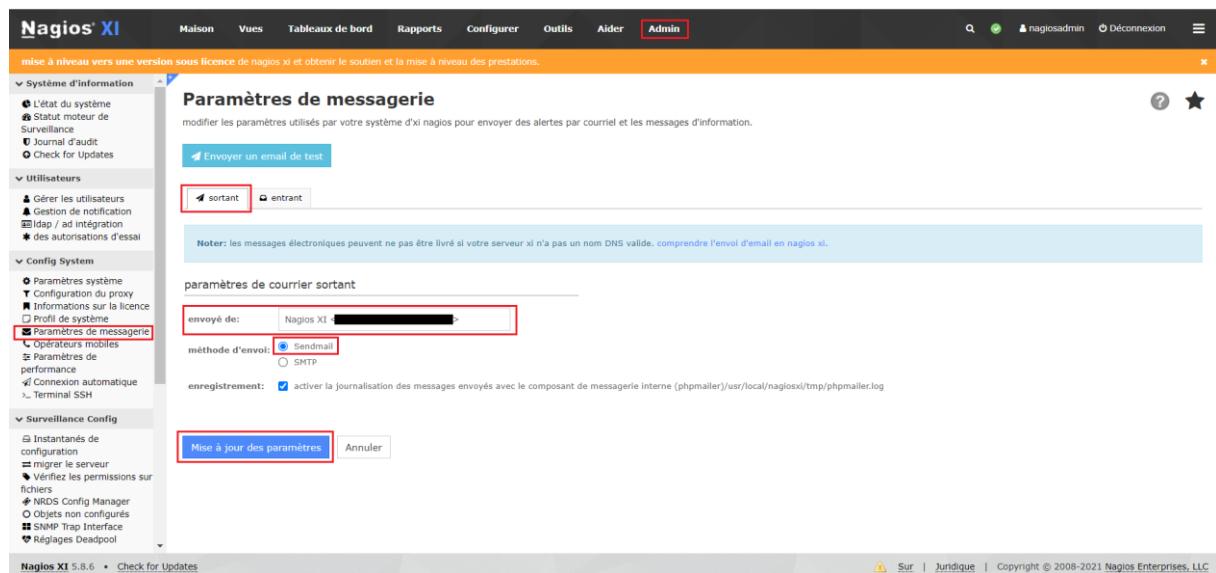
Ce qui permet d'avoir un historique d'activité pour les temps où l'administrateur n'est pas présent.

Les informations généralement nécessaires sont les suivantes :

- Le nom de la machine sur laquelle le problème est survenu ;
- L'élément qui est en faute sur la machine ;
- La criticité de l'alerte ;
- L'heure où le problème a été détecté ;
- Un petit texte explicatif du problème (une ligne ou deux maximums).

Nous allons utiliser la méthode **Sendmail** pour pouvoir configurer l'alerte par mail.

**Étape 1 :** Nous allons cliquer sur **Admin** puis **paramètre de messagerie** et remplir les cases.



**Figure 47 :** Configuration du paramètre de messagerie

**Étape 2 :** On met à jour les informations renseignées puis on envoie un message de test en cliquant sur **envoyer un message de test**.

The screenshot shows the Nagios XI web interface with the following details:

- Header:** Nagios XI, Maison, Vues, Tableaux de bord, Rapports, Configurer, Outils, Aider, Admin.
- Breadcrumbs:** mise à niveau vers une version sous licence de nagios xi et obtenir le soutien et la mise à niveau des prestations.
- Left sidebar:**
  - Système d'information: L'état du système, Statut majeur de Surveillance, Journal d'audit, Check for Updates.
  - Utilisateurs: Gérer les utilisateurs, Gestion de notification, LDAP / ad intégration, des autorisations d'essai.
  - Config System: Paramètres système, Configuration du proxy, Informations sur la licence, Profil de système, Paramètres de messagerie, Options mobiles, Paramètres de performance, Connexion automatique, Terminal SSH.
  - Surveillance Config: Instantanés de configuration, migrer le serveur, Vérifiez les permissions sur fichiers, NRDS Config Manager, Objets non configurés, SNMP Trap Interface, Réglages Deadpool.
- Current Page:** Paramètres de messagerie d'essai
- Content:**
  - A message box contains: "Un email de test a été envoyé à [REDACTED] Mailer a dit: [12-03-2021 06:41:14] Message sent! (method=sendmail), Referer: admin/testemail.php".
  - Text below: "Utiliser pour envoyer un message de test à votre actuellement connecté à l'adresse de l'utilisateur pour vérifier que vous pouvez recevoir des alertes de nagios xi."
  - Input field: "Un courriel sera envoyé à [REDACTED]" with placeholder "Changez votre adresse e-mail".
  - Buttons: < Arrière, Envoyer un message de test.
- Footer:** Nagios XI 5.8.6 • Check for Updates, Sur | Juridique | Copyright © 2008-2021 Nagios Enterprises, LLC.

**Figure 48 :** Envoi de message de test

On voit sur la figure ci-dessus que le message de test a été envoyé à l'adresse mail qu'on a renseigné.

The screenshot shows a Gmail inbox with the following details:

- Header:** Gmail, Rechercher dans les messages.
- Left sidebar:** Nouveau message, Boîte de réception, Messages suivis, En attente.
- Message Preview:**
  - Subject: Test de messagerieNagios XI
  - From: Nagios XI
  - Content: Il s'agit d'une notification par courrier électronique de test à partir de Nagios XI.
  - Time: 11:13 (il y a 1 heure)
- Footer:** 1 sur 76, various icons for reply, forward, etc.

**Figure 49 :** Vérification de la réception du mail de test

## II.6. Devis estimatif du matériel pour la mise en place de la solution

Le tableau ci-dessous présente l'ensemble des équipements à utiliser, ainsi que leur coût.

**Tableau 5 : Devis estimatif du matériel**

Désignation	Quantité/ Durée	Prix unitaire (FCFA)	Montant HT (FCFA)
Ordinateur bureau HP Core i5-8500T RAM 8Go Disque dur 1 To Processeur 2.60GHz Système d'exploitation 64 bits	01	400.000	400.000
Serveur Nagios XI	01	-	-
Licence (plus fonctionnalité de Nagios) renouvelable	01	1.158.996	1.158.996
Prestations (Mise à jour du logiciel) à chaque sortie d'une nouvelle version	-	-	-
Formation de 5 jours	35h	1.798.851	1.798.851
<b>Total</b>			<b>3.357.847</b>

## CONCLUSION GENERALE

Cette période de stage au sein de l'entreprise DANON'S GROUP nous a permis de connaître les réalités du milieu professionnel. Travailler au quotidien avec des professionnels du domaine sur une diversité de problèmes et d'environnement, nous a non seulement fait gagner en connaissances pratiques mais à connaître le monde professionnel.

L'étude nous a permis de comprendre l'importance de la supervision dans la mise en place des réseaux et systèmes informatiques au sein d'une structure et nous amène aujourd'hui à affirmer que : « le déploiement d'un système informatique ou d'un réseau quel que soit sa taille (petit, moyen ou grand), ne serait efficace que s'il intégrait un système de supervision » car la supervision augmente la qualité de service des réseaux et assure la réactivité des acteurs.

En effet, l'objectif de notre projet était de permettre à l'administrateur de l'entreprise de mieux superviser les équipements et les services de son réseau. Une solution de supervision permet de diminuer le taux lors de diagnostic des pannes et faciliter les tâches de l'administrateur réseau.

Plus le nombre des équipements et services informatiques augmente, plus les tâches de l'administrateur deviennent trop compliquées et il n'arrive pas à les assurer convenablement. Ce qui engendre une perte du temps et un travail non accomplie.

Ce stage fut pour nous l'occasion de mettre en pratique les connaissances acquises durant notre formation académique et d'acquérir des compétences sur l'administration réseau et la supervision à travers la mise en place du logiciel de supervision Nagios XI.

Comme perspective, nous proposons l'amélioration de ce travail par :

- La configuration des notifications par SMS ;
- Configuration d'alerte par mail en utilisant la méthode SMTP ;

## BIBLIOGRAPHIE

- [1] Orsenna « **Mise en œuvre d'une solution de supervision Nagios XI V 5.4.13** », 53 pages.
- [2] *Rapport de stage réalisé par Chamseddine Oueslati « **Mise en place d'une solution de supervision open source, Cas d'étude la Poste tunisienne** »*, Université Virtuelle de Tunis ; 65 pages.
- [3] *Rapport de stage réalisé par HOUACINE Yasmine et DJALI Lylia « **Mise en place d'un outil de supervision dans un réseau d'entreprise. Cas d'étude : OPGI** »*, Université Bejaia ; 79 pages.
- [4] *Rapport de stage réalisé par Ghada Ben Sassi « **Mise en place d'un outil de supervision de réseau d'entreprise** »*, Université Virtuelle de Tunis ; 76 pages.
- [5] *Rapport de stage réalisé par DJEGMDE Harouna « **Etude et mise en place d'un serveur de supervision avec Nagios et Cacti : cas de l'ONASER** »*, Université Aube Nouvelle ; 76 pages.
- [6] *Rapport de stage réalisé par BANAO Hamed « **Déploiement d'une solution de supervision réseau basée sur Nagios** »*, Université Aube Nouvelle ; 86 pages.

## WEBOGRAPHIE

- [7] <http://www.memoireonline.com> consulté le 09 Mai 2021 à 11h 10min.
- [8] <http://www.nagios.org> site officiel de nagios, consulté le 15 Mai 2021 à 15h 27min.
- [9] <https://support.nagios.com> consulté le 16 Mai 2021 08h 35min.
- [10] <http://exchange.nagios.org/> consulté le 17 Mai 2021 20h 47min.
- [11] <http://www.o00o.org/monitoring/bases.html> consulté le 29 Mai 2021 à 23h 40min.
- [12] <https://community.fs.com/fr/blog/dhcp-vs-static-ip-differences.html> consulté le 02 Juin 2021 à 13h 38min.
- [13] <https://www.nagios.org/ncpa/#downloads> consulté le 08 Juin 2021 à 09h 36min.
- [14] <https://www.wifi-france.com/mikrotik/mikrotik-rb951ui-2hnd> consulté le 08 Juin 2021 à 11h 40min.

## TABLE DES MATIERES

SOMMAIRE .....	
DEDICACE.....	II
REMERCIEMENT .....	III
AVANT - PROPOS .....	IV
LISTE DES SIGLES ET ABREVIATIONS .....	V
LISTE DES FIGURES .....	VI
LISTE DES TABLEAUX.....	VIII
RESUME.....	IX
ABSTRACT .....	X
INTRODUCTION GENERALE.....	1
PROBLEMATIQUE .....	2
CHAPITRE I : Présentation de la structure de formation et de la structure d'accueil .....	3
Introduction .....	3
I.    Structure de formation (Université Aube Nouvelle) .....	3
I.1. présentation générale.....	3
I.2. Objectifs .....	3
I.3. Formations .....	5
I.4. La filière Technologie des réseaux et systèmes .....	6
II.    Structure d'accueil (DANON'S GROUP).....	7
II.1. Présentation générale .....	7
II.1.1. Visions .....	7
II.1.2. Missions .....	7
II.1.3. Valeurs .....	8
II.1.4. Organisation et fonctionnement.....	8
II.1.5. Produits et services de DANON'S GROUP .....	10
II.2. Présentation du réseau informatique de DANON'S GROUP .....	11
CHAPITRE 2 : Étude théorique et l'état de l'art et choix de l'outil .....	14
Introduction .....	14
I.    La supervision informatique.....	14
I.1. Définition .....	14
I.2. Rôle de la supervision .....	15
I.3. La supervision des réseaux.....	15
I.3.1. Définition .....	15
I.4. Principe de la supervision .....	15

I.5. La norme ISO 7498/4.....	16
I.5.1. Gestion des performances .....	16
I.5.2. Gestion des configurations.....	17
I.5.3. Gestion de la comptabilité.....	17
I.5.4. Gestion des anomalies.....	17
I.5.5. Gestion de la sécurité .....	17
II.    Les aspects de la supervision.....	18
II.1. Fonctionnement d'une plateforme de supervision.....	18
II.2. Les méthodes de la supervision .....	18
II.3. Les standards de la supervision .....	19
II.3.1. Intelligent Platform Management Interface (IPMI) .....	19
II.3.2. Java Management Interface (JMX).....	20
II.3.3. Common Information Model (CIM) .....	20
II.3.4. Information Technology Infrastructure Library (ITIL) .....	20
II.3.5. Standard Based Linux Instrumentation for Manageability (SBLIM) .....	20
II.3.6. Web Based Enterprise Management (WEBBEM).....	21
II.3.7. Web Services for Management (WS-MANAGEMENT) .....	21
II.3.8. Windows Management Instrumentation .....	21
II.3.9. Simple Network Management Protocol (SNMP) .....	21
II.3.9.1. Présentation.....	21
II.3.9.2. Les différentes versions du SNMP .....	22
II.3.9.3. Architecture .....	22
II.3.9.4. Principe de fonctionnement .....	23
II.3.9.5. La MIB.....	24
II.3.9.6. L'agent SNMP .....	24
II.3.10. Internet Control Message Protocol (ICMP) .....	25
II.4. Étude comparative des outils de supervision open source.....	25
II.4.1. Cacti .....	25
II.4.2. Zabbix .....	26
II.4.3. Nagios .....	27
II.5. Tableau comparatif des outils de supervision .....	28
III.    Étude technique détaillée de Nagios XI .....	29
Introduction .....	29
III.1. Présentation de Nagios .....	29
III.2. Choix de l'outil.....	29

III.3. Architecture de Nagios .....	30
III.4. Principe de fonctionnement de Nagios.....	31
III.5. Les plugins .....	32
III.5.1. Les plugins locaux.....	33
III.5.2. Les principaux plugins .....	33
III.6. Supervision passive et active.....	34
III.6.1. Les plugins actifs avec NRPE .....	34
III.6.2. Les plugins passifs avec NSCA.....	35
III.7. Les fichiers de configurations .....	36
Conclusion.....	37
<b>CHAPITRE 3 : Mise en place de la solution de supervision adoptée .....</b>	<b>38</b>
Introduction .....	38
I. Environnement de travail .....	38
I.1. Environnement matériel .....	38
I.2. Environnement logiciel .....	38
I.2.1. Oracle VM VirtualBox.....	38
I.2.2. Système d'exploitation.....	38
I.2.3. Navigateur .....	39
II. Installation et configuration de Nagios XI .....	39
II.1. Prérequis .....	39
II.2. Installation de Nagios XI .....	39
II.2.1. Configuration de l'adresse IP du serveur.....	45
II.3. Supervision d'une machine Windows .....	49
II.3.1. Installation de l'agent NCPA .....	49
II.3.2. Configuration de Windows dans Nagios XI .....	52
II.4. Supervision d'un équipement réseau (routeur Mikrotik).....	54
II.4.1. Description du routeur Mikrotik .....	54
II.4.2. Configuration du protocole SNMP sur le Mikrotik .....	54
II.4.3. Ajout du Mikrotik sur le serveur Nagios XI .....	56
II.5. Notification par mail .....	59
II.6. Devis estimatif du matériel pour la mise en place de la solution.....	61
<b>CONCLUSION GENERALE .....</b>	<b>62</b>
<b>BIBLIOGRAPHIE .....</b>	<b>XII</b>
<b>WEBOGRAPHIE.....</b>	<b>XIII</b>
<b>TABLE DES MATIERES .....</b>	<b>XIV</b>

