Sommaire

Liste des figures

Introduction générale

Ces dernières années le développement de l'internet et des nouvelles technologiques ne cesse plus d'évolué pour faciliter de plus en plus la vie quotidienne et professionnel.
Les entreprises utilisent leurs réseaux pour y mettre ses données, ils doivent alors être toujours disponible et garantissent la qualité de service.
Les réseaux informatiques représentent un élément de base pour la transmission des données entre les sites distants. Sur les réseaux physiques de nombreuses composantes sont donc à surveiller : l'utilisation de la largeur de bande, l'état de fonctionnement des liens, les problèmes de câblage, le bon cheminement de l'information entre les machines, etc. Pour ce faire différents points stratégiques sont à observer comme les routeurs, les serveurs, les liens, les postes, les imprimantes. Ainsi, en cas de panne ou de mauvais fonctionnement sur le réseau, l'administrateur doit pouvoir interpréter l'information reçue pour identifier la source du problème. Pour cela on a vu l'utilité de recourir aux outils de supervision des réseaux afin d'accomplir cette tâche.
C'est dans ce cadre que se situe ce projet de fin d'études. Il est conduit et développé au sein de la société OTC (Office de la Topographie et de Cadastre) dans le but de mettre en place un outils de supervision du réseau permettant de vérifier si les routeurs sont fonctionnels, afficher une cartographie de réseaux, et envoyer en cas de problème une notification à l'administrateur.

Le présent document est structuré en quatre chapitres.

Dans le premier chapitre nous décrivons l'entreprise d'accueil et le cadre du projet. Tout d'abord nous présentons l'organisme d'accueil et les différentes taches effectués par l'office. Ensuite, nous traitons le sujet de travail à réaliser ainsi que ses différentes étapes.
Dans le second chapitre nous présentons une étude théorique du sujet. Le troisième chapitre est consacréé à la spécification des besoins et les outils nécessaires à la réalisation de l'application.
Le quatrième chapitre est réservé pour la spécification et l'implémentation et les interfaces de tests de l'application.

Chapitre 1

Présentation de l'organisme d'accueil et cadre du projet

Introduction

Ce chapitre introductif a comme objectif de mettre notre travail dans son contexte général. Tout d'abord, nous commençons par faire une présentation de l'organisme d'accueil OTC ou nous avons effectué notre stage, ensuite nous présentons le sujet de ce projet en détaillant son cadre et ses fonctionnalités.

1. Présentation de l'organisme d'accueil

L'Office de la Topographie et du Cadastre – **OTC** est un Etablissement public de la Ministère de l'équipement, de l'aménagement du territoire et du développement durable .elle offre plusieurs fonctionnalités aux publics concernant les travaux d'états.

Les activités du service topographique se limitaient aux travaux topographiques relatifs à l'immatriculation foncière facultative.

Les activités du service se sont développées pour englober les travaux d'immatriculation foncière obligatoire en application, l'entretien du réseau géodésique et du réseau de nivellement général.

2. Activité de l'OTC

2.1. Activité topographiques

2.1.1. Immatriculation foncière facultative

Elle a pour objet d'assainir la propriété et la doter d'une organisation appropriée aux exigences des crédits.

Cette procédure est l'œuvre :

- Du tribunal immobilier qui engage les procédures de l'immatriculation.
- De l'office de la topographie et du cadastre qui assure le bornage, le levé topographique et l'établissement du plan.
- La conservation de la propriété financière qui inscrit l'immeuble sur le registre foncier en le dotant d'un numéro de titre.

2.1.2. Cadastre : immatriculation foncière obligatoire

Elle suit le même processus que l'immatriculation foncière facultative.

2.1.3. Lotissements

Le morcellement ou le lotissement au sol ou en copropriété est l'opération de divinisions d'une parcelle de terrain d'un titre foncier en deux ou plusieurs lots en vue de leurs mutations partielles.

2.1.4. Rétablissement des limites

Le rétablissement des limites est une opération qui permet de restituer exactement, sur le terrain, les limites totales ou partielles d'une propriété immatriculée, il s'effectue avec la précision du levé initial**.**

2.1.5. Travaux topographiques divers (TPD)

L'OTC peut exécuter ,par contrat , les travaux de plans parcellaires de levés topographiques de plans côtés ,de profils en long et en travers, de délimitation du domaine public, d'expertises, d'enquêtes foncières…

2.1.6. Systèmes d'informations foncières

Afin de satisfaire des utilisateurs de plus en plus exigeants dans le domaine topographique, l'office de la topographie et du cadastre a procédé à la mise en place d'un système d'informations foncières (SIF) fiable et simplifié permettant une meilleur gestion des titres foncières et un traitement rapide de l'information, avec possibilité de mise à jour à tout moment **.**

2.2. Activités Géodésiques

2.2.1. Géodésie et Nivellement

L'objectif de la géodésie est de mettre en place un système de référence unique qui constitue la base de tous les travaux topographiques et cartographiques.
Ainsi l'office de la Cartographie et de Cadastre a équipé le territoire Tunisien des réseaux géodésiques indispensable à son infrastructure (primordial, secondaire et tertiaire).

L'Office de la Topographie et du Cadastre a adopté les techniques du système de Positionnement Global **GPS** et a introduit les techniques du GPS permanent et les activités gravimétriques.

De même, l'Office de la Topographique et du cadastre dispose d'un réseau de repères de nivellement dont les altitudes sont déterminées par rapport au niveau moyen de la mer avec une précision millimétrique nécessaire à :

- L'implantation des projets d'infrastructure
- La mise en place des réseaux hydrauliques et autres
- Le contrôle des barrages, des stades, des échangeurs et des constructions élevées

Il a introduit également les techniques de nivellement électronique dans sa chaine de production.

2.2.2. Travaux d'infrastructure de base

L'exécution des travaux de structure des lignes centrales des axes routiers, des gazoducs, des pipelines de gaz, des canaux d'irrigation, des puits de pétrole, des ports, de la surveillance des barrages, des aéroports, des titres des pistes, des changements des modèles d'antennes**.**

2.3. Photographie Aérienne

2.3.1. Prises de vues aériennes

L'Office de la Topographie et du cadastre dispose d'un avion photographe (en collaboration avec le centre national de cartographie et de télédétection) destiné à prendre des photographies aériennes nécessaire au cadastre .

De même, l'OTC satisfait, sur demande, divers autres besoins des opérateurs de l'Urbanisme, de l'Aménagement du Territoire et de l'Environnent.

3. Missions principales de l'OTC

L'office de la topographie et du cadastre a pour mission :

- L'établissement des plans topographiques de toute sorte, à l'exclusion de ceux relatifs à l'immatriculation foncière.
- L'établissement des plans de morcellement et lotissement des terrains et des constructions soumises au régime de la copropriété des immeubles divisés par étages ou par appartements situés dans les zones couvertes par ces plans d'aménagement ou dans les zones requérant l'établissement de ces plans.

- L’établissement des plans d’incorporation et de fusion
- Le rétablissement d’un système d’information géographique conforme à la spécialité et dans la limite des missions précitées
- L’exécution et le contrôle des travaux techniques d’immatriculation de la propriété foncière et du cadastre
- La définition et la mise à jour les cartes de report assurant l’inventaire des immeubles immatriculés
- L’exécution des travaux topographiques en Tunisie et à l’étranger et de procéder, également à la demande, à la délimitation des domaines publics, des terres domaniales, ainsi que les circonscriptions administratives.
- L’exécution des travaux nécessaires en Tunisie pour assurer sur le territoire national, l’implantation et la conservation d’un réseau de nivellement de précision.
- L’entreprise des études et des recherches dans les domaines de sa spécialité ainsi que dans les domaines annexes ou connexes.
- Le rétablissement des limites de propriété.
- Les travaux topographiques divers.
- L'établissement des cartes touristiques et thématiques.
- La prise de vues aériennes et l''établissement des plans topographiques à grande échelle.

Ces travaux constituent la base et la référence de tous les projets de développement et d'infrastructure.

L’exécution de certains de ces taches se fait en se basant sur des données enregistrés et récupérés par le billais des stations appelés stations GNSS (Global Navigation Satellite System).

4. Stations GNSS

Le réseau GNSS (Global Navigation Satellite System) permanent :Ce terme générique désigne non seulement le GPS américain mais également tous les autres systèmes (le système russe Glonass, le système européen Galileo, le système chinois Compass/ Beidou, etc…) il faut insister sur le fait que ce nouveau récepteur est compatible avec tous les systèmes mondiaux et ceux à venir [15].

En fait c'est un réseau de plusieurs centaines de stations GNSS qui enregistrent en continu les informations envoyées par les satellites des différentes constellations de satellites artificielles permettant de se localiser en tout point de la surface terrestre.

Les données enregistrées au niveau des stations sont mises à disposition des utilisateurs sous la forme de fichiers horaires ou journaliers, dans un délai le plus bref possible, pour permettre un positionnement différentiel centimétrique.

Figure 1 : Station Permanente GNSS

5. Etude de l'existant

L'OTC dispose d'un réseau informatique composé de :

- Des stations GNSS: Enregistrement et envoi des données au format RINEX.
- Une station Météo: Enregistrement des données Météorologique.
- Un Tilt Meter: Détecteur de mouvements et d'inclinaison.

En plus, chaque station contient des équipements de protection électrique de communication qui ont pour rôle de relier les stations au serveur situé au à Tunis. Ces stations GNSS permanentes permettant de fournir plusieurs types de données.

6. Problématique

Il est communément admis qu'aujourd'hui, il est de plus en plus difficile d'administrer un réseau informatique tant les solutions sont complexes, les éléments constituant ces réseaux sont diversifiés et les besoins fonctionnels et de sécurité sont variés. En effet le nombre d'équipements à gérer est souvent de plus en plus important et diversifié : stations, serveurs, imprimantes, etc. Le plus grand souci d'un administrateur est la rupture d'une connexion

réseau. En effet, il doit pouvoir la détecter et l'identifier le plus rapidement possible et réagir en conséquence pour y apporter les solutions correctives ainsi que les réparations nécessaires.

Ce besoin de réactivité nécessite donc de pouvoir surveiller de manière continue l'état du réseau et des systèmes d'information. C'est là où intervient la mission de supervision du réseau de l'OTC. Elle doit permettre d'anticiper les problèmes en faisant remonter des informations sur l'état des équipements. Plus le système est important et complexe, plus la supervision devient compliquée sans des outils adéquats.

7. Contexte du projet

Toute application de supervision réseau est destinée avant tout à simplifier la tâche de l'administrateur qui est tenu d'intervenir en cas de panne. Celle que nous devons mettre en place doit assurer aussi cette mission. Elle se charge de détecter tout d'abord la faille, de la localiser, avec la possibilité d'envoyer un mail à l'administrateur ou bien au groupe d'utilisateur et ensuite d'essayer de la réparer afin d'assurer la continuité de fonctionnement du réseau dans les meilleures conditions de performance possibles.

Cette solution doit permettre de localiser les nœuds administrés, d'envoyer les informations sur les équipements défectueux vers le nœud de supervision et ainsi de prendre en charge le maintien.

Notre application de supervision doit offrir donc plus de simplicité d'utilisation, plus d'efficacité mais aussi plus de visibilité, elle devra non seulement tenir compte des problèmes actuels mais également être capable d'évoluer facilement et efficacement au rythme des besoins.

A la fin de notre travail, nous devons pouvoir :

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

8. Architecture du réseau informatique de l'OTC

Comme il est indiqué dans la figure 1, le réseau de l'OTC est constitué principalement par des liaisons MPLS en fibres optiques, où tous les sites sont connectés en VPN et sont centralisés et administrés par l'opérateur Tunisie Télécom. Ces liaisons connectent un ensemble de routeurs de type cisco 1841 au serveur situé au siège de l'OTC. Les routeurs se trouvent dans plusieurs sites couvrant ainsi tout le territoire Tunisien.

Dans ce projet, nous allons surveiller les routeurs distants liés chacun à une machine située derrière ce routeur appelée station GPS permanente (GNSS).

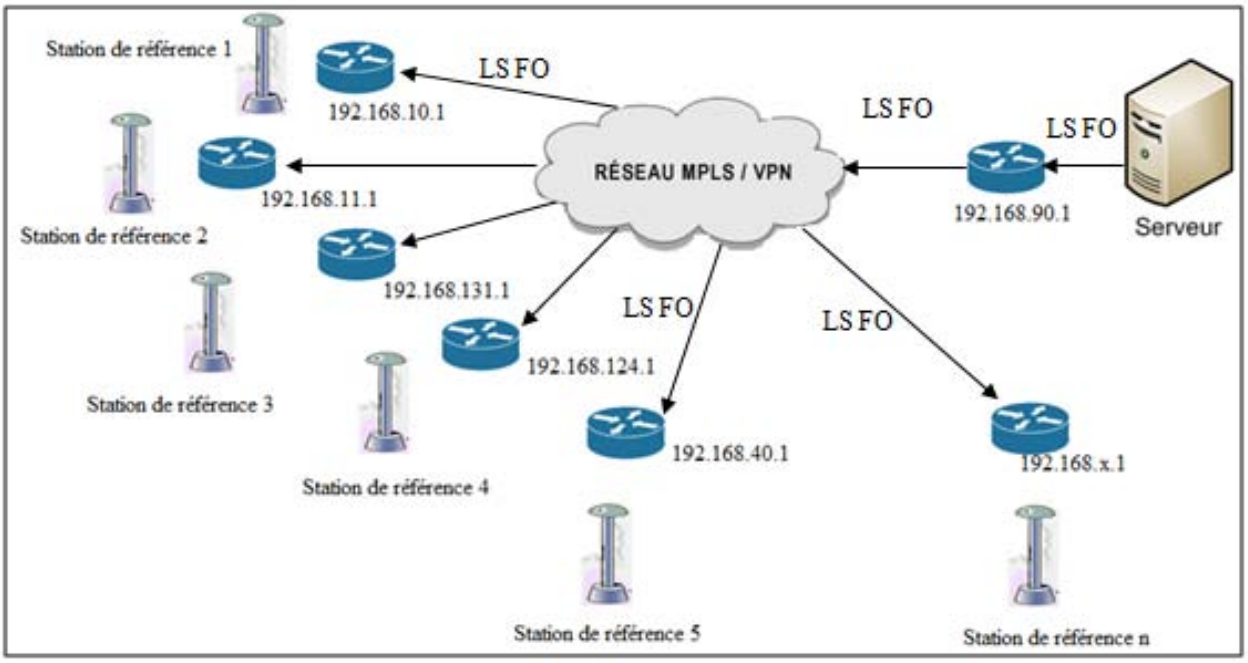


Figure 2: Architecture réseau de L'OTC

Chaque station de référence est implémentée comme suit :

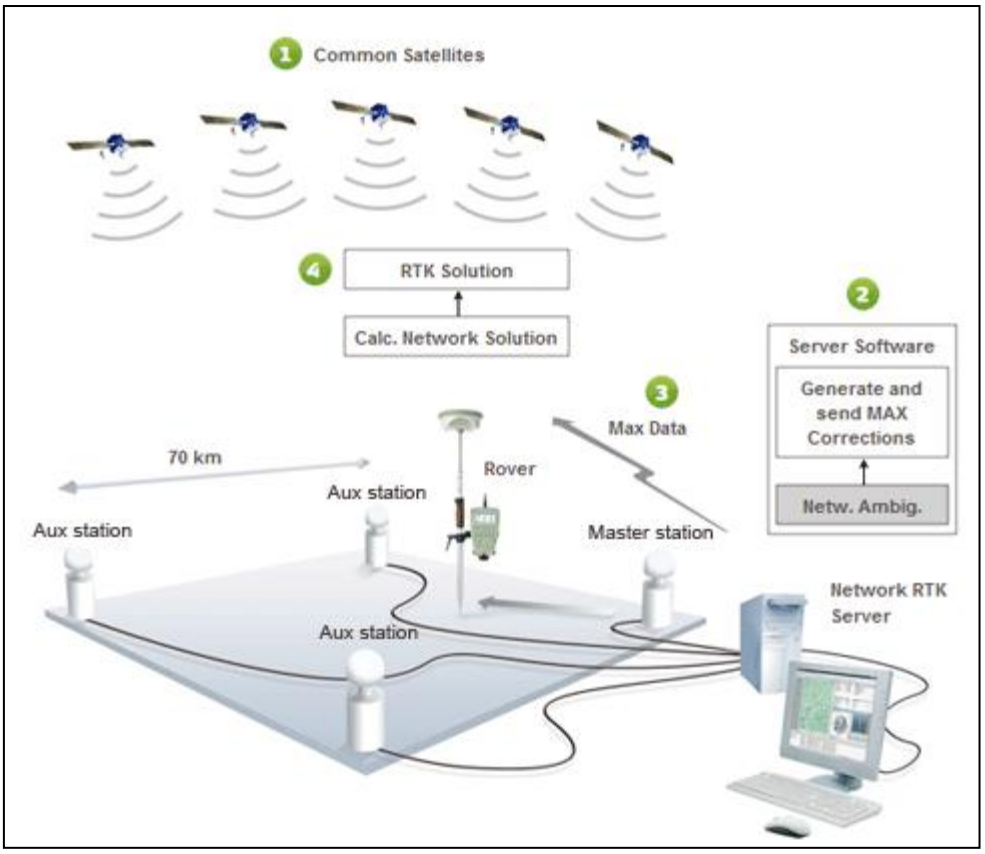


Figure 3: Exemple station de référence

Le principe de fonctionnement d'une station se résume en 4 étapes (figure 2) :

- le rover et le serveur de réseau RTK (à travers les stations de référence) observent un ensemble de satellites. Les données des stations de références sont envoyées aux serveurs toutes les secondes
- Résoudre les ambiguïtés réseau: à l'aide d'un algorithme approprié, le serveur de réseau RTK résout les ambiguïtés du réseau et réduit les données satellitaires pour cette ambigüité.
- Génération des corrections RTK: Le serveur génère et envoie les corrections RTK au rover quelque soit la norme de représentation standard ou non standard (ambigüe).
- Solution RTK : Le rover utilise les corrections RTK pour calculer une solution RTK afin qu'elles soient ensuite transmis par le serveur à l'utilisateur via l'internet mobile.

8.1. Réseau VPN

Sur la longue route menant à la protection de la vie privée sur Internet, on entend de plus en plus parler des réseaux privés virtuels (VPN). Cette technique permet la création d'une liaison chiffrée entre une machine et un serveur hébergé sur Internet (par exemple chez un

fournisseur d'accès se trouvant dans n'importe quel pays). Tous vos accès à Internet seront alors vus à partir de l'adresse IP de ce serveur VPN et non plus par celle de la machine en question [24].

Certaines entreprises utilisent leur réseau local (LAN) pour communiquer avec des filiales, des clients ou même avec le personnel qui sont géographiquement éloignées, et ce via une interconnexion avec le réseau internet. Mais dans ce cas les données transmis sont plus vulnérable qu'une circulation des données sur un réseau interne à une entreprise car on ne peut jamais être sûre que sur le chemin parcouru la liaison ne soit pas intercepté.

La solution à ce problème se trouve dans l'utilisation d'un réseau VPN (Virtual Private Network). Ce réseau est dit **Virtual** car il relie deux réseaux physiques (réseaux locaux) par une liaison non fiable (Internet), et P**rivate** car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données.

Le principe de fonctionnement d'un tel réseau VPN consiste à utiliser le réseau Internet comme support de transmission et ce en utilisant un protocole d'encapsulation qui permet d'encapsuler les données à transmettre de façon chiffrée [21].

Le réseau de l'**OTC** se compose principalement d'un serveur et de 32 routeurs se trouvant dans différents sites sur le territoire Tunisien. Ces routeurs sont liés entre eux par des liaisons LS en fibres optiques constituants ainsi un **VPN/MPLS** dont les données circulant entre les différents sites réseau ne transitent pas via Internet.

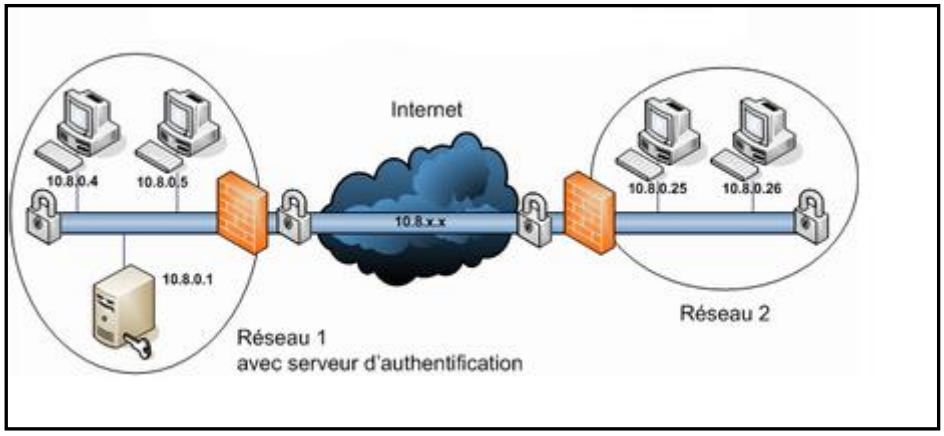


Figure 4 : principe de fonctionnement d'un réseau privé virtuel (VPN)

8.2. Protocole MPLS

MultiProtocol Label Switching (MPLS) est un protocole de transport de données développé par Cisco dont le principe se base sur la commutation d'étiquettes (labels). Ces derniers sont

simplement des nombres entiers et qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie. Les routeurs permutant alors ces labels tout au long du réseau jusqu'à destination, sans avoir besoin de consulter l'entête Ip et leur table de routage.

Le protocole MPLS vient alors pour assurer la gestion des VPN-IP et ainsi satisfaire les besoins des operateurs des servives VPN.

VPN-MPLS est donc une famille de méthodes donnant une plus grande puissance aux commutateurs pour améliorer les performances de réseau IP (Internet Protocole) et ce par le principe de commutation multiprotocole par étiquette (MPLS).

VPN-MPLS permet aux ingénieurs de réseau la flexibilité de transporter et de router plusieurs types de trafic réseau et d'accélérer la transmission des informations au sein d'un backbone IP.

8.3. Routeurs

Un routeur est un élément intermédiaire dans un réseau informatique qui permet de choisir le chemin à emprunter par le message à envoyer. Ce routage est réalisé selon un ensemble de règles formant la table de routage. Ils manipulent les données (qui circulent sous forme de datagrammes: paquets) afin de rendre le passage d'un type de réseau à un autre plus souple. Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en terme de la taille des paquets de données. Les routeurs ont donc la possibilité de fragmenter les paquets de données pour permettre leur circulation.

Les routeurs sont capables de créer des cartes (tables de routage) des itinéraires à suivre en fonction de l'adresse visée grâce à des protocoles dédiés à cette tâche.

Un routeur possède plusieurs interfaces réseau, chacune connectée sur un réseau différent. Il possède ainsi autant d'adresses IP que de réseaux différents sur lesquels il est connecté.

L'OTC utilise dans son architecture réseau des routeurs Cisco 1841 qui se caractérise par une importante valeur ajoutée par rapport aux générations précédentes de routeurs. Ses principales caractéristiques différenciatrices sont : la multiplication par cinq des performances sécurité ainsi qu'une augmentation considérable en terme de capacités et de densité d'emplacements d'interfaces. Il peut supporter plus de 30 cartes. De plus, le routeur Cisco 1841 dispose en option d'un système de prévention des intrusions (IPS), de fonctions de pare-feu à inspection d'états, d'un renforcement des performances des réseaux privés virtuels (VPN) grâce à des fonctions de cryptage matériel embarquées. Il dispose de nouvelles interfaces haute densité offrant au final un large choix d'options de connectivité Lan / Wan qui associé à une haute densité d'emplacements comme des interfaces commutateurs LAN multiports intégrés. Ces

interfaces garantissent une évolutivité maximum de la plateforme pour répondre aux besoins d'extension future du réseau [25]

Conclusion

Au cours de ce chapitre, nous nous sommes intéressées à la présentation de l'entreprise d'accueil déterminant par la suite la problématique, qui nous intéresse dans ce projet, se manifestant dans la bonne supervision de leur réseau informatique. Nous entamerons dans le chapitre suivant une étude théorique de la notion d'administration et de supervision réseau.

Chapitre 2

Etude théorique et état de l'art

Introduction

Les réseaux sont devenus indispensables au bon fonctionnement général de nos entreprises et administrations. Tout problème ou panne sur ces réseaux peut avoir de lourdes conséquences aussi bien financières qu'organisationnelles. C'est pour cela la supervision des réseaux est une nécessité primordiale et indispensable. Elle assure une suivie de la disponibilité des services en ligne, d'avoir une vue globale sur le fonctionnement et les problèmes pouvant survenir sur un réseau et aussi de disposer des indicateurs sur les performances de son architecture. Nous consacrons le présent chapitre à la présentation des concepts de base de supervision des réseaux.

1. La supervision des réseaux

1.1. Définition

La supervision réseau est un ensemble de protocoles, matériels et logiciels informatiques assurant plusieurs les activités suivantes : surveiller, visualiser, analyser et agir.

Cette opération est assuré par l'utilisation de ressources réseaux adaptées (matérielles ou logicielles) capable de fournir des informations sur l'état des réseaux et ses machines distantes. Il faut donc disposer d'une console de supervision qui regroupe et synthétise toutes les informations. On supervise pour avoir une visibilité sur le système d'information. Cela permet de disposer rapidement des informations, de connaître l'état de santé du réseau, des systèmes, ainsi que leurs performances. Ce qui donne rapidement une image du système étudié.

Grace à Ces informations on peut gérer de manière automatique les pannes et les problèmes de surcharge survenant sur le réseau [1].

1.2. Principe

Le suivi régulier du bon fonctionnement de l'ensemble des équipements présents sur le réseau d'une entreprise et l'optimisation permanente de ses performances sont des fonctions incontournables.

En général, La mise en place d'une solution de supervision permet d'avoir une vue d'ensemble en temps-réel des équipements supervisés. Elle permet de visualiser à tout moment l'état des différents équipements configurés. Ainsi les objectifs sont multiples:

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

Un administrateur peut être informé, par le biais d'une alarme (SMS, mail..), à n'importe quel moment des problèmes qui peuvent survenir sur les équipements [2].

1.3. Fonctionnement d'une plateforme de supervision

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

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

1.4. Les méthodes de supervision

L'opération de supervision se fait selon 2 manières (figure 4), la supervision active et la supervision passive :

- La *supervision active* : consiste sur le fait que l'outil de supervision décide quand il fait le test sur l'équipement à superviser .elle se base sur l'envoi des requêtes avec différents protocoles de communication vers une destination d'un équipement pour tester sa connectivité et son bon fonctionnement.
- Dans la *supervision passive*, c'est l'hôte qui décide quand elle renvoie son information vers la plate-forme de supervision .Ses informations sont de types des traps SNMP, syslogs etc., puis déclenche une action en fonction de l'analyse des informations reçues.

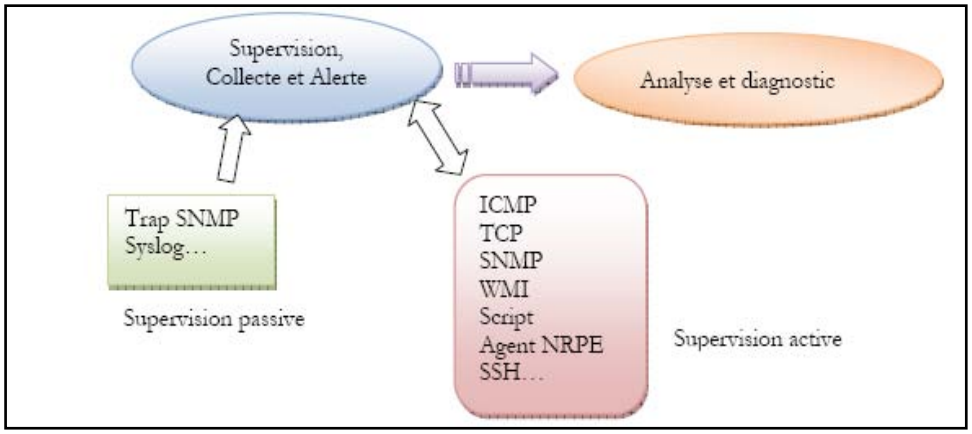


Figure 5: supervision passive et active

2. Protocole d'administration réseau

2.1. SNMP

SNMP est un protocole principalement utilisé pour superviser des équipements réseaux (routeurs, switchs…), des serveurs ou même des périphériques tels que baies de disques, sondes météorologique, onduleurs...

C'est le protocole de supervision le plus simple et le plus utilisés pour la gestion des reseaux.il permet aux administrateurs réseau de gérer, à distance, les équipements du réseau et de diagnostiquer les problèmes survenant sur un réseau.

2.1.1. Principe de fonctionnement

SNMP fonctionne avec les technologies utilisant les protocoles TCP/IP et s'appuie sur le protocole UDP (User Datagram Protocol) (figure 5).

SNMP est basé sur trois éléments :

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

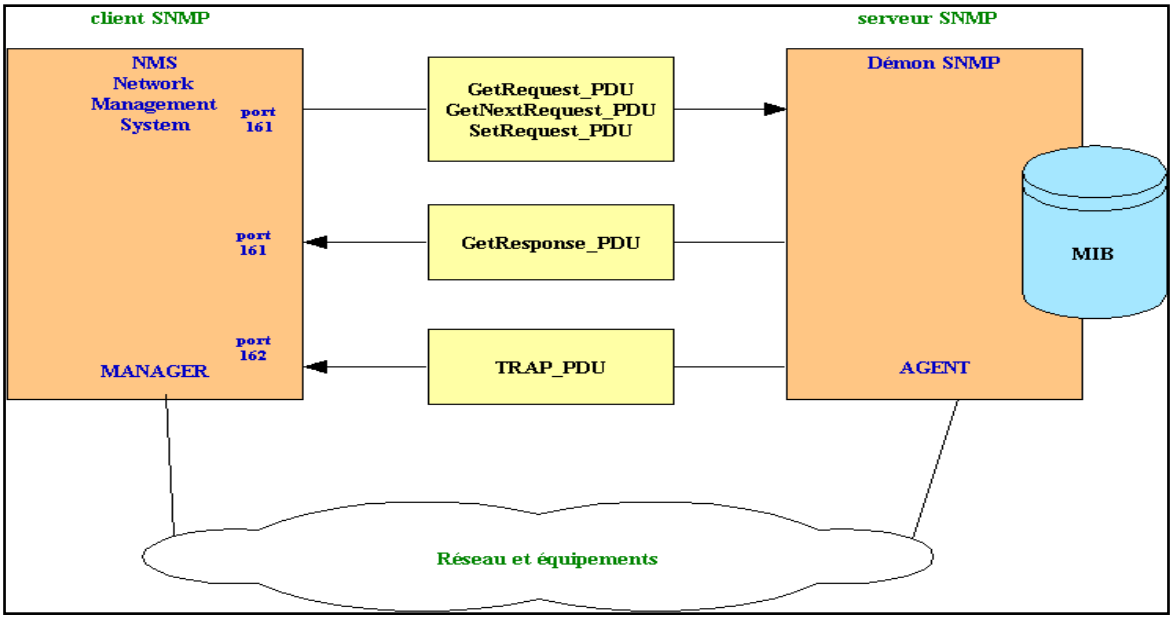


Figure 6 : fonctionnement SNMP

Chaque équipement sur lequel intervient l'administrateur via SNMP doit disposer d'un agent SNMP qui y soit installé. L'interrogation d'un agent se fait en lui envoyant des messages sur le port UDP 161. L'agent envoie des alertes à la console sur le port UDP 162. [10]

Les objets collectés sont des informations matérielles, des paramètres de configuration, des statistiques de performance ou bien d'autres sont regrouper dans la base de données MIB. [11]

2.1.2. MIB

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

2.2. ICMP

ICMP (*Internet Control Message Protocol*) est un protocole de gestion des informations concernant les erreurs des hôtes qui lui sont connectées. ICMP crée et envoie des messages à l'adresse IP source, indiquant qu'une passerelle vers l'Internet tel qu'un routeur, un service ou une hôte ne peuvent pas être atteints pour la livraison de paquets. Tout dispositif de réseau IP a la capacité d'envoyer, recevoir ou traiter des messages ICMP.

ICMP n'est pas utilisé régulièrement dans les applications de l'utilisateur final, il est utilisé par les administrateurs réseau pour contrôler les connexions Internet dans les utilitaires de diagnostic, y compris ping et traceroute.

3. Logiciels existants

3.1. Les logiciels libres

Un logiciel libre est un logiciel dont la licence permet de sauvegarder la liberté de l'utilisateur. Pour qu'un logiciel puisse être qualifié de « libre », quatre libertés fondamentales doivent être conservées: la liberté d'exécuter, de modifier le logiciel, la liberté d'en redistribuer des copies ou de distribuer des versions modifiées (Gratuitement ou contre de l'argent). Evidemment les deux logiciels libre de supervision les plus connus sur le marché sont: Nagios et Zabbix.

3.1.1. Nagios

C'est une application open source permettant la surveillance système et réseau. Elle surveille des services spécifiés des hôtes Windows et linux en alertant lorsque les systèmes vont mal.
Nagios, qui est une évolution de Netsaint auquel a été ajoutée, entre autres, la gestion du protocole SNMP, est conçu pour fonctionner sous un système d'exploitation Linux. Cet outil propose de superviser les machines et les services d'un réseau via des plugins indépendants, chacun responsable d'un test particulier [12].

Nagios récupère les informations fournies par les services de surveillance et les analyse. Si le résultat de cette analyse fait remonter un problème, les services de surveillance peuvent envoyer des avertissements à l'administrateur du réseau de différentes manières : courriers électroniques, messages instantanés, SMS, etc [3].

a. Architecture

Nagios repose sur un serveur web et des CGI. Il intègre une base de données de type *MySQL* pour y stocker des informations de supervision. L'architecture standard de Nagios peut donc être représentée de la manière suivante : [2]

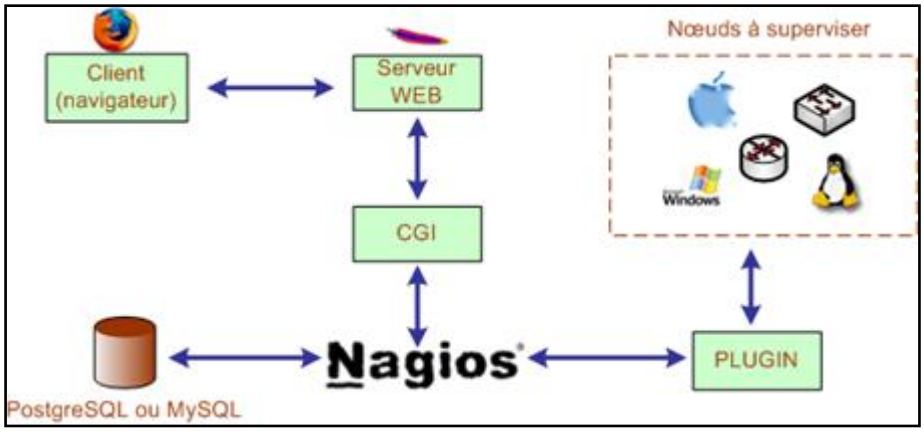


Figure 7: Architecture de Nagios

Comme le montre la figure si dessus l'architecture de Nagios se base sur le paradigme serveur-agent. D'une manière générale, un serveur fait office de point central de collecte des informations. Les autres machines du réseau exécutent un agent chargé de renvoyer les informations au serveur [4].

Nagios va être couplé avec Centreon permettant par ceci de faciliter l'administration mais aussi de remonter les graphes et d'effectuer du reporting .

Les principaux avantages et les inconvénients de Nagios sont :

b. Avantages

Nagios possède de nombreuses fonctionnalités, dont voici les principales [13] [4]:

- Surveillance des services réseaux (SMTP, POP3, HTTP, PING, etc)
- Surveillance des ressources des équipements (serveur, routeur, etc) comme la charge du processeur, des informations sur l'utilisation des disques durs, les processus en cours.
- Interface web, pour voir l'état actuel du réseau, notification et historique des problèmes, fichiers log, etc.
- Surveillance des données environnementales comme par exemple la température.
- Système simple de plugins permettant aux utilisateurs de développer facilement leurs propres vérifications de services.

c. Inconvénient

Les principaux inconvénients de nagios sont :

- Configuration compliquée qui oblige une très bonne connaissance de Nagios.

- Graphes pas assez clairs.
- Administration compliquée

3.1.2. Zabbix

Zabbix est un logiciel de monitoring réseau Open source et multiplateforme. Il permet de surveiller le statut de divers services réseau, serveurs, postes de travail et autres matériels (routeurs, pare-feu, imprimantes, etc.) [6]

Zabbix offre des vues graphiques (générés par RRDtool) et des alertes sur seuil. Il peut être décomposé en 3 parties séparées: Le serveur de données, l'interface de gestion et le serveur de traitement. Chacune d'elles peut être disposée sur une machine différente pour répartir la charge et optimiser les performances. Un agent ZABBIX peut aussi être installé sur les hôtes Linux, UNIX et Windows afin d'obtenir des statistiques comme la charge CPU, l'utilisation du réseau, l'espace disque... Le logiciel peut réaliser le monitoring via SNMP [7].

a. Caractéristiques

Pour Zabbix on distingue les caractéristiques suivantes :

- Outil de supervision libre
- Auto découverte des machines du réseau
- Mise en place de tests indépendants sur les machines
- Gestion des alertes

b. Avantages

Citons quelques caractéristiques de l'outil de supervision Zabbix :

- Facilité d'installation
- Génération facile des graphs
- Facilité de consultation des graphs en fonction du temps
- Affichage clair des erreurs sur le Dashboard

c. Inconvénients

Parmi les inconvénients de Zabbix on distingue :

- Chaque machine à superviser doit disposer du client Zabbix
- Limité au ping sans le client

- Problème de configuration sur le switch

3.2. Les logiciels propriétaires

Parmi les logiciels propriétaires à licences payantes les plus connus nous allons étudier HP openview et cisco works.

3.2.1. 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 [13].

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

HP OpenView 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 [13].

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).

a. Avantages

HP OpenView possède des avantages parmi lesquelles on trouve :

- Une vue globale du réseau.
- Une vision des différents incidents.

b. Inconvénients

L'inconvénient majeur de l'outil HP OpenView est :

- Coût d'acquisition et de support

3.2.2. CiscoWorks

Cisco Works (**N**etwork **C**onnectivity **M**onitor **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, ***Cisco Works*** NCM détecte les modifications apportées aux périphériques Cisco et ajuste son analyse en conséquence [8].

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, et il est possible pour chaque équipement de configurer des VLANs dans une interface graphique simple, sans taper une ligne de commande en mode console [8].

a. 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.

b. Inconvénients

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

4. Solution Retenue

Le monde des outils de supervision est très vaste, dans ce rapport on eu recours à étudier quelques outils qui sont les plus connus sur le marché.

Dans notre cas, les solutions **Hp OpenView** et **Cisco Works** ne seront pas retenues car ils ne sont pas libre, sont couteuses et leurs interfaces sont plus compliquée à personnaliser que par exemples celles basées sur **Nagios.**

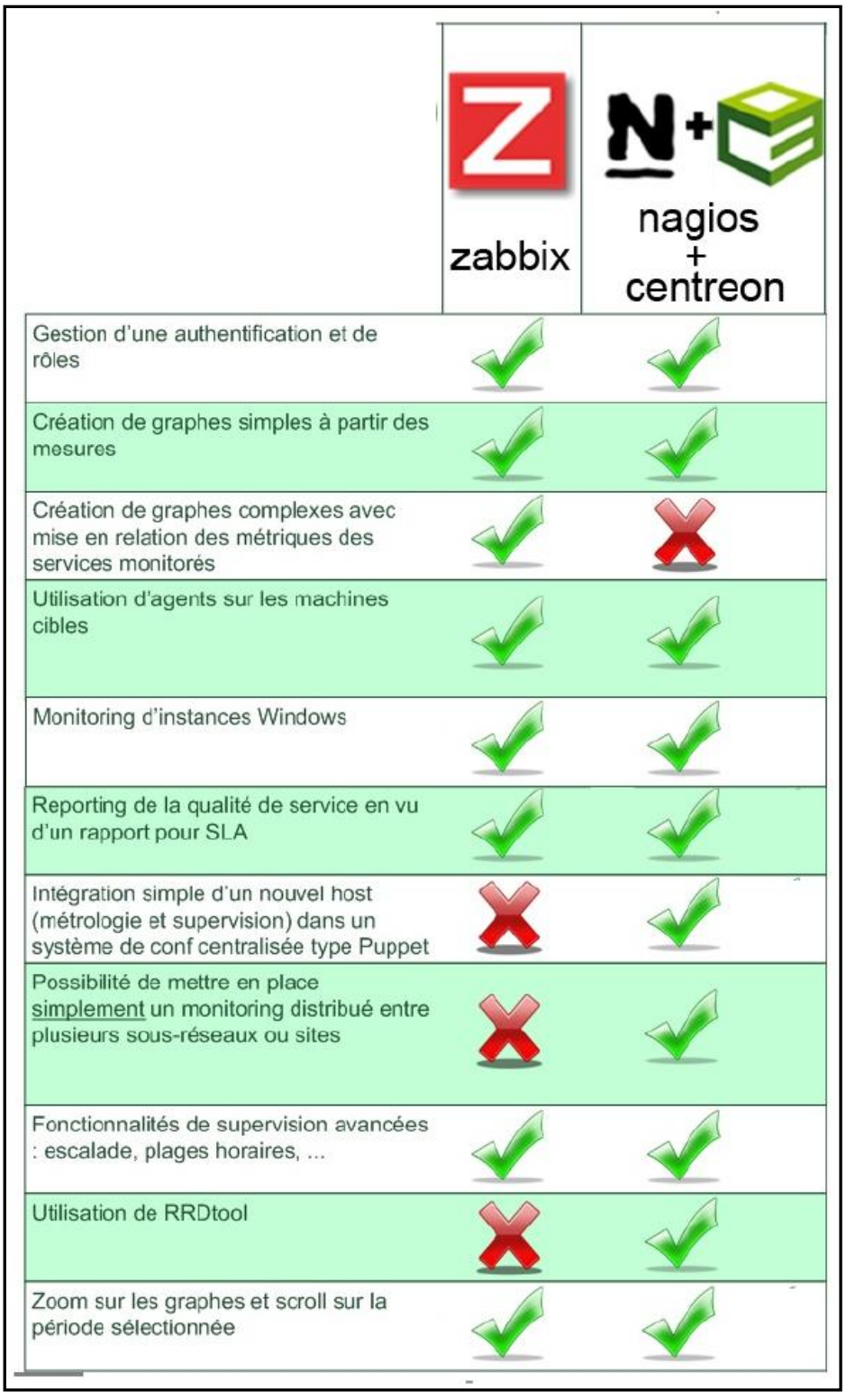


Figure 8 : Tableau comparatif entre Nagios et Zabbix

Selon les critères et les caractéristiques de chacun des logiciels libres cités dessus nous décidons l'utilisation de Nagios comme logiciels de supervision.

En effet, Nagios, couplé à Centreon, est une solution très performante, il est initiateur dans le monitoring possédant une large communauté qui met à disposition, en libre accès, des plugins SNMP préconfigurés [22].

L'utilisation de Centreon est préférée puisqu'il est :

- Le plus facile à configurer, adapter aux besoins et à mettre en place
- Le plus populaire en termes de qualité de monitoring avec une communauté très active et les ressources en documentations techniques sont donc nombreuses.
- Il nécessite moins de ressources pour le mettre en production.

Conclusion

Des solutions citées ci-dessus, HP OpenView, CiscoWorks, Zabbix et Nagios sont les plus connues. Qu'elles soient «Open Source » et gratuites ou propriétaires, chacune a ses particularités qui lui sont propres. Ces outils ont principalement pour objectif de connaître à tout instant l'état des nœuds critiques (serveurs, switchs, routeurs), l'état des services tournant sur les différents serveurs, d'envoyer des alarmes, de générer des comptes rendus graphiques. Ils doivent également être capables d'analyser le trafic réseau afin de permettre une meilleure répartition des ressources réseaux. Certains outils sont également des solutions payantes, donc à écarter de nos choix [13].

Après avoir décrit les plateformes de supervision existantes sur le marché, nous entamerons dans le chapitre suivant les différents besoins nécessaires à la réalisation de notre application.

Chapitre 3

Spécification des besoins, Conception et présentation des outils proposés

Introduction

Une étape primordiale dans le déroulement du projet se focalise sur le choix et l'étude de la solution ainsi que la phase de spécification des besoins. Dans ce chapitre, nous présentons l'étude de notre outil de supervision choisi et son mode de fonctionnement ensuite nous détaillons les besoins fonctionnels et non fonctionnels.

1. Spécifications des besoins

1.1. Besoins fonctionnels

L'objectif de ce projet est de mettre en place une solution de monitoring sur une machine virtuelle grâce à l'outil de virtualisation VirtualBOX. Cette application doit permettre de collecter des informations concernant une infrastructure informatique à plusieurs niveaux :

- La supervision des ressources des serveurs (charge du processeur, occupation des disques durs, utilisation de la mémoire paginée) sur la plupart des systèmes d'exploitation.
- La supervision des services réseau (SMTP, HTTP, NNTP, ICMP, SNMP, LDAP, etc…) en local ou sur des machines distantes.
- L'interfaçage avec le protocole SNMP.
- La vérification des services se fait en parallèle.
- La remontée des alertes est entièrement paramétrable grâce à l'utilisation de plugins
- Acquittement des alertes par les administrateurs.

1.2. Besoins non fonctionnels

Afin d'offrir une solution complète et performante à différents niveaux, notre plateforme doit couvrir les besoins non fonctionnels suivants :

- **Facilité d'utilisation** : Le système offre une interface simple facile à utiliser en donnant à l'administrateur la possibilité d'agir sur les ressources qu'il manipule.
- **Sécurité** : L'accès aux données doit être authentifié et autorisé par des moyens de sécurité.
- **Fiabilité** *:* Il faut garantir la qualité du contenu et la pertinence des informations. Le produit doit fonctionner correctement.

- **Rapidité** : Le logiciel de supervision prévient dés qu'un problème survient avant même que la plupart des utilisateurs en aient conscience.
- **Extensibilité**: Le système doit être extensible et permet d'ajouter et de supporter d'autres fonctionnalités et d'intégrer tout type d'équipement réseau.
- **La performance** : une application doit être avant tout performant c'est à dire à travers ses fonctionnalités, elle répond à toutes les exigences des usagers d'une manière optimale.

2. Formulation des besoins sous forme de cas d'utilisation

2.1. Présentation du langage de modélisation UML

UML (*Unified Modeling Language*) est un langage graphique de modélisation des données et des traitements. Il possède de multiples avantages : C'est un support de communication performant, il décrit une application en fonction des méthodes objet avec lesquelles elle a été construite. Il cadre l'analyse et facilite la compréhension de représentations abstraites complexes et il se caractérise par sa notation graphique simple qui permet d'exprimer visuellement une solution objet [28].

Dans UML chaque diagramme permet d'exprimer certains points d'un même problème. La combinaison de plusieurs digrammes permettra donc d'avoir une vue complète du système informatique. Ainsi en fonction du problème à résoudre, il convient de choisir les diagrammes adéquats à utiliser. [28].

Pour la réalisation de ce projet, il a fallu disposer d'un environnement de travail adéquat du point de vue conception, déploiement et test tout en prenant en compte les différentes technologies adoptées. Le logiciel StarUML nous a semblé être l'outil simple et idéal pour concevoir notre système vu les fonctionnalités qu'il offre.

2.2. Diagrammes des cas d'utilisations

Un diagramme de cas d'utilisation est un moyen simple d'exprimer des besoins. Il montre le comportement d'un composant, une classe ou un système, tel qu'un utilisateur extérieur le voit. Il correspond à un ensemble de transactions effectuées au cours d'une interaction entre l'acteur et le système.

2.2.1. Identification des acteurs

Globalement, nous avons distingué un seul acteur: l'administrateur, celui qui aura la fonction de la supervision réseau .en fait son rôle consiste à superviser le réseau en récupérant des informations sur les équipements et réparer les pannes détectées. Cet acteur utilise le système à travers un ensemble d'interfaces bien définies. Il doit s'authentifier pour qu'il puisse utiliser le système**.**

2.2.2. Description des cas d'utilisation

Afin de décrire les exigences fonctionnelles de notre système, voici une description du cas d'utilisation globale ainsi que d'autres qui sont les principaux.

a. Diagramme de cas d'utilisation générale

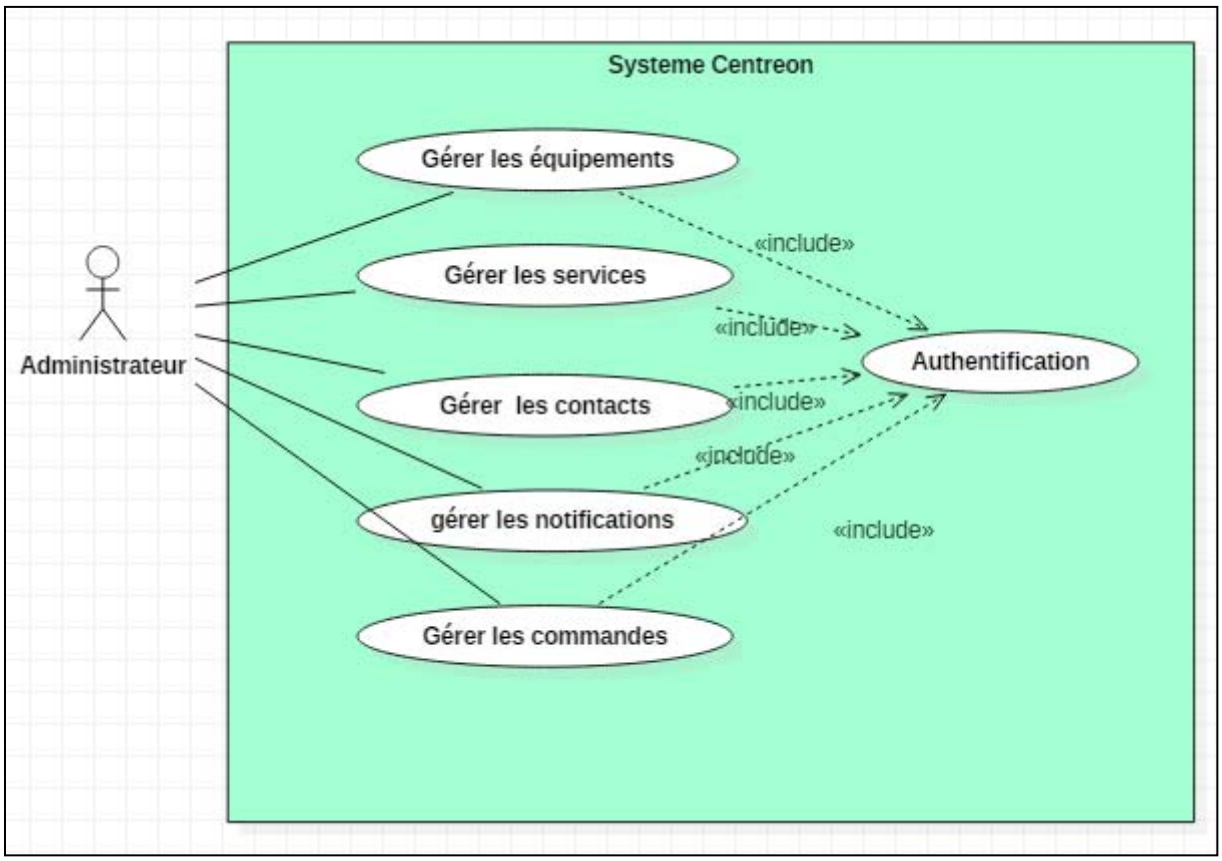


Figure 9 : Diagramme de cas d'utilisation générale du système

a. Diagramme de cas d'utilisation « s'authentifier »

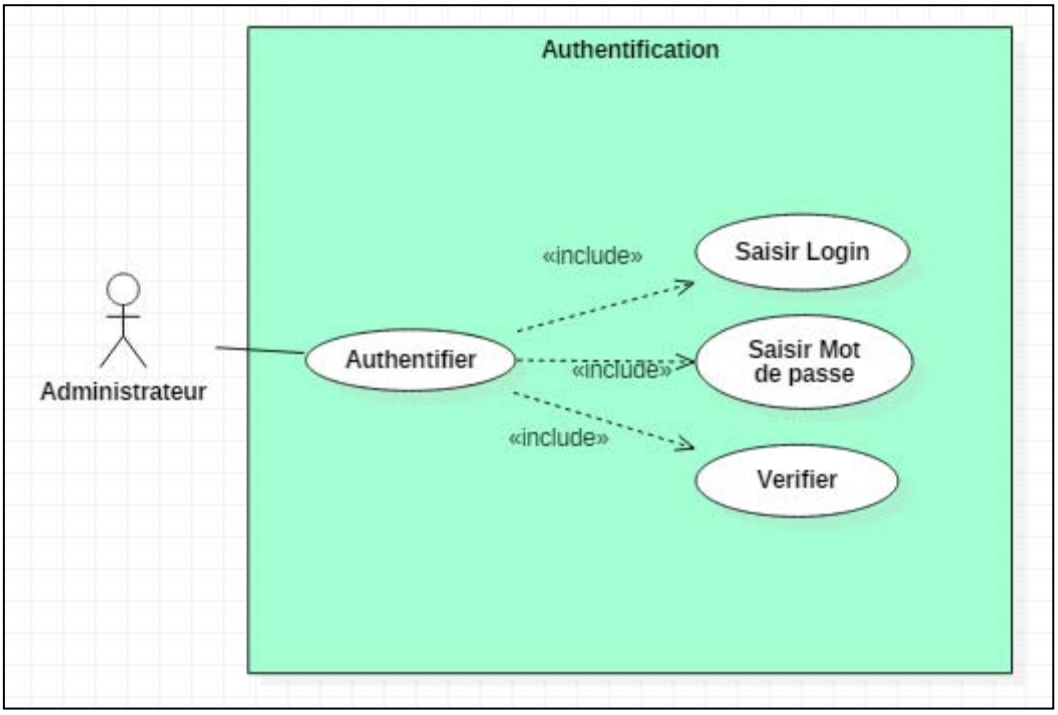


Figure 10 : Diagramme de cas d'utilisation « Authentification »

- **Titre : Authentification**
- **Objectif:** se connecter au système.
- **Acteurs: A**dministrateur.
- **Pré-Condition**: L'enchaînement démarre lorsque l'administrateur demande d'accéder au système.

Scénario nominal

- L'administrateur demande à s'authentifier.
- Le système affiche la page d'authentification.
- L'administrateur fournit son login et son mot de passe.

Enchaînement d'exception

Un message d'erreur sera affiché si le login et/ou le mot de passe sont incorrects.

Post-condition

L'administrateur peut accéder aux différentes fonctionnalités du système.

b. Diagramme de cas d'utilisation « Gestion des services »

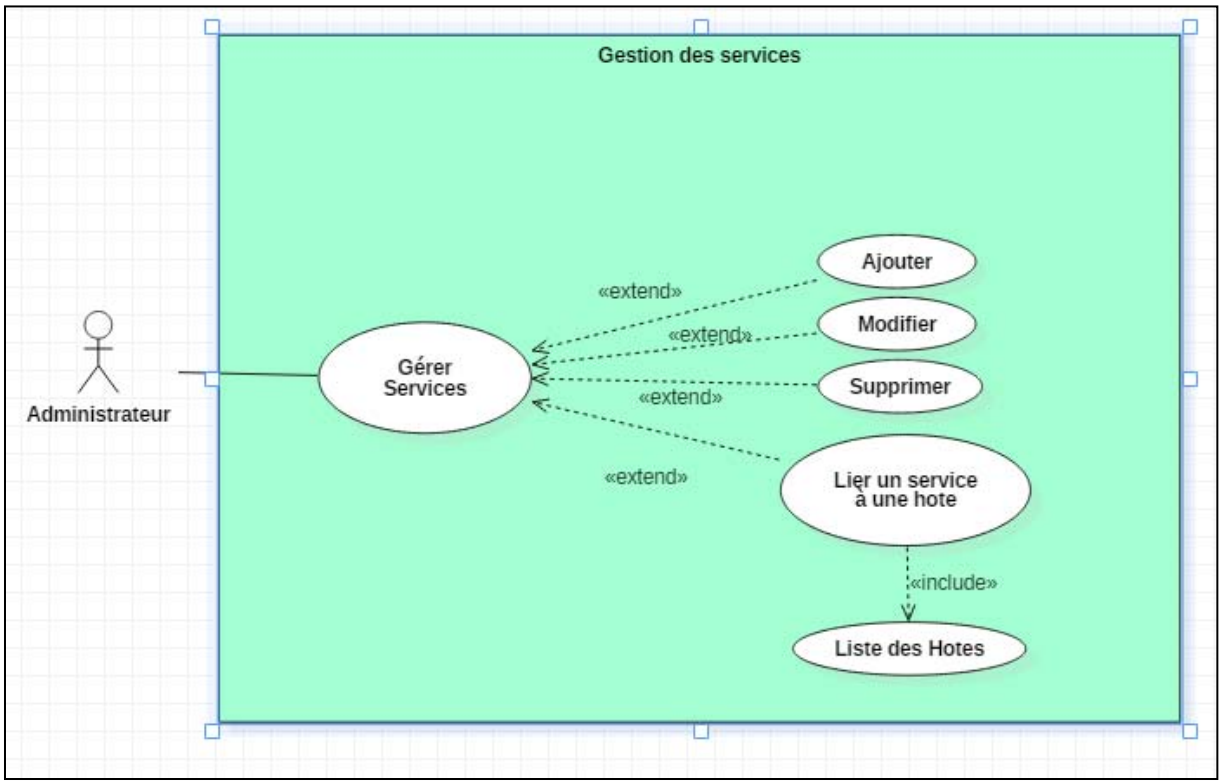


Figure 11 : Diagramme cas d'utilisation Gestion des services

- **Titre :** Gestion des services
- **Objectif:** ajouter, modifier, supprimer un service ou lier un service à une hôte parmi la liste des hôtes.
- **Acteurs: A**dministrateur.
- **Pré-Condition**: L'administrateur est déjà identifié.

Scénario nominal

- L'administrateur affiche la partie de gestion des services.
- L'administrateur choisi une opération à faire.
- L'administrateur effectue l'opération choisie précédemment.
- Le système enregistre les modifications effectuées.

Enchaînement d'exception

Un message d'erreur sera affiché si les informations introduites lors de l'opération sont incorrects ou si un champ obligatoire est vide.

Le Diagramme d'activités est un autre diagramme important dans UML pour décrire les aspects dynamiques du système. Il est essentiellement un organigramme pour représenter le flux d'une opération vers une autre opération.
La description d'un cas d'utilisation par un diagramme d'activités correspond à sa traduction algorithmique.

2.2.3. Diagramme d'activité « Notification »

Ce diagramme décrit les différentes activités que prend le système lorsqu'il détecte un service ou équipement non fonctionnel. A ce stade le système commence par vérifier l'état du service correspondant à l'hôte jusqu'à la validation de l'état non-ok. Ensuite, il récupère la liste des contacts afin d'en choisir un et le notifier par un mail.si l'intervalle de temps de la prochaine notification est écoulé et que l'état du service est encore non-ok, le système recommence la vérification des services.

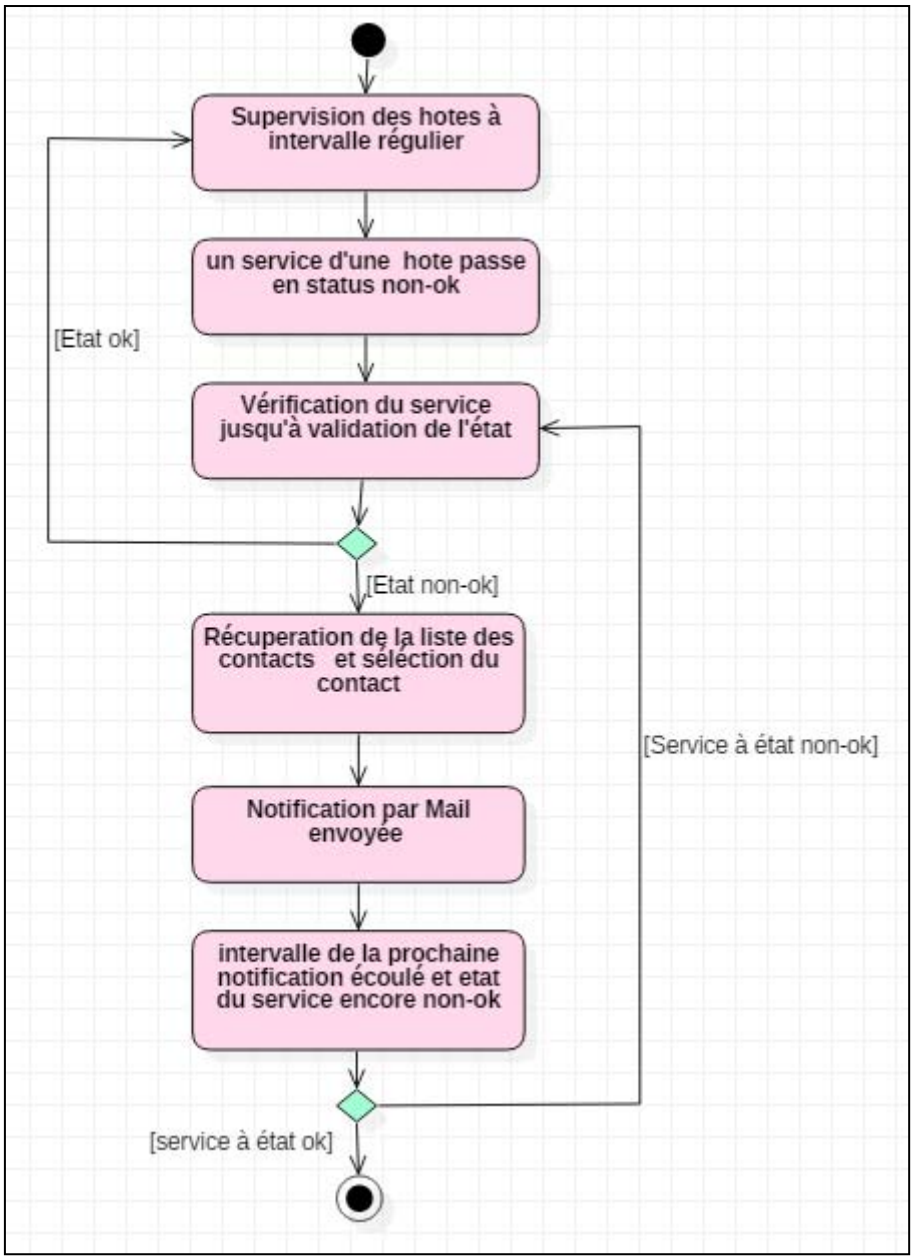


Figure 12: Diagramme de cas d'activité Notification

2.2.4. Diagramme de séquence

Un diagramme de séquence est un diagramme d'interaction qui montre comment les processus fonctionnent entre eux et dans quel ordre. Il est une construction d'un graphique de séquence de message. Un diagramme de séquence montre les interactions d'objets disposés selon un ordre chronologique. Il représente les objets et les classes impliquées dans le scénario. Les diagrammes de séquence sont généralement associés aux diagrammes de cas d'utilisation dans la vue logique du système.

a. Diagramme de séquence cas d'utilisation « Authentification »

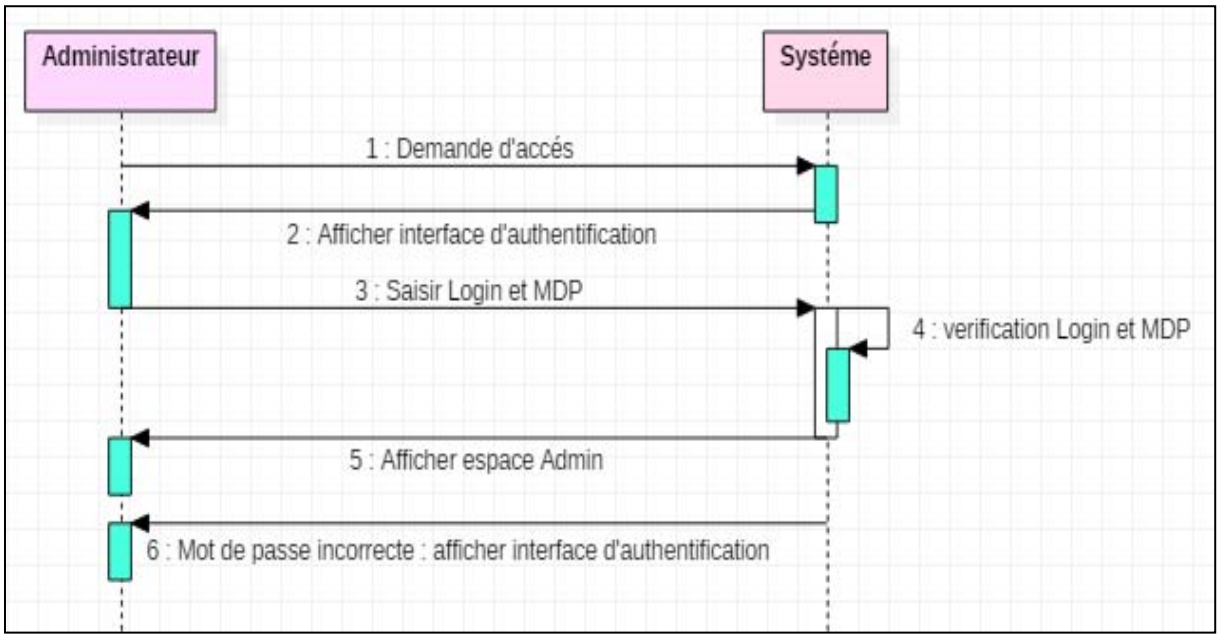


Figure 13 : Diagramme de séquence « Authentification »

b. Diagramme de séquence modification d'un service

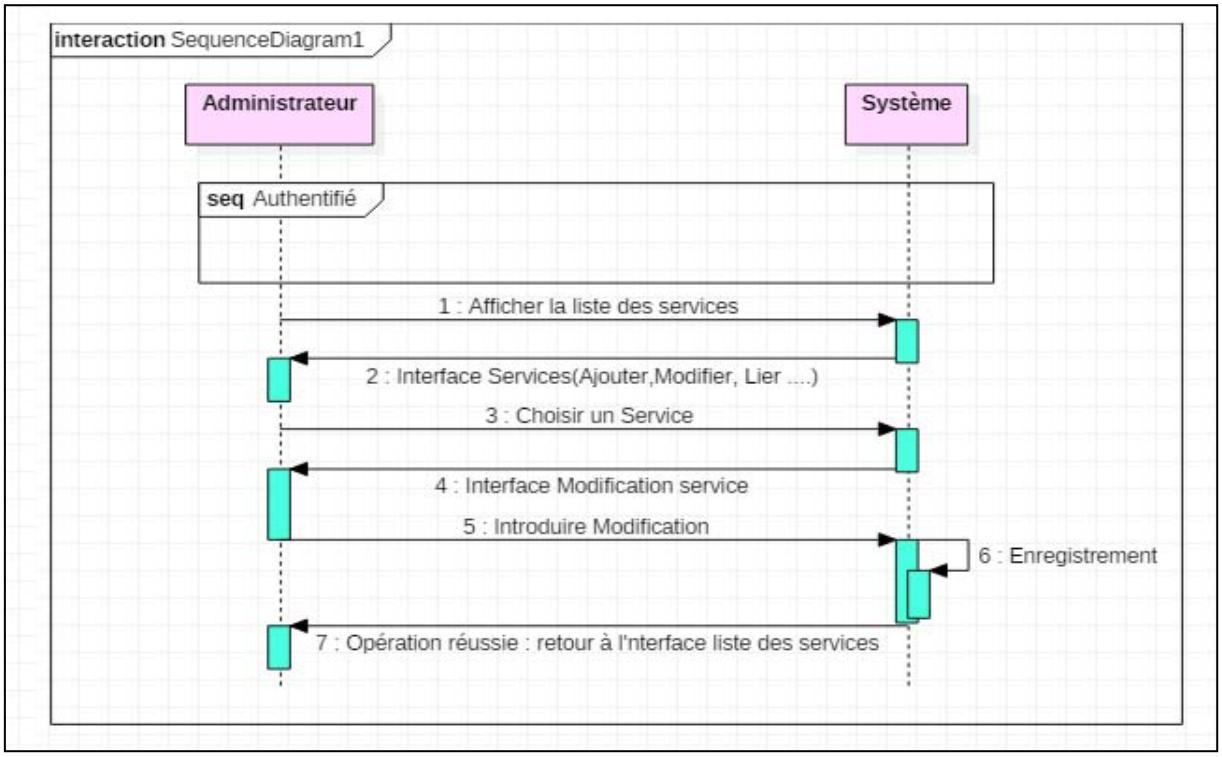


Figure 14 : Diagramme de séquence « Gestion d'un service »

2. Principe de fonctionnement de l'outil à réaliser

D'abord on a commencé par l'installation du logiciel de virtualisation qui est dans notre cas VirtualBox, sur lequel on a ensuite mis en place une machine Virtuelle possédant une image iso Ubuntu 12.04 LTS comme système d'exploitation. Sur ce dernier on a installé :

- L'outil de supervision Nagios avec ses différents plugins qui seront nécessaire à son fonctionnement. Afin de faciliter l'exploitation de ce Nagios.
- Centreon qui est un logiciel de supervision joue le rôle d'une interface graphique pour Nagios et il va faciliter l'utilisation des fonctionnalités de Nagios.
- Configuration des différents équipements à superviser ainsi que les services qu'on a besoin.
- Configuration de Cenreon à l'envoie des alertes lors d'un problème au niveau d'un équipement. On a voulu utilisé les 2 méthodes disponible sur Centreon qui sont l'envoie des alertes par mails et par SMS.

➔ Bien qu'il existe des solutions payantes de pack SMS, on a voulu piloter notre outil avec un Mobile GSM. Mais dans ce cas, nous avons besoin d'un téléphone portable compatible au

commande AT ce qui n'existe plus encore dans nos jours, c'est pour cela on a fait la configuration sur Nagios afin qu'un jour on ajoutera un modem GSM et tout sera disponible pour fonctionner.

L'installation et la mise en place des différents outils nécessaires au fonctionnement de Nagios est détaillé dans la section Annexe.

3. Présentation de Nagios

Nagios est un logiciel de supervision de réseau libre sous licence GPL (General Public Licence*)*. Il a été conçu pour tourner sous le système d'exploitation Linux. Il a pour fonction de surveiller les hôtes et les services spécifiés, alertant l'administrateur des états des machines et équipements présents sur le réseau.

Bien qu'il fonctionne dans un environnement Linux, ce logiciel est capable de superviser toutes sortes de systèmes d'exploitation (Windows XP, Windows 2000, Windows 2003 server, Linux , Mac OS entre autres) et également des équipements réseaux grâce au protocole SNMP.

Cette polyvalence permet d'utiliser Nagios dans toutes sortes d'entreprise, quelque soit la topologie du réseau et les systèmes d'exploitation utilisés au sein de l'entreprise.

Ce logiciel est composé de trois parties :

- Le moteur de l'application, qui gère et ordonnance les supervisions des différents équipements.
- Les plugins qui servent d'intermédiaire entre les ressources que l'on souhaite superviser et le moteur de nagios. Pour accéder à une certaine ressource sur un hôte, il faut un plugin coté Nagios et un autre coté hôte administré.
- L'interface web qui permet d'avoir une vue d'ensemble des états de chaque machine du parc informatique supervisé et ainsi pouvoir intervenir le plus rapidement possible en ciblant la bonne panne [9].

3.1. Mode de fonctionnement

Nagios utilise des plugins, installés sur la machine supportant Nagios et l'hôte à superviser, pour informer cette dernière des informations qu'il souhaite récupéré afin de les analyser.

Le résultat de cette analyse fait remonter un problème, les services de surveillance peuvent envoyer des avertissements à l'administrateur du réseau de différentes manières : courriers électroniques, messages instantanées, SMS, etc.

Pour ce projet, nous avons décidé d'utiliser le mode active pour la récupération des informations. Dans ce mode, Nagios prend l'initiative d'envoyer une requête pour obtenir des informations. Ceci évite donc de configurer les postes à superviser.

3.2. Architecture

Nagios peut être décomposé en trois parties:

- **Un ordonnanceur**, chargé de contrôler quand et dans quel ordre les contrôles des services sont effectués.
- **Des plugins (greffons)**
- Une **interface graphique** qui affiche de manière claire et concise l'état des services surveillés.

L'architecture standard de Nagios peut donc être représentée de la manière suivante [2] :

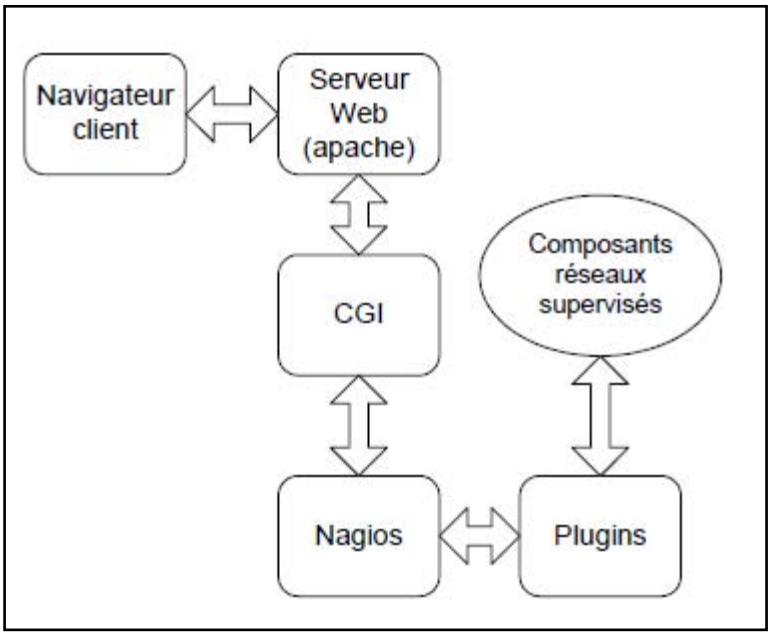


Figure 15: Architecture de Nagios

Comme le montre la figure si dessus l'architecture de Nagios se base sur le paradigme serveur-agent. D'une manière générale, un serveur fait office de point central de collecte des informations. Les autres machines du réseau exécutent un agent chargé de renvoyer les informations au serveur [4].

Nagios va être couplé avec Centreon permettant par ceci de faciliter l'administration mais aussi de remonter les graphes et d'effectuer du reporting.

3.3. Les plugins

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

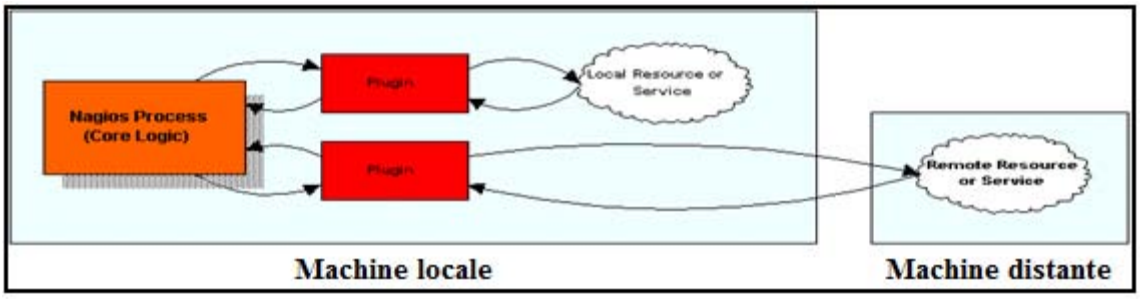


Figure 16: principe de fonctionnement des plugins

C'est le résultat de l'exécution du plugin qui est interprété par Nagios pour déterminer l'état du service ou de la station testée. Chacun peut donc définir son propre plugin et le rajouter aux plugins disponibles par défaut ce qui permet un grand nombre de tests possibles. Ainsi, le plugin devra être exécutable avec les droits de l'utilisateur Nagios, il devra afficher un message de préférence sur une seule ligne décrivant la situation du service (par exemple :
« Temps de réponse OK : 0.586 secondes ») et posséder un code de retour qui indique le statut du service [16].

- 0 : *OK*, le service fonctionne correctement
- 1 : *Warning*, le service est dégradé
- 2 : *Critical*, le service ne fonctionne plus
- 3 : *Unknown*, impossible de déterminer l'état du service

Il existe notamment des plugins Nagios nommée NRPE et NCSA qui fonctionnent un peu sur le même principe que ceux de Zabbix. NRPE est un agent esclave qui attend les ordres du moteur Nagios (polling) et NCSA envoi de lui-même les données (trapping) [17].

3.3.1. L'agent NRPE

NRPE (Nagios Remote Plugin Executor) est un addon (programme fourni par nagios.org pour améliorer et étendre les fonctionnalités de Nagios**)** utilisé pour exécuter des plugins (dite Actif) pour surveiller les ressources «locales» sur (Linux / Unix) des systèmes distants. Certaines ressources ne peuvent pas être surveillé via SNMP ou en utilisant d'autres agents à

travers le réseau, on doit donc les vérifier en utilisant des programmes installés localement sur les machines à surveiller et de transmettre les résultats au serveur Nagios.

Principe de fonctionnement

Son principe de fonctionnement est simple : il suffit d'installer le démon sur la machine distante et de l'interroger à partir du serveur Nagios [18].

- le plugin installé sur le serveur Nagios initie une connexion sur le démon distant
- le démon exécute le plugin demandé
- le démon retourne au serveur Nagios le code de retour de l'exécution du plugin ainsi que la sortie standard.

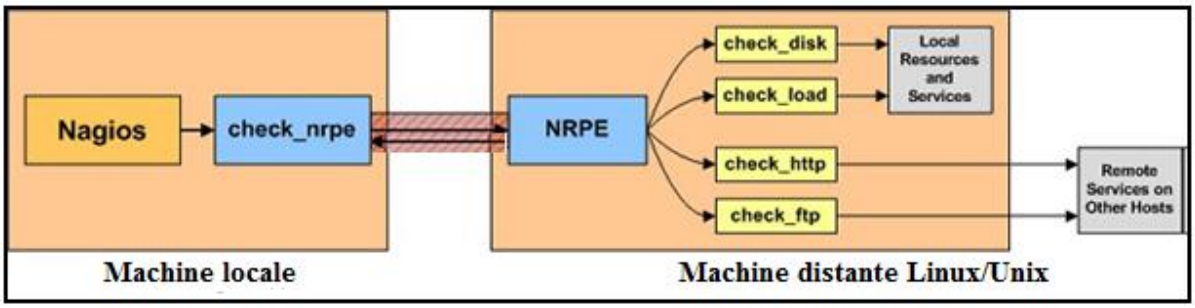


Figure 17 : Fonctionnent du plugin NRPE

Le grand avantage de cet agent est qu'il permet de réduire les charges sur le serveur Nagios. De plus certains greffons sont à exécuter obligatoirement en local.

3.3.2. Le démon NCSA

NCSA (Nagios Service Check Acceptor) est un démon Linux / Unix qui permet d'intégrer des alertes passives et des contrôles depuis les machines distantes et les applications avec Nagios.

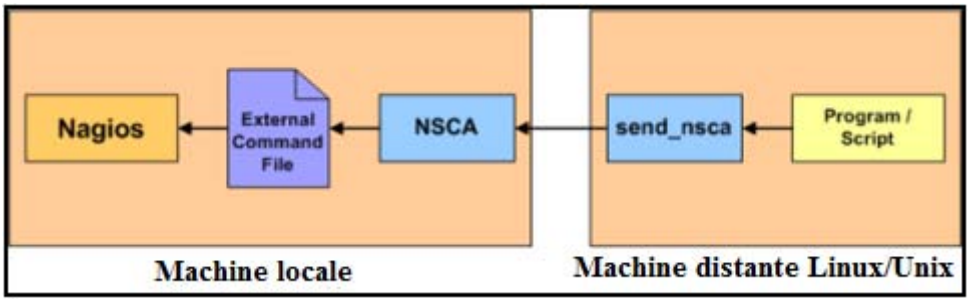


Figure 18: Fonctionnement de NSCA

NSCA fonctionne comme un démon sur le serveur Nagios. Il écoute les informations envoyées par les ordinateurs distants en utilisant le programme de send_nsca (sur les machines Unix / Linux) ou NSClient ++ (souvent utilisé sur les machines Windows). Les données seront cryptées en utilisant la méthode spécifiée dans send_nsca.cfg (ou nsc.ini dans le cas de NSClient ++). Le démon va valider les données de façon fondamentale en décryptant l'information en utilisant le mot de passe qui est stockée dans le fichier de nsca.cfg locale.

4. Centreon

4.1. Présentation

Centreon est une application open source et gratuite qui permet de gérer Nagios et ses fichiers de configuration via une interface Web. L'avantage de Centreon est qu'elle dispose d'une interface plus intuitive et conviviale [17].
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 : Page d'accueil avec Le "Tactical Overview" de Nagios permettant un coup d'oeil rapide aux problèmes survenus et accès aux statistiques des performances du moteur et de ses composants.
- Monitoring : Possède plusieurs vues, mais reprend la grande idée de l'arbre des groupes d'équipements. Reprend également la vue Nagios.
- Views : Permet d'accéder à tous les graphiques avec un menu arborescent. Accès 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.

4.1.1. Avantages

Le choix de Centreon s’est basé sur les avantages suivants :

- La robustesse et la renommée de Nagios
- Une interface beaucoup plus sympathique, permettant de tout configurer, de garder un œil sur tout le réseau en permanence

- Les utilisateurs de Nagios ne seront pas perdus pour autant, l'interface reprenant avantageusement certaines vues Nagios
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau.
- Une entreprise qui pousse le développement
- Peut être décoléré du serveur Nagios et tourner tout seul sur un autre serveur

4.1.2. Inconvénients

Centreon possède des inconvénients parmi lesquelles :

- L'interface peut paraître complexe car il existe beaucoup d'options .
- Un développement qui n'est pas encore en phase avec celui de Nagios : Parfois des problèmes de compatibilité.
- Un peu plus lourd que du Nagios pur.

4.2. Principe de fonctionnement

Le principe de fonctionnement de Centreon est simple. L'administrateur configure les options de supervisions, hôtes, services, plugins, etc…grâce à son interface graphique.
Ensuite toutes ces configurations sont stockées dans une base de données, mais elles ne sont pas immédiatement appliquer au moteur Nagios qu'aprés avoir relancer Centreon.
Dans certains cas l'administrateur fait une faute de frappe lors de la configuration d'un fichier, ce qui entraine le non fonctionnement de nagios et par la suite une perte de temps de la part l'administrateur en essayant de retrouver l'erreur. Centreon évite ce problème car il contrôle les données entrées par l'administrateur avant de les valider [9].
Il est aussi possible avec Centreon de créer ses propres commandes selon les besoins afin de configurer les services voulus.

5. Complément de Nagios

5.1. NDOutils

NDOUtils est un addon qui permet à Nagios de stocker les données dans une base de données MySQL notée par NDO. Cet addon est composé de deux briques: NDOMOD et NDO2DB. Le premier (NDOMOD) va prendre les événements à partir du daemon Nagios et les envoyer via une socket (TCP ou UNIX) vers le second (NDO2DB) qui va les convertir dans un format compatible avec la base de données choisie (MySQL) [19].

5.2. NSClient + +

NSClient++ est un service pour toutes versions de Windows (NT, 2000, 2003, 2008, XP, Vista, 7) qui combine les fonctionnalités d'un agent de supervision dédié à l'environnement Windows ainsi que les fonctions de transport NRPE et NSCA pour cet environnement. Il est disponible en version 32 et 64 bits. Du fait de ces triples fonctions, le fichier de configuration de NSClient++ est assez long mais également assez simple. Il est aujourd'hui considéré comme l'agent de supervision standard Nagios pour plateformes Windows.

La supervision des machines Windows se fait grâce à l'agent NSClient++ qui doit être installé sur la machine distante à superviser. Le schéma suivant présente les différents composants qui doivent être mis en place et leur interaction pour que la supervision soit opérationnelle.

Pour la supervision d'une hôte distante dont le système d'exploitation est Windows :

- en mode NSClient : NSClient++ joue le rôle d'un certains nombre des plugins Nagios. En fait des modules de NSClient++ permettent par exemple de surveiller la CPU et les disques durs. NSClient++ peut aussi exécuter des scripts, par exemple en Perl ou en Python
- en mode NRPE NSClient prend le rôle de NRPE, il devient alors possible que NSClient exécute des plugins de Nagios sur la machine local et transmettre ces résultats de surveillance au serveur hébergeant Nagios.

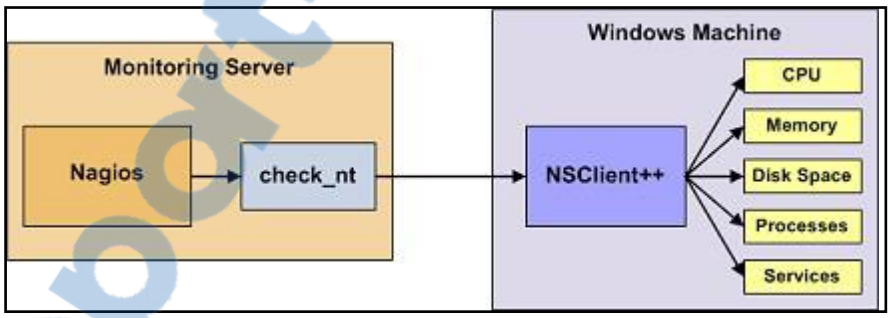


Figure 19: Vérification NSClient++

NSClient++ se base sur une architecture client/serveur. La partie cliente (nommée check_nt), doit être disponible sur le serveur Nagios. La partie serveur (NSClient++) doit être installée sur chacune des machines Windows à surveiller. Le principe de supervision des autres équipements réseaux (Routeurs, Commutateurs, etc...) reste le même.

Conclusion

Le but de ce chapitre était de présenter en détails l'outil de supervision choisi ainsi que ses compléments. Certains ont été choisis pour leur nécessité comme les greffons NRPE et

NSClient, et d'autres participaient surtout à l'amélioration de la manipulation et l'utilisation de Nagios, et surtout facilité de sa configuration.

Le chapitre suivant entamera l'aspect technique de mon projet ainsi sa mise en place jusqu'aux exemples d'utilisations.

Chapitre 4

Mise en place du système de supervision

Introduction

Au cours de ce chapitre, nous nous intéressons à la description de la phase de réalisation de notre application. Nous commençons par la spécification des différents environnements de développement, matériels et logiciels. Ensuite nous décrivons les points les plus intéressants de l'application tout en donnant un aperçu sur les différentes parties développées au cours de ce projet.

1. Environnement de travail

1.1. Environnement matériel

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

- Intel(R) Core ™ i3-3217U (1.80 Ghz)
- Go de RAM
- Disque dur de capacité 500 Go.
- Système d'exploitation Windows 7 Edition Intégrale

1.2. Environnement logiciel

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

1.2.1. Oracle VM VirtualBox

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

1.2.2. Système d'exploitation

Dans ce projet on a décidé d'utiliser l'image iso des 2 systèmes d'exploitation suivants :

- La distribution Ubuntu 12.04 LTS sur laquelle on a installé Nagios
- Windows XP comme machine distante à superviser sur laquelle on a installé NSClient++.

1.2.3. Outils de supervision

- La solution de supervision Nagios-3.4.1
- Les plugins de Nagios-1.4.16
- Un complément à Nagios pour faciliter sa configuration et son administration Centreon-2.5.4.
- Le plugin NDOutils-2.0.0 pour le stockage des données de Nagios dans la base de données MySQL et le partage de ces données avec Centreon.

2. Installation et configuration de Nagios

2.1. Les pré-requis pour Nagios

Pour l'installation de Nagios, il est recommandé de vérifier que certains dépendances sont autorisés sur la machine à utiliser comme serveur principale .on a alors besoin de :

- **Build-essential, gcc, g++, cpp** : outils pour compilation

```
Apt-get install gcc g++ cpp build-essential
```

- **Apache2, PHP5** : pour la consultation, l'affichage des données.

```
Apt-get install apache2 apache2-mpm-prefork
```

```
Apt-get install php5 php5-mysql
```

```
Apt-get install php-pear php5-ldap php5-snmp php
```

- **MySQL** : pour le stockage des données

```
Apt-get install mysql-server-5.1 libmysqlclient15-dev
```

- **Les librairies RRDTools** : pour les graphiques

```
Apt-get install rrdtool librrds-perl
```

- **les librairies Perl :**

> **Apt-get install** libconfig-inifiles-perl libcrypt-des-perl libdigest-hmac-perl libdigest-sha1-perl libgd-gd2-perl

- **Les librairies GD**:

> **Apt-get install** libgd2-xpm libgd2-xpm-dev libpng12-dev

- **SNMP:**

> **Apt-get install** snmp snmpd libnet-snmp-perl libsnmp-perl

Le reste des étapes d'installation et de configuration des différents logiciels « Nagios-3.4.1» et ses plugins « Nagios-plugins-1.4.16 », « Centreon-2.5.4 » et « NDOUtils-2.0.0 » seront détaillées dans l'annexe.

3. Les interfaces de l'application

L'application développée est destinée à des administrateurs de réseaux, il permet de réaliser des tests sur les machines distante pour vérifier s'ils sont en fonction.

D'abord l'administrateur doit s'authentifier en entrant son login et son mot de passe, 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/ ».**

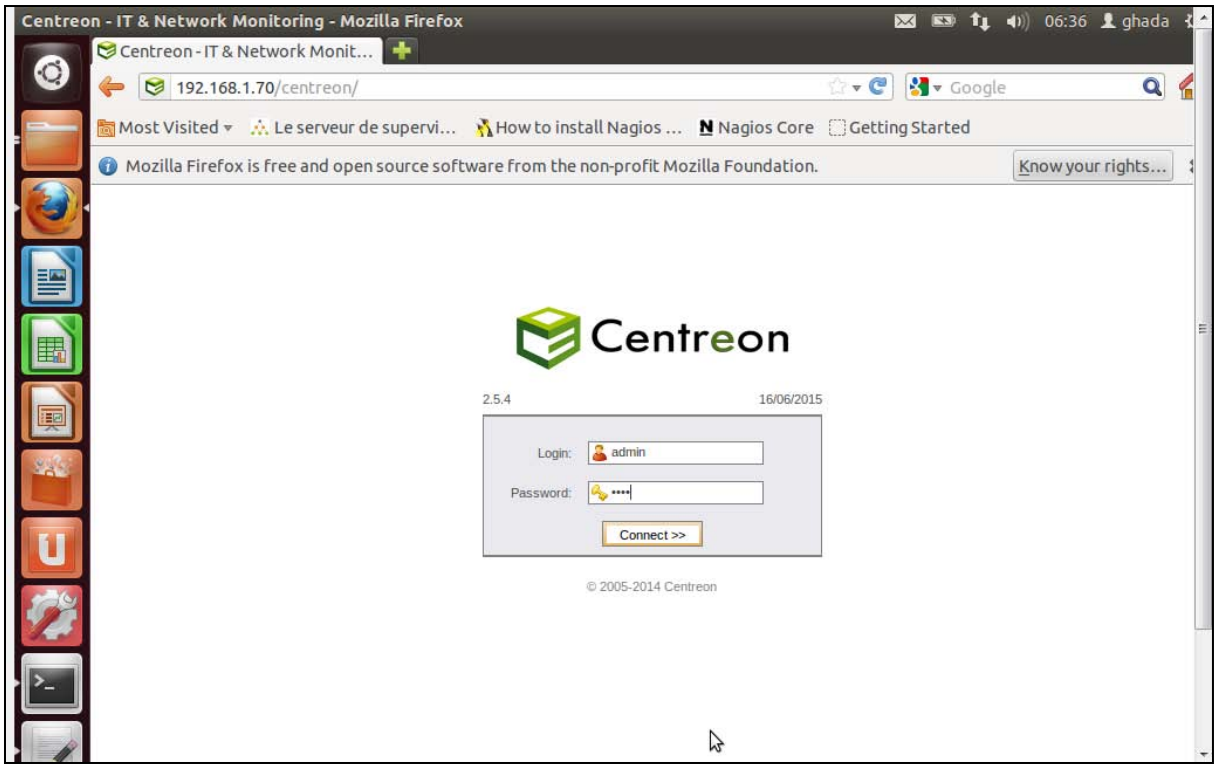


Figure 20 : Interface d'identification de Centreon

La première vue après authentification est présenté dans la figure 20 si dessous. Elle donne une idée générale sur l'état de fonctionnement des hôtes ainsi que les services qui lui sont associés.

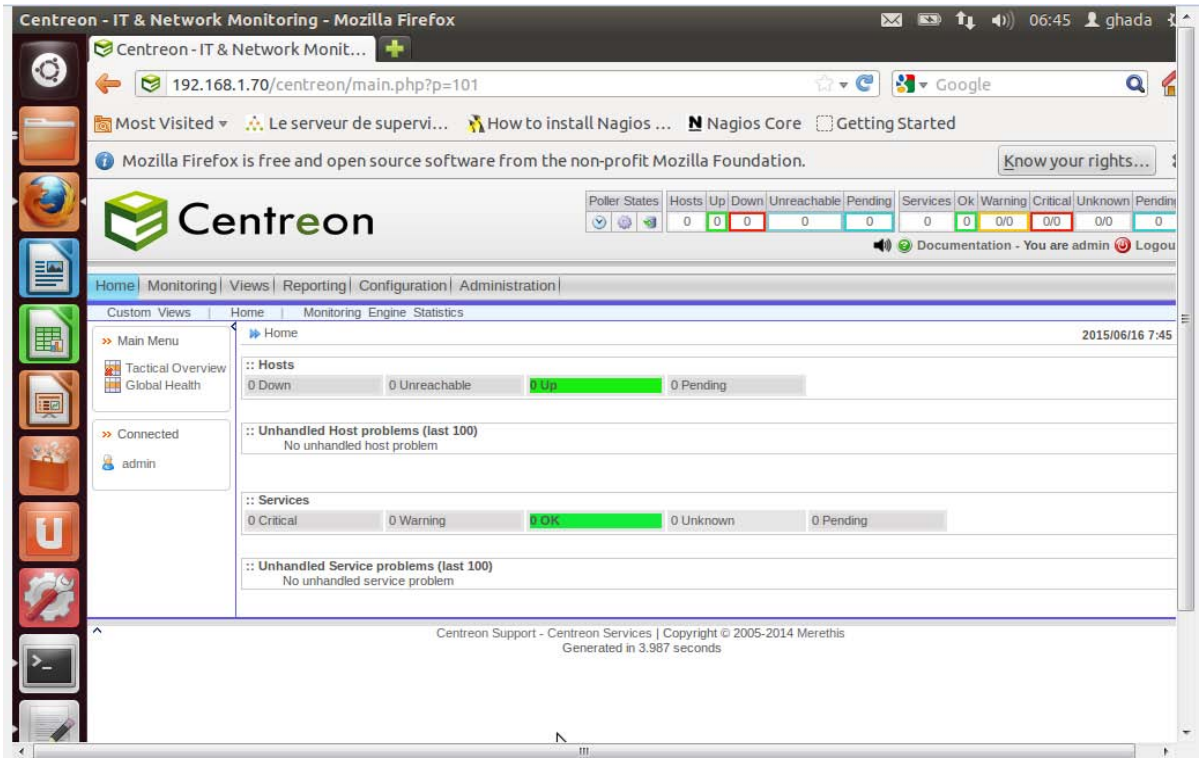


Figure 21 : Page d'accueil après authentification

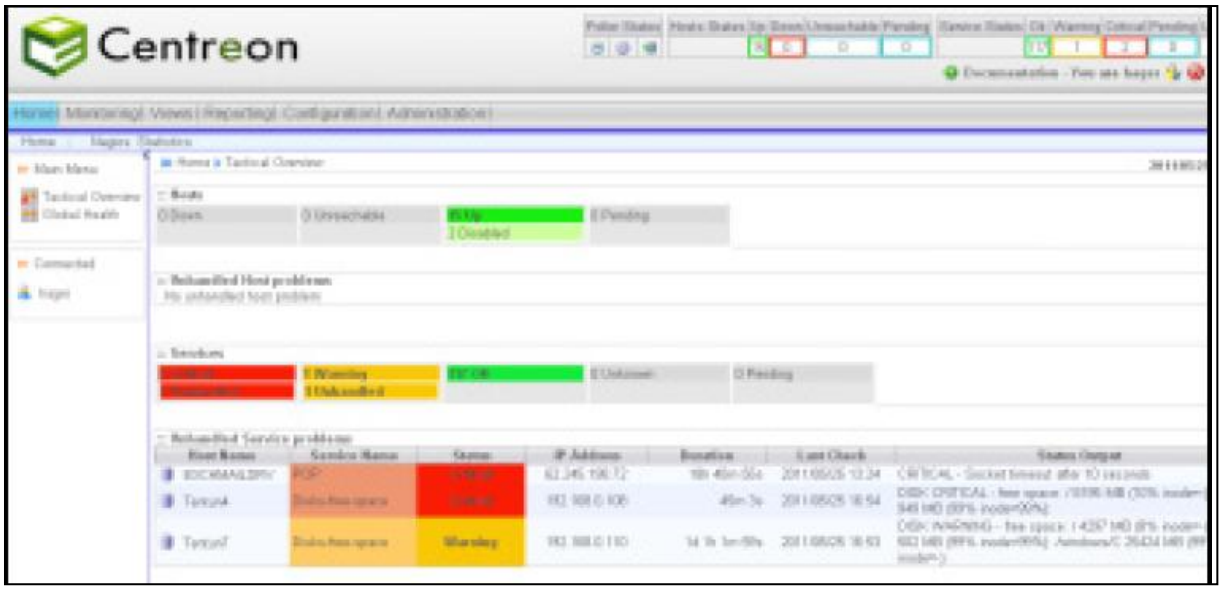


Figure 22 : interface vue globale sur les statuts des hôtes

L'interface Tactical Overview (**figure 22**) permet d'avoir une vue globale sur les statuts des équipements supervisés et des services qui lui sont liés .cette vue donne un aperçu rapide sur l'état du réseau.

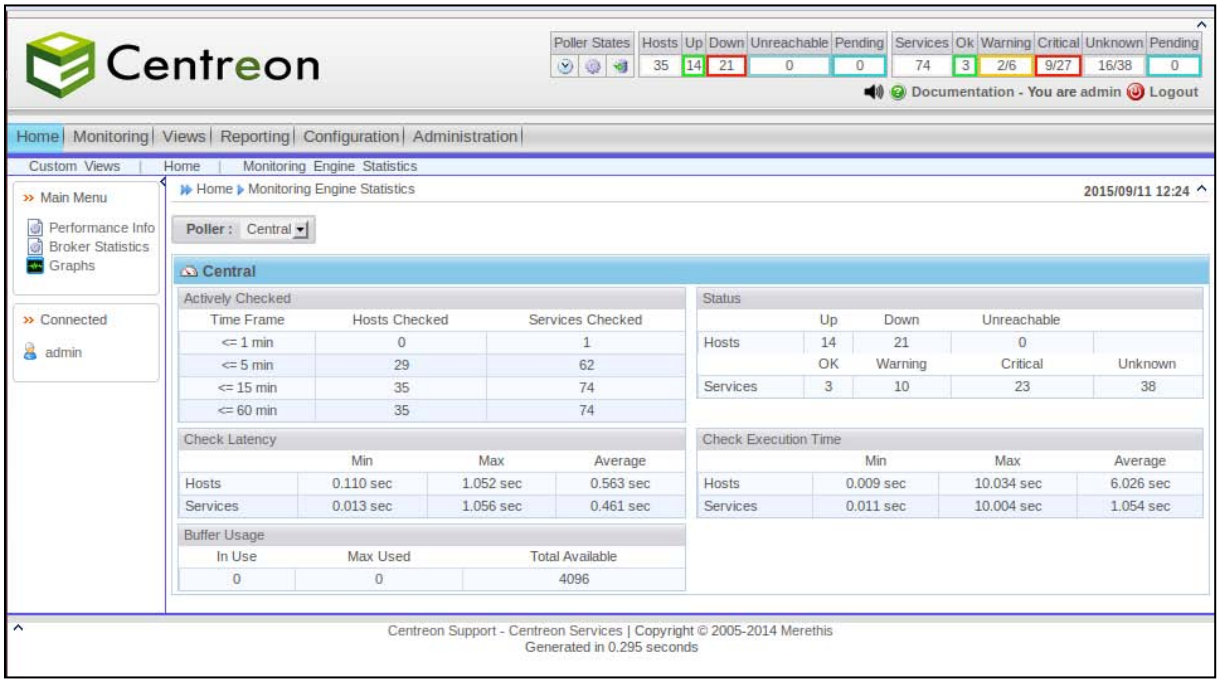


Figure 23 : interface des statistiques de Nagios

La **figure 23** représente l'interface de Centreon montrant les statistiques du moteur de supervision Nagios. Elle donne une vue globale sur l'historique des activités contrôlés dont le nombre d'hôtes et le nombre de services.

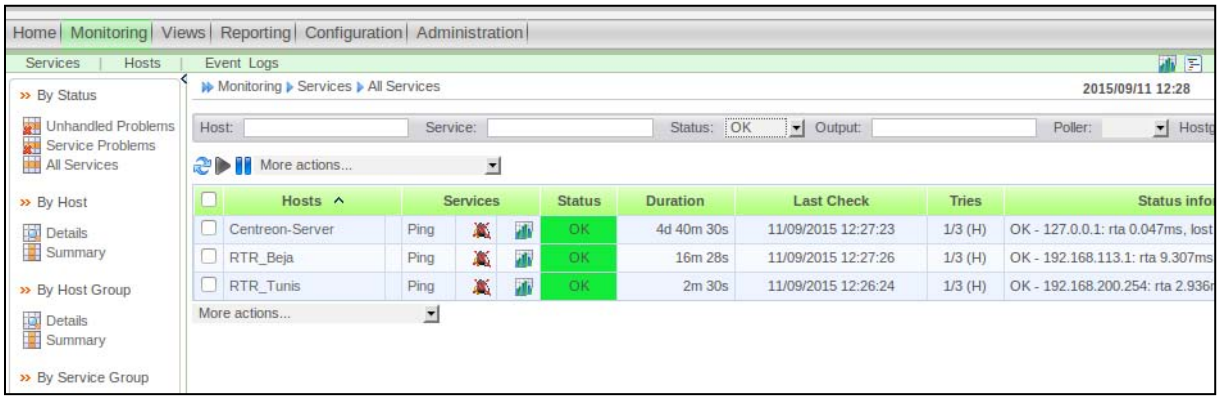


Figure 24 : interfaces des services UP

La figure si dessus montre l'état des services actives que nous avons configuré.

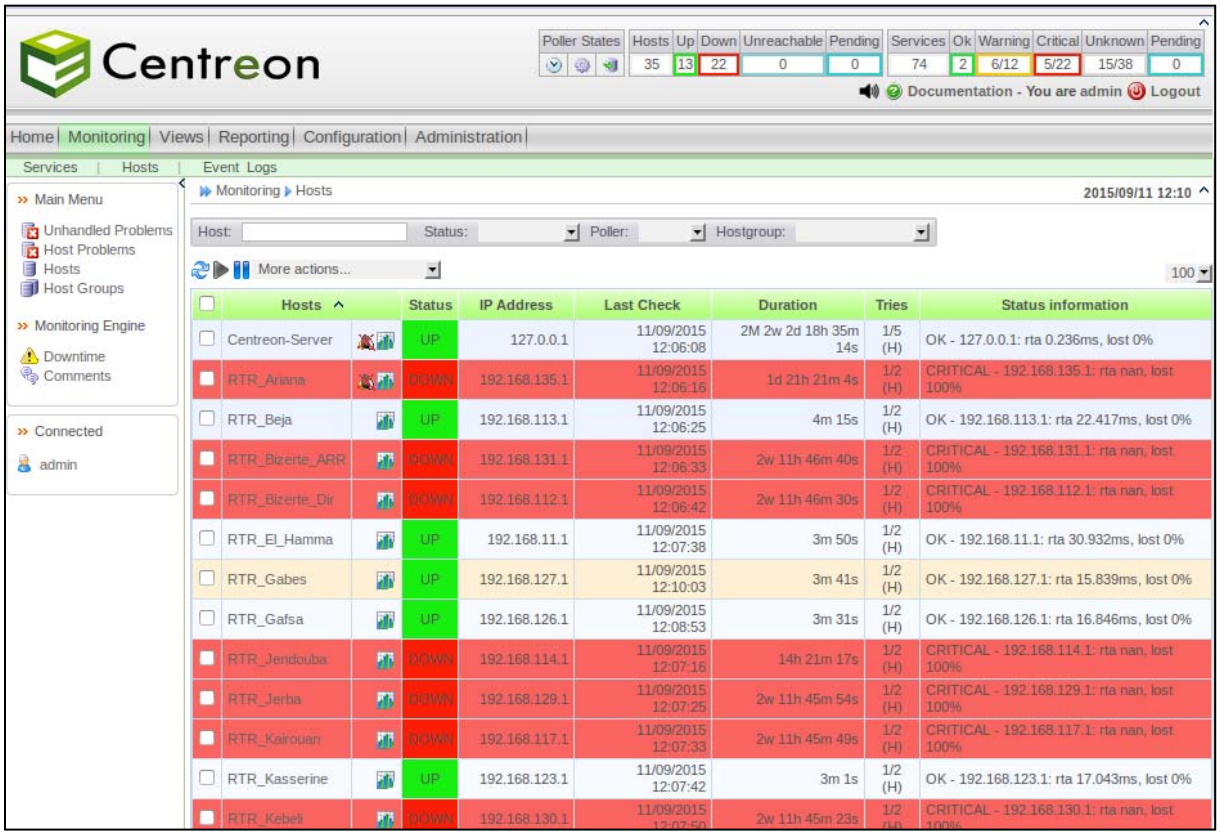


Figure 25 : listes des équipements supervisés

La figure 18 nous permet de voir le statut de manière globale de tous les équipements supervisés, d'une manière générale de savoir si ils sont en ligne (état :UP) ou si ils ont un autre statut (état : Down, Warning, Critical, Unknown).

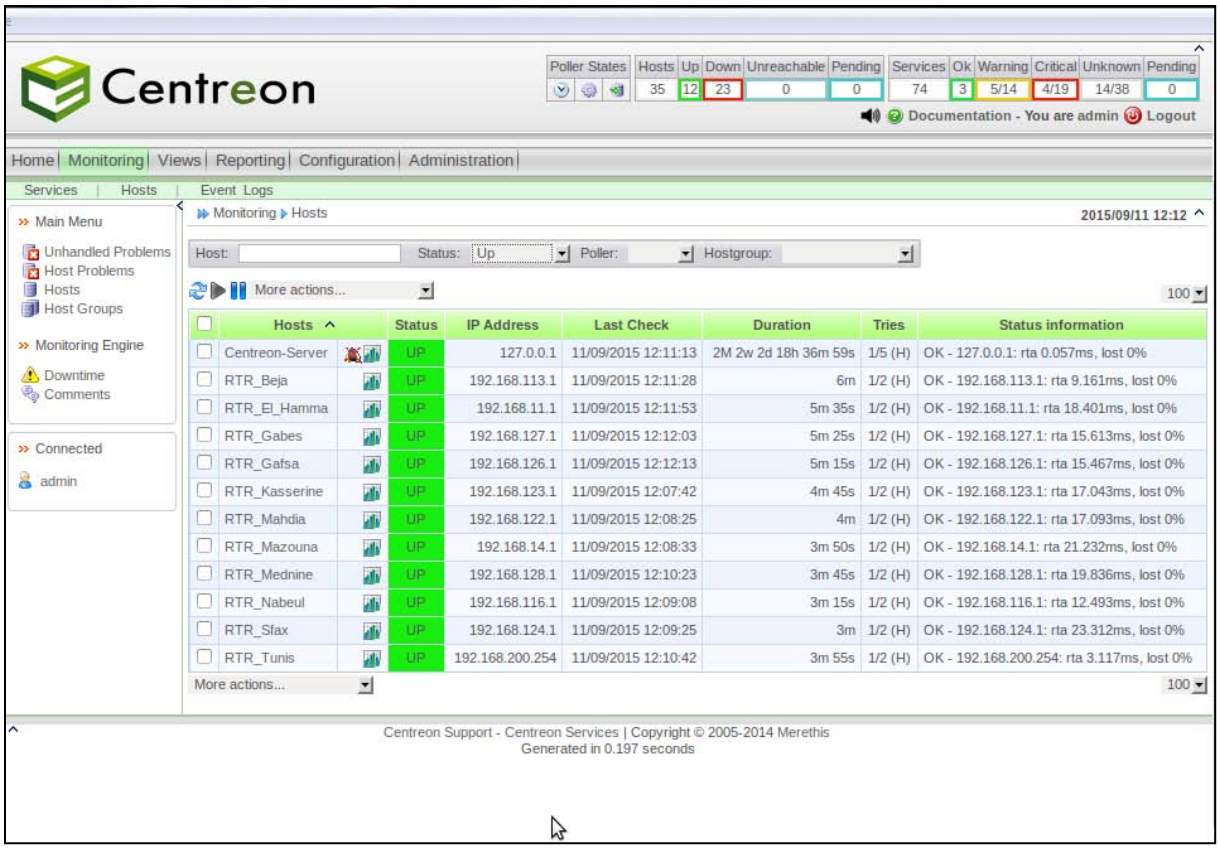
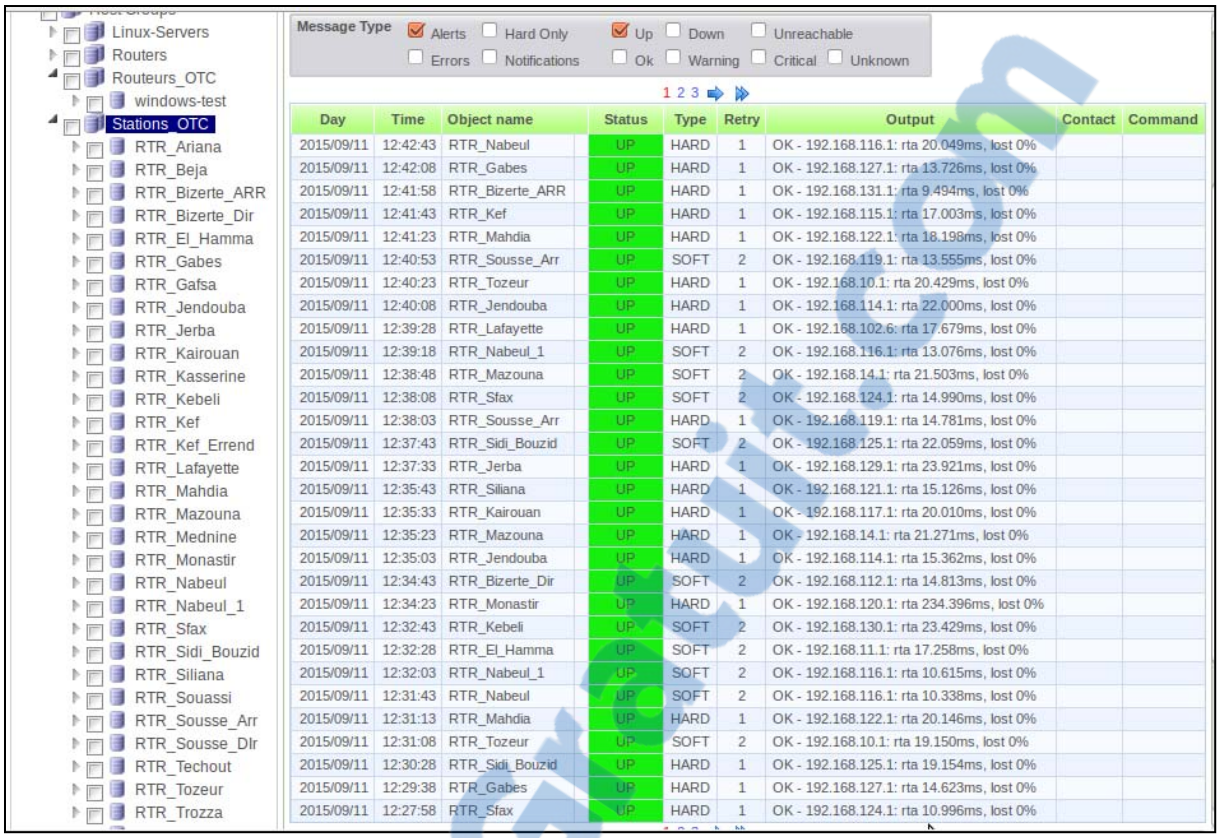


Figure 26 : Liste des hôtes en marche UP

Cette interface représente un exemple de choix de regroupement des équipements supervisés, selon leur statut qui est actif (a l'état UP). On peut aussi les visualiser selon d'autres états de fonctionnement. Cette interface affiche les adresses IP, les derniers contrôles subits sur les machines ainsi que d'autres informations.

On peut aussi lister les différentes machines que l'on supervise selon des groupes d'équipements et des groupes de services déjà créé.



Day	Time	Object name	Status	Type	Retry	Output	Contact	Command
2015/09/11	12:42:43	RTR_Nabeul	UP	HARD	1	OK - 192.168.116.1: rta 20.049ms, lost 0%		
2015/09/11	12:42:08	RTR_Gabes	UP	HARD	1	OK - 192.168.127.1: rta 13.726ms, lost 0%		
2015/09/11	12:41:58	RTR_Bizerte_ARR	UP	HARD	1	OK - 192.168.131.1: rta 9.494ms, lost 0%		
2015/09/11	12:41:43	RTR_Kef	UP	HARD	1	OK - 192.168.115.1: rta 17.003ms, lost 0%		
2015/09/11	12:41:23	RTR_Mahdia	UP	HARD	1	OK - 192.168.122.1: rta 18.198ms, lost 0%		
2015/09/11	12:40:53	RTR_Sousse_Arr	UP	SOFT	2	OK - 192.168.119.1: rta 13.555ms, lost 0%		
2015/09/11	12:40:23	RTR_Tozeur	UP	HARD	1	OK - 192.168.10.1: rta 20.429ms, lost 0%		
2015/09/11	12:40:08	RTR_Jendouba	UP	HARD	1	OK - 192.168.114.1: rta 22.000ms, lost 0%		
2015/09/11	12:39:28	RTR_Lafayette	UP	HARD	1	OK - 192.168.102.6: rta 17.679ms, lost 0%		
2015/09/11	12:39:18	RTR_Nabeul_1	UP	SOFT	2	OK - 192.168.116.1: rta 13.076ms, lost 0%		
2015/09/11	12:38:48	RTR_Mazouna	UP	SOFT	2	OK - 192.168.14.1: rta 21.503ms, lost 0%		
2015/09/11	12:38:08	RTR_Sfax	UP	SOFT	2	OK - 192.168.124.1: rta 14.990ms, lost 0%		
2015/09/11	12:38:03	RTR_Sousse_Arr	UP	HARD	1	OK - 192.168.119.1: rta 14.781ms, lost 0%		
2015/09/11	12:37:43	RTR_Sidi_Bouzid	UP	SOFT	2	OK - 192.168.125.1: rta 22.059ms, lost 0%		
2015/09/11	12:37:33	RTR_Jerba	UP	HARD	1	OK - 192.168.129.1: rta 23.921ms, lost 0%		
2015/09/11	12:35:43	RTR_Siliana	UP	HARD	1	OK - 192.168.121.1: rta 15.126ms, lost 0%		
2015/09/11	12:35:33	RTR_Kairouan	UP	HARD	1	OK - 192.168.117.1: rta 20.010ms, lost 0%		
2015/09/11	12:35:23	RTR_Mazouna	UP	HARD	1	OK - 192.168.14.1: rta 21.271ms, lost 0%		
2015/09/11	12:35:03	RTR_Jendouba	UP	HARD	1	OK - 192.168.114.1: rta 15.362ms, lost 0%		
2015/09/11	12:34:43	RTR_Bizerte_Dir	UP	SOFT	2	OK - 192.168.112.1: rta 14.813ms, lost 0%		
2015/09/11	12:34:23	RTR_Monastir	UP	HARD	1	OK - 192.168.120.1: rta 234.396ms, lost 0%		
2015/09/11	12:32:43	RTR_Kebeli	UP	SOFT	2	OK - 192.168.130.1: rta 23.429ms, lost 0%		
2015/09/11	12:32:28	RTR_El_Hamma	UP	SOFT	2	OK - 192.168.11.1: rta 17.258ms, lost 0%		
2015/09/11	12:32:03	RTR_Nabeul_1	UP	SOFT	2	OK - 192.168.116.1: rta 10.615ms, lost 0%		
2015/09/11	12:31:43	RTR_Nabeul	UP	SOFT	2	OK - 192.168.116.1: rta 10.338ms, lost 0%		
2015/09/11	12:31:13	RTR_Mahdia	UP	HARD	1	OK - 192.168.122.1: rta 20.146ms, lost 0%		
2015/09/11	12:31:08	RTR_Tozeur	UP	SOFT	2	OK - 192.168.10.1: rta 19.150ms, lost 0%		
2015/09/11	12:30:28	RTR_Sidi_Bouzid	UP	HARD	1	OK - 192.168.125.1: rta 19.154ms, lost 0%		
2015/09/11	12:29:38	RTR_Gabes	UP	HARD	1	OK - 192.168.127.1: rta 14.623ms, lost 0%		
2015/09/11	12:27:58	RTR_Sfax	UP	HARD	1	OK - 192.168.124.1: rta 10.996ms, lost 0%		

Figure 27 : Interface des journaux d'évènements

La figure 27 représente une vue globale sur les machines ayant subit un problème à un moment précis. Un message de notification de type alerte sera envoyé par mail et par SMS au superviseur responsable indiquant le nom de la machine, son adresse IP et l'état de la machines en question (Down, critical , unknown ….)

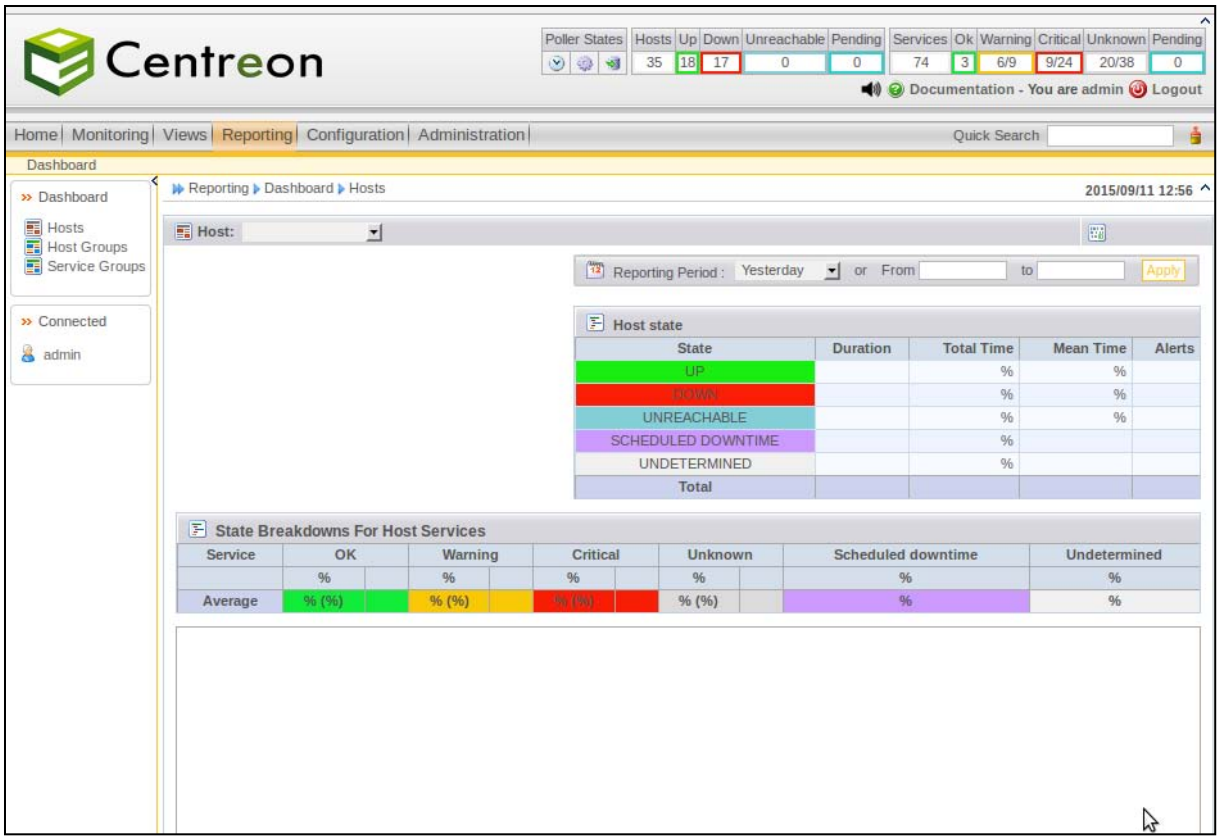


Figure 28 : Interface Reporting

L'interface Reporting décrite si dessus nous donne la possibilité de faire un graphique (après avoir choisi l'équipement sur lequel on veut récolter des informations) par rapport au pourcentage de fonctionnement des services ou du statut.

Figure 29: Interface Détails des services

Cette figure (figure 29) affiche les différentes hôtes du réseau avec un détails du statut de chaque service.

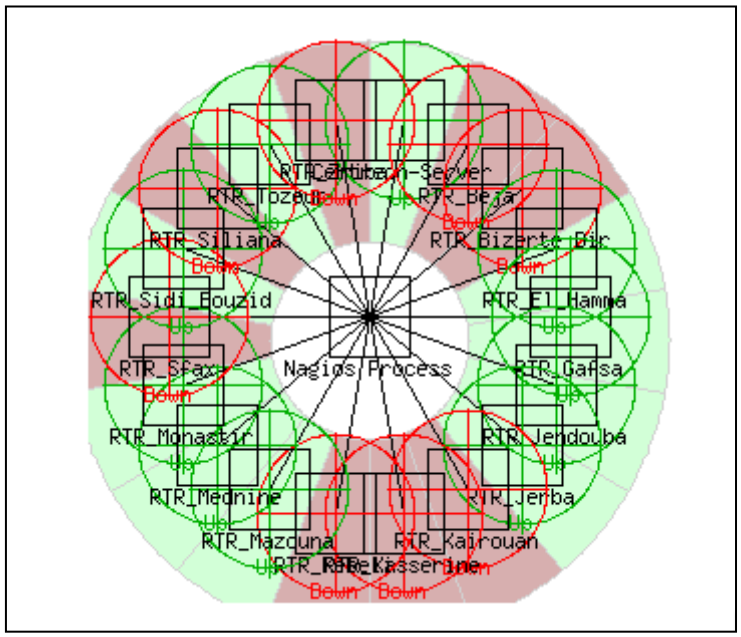


Figure 30 : Map des hôtes supervisées

Cercle en Vert : représente les hôtes ayant un état UP (en service)

Cercle en Rouge : représente les hôtes ayant un état DOWN (hors-service)

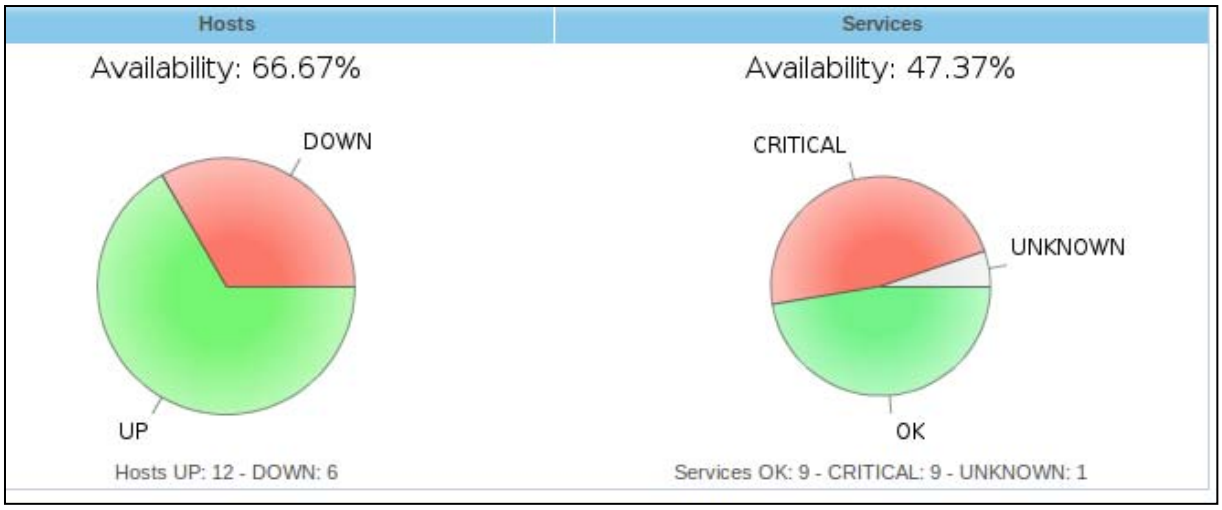


Figure 31 : Interface de l'état globale des hôtes et des services

4. Configuration des notifications

Afin de pouvoir envoyer des alertes par mail depuis Nagios on a besoin d'installer d'abord l'outil correspondant. Cela peut se faire de plusieurs manières : utiliser SSMTP, Postfix ou bien encore sendmail. Mais les deux dernières solutions semblent être des solutions lourdes et difficile a mettre en place. C'est pour cela que nous avons choisis d'utiliser une solution plus simple et plus performante avec SSMTP.

SSMTP (Server Simple Mail Transfer Protocol) est un programme qui délivre le courrier électronique à partir d'un ordinateur local à un serveur de courrier configuré. Il n'est pas un serveur de messagerie (comme serveur de messagerie Sendmail riche en fonctionnalités) et ne reçoit pas de courrier. Une de ses principales utilisations est pour la transmission e-mail automatique (comme les alertes du système) de votre machine à une adresse de messagerie externe.

4.1. Notification par mail

```
root@ghadabens-VirtualBox:~# apt-get install ssmtp
```

On vérifier l'installation avec

```
root@ghadabens-VirtualBox:~# whereis sendmail
```

On doit avoir /usr/sbin/sendmail

Puis on fait

```
root@ghadabens-VirtualBox:~# ls -la /usr/sbin/sendmail
```

On doit avoir SSMTP.

Maintenant on configure le fichier ssmtp.conf

```
root@ghadabens-VirtualBox:~# nano /etc/ssmtp/ssmtp.conf
```


```
root@ghadabens-VirtualBox:~# sudo apt-get install snmp snmpd libnet-snmp-perl
libsnmp-perl
```

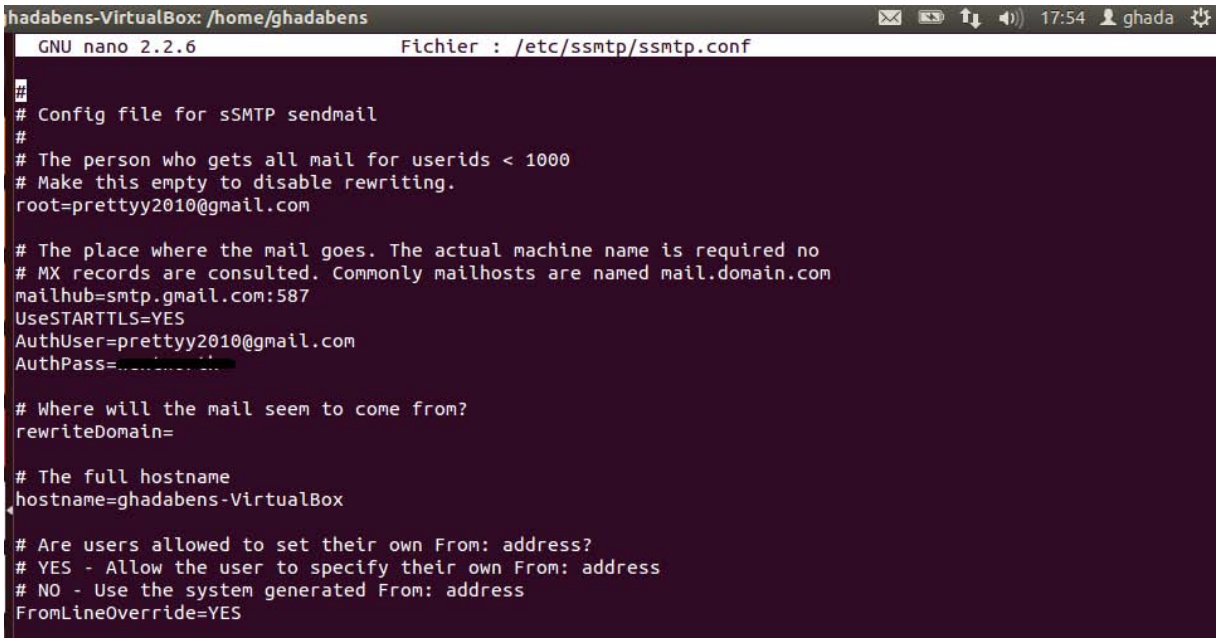


Figure 32 : configuration ssmtp pour l'envoi des mails d'alerte

La figure 32 représente la configuration du fichier ssmtp.conf du protocole ssmtp protocole responsable d'envoie des mails. Le résultat de cette configuration est présentée dans la figure 33 si dessous.

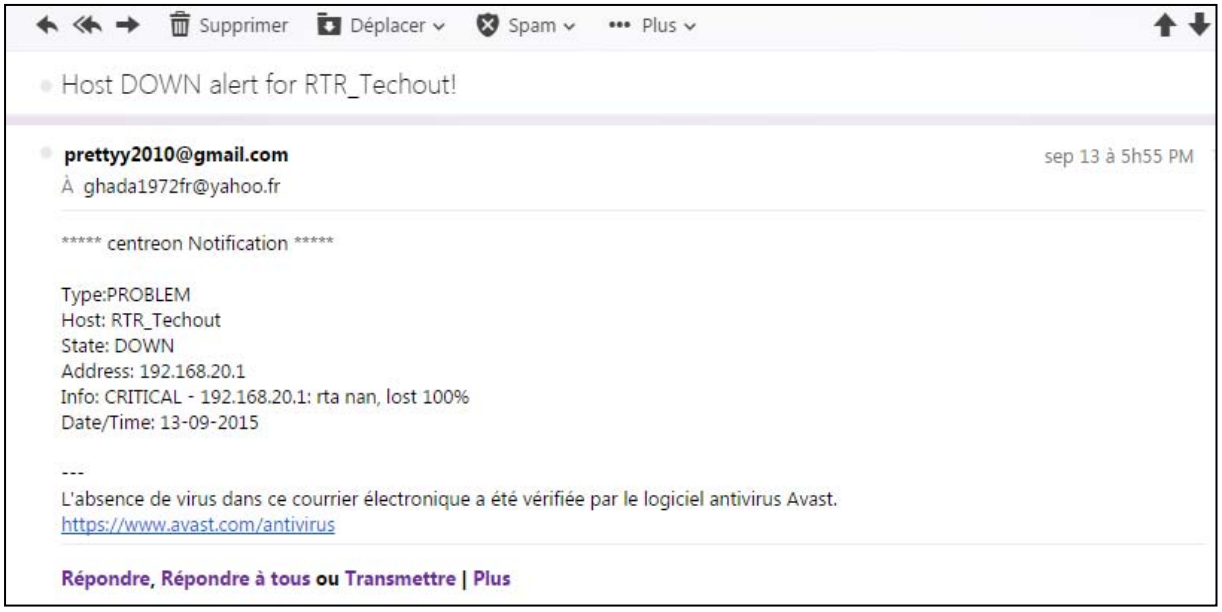


Figure 33 : Mail d'alerte reçue

4.2. Notifications par SMS

Nagios n'intègre pas de solution SMS par défaut, pour cela nous allons utiliser une autre application « gsm-utils » qui permet de commander un téléphone mobile lié par un câble USB à notre machine Nagios et donc d'envoyer des SMS par ligne de commande.

Par la suite, on va déclarer les commandes **notify-host-by-sms** et **notify-service-by-sms** qui vont intégrer la commande pour envoyer les SMS. (nano /usr/local/nagios/etc/objects/commands.cfg).

```
define contact{
alias                           admin
contactgroups                   supervisors
service_notification_period     24×7
host_notification_period        24×7
service_notification_options     w,u,c,r
host_notification_options       d,u,r
service_notification_commands   notify-service-by-email, notify-service-by-sms
host_notification_commands      notify-host-by-email, notify-host-by-sms
email                           ghada1972fr@yahoo.fr
pager                           +21621419100

host_notifications_enabled          1
service_notifications_enabled       1

}
```

Figure 34: configuration contact

Figure 35 : Définition des commandes de Notification

Conclusion

Dans ce chapitre nous avons mis l'intérêt sur l'aspect pratique de notre projet, en détaillant les étapes de la mise en place, la configuration et l'utilisation de ma solution, en mettant l'accent sur l'importance de l'apport de Centreon à Nagios, concernant la facilité de la configuration et la livraison des comptes rendus et d'analyses plus rapidement

Conclusion générale

Dans ce rapport nous avons décrit le travail effectué durant la période du projet .Nous avons atteint presque l'objectif initial de ce projet, ainsi l'administrateur peut contrôler les routeurs de son réseaux a travers l'outil de supervision effectué. Par contre aucun ne peut accéder à cette application sans avoir permission. Notre application comporte une cartographie présentant les différents équipements surveillés et elle permet de renseigner l'administrateur sur l'état des machines, le trafic écoulant, etc. Enfin, l'administrateur peut être averti par un message textuel, sous forme SMS et par Mail, dont le contenu indiquera la machine défectueuse.

Au terme de ce travail élaboré dans le cadre de mon projet de fin d'études, Nous avons considéré que ce projet nous a été bénéfique vu qu'il nous a permis de consolider nos connaissances vers la manipulation d'une application qui sera utile dans le domaine de la supervision informatique. En effet, l'apport de ce projet se résume surtout dans la découverte d'un nouveau domaine vaste et innovant qui est le contrôle et l'administration des réseaux des entreprises. De même, il nous a apporté énormément de connaissances tant au niveau du protocole SNMP qu'au niveau des équipements réseau.

Enfin nous considérons que le travail effectué au cours de ce projet peut être davantage enrichi et amélioré par de nouvelles fonctionnalités. En effet, nous pourrons envisager de :

- Implémenter d'autres stations (routeurs) dans d'autres sites afin de couvrir toutes la Tunisie et ainsi d'améliorer la précisions des donnes reçus (projet en cours).
- implémenter un ensemble de traps spécifiques: tels que la définition des seuils de déclenchement des alarmes pour distinguer un état opérationnel normal du réseau d'un état congestionné.
- Intégrer le Serveur Centreon satellite pour pouvoir ajouter des graphiques correspondant à notre infrastructure réseau.

Annexes

Installation de Nagios

Après installation des paquets perquise cité-dessus on commence l'installation de Nagios en suivant les étapes si dessous :

Création du compte user et des groupes de Nagios

```
root@ghadabens-VirtualBox:~# Sudo su
root@ghadabens-VirtualBox:~# /usr/sbin/useradd -m nagios
root@ghadabens-VirtualBox:~# passwd nagios
root@ghadabens-VirtualBox:~# /usr/sbin/groupadd nagios
root@ghadabens-VirtualBox:~# /usr/sbin/usermod -G nagios nagios
root@ghadabens-VirtualBox:~# /usr/sbin/usermod -G nagios www-data
```

Téléchargement des sources

Toujours sous en mode root :

```
root@ghadabens-VirtualBox:~# cd /usr/src
root@ghadabens-VirtualBox:~# wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-3.4.1.tar.gz
root@ghadabens-VirtualBox:~# tar xvzf nagios-3.4.1.tar.gz
root@ghadabens-VirtualBox:~# cd nagios
root@ghadabens-VirtualBox:~# ./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-command-user=nagios
root@ghadabens-VirtualBox:~# make all
root@ghadabens-VirtualBox:~# make install
root@ghadabens-VirtualBox:~# make install-init
root@ghadabens-VirtualBox:~#
root@ghadabens-VirtualBox:~# make install-config
```

➔Voilà nous avons installé Nagios .Maintenant nous allons installer ses plugins nécessaires:

On fait un **cd ..** pour revenir au répertoire précédent c'est-à-dire **sous /usr/src**

```
root@ghadabens-VirtualBox:~#  wget http://nagios.plugins.org/download/nagios-plugins-1.4.16.tar.gz
root@ghadabens-VirtualBox:~# tar xvzf nagios-plugins-1.4.16.tar.gz
root@ghadabens-VirtualBox:~# cd nagios-plugins-1.4.16/
root@ghadabens-VirtualBox:~# ./configure –with-nagios-user=nagios –with-nagios-group=nagios –with-openssl=/usr/bin/openssl
root@ghadabens-VirtualBox:~# make
root@ghadabens-VirtualBox:~# make install
```

Configurons maintenant l'accès Web de Nagios:

```
root@ghadabens-VirtualBox:~# htpasswd -c /usr/local/nagios/etc/ htpasswd.users nagios
New password:****
Re-type new password:****
```

Adding password for user nagios

Testons maintenant la configuration de Nagios grâce a la commande suivante :

```
root@ghadabens-VirtualBox:~# /usr/local/nagios/bin/nagios –v /usr/local/nagios/ /nagios.cfg
```

Si tout se passe bien nous devons voir ceci :

```
Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

On relance Nagios :

```
root@ghadabens-VirtualBox:~#  /etc/init.d/nagios start
```

On ouvre l'interface de Nagios en entrant l'URL : **http://localhost/nagios/**

Installation de la base de données NDO

Nagios et centreon utilise une base de données commune afin qu'ils communiquent entre eux. On commence alors par la création de cette base de donnés en se référant au serveur MySQL que nous avons installé au début.

```
root@ghadabens-VirtualBox:~# mysqladmin -u root -p create ndo
root@ghadabens-VirtualBox:~# mysql -u root -p mysql
```

```
mysql> GRANT ALL ON ndo.* TO "ndouser"@"localhost" IDENTIFIED BY
"ndopassword";
Query OK, 0 rows affected (0.00 sec)
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
mysql> exit
```

Mettons-nous sous le répertoire /usr/src

```
root@ghadabens-VirtualBox:~# cd /usr/src

root@ghadabens-VirtualBox:~# wget http://sourceforge.net/projetcts/nagios/files/
ndoutils-2.x/ndoutils-2.0.0/ndoutils-2.0.0.tar.gz
root@ghadabens-VirtualBox:~# tar xvzf ndoutils-2.0.0.tar.gz
root@ghadabens-VirtualBox:~# cd ndoutils-2.0.0
root@ghadabens-VirtualBox:~# ./configure  –prefix=/usr/local/nagios/ –enable-mysql –
disable-pgsql \ –with-ndo2db-user=nagios–with-ndo2db-group=nagios
root@ghadabens-VirtualBox:~# make
root@ghadabens-VirtualBox:~# cp ./src/ndomod-3x.o /usr/local/nagios/bin/ndomod.o
root@ghadabens-VirtualBox:~# cp ./src/ndo2db-3x /usr/local/nagios/bin/ndo2db
root@ghadabens-VirtualBox:~# cp ./config/ndo2db.cfg-sample/usr/local/nagios/etc/
ndo2db.cfg
root@ghadabens-VirtualBox:~# cp ./config/ndomod.cfg-sample/usr/local/nagios/etc/
ndomod.cfg
root@ghadabens-VirtualBox:~# chmod 775 /usr/local/nagios/bin/ndo*
root@ghadabens-VirtualBox:~# chown nagios:nagios /usr/local/nagios/bin/ndo*
```

Pour que NDO se lance au démarrage du serveur un script (téléchargeable depuis **http://www.nicolargo.com/blogdata/ndo2db**) doit être ajouter dans le fichier /etc/init.d/ndo2db.

```
root@ghadabens-VirtualBox:~# update-rc.d ndo2db defaults
root@ghadabens-VirtualBox:~# chmod +x /etc/init.d/ndo2db
```

Installation de Centreon

Commençons par le téléchargement du logiciel :

On se place dans /usr/src :

```
root@ghadabens-VirtualBox:~# cd /usr/src
root@ghadabens-VirtualBox:~#  wget http://s3-eu-west-1.amazonaws.com/centreon-download/public/centreon/centreon-2.5.4.tar.gz
root@ghadabens-VirtualBox:~# tar xvzf centreon-2.5.4.tar.gz
root@ghadabens-VirtualBox:~# cd centreon-2.5.4
root@ghadabens-VirtualBox:~# ./install.sh –i
```

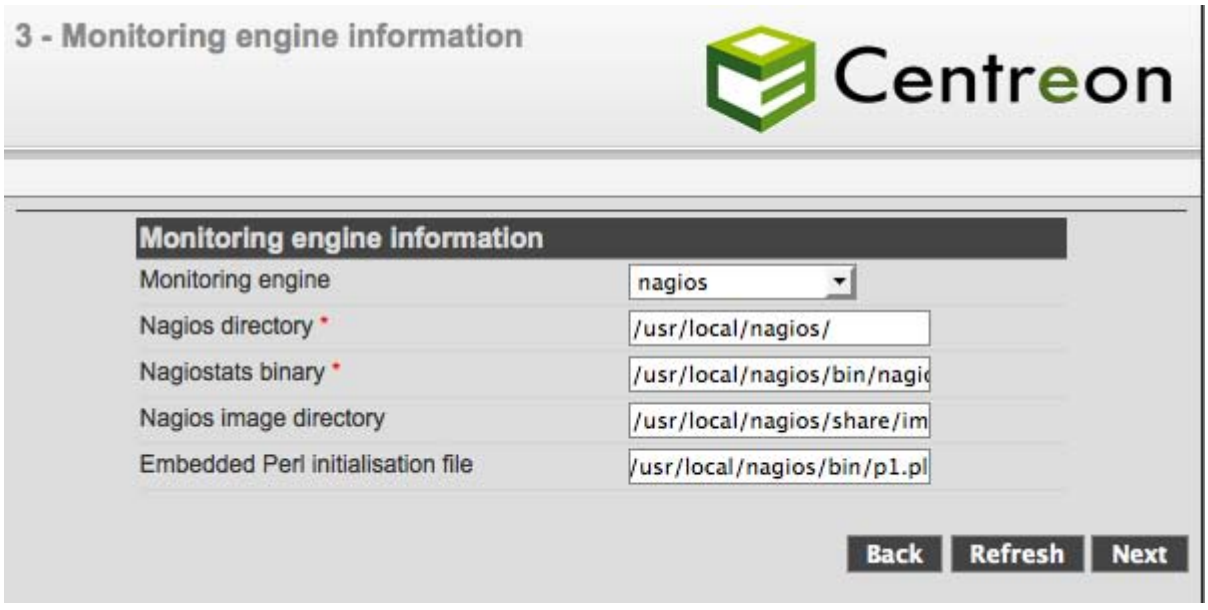
Il ne reste plus qu'à répondre aux questions qui s'affiche par « Y » en acceptant les chemins par défaut. Apres cette étape on redémarre le serveur apache.

```
root@ghadabens-VirtualBox:~# service apache2 restart
```

Ensuite on ouvre le navigateur et on tape : **http://localhost/centreon/**

Une fenêtre apparait pour continuer la configuration de centreon.

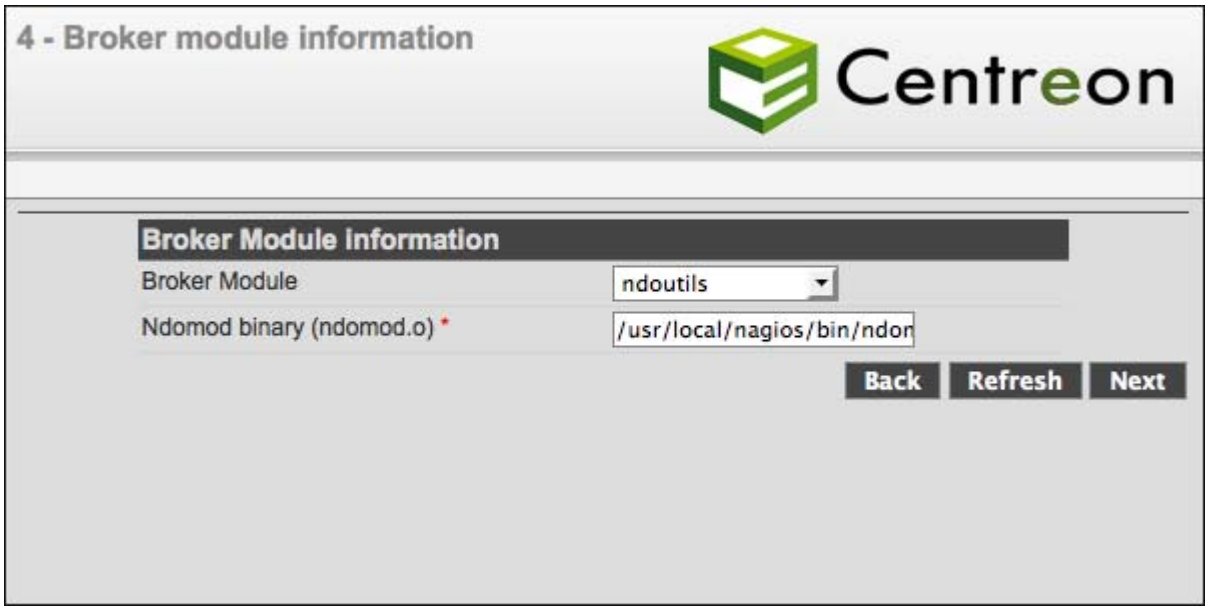
On vérifie que tout est OK et clique sur Next à chaque étape.



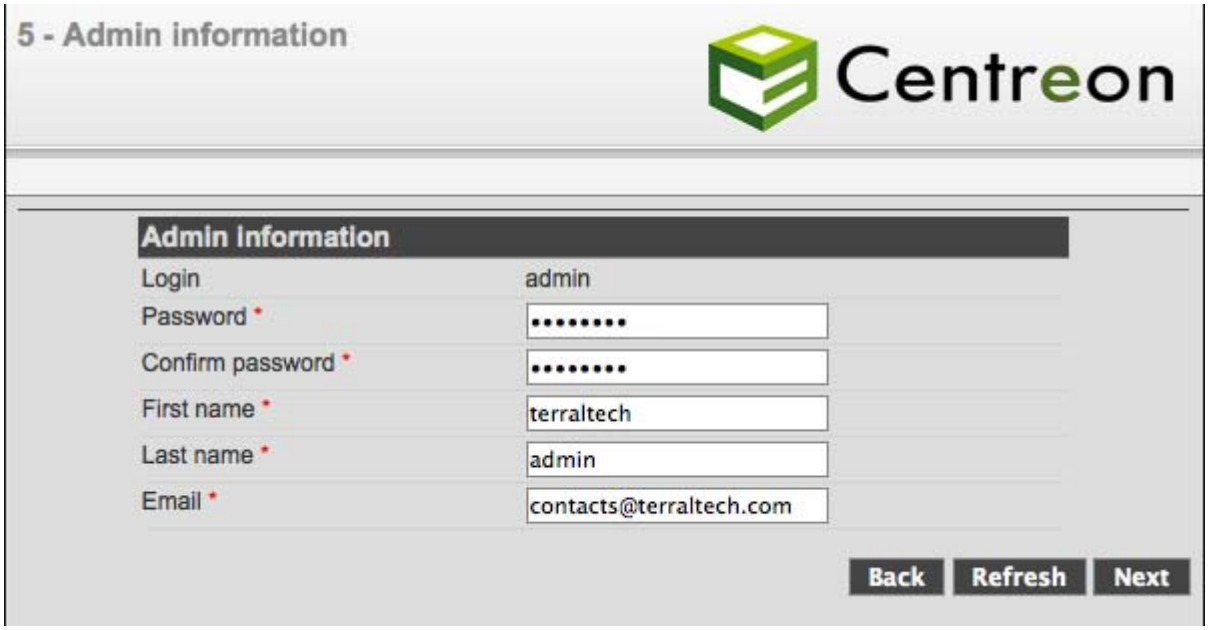
Nagios directory : /usr/local/nagios

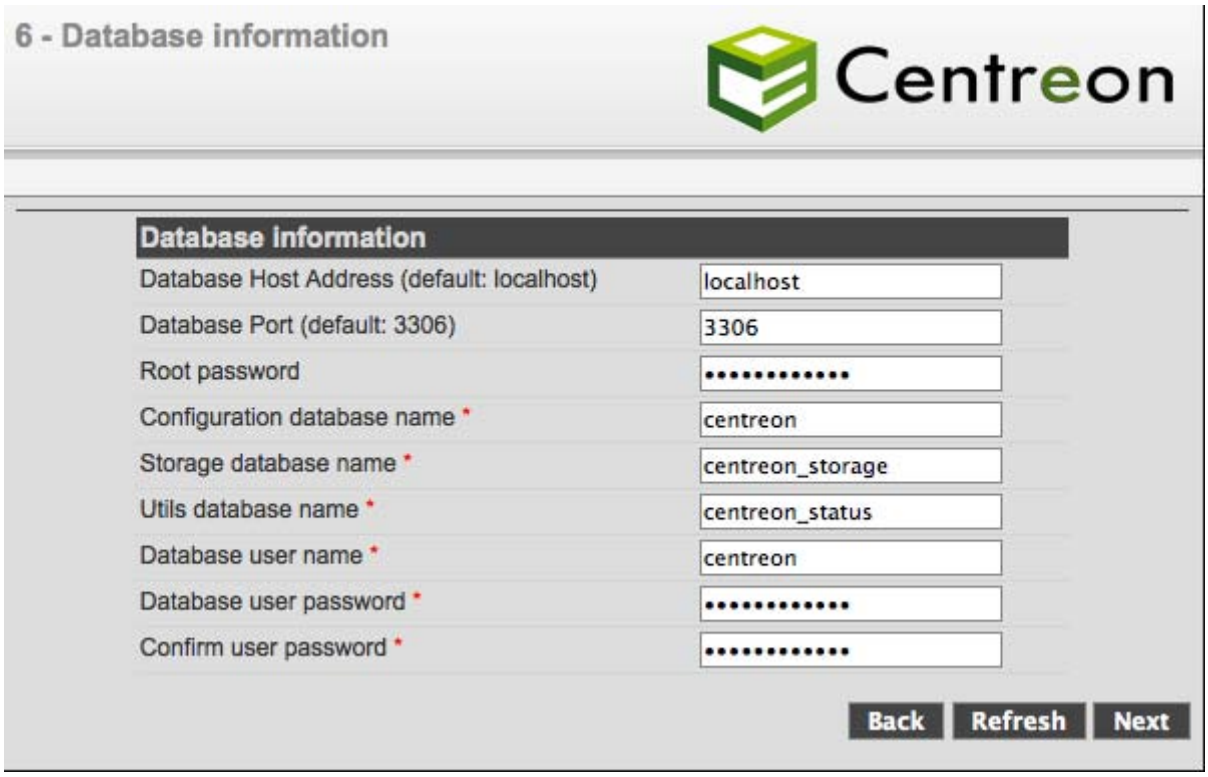
Nagiostats binary : /usr/local/nagios/bin/nagiostats

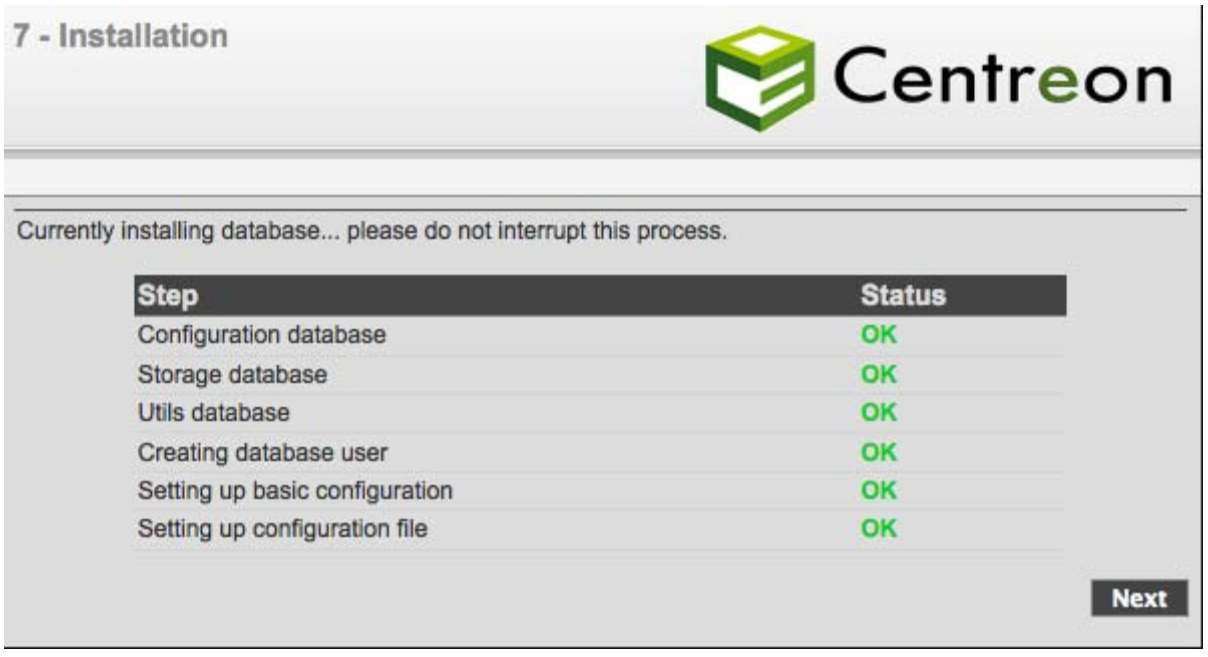
Nagios image directory : /usr/local/nagios/share/images



Ndomod Binry : /usr/local/nagios/bin/ndomod.o




6 - Database information
Centreon
Database information
Database Host Address (default: localhost)
localhost
Database Port (default: 3306)
3306
Root password
Configuration database name *
centreon
Storage database name *
centreon_storage
Utils database name *
centreon_status
Database user name *
centreon
Database user password *
Confirm user password *
Back
Refresh
Next


7 - Installation
Centreon
Currently installing database... please do not interrupt this process.
Step
Status
Configuration database
OK
Storage database
OK
Utils database
OK
Creating database user
OK
Setting up basic configuration
OK
Setting up configuration file
OK
Next

Configuration de SNMP

1- ***Installation du paquet snmp et des pré-requis nécessaires***

```
root@ghadabens-VirtualBox:~# apt-get install snmpd snmp-mibs-downloader
libsnmp-dev
```

2- ***Configuration du fichier snmpd.conf sous /etc/snmp/***

```
#  Listen for connections from the local system only
#agentAddress  udp:127.0.0.1:161
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161
#agentAddress udp::161
```

Bibliographie

Sites Web

[1] : http://fr.slideshare.net/chammem/projet-de-fin-detudes-1-fin

[2] : http://www-igm.univ-mlv.fr/~dr/XPOSE2007/dmichau_supervision/supervision.html

[3] : http://web.univ-pau.fr/~cpham/M2SIR/BIBLIO/DOC04-05/Nagios.pdf

[4] : http://ditwww.epfl.ch/SIC/SA/SPIP/Publications/spip.php?article1450

[6] : http://www.generation-linux.fr/index.php?post/2009/06/03/Zabbix-un-excellent-logiciel-de-supervision-reseau

[7] : http://www-igm.univ-mlv.fr/~dr/XPOSE2010/supervision/zabbix.html

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

[9] : https://fr.scribd.com/doc/106026614/Supervision-Avec-Nagios#scribd

[15] : http://blog.alexandrecazaux.fr/category/gnss/

[17] : http://www.o00o.org/monitoring/solutions.html#centreon

[18] : http://wiki.monitoring-fr.org/nagios/addons/nrpe?s[]=nrpe

[19] : http://blog.zenmail.biz/mise-en-place-des-outils-ndoutils-sur-ubuntu-serveur-part3/

[21] : http://www.commentcamarche.net/contents/514-vpn-reseaux-prives-virtuels-rpv

[22] :http://nicolasbroisin.fr/articles/Etude%20:%20Moyen%20et%20outils%20d%20exploitation

[23] :http://www.hexanet.fr/telecoms/mpls-vpn-interconnexion-sites/index.html#.VexMuuH_PQA

[24] :http://blog.nicolargo.com/2010/10/installation-dun-serveur-openvpn-sous-debianubuntu.html

[26] : https://www.le-vpn.com/fr/pptp/

[27] : http://www.cisco.co/web/FR/documents/pdfs/solutions/borderless/doc8_mus_aag.pdf.

[28] : http://fr.wikipedia.org/wiki/Unified_Modeling_Language

Ouvrages

[10] : Stéphane Aicardi, Protocoles et outils de base liés à la supervision ;(pdf Mathrice 2009)

[11] : Cédric Baillet **«** Les cahiers de la Sécurité : La sécurité de la téléphonie sur IP en entreprise **»**

[12] : David Imanache, Nicolas Joubert, Olivier Mayaud « *Nagios* » 2004 .]

[13] : COPONAT Pierre-Adrien et REYNIER Serge « *Supervision réseau* »

[14] : Ylian SAINT-HILAIRE, « SNMPV3-MODULAIRE : une méthodologie de conception et de la mise en œuvre d'un protocole de gestion de réseau », Novembre ,1998

[16] : ADJIDO Idjiwa, « Mise en place d'une solution de supervision avec Nagios », juin 2005

[20] : Thierry Briche ; Matthieu Voland « Les outils d'administration et de supervision reseau L'exemple de Nagios »

[25] : Cisco Systems ; fiche technique « ROUTEURS A SERVICES INTEGRES DE LA GAMME CISCO 1800 ».