N° d'ordre : 666/RS/TCO Année universitaire : 2017 / 2018

UNIVERSITÉ D'ANTANANARIVO

INSTITUT D'ENSEIGNEMENT SUPERIEUR

ANTSIRABE VAKINANKARATRA (IES-AV)

MENTION TELECOMMUNICATION

MEMOIRE

en vue de l'obtention

du diplôme de LICENCE

Domaine : Science de l'Ingénieur

Mention : Télécommunication

Parcours : Réseaux et Systèmes

Par : **RAMANGASALAMA Tahiana Hortensia**

Titre : ETUDES ET MISE EN PLACE D'UNE SOLUTION DE SUPERVISION RÉSEAU ET SYSTEME (CAS DE L'INSTAT)

Soutenu le lundi 29 avril 2019 devant la commission d'examen composée de :

Président de Jury **:** **M. ANDRIANAIVONDRIAKA Nirina Alain**

Examinateurs **:**

Mme RALAIBOZAKA Tahina Nancy Muriel

M. RASOANAIVO Andrianirina

Directeur de mémoire: **M. RAKOTONDRAMANANA Radiarisainana Sitraka**

TENY FISAORANA

Ny voalohan-teny dia misaotra an'Andriamanitra Lehibe noho izao dingana izao, misaotra azy tamin'ny famindram-pony, ny fitsimbinany sy ny fitantanany hatrany ny fiainana indrindra tamin'ny fanomanana ity asa ity.

Manolotra ny fisaorana ihany koa ho an':

- Andriamatoa RAMANOELINA Panja Armand, Profesora, Filohan'ny Oniversiten'Antananarivo.
- Andriamatoa RAJAONARISON Eddie Franck, Talen'ny « Institut d'Enseignement Supérieur Antsirabe Vakinankaratra (IES-AV) ».

Misaotra manokana an'Andriamatoa RANDRIANANDRASANA Marie Emile, Dokotera sady mpiandraikitra ny sampam-pampianarana Fifandraisan-davitra eto amin'ny oniversite.

Tsy hay ihany koa ny tsy hisaotra an'Andriamatoa ANDRIANAIVONDRIAKA Nirina Alain, Dokotera amin'ny fifandraisan-davitra nanaiky hitarika ny fitsarana izao asa izao.

Manolotra ny fisaorana an'Andriamatoa RAKOTONDRAMANANA Radiarisainana Sitraka, mpampianatra mpikaroka, nanome ireo toromarika rehetra ilaina tamin'ny fanatontosana ny boky.

Tsy hay ihany koa ny tsy hisaotra an'ireo mpanabe manaiky hitsara ny fampisehoana ny boky. Ao :

- Ramatoa RALAIBOZAKA Tahina Nancy Muriel, mpampianatra mpikaroka.
- Andriamatoa RASOANAIVO Andrianirina, mpampianatra mpikaroka.

Tolorana fisaorana manokana ihany koa:

- Andriamatoa RAJAONERA Ida Clément, Tale jeneralin'ny INSTAT, toerana nanaovana ny fianaran'asa.
- Andriamatoa RASOLOFOSON Roger, Tale ny kabinetra Informatika ao amin'ny INSTAT, tamin'ny fandraisana ahy tao amin'ny kabinetrany.
- Andriamatoa RAZAFILALAO Adel Nirina, lehiben'ny « Service Exploitation des Systèmes » ao amin'ny INSTAT tamin'ny fizarana ny traikefa ananany nandritry ny fianaran'asa.

Mankasitraka indrindra ireo mpanabe sy mpandraharaha rehetra eto amin'ny oniversite indrindra ny ao amin'ny sampam-pampianarana « Télécommunication ». Mankatelina an'ny fianankaviana, ny namana, ireo rehetra nandray anjara tamin'ny fanomanana ity boky ity na mivantana izany na ankolaka. Andriamanitra manan-karem-pahasoavana anie hamaly fitia ho anareo rehetra.

REMERCIEMENTS

Avant toute chose, je glorifie Seigneur Dieu Tout Puissant de m'avoir donné toute la force, la santé, le courage et les moyens nécessaires pour l'accomplissement de cet ouvrage.

Je tiens à remercier sincèrement :

- Monsieur RAMANOELINA Panja, Professeur, Président de l'Université d'Antananarivo.
- Monsieur RAJAONARISON Eddie Franck, Maître de Conférences, Directeur de l'Institut d'Enseignement Supérieur Antsirabe Vakinankaratra.
- Monsieur RANDRIANANDRASANA Marie Emile, Docteur et Responsable de la Mention Télécommunication au sein de l'IES-AV.

J'exprime également ma reconnaissance à :

- Monsieur ANDRIANAIVONDRIAKA Nirina Alain, Docteur en Télécommunication qui me fait l'honneur de présider le jury de ce mémoire.

Un grand merci à Monsieur RAKOTONDRAMANANA Radiarisainana Sitraka, Directeur de ce mémoire, pour ses précieux conseils qui m'ont aidé à améliorer mon travail.

Ma gratitude et ma reconnaissance les plus sincères vont aux membres du jury composés de :

- Madame RALAIBOZAKA Tahina Nancy Muriel, Assistante d'Enseignement Supérieur et de Recherche.
- Monsieur RASOANAIVO Andrianirina, Assistant d'Enseignement Supérieur et de Recherche.

Je remercie particulièrement :

- Monsieur RAJAONERA Ida Clément, Directeur Général de l'INSTAT.
- Monsieur RASOLOFOSON Roger, Directeur Informatique de l'INSTAT qui a bien voulu m'accueillir au sein de sa direction.
- Monsieur RAZAFILALAO Adel Nirina, Chef de Service Exploitation des Systèmes, encadreur professionnel pour son accueil, sa disponibilité et le partage de son expertise au quotidien.

Je remercie tous les enseignants et les personnels de l'IES-AV, qui ont consacré la plupart de leur temps à nous partager leurs connaissances.

Enfin, je voudrais remercier profondément ma famille, mes amis, mes collègues étudiants qui m'ont soutenu moralement et m'ont aidé pour la réalisation de mon projet.

Merci infiniment a tous ceux qui ont contribué de loin ou de près à la réalisation de cet ouvrage.

TABLE DES MATIERES

ABREVIATIONS

ADSL	Asymetric Digital Subscriber Line
ASN.1	Abstract Syntax Notation number one
CPU	Central Processor Unit
DHCP	Dynamic Host Configuration Protocol
DI	Direction Informatique
DDSS	Direction de la Démographie et de la Statistique Sociale
DNS	Domain Name Server
DOD	Departement Of Defense
DRID	Direction des Relations Institutionnelles et de la Diffusion
DSM	Direction des Statistiques et des Ménages
EON	Eyes Of Network
FAI	Fournisseur d'Accès Internet
FAN	Fully Automated Nagios
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
GNU	Gnome Not Unix
GPL	Global Public Licence
HDD	Hard Drive Disk
HP/OV	Hewlett Packard Open View
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfert Protocol Secure
IBM	International Business Machines Corporation
IEEE	Institute of Electrical and Electronical Engineers

IETF	Internet Engineering Task Force
IHM	Interface Homme Machine
INSTAT	Institut National de la Statistique
IP	Internet Protocol
IPX	Internet Packet eXchange
ISO	International Organization of Standardization
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Medium Access Control
MAN	Metropolitan Area Network
MBPS	Megabits Per Second
MIB	Management Information Base
MTA	Mail Transfer Agent
MySQL	My Structured Query Language
NDO	Nagios Data Out
NMAP	Network Message Access Protocol
NMS	Network Management Station
NNM	Network Node Manager
NRPE	Nagios Remote Plugin Executor
NSCA	Nagios Service Check Acceptor
OID	Object IDentifier
OSI	Open System Interconnection
PC	Personal Computer
PCI	Peripheral Component Interconnect
PDU	Protocol Data Unit

POP	Post Office Protocol
RAM	Random Access Memory
RFC	Request For Comments
RJ-45	Registered Jack -45
RRD	Round Robin Database
SASL	Simple Authentication and Security Layer
SCOM	Microsoft System Center Operation Manager
SGBD	Systeme de Gestion de Base de Données
SMI	Structure of Management Information
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
STP	Shielded Twisted Pair
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

LISTES DES TABLEAUX ET DES FIGURES

1. Liste des tableaux

2. Liste des figures

INTRODUCTION GENERALE

Le monde actuel parait être sous l'emprise de l'évolution de la technologie de l'information et de la communication. La Télécommunication est une des principales clés du développement de cette technologie. En effet, la Télécommunication est l'ensemble des procédés de transmission d'information à distance avec des moyens de base d'électronique et d'informatique et de transmission filaire, optique ou électromagnétique.

L'échange des informations en Télécommunication est surtout assuré par un ensemble bien organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. Cet ensemble est appelé un système d'information et il tient une place importante dans les entreprises.

Vue la limite de la science, les problèmes rencontrés dans ces systèmes d'informations proviennent généralement de la panne ou du dysfonctionnement des matériels qui sont généralement les ordinateurs. En effet, ces derniers sont d'un grand nombre dans les entreprises.

Etant une étudiante en télécommunication, gérer les incidents du réseau rencontrés dans les entreprises nous parait primordial du fait que la réparation d'une panne peut avoir un très grand impact sur le déroulement du travail des utilisateurs et des employés.

C'est pourquoi, superviser l'état des éléments générant la communication dans les entreprises, les ordinateurs et ses dérivés voire le réseau, nous parait nécessaire. En effet, superviser ces machines permet d'anticiper et de prévoir les éventuels besoin en termes d'équipement pour une gestion optimale du système d'information ou du réseau.

C'est la raison pour laquelle le thème de ce mémoire s'intitule: « Etudes et mise en place d'une solution de supervision réseau et système».

Le présent mémoire résume l'ensemble des actions entreprises pour la réalisation de ce projet dont la première partie est la présentation du réseau informatique en générale ou généralité sur les réseaux. La seconde partie abordera la supervision informatique proprement dite et la troisième partie sera consacrée à la mise en place d'une solution de supervision réseau et système.

CHAPITRE 1
GÉNÉRALITÉS SUR LES RÉSEAUX

1.1 Introduction

De nos jours les systèmes d'informations sont devenus des éléments clés pour les entreprises, ils deviennent de plus en plus complexes, vastes et importants, ce qui demande énormément de temps pour la gestion et la maintenance. Pour pouvoir gérer et maintenir le réseau informatique, étudier les généralités sur les réseaux est primordial.

1.2 Notions sur les réseaux

1.2.1 Définitions

Définition 1.01 :

Un réseau est un moyen qui permet à des individus ou à des groupes de personnes de partager des informations et des services.

En informatique, un réseau est un ensemble d'ordinateurs et de périphériques connectés les uns avec les autres dont le but est de faire circuler et partager des ressources ou informations dans un certain domaine géographique.

Définition 1.02 :

Le réseau informatique est donc, un ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangent des informations sous forme numériques.

Définition 1.03 :

L'internet, c'est un réseau public mondial sur lequel des millions d'ordinateurs sont interconnectés grâce à la pile de protocole Transmission Control Protocol/Internet Protocol ou TCP/IP.

Définition 1.04 :

L'intranet, c'est un réseau basé sur les mêmes protocoles TCP/IP qui exploite les mêmes applications que sur Internet sauf que son accès est réservé aux employés de l'entreprise concernée.

Définition 1.05 :

L'extranet, c'est une interconnexion d'Intranet à travers l'Internet au moyen du tunnel Virtual Private Network ou VPN, c'est-à-dire que les échanges sont sécurisés sur un cryptage de données.

1.2.2 Nécessité d'un réseau

Le réseau informatique est nécessaire pour :

- Le partage et le transfert de fichiers ;
- La sécurisation des données ;
- Le partage d'application: compilateur, système de gestion de base de données ou SGBD ;
- Le partage d'imprimante ;
- L'interaction avec utilisateurs connectés : messagerie électronique, conférence électronique, talk, etc. ;
- Le transfert de la parole (réseaux téléphoniques) ;
- Le transfert de la vidéo et des données (Réseaux à Intégration de Service ou Multimédia) ;
- La sauvegarde et le traitement de données.

1.2.3 Terminologie

Cette terminologie comprend quelques vocabulaires de base du réseau informatique comme :

Station de travail : c'est toute machine capable d'envoyer des données sur des réseaux et ayant sa propre carte d'interface réseau.

Nœud : c'est une station de travail, une imprimante, un serveur ou toute entité pouvant être adressés par un numéro unique. L'unicité de cette adresse est garantie par le constructeur d'une carte réseau qui ce dernier donne un numéro et ce numéro ne peut pas être changé par une personne.

Serveur : c'est une machine sur laquelle tourne un logiciel serveur offrant des services à des logiciels utilisateurs. C'est aussi un dépositaire central d'une fonction spécifique : serveur de base de données, de calcul, de fichier, etc.

Client : c'est une machine sur laquelle tourne un logiciel client (programme qui traite des informations qu'il récupère auprès d'un serveur).

Protocole : c'est un spécifique standard qui permet la communication entre deux équipements. Par ailleurs, c'est l'ensemble des règles et des procédures qui définissent le type de codage et la vitesse utilisée pendant la communication, ainsi que la façon d'établir et de terminer la connexion.

Paquet : c'est la plus petite entité d'information pouvant être envoyée sur le réseau. Un paquet contient en général l'adresse de l'émetteur, l'adresse du récepteur et les données à transmettre.

Routeur : c'est un périphérique qui détermine la prochaine destination du paquet.

Topologie : c'est une organisation physique et logique d'un réseau.

L'organisation physique concerne la façon dont les machines sont connectées (bus, anneau, étoile, maillée, arborescent, etc..). La topologie logique montre comment les informations circulent sur le réseau (diffusion, point à point).

1.3 Types de réseaux

En général, il y a trois (3) types de réseaux informatiques suivant la distance qui sépare les ordinateurs ; selon leurs tailles (nombre de machines), leur vitesses de transfert, et leur étendue géographiques. Ce sont :

- Réseau LAN (Local Area Network) ;
- Réseau MAN (Metropolitan Area Network) ;
- Réseau WAN (Wide Area Network).

1.3.1 Réseau Local LAN

Le réseau est LAN, lorsque les ordinateurs reliés entre eux sont situés dans un même site (par exemple une entreprise, université, etc.) c'est-à-dire que le réseau est limité dans un terrain géographique réduite comme un bâtiment par exemple.

Une connexion en réseau local ou LAN comprend trois éléments principaux qui sont le système de câblage, l'adaptateur réseau (carte réseau), le logiciel d'exploitation.

La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (réseau Fast Ethernet) et 1 Gbps (en FDDI ou Gigabit Ethernet). La taille d'un réseau local peut atteindre jusqu'à 100, voire 1000 utilisateurs. [1.01]

Les services en réseau local peuvent se faire sous deux modes de fonctionnement :

- Dans un environnement d'égal à égal (peer to peer en anglais, noté P2P), dans lequel la communication s'établit d'ordinateur à ordinateur sans ordinateur central et ou chaque ordinateur possède un rôle similaire ;
- Dans un environnement « client/serveur », dans lequel l'ordinateur central fournit des services réseaux aux utilisateurs.

C'est le type de réseau le plus répandu dans les entreprises puisqu'elle permet de relier les ordinateurs et les périphériques à proximité les uns des autres.

1.3.2 Réseau MAN

C'est un type de réseau récemment apparu et peut regrouper un petit nombre de réseaux locaux au niveau d'une ville ou d'une région et l'infrastructure peut être privée ou publique. C'est donc un réseau étendu sur une dizaine de kilomètre.

Un réseau MAN est formé de commutateurs ou de routeurs interconnectés par des liens de haut débit (en général en fibre optique).

1.3.3 Réseau WAN

Ce type de réseau permet l'interconnexion de réseaux locaux métropolitains à l'échelle de la planète, d'un pays, d'une région ou d'une ville. C'est un réseau à une couverture nationale (Transpac) ou internationale (Internet). [1.02]

Les débits disponibles résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Le WAN fonctionne grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau.

1.4 Equipements réseaux

Un réseau informatique est établi à l'aide des équipements réseaux qui sont les supports de transmission et les dispositifs d'interconnexion.

1.4.1 Supports de transmission

Les supports de transmission sont des canaux physiques nécessaires pour relier les différentes unités de communication. Ils sont caractérisés par leurs impédances caractéristiques et leurs bandes passantes. [1.03]

On distingue 2 types de supports de transmission :

- Les supports avec un guide physique
- Les supports sans guide physique

1.4.1.1 Les supports avec un guide physique :

a. Paire torsadée :

C'est un câble composé de deux conducteurs en cuivre identique, isolé l'un de l'autre et enroulé de façon hélicoïdale autour de l'axe de symétrie longitudinal de façon à obtenir 4 paires torsadées dont chacun des extrémités va entrer dans le connecteur RJ45 [1.04]. Cet enroulement autour de l'axe

symétrique réduit les conséquences des inductions électromagnétiques parasites provenant de l'extérieur dans lequel la paire torsadée remplit sa fonction de transmission.

Le câble à paire torsadée est souvent utilisé pour les communications de téléphone et la plupart des réseaux Ethernet modernes.

Il existe deux types de paires torsadées :

- Câble à paires torsadées non blindées Unshielded Twisted Pair ou UTP : C'est le type de paires torsadées le plus utilisé pour les réseaux locaux et un segment de ce câble peut atteindre 100 mètres. Le câble en cuivre UTP couramment utilisé est subdivisé en plusieurs catégories comme Cat5, Cat5e, Cat6, Cat6a et Cat7.
- Câble à paire torsadées blindées Shielded Twisted Pair ou STP: type de câble qui améliore la transmission en utilisant une gaine tressée en cuivre, de meilleure qualité et plus protectrice que celle utilisée en UTP. De plus, une enveloppe en aluminium est disposée autour de chacune des paires qui sont torsadées. Le câble STP permet aussi une transmission plus rapide et sur une plus longue distance.

b. Câble coaxial :

Il est relié à la carte réseau via le connecteur BNC en T. Le câble coaxial est conçu pour transmettre des signaux de haute fréquence. Il est composé de deux conducteurs cylindriques de même axe, l'âme et la tresse, séparés par un isolant. Ce dernier permet de limiter les perturbations dues aux bruits externes [1.05]. Avec la construction de blindage, le câble coaxial peut supporter les longueurs de câble plus longues entre deux dispositifs.

Cette dernière est entourée d'une feuille métallique. L'ensemble du câble est recouvert d'une gaine plastique souple.

c. Fibre optique :

Elle est introduite dans les réseaux informatiques pour pallier plusieurs points faibles des câbles de cuivre.

En effet, elle est constituée d'un fil de verre très fin. D'un point de vue optique, elle comprend un cœur dans lequel la lumière se propage et une gaine externe de protection qui maintient la lumière à l'intérieur du cœur.

La fibre optique permet des vitesses de transmissions extrêmement rapides (jusqu'à 155 Mbps) très utiles pour les transferts d'images, vidéos, et pour le multimédia en général.

Le câble optique est particulièrement adapté à la liaison entre répartiteurs qui est la liaison centrale entre plusieurs bâtiments, et est appelé backbone, ou épine dorsale, car elle permet de connexion sur de longues distances, de quelques kilomètres à 60km dans le cas de fibre monomode, sans nécessité de la mise à la masse. C'est un type de câble très sûr car il est extrêmement difficile de mettre un tel câble sur écoute.

1.4.1.2 Supports sans guide physique :

Ce sont les ondes (hertziennes, radioélectriques et lumineuses) qui réalisent des connexions à distance entre les nœuds par onde radio. La norme la plus utilisée actuellement pour les réseaux sans fil est la norme de l'Institute of Electrical and Electronical Engineers ou IEEE 802.11, plus connue sous le nom de Wireless Fidelity ou Wi-Fi.

Les réseaux filaires restent les plus utilisés en entreprise, leurs choix dépendent de la distance maximum entre les stations, du débit minimum, de la nature des informations, de la fiabilité et du coût. [1.06]

Tableau 1.01 : *Principaux supports physiques de transmission*

Type de support	Facilité d'installation	Débit	Distance max	Temps de propagation	Immunité aux bruits	Coût	Bande passante
Paire torsadée blindée 	Très grande	10 à 100Mbps	200 m	1µs/km	Bonne	Faible	4 MHz
Câble coaxial 	Grande	100 Mbps	500 m	4µs/km	Très bonne	Moyen	50 à 400 MHz
Fibre optique 	Très délicate	Jusqu'à 1Gbps	80 km	1ns/km	Excellente	Elevé	Plusieurs Ghz

1.4.2 Dispositifs d'interconnexion

La possibilité des câbles est limitée. Lorsqu'on veut raccorder plus de deux terminaux, on doit avoir recours à des dispositifs d'interconnexion afin que les informations puissent circuler au sein du réseau [1.07]. Les dispositifs d'interconnexion tiennent une place prépondérante dans un réseau.

1.4.2.1 Répéteur

C'est un équipement simple permettant de régénérer le signal entre deux nœuds du réseau afin d'étendre la distance du câblage d'un réseau. Il travaille uniquement sur la couche physique (la couche 1 du modèle OSI) c'est-à-dire qu'il ne travaille que sur les informations binaires circulant sur la ligne de transmission. Il est utilisé si la distance entre l'ordinateur à connecter est aux alentours de 100 mètres.

1.4.2.2 Concentrateur ou « hub »

C'est un matériel possédant plusieurs interfaces RJ45 permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports. Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé répéteur multiports. Le hub répartit la bande passante entre tous les postes (si un poste envoie un message sur le réseau, tous les postes le reçoivent (quitte à le rejeter s'ils n'en sont pas destinataires) ce qui fait de lui un matériel économique.

1.4.2.3 Commutateur ou « Switch »

Il s'agit d'un autre type de hub ayant une bande passante dédiée pour chaque interface qui est en mode full-duplex afin de limiter les collisions. Il agit au niveau 2 du modèle OSI. Le commutateur analyse les trames sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats.

1.4.2.4 Routeur

C'est un boitier qui a en minimum deux interfaces attribués chacune d'adresse IP. Son rôle, comme son nom l'indique, est de router les paquets d'un réseau à un autre en assurant la liaison inter-réseaux. Il sert à interconnecter les ordinateurs répartis sur différents sites appartenant à une organisation, à un campus, à un établissement ou une entreprise. Le box fourni par le Fournisseur d' Accès Internet ou FAI est un routeur intégré d'un modem Asymetric Digital Subscriber Line ou ADSL, un point d'accès Wi-Fi et a un rôle de passerelle pour relier un réseau privé à Internet.

1.4.2.5 Pare-feu ou « firewall »

C'est un matériel similaire à un routeur mais il est surtout dédié à la sécurisation des réseaux. Il a un rôle de régulateur qui consiste à contrôler les communications à travers les ports. Cela permet d'affiner les trafics et donc d'éviter toute sorte d'intrusion depuis Internet. Actuellement, les firewalls peuvent exister sous forme de logiciels.

1.4.2.6 Carte réseau

La carte réseau se présente sous la forme d'une carte d'extension connectée à un bus (généralement Peripheral Component Interconnect ou PCI). Elle permet le raccordement du Personal Computer ou PC au réseau et prend en charge la gestion des collisions (une collision se produit lorsque deux machines émettent en même temps). Chaque carte réseau comporte une adresse physique unique (adresse MAC).

Une carte réseau doit être installée :

- sur chaque poste du réseau
- sur le serveur
- sur chaque imprimante reliée directement au réseau

1.5 Topologies physiques des réseaux

La topologie physique d'un réseau est sa représentation spatiale définissant comment les nœuds sont interconnectés avec les supports de transmission.

En général, il y a 3 principales topologies :

- La topologie en bus
- La topologie en étoile
- La topologie en anneau

Ces topologies peuvent être combinées pour former une topologie hybride ou maillée [1.08].

1.5.1 Topologie en Bus

C'est la topologie la plus simple d'un réseau. Les équipements sont connectés sur un support commun, une même ligne de transmission par l'intermédiaire d'un câble, généralement coaxial. Les postes sont passifs car ils n'amplifient pas le signal.

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

1.5.1.1 Avantages

- Extension aisée des câbles UTP (par ajout d'un déviateur) ;
- Fonctionnement très simple et fiable ;
- L'ajout de terminaux n'interrompt pas le fonctionnement du réseau (connexion directe) ;

- Facile à mettre en œuvre et à étendre ;
- Une défaillance d'un terminal n'affecte pas le réseau ;
- Moins de longueur de câbles pour connecter les machines donc le support physique est optimisé ;
- Distance maximale de 500m pour les câbles 10 base 5 et 200m pour les câbles 10 base 2.

1.5.1.2 Inconvénients

- Temps d'attente imprévisible due à la méthode d'accès utilisée ;
- Défaillance du réseau en cas de panne du support (80% des pannes du réseau) ;
- Performance réduite en cas de charges importantes (bande passante partagée), ralentissement du réseau quand le trafic devient important ;
- Les machines ne peuvent pas communiquer en même temps car il y a risque de collision ou de conflit ;
- Si un tronçon de câble est défectueux il y a une coupure et donc les machines qui sont au-delà de cette coupure ne fonctionneront pas ;
- Problème difficile à isoler.

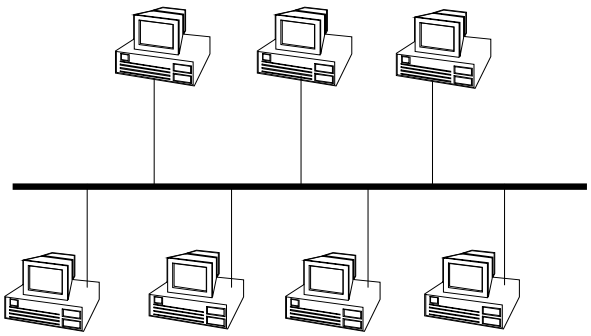


Figure 1.01 : *Topologie en Bus*

1.5.2 Topologie en Etoile

Les ordinateurs du réseau dans cette topologie sont reliés à un système matériel central généralement un concentrateur (Hub). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Cette topologie nécessite souvent une longueur de câblage importante ce qui la rend un peu coûteuse.

Le transfert d'information s'effectue point à point. Le multipoint est possible avec le progrès des autocommutateurs.

1.5.2.1 Avantages

- Robustesse car pas de panne réseau en cas de défaillance des terminaux et des supports.
- Performance en fonction terminal et du nœud central.
- Diagnostic centralisé et facilité de modification.
- Simple dans la réalisation.
- Gestion centralisée.
- Chaque liaison est indépendante des autres.
- Extension facile du réseau par simple addition de câblage ou par addition d'éléments centraux (arborescence de switches).
- La mise en œuvre du réseau est progressive.
- L'évolution du réseau ne nécessite pas de modifications dans le câblage du réseau existant. L'ajout des câbles supplémentaires suffit pour évoluer le réseau.
- Les modifications sont rapides et peu coûteuses.

1.5.2.2 Inconvénients :

- Repose entièrement sur la fiabilité de l'élément central et coût élevé s'il faut câbler beaucoup de nœuds.
- L'ajout d'un poste nécessite un lien jusqu'au serveur d'où une grande longueur de câble.
- Baisse éventuelle de performances s'il faut couvrir une grande distance.
- La panne ou l'inexistence d'un concentrateur entraine une paralysie totale du réseau.
- Beaucoup de câbles.

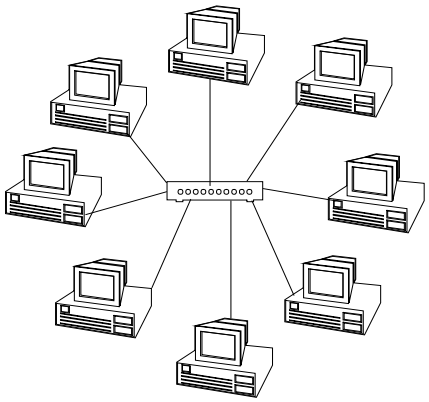


Figure 1.02 : *Topologie en Etoile*

1.5.3 Topologie en Anneau

Norme imposée par le constructeur International Business Machines Corporation ou IBM, c'est la topologie la plus active. Les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour avec une possibilité de distribuer des priorités à des postes.

1.5.3.1 Avantages

- Economise la longueur de câble.
- Support peu coûteux.
- Simple et fiable.
- Facile à étendre.

1.5.3.2 Inconvénients

- La rupture de l'anneau ou détection d'un nœud actif paralyse le réseau.
- Les défaillances de terminaux peuvent causer une panne de réseau (récepteurs inhibés).
- Doublage du support et des organes critiques pour la sécurité (courts circuits).
- Chaque nœud supplémentaire dérive les performances.
- S'il y a une panne ou une coupure du câble c'est tout le réseau qui est en panne.

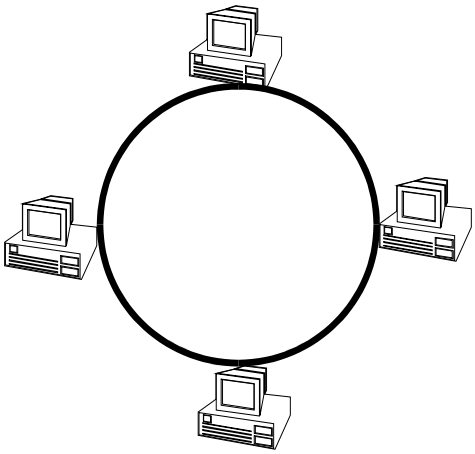


Figure 1.03 : *Topologie en Anneau*

1.6 Architecture ou topologie logique

Le transport des données d'une extrémité à une autre d'un réseau nécessite un support physique ou hertzien de communication. Pour que les données arrivent correctement au destinataire, avec la qualité de service ou QoS (Quality of Service) exigée, il faut en outre une architecture logicielle chargée du contrôle des paquets dans le réseau.

Les deux grandes architectures suivantes se disputent actuellement le marché mondial des réseaux :

- l'architecture Open System Interconnection ou OSI ou interconnexion de systèmes ouverts, provenant de la normalisation de l'International Standardization Organization ou ISO ;
- l'architecture TCP/IP utilisée dans le réseau Internet ;

1.6.1 Architecture OSI

L'Open System Interconnection ou OSI est un modèle créé en 1977 par l'organisme internationale de standardisation communément connu sous ISO afin de permettre la communication entre les systèmes hétérogènes fournis par différents constructeurs. Il s'agit alors d'un système ouvert ayant une architecture en sept couches dont chacune détient un rôle spécifique pour établir les processus émission et réception. [1.09]

Tableau 1.02 : *Couches de l'architecture OSI*

N° des couches	Nom des couches	Définition
Couche 7	**Application**	Point d'accès aux services réseaux. (Ex : messagerie électronique, web, PHP, DNS, audio, etc.)
Couche 6	**Présentation**	Codage des données applicatives, conversion entre données manipulées au niveau applicatif et chaînes d'octets transmises.
Couche 5	**Session**	Synchronisation des échanges et transactions. Permet l'ouverture et fermeture d'une session.
Couche 4	**Transport**	Gère les communications de bout en bout entre processus. (Ex : UDP, TCP, contrôle de congestion, performance de réseau, etc.)
Couche 3	**Réseau**	Gère les communications de proche en proche, entre machines : routage et adressage des paquets. (Ex : algorithme de routage, IPv4, IPv6, etc.)
Couche 2	**Liaison de données**	Gère les communications entre 2 machines adjacentes, directement liées entre elles par un support physique. (Ex : principe de protocole, détection et correction d'erreur, etc.)
Couche 1	**Physique**	Chargée de la transmission des signaux entre interlocuteurs. Emission et réception d'un bit ou d'un train de bit continu. (Ex : fibre, cuivre, satellite, OFDM, etc.)

1.6.2 Architecture TCP/IP

Transmission Control Protocol/Internet Protocol ou TCP/IP est un modèle conçu par le Departement of Defense Americain ou DoD dans les années 1970. DoD réduit les 7 couches de l'OSI à 4 couches.

Parmi ces évolutions, la principale est la généralisation de l'usage du protocole TCP et IP comme standard en matière d'interconnexion de réseau. C'est donc de ce fait que s'est construit un nouveau modèle directement basé sur deux protocoles nommés modèle de référence TCP et IP ; TCP pour fournir un service fiable avec connexion, niveau transport et IP pour assurer une service sans connexion, niveau réseau[1.10]. C'est donc l'origine de l'Internet vue que son but est l'interconnexion des réseaux sur une base planétaire et que le modèle OSI est moins utilisé vue sa complexité.

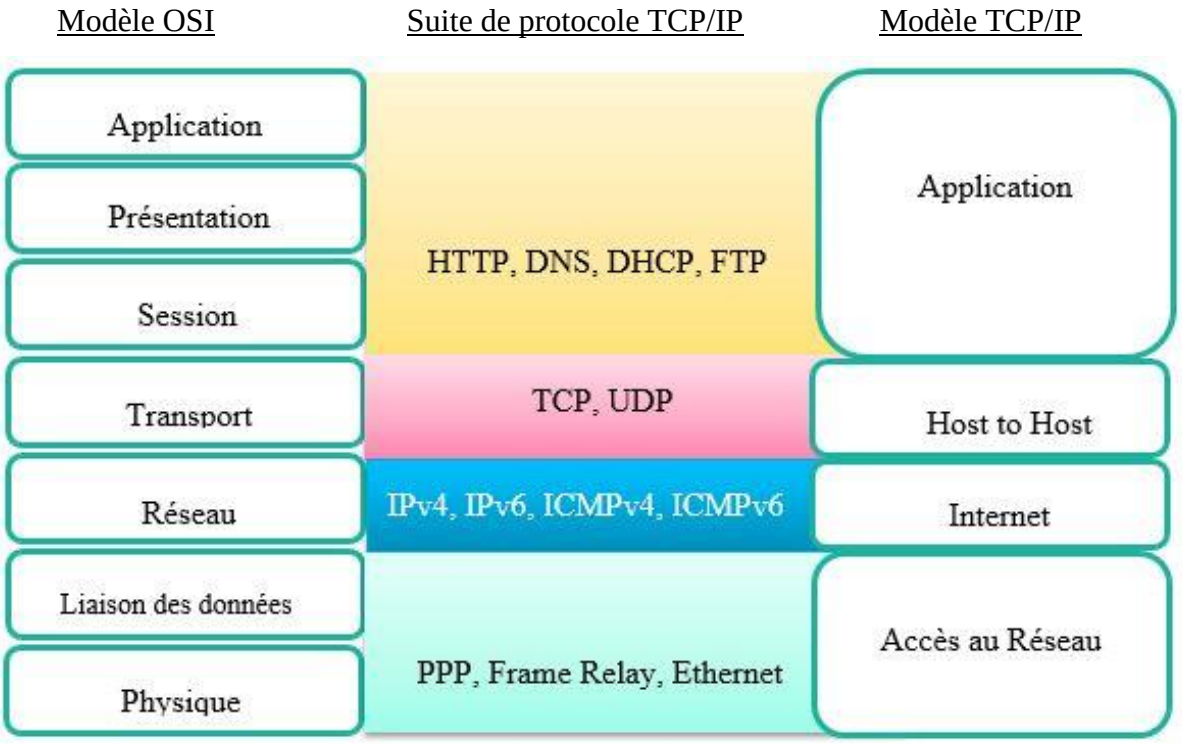


Figure 1.04 : *Correspondance entre modèle OSI et TCP/IP*

1.7 Adressage réseau

Toute pile de protocole identifie un ordinateur expéditeur et un ordinateur destinataire au moyen d'une adresse qui fonctionne de la même manière qu'une adresse postale et permet d'identifier parfaitement un ordinateur précis au sein d'un réseau.

Les adresses IPv4 sont composées de 32 bits soit 4 octets [1.11]. Par convention, ces adresses sont sous forme de 4 nombres décimaux de 0 à 255 séparés par des points.

1.7.1 Classe des réseaux

Il existe cinq classes d'adresse IP. Chaque classe est identifiée par une lettre allant de A à E comme le montre le Tableau 1.03.

Tableau 1.03 : *Classification des réseaux*

Classe	Masque réseau	Adresse réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	Adresses uniques	Adresses uniques
E	Non défini	240.0.0.0 - 255.255.255.255	Adresses uniques	Adresses uniques

L'originalité de ce format d'adressage réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

- La partie réseau (Net-Id) est commune à l'ensemble des hôtes d'un même réseau,
- La partie hôte (Host-Id) est unique à l'intérieur d'un même réseau.

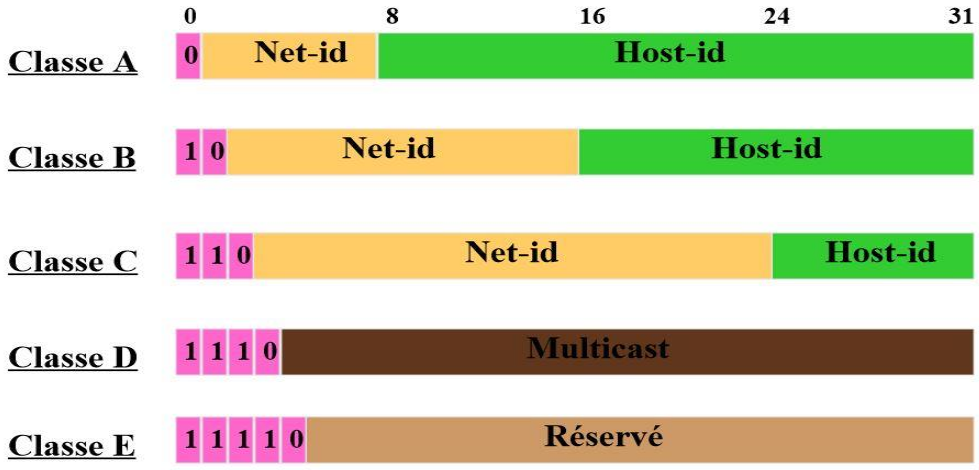


Figure 1.05 : *Subdivision de la partie Host-Id et Net-Id pour chaque classe d'adresse*

1.7.2 Adresse routable – Adresse non routable

Un protocole routable peut transmettre ses paquets de données à un routeur. Ce dernier doit évidemment gérer ce protocole. Les protocoles routables couramment employés sont Internet Protocol ou IP et Internet Packet Exchange ou IPX.

En revanche, NetBEUI, contemporain d'anciens produits Microsoft comme MS-DOS et Windows pour Workgroup, est un exemple de protocole non routable. C'est encore le protocole par défaut des réseaux Microsoft sous Windows 95 et 98. Comme Internet utilise l'adressage IP, en réseau local on ne peut utiliser que quelques plages d'adresses réservées (on parle d'adresses non routables car elles ne seront jamais vues sur Internet), ces plages d'adresses sont : Classe A avec NetID 10.0.0.0,

Classe B entre 172.16.0.0 à 172.31.0.0, Classe C entre 192.168.0.0 à 192.168.255.0. Ce sont des adresses réservées pour usage privé. [1.12]

1.7.3 Adresse IP fixe - Adresse IP dynamique

Chaque poste d'un réseau peut se voir attribuer une adresse IP permanente : c'est l'adresse IP fixe (configuré manuellement).

Chaque poste peut être configuré pour obtenir une adresse dynamique : un serveur DHCP (Dynamics Host Control Protocol) délivre alors une adresse IP à chaque demande de connexion au réseau. Cette adresse change à chaque connexion.

Un serveur est normalement configuré en adresse IP fixe.

1.8 Cadre d'étude

Un cadre d'étude pour la mise en place de ce projet est nécessaire afin de bien définir quel genre de supervision sera mise en place dans ce livre et d'avoir un exemple concret de la supervision.

Appliquer la supervision au sein d'une entreprise de renom serait bien un atout pour le projet. C'est pourquoi, le stage d'une durée de 3 mois passé au sein de la Direction Informatique de l'INSTAT a permis d'avoir un cadre d'étude idéal pour la supervision ainsi qu'une expérience professionnelle dans le monde du travail et des connaissances en réseau informatique.

1.8.1 Présentation de l'INSTAT

L'INSTAT ou l'Institut National de la Statistique a été créé le 25 Novembre 1947 et a pour but de mettre sur pied une institution dont la mission serait de produire les principales statistiques officielles de la nation.

- Dénomination : INSTAT
- Siège : ANOSY-ANTANANARIVO
- Boite postale : 485
- Tel : 22 216 52
- Site : www.instat.mg

1.8.2 Organigramme de l'INSTAT

L'INSTAT possède 7 directions qui sont la Direction Administrative et Financière, la Direction Informatique, la Direction des Relations Institutionnelles et de la Diffusion, la Direction des Synthèses Economiques, la Direction des Statistiques Economiques et la Direction de la Démographie et des Statistiques Sociales. La Figure 1.06 montre son organigramme.

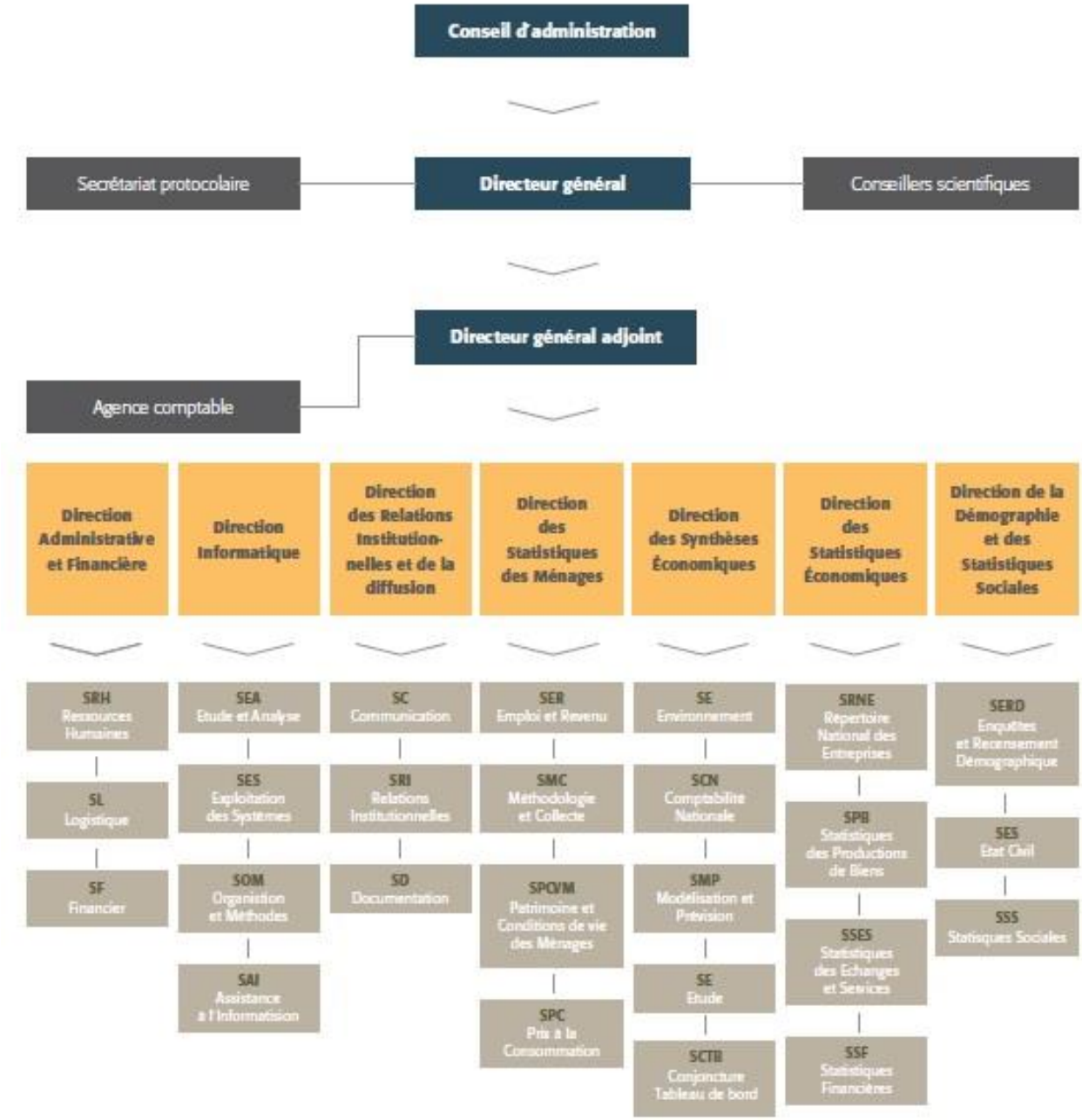


Figure 1.06 : *Organigramme de l'INSTAT*

1.8.3 Département d'accueil : la Direction Informatique

Comme le stage s'est effectué au sein de la Direction Informatique de l'INSTAT, l'analyse qui suit sera donc basé sur le réseau et les matériels informatiques en général.

En effet, cette direction a pour mission d'assurer le traitement informatique des données et de concevoir la politique à suivre en matière d'équipements matériels et logiciels informatiques au niveau de l'entreprise.

A ce titre, elle est notamment chargée de :

- Concevoir, mettre en place et gérer les systèmes informatiques de l'INSTAT en coordination avec le développement de l'Informatique à Madagascar et en particulier dans l'administration publique ;
- Développer et assurer l'évolution des applications informatiques et des bases de données statistiques ;
- Apporter son appui technique aux administrations en matière de système informatique ;
- Assurer l'harmonisation des supports de collecte des bases de données.

L'organigramme de la direction informatique est présenté par la Figure 1.07.

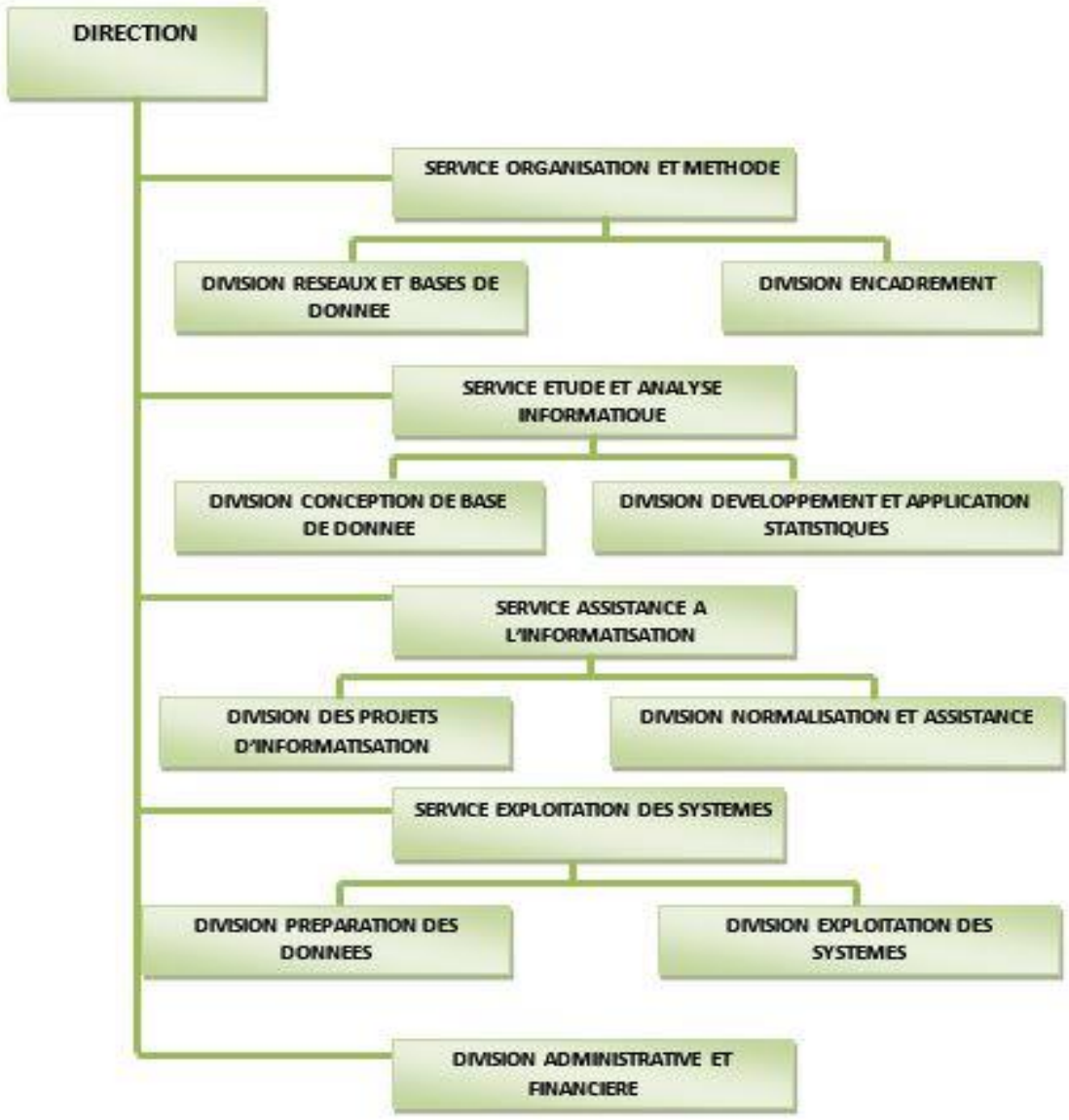


Figure 1.07 : *Organigramme de la Direction Informatique*

1.8.4 Présentation de l'environnement informatique

1.8.4.1 Architecture et type de réseau

L'immeuble de l'INSTAT comporte 3 étages et chaque porte de ces étages possède au minimum deux ordinateurs. La source de la connexion Internet de l'entreprise provient du capteur haut débit allant de 20Mbits à 70Mbits qui se trouve sur le toit du bâtiment. Ce capteur est une antenne Wimax fixe qui opère dans les bandes de fréquence de 2,5 et 3Ghz et fait une capture du réseau wifi au niveau du ministère des finances et du budget. Un routeur est ensuite relié par un switch qui ce dernier est relié à d'autres switch reliés à des ordinateurs et à un serveur d'imprimante. Les liaisons se font par des câbles droits.

L'entreprise utilise 2 types de réseau : la première le réseau LAN (Local Area Network) et la deuxième le réseau WAN (Wide Area Network).

Le réseau LAN est utilisé pour les taches internes de l'entreprise telle que le partage de données entre employés. Certains ordinateurs ne sont pas encore mis en réseau.

Le réseau WAN est utilisé pour héberger le site web de l'entreprise et aussi pour le serveur mail.

Pour la connexion Internet, certains ordinateurs utilisent la câble paire torsadée et d'autre utilisent le Wi-Fi sécurisé par Wi-Fi Protected Access ou WPA2.

En général, la structure du réseau de l'entreprise est dans la catégorie de topologie en Etoile.

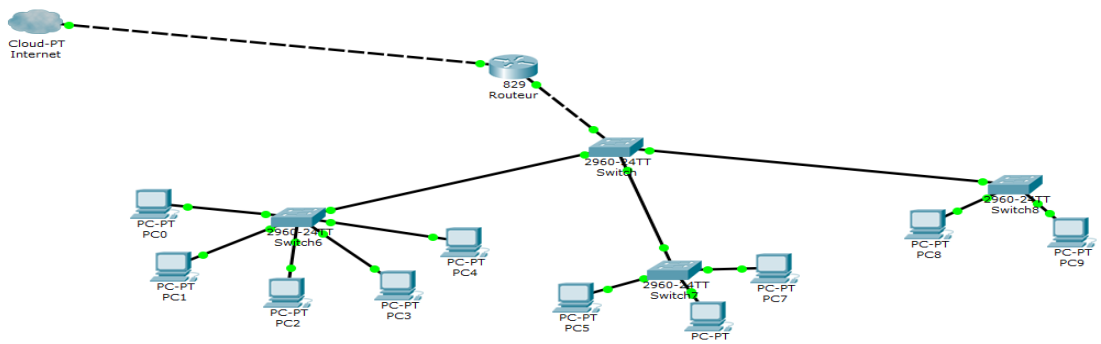


Figure 1.08 : *Architecture simplifiée du réseau de l'INSTAT*

1.8.4.2 Matériels existants

L'INSTAT possède plusieurs ordinateurs clients (250 ordinateurs) destinés pour chaque utilisateur au niveau de l'établissement. Les systèmes d'exploitation dans ces ordinateurs sont Windows XP, Windows 7, Windows Server 2008 et Windows10.

Tableau 1.04 : *Description de quelques ordinateurs au sein de l'Instat*

Marque	Processeur	Capacité RAM	Disque Dur	Système d'exploitation
NEC	700Mhz-2,8GHz	128 Mo-1Go	20-180Go	Windows XP SP2
COMPAQ	700Mhz-2,8GHz	128 Mo-1Go	20-180Go	Windows XP SP2
SIEMENS	700Mhz-2,8GHz	128 Mo-1Go	20-180Go	Windows XP SP2

Les switch multiport (24 ports et 48 ports) de marque D-link DES-1016D jouent le rôle d'interconnexion entre les machines. Elles sont au nombre de 9. L'entreprise dispose aussi d'un routeur et d'un serveur d'impression sous UNIX qui sert à gérer les imprimantes dans la salle de serveur pour traiter les fiches de paie des employés.

1.8.5 Critiques de l'existant

Lors de notre étude, les problèmes suivants peuvent être rencontrés au sein de l'INSTAT:

- Arrêt immédiat de certains ordinateurs causé par le réchauffement du processeur.
- Ayant un très grand nombre d'ordinateurs à gérer l'administrateur est incapable de vérifier ni détecter les défaillances des équipements (Central Processor Unit ou CPU, HDD, Etat de mémoire) ni les surcharges.
- Les employées doivent appeler l'administrateur à chaque fois que leur matériel informatique ne fonctionne pas.
- Arrêt du travail des employés à cause de la panne.
- Longue attente du rétablissement des équipements en panne.
- Aucun outil de supervision système et réseau n'est mis en place au sein de l'entreprise.
- Un taux important de temps est gaspillé lors du diagnostic des pannes ce qui influe sur la qualité du service et donc le bon fonctionnement de l'entreprise.
- Plus le nombre des équipements et des services augmente plus les tâches de l'administrateur deviennent trop compliquées et il n'arrive pas à les assurer convenablement.
- Vue l'absence d'un outil de supervision, l'administrateur n'est pas alerté en cas de problèmes de fonctionnements anormaux.

1.8.6 Solutions envisagées

Suite aux problèmes cités dans le paragraphe précédent, la mise en place d'un outil de supervision système et réseau qui assurent les fonctionnalités suivantes est proposée:

- Diagnostiquer l'état du réseau.
- Vérifier la disponibilité des serveurs en surveillant les ressources et les performances systèmes (CPU, Disques durs et partitions, RAM,…).
- Déclencher des alertes lors de la détection des pannes.
- Générer des graphes, des cartographies et des rapports.
- Avoir une interface graphique compréhensible pour l'interaction entre l'utilisateur et le logiciel.
- N'avoir aucun impact sur les performances et ne désencombre pas le réseau lors de la remontée des informations.

1.9 Conclusion

En bref, un réseau informatique est la mise en communication entre machines informatiques dans le but de partager des informations (ressources). Il est un large domaine qui concerne plusieurs entités physiques et logiques ayant chacune un rôle bien défini. C'est l'interconnexion de ces entités qui permet la communication, l'accès à internet et aux ressources partagées ainsi que la mise à disposition d'une plateforme de travail collaboratif. Physiquement, le réseau informatique peut être de type LAN, MAN, WAN, cela dépend de l'emplacement des ordinateurs interconnectés entre eux. Il peut aussi se présenter sous différents topologies dans les bâtiments comme la topologie en bus, en étoile, en anneau et hybride. D'une vue logique, le modèle OSI et TCP/IP, des modèles de normalisation des communications permettent plusieurs ordinateurs dans un réseau de dialoguer entre eux cela par la superposition de plusieurs couches dans ces protocoles ayant des fonctionnalités bien définis. Ces modèles ont pour but de garantir un maximum d'évolutivité et d'interopérabilité entre les ordinateurs. Le domaine du réseau est donc un domaine très vaste d'où il est impératif de surveiller de près tous les équipements pour éviter l'arrêt des activités. Avant de mettre en place une plateforme de supervision, il est indispensable d'avoir un cadre d'étude pour le projet et de bien étudier et comprendre l'infrastructure réseau sur laquelle travailler, le réseau de l'INSTAT. Un cahier de charge, une critique de l'existent ont été fait pour identifier les besoins de l'entreprise. En effet, il faut bien s'axer davantage sur les problèmes fréquents confrontés par les utilisateurs vue que le but du projet est de les repérer facilement et de pouvoir intervenir dans les plus brefs délais.

CHAPITRE 2
SUPERVISION INFORMATIQUE

2.1 Introduction

Etant donné la vastitude du monde du travail qui affecte aussi l'infrastructure du réseau informatique, un outil de supervision devient nécessaire pour accompagner les administrateurs et techniciens réseaux afin de leur simplifier la tâche. Une plate-forme de supervision est un outil indispensable pour une entreprise dotée d'un grand parc informatique du fait que l'arrêt d'un service ou matériel peut avoir des conséquences financières assez importantes. Mais d'abord, c'est quoi la supervision ?

2.2 Définition

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 (email ou SMS par exemple) les administrateurs.

Cette définition de la supervision est décrite plus en détail dans la norme ISO7498/4. Plusieurs actions sont ainsi réalisées: Acquisition de données, analyse, puis visualisation et réaction. [2.01]

2.3 Concept de supervision

Le concept de supervision réseau est né au début des années 1980, lors de la croissance importante de mises en place de réseaux informatiques dans les entreprises. La taille grandissante de ceux-ci ainsi que leur hétérogénéité posaient un réel problème de gestion et d'administration, multipliant les besoins en main d'œuvre d'experts administrateurs. C'est donc à cette époque qu'ont été menées les premières réflexions sur un nouveau concept, celui de la supervision.

2.4 Intérêt et rôle

La supervision doit permettre de gérer les anomalies (détection et résolution des problèmes), les configurations (inventaire, configuration matérielle et logicielle), les performances (évaluer les comportements et optimiser le fonctionnement), la sécurité (filtrage des accès, redondance des équipements, sauvegarde) et la comptabilité (déterminer l'utilisation et le coût de ressources réseau). La supervision doit correspondre à un système réactif et proactif.

2.5 Mode de fonctionnement

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).

2.5.1 Supervision réseau

Le terme réseau signifie ici l'aspect communication entre les machines. Le rôle est de s'assurer du bon fonctionnement des communications et de la performance des liens (débit, latence, taux d'erreurs). C'est dans ce cadre qu'une adresse IP est vérifiée si elle est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau.

2.5.2 Supervision système

La surveillance se cantonne dans ce cas à la machine elle-même et en particulier ses ressources. Comme par exemple contrôler la mémoire utilisée ou la charge processeur sur le serveur, une analyse des fichiers de logs système est nécessaire.

2.5.3 Supervision applicative

Cette technique est plus subtile, c'est elle qui va nous permettre de vérifier le fonctionnement d'une application lancée sur une machine.

Cela peut être par exemple une tentative de connexion sur le port de l'application pour voir si elle retourne ou demande bien les bonnes informations, mais aussi de l'analyse de logs applicatifs. [1.04]

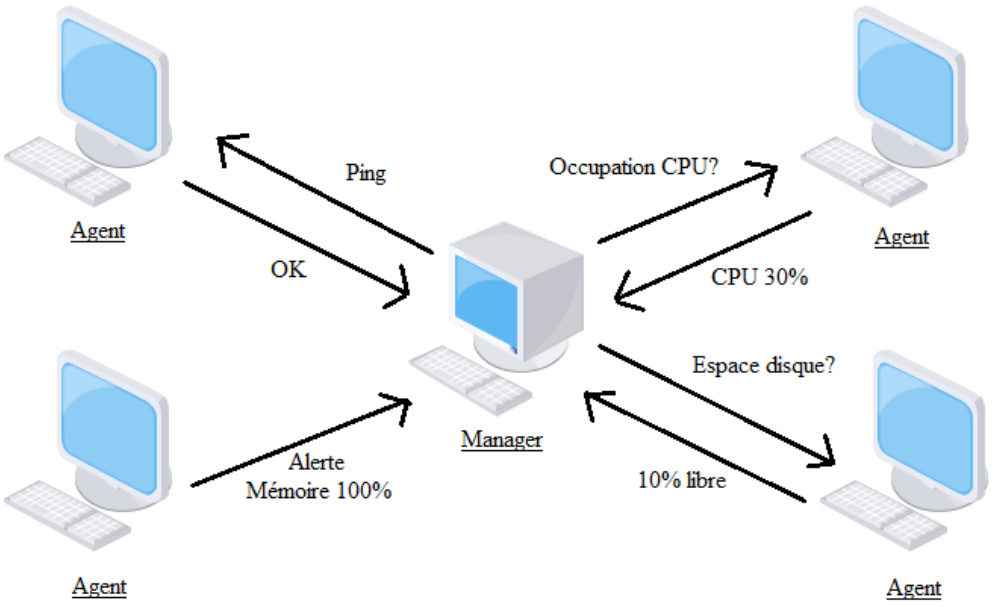


Figure 2.01 : *Mode de fonctionnement de la supervision*

2.6 Déploiements des logiciels de supervision

2.6.1 Déploiement centralisé

La supervision n'est assurée que par un seul ordinateur, avec éventuellement une ou plusieurs machines miroirs synchronisées. La visualisation des éléments du réseau (alarmes, état des nœuds, etc..) est alors centralisée en un point unique. Ce type de supervision reste tout de même sensible, car toute la gestion repose sur une seule station. Si celle-ci vient de tomber en panne, tout le processus de supervision est alors compromis. De plus, la machine étant seule, elle doit être suffisamment robuste pour pouvoir traiter l'ensemble des données de supervision du réseau. Enfin, la machine effectue la totalité des requêtes de supervision, ce qui a pour conséquence d'augmenter fortement le trafic du réseau en provenance de cette machine.

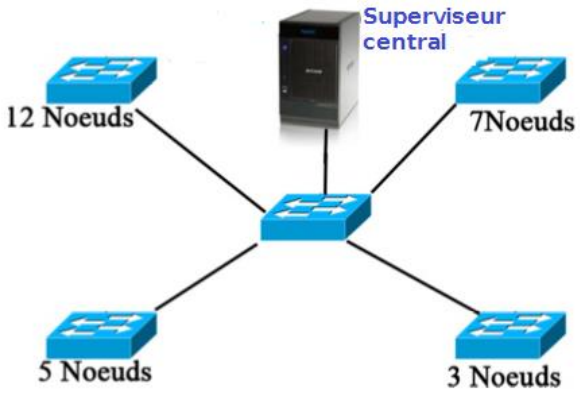


Figure 2.02 : *Déploiement centralisé*

2.6.2 Déploiement hiérarchique

La supervision est assurée ici de manière hiérarchique. Un serveur de supervision central dialogue avec d'autres serveurs de supervision ne s'occupant chacun que d'un segment de réseau. Ces mêmes serveurs peuvent aussi avoir d'autres serveurs sous leurs responsabilités. Ils sont à la fois clients et serveurs de supervision. Ce type de déploiement est bien plus délicat à mettre en œuvre qu'un simple déploiement centralisé mais offre une tolérance aux pannes bien plus élevée. En effet, si un serveur supervisant un segment tombe en panne, seul le segment concerné ne sera plus supervisé. De plus un tel déploiement permet d'avoir plusieurs visions du réseau : une vision globale, depuis le serveur central, une vision d'un segment depuis un serveur supervisant un segment, etc... Toutefois, il ne faut pas occulter le fait qu'un déploiement hiérarchique reste plus coûteux en temps de réponse qu'un déploiement centralisé, les différents serveurs devant se synchroniser pour faire remonter les informations au niveau hiérarchique le plus haut.

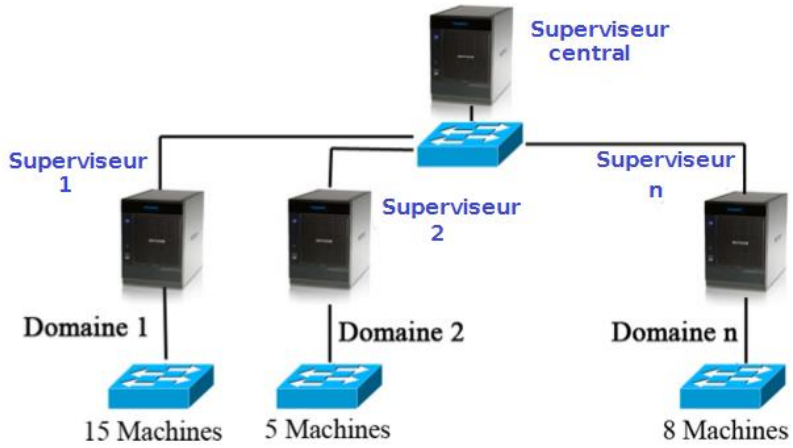


Figure 2.03 : *Déploiement hiérarchique*

2.6.3 Déploiement distribué

Ce déploiement combine l'approche centralisée et l'approche hiérarchique. Chaque station de supervision tient à jour une base de données complète. Toute les stations échangent donc entre elles les données de supervision sans restriction.

Cela permet de spécialiser certaines machines sur un traitement de supervision précis (alarme, sécurité, performances, etc..). Toutefois, il convient de bien définir le degré de responsabilité et de coopération entre les machines.

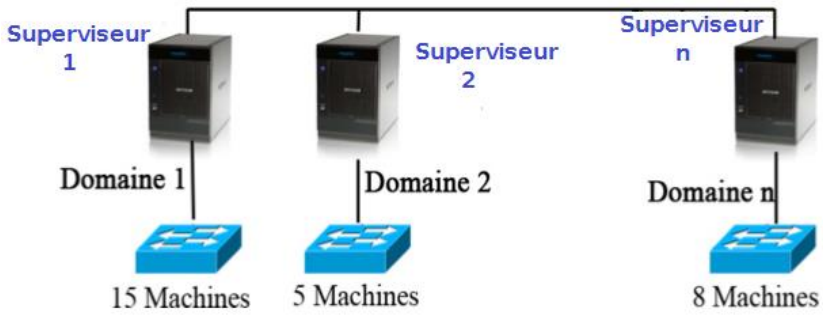


Figure 2.04 : *Déploiement distribué*

2.7 Norme ISO 7498/4

Le concept de supervision a été normalisé par International Organisation for Standardisation ou ISO. Les différentes fonctions qui ont été défini par l'ISO sont : la gestion des performances, la gestion des configurations, la gestion de la comptabilité, la gestion des anomalies et la gestion de la sécurité.

2.7.1 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. [2.02]

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

2.7.2 Gestion des configurations (Management Configuration)

La gestion de configuration permet d'identifier, de paramétrer et de contrôler les différents objets du réseau. Les procédures requises pour gérer une configuration sont : [2.02]

- la collecte d'information
- le contrôle d'état
- la sauvegarde historique de configurations de l'état du système.

2.7.3 Gestion de la comptabilité (Accounting Management)

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. [2.02]

2.7.4 Gestion des anomalies (Fault Management)

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. Quand cela est possible, elle règle elle-même automatiquement l'anomalie.

2.7.5 Gestion de la sécurité (Security Management)

La gestion de la sécurité contrôle l'accès aux ressources en fonction des politiques de droits d'utilisations 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. [2.02]

2.8 Protocole SNMP

Le protocole mis en jeu dans la supervision est le protocole Simple Network Management Protocol ou SNMP, c'est pourquoi dans ce paragraphe, SNMP et ses dérivés seront l'intérêt de cette étude.

2.8.1 Présentation

SNMP est le protocole de gestion de réseaux proposé par l'Internet Engineering Task Force ou IETF. Il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux. SNMP est un protocole relativement simple. Pourtant l'ensemble de ses fonctionnalités est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications : les bases de données, les serveurs, les logiciels, etc. [2.03]

Les buts du protocole SNMP sont de :

- connaître l'état global d'un équipement (actif, inactif, partiellement opérationnel...) ;
- gérer les évènements 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.

2.8.2 Différentes versions du SNMP

Depuis la création de SNMP, ce protocole a connu des améliorations très importantes.

Cependant les précédentes versions (la V1 et la V2C) sont encore les versions les plus utilisées actuellement.

Un support de SNMP V3 a récemment été lancé car il est plus sécurisé si on le compare à ses prédécesseurs.

- SNMP V1 : C'est la première version du protocole. La sécurité de cette version est minimale car elle basée uniquement sur la chaîne de caractère appelée "communauté". Cette version du protocole est définie dans les RFC 1155 et 1157. [2.04]
- SNMP V2C : C'est un protocole révisé, qui comprend les améliorations de SNMP V1 dans différents domaines tels que les types de paquets, les éléments de structure Management Information Base ou MIB et les requêtes protocolaires MIB. Cependant ce protocole utilise la structure d'administration de SNMP V1 (à savoir "communauté") d'où le terme SNMP V2C.

- SNMP V3 : Aussi connu sous le nom de version sécurisée de SNMP. SNMP V3 facilite la configuration à distance des entités SNMP. [2.04]

Ces trois versions sont les principales, même si des versions intermédiaires ont vu le jour (SNMPSec, SNMP V2, SNMP V2U, SNMP V2P), celles-ci ne présentent que des mises à jour mineures plutôt que de véritables améliorations.

Actuellement les versions les plus utilisées (par ordre d'utilisation) sont : SNMP V1, SNMP V3 puis SNMP V2C.

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 ou un hub.

2.8.3 Architecture SNMP

Les différents éléments que l'on peut identifier avec le protocole SNMP sont synthétisés par le schéma ci-dessous.

- Le manager 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.
- Les agents SNMP : ce sont les équipements (réseau ou serveur) qu'il faut superviser.

2.8.3.1 Manager SNMP

C’est un daemon à installer sur la station d’administration et qui lance des requêtes vers l’agent SNMP pour recueillir les informations de contrôle. Ces dernières sont fournies ensuite au Network Management Station ou NMS qui est une application de supervision permettant de les traiter et de les interpréter.

Il est à préciser ici qu’un daemon est un programme qui exécute une tache en arrière-plan.

2.8.3.2 MIB

Chaque agent SNMP maintient une base de données décrivant les paramètres de l'appareil géré. Le Manager SNMP utilise cette base de données pour demander à l'agent des renseignements spécifiques. Cette base de données commune partagée entre l'agent et le Manager est appelée Management Information Base ou MIB.

Généralement ces MIB contiennent l'ensemble des valeurs statistiques et de contrôle définis pour les éléments actifs du réseau. SNMP permet également l'extension de ces valeurs standards avec des valeurs spécifiques à chaque agent, grâce à l'utilisation de MIB privées.

Un fichier MIB est écrit en utilisant une syntaxe particulière, cette syntaxe s'appelle Structure of Management Information ou SMI3, basée sur Abstract Syntax Notation number one ou ASN.1 tout comme SNMP lui-même.

La structure d'une MIB est une arborescence hiérarchique dont chaque nœud est défini par un nombre ou un Object IDentifier ou OID. Chaque identifiant est unique et représente les caractéristiques spécifiques du périphérique géré. Lorsqu'un OID est interrogé, la valeur de retour n'est pas un type unique, elle peut être de type texte, entier, compteur, tableau. Un OID est donc une séquence de chiffres séparés par des points. Par exemple, l'OID ifDescr (1.3.6.1.2.1.2.2.1.2) est une chaîne de caractères contenant des informations concernant une interface réseau). [2.05]

En résumé, les fichiers MIB sont l'ensemble des requêtes que le Manager peut effectuer vers l'agent. L'agent collecte ces données localement et les stocke, tel que défini dans la MIB. Ainsi le Manager doit être conscient de la structure (que celle -ci soit de type standard ou privée) de la MIB afin d'interroger l'agent au bon endroit.

2.8.3.3 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 lancé par le manager [2.06].

Il est donc un daemon qui s'exécute sur une machine à superviser.

Les principales fonctions d'un agent SNMP sont:

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

Les agents se trouvent au niveau de chaque interface qui connecte l'équipement managé au réseau. Ces équipements peuvent être des switch, des hubs, des routeurs et des serveurs.

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. Par exemple, il pourra émettre une alerte si le débit d'une interface réseau, atteint une valeur considérée par l'administrateur comme étant critique. Plusieurs niveaux d'alertes peuvent ainsi être définis, selon la complexité de l'agent (température du processeur, occupation disque dur, utilisation CPU...).

2.8.4 Requêtes SNMP

Le mécanisme de base du protocole SNMP est constitué d'échanges de type requête/réponse appelé Protocol Data Unit ou PDU. En fonction de la version du protocole SNMP utilisé, différentes commandes sont possibles. La structure des paquets utilisés par le protocole SNMP V1, est définie dans la RFC 1157. Les requêtes SNMP vont contenir une liste d'OID à collecter sur l'agent SNMP.

Les types de requêtes du manager SNMP vers l'agent SNMP sont :

- Get Request : Le manager interroge un agent sur les valeurs d'un ou de plusieurs objets d'une MIB.
- Get Next Request : Le manager interroge un agent pour obtenir la valeur de l'objet suivant dans l'arbre des objets de l'agent. Cette interrogation permet de balayer des objets indexés de type tableau.
- Get Bulk Request : Introduite avec la version 2 du protocole SNMP, cette requête permet de mixer la commande GET et GETNEXT pour obtenir des blocs entiers de réponses de la part de l'agent.
- Set Request : Le manager positionne ou modifie la valeur d'un objet dans l'agent.

Les réponses ou informations de l'agent vers le manager sont :

- Get Response : L'agent répond aux interrogations du manager.
- Trap : L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du manager.
- Notification : Introduite avec la version 2 du protocole SNMP. L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du manager.

- Inform : Introduite avec la version 2 du protocole SNMP. L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent attend un acquittement de la part du manager et il y aura une retransmission en cas de non réponse.

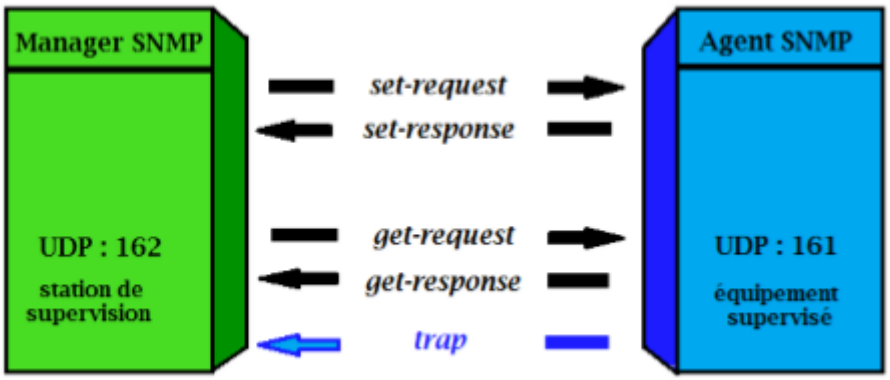


Figure 2.05 : *Illustration des échanges entre agent et manager SNMP*

SNMP utilise généralement User Datagram Protocol ou UDP comme protocole de transport pour délivrer les requêtes et leurs réponses. Les ports utilisés sont le 161 pour l'agent et le 162 pour le manager. [2.07]

2.8.5 Format des messages SNMP

Le message SNMP dans son ensemble est une séquence de 3 champs :

Version (integer)	Communauté (Octet String)	Protocol Data Unit ou PDU (type construit)

- La version du protocole identifié par un entier. Cet entier est 0 pour SNMPv1.
- La communauté : un environnement d'accès contenant une chaîne de caractère pour un groupe de manager. Un agent ne connaissant pas le nom de la communauté est exclu.
- Le PDU est un type construit (dans le jargon ASN.1), et est donc constitué de plusieurs champs. Son contenu varie selon qu'il s'agisse d'une commande réponse ou d'une trap [2.08]. Il est utilisé pour la communication entre les entités SNMP.

2.9 Outils de supervision

De nombreuses plateformes de supervision existent aujourd'hui. Certaines se contentent de connaître à tout instant l'état des nœuds du réseau, d'autres permettent également de connaître l'état

des services sur ces nœuds, les derniers offrent la possibilité de ressortir de nombreuses statistiques du réseau permettant une analyse assez fine.

En effet, un outil ou plateforme de supervision doit avoir les options dans la Figure 2.06.

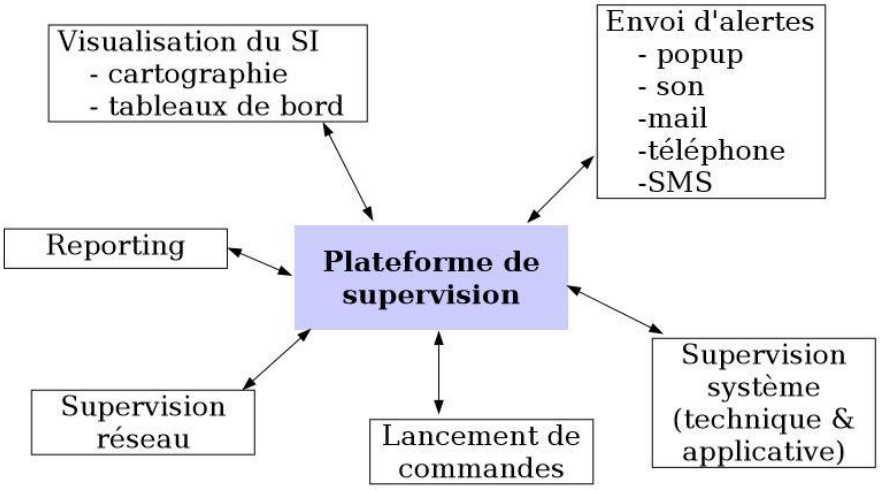


Figure 2.06 : *Fonctionnalités d'un outil de supervision*

Deux alternatives sont possibles pour pouvoir superviser, soit utiliser :

- Des logiciels payants
- Des logiciels gratuits

2.9.1 Logiciels payants ou offres éditeurs

Aussi appelés offres éditeurs ou propriétaires, les logiciels payants sont des logiciels dont on achète une ou plusieurs licences pour pouvoir les utiliser.

2.9.1.1 Scom (Microsoft System Center Operation Manager)

Développé par le géant Microsoft, Scom est un programme de supervision réseau qui permet le monitoring des différents équipements grâce à une interface logicielle. Ses principales caractéristiques sont :

- Automatisation du déploiement des stratégies de surveillance pour les systèmes et applications installés ;
- Collecte des événements applicatifs, systèmes et compteurs de performances ;
- Surveillance avec corrélation de ces éléments et des alertes proactives ;
- Collecte d'audit des journaux d'événements sécurité ;
- Fonctions de création de rapports et d'analyse ;
- Générer des rapports sur les niveaux de performances ;

- Des tâches et des connaissances personnalisables associées à certaines alertes ou applications ;
- Intégration complète de PowerShell, nouveau langage de script des systèmes Windows ;
- Avoir des informations précises sur l'état des serveurs et générer en temps réel des alertes ;
- Concentrer la surveillance des systèmes d'information en un produit unique de supervision ;
- Obtenir la visibilité nécessaire pour assurer la protection des renseignements et surveiller son environnement ;
- Améliorer l'efficacité des opérations informatiques via des pratiques éprouvées intégrées dans les packs d'administration ;
- Générer des rapports sur les niveaux de services afin d'aider à analyser l'état de fonctionnement du système d'information ;
- Permettre de générer des tableaux de bord et rapports sur l'historique du fonctionnement des serveurs et objets managés.

2.9.1.2 HP OpenView

OpenView est le nom générique sous lequel sont regroupés un ensemble d'applications destinées à la supervision d'un réseau informatique. Elles sont organisées autour d'un produit central : Hewlett-Packard OpenView ou HP/OV Network Node Manager ou NNM qui fournit une série d'outils pour vérifier la configuration d'un réseau, prendre en compte des évènements, isoler les alarmes et analyser les performances des réseaux TCP/IP. HP/OV s'appuie sur le protocole SNMP et permet de :

- découvrir automatiquement les nœuds (stations) et les éléments du réseau ;
- fournir une description détaillée de l'état de chaque agent SNMP du réseau à l'aide des MIBs ;
- Une interface graphique permet un affichage de l'état courant des équipements en fonctions de différentes couleurs (système de MAP). Un système d'alarme permet de synchroniser le tout avec des déclenchements d'alarmes si un hôte change d'état ou devient injoignable, et des actions peuvent alors être effectuées.

Ses principaux atouts sont les suivants :

- Une vue globale du système d'information ;

- Une vision des différents incidents ;
- Un contrôle homogène des différents matériels.

HP/OV Network Node Manager est utilisé pour surveiller principalement les équipements réseau (commutateurs, …), les serveurs et les machines UNIX.

2.9.1.3 IBM Tivoli

Les solutions IBM Tivoli Monitoring sont conçues pour une meilleure gestion des applications en ligne essentielles à l'entreprise en :

- surveillant de manière proactive les ressources système vitales ;
- en détectant efficacement les goulets d'étranglement et les problèmes potentiels ;
- en répondant automatiquement aux événements.

En s'appuyant sur les meilleures pratiques pour identifier et résoudre les problèmes d'infrastructure, il a été conçu pour aider les opérateurs à surveiller et gérer les matériels et logiciels essentiels, comprenant les systèmes d'exploitation, les bases de données et les applications sur des environnements répartis.

Ce moniteur de supervision se classe parmi les leaders du domaine, puisqu'il offre de nombreux avantages. En effet, il :

- Surveille les composants vitaux de l'infrastructure à la demande, en aidant à isoler et prévenir rapidement les problèmes de performance ;
- Visualise les mesures de performances historiques et en temps réel sous forme de tableaux et graphiques, avec en plus des conseils spécialisés et des actions automatiques au sein d'IBM Tivoli Enterprise Portal ;
- Consolide la surveillance et la gestion de systèmes répartis et de systèmes hôte à l'aide d'une seule console de travail personnalisable ;
- Fournit des outils de surveillance puissants et personnalisables à davantage d'opérateurs nécessitant beaucoup moins de compétences et formation en programmation pour déployer le produit ;
- Aide à réduire les coûts opérationnels informatiques globaux en simplifiant l'installation et la configuration, et en déployant des règles allégées avec des fonctionnalités de surveillance automatique ;
- Permet une personnalisation de la console de travail ;
- Fournit une installation et une surveillance simple ;

- Effectue automatiquement le suivi de l'état des principaux composants de votre environnement informatique complexe et reçoit des alertes uniquement en cas d'incident;
- Aide à optimiser l'offre de services informatiques en intégrant des produits de gestion et des processus informatiques pour stimuler les performances et respecter les accords de niveau de service ;
- Aide à optimiser le temps de réalisation en simplifiant l'installation et la surveillance, avec également des fonctionnalités de gestion s'appuyant sur des technologies pointer-cliquer.

2.9.2 Logiciels gratuits et Open Source

Il faut savoir qu'il existe des dizaines de solutions Open Source dédiées à la supervision, le principal critère de choix réside dans les différents cas d'utilisation. Nous allons donc présenter les principaux outils de supervision réseau open source tout en dégageant leurs avantages et inconvénients :

2.9.2.1 Zabbix

a. Présentation de l'outil :

Zabbix est un outil de supervision permettant de superviser réseau, systèmes (processeur, disque, mémoire, processus,…). Zabbix offre des vues graphiques (générés par RRDtools) 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. [2.09]

b. Avantages

Zabbix est :

- Une solution très complète : cartographie de réseaux, gestion poussée d'alarmes via SMS, Jabber ou Email, gestion des utilisateurs, gestion de pannes, statistiques et reporting ;

- Une entreprise qui pousse le développement et est une communauté croissante ;
- Un logiciel possédant 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.

c. 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.

Zabbix est une application libre (open source) de supervision des systèmes et des réseaux. Par sa polyvalence, Zabbix peut superviser et vérifier les statuts d'une multitude de services réseaux, ou systèmes, ce qui fait de lui un outil complet proposant des fonctionnalités relatives à la supervision (alertes, mesures, actions sur conditions...).

Le principal reproche vient de l'aspect graphique où dans certains cas la lisibilité laisse à désirer. Certains lui reprochent également son interface web dite un peu "vieillotte" et la prise en main initiale n'est pas forcément intuitive.

2.9.2.2 Nagios

a. Présentation de l'outil

Nagios (anciennement appelé Netsaint), créé en 1999 par Ethan Galstad est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services à spécifier, en alertant ainsi des anomalies détectées et lorsqu'ils reviennent dans l'état nominal. [2.10]. C'est un logiciel libre sous licence GPL v2. C'est un outil très complet pouvant s'adapter à n'importe quel type d'utilisation avec des possibilités de configuration très poussées. La modularité et la forte communauté (> 250 000) qui gravite autour de Nagios (en participant au développement de nombreux plugins et addons) offrent des possibilités en terme de supervision qui permettent aujourd'hui de pouvoir superviser pratiquement n'importe quelle ressource.

Par ailleurs, il est aussi ce que l'on appelle un ordonnanceur, c'est-à-dire qu'il va lancer les différents tests de supervision, appelés contrôles, sur les hosts et services. Il reste l'outil de supervision le plus utilisé à l'heure actuelle, sa configuration sous forme de cahiers, peut s'avérer vite repoussante mais en fait cependant un candidat idéal pour l'automatisation.

b. Avantages

- Reconnu auprès des entreprises, grande communauté ;
- Très puissant et modulaire ;
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs;
- Une solution permettant une cartographie du réseau ;
- Beaucoup de documentations sur le web ;
- Performances du moteur ;
- La remontée des alertes est entièrement paramétrable grâce à l'utilisation de plugins (alerte par courrier électronique, SMS, etc…).

c. Inconvénients

- Interface non ergonomique et peu intuitive ;
- Configuration fastidieuse via beaucoup de fichiers et difficile à installer ;
- Pour avoir toute les fonctionnalités il faut installer des plugins, de base c'est assez limité ;
- Dispose d'une interface compliquée ;
- Ne permet pas d'ajouter des hôtes via Web ;
- Besoin d'un autre outil pour faciliter sa configuration ;
- Pas de représentations graphiques.

Les mises à jour de la configuration se font en mode « lignes de commandes » et doivent être réalisées côté supervision comme côté serveur à superviser.

Il est considéré comme étant la référence des solutions de supervision Open Source.

L'inconvénient de Nagios reste son IHM (Interface Homme Machine) très basique. Il faut avouer que son interface ne donne pas spécialement envie d'être consultée, en effet au-delà de la pertinence de l'information, il faut de la compréhension et de l'interprétation.

C'est sur ce constat que vient se créer la prochaine solution décrite : Centreon.

2.9.2.3 Centreon

Centreon (anciennement appelé Oreon) est un logiciel de supervision réseau qui a vu le jour en 2003. Fondé sur le moteur de récupération d'informations Nagios, il fournit une interface simplifiée pour rendre la consultation de l'état du système accessible à un plus grand nombre d'utilisateurs, notamment à l'aide de graphiques.

En effet, Centreon propose une interface web différente de celle de Nagios, des représentations graphiques élaborées et personnalisables et y ajoute des fonctionnalités (génération de la configuration de Nagios, stockage des données de performance, interface ergonomique...). Centreon intègre la gestion de tous les fichiers de configuration de Nagios, un module de chargement de configuration de Nagios avec des tests de validité des configurations (debugger de Nagios). Par ailleurs, Centreon possède des fiches d'identité serveurs/équipements réseaux regroupant les informations de base sur ces types de ressources.

Des alertes sont émises en cas de diminution de la qualité de service et la notification est hiérarchisée.

a. Avantages

- Une installation complète et automatique des packages nécessaires à l'utilisation de NAGIOS ;
- Facilite la configuration de Nagios ;
- Une découverte automatique du réseau via Network Message Access Protocol ou NMAP ;
- Graphe le résultat des alertes, système de reporting.

b. Inconvénients

- Requiert plus de ressources matérielles comme Nagios ce qui fait de lui un outil à part entière.

Il propose donc au sein d'une même interface tout ce qui est nécessaire à la surveillance de l'infrastructure et donc à faire de la supervision pure et dure.

2.9.3 Résultats des différents outils présentés

Le tableau 2.01 représente le résultat de l'étude des outils de supervision. Ce tableau nous servira de comparaison de performance et de modularité des différents outils cités précédemment que ce soit des logiciels payants ou Open Source.

Tableau 2.01 : *Tableau récapitulatif des différents outils de supervision*

	Logiciels Payants			Logiciels Open Source		
	Scom	HP OpenView	IBM Tivoli	Zabbix	Nagios	Centreon
Modularité	-	-	-	Moyenne	Très bonne	Bonne
Performance	Bonne	Bonne	Très bonne	Très bonne	Très bonne	Bonne

2.10 Conclusion

Pour conclure, la supervision est le fait de regarder au-dessus du réseau, de connaître l'état de tous les équipements du réseau que ce soit du niveau de la machine elle-même, le système ou du niveau de l'interconnexion de la machine, le réseau ou des services offerts par la machine, l'application. La supervision peut se faire sous différentes manières, elle peut être assurée que par un seul ordinateur (la supervision centralisé), assuré par des serveurs d'ordre hiérarchique (la supervision hiérarchique) , assuré par plusieurs serveurs occupant chacun un segment précis du réseau (la supervision distribuée). Son concept a été normalisé par l'ISO et le protocole mis en jeu est le protocole SNMP. En effet, ce protocole existe sous plusieurs versions et possède une architecture propre à elle. Son mécanisme de base, constitué d'échange de type requête/réponse favorise son rôle de protocole de gestion réseau.

Vue l'effervescence des problèmes rencontrés dans un réseau informatique, les chercheurs scientifiques ont trouvés une solution pour pouvoir superviser facilement un réseau. C'est l'automatisation de la supervision par des logiciels. Plusieurs solutions peuvent être mises en place, des logiciels payants et des logiciels gratuits et Open Source. Des logiciels payants comme Scom, HP/OpenView et IBM Tivoli ont été analysé dans ce chapitre. Egalement, le monde de l'Open Source a été examiner cela par l'observation de Zabbix, Nagios et Centreon, trois logiciels Open Source qui sont très connus sur le marché. Toutes ces solutions de supervision, qu'elles soient payantes ou gratuites ont plus ou moins de possibilités, de compatibilités matérielles et d'évolution future malgré quelques inconvénients.

CHAPITRE 3
MISE EN PLACE D'UNE SOLUTION DE SUPERVISION

3.1 Introduction

Dans ce chapitre, la mise en place d'une solution de supervision pour l'INSTAT, notre cadre d'étude sera élaboré. Notre cadre d'étude a en effet besoin d'un outil de supervision performant, libre et gratuit pour alléger les dépenses de l'entreprise et pour superviser sans encombre le réseau informatique.

Pour cela donc, un choix entre les différents outils cités dans le précédent chapitre est nécessaire. Ce choix dépendra bien sûr du besoin de l'INSTAT.

3.2 Choix d'une solution de supervision à appliquer au sein du réseau

Si l'on retient ce critère dans le choix d'une solution open source stable ou même payant, Nagios sort largement vainqueur. De plus d'être gratuit, cette solution est en effet la référence en matière de supervision dans le monde de l'Open source et est le plus documenté sur Internet.

Développé depuis 20 ans, il possède une communauté sans égale et des possibilités très étoffés. Il est une application Open Source de surveillance des équipements systèmes et réseaux qui est une référence en supervision grâce à son appui sur un système de plugins permettant la collecte d'informations et dispose d'une interface web représentant tous les indicateurs. Il est très modulaire : il peut s'interfacer avec de nombreux outils externes.

Il a cependant une réputation, méritée, d'être relativement complexe à prendre en main, notamment la partie configuration. C'est pourquoi l'installation et l'utilisation de Centreon, un frontend web qui permet la configuration facile de Nagios est demandée si on veut utiliser Nagios.

En effet, un logiciel de supervision « tout en un » gratuit incluant en même temps Nagios et Centreon vient à point pour faciliter la configuration fastidieuse de Nagios et pour une prise en main et installation facile. Pour offrir aux administrateurs un gain de temps d'installation et de configuration ce logiciel tout-en-un possède plusieurs interfaces. Cet outil de supervision s'appelle Fully Automated Nagios.

3.3 Généralités sur Fully Automated Nagios

3.3.1 Présentation de Fully Automated Nagios

Fully Automated Nagios ou FAN est une solution simple et rapide pour avoir un système de supervision. Le but du projet FAN est de proposer une image iso prête à l'emploi du logiciel de

supervision Nagios entouré de divers outils et addons [3.01]. Initié par Cédric Temple en 2008, FAN est une distribution GNU/Linux et propose une installation simple et efficace pour mettre en place Nagios, Centreon et Nagvis en une installation. L'environnement FAN est donc un environnement déjà configuré, les administrateurs n'ont plus qu'à rajouter les éléments à superviser.

3.3.2 Architecture de Fully Automated Nagios

La Figure 3.01 ci-dessous montre comment Centreon et Nagios interagissent l'un avec l'autre. [3.02]

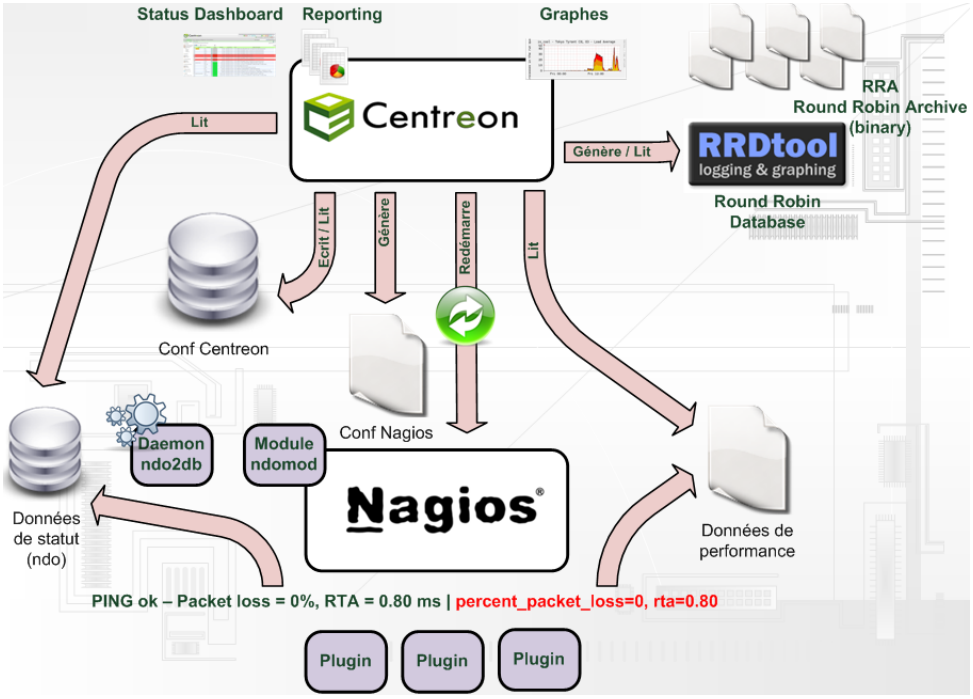


Figure 3.01 : *Architecture de Fully Automated Nagios*

Nagios est le moteur de la supervision tandis que Centreon procure une interface pour la supervision.

3.3.3 Objets inclus dans FAN

Les outils intégrés dans FAN sont: [3.03]

- Nagios : cœur de la supervision;
- Nagios plugins : plugins pour superviser différents équipements ;
- Centreon : interface web pour Nagios (Centreon est l'une des meilleures pour cela) ;
- NagVis : cartographie avancée (géographique, fonctionnelle, par services...) ;
- NDOUtils : stocke les données en provenance de Nagios dans une base MySQL ;

3.4 Configuration des éléments à superviser avec FAN

La supervision avec FAN plus précisément Nagios nécessite la mise en place d'un agent chez l'hôte à superviser et l'activation du protocole SNMP pour certains. Pour cela, il faut installer des agents

comme NRPE, NSCA ou NSClient++ afin d'assurer la communication entre le serveur de supervision et les clients.

3.4.1 NRPE

Nagios Remote Plugin Executor ou NRPE est un agent de supervision qui permet la récupération des informations à distance lors de la supervision d'un serveur Linux. Il a le grand avantage d'exécuter les commandes dans la machine à superviser ce qui lui permet ainsi de répartir les charges. Il est livré avec un ensemble de commandes check définis par défaut dans son fichier de configuration et nécessite l'installation des plugins Nagios aussi.

Ce programme tourne en tâche de fond sur la machine distante et traite les requêtes d'exécution venant du plugin check_nrpe sur l'hôte Nagios. Lorsqu'il reçoit une requête d'un hôte autorisé, il exécute la ligne de commande associée (les Paramètres) avec la commande reçue et envoie le résultat de l'exécution. [3.04]

Check_nrpe est un plugin qui tourne sur l'hôte Nagios et il est utilisé pour le processus NRPE sur les machines distantes. Ce programme demande donc l'exécution du plugin sur la machine distante et attend cette exécution et son résultat et le code de retour.

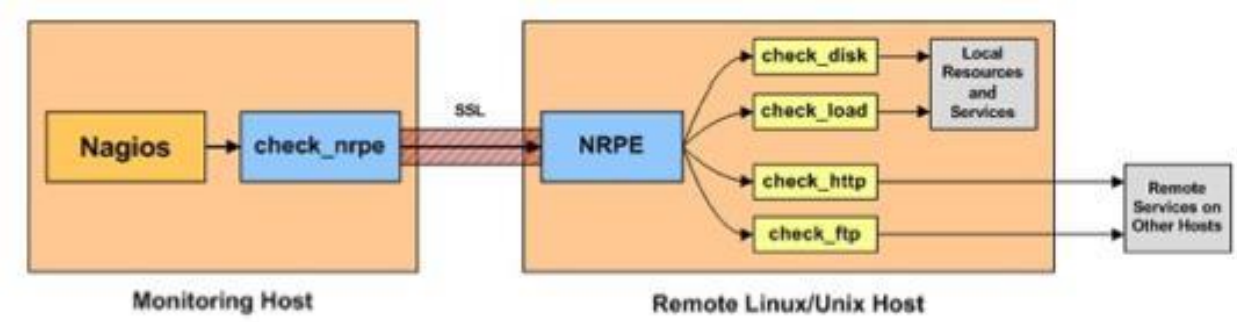


Figure 3.02 : *Fonctionnement de NRPE avec Nagios*

3.4.2 NSClient++

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

NSClient++ est un daemon de surveillance simple et efficace pour les systèmes d'exploitation Windows. Il a été conçu spécialement pour Nagios, mais il n'en est pas dépendant. NSClient++ pourrait sans doute, être intégré dans n'importe quel logiciel de surveillance. La structure du daemon consiste en un service simple qui charge les plugins d'une pile interne. Ces derniers peuvent alors demander des informations résultantes de l'exécution de ces plugins. [3.04]

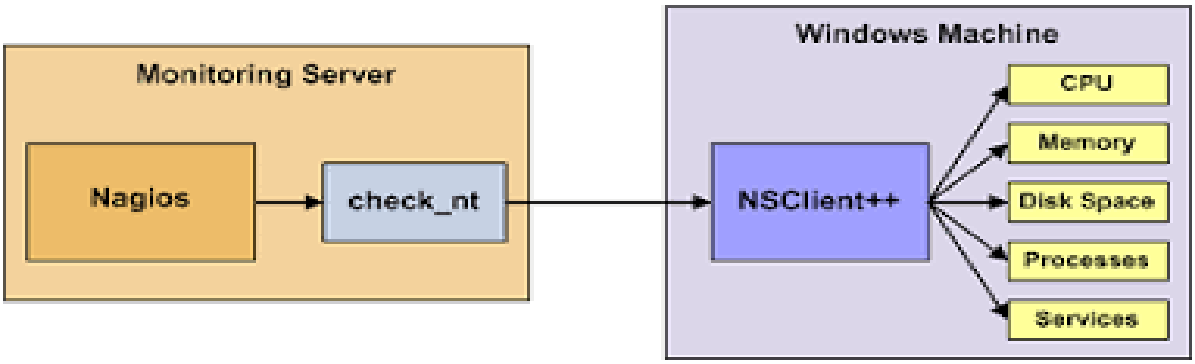


Figure 3.03 : *Fonctionnement de NSClient++ avec Nagios*

3.4.3 NSCA

Le module Nagios Service Check Acceptor ou 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 auto déclenchées.

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 envoi le résultat au serveur Nagios. Enfin le serveur Nagios interprète les résultats et lance le traitement adéquat. [3.04]

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

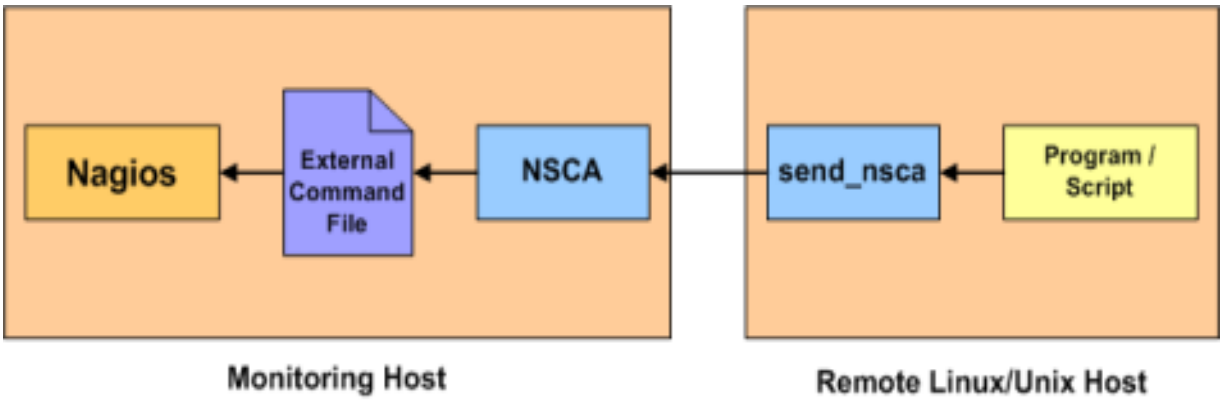


Figure 3.04 : *Fonctionnement de NSCA avec Nagios*

3.5 Simulation

Avant de mettre en place cet outil de supervision Fully Automated Nagios, une phase de simulation est nécessaire pour savoir de fond en comble comment superviser un réseau depuis ce logiciel. Nous verrons comment l'installer, le configurer et l'utiliser. La simulation se fera sur Virtualbox.

3.5.1 Virtualbox

VirtualBox est un hyperviseur permettant la virtualisation afin de créer et gérer des machines fonctionnant sous des mêmes ou différents systèmes d'exploitation sur une seule machine réelle. [3.05]

3.5.2 Description de la simulation à faire

Cette simulation sera dédiée à la supervision de l'état des hôtes Windows et Linux ainsi que les services qui fonctionnent dedans avec Fully Automated Nagios.

D'abord, une création des machines dans Virtual box selon la Figure 3.05 sera faite. Ces machines sont le serveur de supervision FAN, une hôte Windows7 nommé Client Windows, une hôte Windows2008 R2 nommé winserver et une hôte Linux de type Debian. Au total donc, on crée 4 machines.

Ensuite, mettre les 4 machines sur un même réseau, d'après la Figure 3.06. Puis, configurer le serveur de supervision Fully Automated Nagios pour qu'il soit prêt à l'usage. Après, préparer les machines à superviser pour que leur état puisse être consulté depuis le serveur. Enfin, passer le logiciel de supervision FAN à un test de la réactivité.

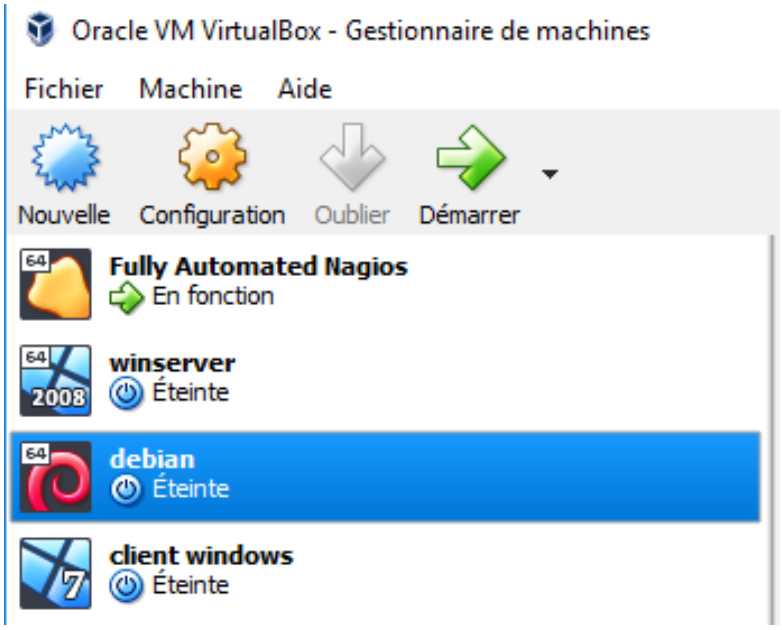


Figure 3.05 : *Création des machines dans Virtualbox*

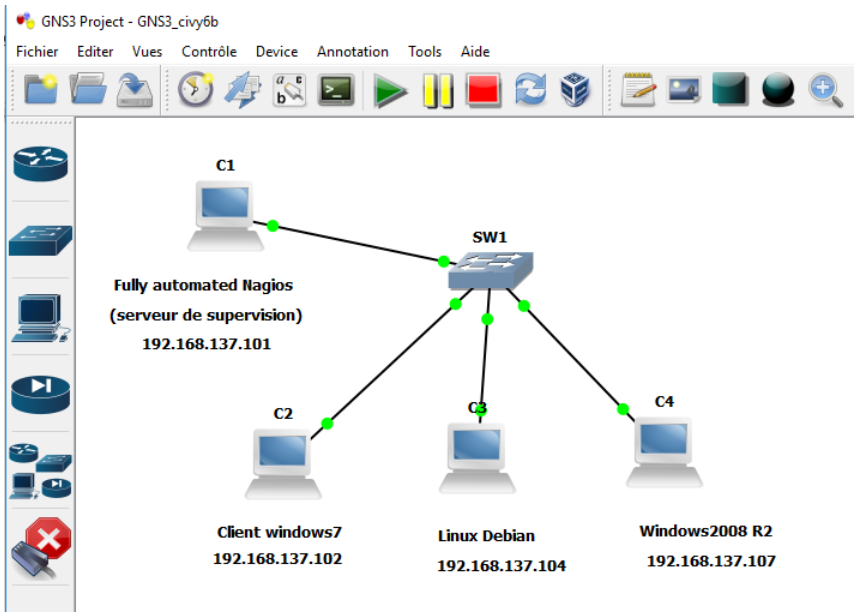


Figure 3.06 : *Emulation de la simulation sur GNS3*

3.5.3 Configuration du réseau dans la simulation

Virtual Box fournit jusqu'à huit cartes Ethernet PCI virtuelles pour chaque machine virtuelle. Pour chaque carte sélectionnée, un choix sur le mode de virtualisation exécutée par la carte virtuelle par rapport au matériel réseau physique sur l'hôte peut se faire. [3.05]

Dans Virtual box, coté superviseur, pour pouvoir avoir accès à l'interface web de FAN à ouvrir sur le navigateur de notre ordinateur réel et en même temps avoir accès à Internet, l'activation de 2 cartes réseaux est indispensable: l'un configuré en Réseau Privé Hôte et l'autre en NAT. On peut aussi n'activer qu'une seule carte tout en accédant à ces connectivités par le mode Accès par pont.

Coté clients, Linux et Windows, la carte réseau doit être en mode Réseau Privé Hôte pour faire la connectivité entre le superviseur et les clients.

3.5.4 Installation du serveur FAN

Récupérer la version de FAN qui correspond le mieux à nos attentes sur le site web de FAN. Ici, l'installation de FAN 2.4 qui est la version la plus récente, développé en mars 2013 a été choisi.

FAN peut être installé sous 3 modes : en mode standalone graphique, en mode distribué et en mode standalone par ligne de commande.

Après avoir insérer le disque d'installation et lancer l'installation en Standalone, un choix de la langue d'installation et l'agencement du clavier s'impose. Puis éditer un mot de passe pour le serveur de supervision. Ejecter le disque avant de redémarrer le serveur.

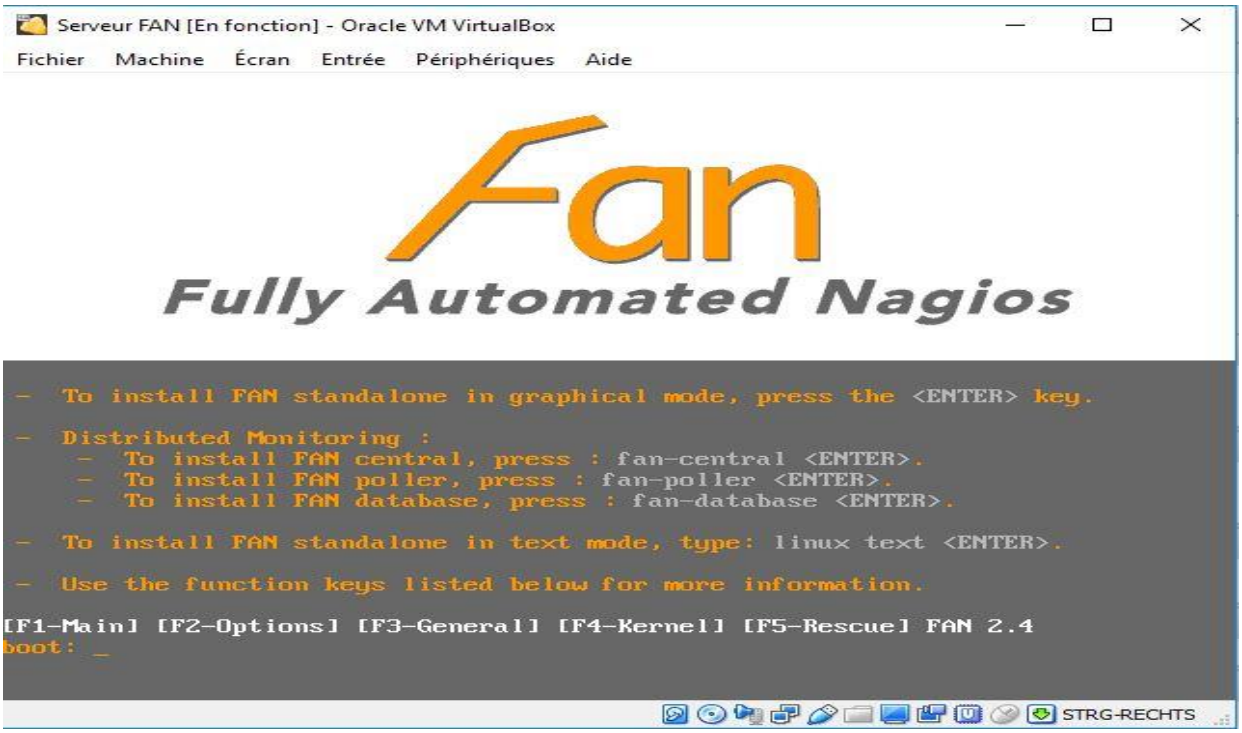


Figure 3.07 : *Début de l'installation de FAN*

3.5.5 Configuration du serveur

3.5.5.1 Configuration du réseau

L'adresse IP du serveur doit être changée en adresse IP fixe ou statique. Pour ce faire, configurer l'interface eth0 du serveur en utilisant la commande « vi » ou « nano ».

```
[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0_
```

Par la suite, éditer l'adresse IP fixe, le masque du réseau, la passerelle :

```
# Intel Corporation 82540EM Gigabit Ethernet Controller
DEVICE=eth0
BOOTPROTO=static
DHCPCLASS=
HWADDR=08:00:27:05:E7:A4
ONBOOT=yes
IPADDR=192.168.137.101
NETMASK=255.255.255.0
GATEWAY=192.168.137.1
```

Une fois le réseau configuré, l'interface web d'accueil du serveur de supervision peut être consulté en ouvrant un navigateur web et en tapant http://ip_du_serveur/ sur la barre des Uniform Resource Locator ou URL.

Pour ouvrir l'interface de Nagios, Centreon et Nagvis le nom d'utilisateur et le mot de passe est « nagiosadmin ».

Figure 3.08 : *Page d'accueil de Fully Automated Nagios*

3.5.5.2 Configuration des notifications

Pour pouvoir être alerté des changements d'états des machines à superviser, Postfix, un serveur mail pour les notifications est déjà installé dans Fully Automated Nagios.

Fully Automated Nagios est donc capable par défaut d'envoyer des messages grâce à Postfix, un célèbre Mail Transfert Agent ou MTA de l'univers du libre [3.06]. Par défaut beaucoup de messages sont envoyés à l'utilisateur root, or pour les consulter la procédure serait complexe, car il faudrait soit les lire en console, soit mettre en place un serveur POP/IMAP. En effet, le plus simple va être de définir une redirection.

Le fichier « /etc/aliases » permet de configurer des alias ou redirection pour les mails des comptes utilisateurs.

```
[root@localhost ~]# nano /etc/aliases
```

Ensuite, aller jusqu'à la ligne « root » et compléter par l'adresse de l'utilisateur concerné.

```
# Person who should get root's mail
#root:          hortensiaramangasalama@gmail.com
```

Pour compiler le fichier, taper la commande « newaliases » et redémarrer postfix.

```
[root@localhost ~]# newaliases
[root@localhost ~]# service postfix restart
```

Maintenant, passer au paramétrage de postfix par le fichier main.cf.

```
[root@localhost ~]# nano /etc/postfix/main.cf
```

Pour préciser l'adresse mail à utiliser pour envoyer les mails, on crée le fichier sasl/passwd.cf et y éditer l'identifiant du compte Gmail et le mot de passe correspondant.

```
gmail_smtp.l.google.com hortensiaramangasalama@gmail.com:[redacted]
smtp.gmail.com hortensiaramangasalama@gmail.com:[redacted]
```

Puis, rediriger les mails vers le serveur par le protocole Simple Mail Transfert Protocol ou SMTP de Gmail avec le port 587 qui est un port associé à Transport Layer Security, une méthode plus sécurisée de remise de courrier.

```
relayhost=[smtp.gmail.com]:587
smtp_sasl_auth_enable=yes
smtp_sasl_password_maps= hash:/etc/postfix/sasl_passwd
smtp_use_tls=yes
smtp_sasl_security_options=noanonymous
smtp_sasl_tls_security_options=noanonymous
```

Du Framework Simple Authentication and Security Layer ou SASL sera utilisé avec le protocole SMTP puisqu'il peut être adapté aux détails du fonctionnement de tout protocole spécifique. C'est un protocole surtout connu pour l'authentification.

Lancer ces commandes puis redémarrer le service postfix après chaque configuration.

```
[root@localhost ~]# chown root:root /etc/postfix/sasl_passwd
[root@localhost ~]# chmod 600 /etc/postfix/sasl_passwd
[root@localhost ~]# postmap /etc/postfix/sasl_passwd
[root@localhost ~]# /etc/init.d/postfix restart
Arrêt de postfix :                                         [  OK  ]
Démarrage de postfix :                                     [  OK  ]
```

Tester maintenant la redirection mail pour voir si le serveur de messagerie Postfix est prêt à l'emploi.

```
[root@localhost ~]# mail -s ESSAI hortensiaramangasalama@gmail.com
Bonjour, ceci est un test
.
Cc:
```

Aller dans la boite mail maintenant pour voir si le message est bien arrivé après avoir bien éditer les commandes vues précédemment. Dans la boite, c'est le super utilisateur « root » qui envoie le message vers le compte mail de l'utilisateur concerné.

Comme le montre la Figure 3.09, le message pour l'essai est bien arrivé à destination.

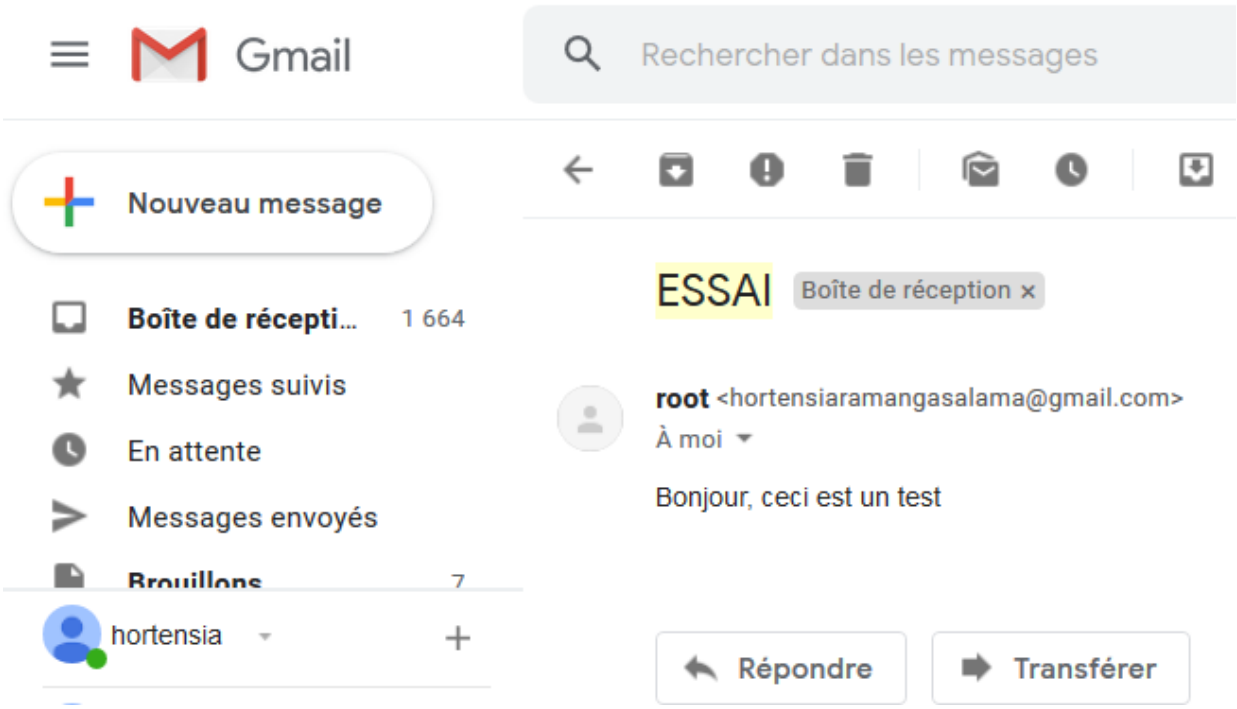


Figure 3.09 : *Réception d'un mail dans Gmail pour le test de postfix*

Le mail pour l'essai est bien arrivé dans la boite e-mail comme le montre la Figure 3.09. Le serveur Postfix est maintenant fonctionnel.

3.5.6 Configuration des machines à superviser

3.5.6.1 Activation du protocole SNMP dans Windows

Pour la prise en main à distance d'un poste Windows, on peut avoir recours à l'outil « rdesktop » qui est à installer sur le serveur de supervision. On active le « Bureau à Distance » dans les propriétés système de Windows.

L'activation du protocole SNMP dans les machines sous Windows est plus simple car cela peut se faire en mode graphique. Puis, disposer du programme NSCA pour ajouter NSClient++ parmi les services. Ensuite, indiquer les informations nécessaires afin d'autoriser la supervision sur la machine Windows.

Aller dans Paramètres> Panneau de configuration> Programmes et fonctionnalités> activer ou désactiver les fonctionnalités Windows. Cocher Protocole SNMP et Fournisseur SNMP WMI et cliquer sur OK.

Cette activation du protocole Simple Network Management Protocol ou SNMP de l'ordinateur Windows à superviser est nécessaire parce que c'est ce protocole qui se chargera de faire la communication entre le superviseur et la machine à superviser.

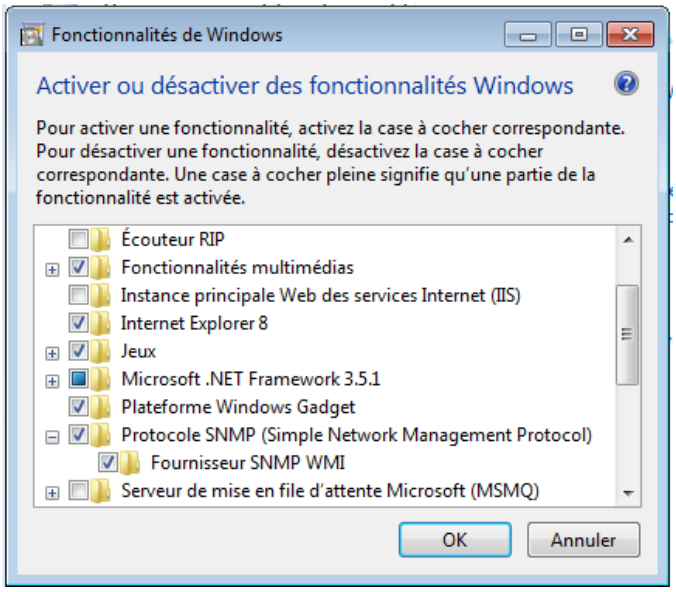


Figure 3.10 : *Activation de SNMP*

3.5.6.2 Installation de NSClient++

NSClient++ est un service pour toutes versions de Windows (NT, 2000, 2003, XP et Vista) qui combine les fonctionnalités d'un agent de supervision dédié à l'environnement Windows ainsi que les fonctions de transport NRPE et NSCA.

3.5.6.3 Installation de NRPE pour Linux

L'installation de NRPE sur Linux se fait via la ligne de commande tout en éditant l'adresse IP de notre serveur FAN lors de l'installation de NRPE.

3.5.7 Ajout d'utilisateur dans le serveur FAN

Un utilisateur est la personne qui reçoit les alertes et les notifications. Le nom, l'adresse mail et les champs de notifications sont à compléter selon le type d'options d'hôte ou de service à notifier. Cet ajout se passe dans l'interface de Centreon.

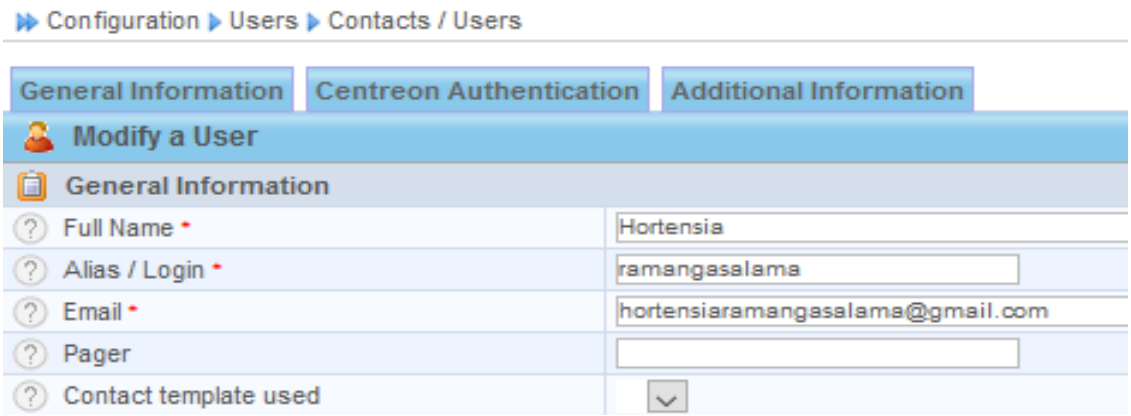


Figure 3.11 : *Exemple d'ajout d'utilisateur*

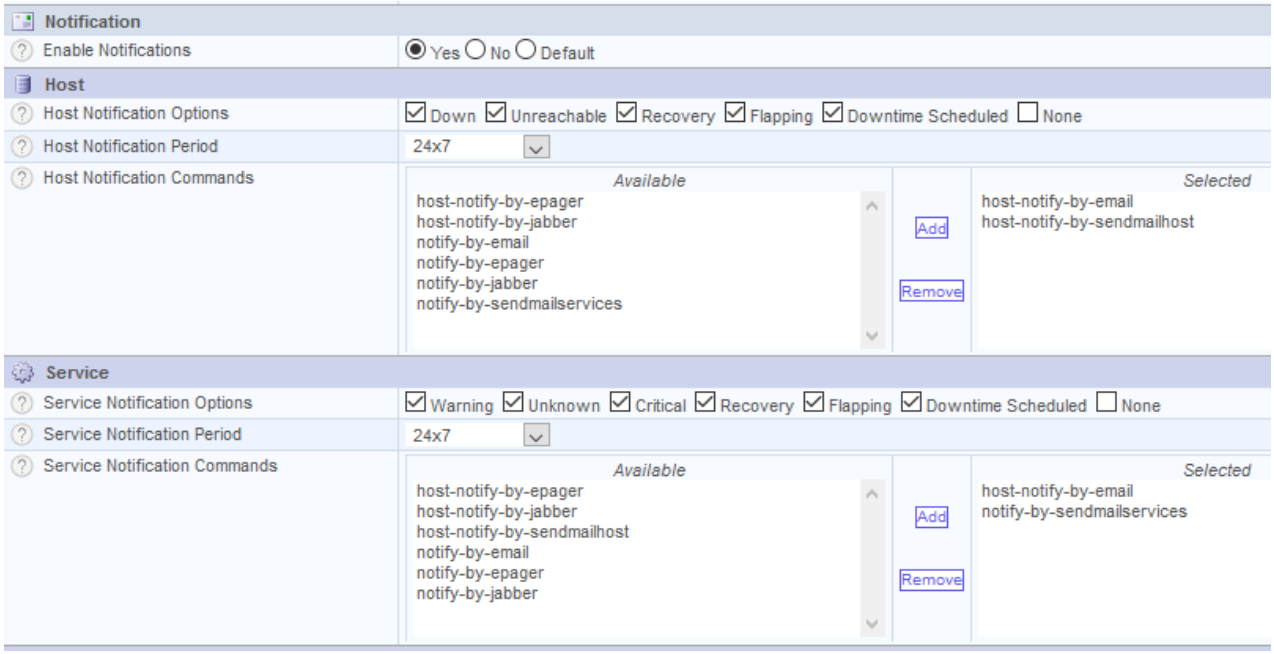


Figure 3.12 : *Option des notifications pour les hôtes et services dans l'ajout d'utilisateur*

3.5.8 Ajout des hôtes ou client sur le serveur FAN

Pour pouvoir ajouter une hôte à superviser, les configurations à entreprendre se trouvent dans l'interface de Centreon. Cliquer sur Configuration> host> add et compléter les champs nécessaires. L'essentiel dans l'ajout d'hôte est : l'attribution de nom d'hôte, l'adresse IP de l'hôte, les temps des vérifications (période et intervalle), les commandes, les notifications. Avec FAN, la supervision peut se faire sur des hôtes Windows, linux, des Switch, des routeurs, des imprimantes.

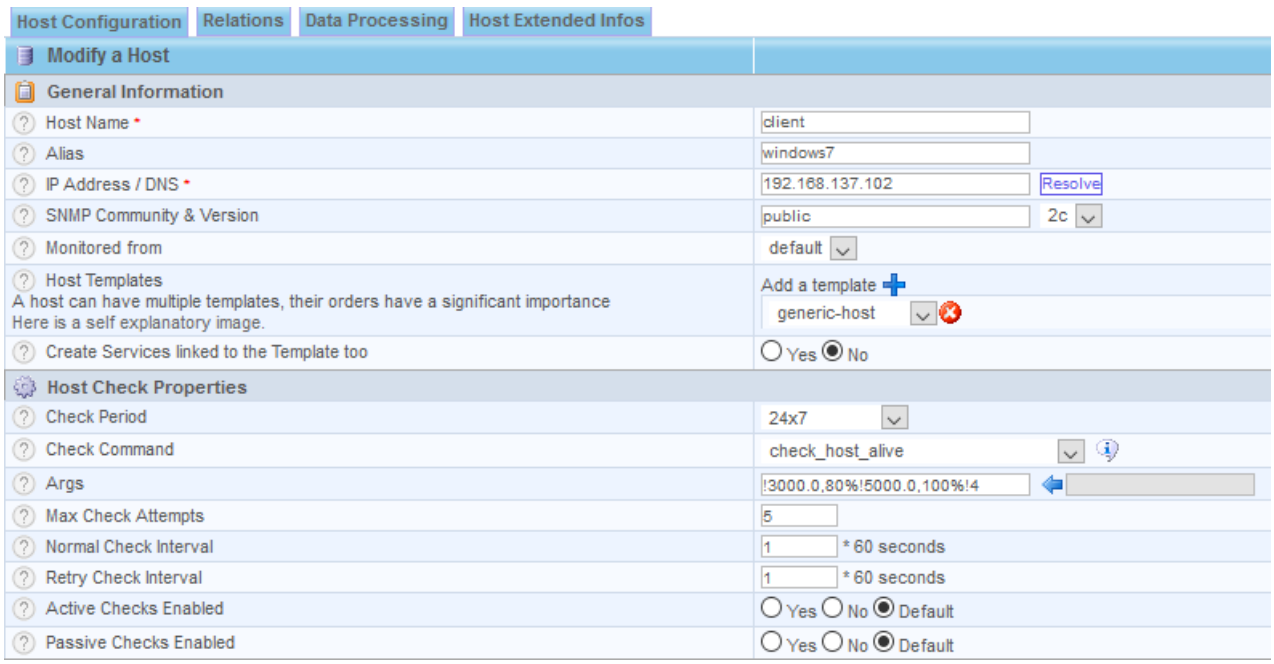


Figure 3.13 : *Exemple d'ajout d'un hôte*

3.5.9 Ajout de service relié aux hôtes dans FAN

Différents types de service peuvent être supervisé avec FAN : Ping, CPU, mémoire, disque, processeur, processus, HTTP, HTTPS, FTP, DNS, LDAP, etc... La Figure 3.14 est un exemple de l'ajout d'un service CPU.

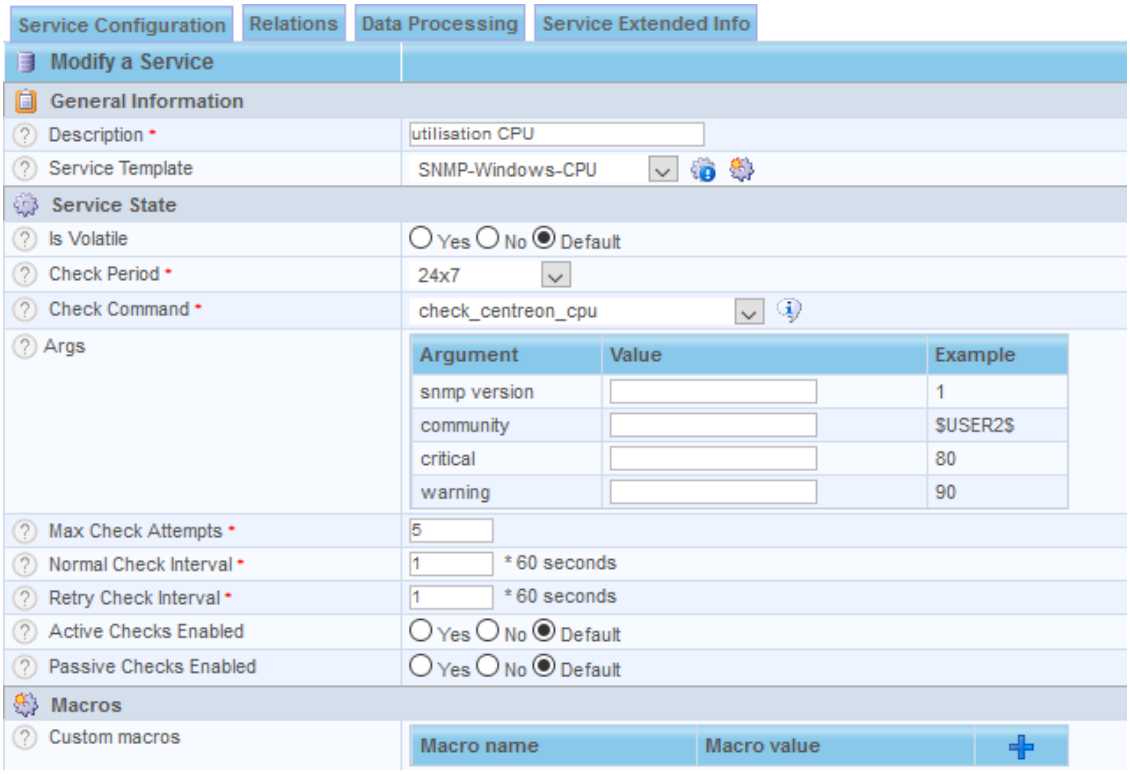


Figure 3.14 : *Exemple d'ajout de service CPU*

Après chaque ajout d'utilisateur, d'hôte ou de service, pour que les configurations soient prisent en compte, ne pas oublier d'exporter les configurations vers le moteur de supervision Nagios. Pour cela, aller dans Configuration > Monitoring Engines > cocher toutes les cases, passer en méthode Restart et cliquer sur Export.

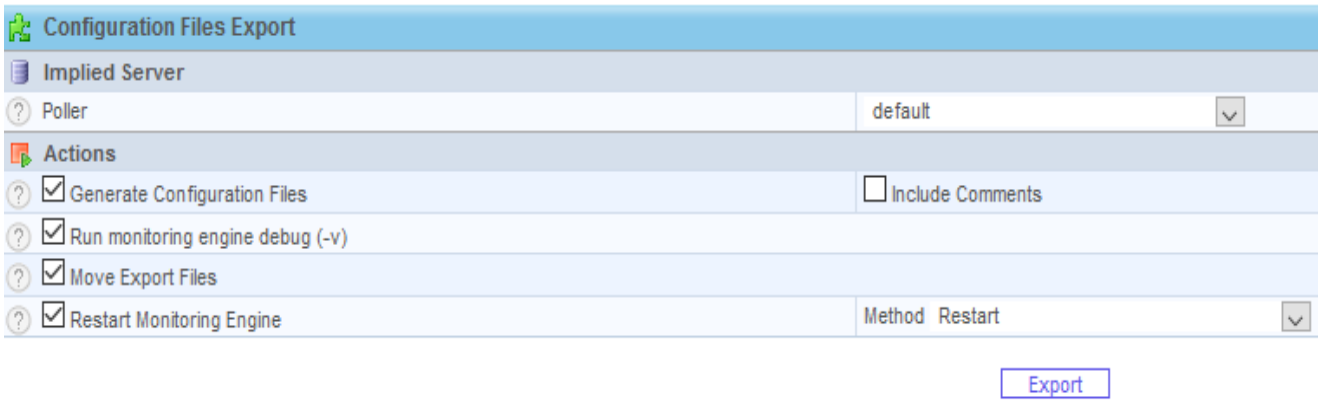


Figure 3.15 : *Export des modifications vers nagios*

3.5.10 Ajout d'une carte sur Nagvis

Aller dans Option> gérer les fonds de carte pour ajouter un fond de carte et pour ajouter une carte: option> gérer les cartes et compléter les champs comme le montre la Figure 3.16. Un fond de carte doit être chargé avant de créer une carte puisque le fond de carte sera utilisé pour la carte.

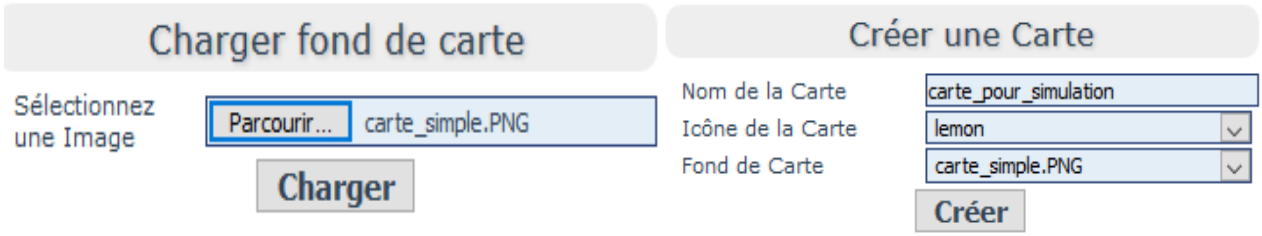


Figure 3.16 : *Ajout de fond de carte et de carte dans Nagvis*

3.5.11 Visualisation de la supervision avec FAN

3.5.11.1 Etats

Les états sont des indicateurs pour les hôtes et les services. Chaque statut a une signification bien précise pour l'objet. L'état des hôtes peut être tout de suite connu grâce aux couleurs qui ont une signification bien précise.

A chaque état correspond un code généré par la sonde de supervision en fonction des seuils par l'utilisateur [3.07].

a. Différents états d'un hôte

Le Tableau 3.01 résume les états possibles pour un hôte et sa description à partir des codes couleurs.

Tableau 3.01 : *Différents états d'hôte possible avec FAN*

Statut	Code de retour	Description
UP	0	L'hôte est disponible et joignable
DOWN	1	L'hôte est indisponible
UNREACHABLE	2	L'hôte est injoignable
PENDING	3	Statut en attente: l'hôte n'est pas encore contrôlé par l'ordonnanceur

b. Différents états d'un service

Tableau 3.02 : *Différents états de service possible avec FAN*

Statut	Code de retour	Description
OK	0	Le service ne présente aucun problème
WARNING	1	Le service a dépassé le seuil d'alerte
CRITICAL	2	Le service a dépassé le seuil critique
UNKNOWN	3	Le statut du service ne peut pas être vérifié (exemple: agent SNMP DOWN)
PENDING	4	Le statut est en attente: service pas encore contrôlé par l'ordonnanceur

La Figure 3.17 est un exemple concret des différents états expliqué dans le Tableau 3.02.

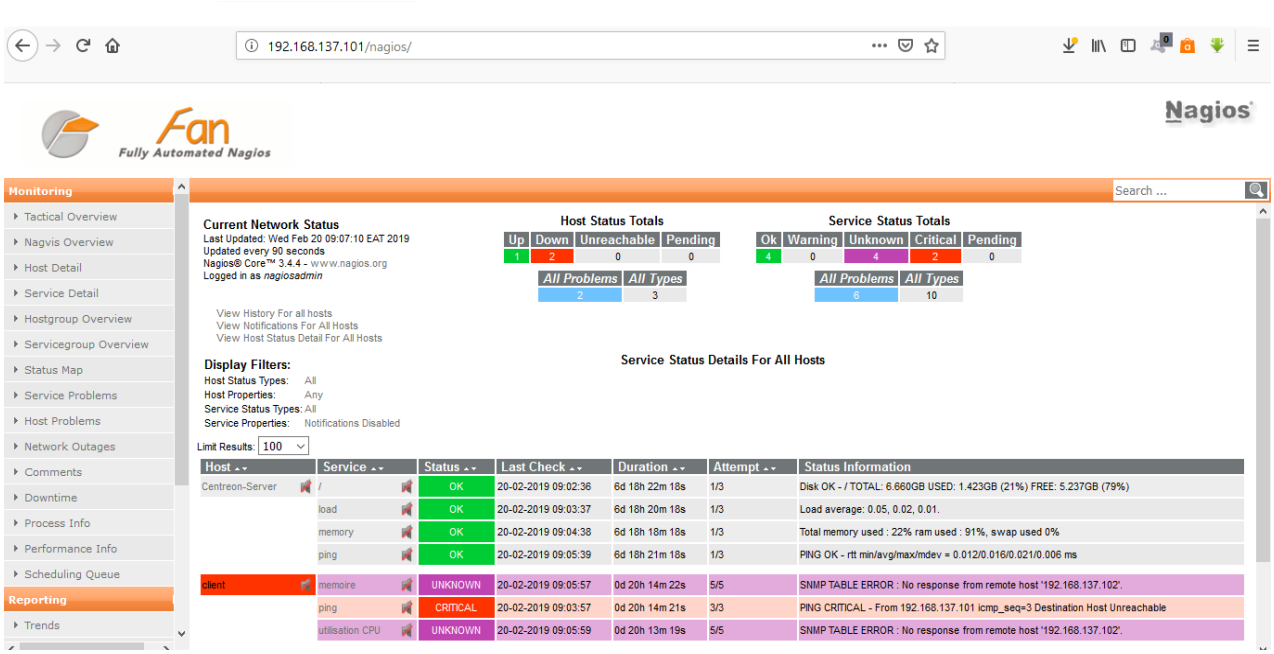


Figure 3.17 : *Visualisation des états sur l'interface de Nagios dans FAN*

3.5.11.2 Graphes

L'interface de Centreon possède deux types de graphes : des graphes de performance et des graphes d'historique. Les graphiques de performances ont toujours comme abscisse une période de temps et comme ordonnée une unité (Volts, Octets...). Les graphiques d'historique ont toujours comme abscisse une période de temps, leurs ordonnées ne varient pas. [3.08]

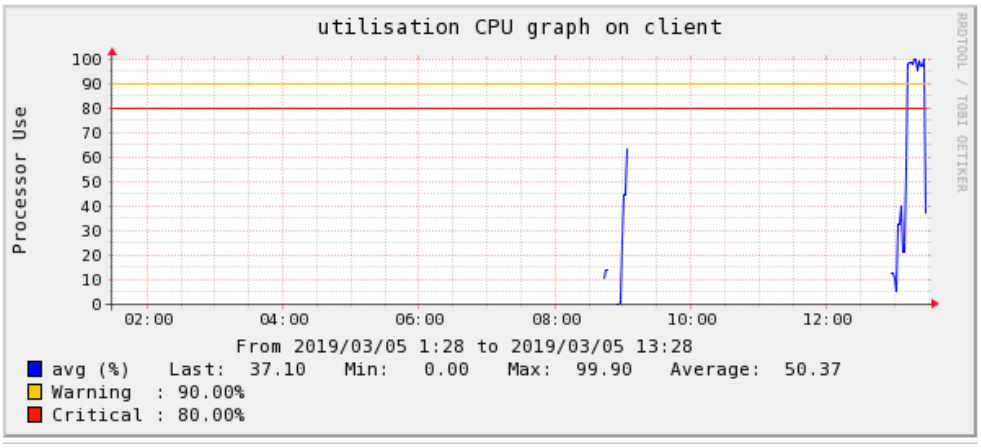


Figure 3.18 : *Graphe de l'utilisation du CPU avec historique*

Illustration du graphe : L'hôte nommée « client » était fonctionnel entre 08 :00 et 10 :00 du matin avec un taux d'utilisation de CPU montante. Vers 13h, après une longue extinction de l'hôte il redémarre avec une utilisation du CPU montante jusqu'à dépasser le seuil critique, la ligne rouge 80% et le seuil d'alerte qui est 90% la ligne jaune.

3.5.11.3 Tableau de bord

Les tableaux de bord permettent d'avoir une vue globale de l'état de tous les hôtes supervisés et des services. Il permet de connaître en pourcentage le total d'hôte allumé et éteinte, les services en état critique, inconnu et fonctionnel [3.08]. Les rapports de disponibilités des objets accessibles via l'interface web Centreon permettent donc de visualiser de manière intuitive le taux de disponibilité d'un hôte, d'un groupe d'hôtes ou d'un groupe de services sur une période de temps donnée.

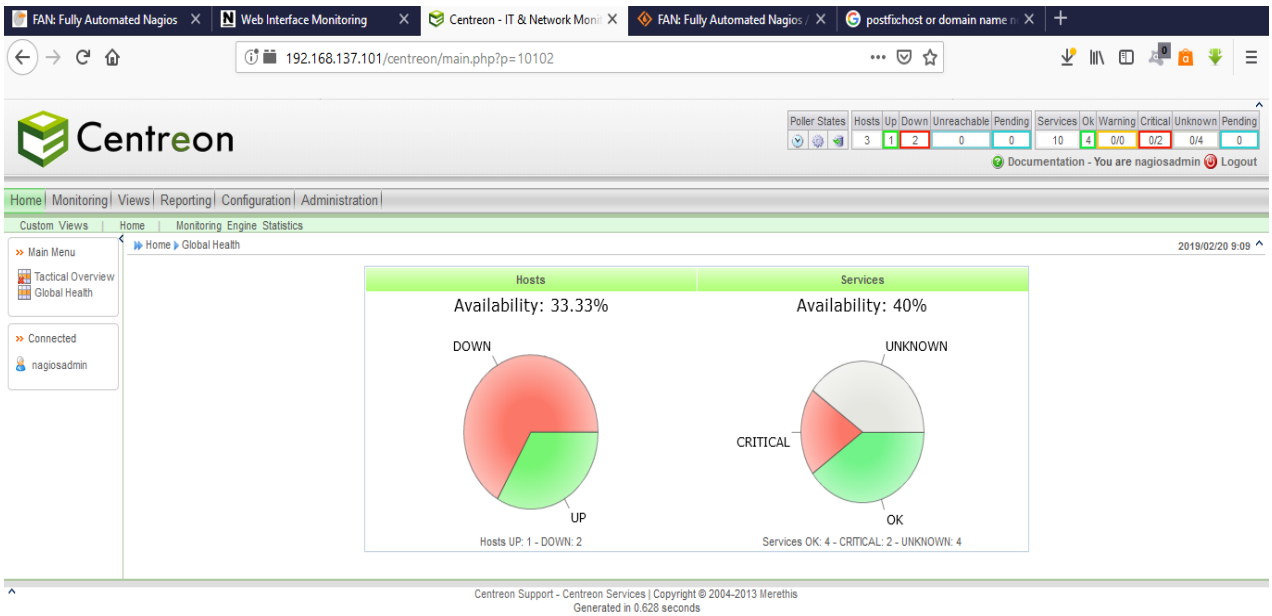


Figure 3.19 : *Tableau de bord de FAN via Centreon*

Le tableau de bord HOSTS indique que 33.33% des hôtes sont allumés, la partie en verte et 66,67% sont éteintes, celles en rouge. Le tableau de bord SERVICES indique que 40% des services sont en bonne états, 40% est en état inconnu et 20% est en état critique.

3.5.11.4 Carte sur Nagvis

Nagvis permet : [3.09]

- d'avoir une vue sur le réseau
- d'identifier facilement les hôtes
- de savoir l'état des hôtes et des services liés aux hôtes

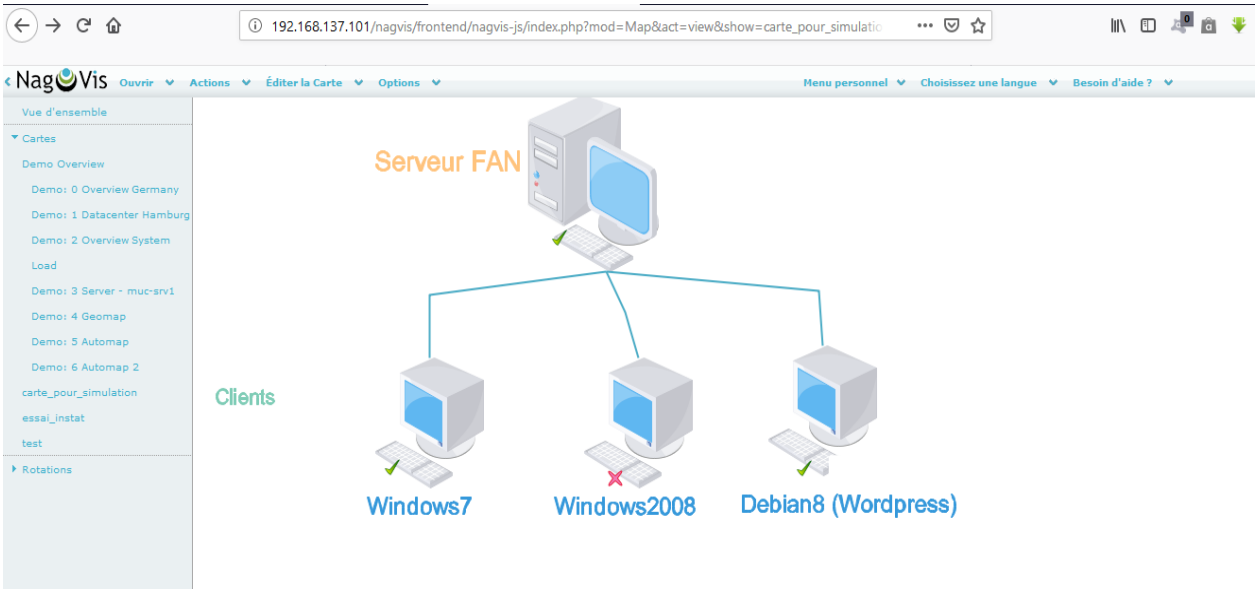


Figure 3.20 : *Interface de Nagvis*

3.5.11.5 Journaux d'évènements

Les journaux d'évènements ou « Event Logs » dans l'interface de Centreon permettent de [3.10]:

- Visualiser les différents changements de statuts et états des objets supervisés
- Voir les notifications envoyées ainsi que leurs destinataires

Ces journaux peuvent être visualisés sur une période donnée.

Un extrait de journal contient beaucoup de détails sur la supervision d'un hôte : la date, l'heure, le nom de l'hôte, l'état de l'hôte, détails du service, le récepteur de notification par mail.

L'extrait de journal de la Figure 3.21 montre quand est ce que l'hôte a été allumé et éteinte, quand est-ce qu'on a reçu des notifications d'alerte concernant l'hôte, qui a reçu les notifications d'alerte de l' hôte et quel changement d'état des services CPU, mémoire et Ping est apparue.

Day	Time	Host	Status	Status	Type	R	Output	Contact	Command
2019/03/06	16:13:25	client	memoire	UNKNOWN	HARD	2	SNMP TABLE ERROR : No response from remote host '192.168.137.102'.		
2019/03/06	16:13:25	client	utilisation CPU	UNKNOWN	HARD	2	SNMP TABLE ERROR : No response from remote host '192.168.137.102'.		
2019/03/06	16:05:15	client	utilisation CPU	OK	HARD	5	CPU utilization percentage : 30%		
2019/03/06	16:04:40	client	ping	OK	HARD	3	PING OK - rtt min/avg/max/mdev = 1.984/2.447/3.126/0.493 ms		
2019/03/06	16:04:25	client		UP	NOTIF		PING OK - Packet loss = 0%, RTA = 3.69 ms	Hortensia	host-notify-by-email
2019/03/06	16:04:25	client		UP	NOTIF		PING OK - Packet loss = 0%, RTA = 3.69 ms	Hortensia	host-notify-by-sendmailhost
2019/03/06	16:04:25	client		UP	HARD	1	PING OK - Packet loss = 0%, RTA = 3.69 ms		
2019/03/06	16:04:20	client	memoire	OK	HARD	5	Total memory used : 18% ram used : 27%, swap used 13%		
2019/03/06	10:54:51	client		DOWN	NOTIF		CRITICAL - Host Unreachable (192.168.137.102)	Hortensia	host-notify-by-email
2019/03/06	10:54:49	client		DOWN	NOTIF		CRITICAL - Host Unreachable (192.168.137.102)	Hortensia	host-notify-by-sendmailhost
2019/03/06	10:54:49	client		DOWN	HARD	5	CRITICAL - Host Unreachable (192.168.137.102)		
2019/03/06	10:53:04	client	ping	CRITICAL	HARD	1	PING CRITICAL - From 192.168.137.101 icmp_seq=3 Destination Host Unreachable		
2019/03/06	10:50:49	client	memoire	UNKNOWN	HARD	1	SNMP TABLE ERROR : No response from remote host '192.168.137.102'.		
2019/03/06	10:50:49	client	utilisation CPU	UNKNOWN	HARD	1	SNMP TABLE ERROR : No response from remote host '192.168.137.102'.		
2019/03/06	10:45:39	client	utilisation CPU	OK	NOTIF		CPU utilization percentage : 34%	Hortensia	host-notify-by-email
2019/03/06	10:45:39	client	utilisation CPU	OK	NOTIF		CPU utilization percentage : 34%	Hortensia	notify-by-sendmailservices

Figure 3.21 : *Journal d'évènement de l'hôte nommé client sur Centreon*

3.5.12 Réactivité du serveur face aux incidents

3.5.12.1 Création d'incident

La solution de supervision doit être réactive au changement d'état des hôtes, c'est pourquoi pour voir cette réactivité de FAN, nous allons créer un incident.

Sur la machine Client Windows, on va occuper le maximum de CPU tandis que la machine Debian, on va l'éteindre. La machine Windows2008 R2, on la laisse toujours éteinte.

3.5.12.2 Vérification de la réaction du serveur

En cas de service en état critique, une alarme sonne sur le serveur (un bip sonore). A part cela, une notification par mail arrive dans la boite e-mail de la personne qui supervise ainsi qu'un changement d'état apparait sur l'interface de Nagios, Centreon et Nagvis.

a. Réception d'une alerte par mail

Puisque la notification par mail de FAN a été déjà configurée, une alerte par mail doit donc être reçue au niveau du compte de l'utilisateur concerné.

L'hôte Windows a eu un problème d'utilisation CPU, normalement une notification dans la boite e-mail apparait comme le montre la Figure 3.22. Il en est de même pour l'hôte Linux Debian éteinte, une notification informant la personne à contacter arrive dans la boite e-mail comme le montre la Figure 3.23 que Debian est éteinte.

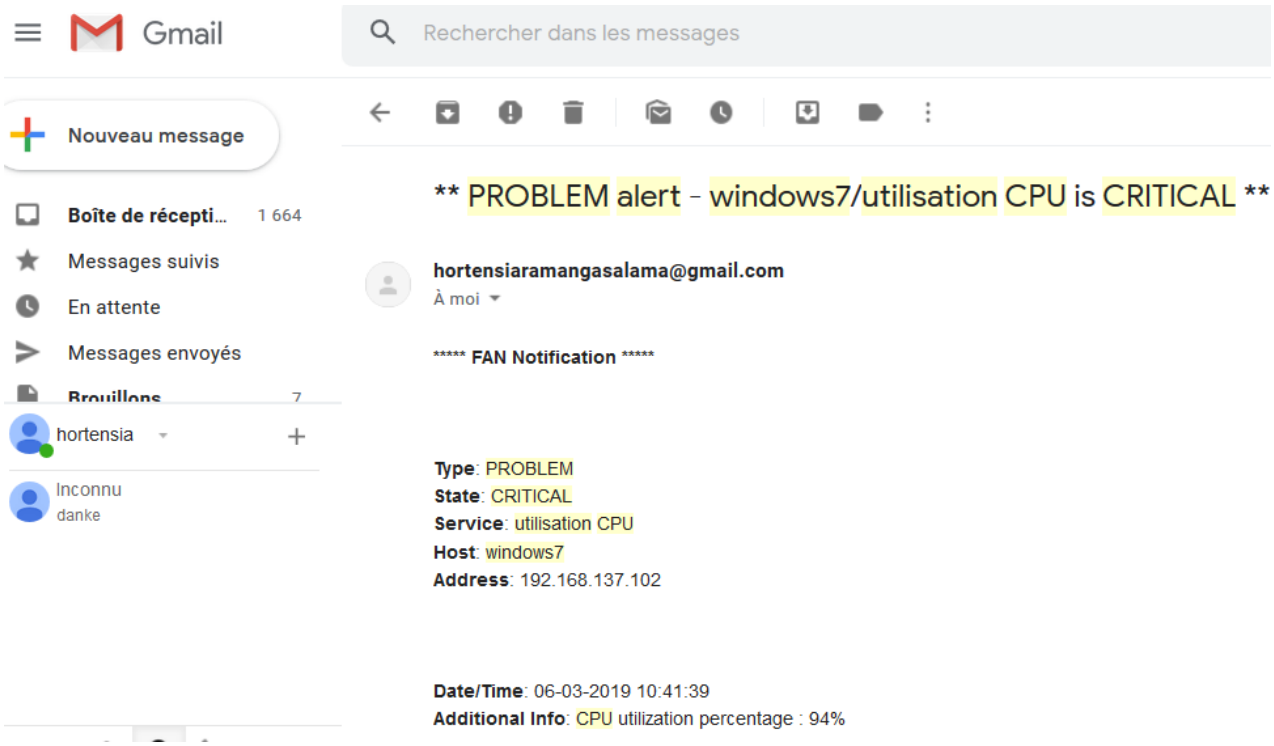


Figure 3.22 : *Notification d'utilisation CPU pour l'hôte client Windows*

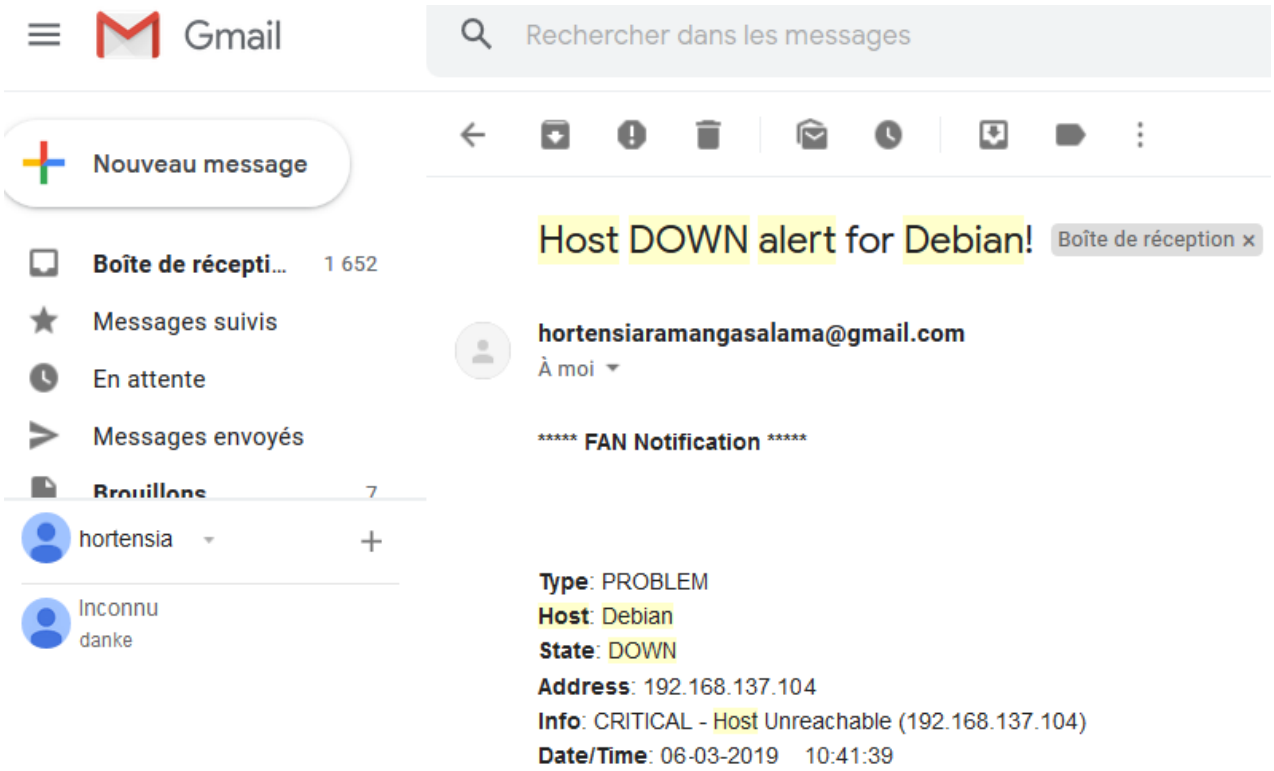


Figure 3.23 : *Notification d'arrêt de l'hôte Linux*

Des informations sur le problème sur l'hôte sont notifiés dans le mail comme la date de l'incident, l'adresse IP et l'état de l'hôte ou du service concerné par le problème.

b. Changement d'état sur les interfaces de Nagios, Centreon et Nagvis

L'interface de Nagios informe que l'hôte Debian est éteinte ce qui signifie que son Ping est en état critique et injoignable c'est pour cela qu'il est en rouge d'après la Figure 3.24. L'interface de Nagvis et de Centreon informe aussi de cette extinction de l'hôte d'après la Figure 3.25 et la Figure 3.26.

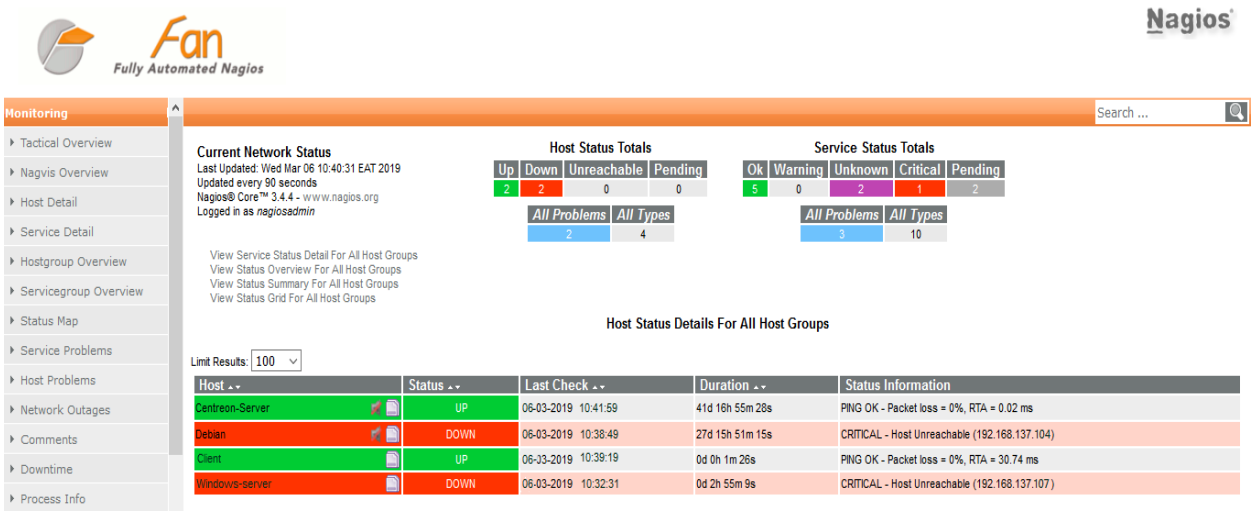
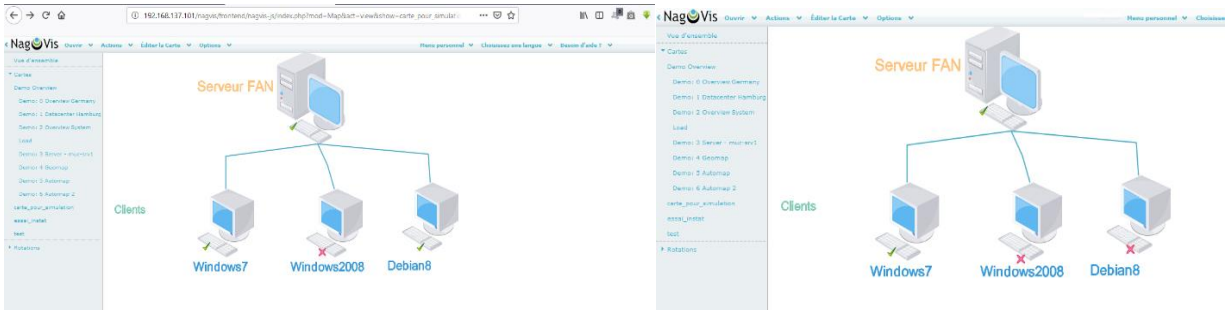
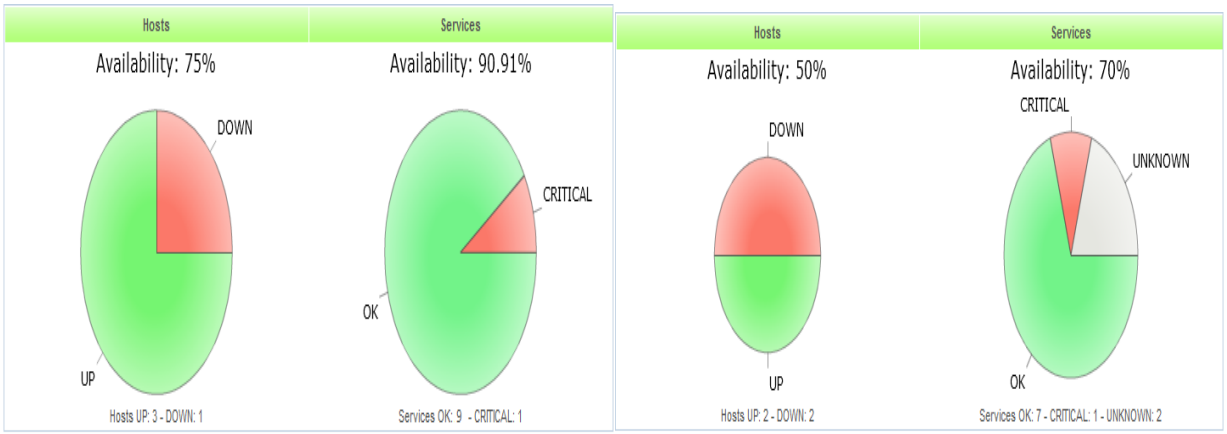


Figure 3.24 : *Changement d'état sur Nagios*



AVANT APRES

Figure 3.25 : *Changement d'état de l'hôte Linux dans l'interface de Nagvis*



AVANT APRES

Figure 3.26 : *Changement d'état du Tableau de bord de Centreon*

Le journal d'évènement de Centreon montre des détails sur les incidents aperçus comme le changement d'état du CPU de l'hôte nommé cliente, la date de l'incident, la personne qui a reçu le mail de notification d'alerte et bien sûr le détail du problème comme affiché sur la Figure 3.27.

2019/03/06	10:41:39	client	utilisation CPU	CRITICAL	NOTIF		CPU utilization percentage : 94%	Hortensia	host-notify-by-email
2019/03/06	10:41:39	client	utilisation CPU	CRITICAL	NOTIF		CPU utilization percentage : 94%	Hortensia	notify-by-sendmailservices
2019/03/06	10:41:39	client	utilisation CPU	CRITICAL	HARD	5	CPU utilization percentage : 94%		
2019/03/06	10:33:40	client	utilisation CPU	OK	HARD	5	CPU utilization percentage : 37%		
2019/03/06	10:33:05	client	ping	OK	HARD	3	PING OK - rtt min/avg/max/mdev = 1.691/2.077/2.434/0.304 ms		
2019/03/06	10:32:46	client		UP	NOTIF		PING OK - Packet loss = 0%, RTA = 2.53 ms	Hortensia	host-notify-by-email
2019/03/06	10:32:45	client		UP	NOTIF		PING OK - Packet loss = 0%, RTA = 2.53 ms	Hortensia	host-notify-by-sendmailhost

Figure 3.27 : *Journal de client : état du CPU devenu critique dans Centreon*

3.6 Implantation de FAN

Ce serveur de supervision a été implémenté dans la partie rez-de-chaussée de l'INSTAT, bureaux de la Direction Informatique, Direction des Statistiques de Ménage et Direction de la Démographie et de la Statistique Sociale. Les bureaux de DRID, DIR TANA et salle des archivistes n'ont pas pu être supervisé pour des raisons de travail des employés et pour la différence de switch utilisé dans la partie Nord et la partie Sud du rez-de-chaussée de l'INSTAT. La partie au-dessus de la ligne verte comme le montre le schéma suivant est donc la partie d'essai de la solution de supervision FAN.

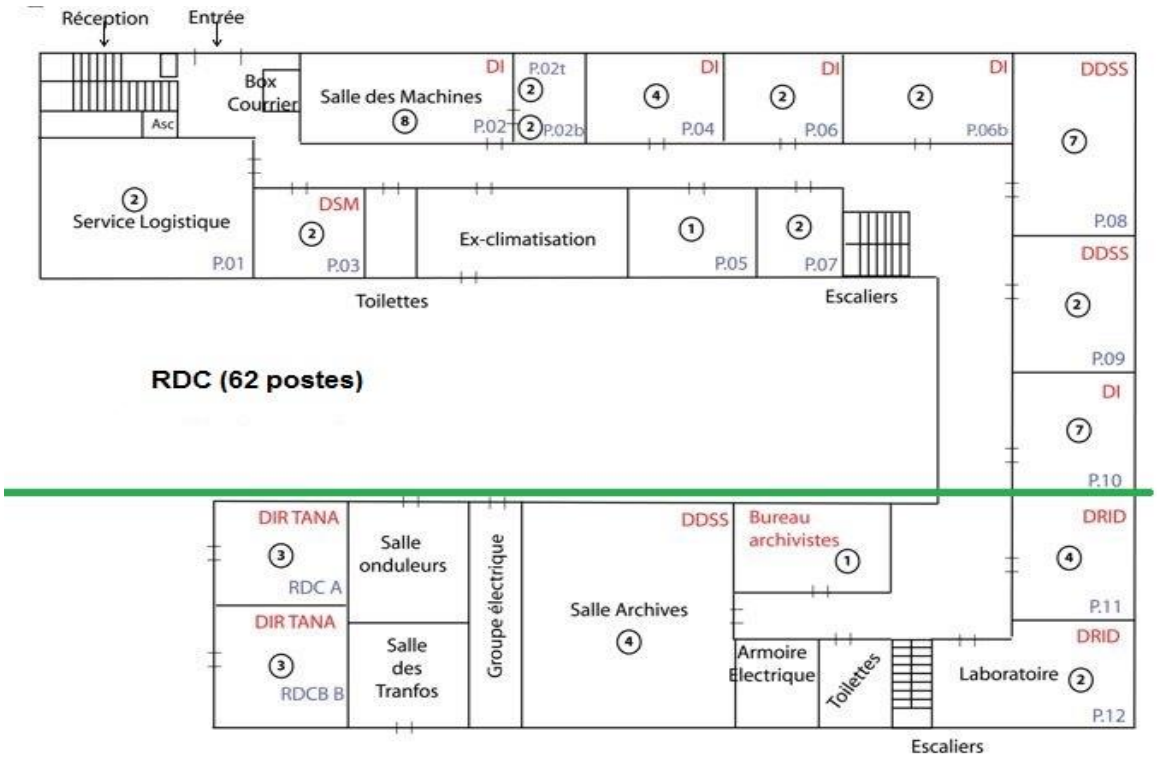


Figure 3.28 : *Plan réseau du rez-de-chaussée de l'INSTAT*

Lors de l'essai technique, le total des machines à superviser est au nombre de 43. Les services mémoire, RAM, CPU, disque et Ping sont les services à superviser et les mails atterriront dans notre boite mail pour éviter d'encombrer le mail de notre technicien réseau lors du test. Les modifications et la prise en main ont été entreprises avec l'aide du technicien réseau.

L'installation du serveur s'est fait en mode standard (mono serveur) et a été déployer de manière centrale (déploiement centralisé). Lors de l'installation donc, on a opté à l'installation de FAN central. Vue que le nombre d'équipements à surveiller est petit, la mise en œuvre d'une architecture distribuée n'est pas nécessaire et serait considéré comme de la sur qualité.

Comme la majorité des ordinateurs chez l'INSTAT fonctionne sous Windows, il nous est courant d'installer NSClient++ sur les stations de travail à superviser et d'activer SNMP.

Au cours de la mise en place du projet, on a pu savoir que les 8 ordinateurs dans la salle des machines ainsi que les 4 autres dans la salle d'à côté ne sont pas fonctionnels c'est pourquoi, le nombre de machine à superviser se réduit à 31.

Le journal d'évènement de la Figure 3.29 détaille l'état des services supervisés sur un groupe d'hôte.

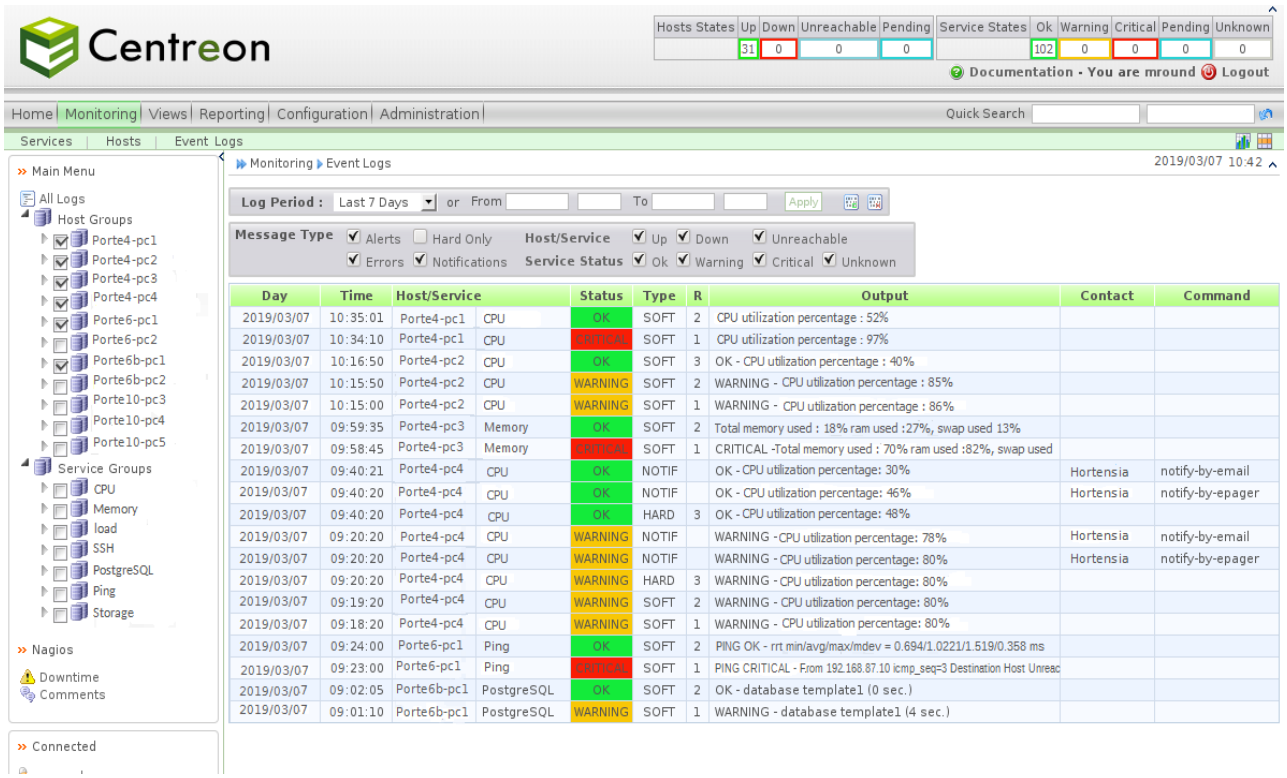


Figure 3.29 : *Extrait du journal d'évènement sur les services*

L'interface de Nagvis procure une vue du réseau supervisé comme le montre la Figure 3.30. Des détails sur les hôtes s'affichent quand on passe le curseur sur les icones vertes et rouges.

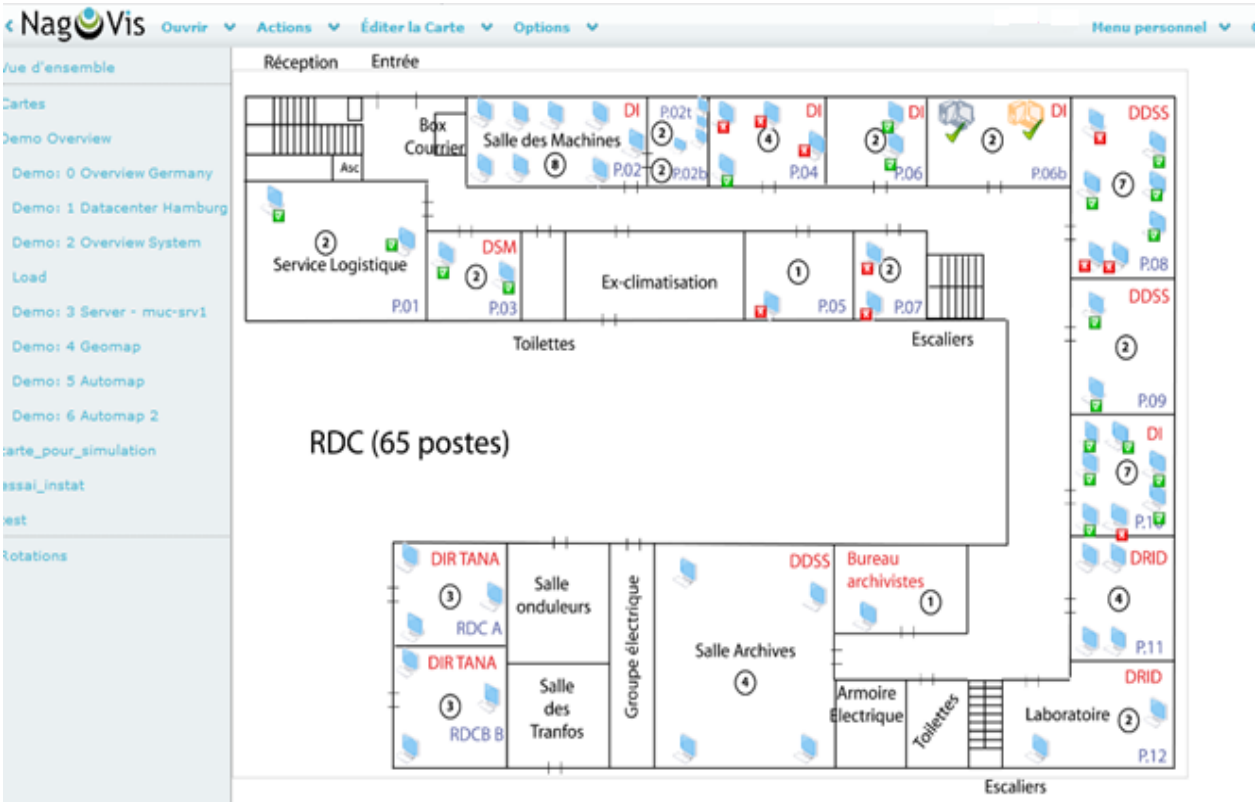


Figure 3.30 : *Supervision depuis Nagvis du réseau de l'Instat*

Lors de l'extinction ou le démarrage des machines, des alertes de notification atterrissent dans la boite e-mail informant l'administrateur de l'état des hôtes. La Figure 3.31 désigne les notifications d'arrêt des hôtes lors des heures de pause puisque l'essai s'est effectué vers l'heure de pause.

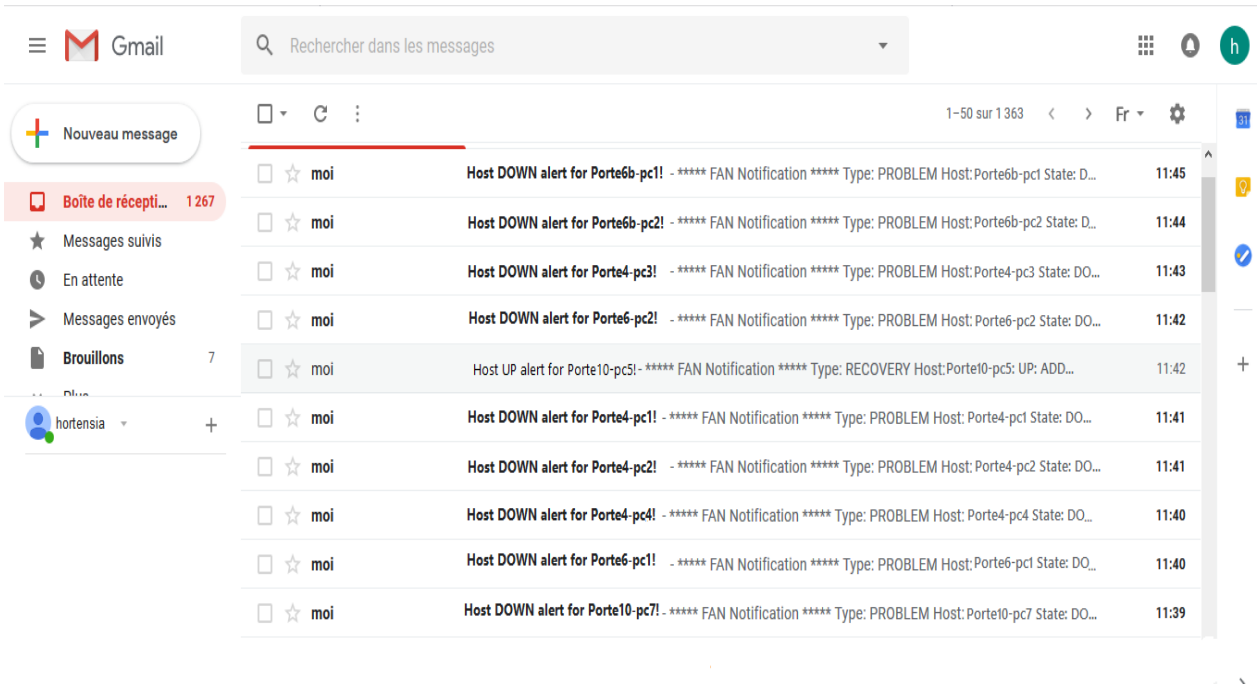


Figure 3.31 : *Extrait des alertes de notification atterrissant dans la boite e-mail*

3.7 Impact pour l'entreprise

Avec la mise en place de ce projet de supervision système et réseau, les techniciens informatiques ont pu voir les problèmes souvent rencontrés sur les stations de travail et anticiper sur d'éventuelles pannes futures par l'utilisation du logiciel libre FAN. Des disques durs de machine qui étaient pleins à 95 % ou des processeurs bloqués à 100% ont été trouvés. De plus, ils ont maintenant une vue globale sur tous les postes de travail dans le réseau grâce à Nagvis inclus dans FAN. Il leur est facile d'identifier les machines depuis leur bureau en cas de problème sur les machines à superviser.

Par ailleurs, l'interface de Centreon et de Nagios donnent plus de détails sur ce qui se passe au sein de l'utilisateur grâce aux graphes, aux journaux d'évènement permettant de savoir l'allure des changements d'états, la moyenne des services supervisés, ce qui met l'administrateur à connaître ce qui va se passer dans les prochaines heures comme l'arrêt d'un service ou d'un hôte faute d'un état très critique avant même que l'utilisateur ou l'employé se rend compte. Grace aux notifications par mail aussi, l'administrateur peut s'éloigner de l'écran de son serveur tout en ayant des nouvelles sur ce qui se passe sur le réseau informatique de l'entreprise.

Grace à ce serveur de supervision aussi, on a pu essayer de réparer un maximum de problème pour avoir une carte sur Nagvis avec moins d'alerte possible. Par ailleurs, on a pu identifier quelques équipements qui n'existaient plus ou qui avaient changé d'adresse IP comme les 8 ordinateurs dans la salle de machine.

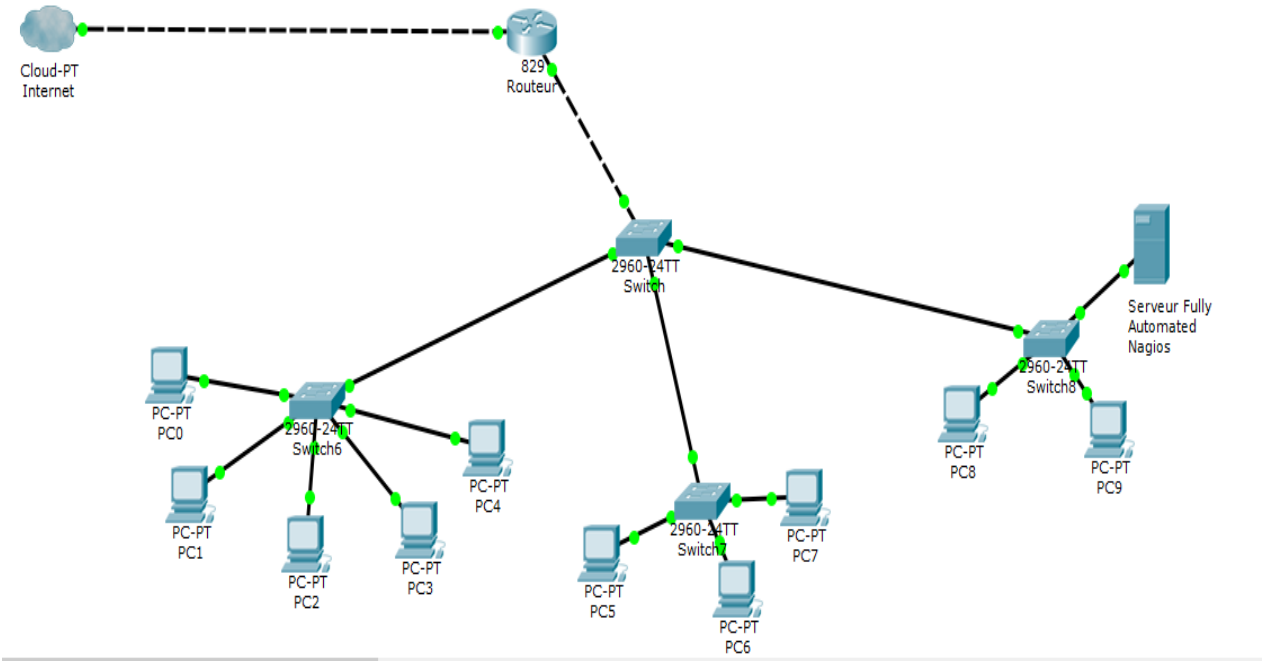


Figure 3.32 : *Nouvelle topologie avec le serveur de supervision FAN*

3.8 Conclusion

En guise de conclusion, suite à une comparaison des différents logiciels de supervision, notre choix s'est orienté vers Nagios, un logiciel open-source performant et très reconnu dans le monde de la supervision. En effet, ce choix a été le fruit de l'étude du besoin de l'INSTAT. Pour être plus pratique et avoir une solution plus bénéfique, on a opté à l'installation de Nagios garni d'autres outils qui sont Centreon et Nagvis. Le nom de cette solution pratique est Fully Automated Nagios et elle fournit tous ces outils en une seule installation. Son installation est très intuitive, les configurations à faire pour sa mise en marche ne sont pas fastidieuses et sa mise en place a permis de comprendre la prise en main et le fonctionnement de la supervision. Les agents NSClient++ et NRPE sont à installés chez l'hôte à superviser pour pouvoir utiliser cette solution. FAN permet de visualiser facilement tous les éléments d'un réseau informatique à travers ces trois interfaces web conviviales affichant des informations globales et détaillées. De plus, à part la détection des alertes et des problèmes, elle les notifie dans l'objectif d'alerter les bonnes personnes au bon moment et de la bonne manière par le serveur de messagerie Postfix d'après la simulation faite. Son implantation au sein de l'INSTAT s'est fait en mono serveur, déployé de manière centralisée et a permis aux administrateurs de connaître en temps réel l'état du réseau et d'avoir une vue du réseau avec Nagvis. En perspective du projet de mise en place, une optimisation du mécanisme d'alerte est envisagée par l'utilisation de la notification par SMS qui est sans doute plus pratique que les mails exigeant une connectivité en permanence à Internet.

CONCLUSION GENERALE

Pour conclure, nous avons vue qu'avant de se focaliser dans la supervision, il est indispensable de connaitre le monde à superviser, le réseau informatique. Des études sur les généralités sur le réseau a été faite dans le premier chapitre afin de bien comprendre le domaine sur lequel la supervision se fera. On a vue les différents types de réseaux, leur architectures, les normes qui les régissent ainsi que les termes à connaître au sein d'un réseau. Pour pouvoir appliquer la supervision, un cadre d'étude a été analysé pour permettre de définir les critères attendues en terme de supervision.

Le second chapitre a été surtout marqué par le concept de la supervision, les normes , les différents manières de déployer la supervision ainsi que le protocole responsable de la supervision qui est le protocole SNMP. En outre, sa définition, son mode de fonctionnement et son but ont été évoqué afin de souligner à quel point la supervision est indispensable face a l'augmentation de nombres de technologies à gérer dans les entreprises et des problèmes souvent rencontrés sur ces techonologies. Un comparatif entre différents outils de supervision payants et gratuits nous a été nécessaire pour avoir une solution de supervision la plus optimale pour notre cadre d'étude.

Dans le dernier chapitre, notre choix pour la supervision s'est tourné vers Nagios, un logiciel gratuit et libre qui est surtout connu pour sa modularité et sa performance. Afin de travailler efficacement, une installation de Nagios garni d'autre outils Centreon et Nagvis a été entreprise. Le nom de cette solution incluant les trois a la fois est Fully Automated Nagios et elle permet des alertes de notification par mail avec Postfix. Avant la mise en place du projet au sein du cadre d'étude, une simulation ainsi qu'une compréhension des configurations à faire a été faite pour avoir un exemple concret de la supervision.

La réalisation du stage au sein de la Direction Informatique de l'INSTAT qui est le cadre d'étude dans ce projet m'a permis d'acquérir maintes connaissances dans le monde de la supervision des réseaux informatiques, surtout de l'environnement Unix et CentOs, et plus précisément dans le professionnalisme.

Comme nous avons vue dans le corps de ce livre, nous avons réalisé une mise en place de supervision centralisée avec FAN. Nous espérons qu'à la prochaine fois, notre recherche sera continuée à une architecture très vaste en utilisant l'outil de surveillance Eyes Of Network avec une notification permettant d'effectuer aisément un redémarrage automatique et des notifications par SMS pour des remontées d'alerte plus rapide.

ANNEXES

Annexe 1 : CONFIGURATION DES MACHINES A SUPERVISER

A1.1 Installation de NSClient++ sur Windows

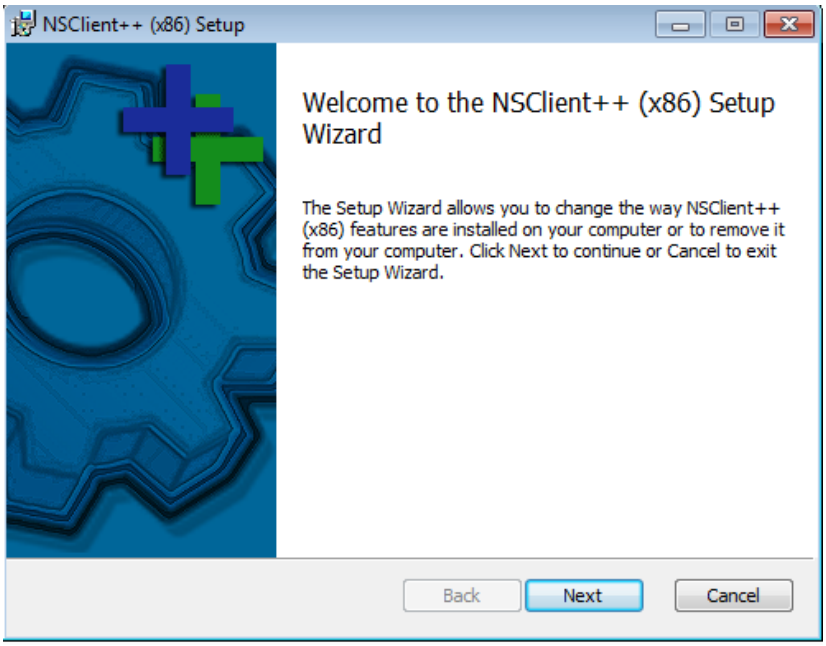


Figure A1.01 : Début de l'installation de NSclient++

Entrer l'adresse IP du serveur FAN ainsi que le mot de passe du serveur FAN. Cocher les 2 dernières cases puis continuer l'installation.

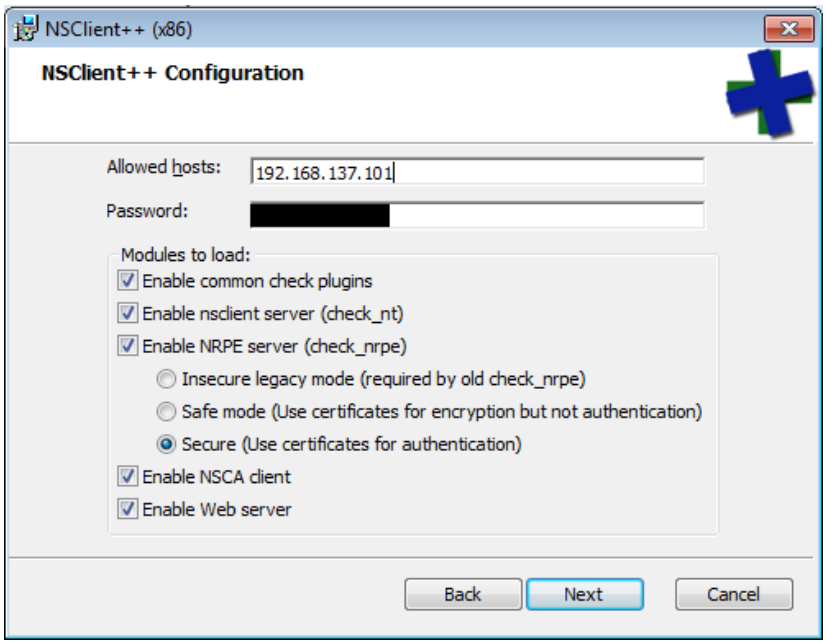


Figure A1.02 : L'attribution de l'adresse ip du serveur FAN sur NSClient++

A1.2 Démarrage du service SNMP, du service interruption SNMP, de NSClient++

Il faut démarrer le service SNMP, interruption SNMP et NSClient++ pour que la machine Windows puisse être surveillée. Pour cela, aller dans propriétés du service SNMP cela par l'exécution du programme « services.msc ». Sélectionner ensuite le service à démarrer puis cliquer sur démarrer le service.

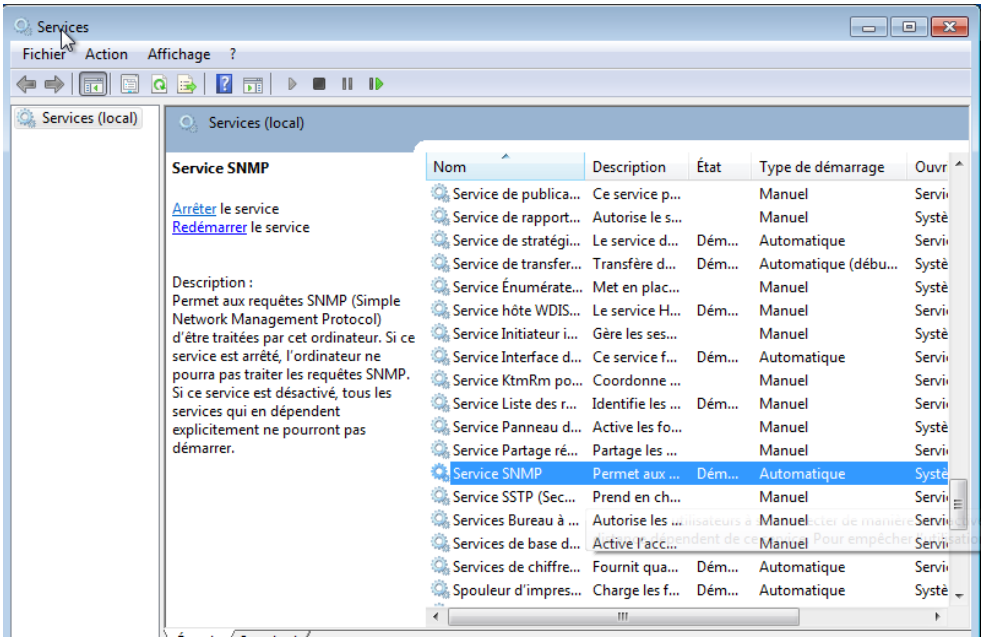


Figure A1.03 : démarrage du service SNMP

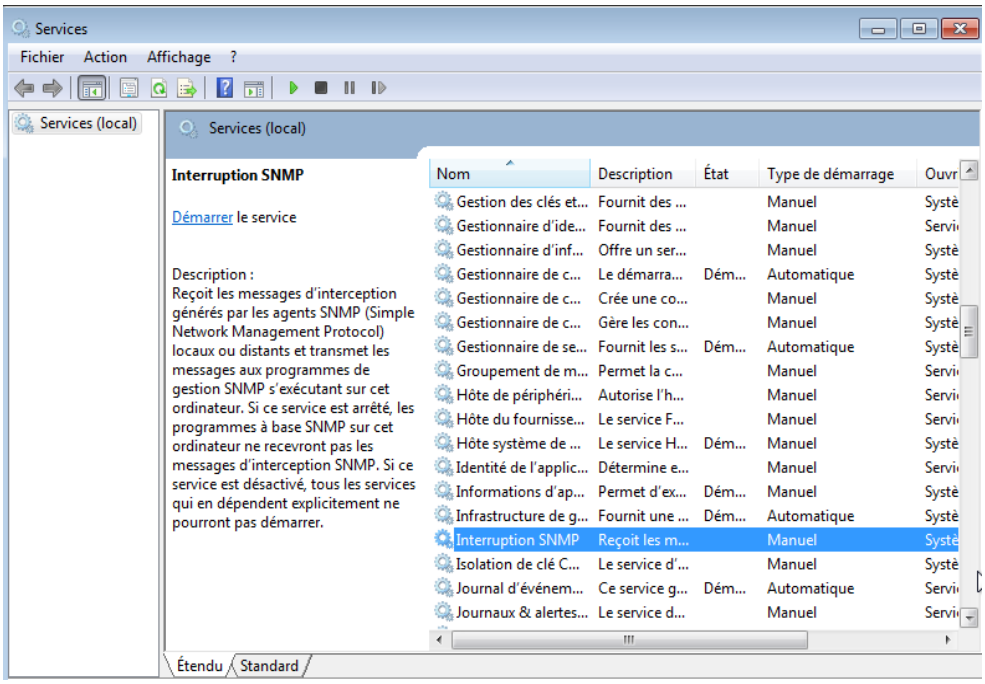


Figure A1.04 : Démarrage du service interruption SNMP

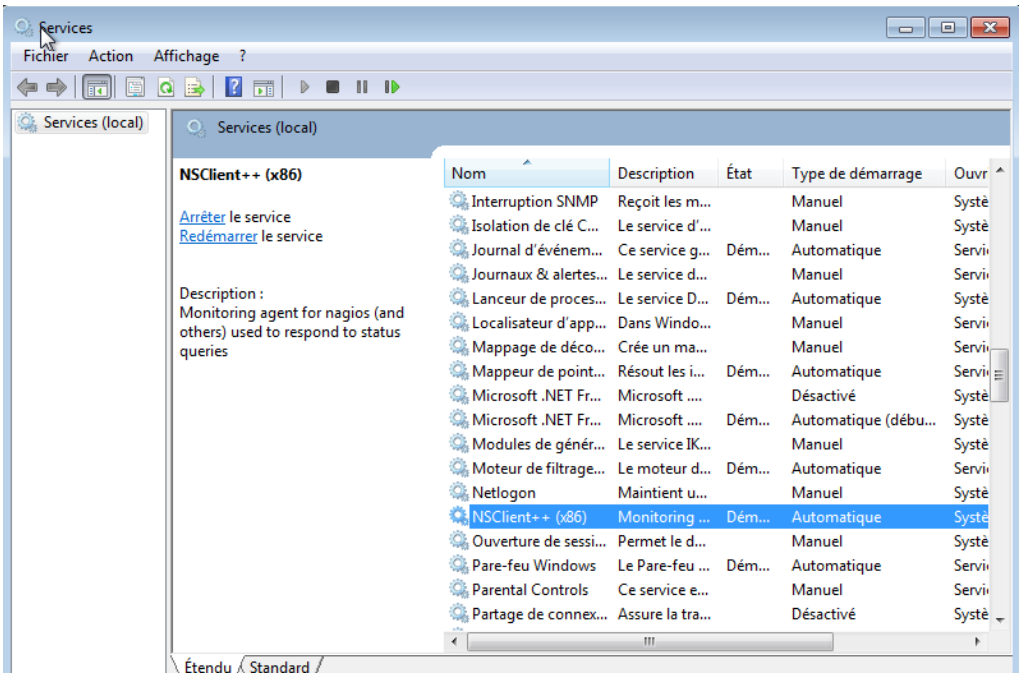


Figure A1.05 : Démarrage de NSClient++

La supervision ne peut se faire sans le démarrage de ces services dans l'hôte Windows à superviser.

En effet, SNMP permet aux requêtes d'être traités par l'ordinateur. Si ce service est alors arrêté, l'ordinateur ne pourra pas traiter les requêtes SNMP. Si ce service est désactivé, tous les services qui en dépendent ne pourront pas démarrer.

Quant à l'interruption SNMP, elle reçoit les messages d'interceptions générés par les agents SNMP locaux ou distants et transmet les messages aux programmes de gestion SNMP s'exécutant sur l'ordinateur. Si ce service est arrêté, les programmes à base SNMP sur l'ordinateur ne recevront pas les messages d'interception SNMP. Si ce service est désactivé, tous les services qui en dépendent explicitement ne pourront pas démarrer.

NSClient++ est un agent pour Nagios utilisé pour répondre les requêtes.

A1.3 Installation de NRPE sur Linux

Installer nagios-nrpe-server

```
apt-get install nagios-nrpe-server
```

Editer ensuite le fichier nrpe.cfg dans le dossier /etc/nagios

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

Trouver la ligne « allowed host »

```
allowed_hosts=127.0.0.1
```

Changer l'adresse IP 127.0.0.1 par l'adresse du serveur FAN

```
allowed_hosts=192.168.137.101
```

En bas du fichier de configuration, les commandes de check de NRPE sont dans le dossier /usr/lib/nagios/plugins. Les commandes sont personnalisables et l'ajout des check peuvent se faire en toute volonté. On peut modifier les check_users, les check_load, les check_disk, les check_zombie_procs, les check_total_procs, etc.

```
# The following examples use hardcoded command arguments...
command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -w 15,10,5 -c 30,25,20
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hda1
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
```

Dans notre cas, un essai pour le check d'espace disque utilisé par la partition sda1 en Gigabit sera envisagé. Pour cela, modifier la ligne de la capture précédente :

```
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hda1
```

Par :

```
command[check_sda1]=/usr/lib/nagios/plugins/check_disk -u GB -w 20% -c 10% -p /dev/sda1
```

Il ne reste qu'à enregistrer les modifications et relancer NRPE pour que les modifications soient prises en compte.

```
service nagios-nrpe-server restart
```

Annexe 2 : LISTE DE QUELQUES COMMANDES DANS FAN

Tableau A2.01 : Liste de quelques commandes pour la supervision système sur les hôtes dans FAN

Nom de service	Description du service	Commande	Ligne de commande	Description de la commande
Charge moyenne	Une moyenne de la charge système, une mesure de la quantité de travail que fait le système durant une période considérée.	Load	Check_load –w 1, 1,1 –c 2, 2,2	Permet de vérifier la charge moyenne sur les Unix. Un warning est levé pour une valeur de 1 et un critical pour 2.
RAM	Mémoire vive : à court terme, stocke des informations provisoires.	Mem	Check_mem pl –w 90 –c 95	Lève un warning des que la mémoire est utilisée à 90% et un critical à 95%.
SWAP	Espace d'échange servant à étendre la mémoire utilisable par un système d'exploitation, par une partition dédiée.	Swap	Check_swap –w 80% -c 50%	Si le swap est utilisé à plus de 20%, un warning est levé. S'il est supérieur à 50%, c'est un critical. Les seuils de check_swap sont exprimés en pourcentage.

DISQUE	Espace de stockage d'information	Disk	Check_disk –w 80 –c 90	Lève un warning des que la mémoire est utilisée à 80% et un critical à 90%
PROCESSEUR	Programme permettant d'exécuter des programmes écrits dans un langage donné	Cpu	Check_cpu –w 90 –c 95	Lève un warning des que la mémoire est utilisée à 90% et un critical à 95%
PROCESSUS	Programme en cours d'exécution par un ordinateur	Procs	$USER1$/check_procs –c $ARG1$ -w $ARG2$ –c $ARG3$	Le paramètre –C indique le nom du service et les paramètres –w et –c indiquent le nombre de processus requis pour déclencher une alerte warning et critical

Tableau A2.02 : Liste de quelques commandes pour la supervision réseau sur les hôtes dans FAN

Nom du service	**Description du service**	**Commande**	**Ligne de commande**	**Description de la commande**
LDAP	protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau.	Check_ldap	$USER1$/check_ldap –H $HOSTADDRESS$ -b $ARG1$	Elle prend comme argument le serveur à interroger avec –H et à la requête à effectuer avec -b

DNS	Service permettant d'établir une correspondance entre une adresse IP et un nom de domaine de trouver une info à partir de nom de domaine	Check_dns	$USER1$/check_dns –H $ARG1$ -s $HOSTADDRESS$	Elle prend en paramètre –H, l'enregistrement a récupérer, et –s, le serveur DNS interrogé
DHCP	permet à chaque station connectée au réseau d'obtenir sa configuration réseau (adresse IP, masque de sous-réseau, passerelle) qui est valable pendant un bail.	Check_dhcp	$USER1$/check_dhcp –s $HOSTADDRESS$ -i $ARG1$	Le paramètre –s permet de spécifier à la commande l'adresse du serveur dont on veut une réponse. Enfin, le paramètre –i permet de choisir l'interface réseau
http	Protocole permettant d'envoyer des pages web a un ordinateur équipé d'un navigateur	Check_http	$USER1$/check_http –H $HOSTADDRESS$	Elle prend comme argument l'adresse du service à tester par le paramètre -H
HTTPS	Combinaison de http avec une couche de chiffrement SSL ou TLS. Service de vérification d'un site	Check_https	$USER1$/check_http –H $HOSTADDRESS$ -S	Elle prend comme argument l'adresse du service à tester par le paramètre -H

FTP	Permettant le transfert de fichiers entre deux machines sur un réseau TCP/IP	Check_ftp	$USER1$/check_ftp –H $HOSTADDRESS$	Elle prend comme argument l'adresse du service à tester par le paramètre -H
SMTP	Permettant un utilisateur d'envoyer un message a un ordinateur connecté sur TCP/IP	Check_smtp	$USER1$/check_smtp –H $HOSTADDRESS$	Elle prend comme argument l'adresse du service à tester par le paramètre -H
POP	Protocole de récupération de courrier électronique sur un serveur de messagerie	Check_pop	$USER1$/check_pop –H $HOSTADDRESS$	Elle prend comme argument l'adresse du service à tester par le paramètre –H
IMAP	Service de lecture et de manipulation des messages comme s'ils étaient stockés localement sur le périphérique	Check_imap	$USER1$/check_imap –H $HOSTADDRESS$	Elle prend comme argument l'adresse du service à tester par le paramètre –H

Une commande est la définition d'une ligne de commande qui utilise un script ou une application afin de réaliser une action. Il est possible d'exécuter cette commande en précisant des arguments.

Il existe trois types de commandes :

- Les commandes de vérification : utilisées par les ordonnanceurs afin de vérifier le statut d'un hôte ou d'un service.
- Les commandes de notification : utilisées par les ordonnanceurs pour alerter les contacts (via mail, SMS...).
- Des commandes diverses: utilisées par les modules complémentaires (pour effectuer certaines actions), par l'ordonnanceur pour le traitement des données...

Toutes les commandes peuvent être configurées au sein du menu Configuration ==> Commandes.

Les champs de configuration pour une commande sont :

- Le champ Nom de la commande qui définit le nom de la commande.
- Le champ Type de commande qui permet de choisir le type de commande.
- Le champ Ligne de commande qui indique l'application ou le script utilisé avec la commande.
- Le bouton Effacer les arguments efface la description des arguments définie. La description des arguments est modifiable.
- Les champs Exemple d'arguments et $HOSTADDRESS$ définissent respectivement des exemples d'arguments (chaque argument commence par un "!") et une adresse IP de test.
- Le bouton Description des arguments permet d'ajouter une description aux arguments de type "$ARGn$". Cette description sera visible lors de l'utilisation de la commande dans un formulaire d'hôte ou de service.
- Le bouton Description des macros permet d'ajouter une description aux macros personnalisées. Ces descriptions seront visibles lors de l'ajout de la commande sur un host ou un service.

Arguments et macros

Au sein du champ Ligne de commande, il est possible de faire appel à des macros ainsi qu'à des arguments.

Une macro est une variable permettant de récupérer certaines valeurs. Une macro commence et se termine toujours par le signe "$".On distingue 2 types de macros :

- Les macros standards : ce sont des macros prédéfinies dans le code source des moteurs de supervision. Ces différentes macros permettent de récupérer la valeur de différents objets au sein des commandes. Par exemple : la macro $HOSTADDRESS$ permet de récupérer l'adresse IP d'un hôte, la macro $CONTACTEMAIL$ permet de récupérer l'adresse mail du contact
- Les macros personnalisées : ce sont des macros définies par l'utilisateur lors de la création d'un hôte ou d'un service. Elles sont utilisées dans les commandes de vérifications. Les macros personnalisées commencent par $_HOST pour les macros personnalisées d'hôtes et par $_SERVICE pour les macros personnalisées de services. Il y a plusieurs avantages à utiliser les macros personnalisées à la place des arguments : La

fonction de la macro est définie dans le nom de celle-ci. La macro $_HOSTMOTDEPASSEINTRANET$ est plus facilement lisible que $ARG1$

Les macros héritent des modèles d'hôtes et de services, la modification d'une seule macro est donc possible pour un hôte ou un service. En revanche, les arguments doivent être tous redéfinis en cas de modification d'un seul argument.

Le nombre d'arguments est limité à 32 contrairement aux macros personnalisées qui sont infinies

Une macro d'hôte est utilisée pour définir une variable qui est propre à l'hôte et qui ne changera pas qu'importe le service interrogé : des identifiants de connexion à l'hôte, un port de connexion pour un service particulier, une communauté SNMP.

Une macro de service est plutôt utilisée pour définir des paramètres propres à un service : un seuil WARNING/CRITICAL, une partition à interroger, etc...

Pour faire appel à ces macros dans une commande de vérification, il faudra les invoquer en utilisant les variables suivantes : $_HOSTUSERLOGIN$, $_HOSTUSERPASSWORD$.

Les arguments sont utilisés afin de pouvoir passer différents paramètres aux scripts appelés par les commandes. Lors de l'exécution de la commande par l'ordonnanceur, chacun des arguments et macros sont remplacés par leur valeur respective. Chaque argument se présente sous la forme $ARGn$ où n est un entier naturel supérieur à 0.

Exemple de ligne de commande utilisant les arguments : $USER1$/check-bench-process-DB -w $ARG1$ -c $ARG2$ -n $ARG3

En effet, il est nécessaire de comprendre ces commandes pour pouvoir personnaliser le type de supervision voulu.

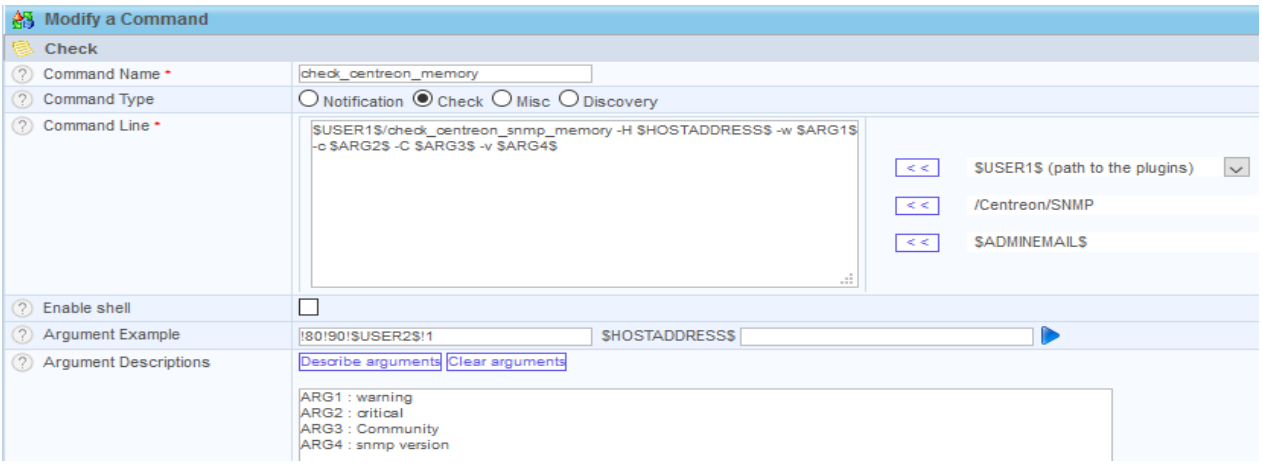


Figure A2.01 : Exemple d'ajout de commande

REFERENCES

[1.01] https://www.wixxim.fr/fiches/le-reseau-local-lan, Janvier 2019.

[1.02] P. Descartes, *« Introduction aux réseaux de télécommunications »*, cours L3, 2006.

[1.03] https://repo.zenksecurity.com/supports/caracteristiques_des_supports_de_transmission.pdf, Janvier 2019.

[1.04] G. Pujolle, «*Réseaux et Télécoms »*, Cours, 3eme Edition Eyrolles, 2008.

[1.05] G. Pujolle, *« Initiation aux réseaux,»*, Cours et exercices, édition Eyrolles 2001, Paris 2001.

[1.06] http://www.mi.parisdescartes.fr/~mea/cours/L3/4_L3_interconnexion.pdf, Janvier 2019.

[1.07] C. Leider et M. Wilensky, *« TCP/IP pour les nuls »*, édition Sybex, 1994.

[1.08] R. Guichard, «Apprenez le fonctionnement des réseaux TCP/IP *»*, 3eme édition Eyrolles, 2013.

[1.09] A. Tanenbum et D. Wetherall, *« Réseaux »*, 5eme édition, 2016.

[1.10] Guy Pujolle *« Les réseaux »*, Edition 2008, 6eme édition Eyrolles, Paris 2008.

[1.11] D. Domard et D. Seret, «*Architecture des réseau »*, Synthèse de cours, Paris 2009.

[1.12] C. Servin, «*Réseaux et Télécoms »*, cours et exercices corrigés, Dunod, Paris 2003.

[2.01] http://www.o00o.org/monitoring/bases.html, Janvier 2019.

[2.02] https://bencherifcheikh.wordpress.com/2012/08/08/le-protocole-snmp/, Janvier 2019.

[2.03] http://www.frameip.com/snmp/, Janvier 2019.

[2.04] http://ram-0000.developpez.com/tutoriels/reseau/SNMP/, Janvier 2019.

[2.05] http://www.frameip.com/snmp/, Janvier 2019.

[2.06] F. Pignet, « *Réseaux Informatiques, Supervision et Administration* », Collection Expert IT, Edition ENI, janvier 2016.

[2.07] W. Satllings, *« SNMP, SNMPv2, SNMPv3 and RMON 1and 2 »,* 3eme édition, décembre 1998, Amérique.

[2.08] L. Walsh, *« SNMP MIB Handbook: Essential guide to MIB development, use and diagnosis »*, 20 Mars 2008.

[2.09] https://www.novel.com/global/latvia/events/2014/29_13_45.zabbix.pdf, Mars 2019.

[2.10] A. Madjoub, *« Nagios, la clé de la supervision informatique »,* Collection Epsilon, Nouvelle Edition, Janvier 2016.

[3.01] http://www.fullyautomatednagios.org/documentation/FAN_Documentation_FR_v2.1-1.pdf, Mars 2019.

[3.02] http://www.fullyautomatednagios.org/documentation, mars 2019.

[3.03] J. Gabes, «*Nagios 3 pour la supervision et la métrologie*», édition Eyrolles, Paris, 2009.

[3.04] M. Maslac, *« Oracle VM Virtualbox for Complete Beginners »,* Geek University Press, 2016.

[3.05] http://www.monpensebete.org/Fiche-réseau-virtualbox.pdf, février 2019.

[3.06] https://www.alsacreations.com/tuto/lire/614-Serveur-mail-Postfix.html, Janvier 2019.

[3.07] L. Fontaine et B. Legros, *« Centreon, maitrisez la supervision de votre systeme d'Information »*, 2eme édition, 2016.

[3.08] https://documentation-fr.centreon.com/docs/centreon/fr/latest/exploitation_guide/04realtime.html, mars 2019.

[3.09] http://www.wiki-monitoring-fr.org/Manuel-d-utilisation-de-Nagvis.html, février 2019.

[3.10] http://www.wiki-monitoring-fr.org/Centreon18.10.2/documentation.html, février 2019.

FICHE DE RENSEIGNEMENTS

Nom : RAMANGASALAMA

Prénoms : Tahiana Hortensia

Adresse de l'auteur : lot 15-C-20 Est Sabotsy Antsirabe 110

Téléphone : +261 34 35 917 48

E-mail : hortensiaramangasalama@gmail.com

Titre du mémoire : ETUDES ET MISE EN PLACE D'UNE SOLUTION DE SUPERVISION RÉSEAU ET SYSTEME (CAS DE L'INSTAT)

Nombre de pages : 65

Nombre de tableaux : 7

Nombre de figures : 46

Directeur de mémoire : RAKOTONDRAMANANA Radiarisainana Sitraka

Titre : DEA en Télécommunication

Téléphone : +261 34 46 363 87

Mail : radiarisainanasitraka@yahoo.fr

FAMINTINANA

Ankehitriny dia maro ireo vokatry ny fivoaran' ny teknolojia indrindra ny eo amin'ny sehatry ny fifandraisana. Ireny fitaovana na teknolojia ampiasaina entina ifandraisana ireny anefa dia matetika misedra olana sy fahasimbana, indrindra ireo ampiasaina any amin'ny sehatry ny asa. Manoloana izany ary dia teraka ny hetaheta ny mba ahafahana manara maso azy ireny mba isorohana aingana ny olana sy ny fahasimban'izy ireny. Misy arak'izany ny karazana fitaovana entina manara maso, ao ny andoavam-bola, ao ny maimaim-poana sy « Open-source ». Fully Automated Nagios, fitaovana maimaim-poana sy « Open Source » entina anaraha maso iray no nohezahina napetraka sy nohadihadiana ato anatin'ity boky ity. Vokatr'izany, nohalalina misimisy kokoa ny toetoetry ny tambazotra, ny fomba fiasan'ny fitaovana entina manara maso ny tambazotra, ireo fitsipika sy karazana fomba entina anaraha-maso ary koa ireo paika arahina raha te-hametraka izany fitaovana entina anaraha-maso ny tambazotra sy ny solosaina izany.

Teny misongadina : fanaraha-maso, tambazotra, solosaina.

RESUME

De nos jours, nombreux sont les fruits de l'évolution technologique surtout les technologies d'information et de communication, le réseau informatique. Dans les lieux de travail, ces technologies d'information et de communication, voire le système d'information sont souvent théâtres d'incident et de problèmes. Face à cela, le concept de la supervision est né afin d'éviter les pannes futures. Pour pouvoir superviser l'état du réseau, plusieurs outils ont été développés par les chercheurs, des outils payants ou gratuits et libres. Dans ce contexte, l'étude et la mise en place d'un logiciel libre de supervision Fully Automated Nagios a été entreprise afin d'avoir des connaissances sur la supervision. De ce fait, ce livre résume les caractéristiques des réseaux informatiques, le fonctionnement et les méthodes de la supervision, les protocoles et les étapes à suivre pour appliquer la supervision réseau et système.

Mots clés : supervision, réseau, ordinateurs, système.

ABSTRACT

Nowadays, many are the fruits of the technological evolution especially in the communication and the computer network. In the workplace, these communication technologies and even the information system are often theaters of incident and problem. Faced with this, the concept of supervision was born in order to avoid future failures. To be able to supervise the state of the network, several tools have been developed by the researchers, tools paid or free. In this context, the study and implementation of a Fully Automated Nagios supervision software was undertaken in order to have knowledge on supervision. As a result, this book summarizes the characteristics of computer networks, the operation and methods of supervision, the protocols and the steps to follow in network and system supervision.

Keywords: supervision, network, computer, system.