République Algérienne Démocratique et Populaire Ministère
de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA
Faculté des Sciences exactes
Département Informatique

Mémoire de fin de cycle

En vue de l'obtention du
Diplôme de Master professionnel en Informatique
Option: Administration et sécurité des réseaux

Thème

La mise en place d'un système de supervision réseau Cas : INSIM Bejaia

Encadreur : Dr Zidani Ferroudja

Co-Encadrant : Mr Bouiche kheireddine

Présenté par :
Mlle Akkou Rima

Devant le jury composé de :

Présidente Dr Bachiri Lina
Examinatrice Mme Rebouh Nadjette

Année Universitaire : 2020-2021

Remerciements

Avant d'entamer ce mémoire, il m'est agréable de témoigner de ma grande gratitude, ma forte reconnaissance et mon profond sentiment de respect à l'honorable de mes encadreurs Mlle. Rebouh Nadjette et et Mr. Bouiche kheireddine pour leurs pertinentes recommandations, leurs précieux conseils et leur suivi continuel tout le long de l'élaboration de cette recherche.

Je salue, en termes de ma haute considération, leurs passion de recherche et leur engouement pour les études. Enfin, je reste reconnaissant à tous ceux qui ont aidé à la bonne conduite du présent mémoire.

Dédicaces

Avant tout, je remercie le grand Dieu, qui nous a aidé à élaborer ce modeste travail.Je dédie ce modeste travail :

A l'âme de mon père.

A ma mère .

A mes frères et mes sœurs Sofiane , Souhila, Walid, Samia,Imane.Naziha.

A ma belle-sœur Imane et ses deux chères filles Eline et Sila.

A mes beaux-frères Ali,Norddine,Lamine,Mohamed al-Cherife.

A mes onclse et mes tantes et cousin(e)s.

A mes chers cousin(e)s : Da farid , Hanane,Allaoua,Youba et Leila.

A toute la famille Akkou et Sekhri sans exception.

A Mes amies Siham,Nesrine,Facila,Rayane,Adada

A tous ceux que j'aime, à tous ceux qui m'aiment et tous ceux qui me sont chers.

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

A tous ceux qui m'ont aidé durant ma vie universitaire.

Rima

Table des matière

Table des figures

Liste des tableaux

Glossaire

A

AD : Active Directory.

ADSL : Asymmetric Digital Subscriber Line.

ARP : Address Resolution Protocol.

C

CATV : Community Antenna Television.

CGI : Compagnie générale immobilière.

Cisco : Challenge Handshake Authentification Protocol.

CPU : central processing unit.

D

DHCP : Dynamic Host Configuration Protocol.

DNS : Domain Name Server.

E

ERP : Enterprise resource planning.

F

FAI : Fournisseur d'Accès à l'Internet.

FDDI : Fibre Distributed Data Interface.

FQDN : fully qualified domain name .

G

GBic : Gigabit interface Converter .

H

HDD : Hard Disk Drive .

HTTP : Hypertext Transfer Protocol.

I

IBM : International Business Machines.

ICMP : Internet Control Message Protocol.

IETF : Internet Engineering Task Force.

INSIM : Institut International de Management.

IP : Internet Protocol.

IRC : Internet Relay Chat .

L

LAN : Local Area Network.

LLC : Logical Link Control.

M

MAC : Media Access Control.

MAN : Métropolitain Area Network.

MAP : Mobile Application Part.

MIB : Management Information Base.

MPLS : Multi-Protocol Label Switching.

MTA : Mail Transport Agent .

N

NAS : Network Attached Storage.

NCM : Network Connectivity Monitor.

NCSA : National Center for Supercomputing Applications.

NRPE : Nagios Remote Plugin Executor.

O

OS : Operating System .

OSI : Open Systems Interconnexion.

OVA : Open Virtual Appliance.

P

PC : Personal Computer.

PHP : Hypertext Preprocessor.

PING : Packet INternet Groper.

PME : Petite ou moyenne Entreprise.

PNG : Portable Network Graphics.

R

RAID : Redundant Array of Independent Disks.

RAM : Random Access Memory.

RRD : Round Robin Database.

S

SMS : Short Message Service.

SMTP : Simple Mail Transfer Protocol.

SNMP : Simple Network Management Protocol.

SQL : Structured Query Language.

STP : Shielded Twisted-Pair.

T

TCP : Transmission Control Protocol.

U

UDP : User Datagram Protocol.

URL : Uniform Resource Locator.

UTP : UnShielded Twisted-Pair.

V

VLAN : Virtual Local Area Network.

VM : Virtuel Machines.

VPN : Virtuel Private Network.

W

WAN : Wide Area Network.

Web : World Wide Web.

WiFi : Wireless Fidelity.

X

XML : Extensible Markup Language.

Introduction générale

Actuellement, les systèmes informatiques dans les entreprises deviennent de plus en plus importants mais aussi complexes. Le besoin de maintenance et de gestion de ces systèmes est rapidement devenu une priorité, d'autant plus qu'une panne ou une perte au niveau de ce système pourrait parfois avoir des conséquences catastrophiques.

Afin de minimiser le nombre de ces pertes, une surveillance et un contrôle s'avèrent indispensable. La notion de « supervision informatique » est apparue et est devenue une tâche vitale pour tout système informatique ; c'est pourquoi les administrateurs systèmes/réseaux font appel à des logiciels de surveillance et de supervision. Ces logiciels vérifient l'état du système ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel sur l'ensemble du parc informatique sous sa responsabilité. Il peut être, aussi, alerté (par email, par SMS, etc.) en cas de problème. Grâce à un tel système, les délais d'interventions sont fortement réduits, sans que les utilisateurs du système en question soient affectés ou se rendent compte des problèmes survenus.

A cet effet, j'ai effectué un stage de cinq mois à L'INSIM Bejaia. Mon objectif consistera à mettre en place une console d'administration réseaux dans le but de garantir le bon fonctionnement de leur infrastructure. Ce manuscrit, illustrant tout le travail que j'ai effectué au cours de ce stage, fait office de rapport de mon projet et est structuré en trois chapitres, précédé d'une introduction générale et clôturé par une conclusion générale.

Dans le premier chapitre , je présenterai des généralités sur les réseaux informatiques, les composants du système informatique d'entreprise et l'organisme d'accueil et le cadre de mon projet.

Le second chapitre portera sur tout ce qui concerne la supervision des réseaux informatiques clôturé par une étude comparative des outils existants qui m'aidera à choisir l'outil approprié à mettre en place pour mon projet.

Le dernier chapitre sera consacré à la mise en place de l'outil de supervision au niveau de l'INSIM Béjaia et la présentation des résultats.

Chapitre I

CHAPITRE Domaine d'étude

I.1 Introduction

Nous présenterons dans ce chapitre, d'abord, des généralités sur les réseaux informatiques, définir ce qu'est un réseau informatique, présenter ses différents composants, les différentes topologies qu'il peut prendre (logiquement ou physiquement), ses différents types par rapport à la distance qui sépare les composants. Nous parlerons par la suite de tout ce qui est utilisé (installations et protocoles) pour répondre aux besoins des utilisateurs en termes de services .Enfin on va mettre notre travail dans son contexte général. Tout d'abord, nous commencerons par faire une présentation de l'organisme d'accueil INSIM Bejaia où nous avons effectué notre stage, ensuite nous présenterons l'objectif de ce projet en détaillant son cadre et ses fonctionnalités.

Partie I : généralités sur les réseaux informatiques

I.2 Réseau informatique

Un réseau informatique est un ensemble d'équipements électroniques (ordinateurs, imprimantes, scanners, modems, routeurs, commutateurs, etc.) interconnectés entre eux physiquement ou grâce à des ondes radio dans le but d'échange d'information (messageries, transfert de fichiers, interrogation de bases de données, etc.). Grâce à un réseau informatique, les utilisateurs peuvent partager entre eux des données et des applications, les sécuriser, communiquer, et accéder à Internet **[1]**.

I.3 Équipements d'un réseau informatique

Les équipements d'un réseau informatique sont les composants matériels et/ou logiciels nécessaires pour connecter un périphérique à un réseau ou pour connecter un réseau à un autre. On peut les classer en deux groupes **[2]** :

I.3.1 Équipements de base

Les principaux équipements de bases nécessaires pour la mise en place d'un réseau sont, de la plus simple entité jusqu'à la plus importante :

A. **Câbles réseaux**

Un câble est le support par lequel l'information passe généralement d'un périphérique réseau à un autre. Il existe plusieurs types de câbles couramment utilisés avec les réseaux locaux :

1. **Paire torsadée**

Une paire torsadée dans sa forme la plus simple (figure I.1) est constituée de deux brins torsadés en cuivre, protégés chacun par une enveloppe isolante. Il existe plusieurs types de paires torsadées **[3]** :

- Câble à paire torsadée **non blindée** UTP .
- Câble à paire torsadée **blindée** STP .

FIGURE I.1 – Paire torsadée.

2. **Câble coaxial**

Un câble coaxial(figure I.2) est constitué de deux conducteurs cylindriques de même axe, l'âme et la tresse, séparées par un isolant. Ce dernier permet de limiter les perturbations dues aux bruits externes. Si le bruit est important, un blindage peut être ajouté. Quoiqu'il perde du terrain, notamment par rapport à la fibre optique, ce support reste encore très utilisé **[4]**.

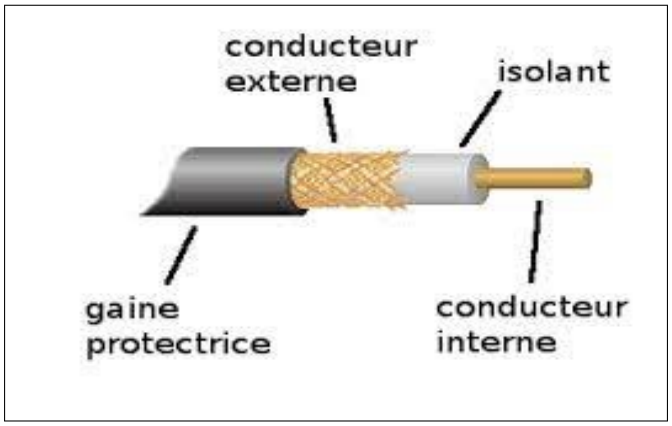


FIGURE I.2 – Câble coaxial.

Les catégories suivantes existent sur les marchés :

- Câbles de type Ethernet,
- Câbles RG-59/U ohms de type CATV (câble de télévision),
- Câble RG-62/U 93 ohms de type IBM,
- Gros coaxial (Thick) RG-11 de couleur jaune lié au protocole Ethernet 10 base 5.

3. **Fibre optique**

C'est un conducteur d'ondes lumineuses. Elle est constituée d'un cœur et d'une gaine optique (figure I.3). Un revêtement primaire assure la tenue mécanique de la fibre et évite les fractures en cas de courbure. Le principe d'isolation totale de la fibre optique permet une réflexion totale des ondes lumineuses entre cœur et gaine. La lumière se propage sans perdition au cœur de la fibre. La fibre requiert à ses extrémités un émetteur de lumière, une diode ou un laser détecteur de lumière **[4]**.

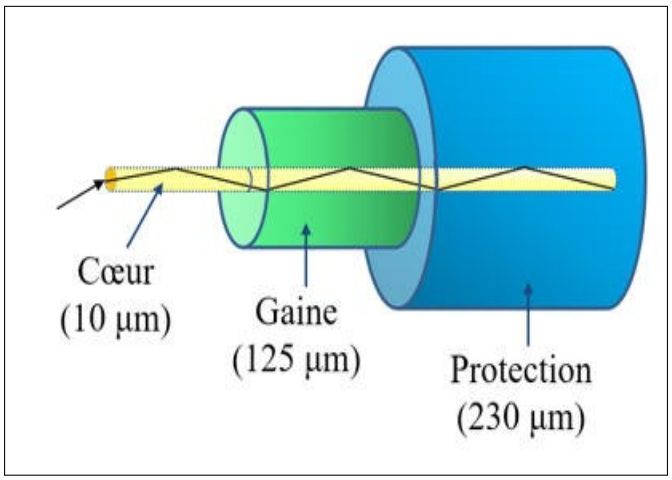


FIGURE I.3 – Fibre optique .

La fibre optique a les caractéristiques suivantes :

- Bande passante élevée,
- Insensibilité aux parasites électriques et magnétiques,
- Faible encombrement et poids,
- Atténuation très faible,
- Vitesse de propagation élevée (en monomode),
- Sécurité,
- Légèreté.

B. **Serveurs (Computing)**

Un serveur informatique offre des services accessibles via un réseau. Il peut être matériel ou logiciel et offre des services à un ou plusieurs clients (parfois des milliers). Les services les plus courants sont :

- Accès aux informations du World Wide Web .
- Courrier électronique .
- Commerce électronique .
- Stockage en base de données .
- Gestion de l'authentification et du contrôle d'accès .
- etc.

Un serveur fonctionne en permanence en répondant automatiquement à des requêtes provenant des autres dispositifs informatiques (les clients) selon le principe du client-serveur. Le format des requêtes et des résultats est normalisé. Il se conforme à des protocoles réseaux. Chaque service du réseau peut être exploité par tout client qui met en œuvre le protocole propre à ce service. Les serveurs sont utilisés par les entreprises, les institutions et les opérateurs de télécommunication. Ils sont courants dans les centres de traitement de données et le réseau Internet **[5]**.

1. **Machine Physique**

Un serveur physique **[6]** (figure I.4), couramment appelé serveur dédié, est un serveur sur lequel on installe généralement un seul système d'exploitation pour gérer une application bien spécifique. C'est un serveur réservé à un usage personnel. L'applicatif, s'exécutant sur ce serveur, dispose de toutes les ressources de la machine. Ainsi, cette applicatif a accès au système d'exploitation, à la mémoire vive, à la capacité de stockage, à la bande passante et à bien d'autres paramètres.

Ce type de serveur permet aussi la centralisation de la gestion de tout le parc informatique d'une entreprise.

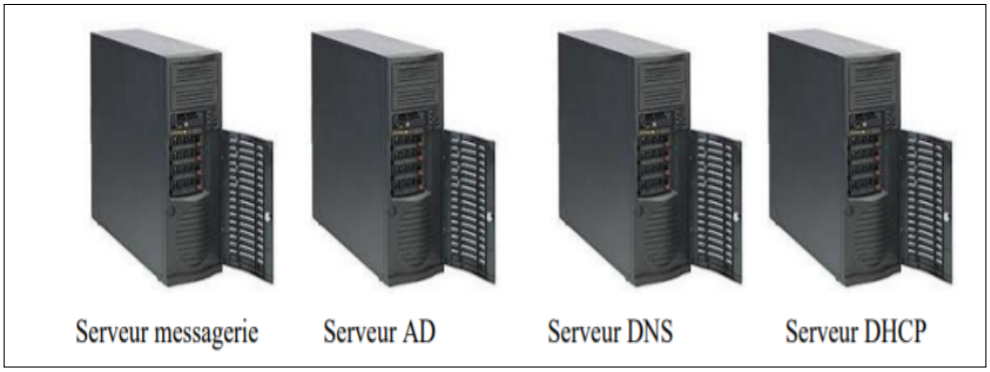


FIGURE I.4 – Machine physique .

2. **Machine virtuelle**

Au cours des dernières années, les avancées technologiques dans le domaine du matériel serveur ont largement devancé les besoins des logiciels exécutés. Le rythme des innovations dans le domaine des serveurs obéit à la loi de Moore(sont des lois empiriques qui ont trait à l'évolution de la puissance de calcul des ordinateurs et de la complexité du matériel informatique), tandis que les besoins des applications exécutées sur ces serveurs augmentent modérément d'une année à l'autre. Le taux d'utilisation des serveurs qui exécutent un système d'exploitation et une pile d'applications directement sur le matériel est généralement inférieur à 15%. Les applications courantes, n'exigeant que peu de ressources telles que des fichiers, des impressions, etc., se trouvent souvent soit sur du matériel ancien et obsolète soit sur de nouveaux serveurs neufs, bien plus puissants que nécessaire. Comment les administrateurs informatiques peuvent-ils récupérer

ce surplus de capacités ? C'est avec les solutions de virtualisation qu'on peut exploiter les ressources d'une machine physique au maximum.

La virtualisation permet d'exécuter plusieurs systèmes d'exploitation sur un même ordinateur. Il faut d'abord installer un système d'exploitation spécial (nommé hyperviseur) directement sur le matériel brut puis installer les systèmes d'exploitation virtuels sur cet hyperviseur. Ces instances de systèmes d'exploitation s'appellent machines virtuelles (VM). Une seule machine physique peut en comprendre plusieurs dizaines, voire plusieurs centaines.

- **Principe de fonctionnement :**

Chaque Système d'exploitation se voit attribuer sa propre part de ressources physiques isolées par un séparateur logique des autres ressources disponibles sur la machine invitée. Cette séparation des ressources est la tâche principale de l'hyperviseur, en plus de l'intégration des services de mise en cluster, de sauvegarde et d'autres ressources permettant l'existence d'hôtes multiples. Les hyperviseurs les plus populaires actuellement sont fabriqués par Microsoft (Hyper-V), VMware (vSphere) et Citrix (XenServer), Proxmox, ou encore Oracle Virtualbox **[7]**. La figure 2. est un exemple de virtualisation avec un hôte physique unique exécutant quatre systèmes d'exploitation, chacun comprenant sa propre pile d'applications.

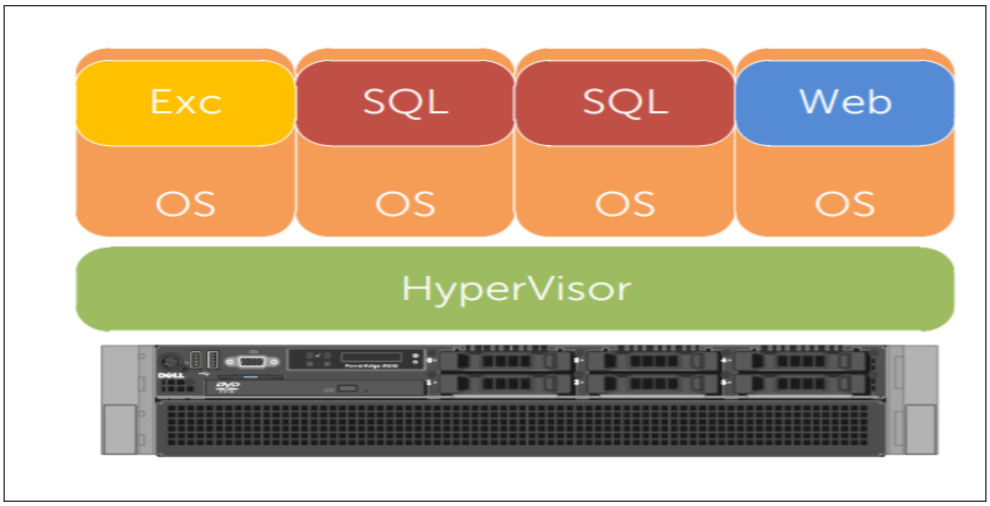


FIGURE I.5 – Machine virtuelle .

3. **Système de fonctionnement /métier**

Le système informatique a besoin, pour son fonctionnement, d'une part à des systèmes de base tels que l'Active Directory (AD), Messagerie, DNS, DHCP, etc. D'autre part à des systèmes métiers qui sont spécifiques au métier de l'entreprise. Par exemple, une entreprise qui exerce dans le domaine de la formation a besoin d'un système de gestion de pédagogie tandis qu'une autre qui fait de la commercialisation a besoin d'un système de facturation.

I.3.2 Equipements d'interconnexion

Un équipement d'interconnexion est un matériel qui permet de relier les ordinateurs d'un réseau ou plusieurs réseaux entre eux. Il existe plusieurs équipements d'interconnexion **[8]** :

- **Concentrateur (Hub)**

  Le Hub (figure I.6) est un dispositif permettant la connexion de plusieurs nœuds à un même point d'accès sur le réseau, en se partageant la bande passante totale. C'est le fameux point central utilisé pour le raccordement des différents ordinateurs dans un réseau de topologie physique en étoile. Le Hub ne fait que renvoyer bêtement les trames vers tous les périphériques connectés. Au contraire, il ne garde pas en mémoire les adresses des destinataires dans une table. Il n'est pas conçu pour décoder l'entête du paquet pour y trouver l'adresse MAC du destinataire. La mise en place d'un Hub surcharge donc le réseau en renvoyant toutes les trames à l'ensemble des machines connectées .

FIGURE I.6 – Hub .

- **Commutateur (Switch)**

  Un commutateur (figure I.7) est un équipement qui relie plusieurs segments (câble ou fibre) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports entre 4 et 100. Il a donc la même apparence qu'un concentrateur.

  Contrairement à un Hub, un Switch ne se contente pas de reproduire sur tous les ports chaque trame qu'il reçoit. Il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Le Switch est souvent utilisée pour remplacer des concentrateurs.

FIGURE I.7 – Commutateur .

- **Routeur**

  Un routeur (figure I.8) est un équipement d'interconnexion de réseau informatique permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

  Il dispose souvent des ports RJ45 pour la connexion avec une Switch ou avec un PC. Il peut avoir des antennes pour le réseau sans fil.

FIGURE I.8 – Routeur .

- **Passerelle**

  Une passerelle (figure I.9) est un dispositif permettant de relier deux réseaux informatiques différents, comme par exemple un réseau local et l'Internet. Ainsi, plusieurs ordinateurs ou l'ensemble du réseau local peuvent accéder à l'Internet par l'intermédiaire de la passerelle. Le plus souvent, elle sert aussi de pare-feu, ce qui permet de contrôler tous les transferts de données entre le local et l'extérieur **[2]**.

FIGURE I.9 – Passerelle .

I.4 Classification des réseaux informatiques

Un réseau est constitué d'équipement appelées nœuds .En fonction de leur étendue et de leur domaine d'applications (figure I.10), ces réseaux sont classifiés en :

I.4.1 Classification selon l'étendue géographique

On a

A. **les réseaux locaux (LAN) :** De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le local Area Network (LAN) , en français réseau local d'entreprise est une infrastructure de communications reliant des équipements informatiques variés, sur une aire géographique limitée, dans le but de partager des ressources communes.

B. **les réseaux métropolitains(MAN) :** Le réseau métropolitain, ou Métropolitain Area Network (MAN), est également nommé réseau fédérateur .Il assure des communications sur des plus longues distances, interconnectant souvent plusieurs réseaux LAN.

C. **Les réseaux étendus(WAN) :** Les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN (Wide Area Network), le plus célèbre est le réseau public internet, dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux**[9]**.

FIGURE I.10 – Types de réseaux avec fil .

I.4.2 Classification selon l'architecture

Il existe deux types d'architecture de réseaux : Architecture Client/serveur et architecture poste à poste.

A. **Architecture Client/serveur**

L'architecture client/serveur (figure I.11) désigne un modèle de communication entre plusieurs ordinateurs d'un réseau. Elle distingue plusieurs postes clients qui communiquent avec un serveur (une machine généralement très puissante en termes de capacités d'entrée/sortie) qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, des connexions, etc. Les services sont exploités par des programmes appelés programmes clients s'exécutant sur les machines clientes **[10]**.

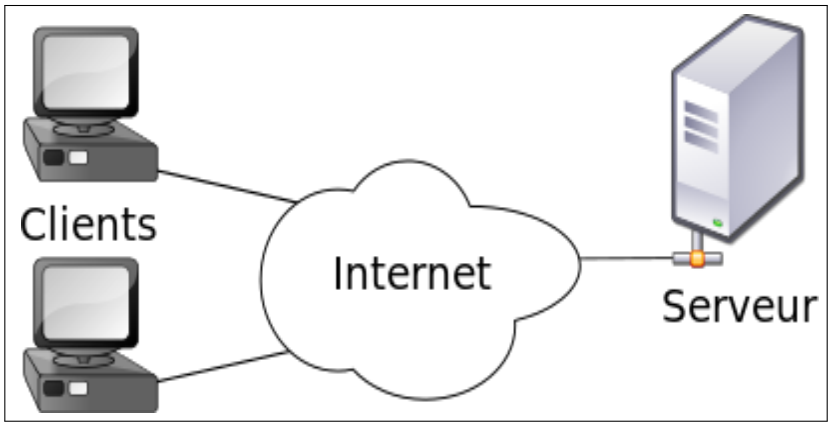


FIGURE I.11 – Architecture client/serveur .

1. **Avantages de l'architecture client/serveur**

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité. Ses principaux atouts sont **[6]** :

- **Ressources centralisées :** Étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée afin d'éviter les problèmes de redondance et de contradiction .
- **Meilleure sécurité :** Car le nombre de points d'entrée permettant l'accès aux données est moins important.
- **Administration au niveau serveur :** Les clients ayant peu d'importance dans ce modèle ont moins besoin d'être administrés.
- **Réseau évolutif :** Grâce à cette architecture, il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure.

2. **Inconvénients de l'architecture client/serveur**

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles, on peut citer **[6]** :

- **Coût élevé :** dû à la technicité du serveur.
- **Maillon faible :** Le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui. Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID [1]).

1. Le RAID est un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes.

B. **Architecture poste à poste (égal à égal)**

Inversement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi, chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela indique notamment que chacun des ordinateurs du réseau est libre de partager ses ressources. Les réseaux poste à poste (figure I.12) ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés.

Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part, tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent.

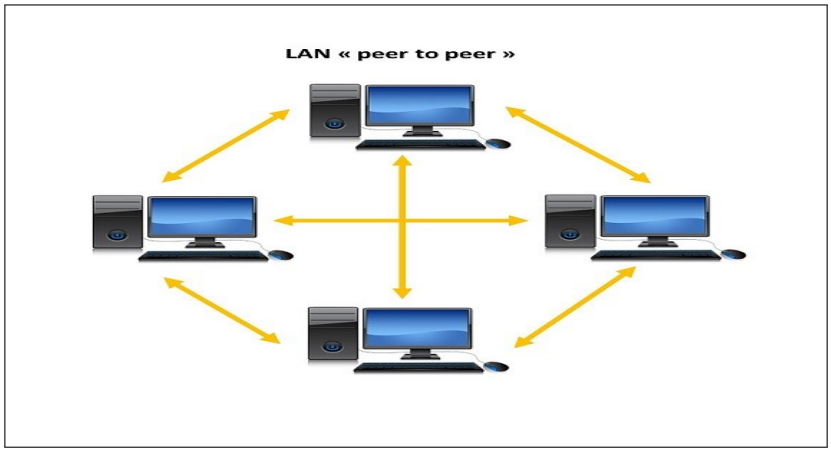


FIGURE I.12 – Architecture poste à poste .

1. **Avantages de l'architecture poste à poste**

   - **Coût réduit :** Il n'existe pas de matériel évolué et donc cher, et en plus il n'y a pas de frais d'administration.
   - **Grande simplicité :** La gestion et la mise en place du réseau et des machines sont peu compliquées **[6]**.

2. **Inconvénients de l'architecture poste à poste**
   - Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer.
   - La sécurité est moins facile à assurer, compte tenu des échanges transversaux.
   - Aucun maillon du système ne peut être considéré comme fiable **[6]**.

I.5 Topologie des réseaux

La manière dont sont interconnectées les machines est appelée « topologie ». On distingue la topologie physique (la configuration spatiale, visible du réseau) de la topologie logique **[3]**.

I.5.1 Topologie logique

Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token-ring et FDDI.

I.5.2 Topologie physique

Elle désigne la manière dont les équipements sont interconnectés en réseau. Dans cette topologie, il y a trois grandes topologies qui sont : topologie en bus, topologie en étoile et topologie en anneau. La figure I.13 illustre les types de topologies physiques.

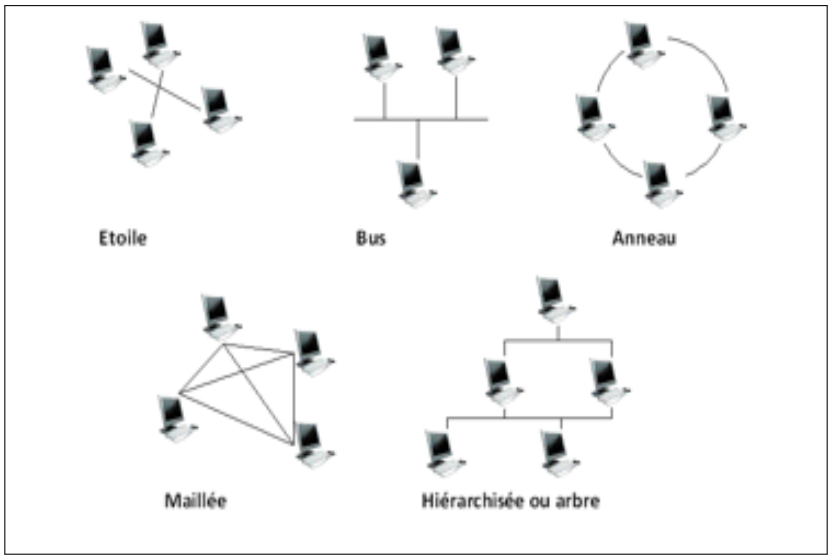


FIGURE I.13 – Types de topologies physiques.

I.6 Modèles réseaux

Le transfert d'information entre deux logiciels informatiques sur deux équipements réseau différent se base sur deux modèles théoriques : le modèle OSI et le modèle TCP/IP. Ces deux modèles sont plus théorique **[11]**.

I.6.1 Modèle OSI (Open System Interconnection)

Le modèle OSI est un modèle de référence pour décrire et expliquer les communications dans un réseau. Il décrit sept couches portant les noms de couche physique, liaison, réseau, transport, session, présentation et application. Les divers protocoles qui définissent le réseau et les communications sont donc répartis dans chaque couche, selon leur utilité. Il est d'usage de diviser ces sept couches en deux : les couches basses, qui se limitent à gérer les fonctionnalités de base, et les couches hautes, qui contiennent des protocoles plus élaborés.

A. Couches basses

Les couches basses, aussi appelées couches matérielles, s'occupent de tout ce qui est traité au bas-niveau, c.à.d. au matériel. Elles permettent d'envoyer un paquet de données sur un réseau et garantir que celui-ci arrive à destination. Elle est généralement prise en charge par le matériel et le système d'exploitation, mais pas du tout par les logiciels réseaux. Les couches basses sont donc des couches assez bas-niveau, peu abstraites et de nombre de trois. Pour résumer, ces trois couches s'occupent respectivement de la liaison point à point (entre deux ordinateurs/équipements réseaux), des réseaux locaux, et des réseaux Internet.

- **La couche physique :** : Elle s'occupe de la transmission physique des bits entre deux équipements réseaux. Elle s'occupe de la transmission des bits, leur encodage, la synchronisation entre deux cartes réseau, etc. Elle définit les standards des câbles réseaux, des fils de cuivre, du WIFI, de la fibre optique, ou de tout autre support électronique de transmission.
- **La couche liaison :** Elle s'occupe de la transmission d'un flux de bits entre deux ordinateurs par l'intermédiaire d'une liaison point à point ou d'un bus. Pour simplifier, elle s'occupe de la gestion du réseau local. Elle prend, notamment, en charge les protocoles MAC, ARP, et quelques autres protocoles.
- **La couche réseau :** Elle s'occupe de tout ce qui a trait à internet : L'identification des différents réseaux à interconnecter, la spécification des transferts de données entre réseaux, leur synchronisation, etc. C'est notamment cette couche qui s'occupe du routage, à savoir la découverte d'un chemin de transmission entre récepteur et émetteur, le chemin qui passe par une série de machines ou de routeurs qui transmettent l'information de proche en proche. Le protocole principal de cette couche est le protocole IP.

B. Couches hautes

Les couches hautes, aussi appelées couches logicielles, contiennent des protocoles pour simplifier la programmation logicielle. Elles requièrent généralement que deux programmes communiquent entre eux sur le réseau. Elles sont implémentées par des bibliothèques logicielles ou directement dans divers logiciels. Le système d'exploitation ne doit pas, en général, implémenter les protocoles des couches hautes. Elles sont au nombre de quatre :

- **La couche transport :**Elle permet de gérer la communication entre deux programmes, deux processus. Les deux protocoles de cette couche sont les protocoles TCP et UDP.
- **La couche session :** Comme son nom l'indique, elle permet de gérer les connexions et les déconnexions et la synchronisation entre deux processus.

- **La couche présentation :**Elle se charge du codage des données à transmettre. Elle s'occupe notamment des conversions de boutisme ou d'alignement, mais aussi du cryptage ou de la compression des données transmises. La figure I.14 montre les couches du modèle OSI.

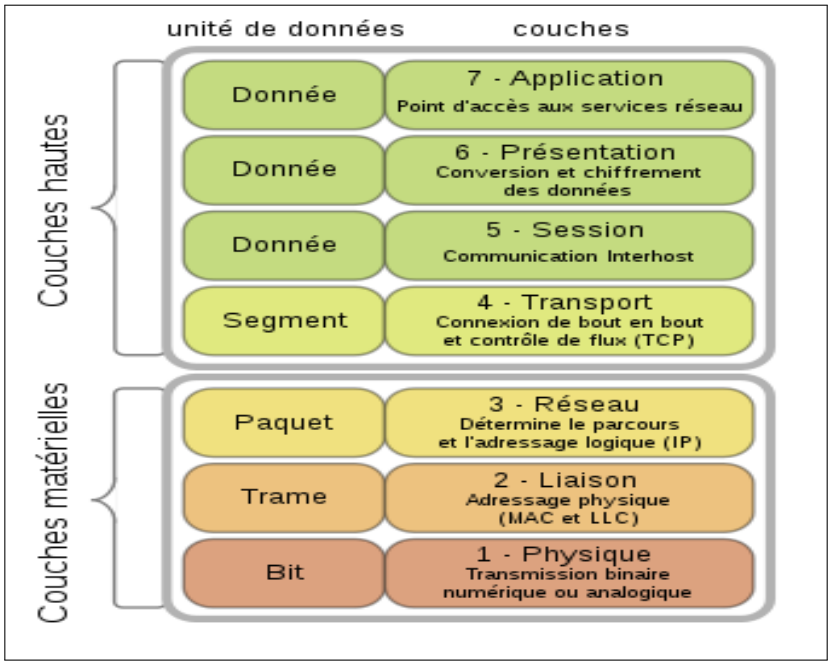


FIGURE I.14 – Couches du Modèle OSI .

I.6.2 Modèle TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application. Afin de connaitre les services de chaque couche, elles seront présentées brièvement ci-dessous l'une après l'autre :

- **Couche application :** Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.
- **Couche transport :** La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles TCP fournit d'excellents moyens de créer avec souplesse des communications réseau fiables.
- **Couche Internet :**Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter-réseau et à les faire parvenir à destination indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

- **Couche Accès Réseau :** C'est la couche la plus basse de la pile TCP/IP. Elle contient toutes les spécificités concernant la transmission des données sur un réseau physique. Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé et permet la conversion des signaux analogiques/numériques. Elle est composée de deux niveaux MAC et LLC. La figure I.15 montre la correspondance entre le modèle OSI et TCP/IP :

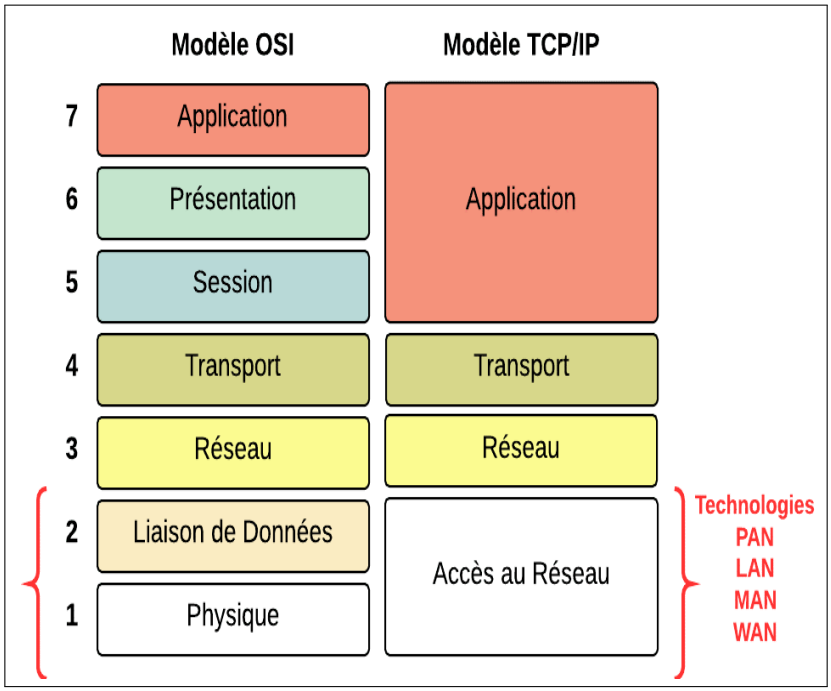


FIGURE I.15 – Correspondance entre le modèle TCP/IP et le modèle OSI .

I.7 Protocoles réseaux

Un protocole de communication est un ensemble de règles et de procédures permettant de définir un type de communication particulier. Les protocoles sont hiérarchisés en couches pour décomposer et ordonner les différentes tâches **[11]**.

I.7.1 Catégories de protocoles

De manière générale, on classe les protocoles en deux catégories selon le niveau de contrôle des données que l'on désire **[12]** :

- **Des protocoles orientés connexion :** Il s'agit des protocoles opérant un contrôle de transmission des données pendant une communication établie entre deux machines. Dans un tel schéma, la machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données qu'elle envoie. Les données sont ainsi envoyées sous forme de flot en utilisant le protocole TCP.
- **Des protocoles non orientés connexion :** Il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données sans prévenir la

machine réceptrice et la machine réceptrice reçoit les données sans envoyer d'accusé de réception à la première. Les données sont ainsi envoyées sous forme de blocs (datagrammes) en utilisant le protocole UDP.

Les protocoles réseaux les plus utilisés sont :

A. **Protocole ARP**

Le protocole ARP (Address Resolution Protocol) fonctionne en couche Internet du modèle TCP/IP correspondant à la troisième couche du modèle OSI. L'objectif de ARP est de permettre la résolution d'une adresse physique par l'intermédiaire de l'adresse IP correspondante d'un hôte distant. Le protocole ARP utilise un mécanisme de « translation » pour résoudre ce besoin **[13]**.

B. **Protocole ICMP**

ICMP est une sorte de sous-couche d'IP qui fonctionne de pair avec ce protocole. Son but est d'offrir des capacités de contrôle et d'interprétation des erreurs. En effet, IP est sans connexion et ne détecte pas les anomalies dans l'inter-réseau.

Le protocole ICMP est, donc, utilisé par les hôtes IP pour spécifier un certain nombre d'événements importants à TCP, tels que :

- Découverte des routeurs.
- Mesure des temps de transit (PING - Packet INternet Groper).
- Redirection des trames, etc.

Les données du datagramme IP sont constituées de l'en-tête et des données ICMP. Dans l'en-tête IP, le numéro de service est mis à 1. Le message ICMP lui-même est repéré par son type et son code **[3]**.

C. **Protocole IP**

Le protocole IP (Internet Protocol) est un protocole réseau de niveau trois. Il permet d'émettre des paquets d'informations à travers le réseau. Il est utilisé pour dialoguer avec les machines entre elles. Ainsi, il offre un service d'adressage unique pour l'ensemble des machines. Il n'est pas orienté connexion, c'est à dire qu'il n'est pas fiable, cela ne signifie pas qu'il n'envoie pas correctement les données sur le réseau, mais il n'offre aucune garantie pour les paquets envoyés sur l'ordre d'arrivée et la perte ou la destruction des paquets. Cette fiabilité dépend de la couche de transport **[14]**.

D. **Protocole SNMP**

SNMP est un protocole de gestion de réseaux proposé par l'IETF [2] .Il est actuellement le protocole le plus couramment utilisé pour la gestion des équipements en réseaux **[15]**. C'est un protocole principalement utilisé pour superviser des équipements réseaux (routeurs, switches, etc.), des serveurs ou même des périphériques tels que les baies de disques, les onduleurs, etc. **[16]**.

Comme son nom l'indique SNMP est un protocole assez simple, mais sa principale force réside dans le fait de pouvoir gérer des périphériques hétérogènes et complexes sur le réseau. De ce fait, ce protocole peut également être utilisé pour la gestion à distance des applications : bases de données, serveurs, logiciels, etc. **[15]**, et de diagnostiquer les problèmes survenant sur un réseau **[16]**.

Partie II : Présentation de l'organisme d'accueil et cadre du projet

I.8 Présentation générale de L'INSIM Bejaïa

INSIM Béjaia, Institut International de Management, est un établissement privé créé en mars 2004, filiale du groupe INSIM Algérie qui a été créé en 1994 dont nous retrouvons : Alger, Oran, Tizi Ouzou, Bejaia, Annaba, Constantine, INSIM Sud (Hassi Messaoud). Il dispose d'un enseignement de qualité conforme aux standards internationaux.

I.8.1 Ses Activités et Objectifs

Agréé par le ministère de la formation et de l'enseignement professionnel, l'établissement dispense des formations dans divers spécialités des sciences de gestion et des technologies de l'information et de la communication. L'INSIM Bejaia intervient dans deux domaines d'activités différentes : La formation et le conseil et accompagnement.

Ces activités sont conçues et développées spécialement en direction des secteurs socio-économiques, tels que les entreprises de production industrielle, des services et autres administrations et institutions publiques. Il comprend le conseil et l'accompagnement proprement dit ainsi que la formation à la carte.

L'INSIM, par le biais de ses formations, a pour objectifs de valoriser la ressource humaine mis à la disposition du secteur économie, administratif et autres institutions, ainsi d'assurer la promotion des candidats en fournissant l'accès aux compétences et qualifications recherchées aussi que d'accompagner les entreprises dans leur processus de mise à niveau et d'implantation des systèmes de gestion.

2. Internet Engineering TaskForce, un groupe informel et international, ouvert à tout individu et participant à l'élaboration de standards Internet.

I.8.2 Organigramme de L'INSIM Bejaia

Le découpage administratif de l'institut est effectué selon une hiérarchie pyramidale selon l'organigramme présenté dans la figure I.16 ci-dessous :

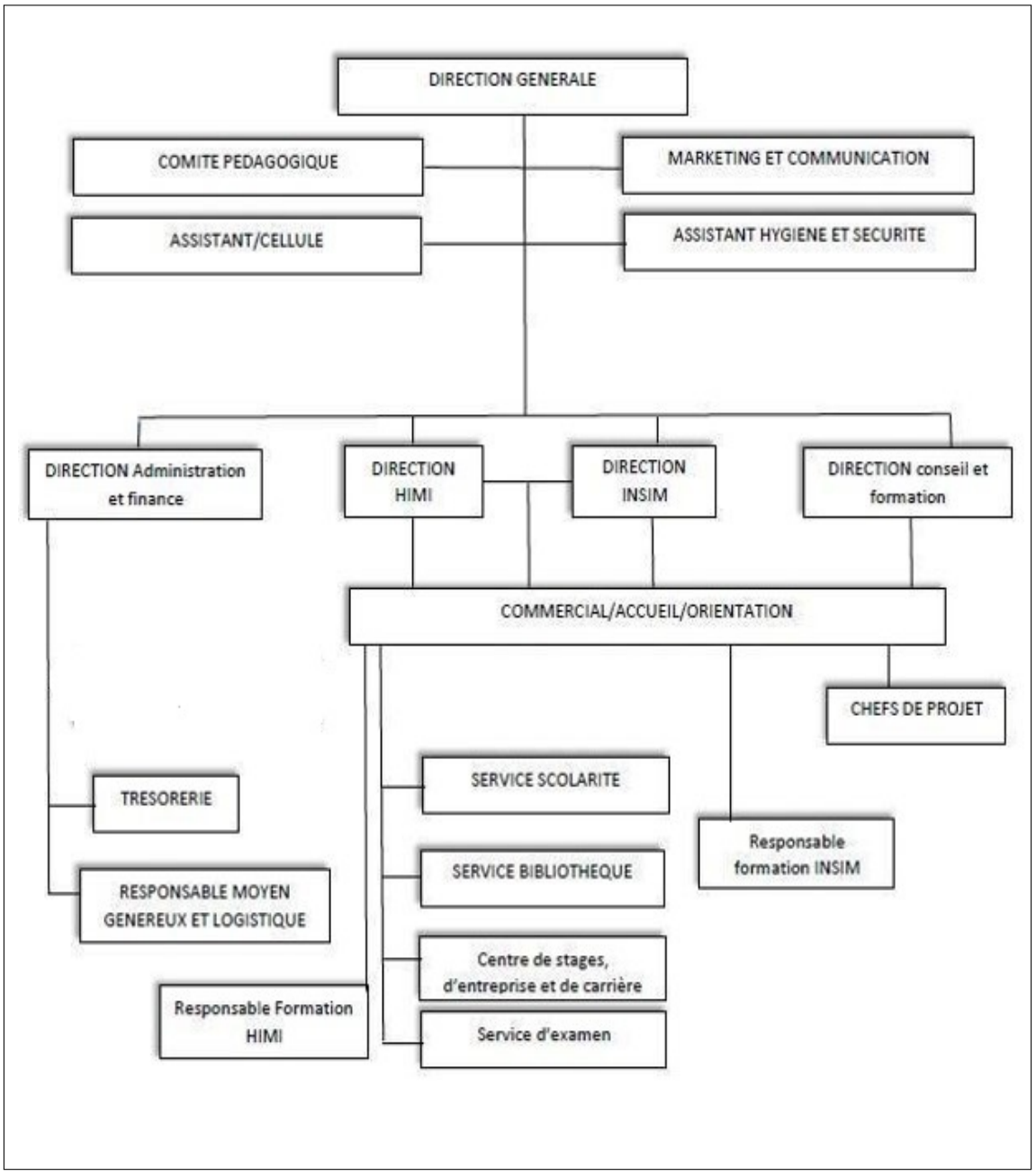


FIGURE I.16 – Organigramme de L'INSIM Bejaia .

I.8.3 Architecture réseaux de INSIM BEJAIA

Comme il est indiqué dans la figure I.17, le réseau de l'INSIM Bejaia est alimenté principalement par une connexion ADSL haut débit, où tous les sites sont connecter au switch central SW1.Le réseaux est protégé par un pare feu(Sophos).Son architecture se compose de :

- Deux hyperviseur de niveau 1 :
  - hyperviseur 1 (Esxi 1) :sur lequel on a installé windows server 2012 (Active Directory,DHCP,DNS et Serveur d'impression) ,Zimbra ,et centreon .
  - hyperviseur 2 (Esxi 2) : sur lequel on a installé ERP (Entreprise ressource planning).
- Deux salles machines Cisco 1 et Cisco 2 chaque salle comporte 14 ordinateur et une salle machine comporte 13 ordinateur y'a aucun différence entre eux c'est juste question d'emplacement .
- Un sw-admin relié à 13 ordinateurs.

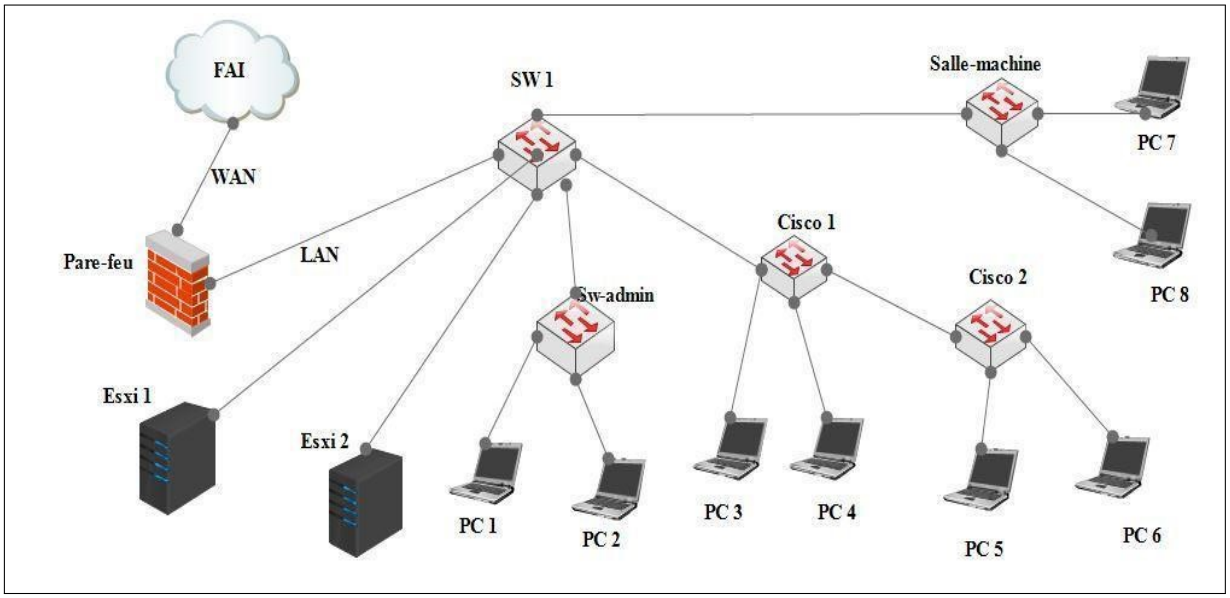


FIGURE I.17 – Architecture réseaux de l'INSIM Bejaia .

I.8.4 Présentation de l'existant

A. **Les ressources logicielles**

Les ressources logicielles de l'INSIM Bejaia sont les suivantes :

- Des systèmes d'exploitation constitués de : Linux, Windows
- Des différents services installés sur les serveurs sont : la messagerie, le DNS, les applications métiers, DHCP, Active Directory.

B. **Les ressources matérielles**

Les éléments qui composent les ressources matérielles de la structure se présentent comme suit dans le tableau I.1 :

Désignation	Tâche	Nombre
Poste de travail	Permettre aux utilisateurs d'accéder aux ressources de l'entreprise.	Non Renseigner
	Permettre aux utilisateurs d'accéder aux ressources de l'entreprise.	Non Renseigner
Serveur	Assure la disponibilité des services locaux.	3
Téléphonie IP	Permettre de faire des appels au sein de l'intranet de l'entreprise.	Non Renseigner
Imprimantes, scanner et photocopieuses	Permettent l'impression, le scannage et la photocopie de tout fichier format numérique ou papier.	14
Switch, routeur, hub, antennes	Permet l'interconnexion des différents équipements du parc informatique.	7 hubs/ Non Renseigner
Onduleur	Protection des équipements contre les microcoupures, les surtensions et les sous tensions.	10

TABLE I.1 – Ressources matériel .

Dans ce tableau I.2 ci-dessus on va détailler quelque caractéristique des ordinateurs composant le réseau de l'INSIM bejaia :

Nombre	Désignation	Caractéristiques
14	Ordinateur portable Dell	Dual Core, RAM 4GO, HDD 500GO
10	Ordinateur portable HP	Peintium 4, RAM 2 GO, 500 GO
6	Ordinateur portable HP	Dual core, RAM 4 GO, HDD 500 GO
2	Ordinateur portable Dell	Powerdge t30Q INTEL Xeon, RAM 8 GO, HDD 2TO
20	Ordinateur portable Dell	Optiplex 320, RAM 4 GO, HDD 500 GO

TABLE I.2 – Caractéristiques des ordinateurs .

I.9 Cadre de projet

I.9.1 Présentation du projet

Dans le cadre de l'obtention d'un diplôme du mastère en administration et sécurité des réseaux à la Faculté de science exacte de Bejaia, ils nous ont demandé d'élaborer un rapport suite à un stage de six mois. C'est dans ce cadre et pour l'année universitaire 2021/2022 que nous avons effectué le présent projet au sein de l'INSIM Bejaia qui porte sur la mise en place d'un système d'administration et de supervision réseau.

I.9.2 Problématique

Après quelques mois passés en entreprise, nous avons relevé les problèmes suivants :

- Un taux important de temps est gâché lors de l'évaluation des pannes ce qui influe sur la qualité du service.
- Plus le nombre d'équipements et des services augmente, plus les tâches de notre service deviennent complexes.
- L'absence d'un outil de monitoring nous prive des alertes en cas de problèmes de fonctionnements anormaux.

Pour conclure nous sommes incapables de vérifier la disponibilité des serveurs, de déterminer la qualité des services qu'ils offrent, ou de détecter la défaillance des équipements (charge CPU, état mémoire, surcharge du disque), ou les surcharges et la pénurie temporaire des ressources. Le seul moyen de détecter ces anomalies ne peut se faire que par la réception des différentes plaintes et réclamations des utilisateurs. Se souciant de la réputation du service et concerné par la satisfaction et le confort des utilisateurs, l'équipe informatique veut à tout prix éviter la confrontation à des utilisateurs mécontents, et ce en travaillant à offrir une meilleure qualité de service à ses utilisateurs en anticipant les pannes et en évitant les arrêts de longue durée gênant les services qui peuvent causer de lourdes conséquences aussi bien financières qu'organisationnelles.

I.9.3 Objectif et résultats attendus

L'objectif de notre étude est la supervision. Il en suit aussi de pouvoir conserver le contrôle du point de vue technique et applicatif. Les attentes pour cette étude sont :

- Supervision générale des équipements .
- Visibilité en temps réel du réseau et des ressources dont dispose un équipement, ce qui permettra d'avoir des informations rapidement, de connaître l'état du réseau et ses performances .
- Garantie de la disponibilité des services .
- Remontées d'alertes en cas de détection d'incidents .
- Proactivité et réaction en cas de panne .

I.9.4 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 des évolutions.

I.9.5 Gestion des configurations

La gestion de configuration permet d'identifier, de paramétrer et de contrôler les différents équipements. Les procédures requises pour gérer une configuration sont :

- La collecte d'informations
- Le contrôle d'état
- La sauvegarde historique de configurations de l'état du système.

I.9.6 Gestion des anomalies

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

I.9.7 Gestion de la sécurité

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.

I.9.8 Groupe de pilotage

Il assure la coordination technique et contrôle la pertinence des solutions proposées et est composé de (figure I.18) :

- M. Bouiche Kheireddine, Consultant en informatique à INSIM Bejaia et notre maître de stage.
- Mme. Zidani Farouja , enseignante à l'Université de Bejaia , notre superviseur.

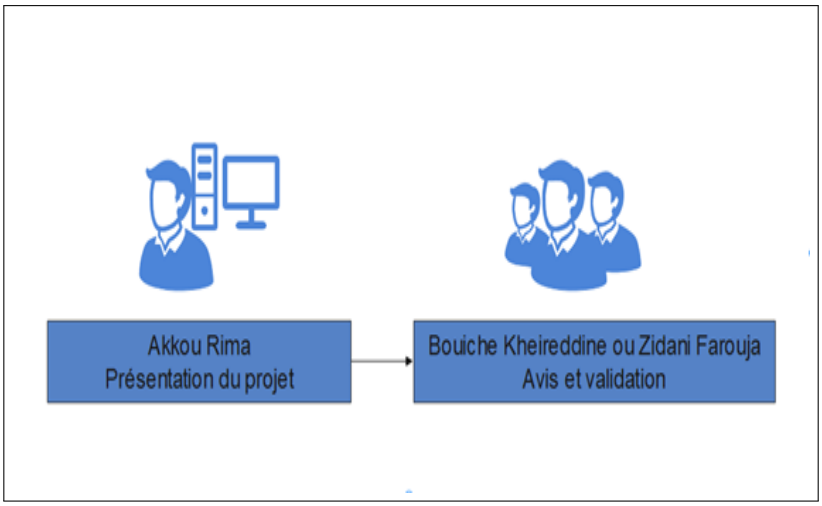


FIGURE I.18 – Équipe du projet.

I.10 Conclusion

Dans ce chapitre, nous avons présenté les réseaux informatiques et tout ce qui a une relation avec notre projet. Ensuite , on a défini la problématique et les besoins de notre organisme d'accueil. Nous devrions trouver des solutions pour répondre à ces besoins. Le chapitre suivant sera consacré à faire un état de l'art sur notre domaine d'étude, les techniques de supervision des réseaux informatiques.

Chapitre II

La supervision

II.1 Introduction

Les systèmes informatiques sont devenus indispensables au bon fonctionnement des entreprises et administrations. Tout problème ou panne survenu sur une partie de ce système pourrait avoir de lourdes conséquences aussi bien financières qu'organisationnelles. Donc, surveiller un tel système devient plus que nécessaire. Dans ce chapitre, nous allons définir précisément le concept de supervision (appelée aussi monitoring), ensuite nous procéderons à une étude comparative des outils de supervision (solutions open-source). Cette étude ressemble à un banc d'essai puisque pour chacun des logiciels nous allons faire une courte présentation et expliquer son fonctionnement, puis finir par ses avantages et ses inconvénients. A la fin, nous préciserons le choix de l'outil retenu durant notre travail.

II.2 Définition de la supervision

La supervision informatique est une technique de surveillance, d'analyses et d'alertes permettant de pallier les problèmes liés à tous les niveaux du fonctionnement informatique d'une entreprise. Elle rend l'entreprise plus performante et surtout proactive. Elle doit répondre aux préoccupations suivantes **[17]** :

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

II.3 Principes de fonctionnement de la supervision

Les principes de fonctionnement de la supervision peuvent être résumés en :

II.3.1 Fonctionnalités de la supervision

On distingue quatre fonctionnalités de la supervision :

A. **La surveillance**

La surveillance informatique résulte de ce que l'on appelle monitoring qui est une activité de mesure d'une activité informatique. La surveillance des équipements d'une infrastructure est la fonctionnalité de base proposée par les différents outils de supervision du marché. Ils permettent de surveiller **[17]** :

- Les ressources d'un équipement informatique.
- Le trafic réseau.
- Les attaques liées au réseau.
- Les flux de données entre applications.

B. **Les notifications**

La notification est employée pour décrire des fonctions d'alerte automatisées entre processus. Mais lorsqu'un incident est détecté, il faut autoriser la réception des notifications informant ainsi qu'un changement d'état vient d'avoir lieu. Ce genre d'évènements est généralement distribué par messagerie, ou par SMS et/ou IRC [1]. Il est même possible de distribuer sélectivement les notifications à un autre groupe d'utilisateurs bien défini en fonction des plages horaires programmées et de répéter cet envoi plusieurs fois lorsque la réparation ou l'acquittement n'est pas réalisé au bout d'un certain laps de temps **[17]**.

C. **Les sondes**

Généralement, les outils de supervision n'effectuent pas eux-mêmes la surveillance de certaines composantes : mémoire, CPU, disques, etc. Ces composantes sont, la plupart du temps, constitutives de scheduler (ou ordonnanceurs) déléguant cette tâche à des sondes. Concrètement, les sondes sont des scripts, des programmes ou plus généralement du code, appelés scheduler, qui effectuent l'ensemble des traitements de vérification et envoient leurs résultats afin de centraliser les informations récoltées. On doit, donc, pouvoir ajouter facilement des sondes en s'appuyant sur les différentes extensions (ou plugins) disponibles **[17]**.

D. **Les dépendances**

Il est primordial que les différents équipements conservent leur interdépendance au sein de l'outil de supervision. Si on prend l'exemple des bases de données, des switchs et des serveurs : le mode opérationnel est vérifié lorsque les bases de données hébergées sur les serveurs sont opérationnelles et que les switchs interconnectant les serveurs sont également en fonction. Ainsi, en précisant la dépendance des serveurs vis-à-vis des bases de données et des switches vis-à-vis des serveurs, on peut alors notifier les cas de pannes. Et cela facilite la détection d'incidents en se concentrant sur l'essentiel de l'information, la panne de l'équipement interdépendant, plutôt que sur l'ensemble des machines en alerte. Cela permet de mieux mettre en évidence l'équipement ou le service en défaut et de faciliter le dépannage et la maintenance **[17]**.

II.3.2 Principe de la supervision

Le principe de la supervision est de s'assurer du bon fonctionnement d'un système. En sommes, superviser n'est pas seulement surveiller, encore il faut pouvoir alerter et analyser les données collectées sur les équipements afin d'être proactif et plus uniquement réactif. On peut résumer la supervision par le graphe de La figure II.1 suivante **[17]** :

1. IRC : Internet Relay Chat, Serveur permettant de dialoguer en direct avec plusieurs personnes .

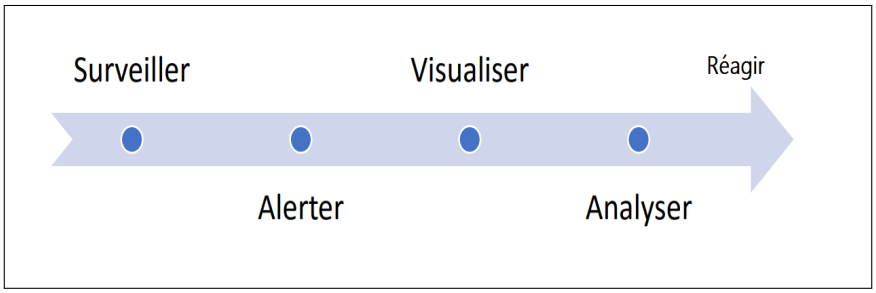


FIGURE II.1 – Principe de supervision .

Il existe plusieurs types de supervisions :

A. **Supervision système**

Ce type de supervision s'applique à surveiller essentiellement l'ensemble des ressources des différents systèmes d'exploitation : mémoire RAM, stockage de masse, type de RAID, etc.

B. **Supervision réseau**

Ici, on cherche essentiellement à surveiller le réseau et ses équipements tels que les commutateurs, les routeurs, etc. L'idée est de s'assurer que ces équipements sont opérationnels, qu'aucun port ou GBic (Gigabit interface Converter) n'est défectueux et que les interconnexions sont effectives. En outre, elle porte sur la surveillance de manière continue de la disponibilité des services du fonctionnement, des débits, de la sécurité mais également du contrôle des flux.

C. **Supervision sécurité**

On peut également aller jusqu'à surveiller les attaques contre le système d'information de l'entreprise. C'est généralement dans ce cadre qu'intervient ce type d'activité, mettant en place l'ensemble des contre-mesures, scrutant et analysant les différents accès et permettant de détecter les tentatives d'intrusions.

D. **Supervision applicative**

La supervision des applications (ou supervision applicative) permet de connaître la disponibilité des machines en termes de services rendus en testant les applications hébergées par les serveurs. La supervision applicative passe par des mesures faites aussi sur le flux de service. On parle alors de validation fonctionnelle. On utilise souvent un sous-ensemble des tests ayant permis la recette d'une application pour n'en prendre que les tests qui sont représentatifs de l'activité sans pour autant générer une charge trop importante ou modifier les données applicatives. La supervision applicative ne peut se faire sans considérer la sécurité applicative.

E. **Supervision métier**

De façon plus générique, on s'intéresse ici à la supervision des différents processus métier. En effet, un métier peut dépendre de plusieurs applications. Il faut, donc, s'assurer que celles-ci sont bien toutes actives et en bon état de fonctionnement.

II.4 Supervision , un outil indispensable en entreprise

La sécurité est le premier facteur à tenir en compte lors de la conception d'un système informatique en entreprise, donc la supervision des systèmes d'information et des parcs informatiques, afin d'assurer la haute disponibilité des services, est aussi cruciale pour cette entreprise.

La supervision en temps réel via des protocoles et les formats de données SNMP, les outils de monitoring réseau et solutions de supervision permettent de détecter rapidement les pertes de capacité du système d'information de l'entreprise. Le manager ou l'opérateur réseau reçoit alors des alertes (souvent par e-mail ou sms) en cas de surcharges, et peut ainsi intervenir directement via l'interface du système monitor.

En tant qu'outil de visualisation complet, le monitoring permet la détection des anomalies sur l'ensemble du système informatique, interne de l'entreprise, les serveurs, les disponibilités réseaux, les imprimantes, les applications, ainsi que tous les autres éléments actifs en contact avec le réseau (routeurs, switches, hubs, etc.). Une telle solution de supervision et de monitoring permet ainsi à l'administrateur de bien monitorer chaque point du réseau et à distance lorsqu'il n'est pas sur place.

II.4.1 Pourquoi opter pour un logiciel de supervision ?

Dans le cas d'une PME (petite ou moyenne Entreprise) ou une grande multinationale, une surveillance réseau efficace, par des logiciels de supervision performants, est très nécessaire pour :

- Effectuer des analyses et des diagnostics réseau constants.
- Veiller en permanence au bon fonctionnement des processus sur le réseau.
- Centraliser les données clés à monitorer et l'information de la santé du réseau.
- Assurer l'envoi d'alertes aux agents de l'équipe informatique dès qu'une anomalie soit détectée.

Les besoins en matière de supervision varient d'une entreprise et d'un métier à l'autre. D'où l'existence, sur marché, de nombreux outils de surveillance disponibles au téléchargement dans toutes les langues, qu'il s'agisse d'éditeurs de logiciels de monitoring open source (souvent gratuits) ou propriétaires (payants sous licence) **[1]**.

II.5 Méthodes de supervision

Deux grandes méthodes s'opposent lorsqu'on parle de la supervision **[22]** :

II.5.1 Mode actif

Le mode actif est une vérification réalisée à intervalles de temps réguliers par le serveur de monitoring, représenté sur la figure II.2 :

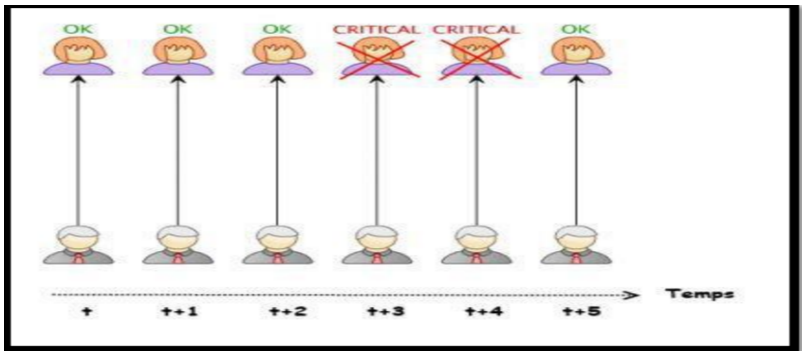


FIGURE II.2 – Mode actif .

A. **Avantages du mode actif**

- À l'initiative du serveur de monitoring, on aura alors un plus grand intérêt à sécuriser le serveur de monitoring, si jamais ce dernier tombe en panne (avec un serveur de réplication par exemple).

B. **Inconvénients du mode actif**

- Temps de réaction un peu plus long car l'équipement est monitoré par le serveur de monitoring qui lui-même monitore d'autres équipements.

II.5.2 Mode passif

Le mode passif est un signal émis par l'équipement monitoré à chaque changement d'état représenté sur la figure II.3 :

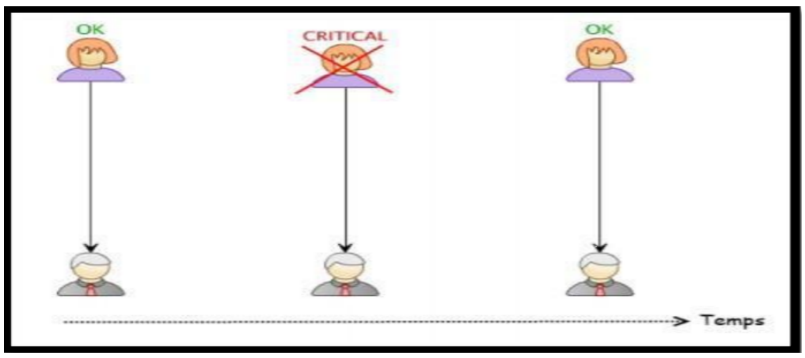


FIGURE II.3 – Mode passif .

A. **Avantages du mode passif**
   - Tous les changements d'états sont remontés.
   - Temps de réaction rapide car l'équipement se supervise lui-même.

B. **Inconvénients du mode passif**
   - À l'initiative de l'équipement actif : Si l'équipement ne fonctionne plus, aucune alerte ne sera remontée.
   - Surcharge du serveur de monitoring lors de l'envoi simultané d'alerte par plusieurs équipements.

II.6 Choix de la méthode de supervision

Pour donner suite à une longue réflexion et afin de déterminer lequel des deux concepts était le plus approprié pour notre projet, nous avons fini par conclure que celui-ci se rapprochait plus du mode actif. Cette méthode est beaucoup plus simple et rapide à mettre en place. Mais l'avantage incontournable de cette méthode reste, principalement, de limiter les charges de notre serveur de monitoring pour qu'il puisse toujours accueillir davantage de machines, car pour rappel en mode actif, c'est le serveur de monitoring qui est à l'initiative des collectes et remontées d'informations sur nos machines, de plus en mode passif si l'équipement ne fonctionne plus, aucune alerte ne sera remontée.

II.7 Types de Monitoring (Supervision et Métrologie)

Avant de commencer à comparer les différentes solutions, il est indispensable de définir quelques termes en relation avec le monitoring(figure II.4) [21].

II.7.1 Métrologie

La métrologie est le fait d'obtenir, de garder et de tracer la valeur numérique d'une charge, par exemple, le pourcentage de CPU utilisé sur un serveur. Bien souvent, la métrologie permet tout simplement de tracer des graphiques. C'est donc le fait de récupérer les informations permettant de tracer son évolution dans le temps. Elle est, donc, caractérisée non pas par le fait de récupérer une valeur à l'instant T, mais de pouvoir afficher et tracer l'évolution d'une charge construite par un ensemble de métriques récupérées dans le temps.

II.7.2 Supervision

La supervision se caractérise d'ailleurs par son système d'alerte, conséquence directe de la vision "à l'instant T". On peut, alors, avertir l'administrateur si un système passe de l'état UP à l'état DOWN et inversement. Au contraire, dans le concept pur de la métrologie, le système d'alerte n'est pas pris en compte car la récupération des valeurs/charges n'est pas forcément faite à l'instant.

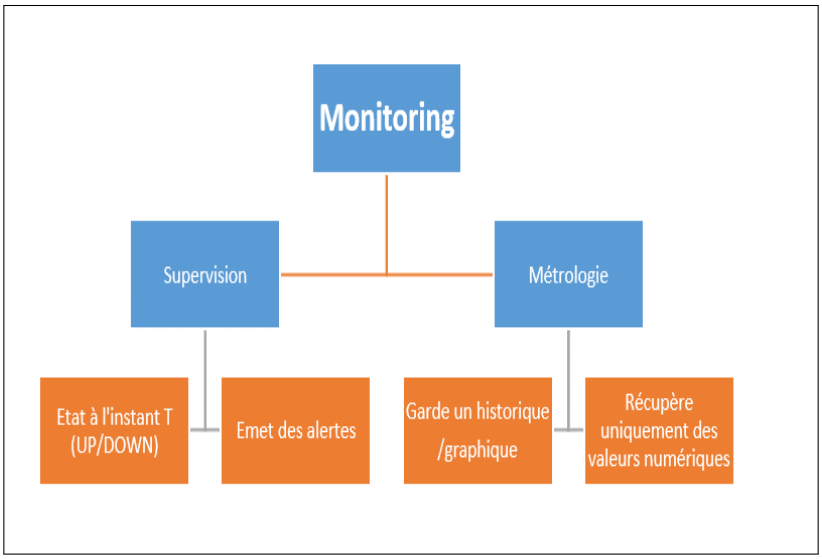


FIGURE II.4 – Supervision et Métrologie .

II.8 Solutions de la supervision

Il existe deux solutions de la supervision :**[17]**

II.8.1 Solutions propriétaires

Les logiciels propriétaires ont un support présent et réactif grâce au contrat mis en place entre le propriétaire et le client.

A. **HP OpenView**

HP OpenView est, à l'heure actuelle, un des logiciels majeurs de la supervision. Il permet le management d'équipements réseaux. Une interface graphique permet un affichage de l'état courant des équipements. Il est basé sur SNMP pour dialoguer avec les différentes machines **[18]**.

HP OpenView permet de gérer des composants d'une infrastructure informatique d'une manière standardisée. Il est principalement utilisé pour la surveillance de serveurs, périphériques, réseaux, bases de données et applications pour assurer que les défauts sont détectés et alertés dans les meilleurs délais. Il est composé de deux systèmes :

- **Système de Map :** Une interface graphique appelée MAP permet un affichage de l'état courant des équipements. Les couleurs permettent de préciser l'état des différents périphériques.
- **Système d'alarme :** HP OpenView intègre un système d'alarme. En effet des requêtes SNMP sont régulièrement envoyées vers les agents. Si un état change ou une machine devient injoignable, une alarme est directement déclenchée et une action peut être entreprise (lancement d'un programme, envoi d'un mail, etc.).

1. **Avantages**
   - Une vue globale du réseau.
   - Une vision des différents incidents.
2. **Inconvénients**
   - Coût d'acquisition et de support.

B. **CiscoWorks**

Ciscoworks (Network Connectivity Monitor NCM) constitue le plus récent développement de la gamme de solutions de gestion Cisco Works, conçues pour faire des réseaux Cisco les plus faciles à administrer et les plus disponibles du marché. Sur un réseau Cisco, NCM est immédiatement prêt à localiser les problèmes de connectivité en temps réel et à identifier leurs répercussions. À mesure que le réseau s'étend et évolue, Ciscoworks NCM détecte les modifications apportées aux périphériques Cisco et ajuste son analyse en conséquence **[19]**.

Il existe d'autres outils de la gamme Cisco Works qui sont adaptés en fonction des besoins et de l'importance du système d'information à étudier. Il existe, notamment, Cisco Network Assistant, un outil gratuit de Cisco, qui permet de vérifier et de configurer à distance les équipements. Il permet en outre de cartographier les équipements Cisco mis en place sur un réseau. Ainsi, il est possible pour chaque équipement de configurer des VLANs dans une interface graphique simple sans taper une ligne de commande en mode console **[19]**.

1. **Avantages**

   Temps moyen de réparation réduit : Cisco Works NCM est capable de repérer les problèmes de connectivité en temps réel et garantit la mise en œuvre d'actions correctrices efficaces, généralement avant que le service de réseau ne subisse une dégradation significative.
2. **Inconvénients**

   La non disponibilité des codes sources présente un inconvénient aux clients qui veulent mettre à jour leurs applications selon leurs besoins.

II.8.2 Solutions Open Source

Il faut savoir qu'il existe des dizaines de solutions Open Source dédiées au Monitoring. Le critère principal de choix réside dans les différents cas d'utilisation. Nous allons présenter quelques logiciels [20].

A. **Zabbix**

Créé en 2001, puis donnant naissance à une entreprise nommée Zabbix SIA en 2005. Zabbix est une solution de supervision open-source de plus en plus prisée. L'entreprise vise à faire de Zabbix un logiciel reconnu dans le milieu de la supervision et créer une communauté autour de lui pour permettre une évolution plus rapide. A côté de cela, cette société propose

un service de maintenance commerciale. Zabbix permet plusieurs moyens d'acquérir les données :

- **Via SNMP :** Comme tous ses concurrents .
- **Via test de service :** Il n'y a rien à installer sur l'équipement surveillé, mais les tests sont limités à des ping ou des tests de protocoles (SMTP, HTTP, etc.) .
- **Via l'agent Zabbix local :** C'est une originalité. Installer un agent permet d'obtenir toute information sur l'équipement sans utiliser le protocole SNMP.

L'architecture logicielle est découpée en composants dans le but de faciliter le monitoring distribué :

- **Serveur :** Le serveur est le cœur de l'application Zabbix. Il centralise les données et permet de les attendre (trapping) ou d'aller les chercher (polling). Il centralise, aussi, toutes les informations de configuration et permet d'alerter les administrateurs en cas de problème.
- **Proxy :** Élément optionnel de l'architecture, il permet de bufferiser les données reçues des différents sites dans le but d'alléger les traitements pour le serveur.
- **Agent :** Une fois installé sur un système, l'agent va collecter les données locales et les envoyer au serveur.
- **Interface Web :** Celle-ci est une partie du serveur bien qu'il n'est pas obligatoire qu'elle se trouve sur la même machine que le serveur. L'interface permet de configurer entièrement Zabbix, d'accéder aux statistiques ainsi qu'à d'autres informations.

Tous ces composants sont écrits en C afin de garder de hautes performances, hormis bien évidemment l'interface Web développée en PHP.

L'interface est divisée en cinq parties, figure II.5 :

- **Monitoring :** C'est la partie affichage des statistiques, des graphiques, des alertes, de la cartographie, etc.
- **Inventory :** C'est l'inventaire des machines et équipements.
- **Report :** Ce sont des statistiques sur le serveur Zabbix et un rapport de disponibilité des services sur les machines supervisées.
- **Configuration :** Comme son nom l'indique, elle permet de configurer entièrement Zabbix.
- **Administration :** Elle permet de gérer les moyens d'alertes (SMS, Jabber, Email, etc.) et les utilisateurs.

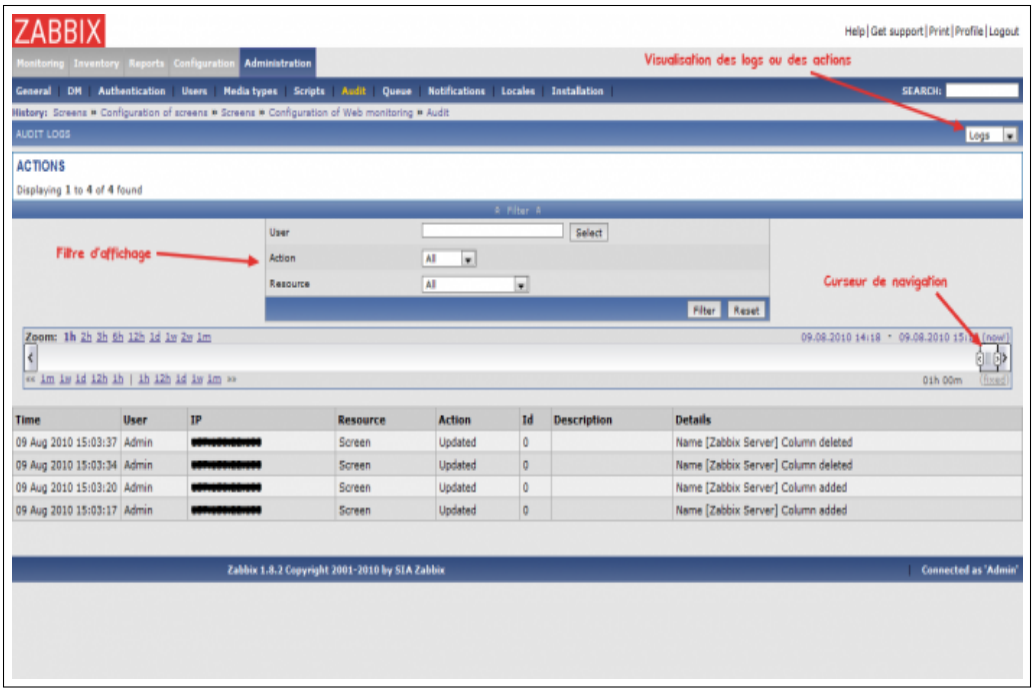


FIGURE II.5 – Interface de Zobbix .

1. **Avantages**

   - 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 une communauté croissante.
   - Une interface vaste mais claire
   - Une gestion des templates poussée, avec import/export xml, modifications via l'interface.
   - Des performances au rendez-vous : L'application a été testée avec succès avec 10000 équipements supervisés.
   - Compatible avec MySQL, PostgreSQL, Oracle, SQLite.

2. **Inconvénients**

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

B. **NetMRG**

Créé en 2001, NetMRG (figure II.6)veut se distinguer des autres logiciels en proposant des petites améliorations : La visualisation des graphiques avec historiques et l'auto-scroll, l'utilisation de modèles (templates) pour ajouter plus facilement de nouveaux graphiques, la mise à jour du logiciel simplifiée, la gestion des jours de travail. L'architecture logicielle est découpée en composants :

- **Moteur C++ :** Il se Charge de récolter les données (Via scripts, Données SNMP ou MySQL). Il est Conçu dans le but de supporter une charge conséquente (Application multi threads grâce à pthreads). Ce moteur est au cœur de l'application, il ordonnance les tâches et gère les interactions en plus de son rôle de récolteur.
- **RRDTOOL :** elle apporte sa puissante gestion des données ainsi que ses atouts indéniables en matière de génération de graphique.
- **Base de données MySQL :** Elle permet de sauvegarder la configuration.
- **Interface :** Elle est réalisée grâce à PHP, qui permet de modifier la configuration et d'afficher les graphiques au format PNG générés par RRDTOOL. Pour retrouver les graphiques, on doit tout d'abord passer par un arbre qui organise les différentes machines et statistiques associées. Ce Device Tree affiche tout d'abord des groupes (Group) qui contiennent des machines (Device), puis on accède aux différents services ou valeurs monitorées (Sub device) avant de trouver à l'intérieur les graphiques (Monitors). Des événements sont également visibles en cas de problème.

1. **Avantages**

   - Performances : L'application semble pouvoir tenir la charge avec énormément de machines surveillées grâce au moteur multi threads.
   - Alarmes : Il est possible de configurer des évènements qui avertissent l'administrateur d'un fonctionnement anormal.
   - Interface : Elle permet de gérer un grand nombre de machines classées dans des groupes.
   - Gestion des utilisateurs.

2. **Inconvénients**

   - Interface : Elle n'est pas très accueillante et est déroutante au début.
   - Configuration : Il n'est pas très aisé d'ajouter de nouveaux équipements à surveiller si on sort du cadre du template prédéfinie.
   - Développement lent, peu de versions et très espacé dans le temps (environ une année).
   - Aucune gestion de carte de réseau, et aspect rudimentaire des alarmes. Aucune gestion de panne.

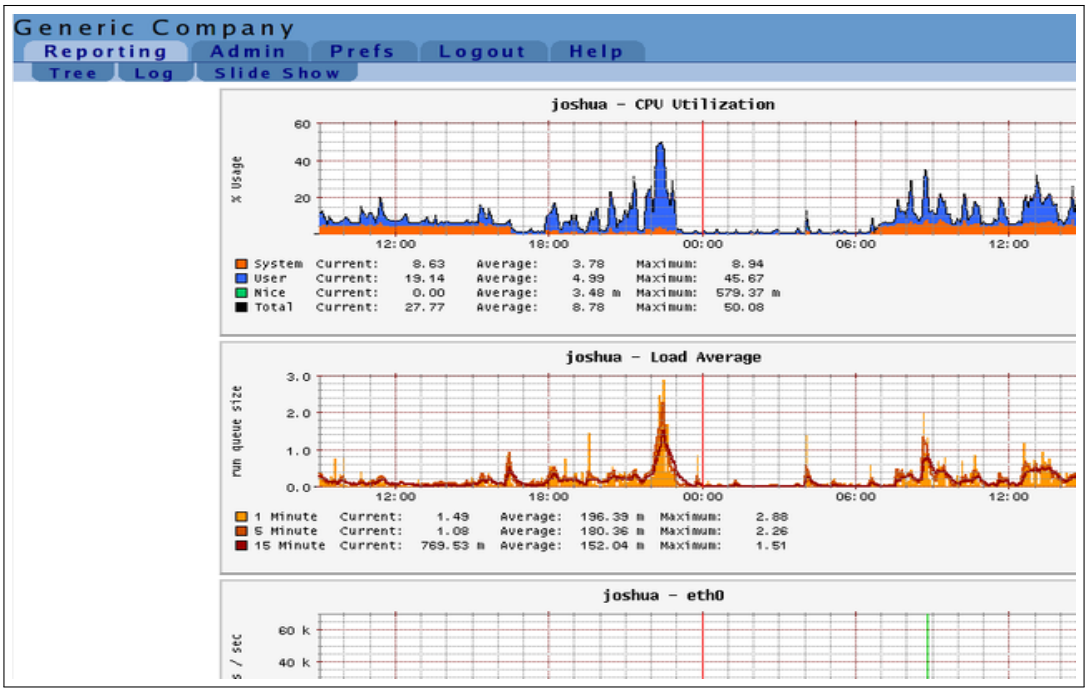


FIGURE II.6 – Interface de NetMRG .

.

C. Cacti

Cacti se base sur RRDTOOL et se présente lui-même comme étant l'interface la plus complète à celui-ci. Cacti utilise également une base MySQL pour stocker la configuration. Depuis la version 0.8.6, Cacti propose un moteur de récolte des données en C, nommé Cactid, utilisant avantageusement les Threads POSIX. Une stratégie qui ressemble étrangement à celle réalisée par NetMRG sauf que Cacti propose de l'utiliser seulement en cas de besoin effectif de performances (dans le cas contraire, c'est le moteur PHP qui prend le relais). Les mêmes fonctionnalités que NetMRG existent sur Cacti : Sources de données multiples via scripts dans de multiples langages, gestion des utilisateurs et ajout d'équipement à partir de modèles (templates) de configuration.

L'interface est divisée en deux, une partie comme ça présente sur la figure II.7 nommée Console permettant de tout configurer et une autre nommée Graphs permettant d'afficher les graphiques. L'originalité réside dans le fait que la partie affichage de graphiques possède trois modes d'affichages :

- **Tree mode :** Il ressemble à l'interface de NetMRG, classement en arbre des différentes machines par groupes. Il est utile pour gérer un grand nombre de machines ou équipements.
- **List mode :** Il permet de lister les graphiques présents sur une machine sélectionnée dans la liste.
- **Preview mode :** Il ressemble à List Mode excepté que les graphiques sont affichées directement au lieu d'un lien vers celui-ci. Il est utile pour avoir un aperçu rapide sur l'état d'une machine et de ses services.

1. **Avantages**

   - Interface : Elle est beaucoup plus claire que celle de NetMRG. Elle permet également beaucoup plus de choses (Plus de modes d'affichages et plus de possibilités de configuration).
   - Configuration : Avec l'utilisation des templates pour les machines, les graphiques et la récupération des données se configurent aisément et entièrement via l'interface web. L'import/ export des templates au format XML est très simple. On peut, aussi, très facilement utiliser des options poussées de RRDTOOL.
   - Performance : Avec le choix du moteur de récolte des données, on peut opter pour la performance ou la simplicité.
   - Gestion des utilisateurs.
   - Communauté sur le web et présence d'une dizaine de plugins permettant d'étendre les fonctionnalités.

2. **Inconvénients**

   - Absence de gestion d'alarmes sauf avec un plugin nommé Thold.
   - Absence de gestion de panne et d'une cartographie de réseau.
   - Développement lent tout comme NetMRG.

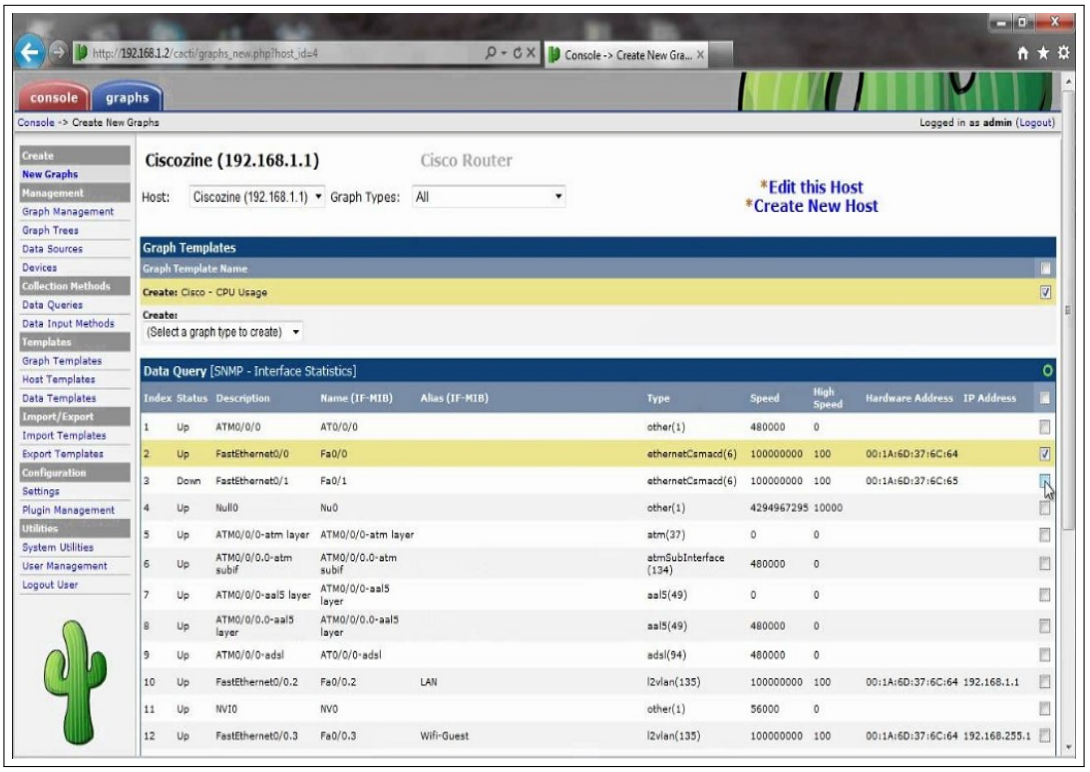


FIGURE II.7 – Interface de Cacti .

D. Nagios

Successeur de NetSaint, Nagios est certainement le logiciel libre le plus connu dans le milieu de la supervision réseau. Appréciée des entreprises ainsi que des particuliers, cette application possède une très grande communauté qui participe activement au développement. L'architecture logicielle est modulaire comme chez ses concurrents :

- Un moteur qui gère l'ordonnancement de la supervision, écrit en C.
- Une interface Web réalisée à l'aide des CGI.
- Des greffons, ou plugins qui étendent les possibilités de Nagios (Plus de 1200 plugins existants sur nagiosexchange.org).

Il existe notamment des plugins Nagios nommée NRPE et NCSA qui fonctionnent presque sur le même principe que ceux de Zabbix. NRPE est un agent esclave qui attend les ordres du moteur Nagios (polling) et NCSA envoie lui-même les données (trapping). L'interface est divisée en trois parties :

- Partie monitoring : Elle permet plusieurs vues : Vue globale, vue précise, vue de la carte du réseau, vue des problèmes, etc. et même une vue 3D.
- Partie reporting : Elle regroupe les tendances des statistiques, les alertes et évènements ainsi qu'un rapport de disponibilités des services.
- Partie configuration classique permettant de tout configurer.

1. **Avantages**

   - Reconnu auprès des entreprises, grande communauté.
   - Pléthore de plugins qui permettent d'étendre les possibilités (agents comme zabbix, reporting amélioré, etc.).
   - Solution complète permettant le reporting, la gestion de panne et d'alarmes, la gestion utilisateurs, ainsi que la cartographie du réseaux.
   - Beaucoup de documentations sur le web.
   - Performances du moteur.

2. **Inconvénients**

   - Interface non ergonomique et peu intuitive.
   - Configuration fastidieuse via beaucoup de fichiers.

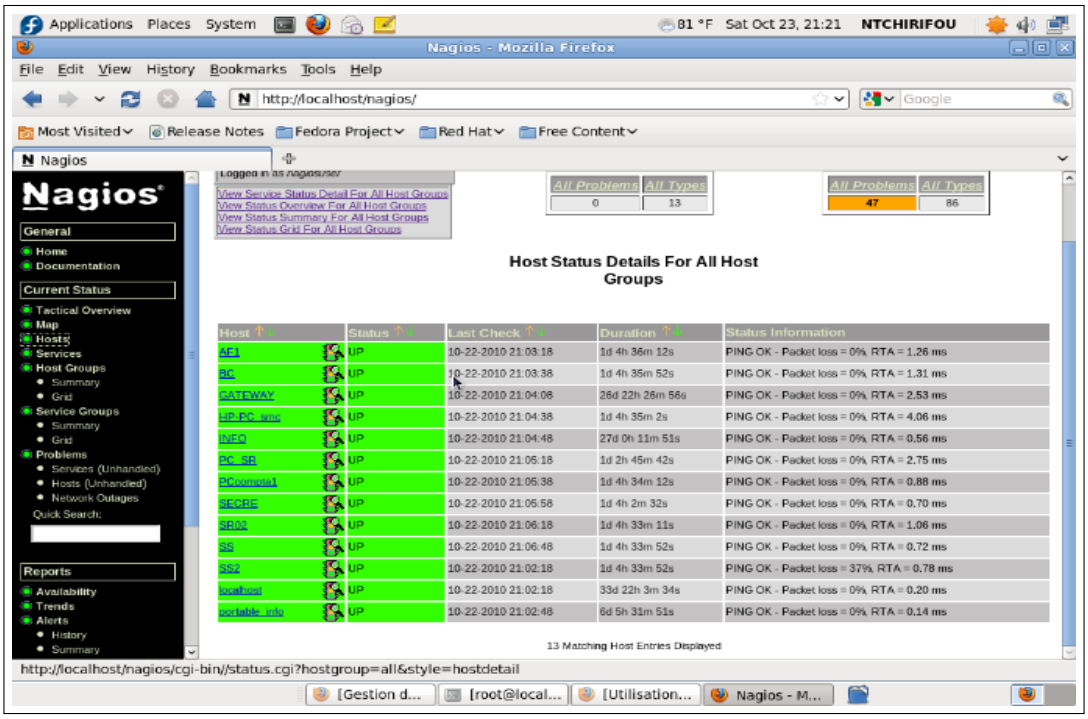


FIGURE II.8 – Interface Nagios .

E. Centreon

Centreon, basé sur Nagios, se présente comme une évolution de celui-ci pour tout d'abord son interface (figure II.9) mais aussi ses fonctionnalités. Créé en 2003 par des français souhaitant améliorer Nagios et son interface très austère, Centreon (anciennement Oréon) a été repris par une nouvelle entreprise nommée Merethis. Centreon reprend, donc, les avantages du moteur de Nagios et permet ainsi d'être entièrement compatible avec des solutions existantes. Son interface reprend un découpage classique :

- **Home :** Une page d'accueil avec Le Tactical Overview de Nagios permettant un coup d'œil rapide aux problèmes survenus et un accès aux statistiques des performances du moteur et de ses composants.
- **Monitoring :** Il possède plusieurs vues, mais reprend la grande idée de l'arbre des groupes d'équipements. Il reprend, également, la vue Nagios.
- **Views :** Il permet d'accéder à tous les graphiques avec un menu arborescent et à une cartographie du réseau en applet Java.
- **Reporting :** Un dashboard ressemblant à celui de Zabbix en ajoutant une frise chronologique de la disponibilité de l'équipement.
- **Configuration :** Pour tout configurer de A à Z.
- **Administration :** Configuration des accès utilisateurs

1. **Avantages**
   - Robustesse et renommée de Nagios.
   - Interface beaucoup plus sympathique, permettant de tout configurer, de garder un oeil sur tout le réseau en permanence.
   - Utilisateurs de Nagios ne seront pas perdus pour autant, l'interface reprenant avantageusement certaines vues Nagios.
   - Solution complète permettant le reporting, la gestion de panne et d'alarmes, la gestion utilisateurs, ainsi que la cartographie du réseau.
   - Entreprise qui pousse le développement.
   - Peut-être décoléré du serveur Nagios et tournée toute seule sur un autre serveur.
2. **Inconvénients**
   - Une interface peut paraître complexe car il existe beaucoup d'options, de vues, etc. Cela nécessite une petite formation.
   - Un développement qui n'est pas encore en phase avec celui de Nagios : Parfois des problèmes de compatibilité.
   - Un peu plus lourd par rapport à Nagios.

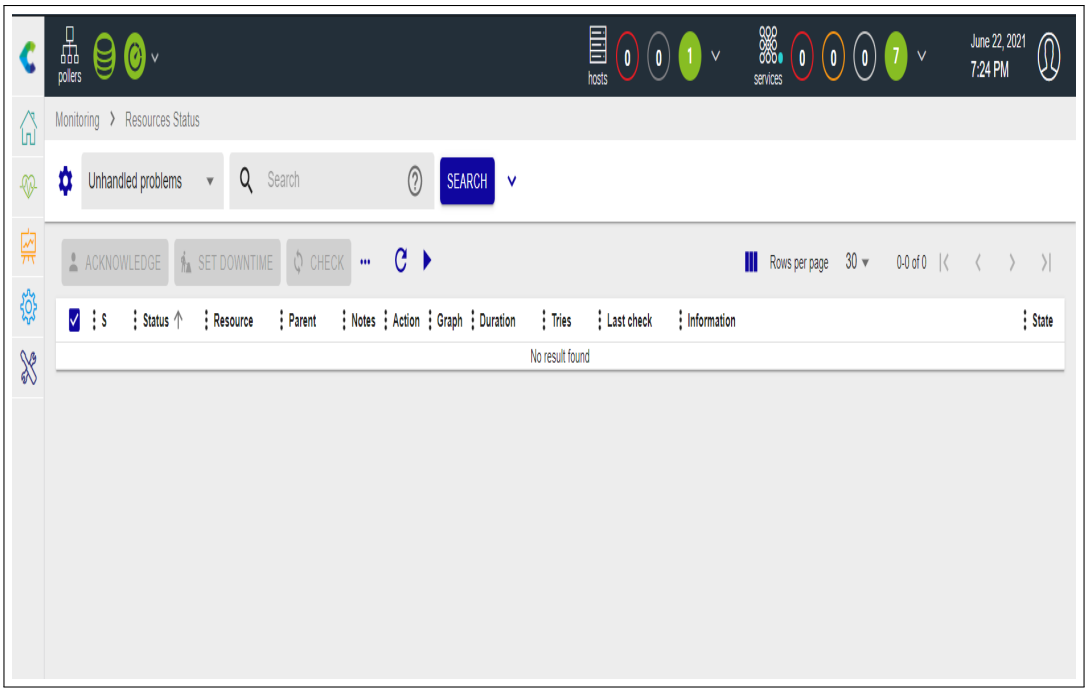


FIGURE II.9 – Interface de Centreon .

II.9 Open source ou propriétaire ?

D'abondantes solutions de monitoring subsistent dans le monde du monitoring, open sources ou propriétaires, qui s'orientent plus vers la niche supervision ou la niche métrologie. Chaque modèle de solution a ses avantages et ses inconvénients (tableau II.1)**[22]**.

Solution de la supervision	Avantage	Inconvénient
Propriétaire	• Bénéficie d'une palette de fonctionnalités avancées et enrichies. • Support technique accompagnant la solution. • Solutions globales répondant à une large gamme de besoins.	• Développement additionnel restreint et coûteux. • Incompatibilités entre fournisseurs dû aux différents produits et protocoles. • Coût d'acquisition et de support pouvant être élevé selon la solution et les contrats.
Open source	• Mises à jour fréquentes, notamment grâce à la communauté active soutenant le développement du produit. • Indépendance des fournisseurs : Il n'y a pas de délais ou de cahier des charges à respecter forçant à faire l'impasse sur des problèmes apparents ou évidents. • Respect des standards facilitant la compatibilité entre les différentes solutions. • Pas de coût d'acquisition : Les solutions sont distribuées librement et restent accessibles à tous en tout temps.	• Le support, principalement communautaire, reste difficile d'y accéder ou inexistant pour certaines technologies émergentes ou peu populaires.

TABLE II.1 – Avantages et inconvénient des solutions de la supervision.

II.9.1 Pourquoi le choix des solutions open sources ?

Pour des raisons financières avancées par ma hiérarchie, l'achat d'une ou plusieurs licences de logiciels propriétaires se voit écarté malgré les solutions confortables proposées, avec des atouts tels que le support et la maintenance au profit de l'amélioration du matériel et des solutions déjà en place.

De mon point de vue, cette décision est raisonnable, car il ne faut pas négliger que le principal atout de ces solutions open sources sont certes la gratuité, mais aussi bel et bien les existantes communautés sur lesquelles s'appuient ces solutions. Universitaires, développeurs, professionnels tous s'associent désormais et forment les primordiaux contributeurs du monde Open Source. Mieux encore, les développeurs de logiciels propriétaires se séparent de leurs antécédentes entreprises dans le but d'ouvrir leurs propres solutions libres.

De plus il est assez fréquent, de se retrouver confronté à des difficultés lorsqu'on débute et si malgré tout on ne trouve pas de réponse dans la documentation officielle de la solution, alors il est possible avec une simple recherche sur Internet, en passant par un moteur de recherche (google.fr, yahoo.fr, bing.fr etc.), réseau social (Discord, Facebook, etc.) ou une recherche vidéo (exposant les manipulations à faire), de trouver une réponse à notre problème, grâce à une communauté très réactive.

Enfin ces solutions qui ont vu le jour et qui sont testées nombre de fois avec des correctifs fréquents, sont totalement crédibles, offrent une modularité (plugins, etc.) et une compatibilité totale. En effet, fini le problème des protocoles propriétaires, les normes sont adoptées et respectées, ce qui permet d'établir une certaine agilité et donc cela autorise l'hétérogénéité du matériel à acheter.

II.9.2 Contrainte des solutions open sources

En adoptant une telle solution, on ne distingue qu'un seul et véritable obstacle, l'obligation constante de demeurer averti sur la technologie. Il faudra régulièrement se rendre sur les forums, les blogs tout ce qui est capable de raisonner l'aspect communautaire, et ainsi d'ouvrir des réponses aux questions posées. Cet échange de bonne méthode permet de mettre à jour fréquemment les solutions et de les adapter en fonction du besoin utilisateur.

II.9.3 Comparaisons des différentes solutions Open sources testées

A. **Zabbix et Cacti**

- Zabbix offre une interface unifiée, avec des fonctions avancées. La partie métrologie présente vraiment des notions intéressantes (graphes complexes de mesures, etc.), malheureusement sa prise en main n'est pas assez intuitive en plus des problèmes de dépendances lors de son installation. Ce qui le rend moins agréable que Centreon par exemple.
- Il s'avère qu'au final Cacti soit un outil de métrologie, même s'il arbore un aspect de supervision, il n'est pas assez développé malheureusement pour conduire à son choix. Après utilisation, ils ont trouvé que

son interface graphique contre-intuitive. Malgré l'effort des développeurs pour améliorer l'interface utilisateur de leur nouvelle version, on dénote toutefois un problème de compatibilité des templates entre les différentes versions du logiciel.

B. **Et donc Centreon ou Nagios ?**

Après quelques recherche sur Nagios et Centreon , ci-dessous les points qu'on peut relever :

- La configuration de Nagios en ligne de commande est actuellement lourde et peu intuitive. Intervient alors l'interface web de Centreon qui apporte un réel atout par rapport à la configuration en ligne de commande Nagios.
- Le problème avec Nagios est que pour bénéficier de ses fonctionnalités avancées, il faut soit intégrer un composant Open Source (PNP4 Nagios, etc.) ou prendre la version payante de Nagios (Nagios XI) qui a un certain coût financier. Ces fonctionnalités avancées comme la génération de graphes est disponible gratuitement sur Centreon.
- Centreon est une entreprise française et propose une documentation officielle complète française.

II.10 Solution retenue : Centreon

Ce qui est admirable avec Centreon est qu'il consomme très peu de ressources et qu'il possède un iso qui est déjà pré-packagé. Grâce à un iso déjà opérationnel, on se retrouve avec un serveur de monitoring dans une solution complète et maintenue au sein d'un même package. L'intérêt est bien entendu de déployer rapidement les outils nécessaires à notre supervision vis-à-vis de notre infrastructure.

L'éditeur français a voulu que Centreon soit une solution de monitoring open source complète, prête à l'emploi, facile à déployer : On télécharge et installe l'image ISO et on monitore immédiatement avec des tableaux de bord comprenant de multiples widgets qui nous renseignent en temps réel de la disponibilité et de la performance de notre SI. Ceci est possible quel que soit le nombre d'équipements à monitorer, qu'ils soient situés dans le même data center ou répartis géographiquement.

Rappelons aussi qu'à la base, Centreon est une surcouche de Nagios même si Centreon possède son propre moteur de monitoring, il est encore possible même sur les dernières versions d'utiliser l'ordonnanceur Nagios. Par ce fait, on peut profiter des deux communautés (Nagios et Centreon), ce qui nous offre un large choix de fonctionnalités et une communauté encore plus vaste.

Notre choix s'est donc porté sur Centreon, afin de bénéficier d'un monitoring complet, avec des possibilités de supervision et métrologie, les générations de configurations automatiques, et son interface intuitive en font un outil de choix à mettre en place.

II.11 Conclusion

Le présent chapitre a été consacré à la présentation détaillée de la notion de supervision, ses enjeux et ses outils propriétaires et open sources afin de choisir le bon outil. Après avoir effectué le choix de l'outil de supervision open source convenable, nous passons à son installation information et sa mise en place en œuvre dans le chapitre suivant.

Chapitre III

Mise en place et fonctionnement du système de supervision

III.1 Introduction

Dans ce chapitre, nous mettrons en évidence une présentation assez exhaustive de l'outil de supervision Centreon tout en donnant beaucoup plus ample informations sur sa mise en œuvre, sur l'environnement de test et sur l'environnement de distribution d'INSIM Bejaia. A la fin du chapitre, nous ferons un récapitulatif des différents coûts de déploiement.

III.2 Environnement de travail

Il existe deux types d'environnement :

III.2.1 Environnement matériel

Afin de mener à bien notre travail, nous avions eu besoin d'un environnement de travail assez convivial. Ainsi les ressources qui étaient présentes sont les suivantes : Le tableau III.1 regroupe les ressources matérielles mises à notre disposition tout au long du déroulement du stage.

Désignation	Caractéristiques
Ordinateur portable Dell	Dual Core, RAM 4GO, HDD 500GO
Ordinateur portable HP	Peintium 4, RAM 2 GO, 500 GO

TABLE III.1 – Ressources matérielles .

III.2.2 Environnement logiciel

Après avoir présenté l'environnement matériel de développement, nous allons rappeler et justifier brièvement les choix techniques que nous avons adoptés. Le tableau III.2 regroupe les ressources logicielles utilisées :

Nom du Logiciel	Éditeur	Licence	Fonction
VMware Workstation	VMware	Gratuit	Outil de virtualisation de poste de travail, utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation.
PuTTY	PuTTY	Gratuit	un émulateur de terminal UNIX qui permet de se connecter à distance à une machine ou un serveur, en utilisant les protocoles SSH, Telnet ou Rlogin.
Mozilla Firefox	Mozilla Fondation	Gratuit	Navigateur web libre permettant d'effectuer des recherches sur internet.

TABLE III.2 – Ressources logicielles .

III.3 Environnement de mise en place

- **Phase de test :** Au cours de cette phase, on a installé une machine virtuelle sur une machine personnelle pour tester la solution choisie et s'adapter à sa mise en place, mais aussi s'assurer si elle répond vraiment aux buts fixés, en essayant de tester deux serveurs distants Windows et Linux.
- **Phase d'installation :** Dans cette installation on va montrer comment installer et configurer Centreon . Pour finaliser cette installation on va ajouter deux hôtes (Windows, Linux) que le serveur Centreon supervisera. Pour réaliser cette maquette, il nous faudra une machine physique équipée de VMware Workstation et deux machines virtuelles qui comprendront un serveur Centreon , une machine Linux ainsi que notre machine physique qui est sous Windows 10.

III.4 Mise en place de la solution

III.4.1 Configuration de la machine virtuelle

Centreon fournit une machine virtuelle prête à l'emploi. Cette machine virtuelle est disponible au format OVA pour les environnements VMware et pour l'outil Oracle VirtualBox. Elle est basée sur le système d'exploitation Linux CentOS 7 et inclut une installation de Centreon permettant de démarrer en toute simplicité notre première supervision. La machine hôte doit avoir les caractéristiques suivantes :

- **Processeur :** Tout processeur Intel ou AMD récent avec au moins 2vCPU.
- **Mémoire :** Selon notre système d'exploitation, nous aurons besoin d'au moins 1 Go de RAM. Pour profiter pleinement de l'expérience, nous avons besoin d'au moins 2 Go de mémoire libre.
- **Espace disque :** La machine virtuelle nécessite au moins 6,5 Go d'espace libre sur notre disque dur. Cependant, si nous souhaitons continuer à utiliser Centreon, il est recommandé d'avoir au moins 10 Go car sa taille augmentera au fil du temps.

III.4.2 Installation Centreon (Annexe A)

Pour l'installation de Centreon, il est recommandé de vérifier que certaines dépendances soient autorisées sur la machine :

1. Vérifions que notre solution de virtualisation (VMWare) est installée sur notre machine et à jour.
2. Aller sur la page de téléchargement de Centreon. Dans la section 1, Appliances est sélectionné par défaut.
3. Dans la section 2, nous sélectionnons la version de Centreon désirée.
4. Dans la section 3, télécharger ton image, cliquez sur le bouton Download à côté de VMWare Virtual Machine (OVA). Une nouvelle page apparaît.
    - Si nous souhaitons être contacté par Centreon, nous entrons nos informations de contact, puis cliquer sur Download.
    - Dans le cas contraire, cliquer sur Direct download.
5. Le fichier téléchargé est une archive compressée : extrayer son contenu dans le répertoire désiré.

III.4.3 Architecture de Centreon

La figure III.1 représente un schéma de notre serveur de monitoring simple car on associe tous les modules de Centreon dans un unique serveur.

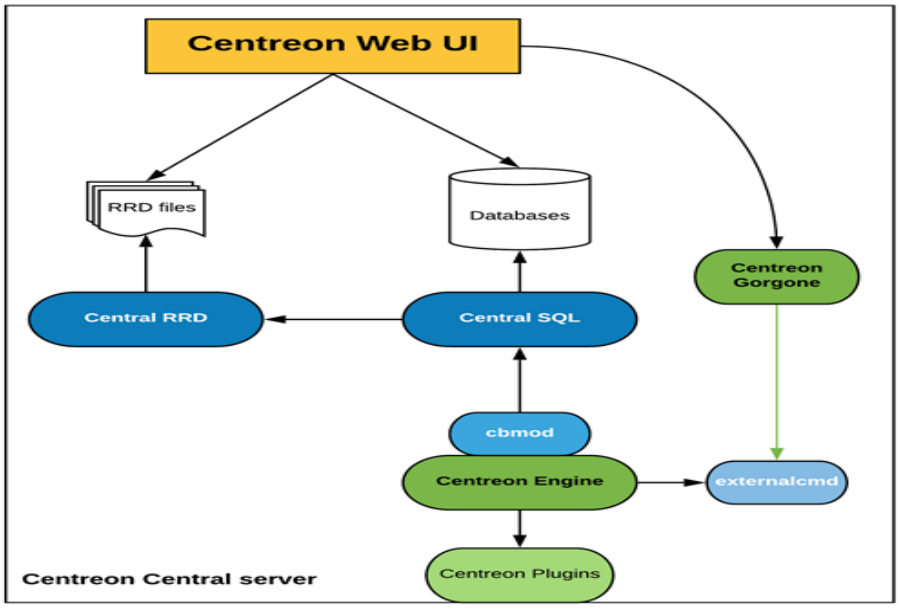


FIGURE III.1 – Serveur Centreon.

Plusieurs entités servent à mettre en place cette architecture :

- Le serveur Apache est chargé d'héberger l'interface web de Centreon.
- Plusieurs bases de données MariaDB sont chargées de stocker la configuration de Centreon, les informations de supervision ainsi que les données de performances.
- Le moteur de supervision supervise le système d'informations .
- Les informations de supervision sont envoyées via cbmod à Centreon Broker SQL.
- Centreon Broker SQL est chargé d'insérer les données de supervision en base de données et de transmettre les données de performances à Centreon Broker RRD.
- Centreon Broker RRD est chargé de générer les fichiers RRD (qui servent à générer les graphiques de performances) .

III.4.4 Interfaces de l'application

L'application développée est destinée à des administrateurs de réseaux, elle permet de réaliser des tests sur les machines distantes pour vérifier s'ils sont en fonction. D'abord, l'administrateur doit s'authentifier en entrant son login et son mot de passe (figure III.2), préconfiguré lors de l'installation et la configuration de centreon, pour accéder à la page d'accueil de Centreon via l'adresse IP « localhost/centreon/ ».

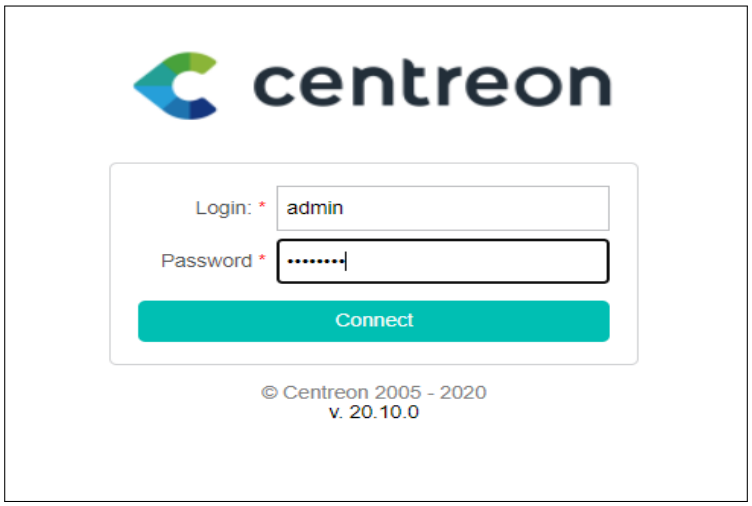


FIGURE III.2 – Interface d'identification de Centreon.

La première vue après authentification est présentée dans la figure III.3 . Elle donne une idée générale sur l'état de fonctionnement des hôtes ainsi que les services qui leur sont associés.

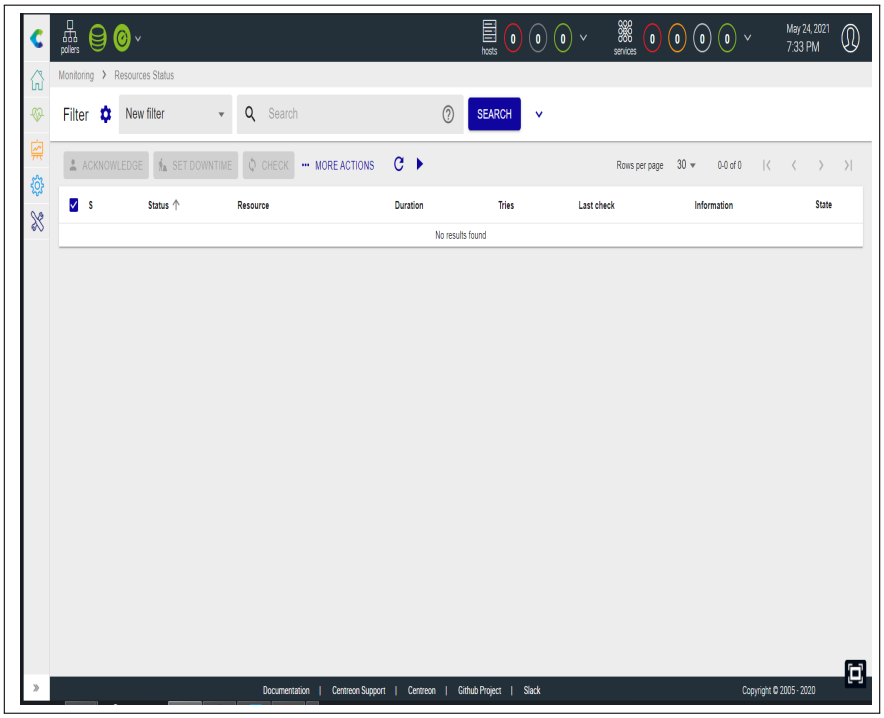


FIGURE III.3 – Page d'accueil après authentification.

L'interface web de Centreon est composée de plusieurs menus, chaque menu a une fonction bien précise (figure III.4) :

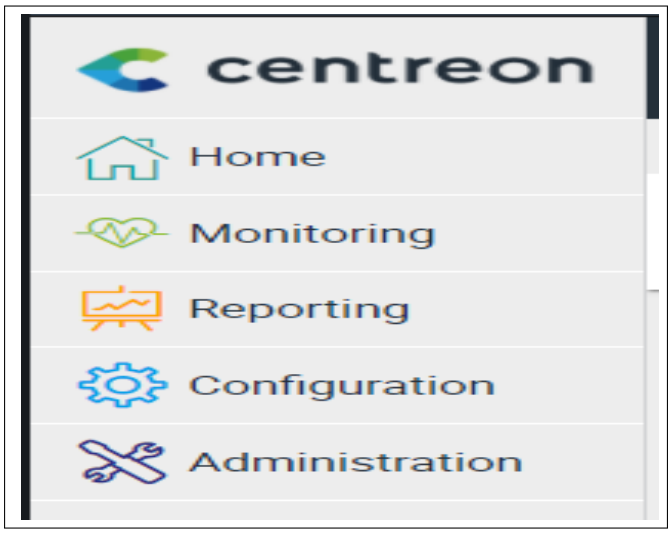


FIGURE III.4 – Menu de Centreon.

- Le menu **Home** permet d'accéder au premier écran d'accueil après s'être connecté. Il résume l'état général de la supervision. Notre espace de travail peut être vide pour l'instant. Une fois que nous avons configuré les widgets personnalisables, nous visualisons les données et les graphiques en fonction de notre personnalisation.
- Le menu **Monitoring** regroupe l'état de tous les éléments supervisés en temps réel et en différé au travers de la visualisation des logs.
- Le menu **Reporting** permet de visualiser de manière intuitive (via des diagrammes) l'évolution de la supervision sur une période donnée.
- Le menu **Configuration** permet de configurer l'ensemble des éléments supervisés ainsi que l'infrastructure de supervision.
- Le menu **Administration** permet de configurer l'interface web Centreon ainsi que de visualiser l'état général des serveurs.

Ainsi, superviser un hôte avec Centreon consiste à configurer l'ensemble des commandes nécessaires à la mesure des indicateurs désirés, puis à déployer cette configuration sur le moteur de collecte afin que ces commandes soient exécutées périodiquement.

Néanmoins, pour simplifier drastiquement la configuration on s'appuiera avantageusement sur des modèles de supervision :

- Un modèle d'hôte (host template en anglais) définit la configuration des indicateurs pour un type d'équipement donné.
- Il s'appuie sur des modèles de service (service templates) qui définissent la configuration des commandes nécessaires à la mesure de ces indicateurs.
- Centreon fournit des Plugins Packs téléchargeables à installer sur sa plateforme de supervision : chaque Plugin Pack regroupe des modèles d'hôtes et des services pour configurer en quelques clics la supervision d'un équipement particulier.

III.4.5 Plugin Pack

Un Plugin Pack est un jeu téléchargeable de modèles de configuration qui permet un déploiement rapide de la supervision de notre infrastructure IT. Les Plugin Packs sont le moyen le plus simple de mettre un hôte en supervision. Un Plugin Pack est constitué de deux éléments, installés séparément **[23]** :

- Un plugin, qui exécute les commandes de supervision depuis un collecteur. Il est installé en ligne de commande.
- Un pack, qui contient des commandes, des modèles de services et des modèles d'hôtes. Il est installé via l'interface de Centreon. Pour chaque type d'équipement, les modèles déterminent quels indicateurs seront supervisés et définissent les valeurs par défaut des seuils Warning et Critical.

III.4.6 Configuration du SNMP dans divers hôtes

SNMP est un protocole de couche application qui fournit un format de message pour la communication entre les gestionnaires et les agents. Il permet aussi de superviser plusieurs appareils de différentes marques (figure III.5). La configuration d'un agent SNMP sur les périphériques se diffère d'un périphérique à un autre.

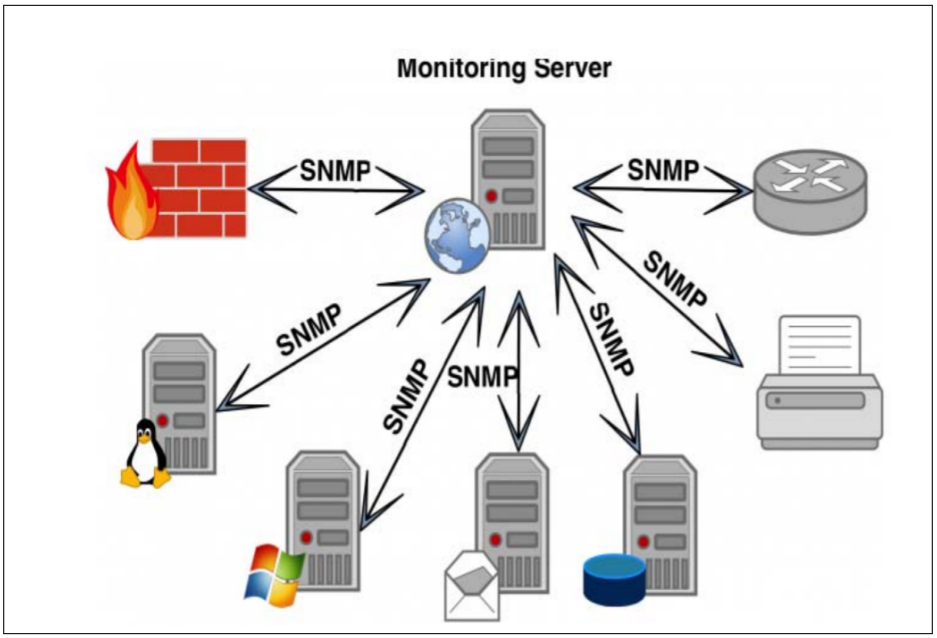


FIGURE III.5 – Configuration SNMP dans divers hôtes .

A. **Configuration de SNMP dans SOPHOS**

Si on souhaite superviser avec centreon le firewall à l'aide du service SNMP, il faut activer et configurer l'agent sur le pare-feu.

1. Depuis l'interface d'administration, aller à ***Administration/ SNMP***. Cocher la case pour activer l'agent, saisir les informations puis cliquer sur Appliquer (figure III.6).

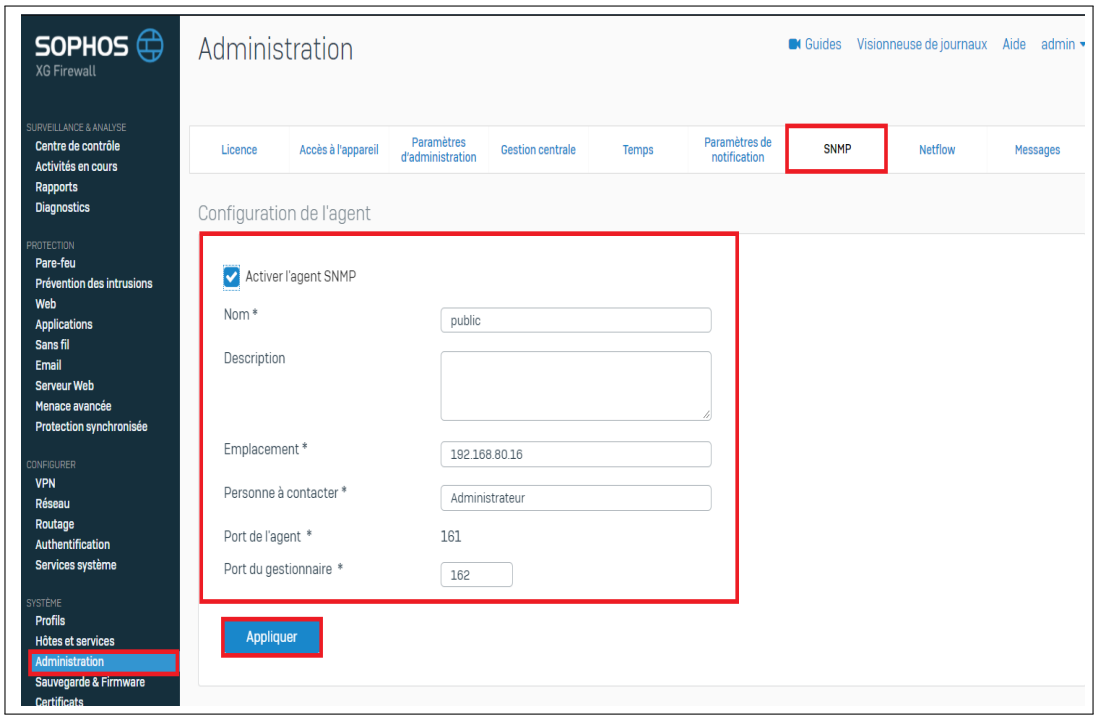


FIGURE III.6 – Configuration de l'agent SNMP dans Sophos.

2. Une fois l'agent activé, cliqué sur le bouton ***Ajouter*** pour déclarer une communauté (figure III.7).

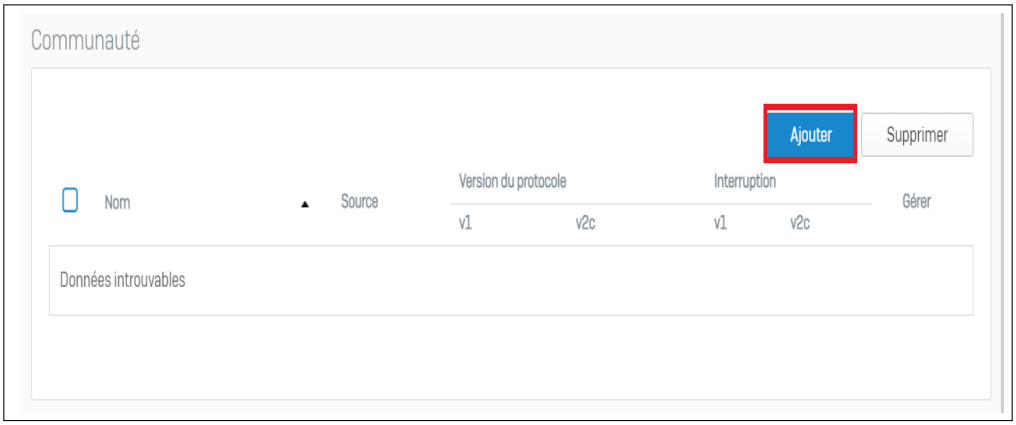


FIGURE III.7 – Ajout d'une communauté .

3. Entrer le nom de la communauté SNMP, l'adresse IP du serveur, sélectionner la version et cliquer sur Enregistrer (figure III.8).

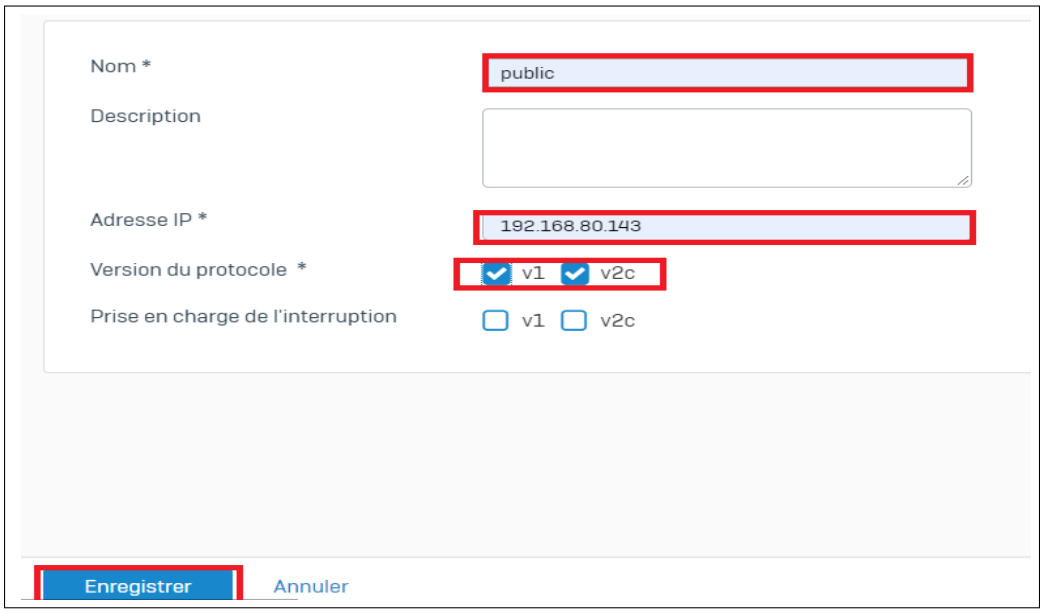


FIGURE III.8 – Information de la communauté.

4. La communauté est ajoutée (figure III.9).

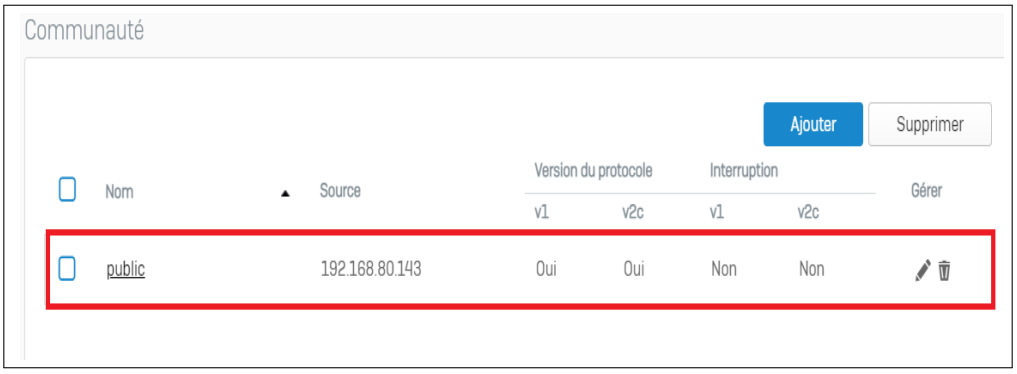


FIGURE III.9 – Communauté ajouté .

A ce niveau, il ne reste plus qu'à configurer Centreon.

B. **Configuration de SNMP dans windows server 2016**

Si on souhaite superviser avec centreon la machine windows server 2016 à l'aide du service SNMP, il faut activer et configurer l'agent sur le windows server 2016.

1. Depuis le gestionnaire du serveur, cliquer sur ***Gérer*** puis sur ***ajouter des rôles et fonctionnalités*** (figure III.10).

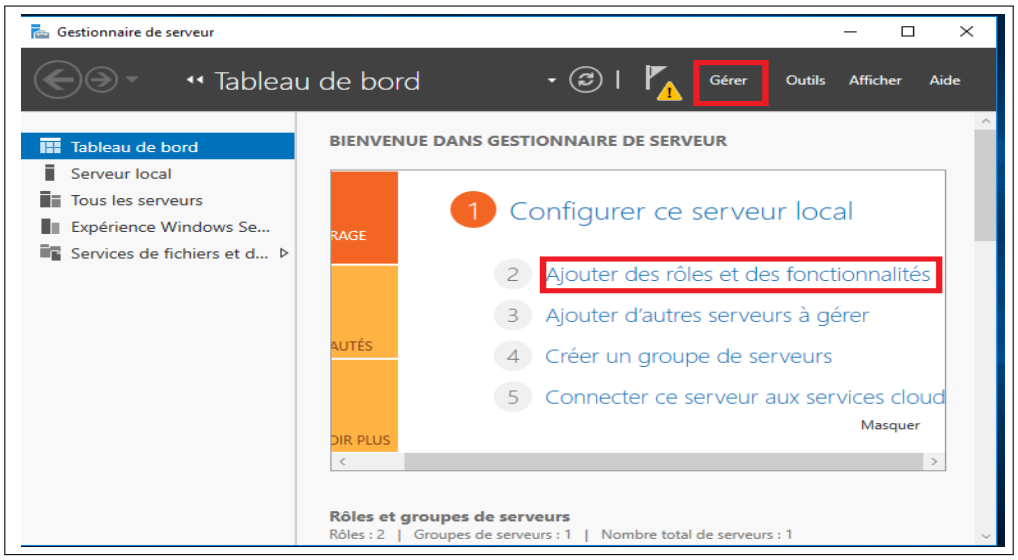


FIGURE III.10 – Tableau de bord de gestionnaire de serveur .

2. À l'ouverture de l'assistant, cliquer sur ***Suivant*** (figure III.11).

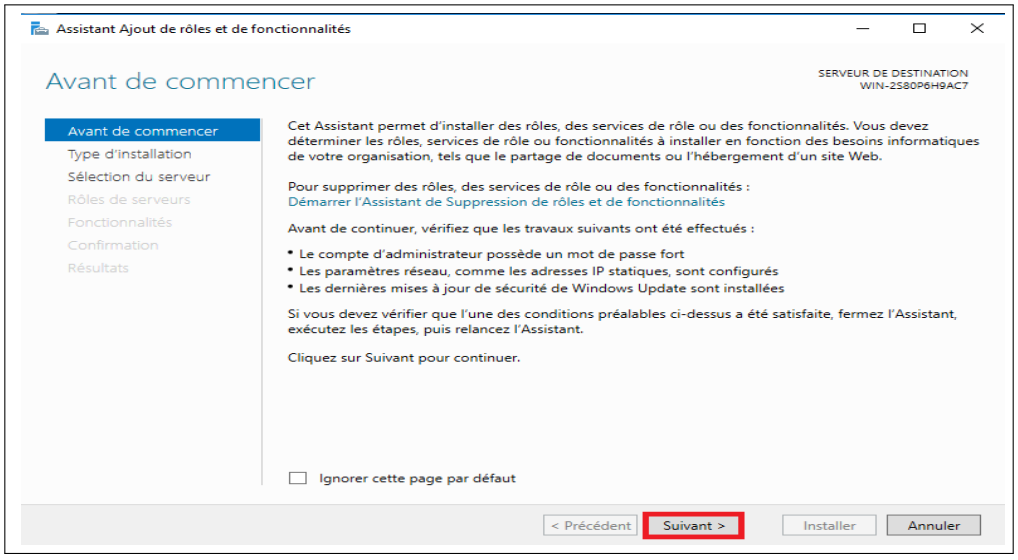


FIGURE III.11 – Assistant ajout des rôles et de fonctionnalité .

3. Sélectionner ***Installation basée sur un rôle ou une fonctionnalité*** et cliquer sur le bouton ***Suivant*** (figure III.12).

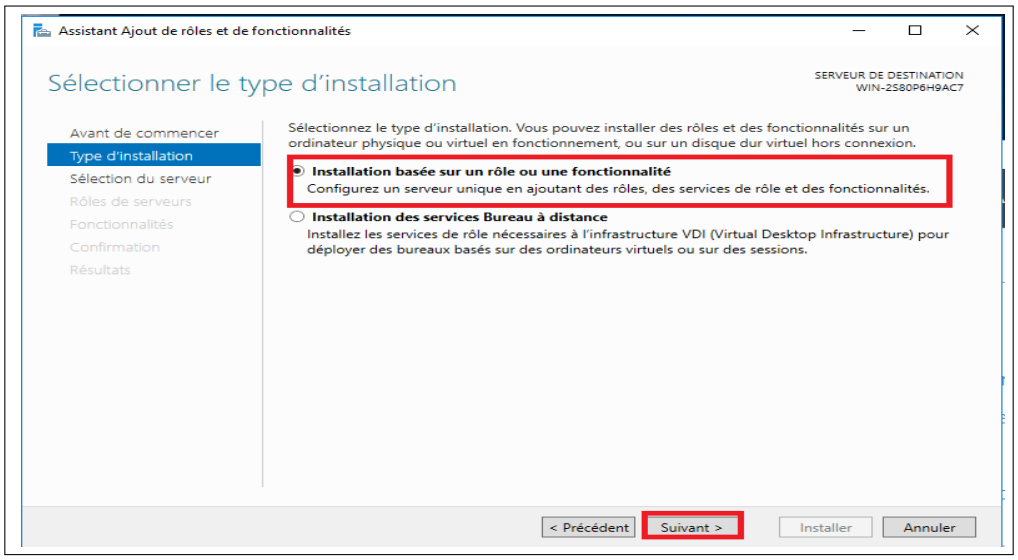


FIGURE III.12 – Type d'installation .

4. Sélectionner le serveur et cliquer sur ***Suivant*** (figure III.13).

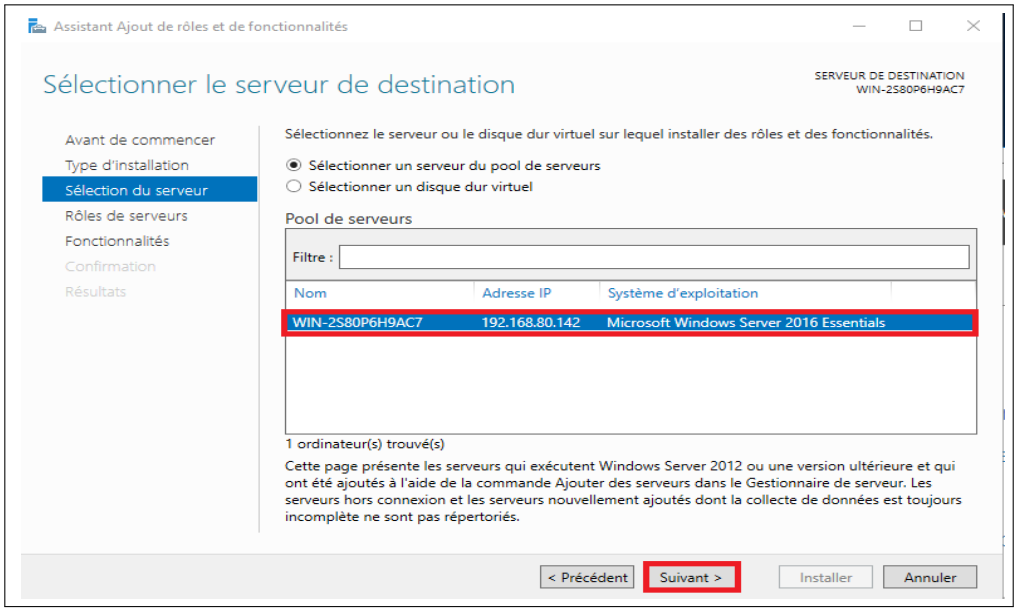


FIGURE III.13 – Serveur de destination .

5. Sur la liste des ***fonctionnalités***, chercher ***Service SNMP*** et cocher la case, confirmer l'installation en appuyant sur le bouton ***Installer***. Une fois l'installation terminée, cliquer sur ***Fermer***.

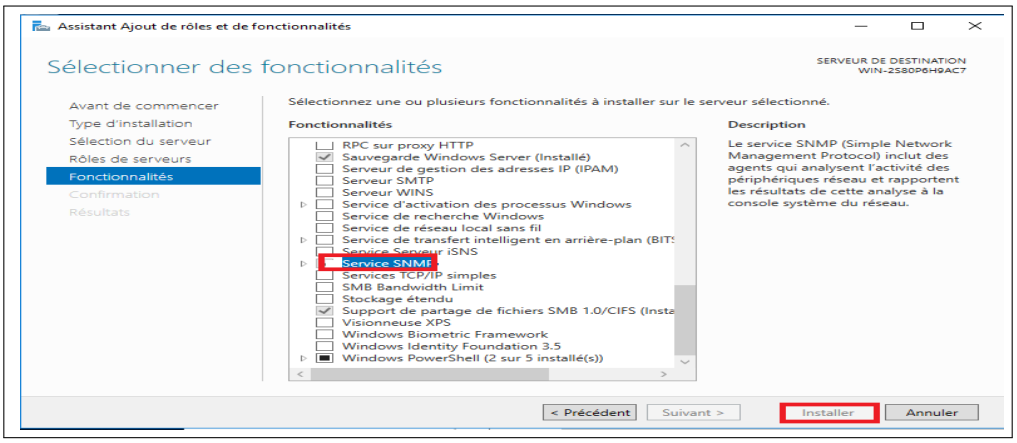


FIGURE III.14 – Installation de service SNMP .

On va maintenant passer à la configuration du service. Pour cela nous allons ajouter une communauté au service SNMP pour permettre son interrogation.

1. Ouvrir une fenêtre exécuter, dans la zone de saisie, entrer ***services.msc*** et cliquer sur ***OK*** (figure III.15).

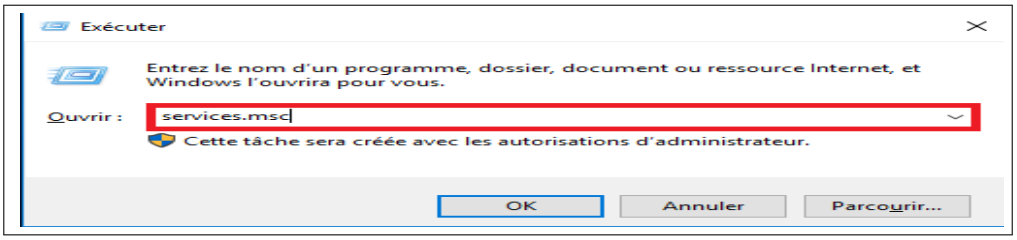


FIGURE III.15 – Services .

2. Dans la liste des services chercher ***Service SNMP***, faire un clic droit dessus et aller sur ***Propriétés*** (figure III.16).

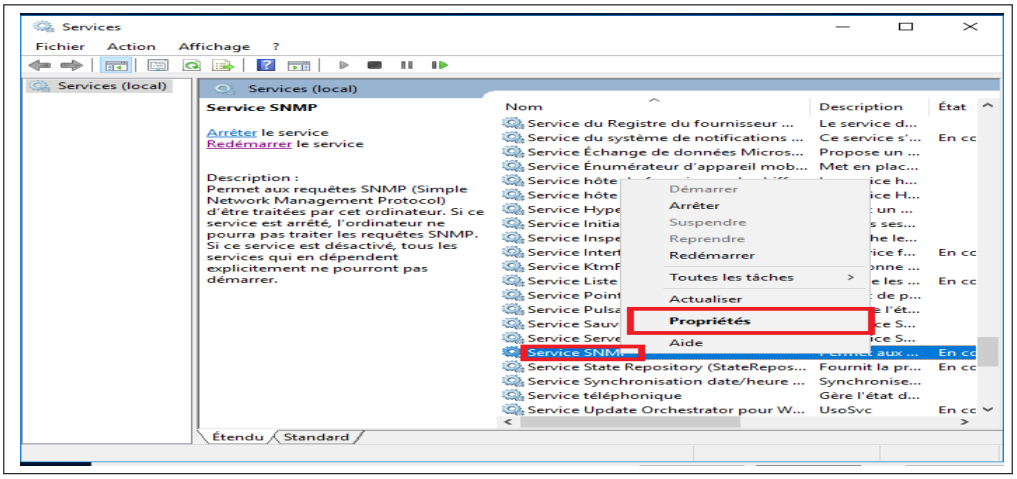


FIGURE III.16 – Service SNMP .

3. Dans la nouvelle fenêtre, aller sur l'onglet ***Sécurité*** et cliquer sur le bouton ***Ajouter*** au niveau de la liste des communautés (figure III.17).

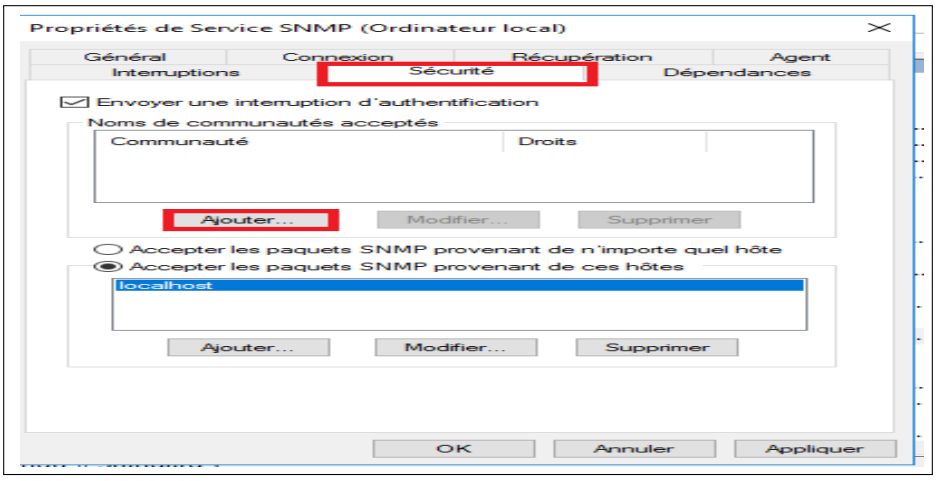


FIGURE III.17 – Propreté de service SNMP .

4. Sélectionner le droit de la communauté, entrer son nom et cliquer sur le bouton ***Ajouter*** (figure III.18).

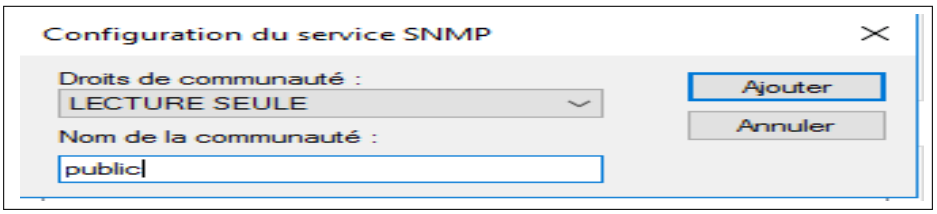


FIGURE III.18 – Communauté de SNMP.

5. Sélectionner ***Accepter les paquets SNMP provenant de ces hôtes***, Appliquer les modifications et cliquer sur ***OK*** pour fermer la fenêtre. Par la suite indiquer les adresses IP autorisées à interroger le serveur centreon et redémarrer le service (1) pour une prise en compte des modifications (figure III.19).

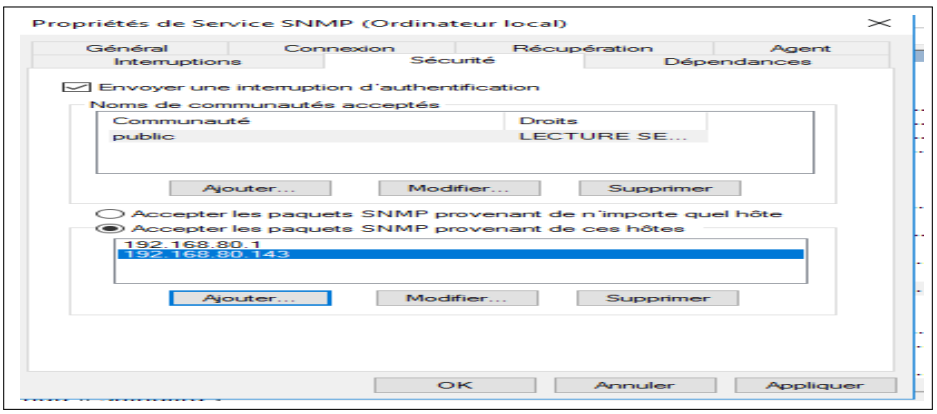


FIGURE III.19 – Interrogation du serveur centreon .

III.4.7 Diagramme d'utilisation générale du système

Afin de décrire les fonctionnelles de notre système, une description du cas d'utilisation globale est donnée dans la figure III.20.

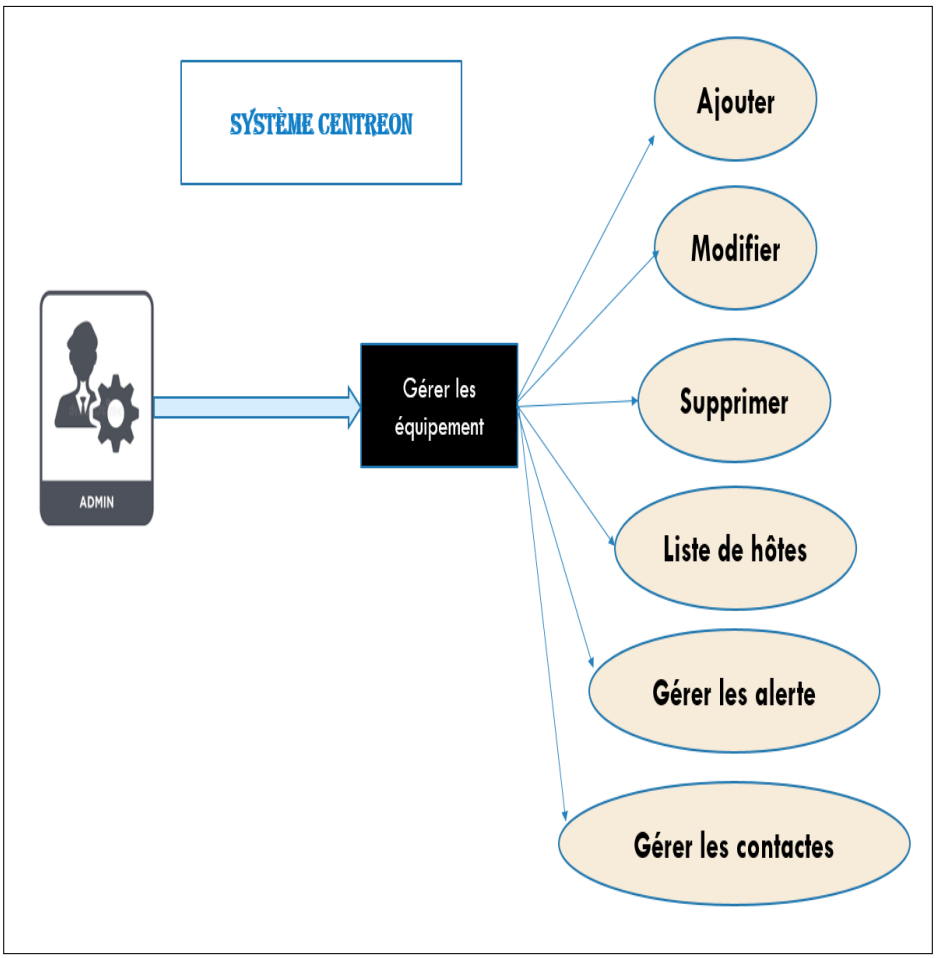


FIGURE III.20 – Diagramme de cas d'utilisation générale du système.

III.4.8 Diagramme d'activité « d'alerte »

Ce diagramme (figure III.21) décrit les différentes activités que prend le système lorsqu'il détecte un équipement non fonctionnel ou en panne.

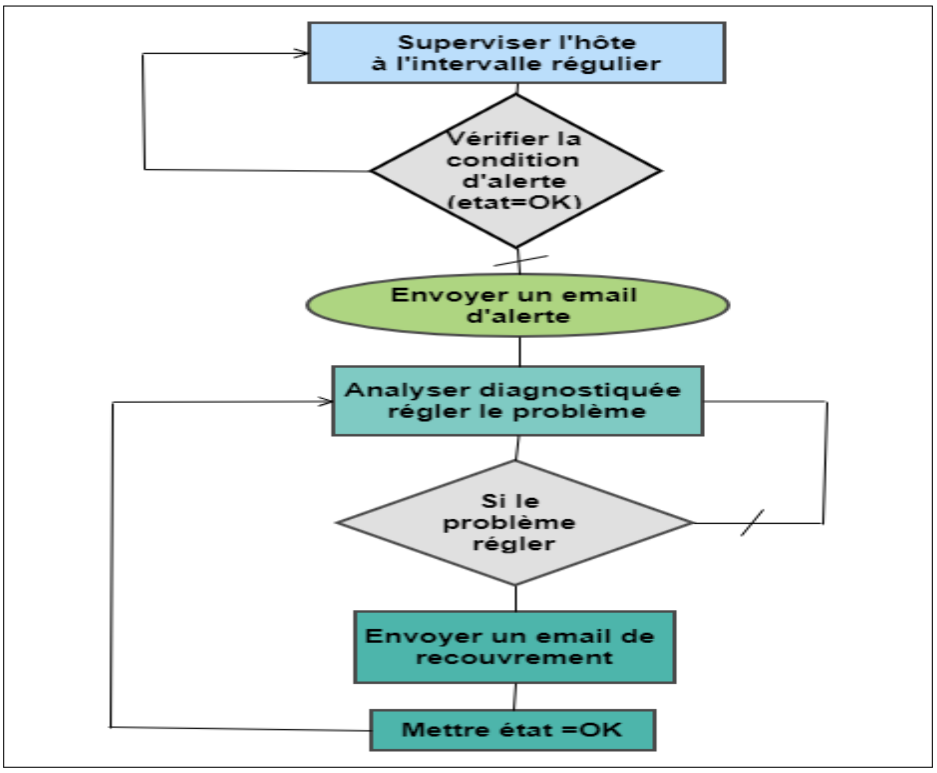


FIGURE III.21 – Diagramme d'activité « d'alerte ».

III.5 Centreon Auto Discovery

Auto Discovery est un module qui permet la découverte dynamique de machines : Centreon AutoDiscovery. Ce plugin est présent dans l'offre Centreon EPP de l'éditeur et permet de :

- Découvrir dynamiquement de nouveaux hôtes,
- Découvrir les points de supervision manquants sur un hôte.

Ce module se base sur trois composants :

- L'interface web pour la découverte et la création de services en lien avec le binaire Centreon .
- Les sondes de découverte.
- Les crons qui permettent d'effectuer une découverte automatisée.

III.6 Configurations nécessaires

Dans cette partie, nous montrerons comment configurer les hôtes,les services et les contacts . On commencera par une configuration globale, ensuite nous montrerons les configurations pour des types de supervision déjà étudiés.

III.6.1 Configuration des hôtes

Un hôte est toute entité possédant une adresse IP correspondant à une ressource du système d'informations. Exemples : Un serveur, une imprimante réseau, un serveur NAS, une base de données, une sonde de température, une caméra IP,...etc.

1. Initialement pour l'ajout d'un hôte , nous devons nous connecter à l'interface web Centreon avec un compte administrateur ou un compte disposant des droits d'accès pour gérer les objets, ensuite se rendre dans le menu ***Configuration > Hosts > Hosts*** et cliquer sur le bouton ***Add*** (figure III.22) :

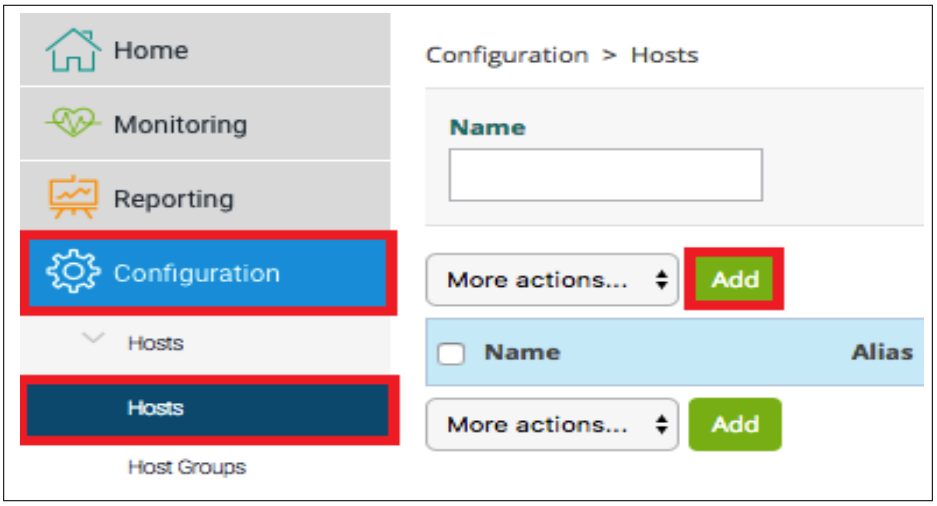


FIGURE III.22 – Configuration d'un hôte .

2. Accéder à un formulaire permettant de définir notre équipement. En remplissant les champs du premier formulaire indiqué dans la figure III.23 :

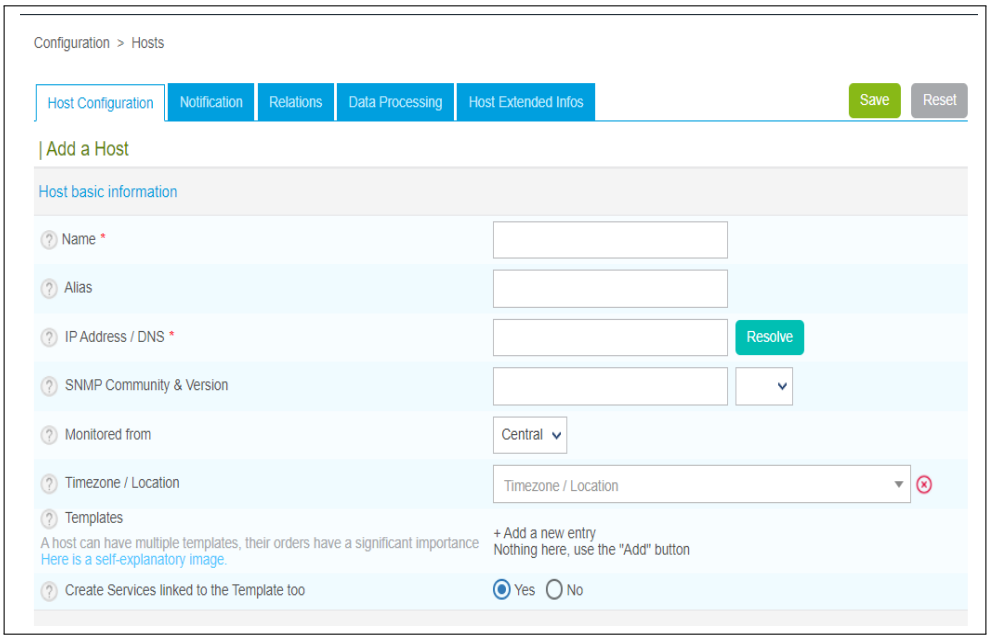


FIGURE III.23 – Formulaire d'ajout d'un hôte (1ère partie) .

Pour démarrer on rempli les champs suivants :

- Le champ **Host Name** définit le nom d'hôte qui sera utilisé par le moteur de supervision.
- Le champ **Alias** indique l'alias de l'hôte.
- Le champ **IP address / DNS** Adresse IP ou nom DNS de l'hôte. Le bouton Resolve permet de résoudre le nom de domaine en interrogeant le serveur DNS configuré sur le serveur central.
- Les champs **SNMP Community & Version** contiennent respectivement le nom de la communauté ainsi que la version SNMP.
- Le champ **Monitored** from indique quel est le serveur de supervision chargé de superviser cet hôte.
- Le champ **Timezone / Location** indique l'emplacement du fuseau horaire des hôtes surveillés.
- Le champ **Host Templates** permet d'associer un ou plusieurs modèles d'hôtes à cet objet.

La figure III.24 représente la 2eme partie du formulaire d'ajout d'un hôte :

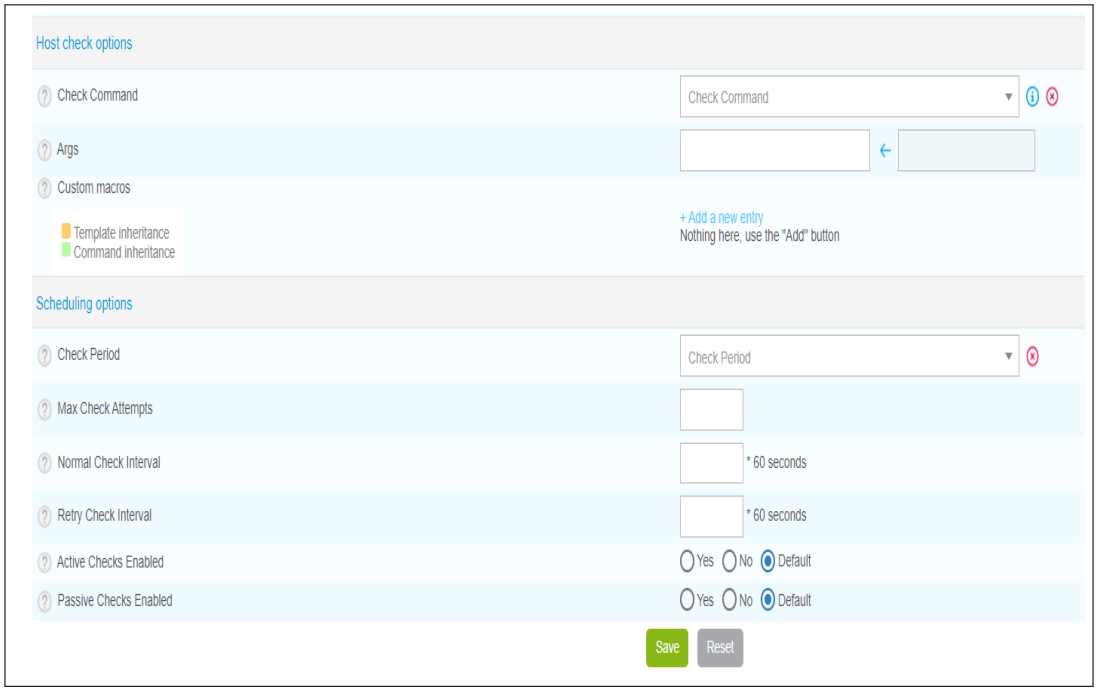


FIGURE III.24 – Formulaire d'ajout d'un hôte (2éme partie) .

La figure III.24 contient les champ suivante :

- Le champ Check Command indique la commande utilisée pour vérifier la disponibilité de l'hôte.
- Le champ Args définit les arguments donnés à la commande de vérification (chaque argument commence avec un "!").

La partie Macros permet d'ajouter des macros personnalisées.

- Les champs Macro name et Macro value permettent respectivement de définir le nom et la valeur de la macro.

- La case Password permet de cacher la valeur de la macro.
  - Pour réinitialiser la macro avec sa valeur par défaut (définie dans le template) cliquez sur
  - Pour afficher la description de la macro, cliquez sur
  - Pour supprimer la macro, cliquez sur
  - Pour déplacer l'ordre des macros, cliquez sur
- Le champ **Check Period** définit la période temporelle durant laquelle l'ordonnanceur vérifie le statut de l'objet.
- Le champ **Max Check Attempts** définit le nombre de contrôles à effectuer avant de valider le statut de l'hôte : lorsque le statut est validé, le processus de notification est enclenché.
- Le champ **Normal Check Interval** est exprimé en minutes. Il définit l'intervalle entre chaque vérification lorsque le statut de l'hôte est OK.
- Le champ **Retry Check Interval** est exprimé en minutes. Il définit l'intervalle de validation du statut non-OK de l'hôte.
- Les champs **Active Checks Enabled** et Passive Checks Enabled activent / désactivent les contrôles actifs et passifs.

A. Configuration de windows server 2016

1. On accède à un formulaire permettant de décrire notre équipement. Nous remplirons les champs de la figure III.25, puis on clique sur bouton ***Save*** :

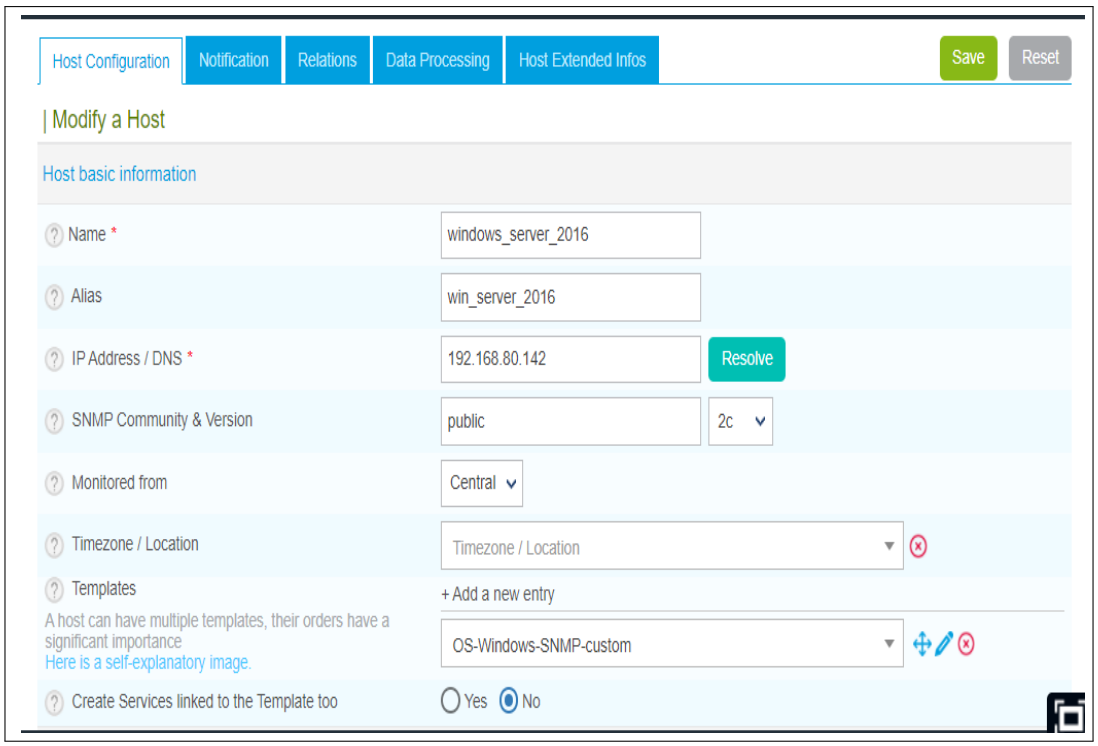


FIGURE III.25 – Configuration de windows server 2016 .

Sauvegarder les modifications en cliquant sur le bouton ***Save***.

2. L'hôte est maintenant défini dans l'interface Centreon web (figure III.26) mais le moteur ne le connaît pas encore !

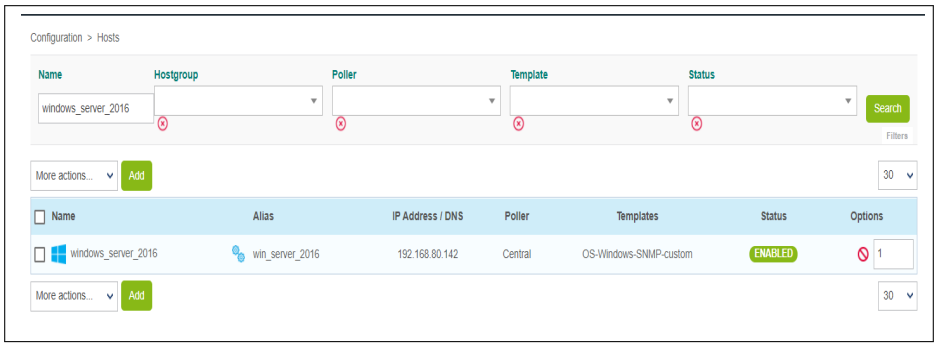


FIGURE III.26 – Hôte défini dans l'interface Centreon web .

3. Le résultat est visible dans le menu ***Monitoring > Status Details > Hosts*** (figure III.27) :

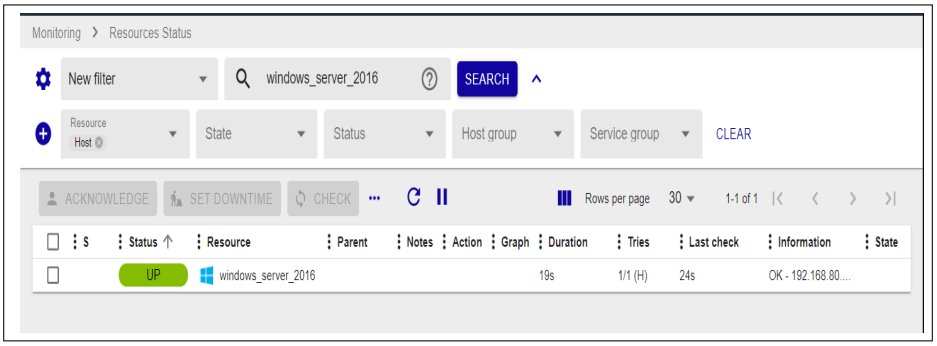


FIGURE III.27 – Résultat de l'ajout windows server 2016 .

B. Configuration de windows 10

1. On accède à un formulaire permettant de décrire notre équipement. Nous remplirons les champs sur la figure III.28 :

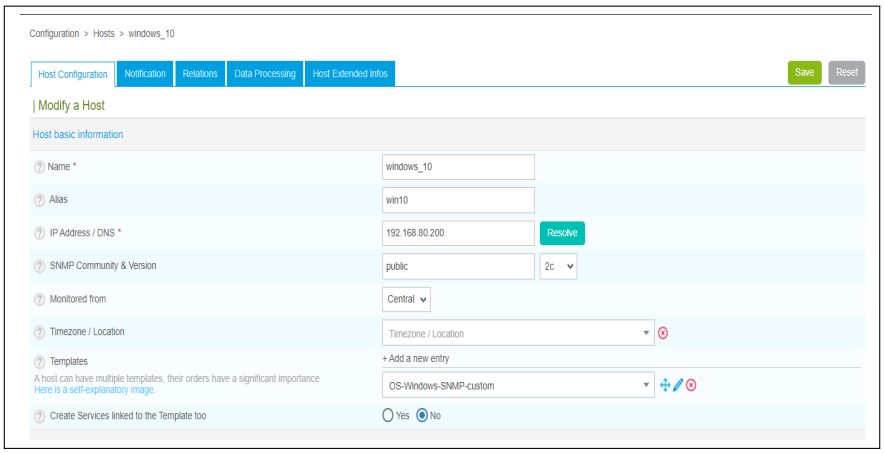


FIGURE III.28 – Configuration de windows 10 .

Sauvegarder les modifications en cliquant sur le bouton *Save*.

2. L'hôte est maintenant défini dans l'interface Centreon web (figure III.29) mais le moteur ne le connaît pas encore !

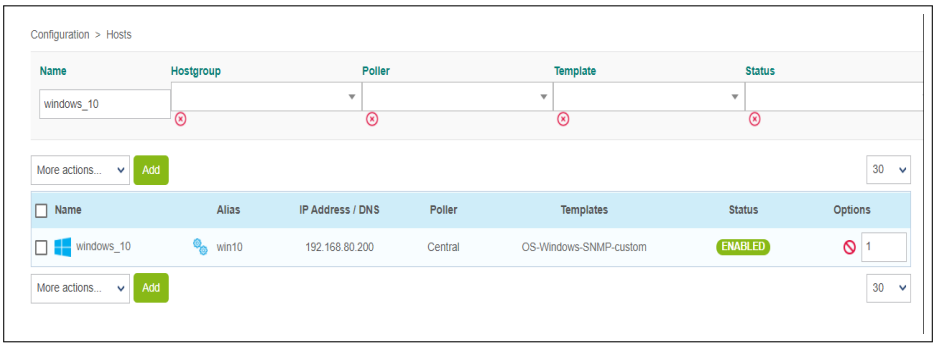


FIGURE III.29 – Windows 10 défini dans l'interface Centreon web .

3. Le résultat est visible dans le menu ***Monitoring > Status Details > Hosts*** (figure III.30) :

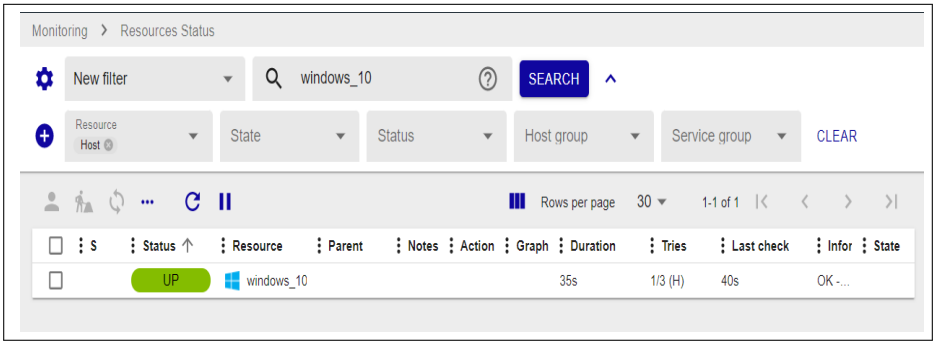


FIGURE III.30 – Résultat de l'ajout de windows 10 .

C. Configuration de SOPHOS XG

1. Comme on l'a décrit précédemment, on accède à un formulaire permettant de décrire notre équipement .Nous remplirons les champs sur la figure III.31 :

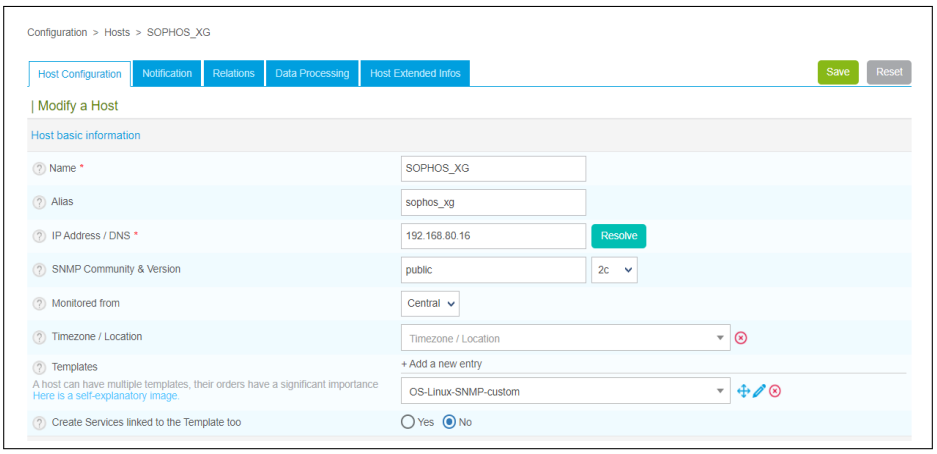


FIGURE III.31 – Configuration de SOPHOS XG .

Sauvegarder les modifications en cliquant sur le bouton ***Save***.

2. L'hôte est maintenant défini dans l'interface Centreon web mais le moteur ne le connaît pas encore !(figure III.32)

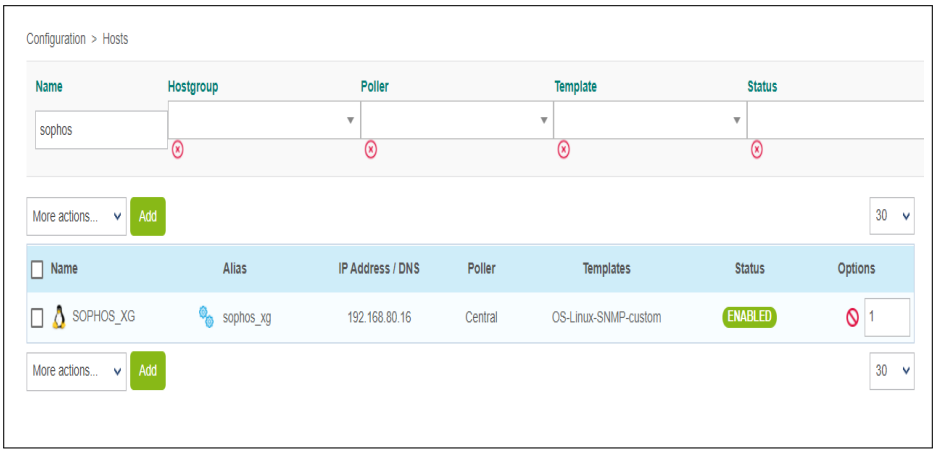


FIGURE III.32 – SOPHOS XG défini dans l'interface Centreon web .

3. Le résultat est visible dans le menu ***Monitoring > Status Details > Hosts*** (figure III.33) :

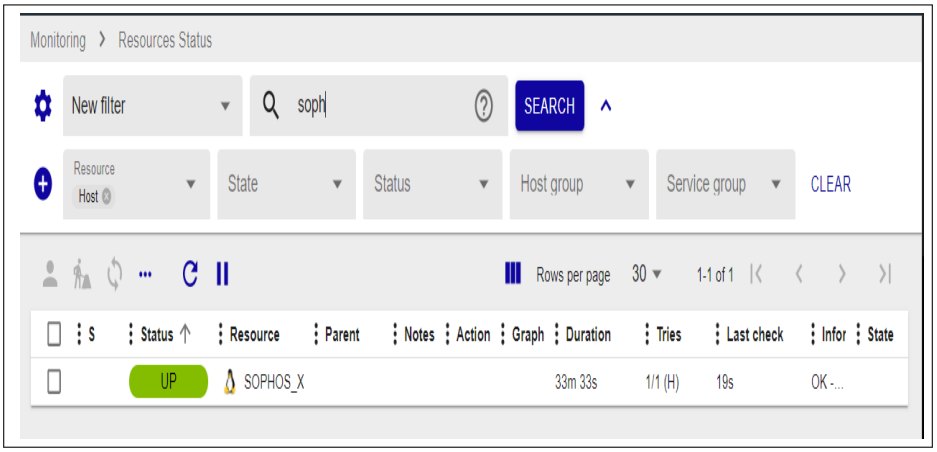


FIGURE III.33 – Résultat de l'ajout de SOPHOS XG .

III.6.2 Configuration des services

Le service peut être lui aussi, basé sur un modèle comme pour les hôtes. Un service intègre une commande (commande qui permet la vérification d'un état) avec ses arguments. Et pour finir, le service est lié à un hôte ou à un groupe d'hôtes.

1. Initialement pour l'ajout d'un service nous devons nous connecter à l'interface web Centreon avec un compte administrateur ou un compte disposant des droits d'accès pour gérer les objets. Ensuite se rendre sur ***Configuration > Services > Services par hôtes, puis on clique sur Ajouter*** (figure III.34) :

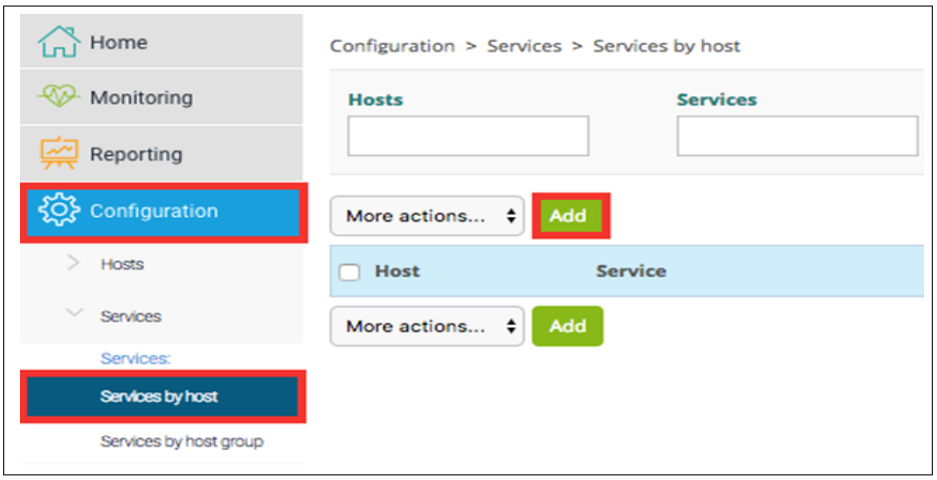


FIGURE III.34 – Configuration d'un service .

2. Nous accédons à un formulaire permettant de définir notre équipement. Pour démarrer la supervision de ce dernier, remplir :

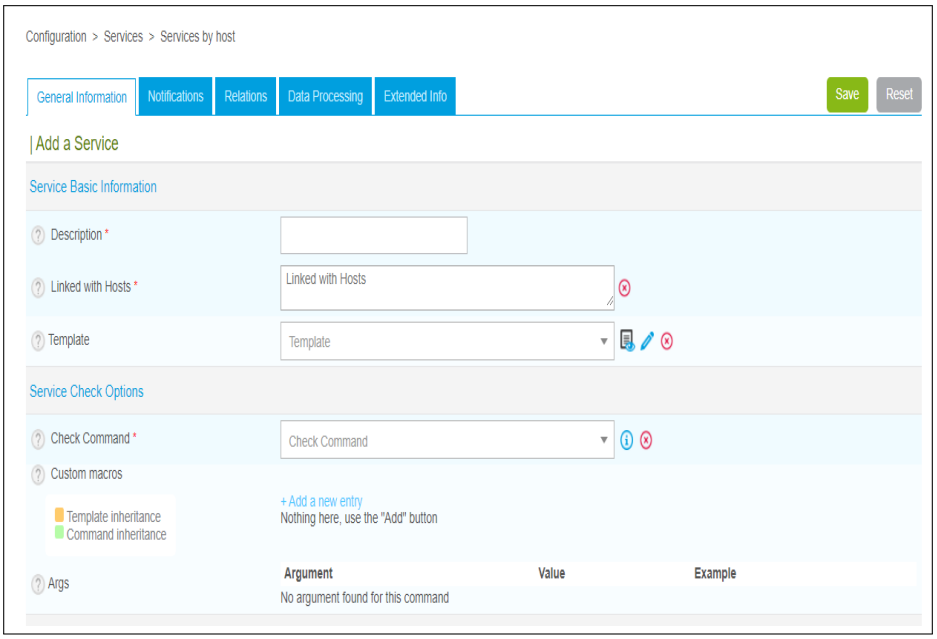


FIGURE III.35 – Formulaire d'ajout d'un service .

La figure III.35 représente les champs nécessaires suivants :

- Le champ **Description** définit le nom du service.
- Le champ Service **template** indique le modèle de service auquel le service est lié.

Pour ajouter un service à un hôte, trois champs seulement sont nécessaires :

- Sélectionner votre hôte via le champ **Linked with Hosts**.
- Définir le nom du point de contrôle via le champ **Description**.
- Sélectionner un modèle de service, par exemple **Base-Ping-LAN via** le champ **Service Template**.

A. Ajout de service PING

1. On accède à un formulaire permettant de décrire notre équipement. Nous remplirons les champs sur la figure III.36 .

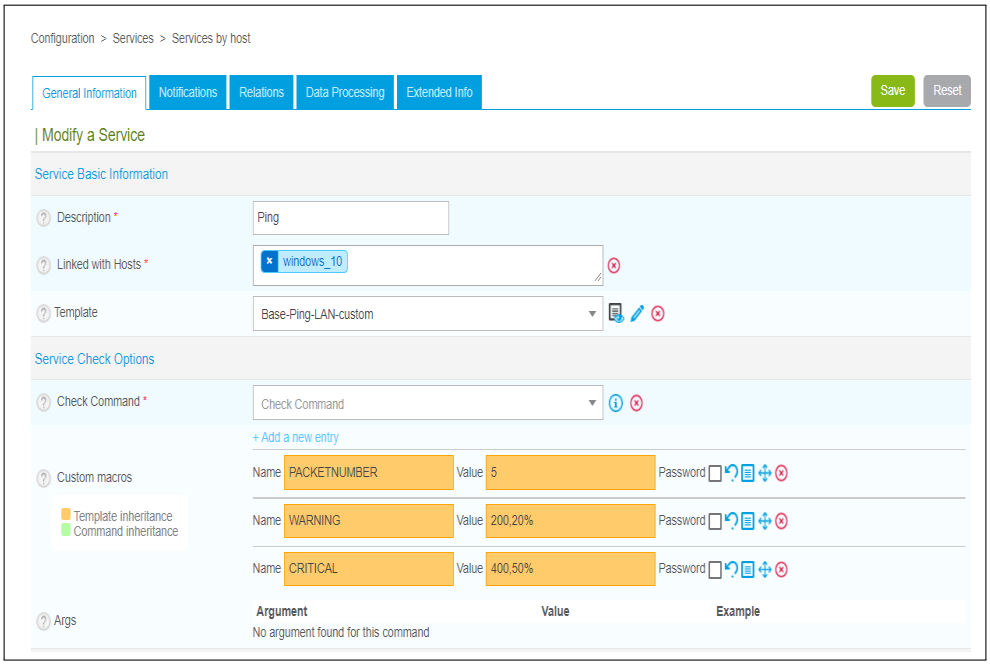


FIGURE III.36 – Ajout de service PING à windows 10 .

Sauvegarder les modifications en cliquant sur le bouton Save.

2. Le service est maintenant défini dans l'interface Centreon web (figure III.37) mais le moteur ne le connaît pas encore !

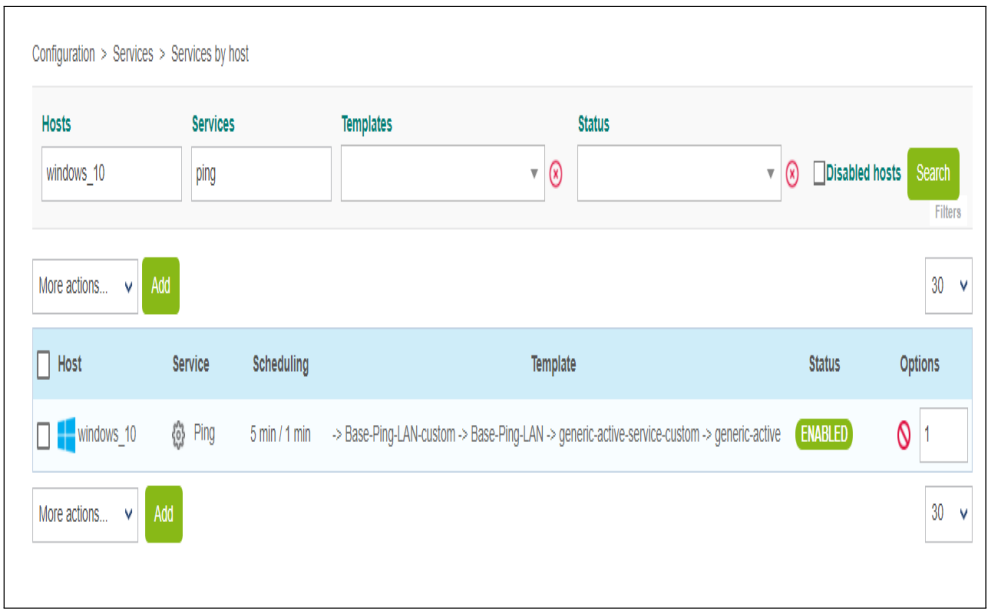


FIGURE III.37 – Service PING défini dans l'interface Centreon web .

3. Le résultat est visible via le menu ***Monitoring > Status Details > Hosts*** (figure III.38) :

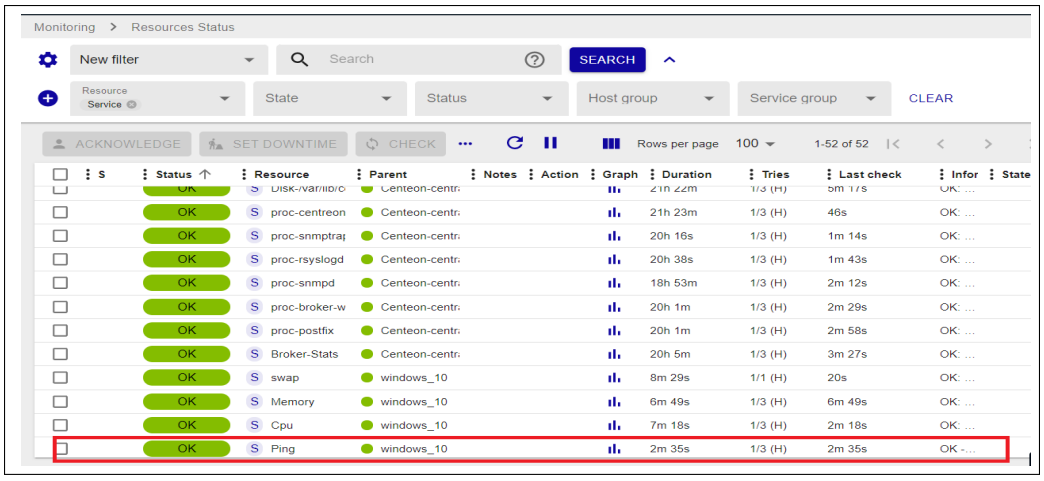


FIGURE III.38 – Résultat de l'ajout de PING à windows 10 .

B. **Ajout de service DISQUE**

1. Comme on l'a décrit précédemment, on accède à un formulaire permettant de décrire notre équipement .Nous remplirons les champs sur la figure III.39 :

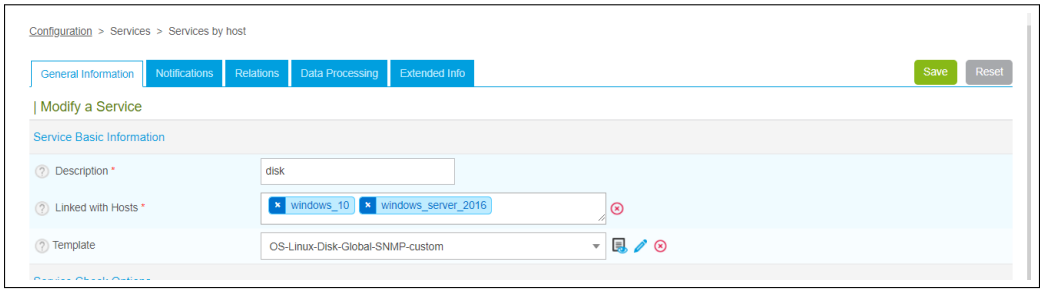


FIGURE III.39 – Ajout de service DISQUE à windows 10 et server 2016.

Sauvegarder les modifications en cliquant sur le bouton ***Save***.

2. Le service est maintenant défini dans l'interface Centreon web (figure III.40) mais le moteur ne le connaît pas encore !

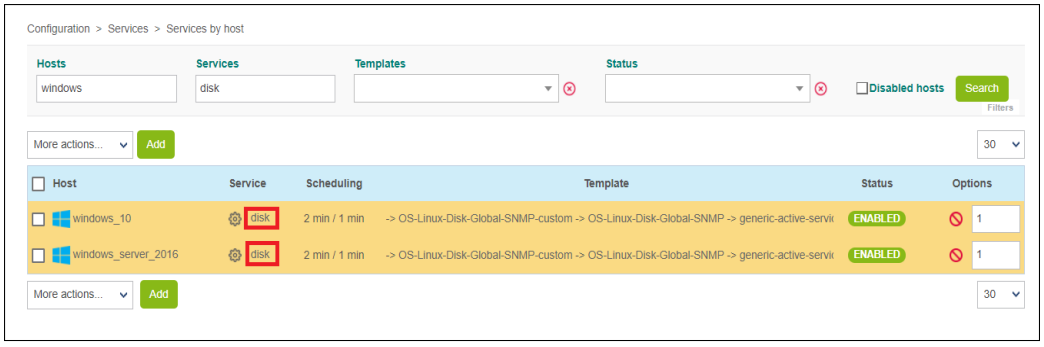


FIGURE III.40 – Service DISQUE défini dans l'interface Centreon web .

3. Le résultat est visible via le menu ***Monitoring > Status Details > Hosts*** (figure III.41) :

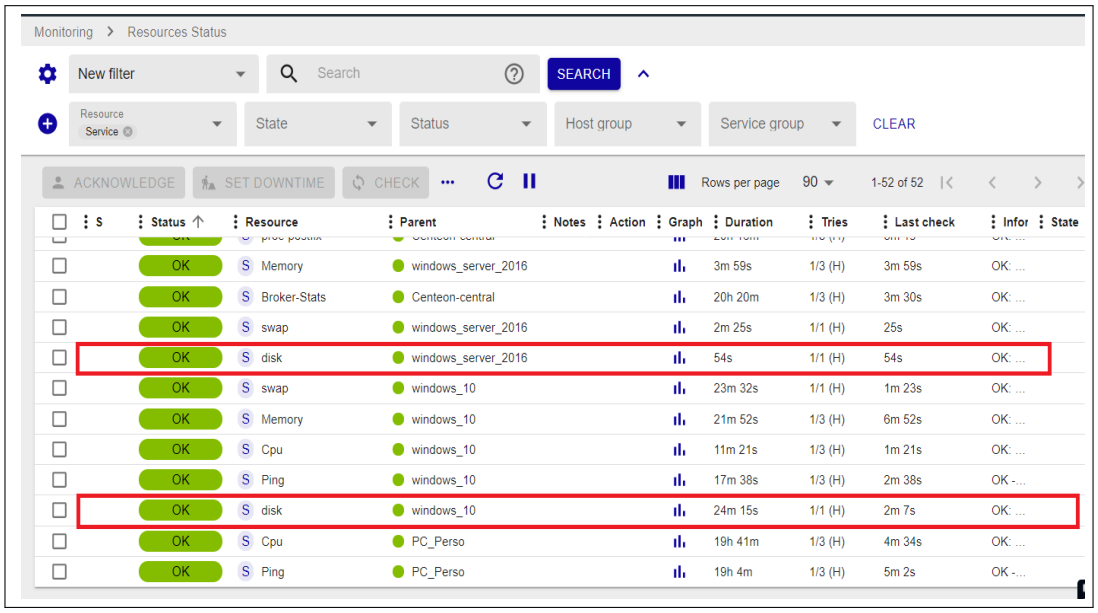


FIGURE III.41 – Résultat de l'ajout de DISQUE à windows 10 et windows server 2016 .

C. Ajout de service SWAP

1. On accède à un formulaire permettant de décrire notre équipement. Nous remplirons les champs sur la figure III.42 :

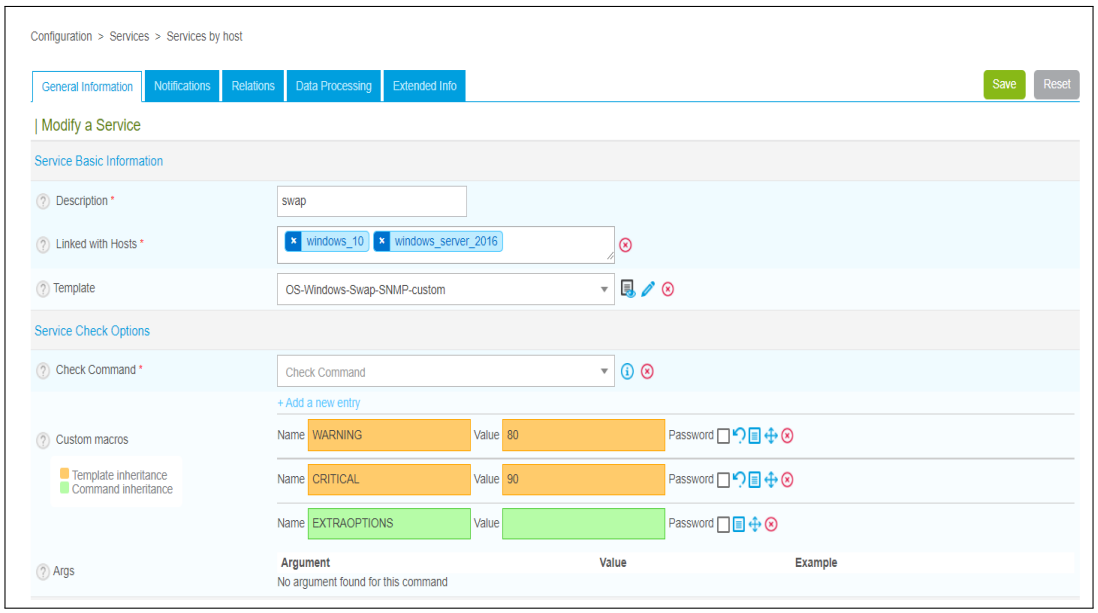


FIGURE III.42 – Ajout de service SWAP à windows 10 et windows server 2016 .

Sauvegarder les modifications en cliquant sur le bouton *Save*.

2. Le service est maintenant défini dans l'interface Centreon web (Figure III.43) mais le moteur ne le connaît pas encore !

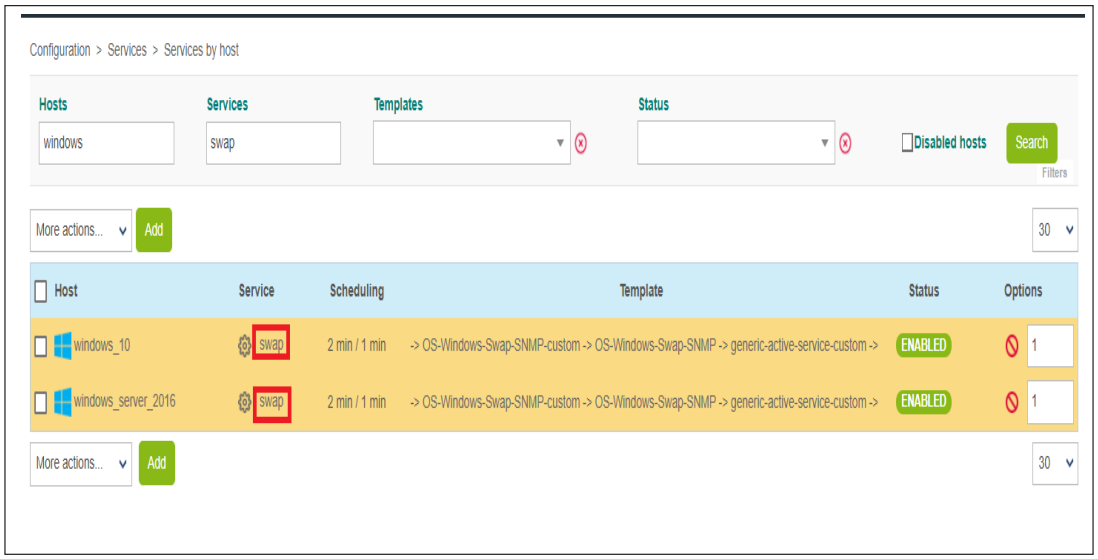


FIGURE III.43 – Service DISQUE défini dans l'interface Centreon web .

3. Le résultat est visible via le menu ***Monitoring > Status Details > Hosts*** (figure III.44) :

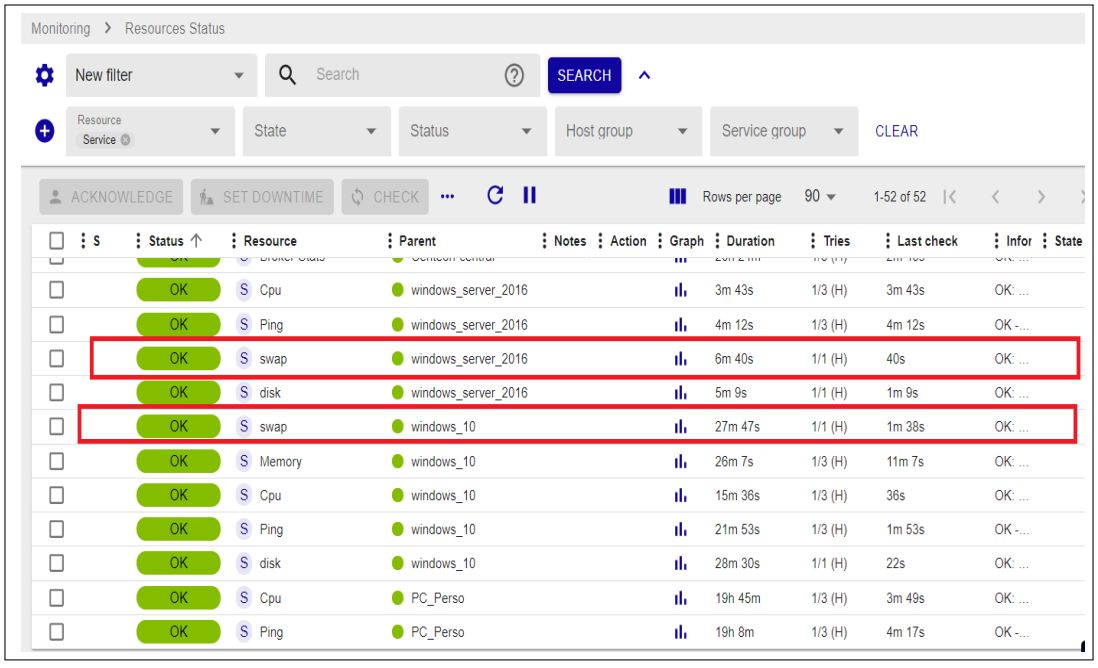


FIGURE III.44 – Résultat de l'ajout de SWAP à windows 10 et windows server 2016.

D. Ajout de service MEMORY

1. Comme on l'a décrit précédemment, on accède à un formulaire permettant de décrire notre équipement. Nous remplirons les champs sur la figure III.45 :

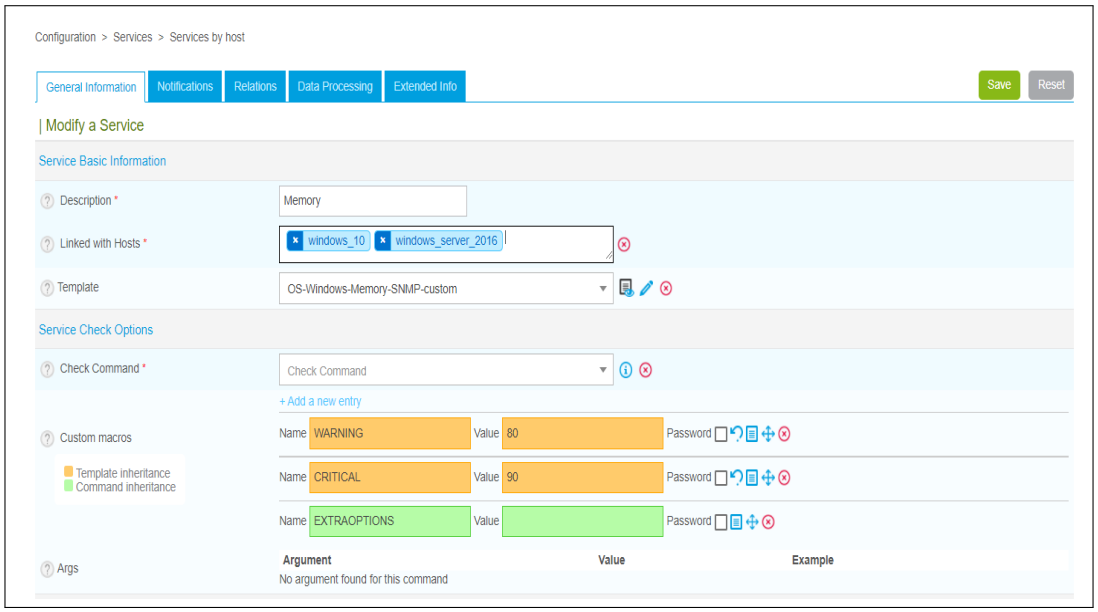


FIGURE III.45 – Ajout de service MEMORY à windows 10 et windows server 2016 .

Sauvegarder les modifications en cliquant sur le bouton *Save*.

2. Le service est maintenant défini dans l'interface Centreon web (figure III.46) mais le moteur ne le connaît pas encore !

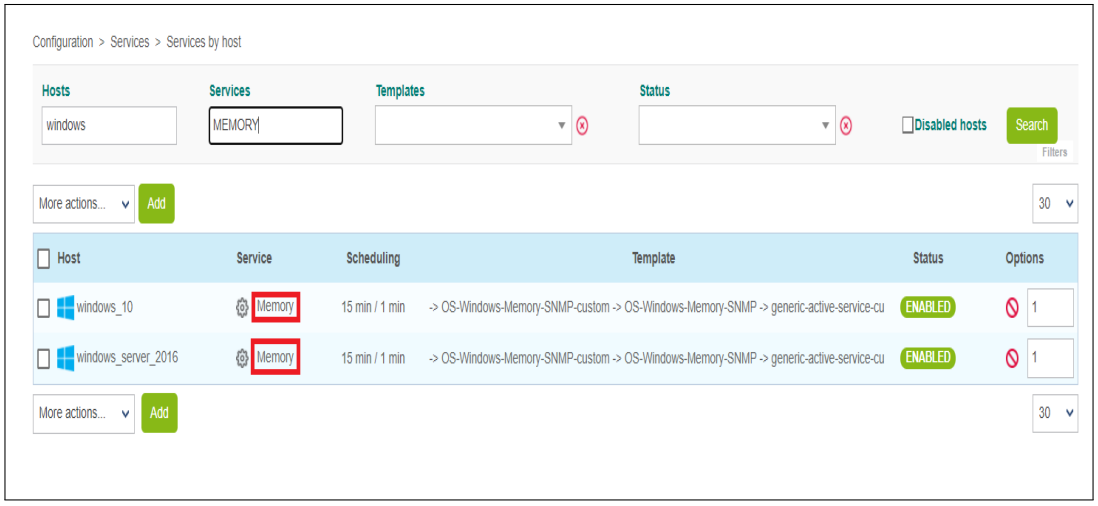


FIGURE III.46 – Service MEMORY défini dans l'interface Centreon web .

3. Le résultat est visible via le menu ***Monitoring > Status Details > Hosts*** (figure III.47) :

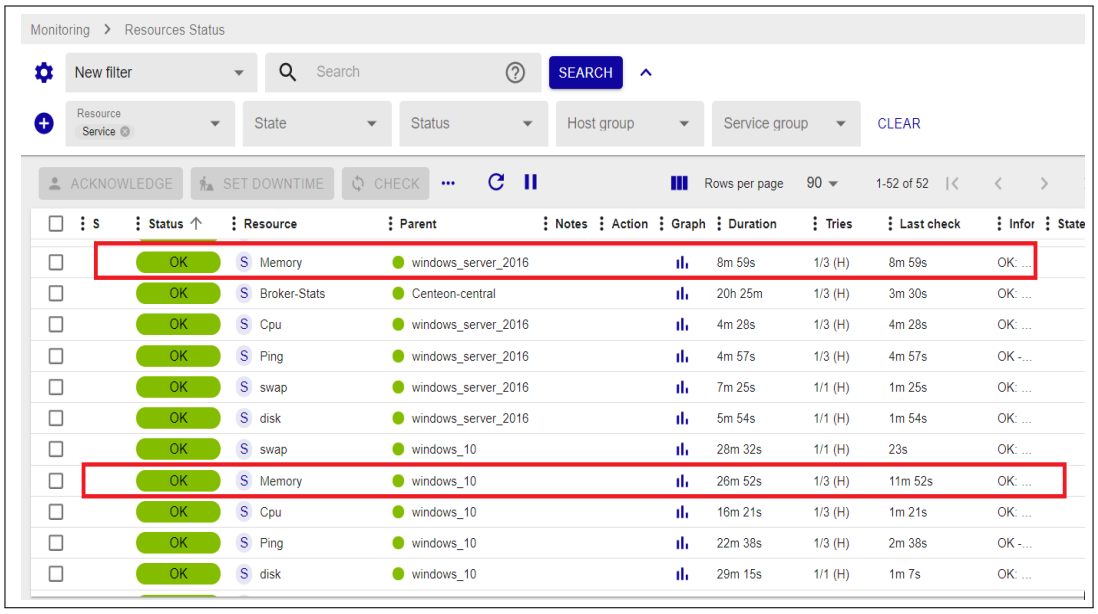


FIGURE III.47 – Résultat de l'ajout de MEMORY à windows 10 et windows server 2016 .

E. **Ajout de service CPU**

1. Comme on l'a décrit précédemment, on accède à un formulaire permettant de décrire notre équipement .Nous remplirons les champs sur la figure III.48 :

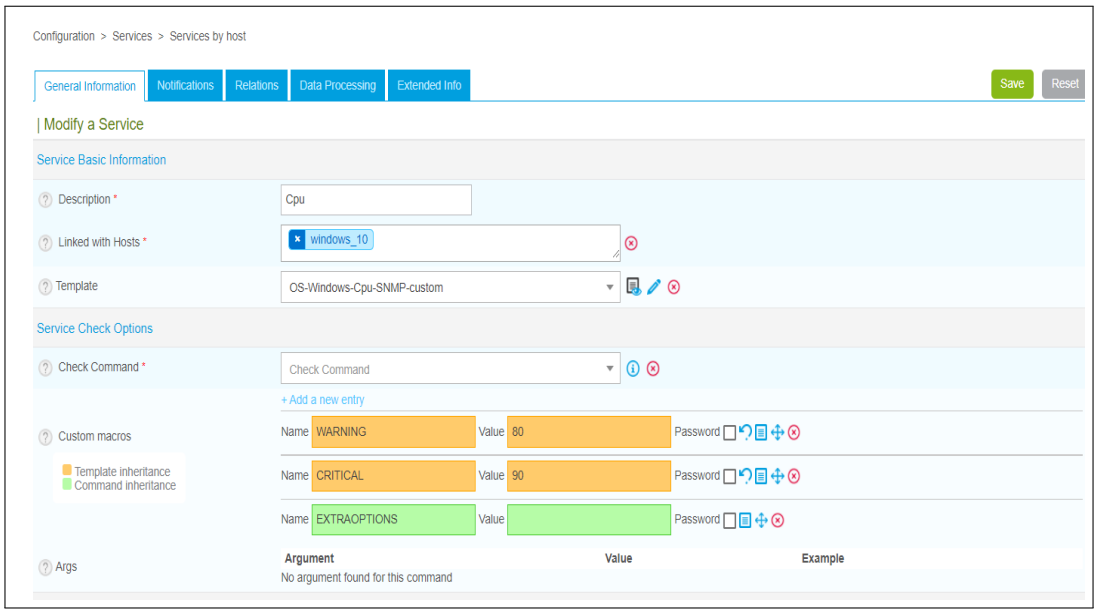


FIGURE III.48 – Ajout de service CPU à windows 10 .

Sauvegarder les modifications en cliquant sur le bouton ***Save***.

2. Le service est maintenant défini dans l'interface Centreon web (figure III.49) mais le moteur ne le connaît pas encore !

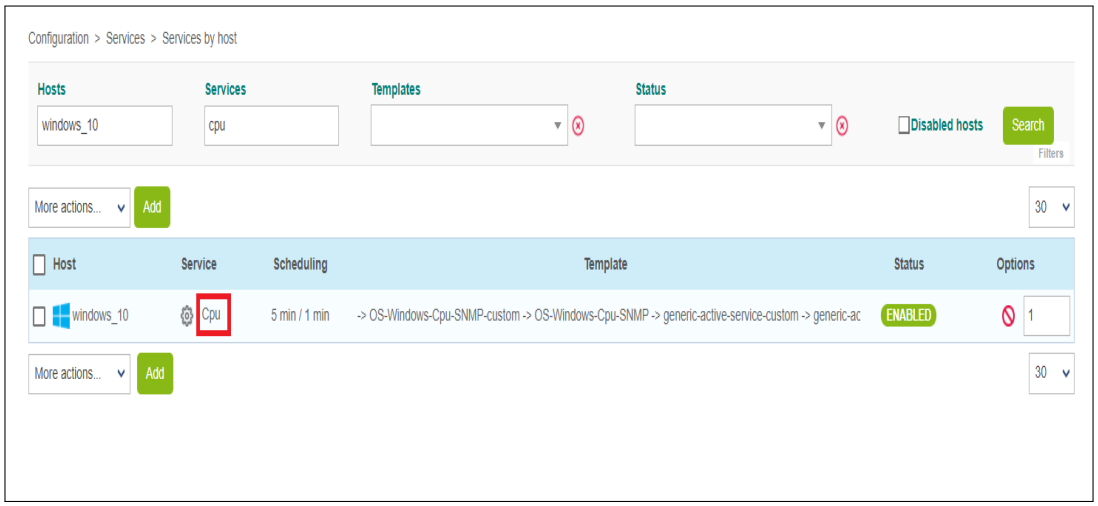


FIGURE III.49 – Service CPU défini dans l'interface Centreon web .

3. Le résultat est visible via le menu ***Monitoring > Status Details > Hosts*** (figure III.50) :

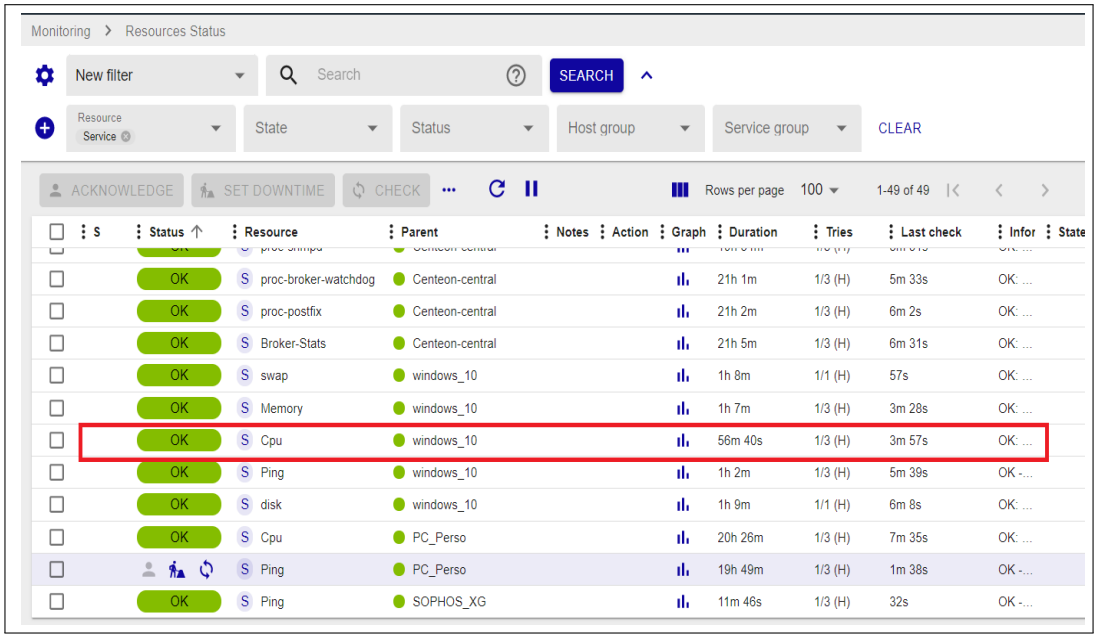


FIGURE III.50 – Résultat de l'ajout de CPU à windows 10 .

III.6.3 Configuration des contacts

Les contacts au sein de Centreon sont utilisés afin de :

- Pouvoir se connecter à l'interface web de Centreon : Chaque contact dispose de ses propres droits afin de se connecter à l'interface web.
- Être alerté en cas de nécessité (notification).

1. Afin d'ajouter un contact, il suffit de se rendre dans le menu ***Configuration > Users > Add*** (figure III.51)

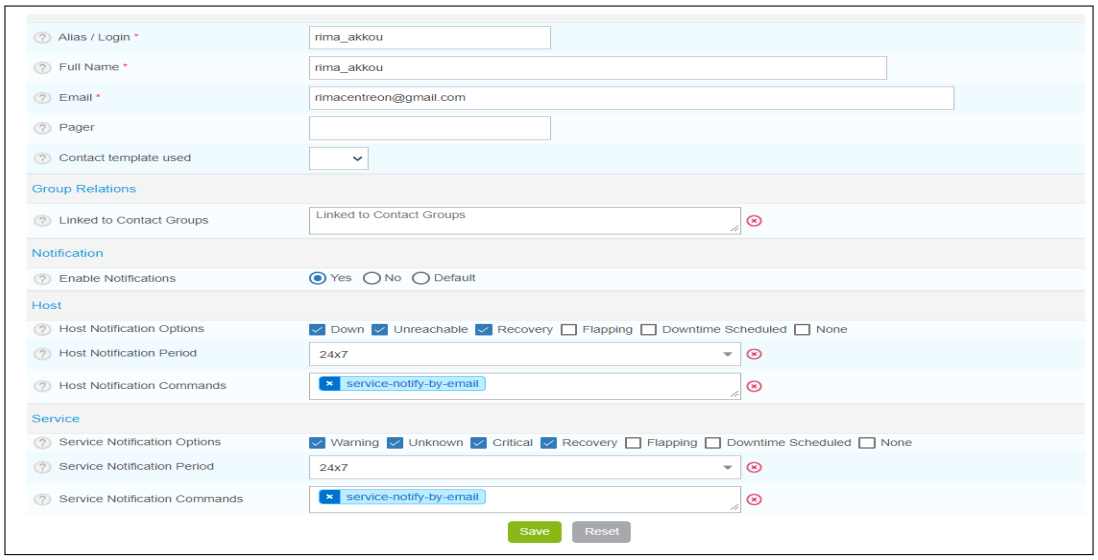


FIGURE III.51 – Ajout d'un contact .

III.7 Équipements à superviser

Nous allons superviser des équipements (figure III.52) existant dans la société et présenter les résultats finaux obtenus. Nous avons quatre équipements (dispositifs) à superviser. Ces équipements sont : Un équipement de sécurité (SOPHOS XG), trois postes de travail. La figure suivante montre ces équipements.

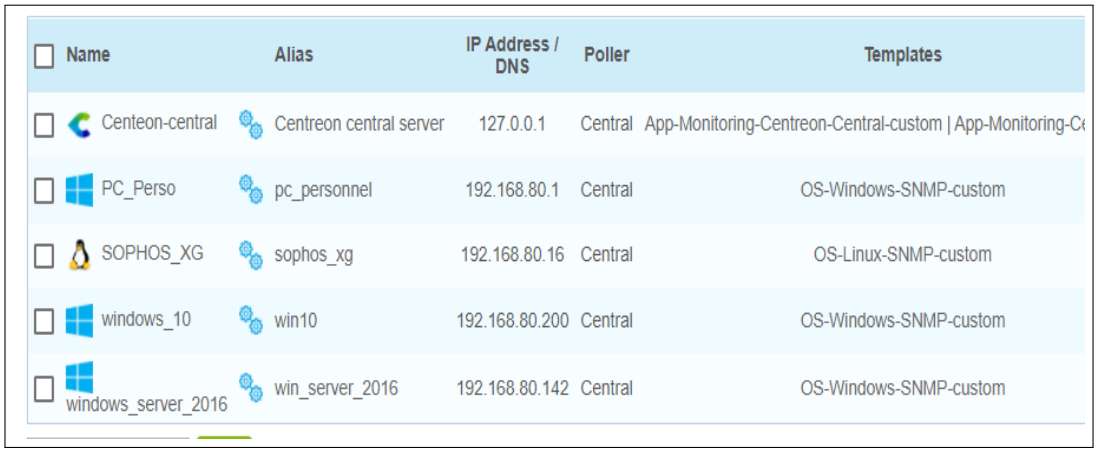


FIGURE III.52 – Équipements supervisé .

Tous les équipements auront une adresse IP du réseau 192.168.80.0/24. Pour chaque équipement, on donne son état en temps réel. L'état de ces équipements est représenté par :

- Espace d'échange
- Processeur
- Mémoire
- Disk du stockage
- PING
- Consommation de la RAM

III.8 Déployer la configuration

Après n'importe quelle manipulation sous centreon, on doit déployer la configuration :

1. Depuis la liste des Pollers, sélectionner le Poller et cliquer sur Exporter la configuration.
2. Cocher ensuite les quatre premières cases, sélectionner la méthode Redémarrer et cliquer sur Exporter (figure III.53) :

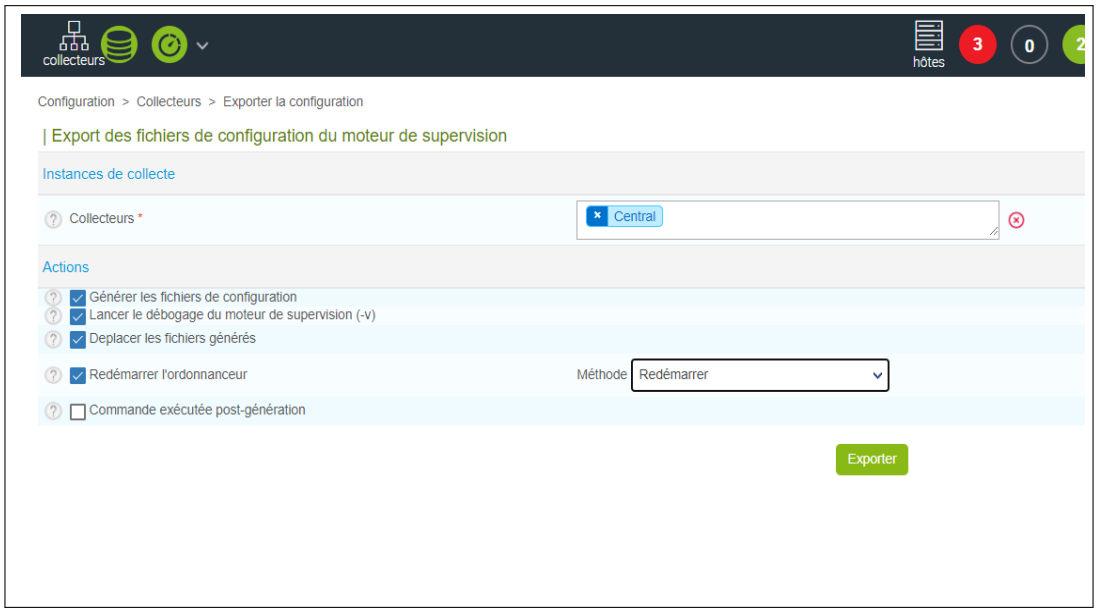


FIGURE III.53 – Exporter la configuration de poller .

3. Le moteur de supervision du Poller va alors démarrer et se connecter au Central (figure III.54) :

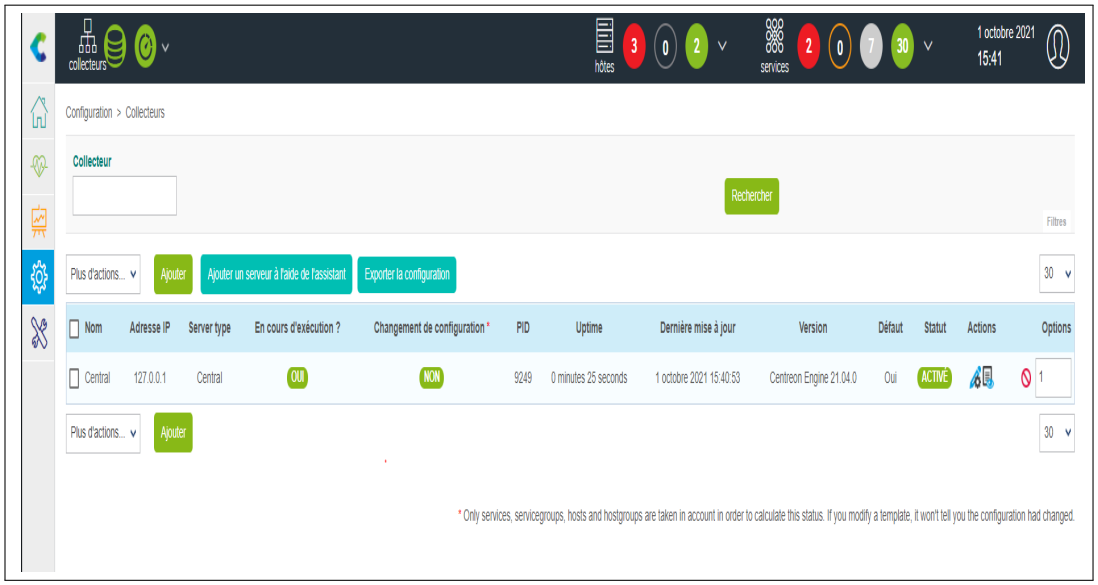


FIGURE III.54 – Moteur de supervision de poller .

III.9 Présentation des tests de fonctionnements

1. L'état des équipements supervisés DOWN/UP sont illustrés sur la figure III.55 :

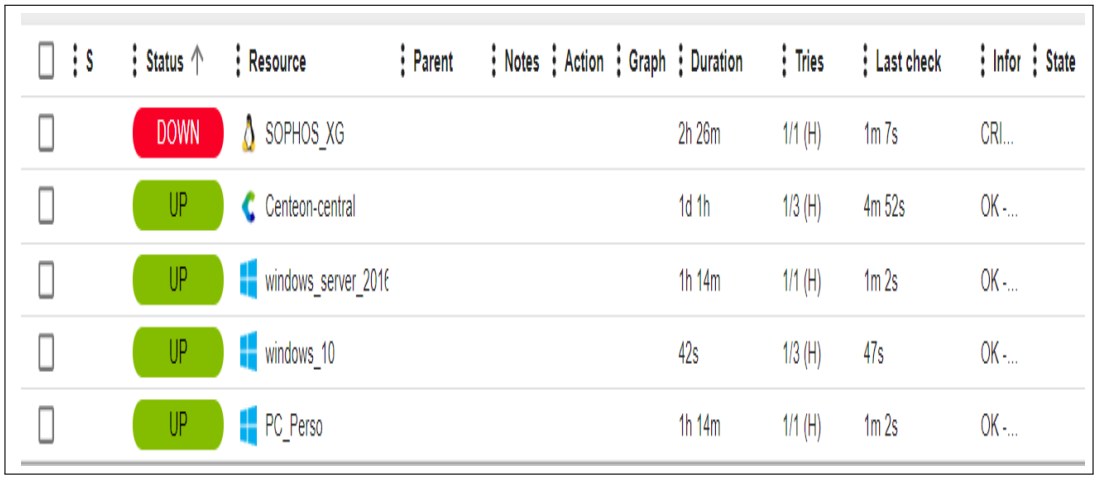


FIGURE III.55 – Etat des équipement supervisé DOWN/UP .

2. Nous laissons le programme faire la collecte et le traitement des données pendant quelques minutes avant d'actualiser l'interface de Centreon (figure III.56)

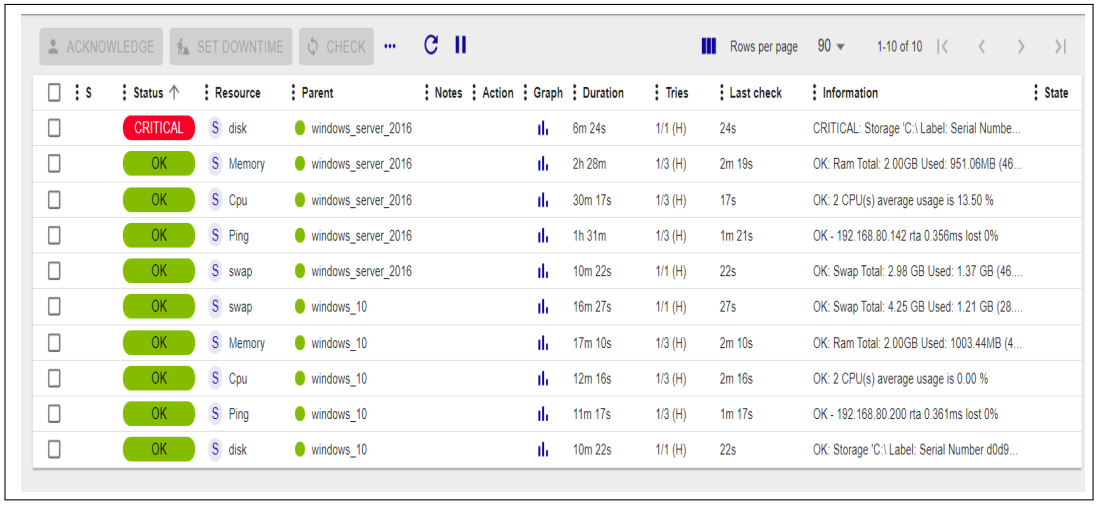


FIGURE III.56 – Résultat du check de windows server et windows 10 .

3. La figure III.56 illustre les états des services pour chaque hôte :
   - **Windows server 2016 :**
     - L'état de l'espace disque est : CRITICAL (figure III.57). En fait pour un disque de 24.51GB, 22.70 sont utilisés représentant 96.29% de la taille totale du disque et 931.16 MB sont libres ce qui est équivalent à 3.71%.

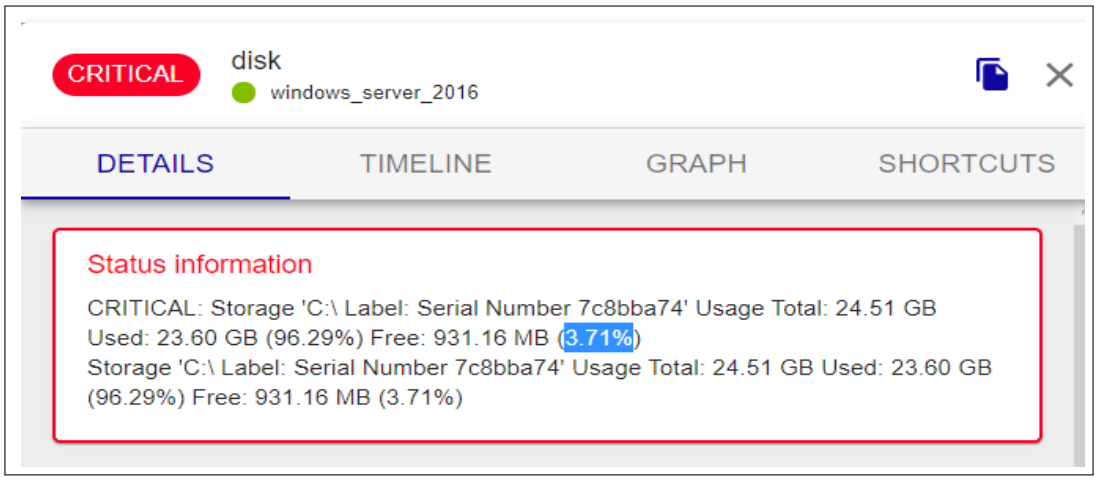


FIGURE III.57 – État de disque du stockage.

- L'état de mémoire : OK.
- L'état de processus : OK.
- L'état de PING :OK.
- L'état de l'espace d'échange.

- **Windows server 2016 :**
  - L'état de mémoire : OK.
  - L'état de processus : OK.
  - L'état de PING : OK.
  - L'état de disque dure : OK.
  - L'état de l'espace d'échange : OK.

4. Supervision de l'hôte et des services de Windows 10 est présentée par la figure III.58

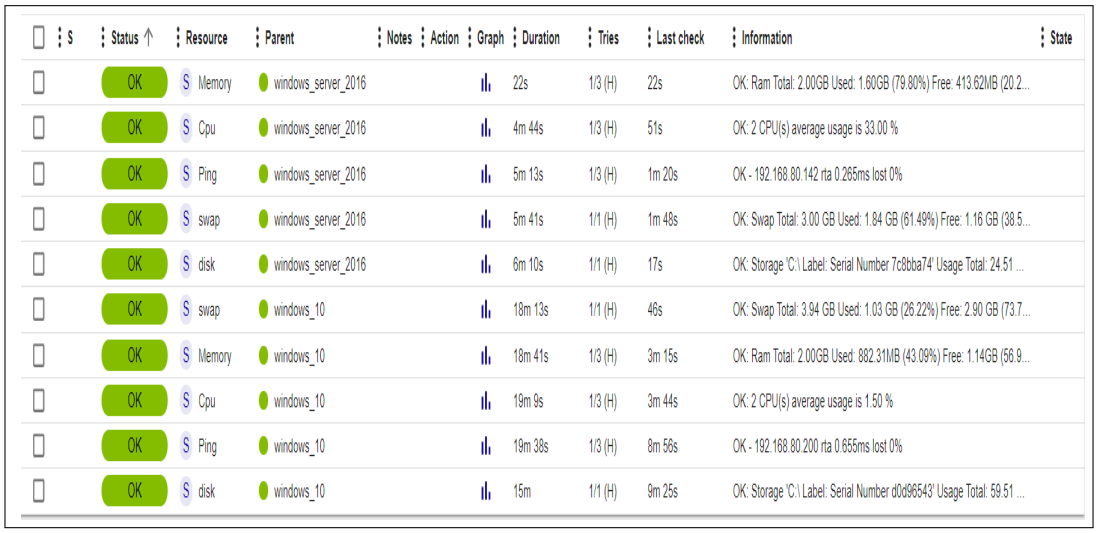


FIGURE III.58 – Supervision de Windows .

III.10 Notification par mail

Malgré l'existence d'une interface web permettant de visualiser l'état d'un hôte ou service en temps réel, la notification des contacts reste toujours obligatoire. Pour envoyer les notifications par mail depuis Centreon il faut d'abord installer l'outil correspondant, cela peut se faire de plusieurs manières : utiliser SSMTP, Postfix ou bien encore Sendmail.

Postfix est un élément étroitement lié à Centreon. Effectivement, il sert à l'envoi des notifications vers votre serveur de messagerie et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail ; c'est pour ces raison qu'elle est adapté.

Les notifications dans Centreon font appel à plusieurs éléments :

- D'une part le MTA (Mail Transport Agent) (Postfix) installé sur le serveur Centreon.
- Un serveur smtp local doit être configuré.
- D'autre part les deux commandes utilisées pour envoyer les mails.
  - *notify-service-by-email*.
  - *notify-host-by-email*.
- Les contacts à notifier.

III.10.1 Configuration de Postfix

1. Dans le terminal de notre serveur, entrer la commande suivante :

```
yum -y install mailx cyrus-sasl-plain
```

2. Redémarrer Postfix :

```
systemctl restart postfix
```

3. Configurer Postfix pour qu'il s'exécute au démarrage :

```
systemctl enable postfix
```

4. Éditer le fichier suivant :

```
vi/etc/postfix/main.cf
```

5. Ajouter les informations suivantes :

```
myhostname = centreon-central
relayhost = [smtp.gmail.com] :587
smtp_use_tls = yes
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash :/etc/postfix/sasl_passwd
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
```

   - Le paramètre myhostname est le hostname du serveur Centreon.
   - Le paramètre relayhost correspond au serveur de messagerie du compte qui enverra les emails.

III.10.2 Configurer les identifiants du compte qui enverra les emails

1. Créer un fichier */etc/postfix/sasl_passwd* :

```
touch/etc/postfix/sasl_passwd
```

2. Ajouter la ligne suivante, en remplaçant identifiant :motdepasse par les informations de connexion du compte qui enverra les emails de notification :

```
[smtp.gmail.com] :587 rymakk9@gmail.com :XXXXXXXX
```

3. Dans le terminal, entrer la commande suivante :

```
postmap /etc/postfix/sasl_passwd
```

4. Pour plus de sécurité, changer les permissions sur le fichier *sasl_passwd* :

```
chown root :postfix /etc/postfix/sasl_passwd*
chmod 640 /etc/postfix/sasl_passwd*
```

5. Recharger Postfix pour prendre en compte les modifications :

```
systemctl reload postfix
```

III.10.3 Tester et diagnostiquer Postfix

1. Pour envoyer un email de test, utiliser la commande suivante (figure III.59) :

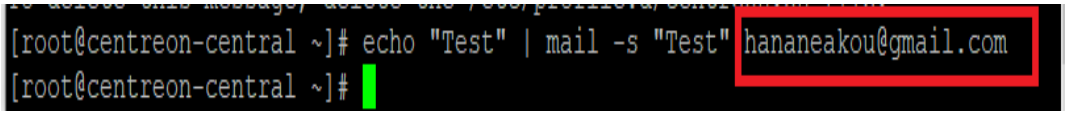


FIGURE III.59 – Email de teste .

2. Le résultat de ce test est présenté dans la figure III.60 :

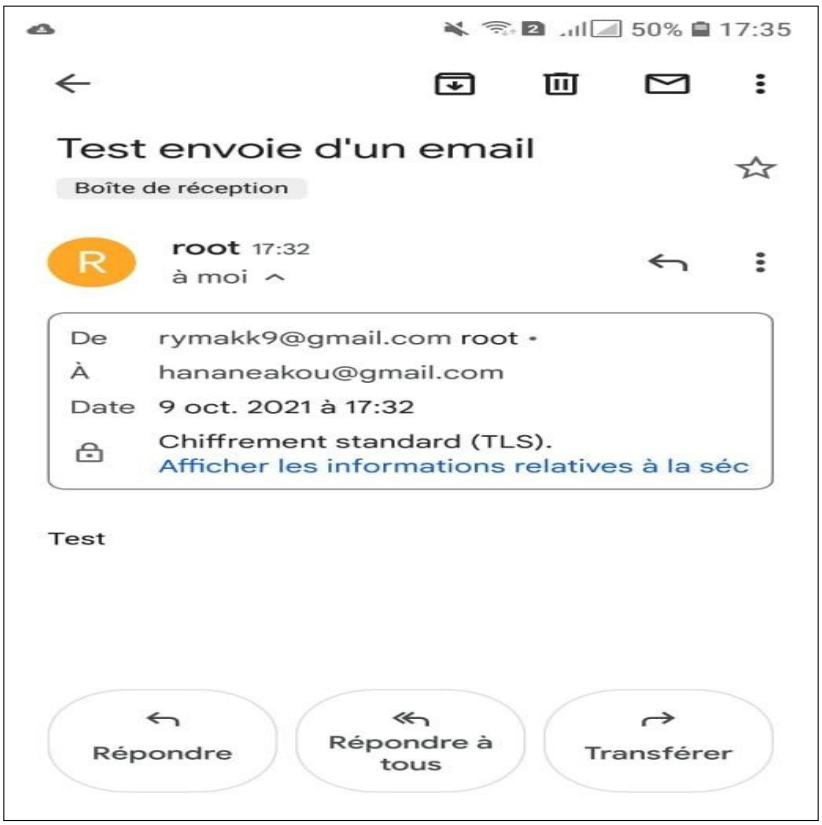


FIGURE III.60 – Tester l'envoi d'un email .

3. Si le destinataire n'a pas reçu l'email, vérifier le fichier log suivant :

```
tail -f /var/log/maillog
```

4. Pour vérifier si votre service Postfix tourne, entrer :

```
systemctl status postfix
```

5. Le résultat devrait ressembler à ça (figure III.61) :

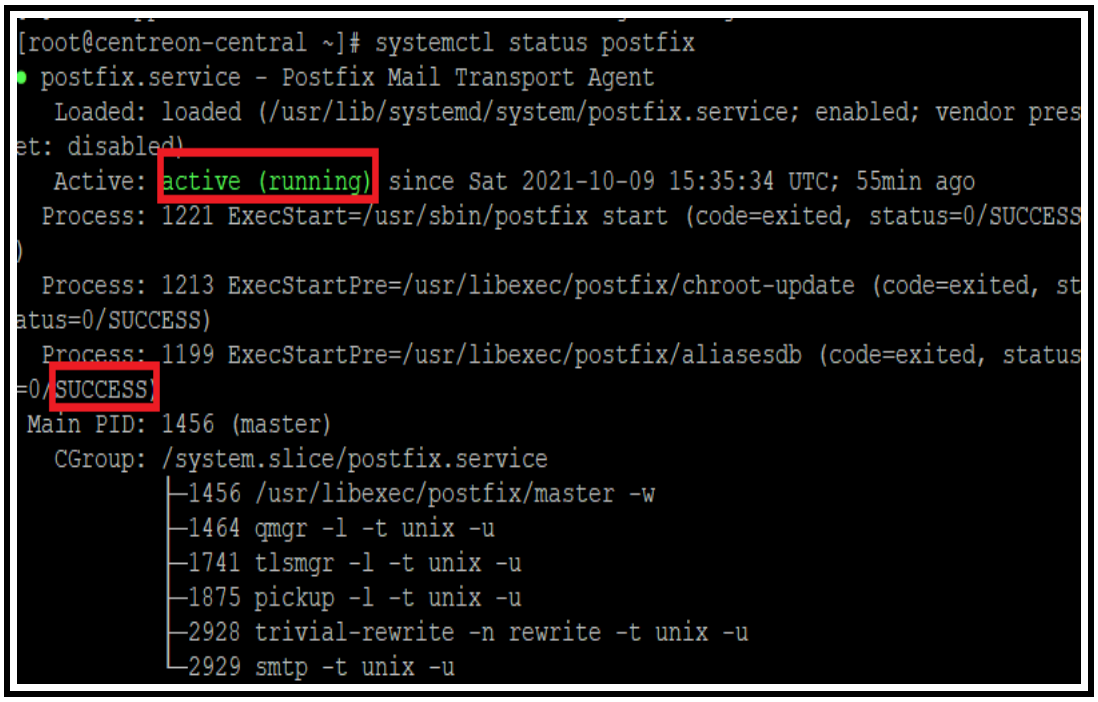


FIGURE III.61 – Résultat commande de vérification de l'état du serveur Centreon .

6. Enfin, on modifie le paramètre du compte Google (figure III.62) pour autoriser les applications non Google moins sécurisées à utiliser l'authentification pour envoyer des e-mails via SMTP en notre nom.

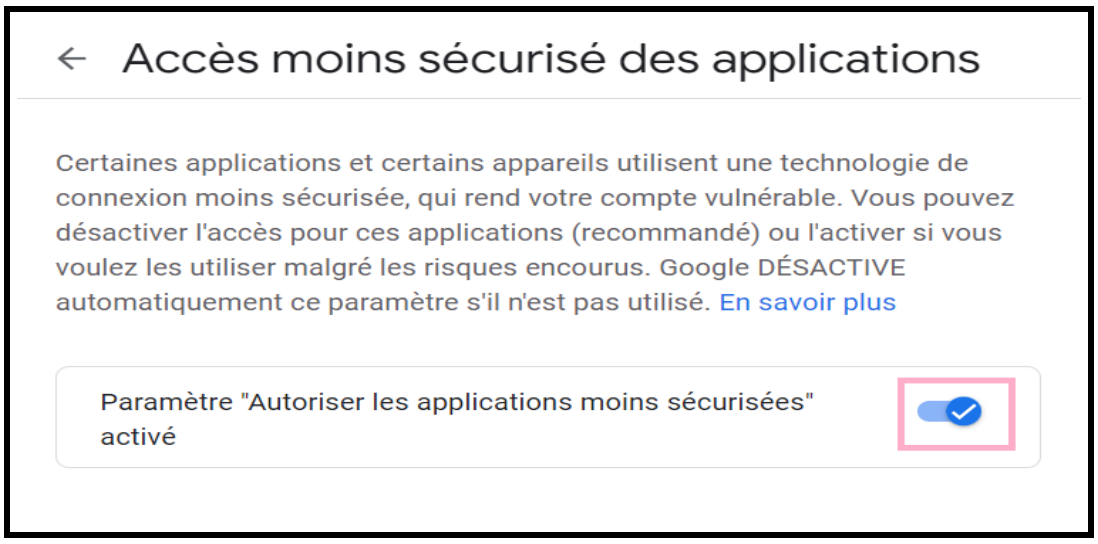


FIGURE III.62 – Paramètre Google .

7. Le résultat de cette configuration est présenté par la figure III.63 :

FIGURE III.63 – Mail d'alerte reçu .

III.11 Conclusion

Dans ce chapitre, nous avons présenté l'aspect pratique de notre projet, où nous avons détaillé les étapes de préparation, configuration et installation de Centreon . Nous avons ensuite présenté les résultats de cette solution sur quelques équipements de l'organisme d'accueil INSIM Béjaia.

Conclusion Générale

Notre projet d'étude avait, pour but de mettre en place une console d'administration réseaux au sein de l'entreprise INSIM Bejaia.

Ce manuscrit a débuté par une généralité sur les réseaux informatiques : Nous avons défini ce qu'est un réseau informatique, présent ses différents composants, les différentes topologies qu'il peut prendre, ses différents types par rapport à la distance qui sépare les composants. Nous avons présenté, par la suite, tout ce qui est utilisé (installations et protocoles) pour répondre aux besoins du projet en termes de services. Enfin, nous avons clôturé le chapitre par présenter l'organisme d'accueil, INSIM Bejaia, où j'ai effectué mon stage pratique et tracer l'objectif à atteindre en détaillant son cadre et ses fonctionnalités.

Le second chapitre de ce mémoire a été consacré à la définition de la supervision, la présentation de ses différents types et aussi les différents outils de mise en place d'un système de supervision de réseau.Il a été clôturée par une étude comparative des différents outils présentés, et une décision de l'outil de supervision retenu pour notre chapitre.

Enfin, durant le dernièr chapitre, nous avons mis en place le système de supervision de réseau au sein de l'INSIM Bejaia et nous avons eu et présenté les différents tests de fonctionnement en temps réel. Les résultats étaient très satisfaisants et répondent à nos besoins et aux besoins de l'organisme d'accueil. Ainsi, ils répondent aux objectifs tracés au début de ce projet.

En guise de perspectives, nous envisageons l'amélioration de ce travail par :

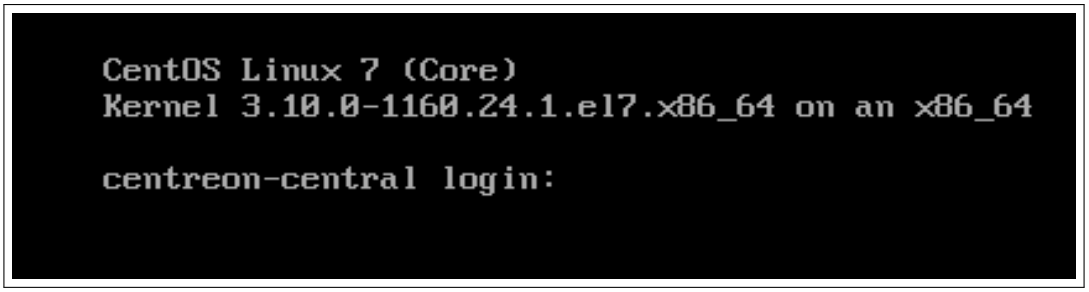
- Migrer les serveurs sur le Cloud.
- Utiliser un système de supervision basé sur les Cloud.
- Remplacer les hubs par des commutateurs et les superviser.

Annexes

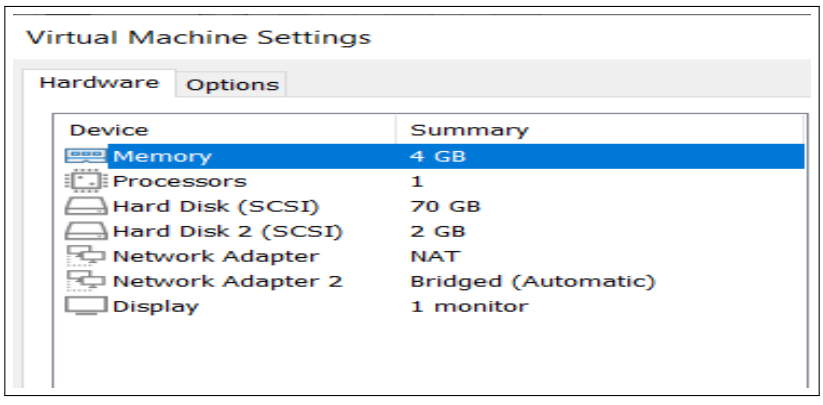
Annexe A

Installation de Centreon

1. Importez le fichier centreon-central.ova dans VMWare. Un terminal s'ouvre : attendez que le serveur démarre. Lorsque celui-ci est prêt, le terminal affiche le message suivant :



2. Selon la structure de votre réseau, dans la configuration de votre machine virtuelle, ajoutez un adaptateur réseau et sélectionnez le réseau via lequel la machine pourra communiquer avec les ressources qu'elle devra superviser.



Pour finaliser la configuration on doit :

3. Connectez-vous au serveur Centreon avec les informations suivantes : login : root, password : centreon.
4. Pour connaître l'adresse IP de votre serveur, tapez ip addr.

```
[root@centreon-central ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:33:df:86 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.137/24 brd 192.168.80.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::7fa:54c3:b138:4b4c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:33:df:90 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.108/24 brd 192.168.1.255 scope global noprefixroute dynamic ens34
       valid_lft 86008sec preferred_lft 86008sec
    inet6 fe80::7d5f:2b28:b7a0:4e99/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@centreon-central ~]#
```

5. Connectez-vous en root au serveur depuis une autre machine avec le terminal de votre choix, à l'aide de l'adresse IP obtenue précédemment.
6. À votre première connexion au serveur, des instructions s'affichent pour vous aider à terminer la configuration :

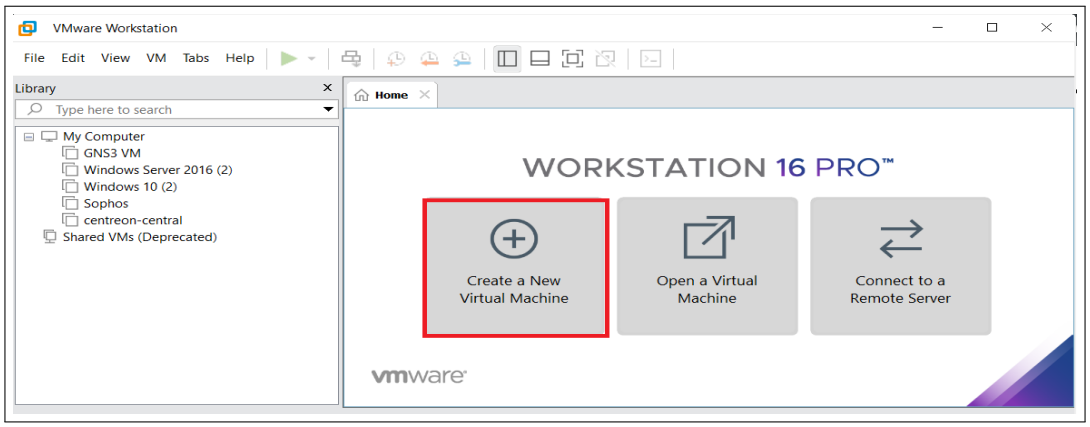
```
Last login: Sun Sep 19 20:10:13 on tty1

 #####   #######  #     #  #######  ######   #######  #######  #     #         ###     #
#     #  #        ##    #     #     #     #  #        #     #  ##    #        #   #   ##
#        #        # #   #     #     #     #  #        #     #  # #   #        #   #  # #
#        #####    #  #  #     #     ######   #####    #     #  #  #  #          #     #
#        #        #   # #     #     #   #    #        #     #  #   # #          #     #     ###
#     #  #        #    ##     #     #    #   #        #     #  #    ##         #     #     ###
 #####   #######  #     #     #     #     #  #######  #######  #     #        #####  #####   ###

Based on CentOS Linux release 7.9.2009 (Core)

+--------------------------------------------------------------------+

Please execute following instruction:

1. Define the timezone of the server (ex. Europe/London):
# timedatectl set-timezone Europe/London

2. Define the PHP timezone (ex. Europe/London) in file /etc/opt/rh/rh-php73/php.d/50-centreon.ini
# systemctl restart rh-php73-php-fpm

3. Change the hostname of the server (ex. centreon-central):
# hostnamectl set-hostname centreon-central

4. Update the Centreon database partitioning (mandatory):
# su - centreon
$ /opt/rh/rh-php73/root/bin/php /usr/share/centreon/cron/centreon-partitioning.php
$ exit

5. Restart Centreon services (mandatory):
# systemctl restart cbd centengine gorgoned

You can disable the CEIP program using Centreon official documentation.

To delete this message, delete the /etc/profile.d/centreon.sh file.
[root@centreon-central ~]#
```

7. Connectez-vous à l'interface web : dans votre navigateur, entrez l'adresse du serveur au format http ://addresse_ip/centreon ou http ://FQDN/centreon. (Par exemple, une URL valide serait http ://192.168.80.137/centreon.)
8. Connectez-vous en utilisant les informations suivantes : Login : admin, password : centreon. Par défaut, votre serveur offre une configuration prédéfinie qui permet de le superviser lui-même.

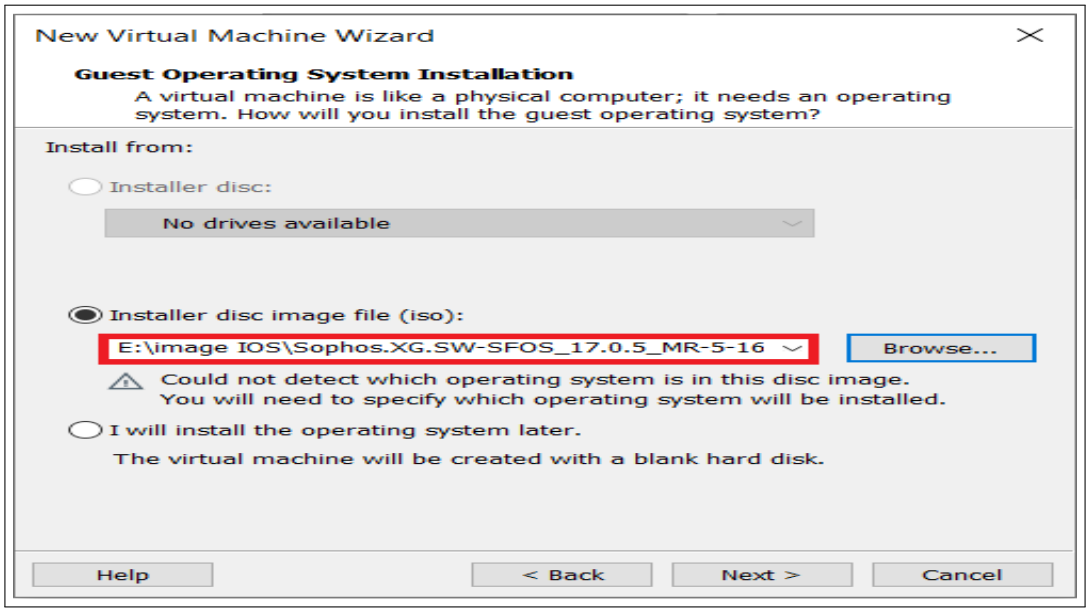
Annexe B

Installation de Sophos

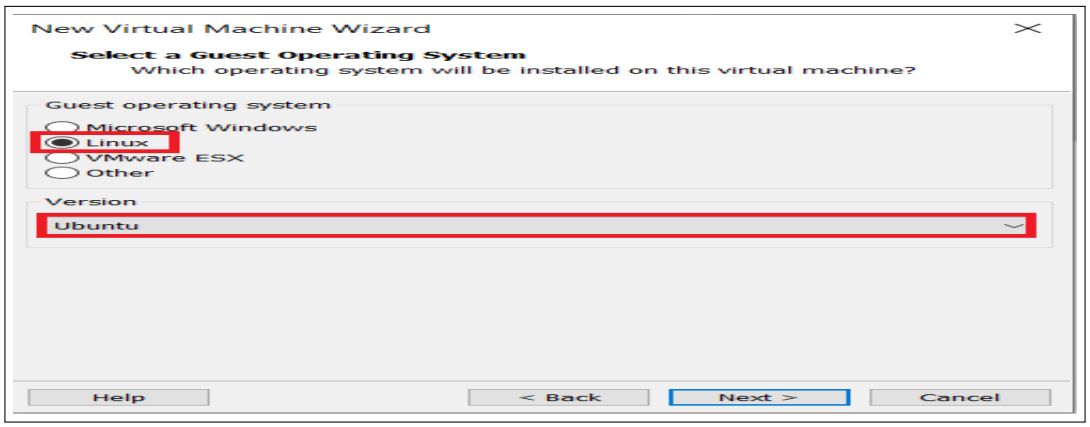
1. Pour notre implémentation nous allons créer une machines virtuelles nommées SOPHOS XG :



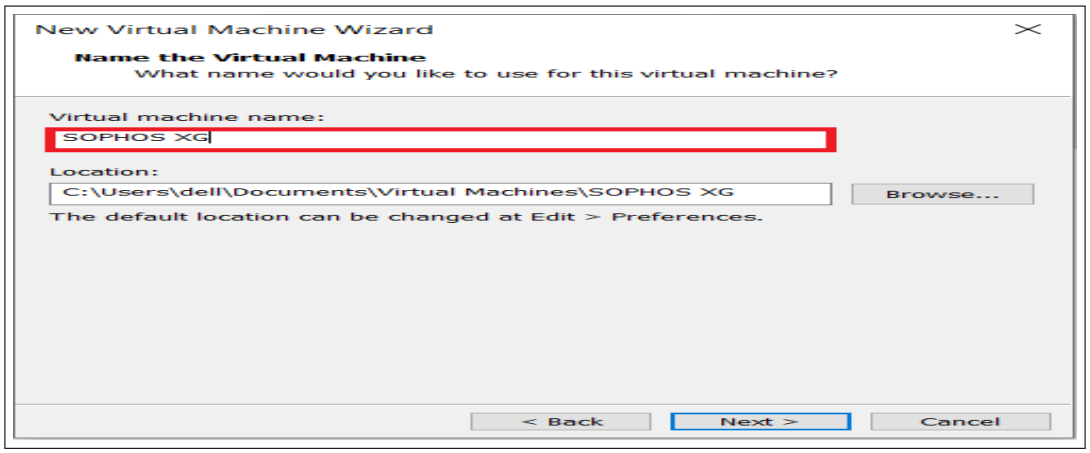
2. Dans la fenêtre ci-dessous, cliquer sur parcourir pour choisir le dossier qui contient l'image Sophos XG.



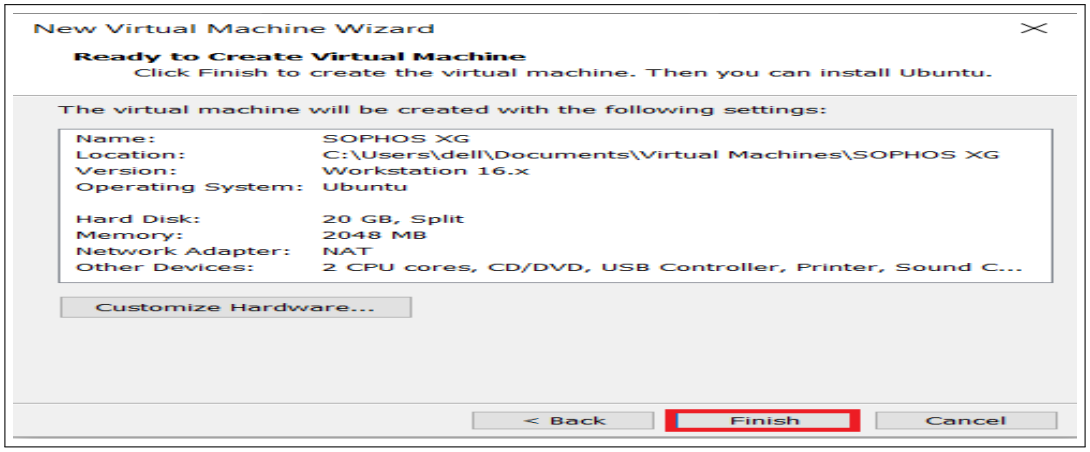
3. Ensuite On doit à présent choisir le système qui sera installé sur la machine virtuel :



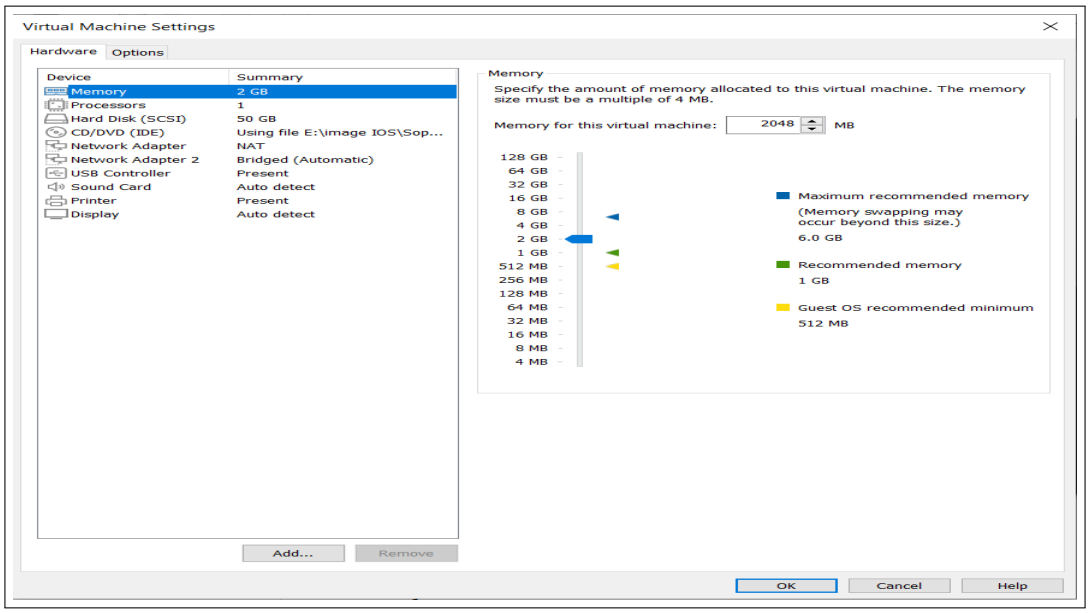
4. Ensuite nommer la machine virtuelle



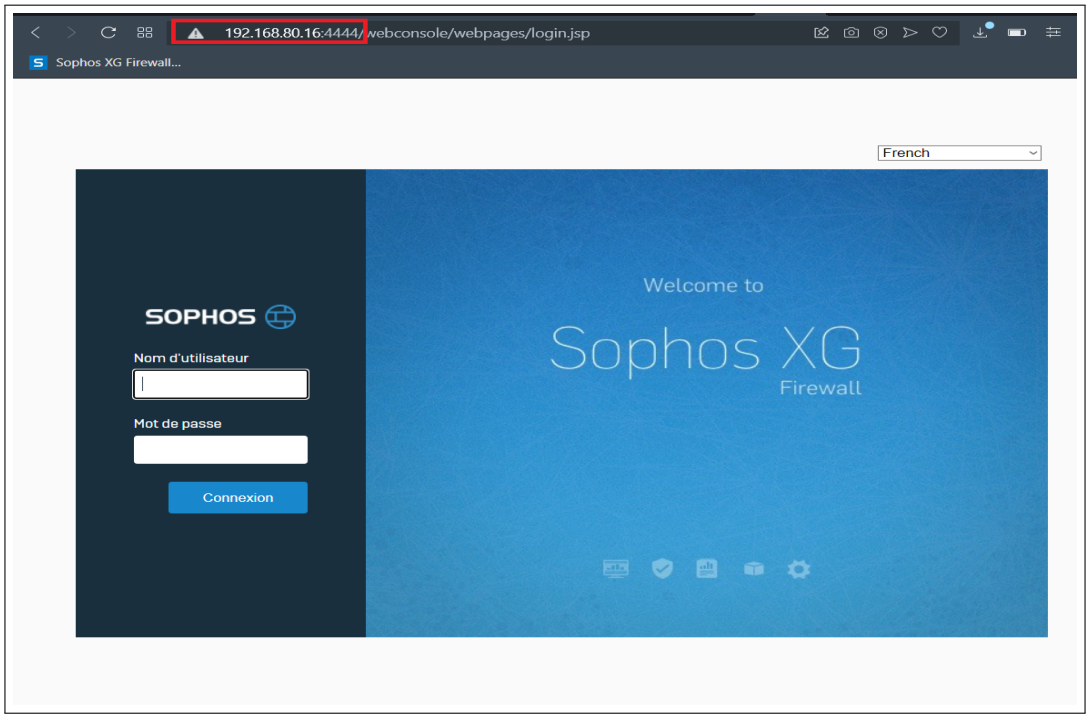
5. Il faut maintenant cliquer sur «finish» pour terminer l'installation.



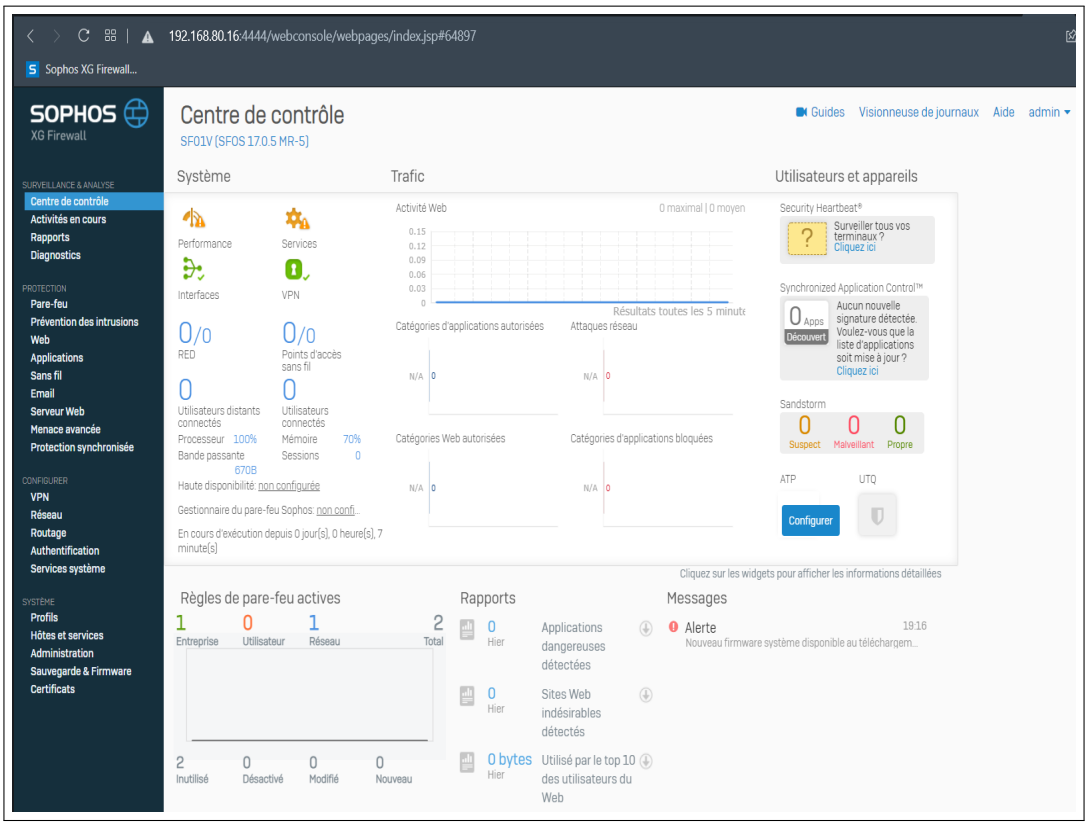
6. Choix des configurations à effectuer sur la machine virtuelle Sophos XG.



7. A présent, il faut se rendre sur le site du pare-feu (192.168.80.16 :4444) où une page d'authentification sera affiché et consistera à saisir le nom d'utilisateur et le mot de passe, puis de cliquer sur «Login» pour s'authentifier, comme c'est décrit ci-dessous :



8. Après s'être authentifié, la plateforme principale Sophos XG sera affichée.



Bibliographie

[1] R. Khaila, «*Installation configuration et administration d'un réseau local avec contrôleur de domaine* » ,2019.

[3] J.Dordoigne , « *Réseaux informatiques - Notions fondamentales*», 8eme édition,2008.

[4] A.Mbonda Nkenko «*Etude et mise en oeuvre d'un système streaming via le réseau internet*», Ecole supérieure des métiers d'informatique et de commerce RDC - Graduat 2013

[5] S.Bouaoud , S.Arabi ,« *La mise en place d'une solution de monitoring et suivi des systèmes informatiques et réseaux (2018/2019)*», consulté le 13/07/2021 .

[6] M.Jeampy,« *Note de cours d'administration Réseau* », L2 Info, ISC/kinshasa,2012 -2013.

[8] I.NZANZU MBAIKULYA ,« *Etude de la mise en place d'un réseau informatique dans une entité étatique décentralisée : cas de la mairie de Beni*», Institut supérieur du bassin du Nil - Ingénieur technicien en réseaux et maintenance informatique, 2015.

[9] P.ATELIN,« *notions fondamentales sur les réseaux informatiques*» , 2009.

[10] D .LACHIVER, « *Utilisation du réseau pédagogique*», édition 2013.

[11] P. ATELIN, « *Réseaux informatiques Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi, ...)*». Editions ENI, 407 pages, 2009.

[14] P. ATELIN , J. DORDOIGNE,« *TCP/IP et les protocoles Internet. Editions ENI*», 190 pages, 2008.

[15] P.Irsapoulle, *« Mise en place d'un outil de supervision et de contrôle distant»*, Mémoire de Master M2, Université de la Réunion, 2014 .

[16] G. BEN SASSI, *«Mise en place d'un outil de supervision de réseau d'entreprise»*, Mémoire de Mastère Professionnel, Université Virtuelle de Tunis, 2015.

[17] P.Djibril, P.Clavair N.Amadou, *«Étude et mise en place d'un outil de supervision du système d'information de SOFTNET»*, 2017/2018.

[18] C.Pierre-Adrien et R.Serge ,*« Supervision réseau »*,2015.

[21] N.kamma Ouandji ,*«Monitoring : supervision et métrologie | Supervision | IT-Connect | Base, Historique, Etat»*, 30 mai 2016.

[22] A.Hatim, *«ETUDE ET MISE EN PLACE D'UNE SOLUTION DE MONITORING OPEN SOURCE»*, 2017/2018 .

Webographie

[2] https ://www.techno-science.net/definition/3788.html.

[7] http ://www.dell.com/virtualization.

[12] https ://web.maths.unsw.edu.au/ lafaye/CCM/internet/protocol.htm , consulter le 10/07/2021.

[13] https ://www.frameip.com/entete-arp/ ,consulter le 10/07/2021.

[19] http ://www.cisco.com/web/FR/documents/pdfs/datasheet/ios/NETWORK_CONNECTIVITY.pdf.

[20] http ://www.o00o.org/monitoring/introduction.html

[23] https ://docs.centreon.com/current/en/

Résumé

Actuellement, les systèmes informatiques et réseaux sont très utilisés dans les entreprises. Ces réseaux sont devenus très importants en termes de nombre des équipements et en termes de services qu'ils offrent.

INSIM Bejaia nous a confié la mise en place d'un outil de supervision de son système d'information à travers un stage de 05 mois ; une solution qui va permettre la supervision complète de son parc informatique. Ainsi, la solution Centreon a été retenue. Nous l'avons choisi après une étude comparative des différents outils de supervision existant sur le marché. L'outil déployé permet de contrôler tout type de système d'information. En somme, l'objectif de ce travail est de coupler la puissance de Centreon au système d'information d'INSIM Bejaia afin de garantir le bon fonctionnement de l'infrastructure en automatisant la gestion,le diagnostic et le contrôle du réseau informatique. Nous avons montré l'efficacité de l'outil de supervision Centreon, à base de protocoles SNMP via plusieurs tests.

Notre outil de supervision est mis en place et fonctionnel au niveau de l'INSIM Bejaia.

Abstract

Currently, computer systems and networks are widely used in companies. These networks have become very important in terms of the number of equipment and in terms of the services they offer.

INSIM Bejaia entrusted us with setting up a supervision tool for its information system through a 5-month internship; a solution that will allow complete supervision of its IT equipment. Thus, the Centreon solution was chosen. We have chosen after a comparative study of the various existing supervision tools on the market. The deployed tool makes it possible to control any type of information system. In short, the objective of this work is to couple the power of Centreon to the information system of INSIM Bejaia in order to guarantee the proper functioning of the infrastructure by automating the management, diagnosis and control of the IT network. We have shown the effectiveness of the Centreon monitoring tool, based on SNMP protocols, via several tests.

Our supervision tool is set up and operational at INSIM Bejaia level.