**Ministère De l’enseignement Supérieur De La Recherche Scientifique**

**Université Jendouba**

[**Institut Supérieur**](https://www.google.tn/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBsQFjAA&url=http%3A%2F%2Fwww.isikef.rnu.tn%2F&ei=ZIzsVLywLI_jauCQgnA&usg=AFQjCNHdSeRZWapnZikF-xlissHpBXNyKg&bvm=bv.86475890,d.d24) **D’informatique Du Kef**

**PROJET FIN D’ETUDES**

**Année universitaire : 2014-2015**

***Dédicace***

*A mon Père,*

*A toute ma famille,*

*A Mes très chères Amis(es),*

*A Mes professeurs de l’I.S.I.K*

*A tous ceux que j’aime,*

*A tous ceux qui m’aiment,*

*A ceux et celles avec lesquelles j’ai passé les meilleur souvenirs de ma vie, je vous remercie pour votre bonne compagnie.*

*Je dédie ce travail en reconnaissance de leur inestimable soutien Durant ce long parcours.*

*Yassine Rhimi*

***Dédicace***

*A mes parents :*

*Grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat affectueux et propice à la poursuite de mes études.*

*Aucune dédicace ne pourrait exprimer mon respect, ma considération et mes profonds sentiments envers eux.*

*Je prie le bon Dieu de les bénir, de veiller sur eux, en espérant qu’ils seront toujours fiers de moi.*

*A tous mes professeurs :*

*Leur générosité et leur soutien m’oblige de leurs témoigner mon profond respect et ma loyale considération.*

*A tous mes amis et mes collègues :*

*Ils vont trouver ici le témoignage d’une fidélité et d’une amitié.*

*Anas Bouafia*

***Remerciements***

*Nos remerciements les plus sincères à toutes les personnes qui auront contribué de près ou de loin à l'élaboration de ce rapport.*

*Au terme de ce travail, Nous tenons à exprimer notre profonde  gratitude ainsi que Nos sincères remerciements à :*

*Mme* ***Rana Alyani,*** *notre encadreur pour sa disponibilité, son aide, son explication, son encouragement et ses conseils fructueux.*

*Mr* ***Amir ben Khlifa*** *notre encadreur au sein de la CNI pour son aide et sa motivation pour le projet, ainsi pour la confiance qu'il nous a témoignée tout au long de ce stage.*

*Notre gratitude va aussi aux membres du jury qui nous ont fait le grand honneur de juger et avoir accepter d’évaluer ce travail.*

*Finalement nous tenons à remercier notre institut qui nous donne l'occasion de s'intégrer à la vie professionnelle durant trois moins et nous espérons que ce travail sera convainquant et satisfaisant.*

***Glossaires***

**DNS** : Domain Name System : le DNS est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine.

**DHCP** : Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d’assurer la configuration automatique des paramètres IP.

**ISIK** : Institut Supérieur d’Informatique du Kef.

**MIB** : (Management Information Base). Sert à faire la translation d’un OID en un nom compréhensible.

**NAS** : Network Attached Storage : Le NAS par contre est une solution simple, pas très chère

**OID** : pour Object Identifier sont des identifiants universels, représentés sous la forme d'une suite de numéro. Ces identifiants vont nous permettre d’obtenir une information sur l’état d’un élément supervisé.

**SNMP** : Simple Network Management Protocol, est un protocole de communication qui permet aux administrateurs réseau de superviser les équipements du réseau.

**SAN**: Storage Area Network: Le SAN est un ensemble complet, performant et n'affectant pas les ressources du réseau car ayant ses équipements dédiés. C'est une solution onéreuse mais qui permet d'évoluer très facilement. Il est donc plutôt conseillé aux grosses entreprises. Mais difficile affaire évoluer. Il est donc destiné aux PME ou particuliers.

**SSH** : Secure Shell est un protocole de communication sécurisé

**PING** : le PING est le nom d'une commande informatique permettant de tester l'accessibilité d'une autre machine à travers un réseau.

***Table des matières***

*Introduction Générale1*

*Chap1 Etude préalable2*

*1.1 Introduction2*

*1.2 Présentation De la Société D’accueil2*

*1.2.1 Présentation générale2*

*1.2.2 Organigramme du CNI3*

*1.2.3 Les missions de CNI3*

*1.2.4 Les Services de CNI3*

*1.3 L’objectif de notre projet 4*

*1.3.1 Etude de l’existant4*

*1.3.1.1 Description De l’existant4*

*1.3.1.2 Critique De L’existant5*

*1.3.1.3 Solution Proposé5*

*1.4. Conclusion5*

*Chapitre 2 Supervision Réseaux 6*

*2.1 Introduction6*

*2.2 Définition6*

*2.3 Les Différents types de Protocoles De Supervision 7*

*2.3.1 SNMP7*

*2.3.1.1 Mécanisme 8*

*2.3.1.2 La MIB9*

*2.3.2. ICMP9*

*2.3.3 Les outils de surveillance d’un réseau9*

*2.3.3.1 Ping9*

*2.3.3.2 MRTG9*

*2.3.3.3 RRDTOOL10*

*2.4. Les différents types des Logiciels De Supervision10*

*2.4.1 Les Solutions De Supervisions Payantes11*

*2.4.1.1 IBM Tivoli Monitoring 11*

*2.4.1.2 BMC Patrol11*

*2.4.1.3 HP OpenView11*

*2.4.2 Les Solutions de Supervision Gratuites12*

*2.4.2.1 Eyes of network12*

*2.4.2.1.1 Les avantages12*

*2.4.2.1.2 Les inconvénients13*

*2.4.2.2 FAN, Fully Automated Nagios13*

*2.4.2.2.1 Les avantages13*

*2.4.2.2.2 Les inconvénients14*

*2.4.2.3 Nagios/Centreon14*

*2.4.2.3.1 Les avantages15*

*2.4.2.3.2 Les inconvénients15*

*2.4.2.4 Tableau comparatif entes les logiciels de la supervision15*

*2.5 Notre choix d’outil 15*

*2.5.1 Présentation de l’outil de supervision Eyes Of Network16*

*2.5.1.1 Architecture16*

*2.5.1.2 Programmes-plugins17*

*2.5.1.3 Les fichiers de configuration17*

*2.6 Conclusion 17*

*Chapitre 3 Les compléments de Eyes Of Network18*

*1.3 Introduction18*

*3.2 Nagios18*

*3.2.1 Présentation18*

*3.2.2 architecture18*

*3.3 Cacti19*

*3.3.1 Présentation19*

*3.4 NAGVIS20*

*3.4.1 Disposition des indicateurs sur une carte de supervision20*

*3.5 Choix des images par l’administrateur Images des éléments supervisés 20*

*3.6 Conclusion 21*

*Chapitre 4 Réalisation et tests22*

*4.1 Introduction22*

*4.2 Environnements de mise en place22*

*4.2.1 Environnement matériels22*

*4.2.1.1 Système Linux entreprise (Centos 6.3)22*

*4.2.2 Environnement logiciels23*

*4.2.2.1 VMware Workstation 23*

*4.2.2.2 La solution de supervision Eyes Of Network23*

*4.2.2.3 GNS323*

*4.3 Mise en place d’Eyes of network23*

*4.3.1 Installation d’Eyes of network23*

*4.3.1.1 Installation23*

*4.3.1.2 Interfaces de Eyes Of Network28*

*4.4 Installation du protocol SNMP29*

*4.4.1 Installation et paramétrage du SNMP sous linux29*

*4.4.2 Installation et paramétrage du SNMP sous Windows30*

*4.4.3 Architecture réseaux sous GNS332*

*4.5 Interface de configuration : Interface web d’EON35*

*4.5.1 Scan du réseau35*

*4.5.2 superviser des hôtes36*

*4.5.3 Superviser un serveur Windows40*

*4.5.4 Superviser un serveur linux40*

*4.5.4 Superviser les actifs41*

*4.6 Synchronisation avec Cacti44*

*4.7 Exemple d’utilisations47*

*4.5.1 Paramétrage de Postfix48*

*4.6 Conclusion50*

*Conclusion générale51*

*Résumé52*

*Annexe53*

*Néographies60*

*Bibliographies61*

***Liste des figures***

*Figure 1.1: vue générale sur le CNI2*

*Figure 2.1: Organigramme du CNI3*

*Figure 3.1: l’architecture du réseau de CNI4*

*Figure 1.2: Architecture SNMP7*

*Figure 2.2: BMC Patrol11*

*Figure 3.2: HP OpenView11*

*Figure 4.2: Eyes of Network12*

*Figure 5.2: FAN, Fully Automated Nagios13*

*Figure 6.2: Nagios/Centreon.14*

*Figure 7.2: Les outils constituents Eyes Of Network16*

*Figure 8.2: Architecture d’ Eyes Of Network16*

*Figure 1.3: Architecture de l’outil Nagios19*

*Figure 2.3: fonctionnalité Cacti19*

*Figure 1.4: l’interface graphique d’installation EON24*

*Figure 2.4: Partitionnement du disque 24*

*Figure 3.4: paramétrages divers25*

*Figure 4.4: mot de passe root du serveur25*

*Figure 5.4: choix des paquets26*

*Figure 6.4: démarrage du processus d’installation d’EON 27*

*Figure 7.4: démarrage du d’EON27*

*Figure 8.4: fenêtre d’authentification28*

*Figure 9.4: interface graphique d’Eyes Of Network 28*

*Figure 10.4: Activation du Protocole SNMP30*

*Figure 11.4: Windows modifie les fonctionnalités30*

*Figure 12.4: invite des commandes31*

*Figure 13.4: panneau des services 31*

*Figure 14.4: propriétés de service SNMP32*

*Figure 15.4:* *Architecture réseaux 32*

*Figure 16.4:* *configuration de nuage 133*

*Figure 17.4: configuration de nuage 2 33*

*Figure 18.4: interconnecter l'interface du routeur avec le nuage 33*

*Figure 19.4: Start routeur 1 34*

*Figure 20.4: console34*

*Figure 21.4: configuration du routeur 135*

*Figure 22.4: Auto-discovery35*

*Figure 23.4: Paramétrage Auto-discovery 36*

*Figure 24.4: configuration du routeur 1 36*

*Figure 25.4: test SNMP37*

*Figure 26.4: test SNMP37*

*Figure 27.4: superviser une Hôte37*

*Figure 28.4: Ajout d’une hôte38*

*Figure 29.4: GroupMembership38*

*Figure 30.4: Inheritance39*

*Figure 31.4: application de la configuration 39*

*Figure 32.4: succès de l'application de la configuration39*

*Figure 33.4: équipenment 40*

*Figure 34.4: etat d’équipement 40*

*Figure 35.4: équipements41*

*Figure 36.4: etat d’équipements41*

*Figure 37.4:* *arrête de routeur2 42*

*Figure 38.4:* *douteur2 est en panne 42*

*Figure 39.4:* *arrête de switch1 45*

*Figure 40.4:* *switch1 est en panne 43*

*Figure 41.4:* *routeur2 et Switch 1 en pannes44*

*Figure 42.4: Synchroniser Cacti avec Nagios44*

*Figure 43.4: Paramétrage Cacti45*

*Figure 44.4: Generic OID Template45*

*Figure 45.4: ajout d'OID* *45*

*Figure 46.4: Graphes de trafic sur les interfaces du routeur146*

*Figure 47.4: Graphes d’espace mémoires utilisé sur Windows46*

*Figure 48.4: Graphes d’espace mémoires utilisé sur CentOS47*

***Introduction Générale***

Actuellement toutes les entreprises sont équipées d’un réseau local au minimum, et de réseaux de longues distances pour les plus importantes d’entre elles. Leurs parcs informatiques englobent une dizaine voir une centaine d’équipements, engendrés par des serveurs de bases de données et des serveurs de traitements.

Vu que ces systèmes informatiques sont au cœur des activités des entreprises, leur maitrise devient Primordiale. Ils doivent fonctionner pleinement et en permanence pour garantir la fiabilité et l’efficacité exigées, et surtout travailler à réduire les problèmes de défaillances, les pannes, les coupures et les différents problèmes techniques qui peuvent causer des pertes considérables.

De ce fait, les administrateurs réseau font appel à des logiciels de surveillance et de supervision de réseaux afin de vérifier l'état du réseau en temps réel de l'ensemble du parc informatique sous leur responsabilité. Et être aussi informés automatiquement (par email, par SMS) en cas de problèmes. Grâce à un tel système, les délais d'interventions sont fortement réduits et les anomalies peuvent être aussitôt prises en main avant même qu’un utilisateur peut s’en apercevoir.

Ainsi, la supervision des réseaux s’avère nécessaire et indispensable. Elle permet entre autre d’avoir une vue globale du fonctionnement et des problèmes pouvant survenir sur un réseau mais aussi d’avoir des indicateurs sur la performance de son architecture. Dans ce cadre, le présent rapport se base sur 4 chapitres:

Chapitre 1 : Présente l’entreprise accueillante, la problématique de notre projet et la solution adoptée.

Chapitre 2 : Présente les notions de base de la supervision et de ses logiciels les plus utilisés actuellement et enfin la solution choisie parmi plusieurs en énumérant ses fonctionnalités et apports.

Chapitre 3 : présente les compléments de la solution choisie.

Chapitre 4 : la réalisation, l’environnement de travail et la mise en place de cette solution.

***Chapitre 1***

***Etude Préalable***

* 1. **Introduction**

Ce chapitre se focalise sur la présentation de l’entreprise accueillante où on concernera la problématique de notre projet et on présentera la solution adoptée pour ce dernier.

* 1. **Présentation De La Société D’accueil**
     1. **Présentation Générale**



*Figure 1.1: vue générale sur le CNI*

Le Centre National de l'Informatique a été créé le 30 décembre 1975 par la Loi n° 75-83 du 30 décembre 1975- Articles 35 à 42, en tant qu’Établissement Public à caractère Industriel et Commercial. En 1997, il a été reclassé Établissement Public à caractère Non Administratif. Il fut rattaché au Premier Ministère avant d'être placé sous la tutelle du Ministère des Technologies de la Communication. Il est doté de la personnalité civile et de l'autonomie financière.

Le CNI offre, depuis 32 ans, à l’Administration publique tunisienne et à ses clients des différents secteurs socio-économiques du pays, un service complet, allant du conseil à l’hébergement en passant par les études, la conception et le développement de différentes applications ( INSAF, ADEB, MADANIA, AMEN, RACHED…).

|  |
| --- |
| **1.2.2**  **Organigramme du CNI** |
|  | |
| *Figure 2.1: Organigramme du CNI*  **1.2.3 Les missions de CNI**  Les Principales missions de CNI sont :   * Mise en œuvre et déploiement de l’Administration. * Maîtrise d’ouvrage déléguée. * Fixation et proposition des méthodes et des normes d’ingénierie et techniques. * Assistance des utilisateurs. * Réalisation d’études : d’orientation, stratégiques et missions d’audit informatique. * Formation dans le domaine de l’informatique au profit des établissements publics.   **1.2.4 Les Services de CNI**  Le Centre National de l’Informatique assure actuellement : La gestion et le développement des applications inter-administratives promues par le gouvernement et qui entrent dans le cadre de la modernisation, Le traitement de l’informatique et l’exploitation des applications.  La réalisation des programmes et des projets informatiques au profit des organismes publics ou privés nationaux et étrangers, et la réalisation de consultations pour le compte de ces organismes.  La maintenance des réseaux et des équipements informatiques pour le compte des ministères et des entreprises publiques. Ainsi le centre National de l’informatique offre une formation continue et de recyclage dans le domaine de l’informatique et de la microinformatique avec des stages de formation ou de perfectionnement pour les ressortissants des pays amis.  **1.3 L’objectif de notre projet**  le projet consistait à reprendre un logiciel de supervision de réseau dont les principales fonctionnalités sont la découverte de la topologie des réseaux à partir des informations récupérables en interrogeant les équipements réseaux avec le protocole SNMP, collecter les pannes et les anomalies du système supervisé, et finalement présenter les données graphiquement La solution serait donc la mise en place des contrôles automatisés chez chacun de nos clients, renvoyant des alertes emails en cas de problème.  **1.3.1 Etude de l’existant**  **1.3.1.1 Description De l’existant**    *Figure1. 3.1: l’architecture du réseau de CNI*  **1.3.1.2 Critique De L’existant**  Ayant un très grand nombre de serveurs à gérer, l’administrateur est incapable de vérifier leurs disponibilité (en ligne ou pas), de déterminer la qualité des services qu’ils offrent, ni détecter la défaillance des équipements.  **1.3.1.3 Solution Proposé**  Nous travaillant à offrir une meilleure qualité de services 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 . Etde mettre en évidence un outil pour contrôler le fonctionnement du réseau, d’étudier les données collectées et de définir des seuils d’alertes qui peuvent servir pour le déclenchement des alertes lors de détection des problèmes. Il s’agit donc et sans doute d’une mise en place d’un système de supervision qui pourra grâce aux différentes fonctionnalités qu’il offre, anticiper les pannes en suivant méticuleusement le fonctionnement du système, Un système de supervision offrira à l’administrateur la possibilité de réagir le plus rapidement possible face aux pannes qui peuvent intervenir afin d’éviter un arrêt de production de trop longue durée.Le but de ce projet est donc de trouver une solution optimale pour la gestion des équipements, offrir la possibilité de devenir « pro actif » face aux problèmes rencontrés, et le plus important, de pouvoir détecter et interpréter en un simple coup d’œil les causes et origines des problèmes rencontrés afin de les fixer le plus rapidement possible.  **1.4. Conclusion**  Ce chapitre a été conçu pour familiariser l’environnement du travail en présentant l’entreprise d’accueil et l’architecture réseau dont elle dispose. Les problèmes que rencontre la société se sont imposés suite à l’étude de l’existant et à sa critique, ce qui nous permet de cerner la problématique de notre  projet Nous étions par la suite proposé des solutions et leur études a notre gérant et finalement nous avons posé notre choix sur la solution que nous jugeons la plus convenable à la société et à la formation que nous estimons acquérir qui est le logiciel de supervision libre « Eyes of network ». Le chapitre suivant attaquera une étude approfondie de la solution choisie. | |

***Chapitre 2***

***Supervision Réseaux***

**2.1 Introduction**

Dans ce présent chapitre, On commence par définir la notion de la supervision et ses objectifs ensuite, analyser de près les fonctionnalités de la solution proposée, son architecture, et les différents services qu’elle offre et finir par énumérer les différents fichiers de configuration sur quoi se base cette solution.

**2.2 Définition**

La supervision des réseaux peut être définie comme l’utilisation des ressources réseaux adaptées dans le but d’obtenir des informations (en temps réel ou non) sur l’utilisation ou la condition des réseaux et de leurs éléments afin d’assurer un niveau de service garanti, une bonne qualité et une répartition optimale et de ceux-ci. La mise en place d’une supervision réseau, a donc pour principale vocation de collecte les informations nécessaires sur l’état de l’infrastructure et des entités qui y sont utilisés, de les analyser et de les rapporter à intervalle régulier.

L’objectif d’une supervision de réseaux peut ainsi se résumer en trois points :

* **Etre réactif**en alertant l’administrateur (e-mail ou sms) en cas de dysfonctionnement d’une partie du système d’information.
* **Etre pro actif**en anticipant les pannes possibles.
* Cibler le problème dès son apparition afin d’agir rapidement de la façon la plus pertinente possible.

**2.3 Les Différents types de Protocoles De Supervision**

**2.3.1 SNMP**

SNMP signifie Simple Network Management Protocol (traduisez protocole simple de gestion de réseau). Il s'agit d'un protocole qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau.

Les buts du protocole SNMP sont de :

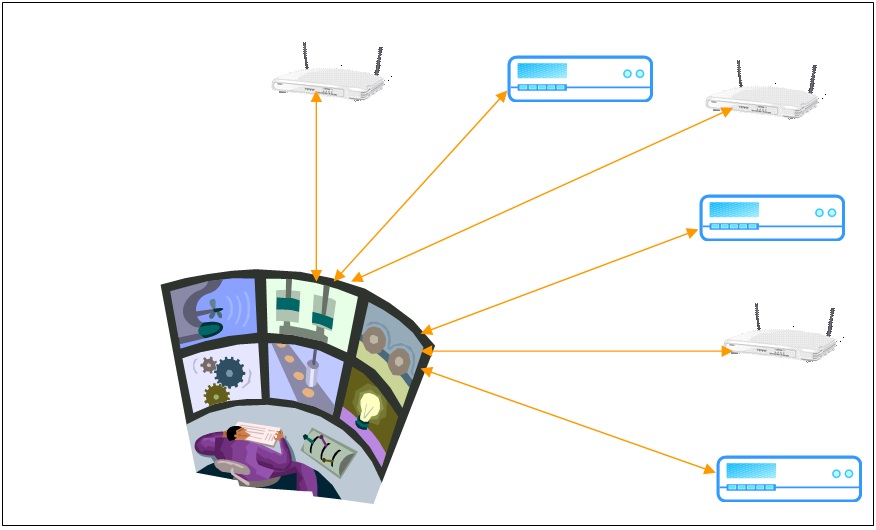
• Connaître l'état global d'un équipement (actif, inactif, partiellement opérationnel...)

• gérer les évènements exceptionnels (perte d'un lien réseau, arrêt brutal d'un équipement...)

• analyser différents métriques afin d'anticiper les problèmes futurs (engorgement réseau...)

• agir sur certains éléments de la configuration des équipements.

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



*Figure 1.2 : Architecture SNMP*

* Les agents SNMP : ce sont les équipements (réseau ou serveur) qu'il faut superviser.
* Le superviseur SNMP : c'est une machine centrale à partir de laquelle un opérateur humain peut superviser en temps réel toute son infrastructure, diagnostiquer les problèmes et finalement faire intervenir un technicien pour les résoudre.
* Le protocole SNMP : c'est le protocole utilisé par les agents SNMP et leur superviseur pour communiquer entre eux.
* La MIB : ce sont les informations dynamiques instanciées par les différents agents SNMP et remontées en temps réel au superviseur.
* Les outils SNMP. Ce sont les différents utilitaires utilisés par le superviseur pour l'aider à diagnostiquer un problème. Ces différents outils sont aussi utilisés lors de la configuration du superviseur pour prendre en compte les spécificités de l'infrastructure.

**2.3.1.1 Mécanisme**

Par soucis de simplicité et donc de rapidité, SNMP ne transporte que des variables et s'appuie sur le protocole UDP (User Datagramme Protocol). SNMP va créer un dialogue entre des agents installés sur des machines à superviser et un serveur de supervision.

Les échanges entre agents et serveur se résument à trois opérations, les alarmes, les requêtes et les réponses :

* Une requête est émise du serveur vers un agent via le port 161 UDP si le serveur veut demander ou imposer quelque chose à cet agent. La requête peut être de quatre types
  + **GetRequest** : Demande la valeur d'une variable à un agent
  + **GetNextRequest** : Demande la valeur suivante de la variable
  + **GetBulk** : Demande un ensemble de variables regroupées
  + **SetRequest** : Demande la modification de la valeur d'une variable sur un agent
* L'agent va ensuite traiter cette requête et émettre une réponse via le même port. Si tout se passe bien, l'agent répond un GetResponse accompagné de la valeur demandée. Mais dans le cas contraire l'agent ajoutera un code d'erreur en réponse (par exemple No Access ou Read Only)
* Une alarme est crée par un agent en cas d'évènement et utilise un message dit de type trap ou de type informe pour prévenir le serveur. Ce message SNMP transite via le port 162 UDP. Les alarmes peuvent prendre les formes suivantes :
  + **Cold Start(0)** : Redémarrage à froid du système
  + **Warm START(1)** : Redémarrage à chaud du système
  + **Link Down(2)** : Le lien réseau n'est plus opérationnel
  + **LinkUp(3)** : Le lien réseau est opérationnel
  + **AuthentificationFailure(4)** : Tentative d'accès à l'agent avec un mauvais nom de communauté
  + **EGPNeighboorLoss(5)** : La passerelle adjacente ne répond plus
  + **EntrepriseSpecific(6)** : Alarme propre aux constructeurs

Étant donné que ces requêtes utilisent des noms de variables, ceux-ci doivent être communs à tout matériel que l'on souhaite monitorer (et supportant SNMP).  
C'est pour cette raison que les données sont stockées dans une base normalisée nommée MIB (Managed Information Base). Cette base organisée de manière hiérarchique et assez compliquée à lire pour un humain. Chaque information (les fameuses variables précédentes) est identifiée par un OID (Object Identifier).

**2.3.1.2 La MIB (Est détaillées dans l’annexe)**

**2.3.2. ICMP (Internet Control Message Protocol)**

ICMP est un protocole de couche réseau (couche 3 du modèle OSI) qui vient palier à l'absence de message d'erreur du protocole IP (Internet Protocol). En effet s’il y a un incident de transmission les équipements intermédiaires vont utiliser ce protocole pour prévenir la machine émettrice. Les paquets ICMP sont encapsulés dans des paquets IP (malgré qu'ils soient au même niveau OSI), et peuvent contenir des bouts de paquets IP pour citer celui ayant généré l'erreur. Afin de catégoriser les erreurs, elles sont divisés en types eux-mêmes parfois Redi vises en codes. Par exemple le type 3 représente un destinataire inaccessible : Il existe 16 codes différents en fonction de la raison pour laquelle le destinataire n'est pas joignable.

**2.3.3 Les outils de surveillance d’un réseau**

**2.3.3.1 Ping**

Voilà un outil très simple, qui remplit une tâche très importante. C'est en effet ce programme qui va nous permettre, en utilisant le protocole ICMP, de savoir si une machine destination est accessible (dans le cas contraire, connaître approximativement la raison via le code d'erreur ICMP) et de mesurer la latence existante entre les deux extrémités.  
L'implémentation est simple, Ping envoi une requête ICMP Echo et attend en retour une requête ICMP Echo Reply. Ping est par exemple souvent utilisé pour réaliser une alerte qui prévient l'administrateur d'une machine quand celle-ci n'est plus joignable.

**2.3.3.2 MRTG**

MRTG est un outil réalisé en Perl et en C, dont le but de surveiller la charge des liens réseaux. Il génère des pages html contenant des images au format PNG qui représentent graphiquement l'état en temps réel de la ressource surveillée. Le principe est simple : un script Perl recherche les données via le protocole SNMP et envoi celles-ci à un programme C qui va les stocker et générer les graphiques.  
A la base l'auteur avait dans le but de surveiller le trafic passant par des routeurs, mais MRTG se basant sur SNMP, les possibilités se sont étendues à toute variable. Encore mieux, on peut aussi créer un script qui surveillera n'importe quel type de donnée non disponible dans SNMP. On possède ainsi un système de surveillance déjà conséquent qui permet sur une même page de surveiller un réseau et de garder les traces des anciennes données.

**2.3.3.3 RRDTOOL**

Du même auteur que MRTG, RRDTOOL est un peu considéré comme une évolution de ce dernier. La gestion de stockage des données a surtout été entièrement revue pour améliorer les performances, pour cela l'auteur a utilisé une technique nommée "Round Robin", d'où le nom "RRDTOOL" (Round Robin Database TOOL).  
Les graphiques se sont également améliorés offrant plus de possibilités, et l'interfaçage entre la récupération de donnée et la génération des images est devenu plus modulaire permettant de réaliser des scripts dans beaucoup de languages différents. RRDTOOL est maintenant un outil incontournable pour générer des graphiques, il est donc utilisé dans quasiment tous les logiciels de supervision open-source.

**2.4. Les Différents types des Logiciels De Supervision**

S’assurant que la supervision est un marché porteur, les sociétés se pressent de plus en plus à investir dans des produits permettant la supervision et une meilleure gestion des réseaux.

 Deux familles apparaissent, celle proposant des solutions généralistes pour la supervision des réseaux, des serveurs, des applications, des sites web.

D’autres offrent une supervision des domaines plus spécifiques citant comme logiciel panorama (Altaworks) qui gère uniquement l’aspect sécurité ou PathWAI (Candle) qui se penche principalement sur la supervision des applications.

* Il existe différents types d'outils de supervision ayant chacun leurs qualités et leurs défauts :
* Solutions propriétaires couteuses
* Utilisation d'outils open source qui ont fait leurs preuves

**2.4.1 Les Solutions De Supervisions Payantes**

IBM Tivoli Monitoring

BMC Patrol

HP OpenView

**2.4.1.1 IBM Tivoli Monitoring**

Il s’agit d’un logiciel de supervision intégré au « frame wok » Tivoli d’IBM  
Il permet la surveillance d’un système informatique (OS réseau applications matériel etc.)  
Et l’envoi d’alertes vers une console de supervision (particulièrement vers Tivoli entreprise console).

**2.4.1.2 BMC Patrol**

****

*Figure 2.2 : BMC Patrol*

Patrol est l’un des plus anciens logiciels de supervision de marché

BMC avec patrol fait figure de pionnier dans le domaine de la supervision sa gamme de produit en matières de supervision est supérieur à l’ensemble des éditeurs concurrents.

On trouve différents dénomination pour les outils patrol tels que performances manager cet outil est multiplateforme et permet donc la supervision sur les environnements UNIX Linux et Windows.

**2.4.1.3 HP OpenView**

****

*Figure 3.2 : HP OpenView*

(Network Node Manager maintenant) : solution payante, référence en matière de supervision réseau.

**2.4.2 Les Solutions de Supervision Gratuites**

Il existe des solutions de supervision libres et professionnelles. L’avantage de ces logiciels libres est la gratuité, la disponibilité du code source et la liberté d’étudier et de modifier le code selon nos besoins et de le diffuser.

De plus, il existe une communauté importante d’utilisateurs et de développeurs qui participent à l’amélioration des logiciels et apportent une assistance par la mise en ligne des documentations et les participations aux forums. . Parmi les plus répandues, reconnues du moment nous pouvons citer

Eyes of network

FAN, Fully Automated Nagios

Nagios/Centreon.

**2.4.2.1 Eyes of network**

****

*Figure 4.2 : Eyes Of Network*

GLPI / OCS / FUSION Gestion de par cet inventaire   
Eyes Of Network est accessible via une interface Web unique dont l’objectif est de réunir les différents acteurs d’un système d’informations ( DSI , Administrateurs , Techniciens , Operateurs ) chacun de ces acteurs dispose d’une vue correspondant à son métier Toutes les informations sont consolidées en Base de Données MYSQL ou BERKELEY  
Eyes of network est un produit sous licence GPL2 sponsorisé et proposé par APX Clod builler dans le cadre de présentations de services Intégration Télé service Support téléphonique et Tierce Maintenance Applicative.

**2.4.2.1.1 Les avantages**

-Permet de regrouper tous les outils ITIL + Supervision dans une même distribution

-Ajouter un gestionnaire de performance

-Interface de configuration web

-Permet de faciliter le déploiement des outils de supervision

-Fait gagner un temps précieux

-SSO permettant de se loguer une seule fois et d’accéder à tous les outils d’administration

- Noyau Linux solide et fiable

-Auto-discovery

-Possibilité d’administrer ses périphériques via SSH/Telnet… depuis son interface web

-Possibilité de s’authentifier via un serveur LDAP

**2.4.2.1.2 Les inconvénients**

-Une configuration en interface Web qui ne supporte pas l’HTTPS   
-Pas de CENTREON

**2.4.2.2 FAN, Fully Automated Nagios**

****

*Figure 5.2 : FAN, Fully Automated Nagios*

Est une nouvelle distribution GNU/Linux dédiée à la supervision Nagios (c'est à dire la surveillance système et réseau). FAN est né du constat que pour disposer d'une solution de supervision Nagios complète.

**2.4.2.2.1 Les avantages**

FAN est une distribution dédiée à la supervision de ce fait, elle dispose des points forts suivants:

* simplicité et rapidité d'installation: en effet, il n'est pas simple d'installer l'ensemble des outils. Par exemple, Centreon dispose de nombreuses dépendances sur des paquets PEAR. Leur installation est souvent déroutante pour des débutants. Avec FAN, l'installation de l'OS et de tous les paquets prend une petite demi-heure.
* intégration: les outils sont préconfigurés et forment une tout logique. Il n'est a priori pas nécessaire de les reconfigurer de manière importante
* complet: de nombreux outils sont disponibles et le spectre fonctionnel est suffisamment large pour convenir au maximum de monde
* le Plan de Reprise d'Activité est plus simple à mettre en œuvre

**2.4.2.2.2 Les inconvénients**

FAN dispose aujourd'hui de points faibles. Ce n'est pas étonnant vu son numéro de version (1.0 aujourd'hui). Les points faibles identifiés pour le moment sont:

- Choix effectués : étant donné que nous ne souhaitions pas packager l'ensemble des outils Nagios existants, des choix ont été faits. Ces choix peuvent être mis en cause, remis en cause et ré-remis en cause, ceci de manière perpétuelle. Ils ont été faits en fonction de deux points : est-ce-que l'outil est parmi les meilleurs aujourd'hui dans sa catégorie ? Combien des membres du projet maîtrisent-ils correctement cet outil ? Des trolls ont été aperçus lors des discussions précédentes et risquent de revenir régulièrement.

* Nagios 3 et Centreon 2 non disponibles pour le moment. Nous travaillons sur le sujet aujourd'hui et espérons disposer très rapidement d'une version de développement avec ces versions.
* la langue anglaise n'est pas correctement parlée (ni écrite d'ailleurs) par tous les membres du projet. J'en suis un parfait exemple : mes échanges avec des personnes non francophones sont très difficiles.
* FAN est un projet encore jeune. Les membres du projet sont en attentes de vos conseils et de vos remarques constructives pour améliorer encore la qualité et tout ce qui peut l'être. N'hésitez pas à faire des retours de bug et des demandes de nouvelle fonctionnalité. N'hésitez pas non plus à nous prodiguez des conseils sur ce site ou sur les blogs associés à FAN (celui du responsable du projet et celui de LKCO).

**2.4.2.3 Nagios/Centreon.**

**

*Figure 6.2 : Nagios/Centreon.*

Nagios est une solution de supervision système très connue, elle permet de surveiller des services (MySQL, ftp, http,…) et des hôtes, pour vérifier s’ils sont opérationnels et avertir dans le cas contraire, il peut aussi découvrir l’environnement réseaux et en dresser une carte.

Centreon est la surcouche à Nagios qui permet de pouvoir l’administrer plus facilement (interface web) et améliore énormément son utilisation.

Nagios a été développé par Ethan Galstad et Centreon par Romain Le Merlus, Julien Mathis, les 2 sous la licence « GNU General Public License Version 2 ».

**2.4.2.3.1 Les avantages**

- Evolutif, par plugins et par modèles,

- Grosse communauté et documentation.

-Peut-être interfacé avec d’autres outils (Cacti, Munin).

- Test avancé de services et de connections (latence, découverte automatique du réseau).

- Solution tout en un.

**2.4.2.3.2 Les inconvénients**

- Besoin de Centreon pour respecter le cahier des charges en termes d’ergonomie

- installation et configuration « lourde »

- l'ajout de Centreon demande plus de ressources

**2.4.2.4 Tableau comparatif entes les logiciels de la supervision**

**(Est détaillées dans l’annexe)**

**2.5 Notre choix d’outil**

Parmi ces solutions libres, les deux logiciels FAN et Eyesofnetwork sont les plus répandus et les plus utilisés. Ce sont les deux solutions les plus adaptées permettant de satisfaire pratiquement tous les besoins de la société. Par les différentes fonctionnalités qu’elles offrent. Une des particularités captivantes d’Eyesofnetwork est sa modularité, on a ainsi estimé

Qu’Eyesofnetwork a été plus adapté aux besoins de mon projet que FAN. En effet, grâce à ses plugins, Eyesofnetwork possède une architecture facilement adaptable à l’environnement. Ces derniers pouvant être ajoutés, modifiés ou même personnalisés et permettent de spécifier les tâches pour aboutir au résultat voulu. De plus Eyesofnetwork est une solution stable, dispose d’une grande communauté de développeurs et est utilisé aussi bien dans les petites et moyennes infrastructures que dans les grands parcs informatiques et utilisé surtout par plusieurs entreprises de renommé, tels que Yahoo (100 000 serveurs), Yellow pipe Web Hosting (7000 serveurs) Bien que ce dernier soit réputé par sa configuration fastidieuse, il peut être couplé à Centreon un logiciel qui lui servira de couche applicative afin de faciliter la configuration et d’établir des interfaces plus ergonomiques et compréhensibles.

**2.5.1 Présentation de l’outil de supervision Eyesofnetwork**

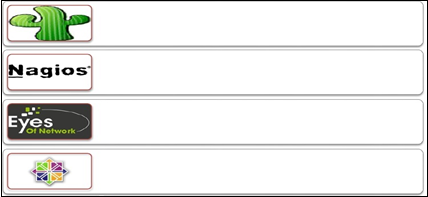
Eyes of Network est une distribution Linux basée sur CentOS et qui est chargée de rassembler tous les outils de supervision réseaux en intégrant les processus ITIL. Elle est actuellement distribuée sous licence GPL.

Eyes of Network inclut les outils suivants:

• Supervision réseau : NAGIOS + NAGIOSBP + NAGVIS.

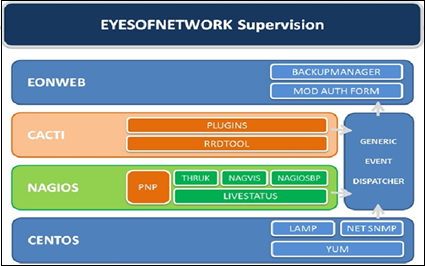
• Gestion des performances : CACTI + WEATHERMAP.

• Interface de configuration : Interface web d’EON + Utilitaire de sauvegarde.



*Figure 7.2 : Les outils constituents Eyes Of Network*

**2.5.1.1 Architecture**



*Figure 8.2: Architecture d’ Eyes Of Network*

Est accessible via une interface Web unique dont l’objectif est de réunir les différents acteurs d’un système d’informations (DSI, Administrateurs, Techniciens, Opérateurs, …).

Chacun de ces acteurs dispose d’une vue correspondant à son métier. Toutes les informations sont consolidées en Base de Données MYSQL.

**2.5.1.2 Programmes-plugins**

Eyes of Network fonctionne grâce à des plugins. Sans eux, il est totalement incapable de superviser et se résumé en un simple noyau. Ces plugins sont des programmes externes au serveur, des exécutables qui peuvent se lancer en ligne de commande afin de tester une station ou service. Ils fonctionnent sous le principe d’envoi de requêtes vers les hôtes ou services choisis lors d’un appel du processus de Eyes of Network, et la transmission du code de retour au serveur principale qui par la suite se charge d’interpréter les résultats et déterminer l’état de l’entité réseau testée.

La relation entre le noyau et les plugins est assurée d’une part par les fichiers de configuration (définitions des commandes) et d’autre part par le code retour d’un plugin.

**2.5.1.3 Les fichiers de configuration**

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

* **Eyes of network.cfg** est le fichier de configuration principal d’Eyes of network. Il contient la liste des autres fichiers de configuration et comprend l'ensemble des directives globales de fonctionnement.
* **Hosts.cfg** définit les différents hôtes du réseau à superviser. A chaque hôte est associé son nom, son adresse IP, le test à effectuer par défaut pour caractériser l'état de l'hôte, etc.
* **Contacts.cfg** déclare les contacts à prévenir en cas d'incident et définit les paramètres des alertes (fréquences des notifications, moyens pour contacter ces personnes, plages horaires d'envoi des alertes...).

**2.6 Conclusion**

Le présent chapitre a été introduit avec une brève présentation de la notion de supervision et ses enjeux. Ensuite on a écrit l’aspect de notre a solution, énuméré ses fonctionnalités et modélisé son architecture. Finalement une partie a été consacrée pour la définition des différents fichiers de configuration générés par l a solution de supervision Eyes of network, précédée par l’énumération des différents plugins de base responsable de l’exécution des tests nécessaires.

***Chapitre 3***

***Les compléments d’Eyes***

***Of Network***

* 1. **Introduction**

Dans ce chapitre on présente tous outils ou compléments que l**’**envisage ajouter à Eyes Of Network afin de mettre en valeur les fonctionnalités qu**’**elle offre optimiser, enrichir et garantir la mise en place d**’**une solution complète, facile à administrer et qui répond aux besoins déjà fixés.

* 1. **Nagios**
     1. **Présentation**

Nagios est un programme libre sous licence GPL qui fonctionne sur linux et qui permet de surveiller le système et le réseau.

Il peut surveiller des hôtes, des services et des actifs réseaux. Son rôle est d’alerter quand un élément supervisé à un problème, c’est un programme modulaire qui se décompose en trois parties :

* Le moteur de l'application qui vient ordonnancer les tâches de supervision.
* L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies.
  + 1. **Architecture**

L’architecture du système ce compose de 5 éléments :

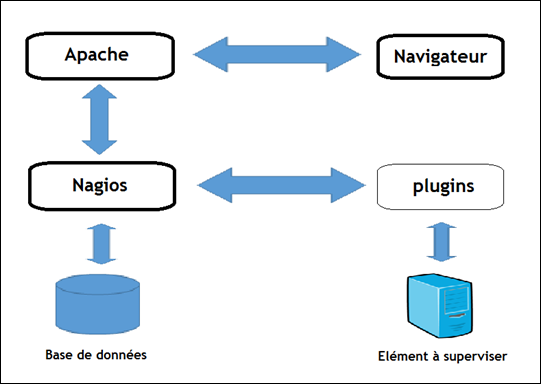
1 - Le serveur Nagios qui récupère les informations des plugins et qui opère en conséquence.

2 -Une base de données qui stocke ces informations.

3 -Des plugins que l’on va choisir en fonction de nos besoins et qui permettent d’obtenir des valeurs sur les éléments supervisés.

4 -Les éléments supervisés qui fournissent les informations.

5 -Une interface web qui permet de gérer le tout.

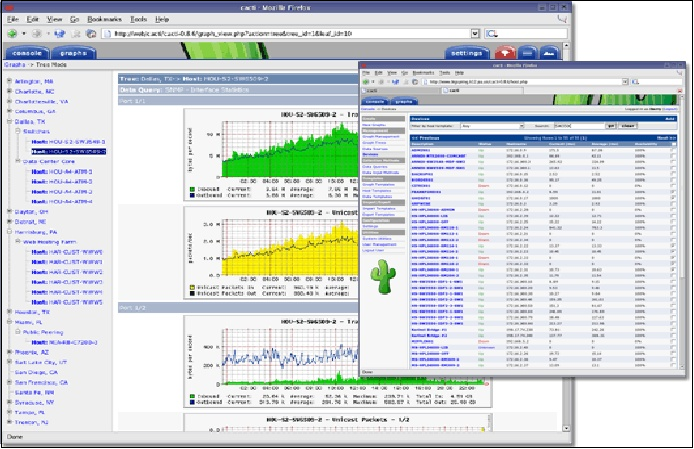
****

*Figure 1.3: Architecture de l’outil Nagios*

* 1. **CACTI**

**3.3.1 Présentation**

Classiquement, Cacti peut créer des graphiques de bandes passantes réseaux avec SNMP, mais en fait, un nombre impressionnant de graphiques peuvent être conçu avec SNMP, des scripts perl ou des scripts Shell. Dans la section des captures d'écran, vous pouvez avoir un aperçu de ce qui peut être fait avec Cacti, La force de Cacti provient du fait qu'il peut être installé et utilisé de manière extrêmement facile. Il n'est pas nécessaire d'être un guru ou de passer des heures et des heures sur l’outil pour le configurer, même un débutant peut l'utiliser très rapidement. Sur le très actif forum de Cacti, il est possible de partager ses modèles(Template) avec d'autres utilisateurs et ainsi de vous faire gagner du temps. Il est également possible d'ajouter des "plugins" à Cacti pour pouvoir intégrer d'autres outils comme ntop ou weathermap.



*Figure 2.3: fonctionnalité Cacti*

* 1. **Nagvis**

Parmi les outils permettant d’agréger les données de supervision de Nagios pour obtenir des écrans de supervision, il en est un qui se détache nettement en termes de fonctionnalités et de stabilité : NagVis. Écrit en PHP, il utilise beaucoup de Javascript afin de donner vie aux pages.

La création des cartes se fait directement depuis son interface web. Cette étape est intuitive. Les fonctionnalités Javascript font que la définition d’un élément et son placement sont faciles.

**3.4.1 Disposition des indicateurs sur une carte de supervision**

**NagVis** propose aux administrateurs de créer leur propre carte de supervision. Celle-ci est un simple fond au format PNG sur lequel ils placent différents indicateurs. Il est possible de choisir ceux-ci dans la liste suivante :

* Hôte
* Service
* Groupe d’hôte
* Groupe de service
* Carte

Si les premiers éléments sont clairement définis, le dernier nécessite quelques explications.

Il permet d’obtenir une hiérarchie entre les cartes. Un état est associé à chaque carte, correspondant à l’état le plus grave des éléments qu’elle contient. Si une carte contient un hôte qui est en état DOWN, alors elle est en état critique.

Les informations peuvent ainsi être remontées aux niveaux supérieurs. Si les niveaux les plus élevés sont verts, c’est que tous les indicateurs définis en-dessous le sont également.

* 1. **Choix des images par l’administrateur Images des éléments supervisés**

En plus de permettre le choix des fonds de carte, NagVis propose aux administrateurs de choisir les images représentant les différents éléments supervisés. Une collection est disponible en standard. Elle est composée d’images au format PNG représentant des croix rouges, oranges ou vertes. Une collection a un nom (NOM) et les images qui la composent doivent être nommées en respectant la forme suivante :

NOM\_ack.png : un problème sur un hôte ayant été pris en compte par un administrateur NOM\_error.png : l’information n’est pas disponible

NOM\_unknown.png : l’état est UNKNOWN

NOM\_critical.png : le service est en état CRITICAL

NOM\_ok.png : le service est en état OK

NOM\_up.png : l’hôte est en état UP

NOM\_down.png : l’hôte est en état DOWN

NOM\_sack.png : un problème sur un service ayant été pris en compte par un administrateur.

NOM\_warning.png : le service est en état WARNING.

Ces images doivent être situées dans le répertoire : /usr/local/nagios/share/nagvis/images/iconsets.

Les administrateurs peuvent définir, sur chaque carte, une collection à utiliser  par défaut. Si un ou plusieurs éléments doivent utiliser une autre collection, il est possible de le spécifier. Les administrateurs peuvent ainsi créer des images de différentes tailles ou plus représentatives des éléments que les simples croix fournies par défaut.

* 1. **Conclusion**

Le but de ce chapitre était de présenter les compléments que nous avons choisis à Eyes Of Network.

***Chapitre 4***

***Réalisation Et Tests***

* 1. **Introduction**

Au sein de ce dernier chapitre, je vais présenter le chronogramme de réalisation de mon projet, de l’environnement de travail et enfin quelques captures écrans des interfaces de EyesOfNetwork.

* 1. **Environnements de mise en place**

**4.2.1 Environnement matériels**

* **Phase de test** : Nous allons au cours de cette phase installé une machine virtuelle (VMware Workstation) sur ma machine personnelle pour tester la solution choisie et s’adapter à sa mise en place, mais aussi de S’assurer si elle répond vraiment aux besoins fixés par la société avant de passer à la phase de production, et ce en essayant de tester des serveurs distants.
* **Phase de production** : Une dizaine de serveurs Windows et Linux à superviser. Nous allons installer un serveur.

Linux (hardware et system exploitation) pour y déployer Eyes Of Network qui a les caractéristiques suivantes :

* Système Linux entreprise (Centos 6.3).
* Microprocesseur Intel® Pentium® 2.53 Ghz Mémoire installé (RAM) 2Go.
* Connexion internet.
  + - 1. **Système Linux entreprise (Centos 6.3)**

CentOS (Community enterprise Operating System) est une [distribution](http://fr.wikipedia.org/wiki/Distribution_Linux) [GNU/Linux](http://fr.wikipedia.org/wiki/GNU/Linux) principalement destinée aux serveurs. Tous ses paquets, à l'exception du logo, sont des paquets compilés à partir des sources de la distribution RHEL ([Red Hat Enterprise Linux](http://fr.wikipedia.org/wiki/Red_Hat_Enterprise_Linux)), éditée par la société [Red Hat](http://fr.wikipedia.org/wiki/Red_Hat). Elle est donc quasiment identique à celle-ci et se veut 100 % compatible d'un point de vue binaire.

* + 1. **Environnement logiciels**
* VMware Workstation
* La solution de supervision Eyes Of Network -3.1 -86\_64 bin.
* GNS3
  + - 1. **VMware Workstation**

C'est la version [station de travail](http://fr.wikipedia.org/wiki/Station_de_travail) du logiciel. Il permet la création d'une ou plusieurs [machines virtuelles](http://fr.wikipedia.org/wiki/Machine_virtuelle) au sein d'un même [système d'exploitation](http://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation) (généralement [Windows](http://fr.wikipedia.org/wiki/Microsoft_Windows) ou [Linux](http://fr.wikipedia.org/wiki/Linux)), ceux-ci pouvant être reliés au [réseau local](http://fr.wikipedia.org/wiki/R%C3%A9seau_local) avec une [adresse IP](http://fr.wikipedia.org/wiki/Adresse_IP) différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte.

**4.2.2.2 La solution de supervision Eyes Of Network**

[Eyes Of Network](http://www.eyesofnetwork.com/?lang=fr)« EON » est une solution complète de supervision, basée sur la distribution GNU/Linux CentOS.

* + - 1. **GNS3**

GNS3 (Graphical Network Simulator) est un [logiciel libre](http://fr.wikipedia.org/wiki/Logiciel_libre) permettant l'émulation ou la simulation des réseaux informatiques.

* 1. **Mise en place d’Eyes of network**
     1. **Installation d’Eyes of network**

Il faut tout d’abord télécharger l’image iso dvd de EON, disponible à l’adresse suivante pour :

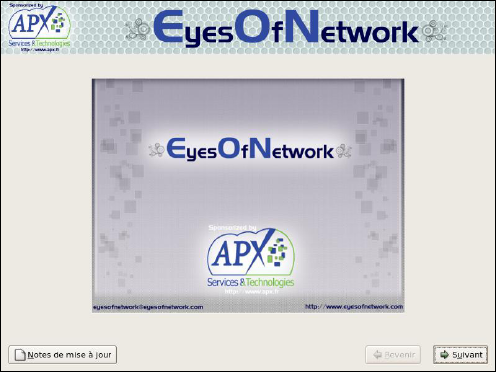
La version 32 bits :<http://download.eyesofnetwork.com/EyesOfNetwork-3.0-i386-bin.iso>.

La version 64 bits :<http://download.eyesofnetwork.com/EyesOfNetwork-3.0-x86_64-bin.iso>.

Une fois l’image téléchargée et gravée, nous pouvons commencer l’installation.

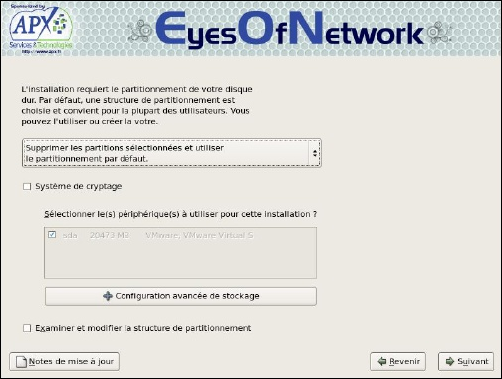
**4.3.1.1 Installation**

Nous allons démarrer sur le DVD, et appuyer sur entrée à l’écran de boot ensuite nous allons choisir la langue du système et le type de clavier et enfin Anaconda, l’interface graphique d’installation, démarrage.



*Figure 1.4: l’interface graphique d’installation EON*

Ensuite nous allons choisir comment partitionner le disque, pour un débutant, il est préférable de laisser le partitionnement par défaut.

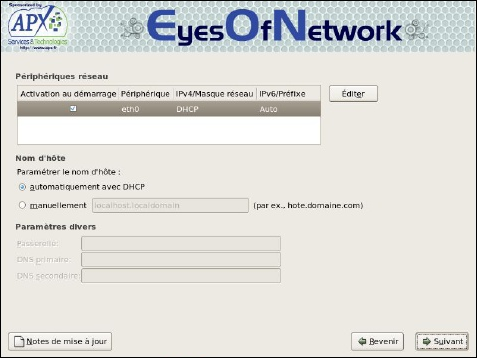


*Figure 2.4: Partitionnement du disque*

Le partitionnement terminé, nous allons passer au paramétrage réseau. Ici dans EDITER : on choisit notre paramétrage IP, il sera toujours possible de le paramétrer post Install avec la commande :

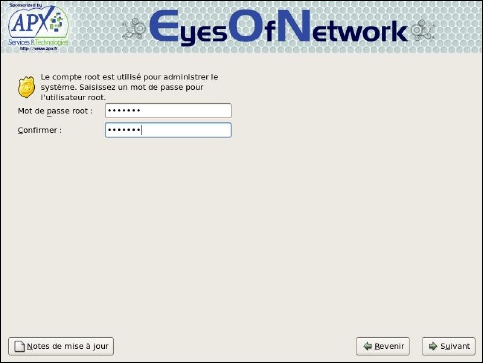
[**root@EON ~]# system-config-network**

Dans le nom d’hôte on va rentrer le nom du serveur comme ceci : nom\_du\_serveur.nom\_du\_domaine Enfin dans paramétrages divers, on rentre la passerelle et les DNS.



*Figure 3.4: paramétrages divers*

Après cette étape, on va choisir notre mot de passe root du serveur.



*Figure 4.4: mot de passe root du serveur*

Maintenant nous allons choisir les paquets à installer. Ces paquets sont rangés en deux catégorie : la catégorie Supervision et la catégorie Production. Voyons ce que contiennent ces catégories plus en détail.

**Supervision :**

**-BASE :** installe le serveur EON.

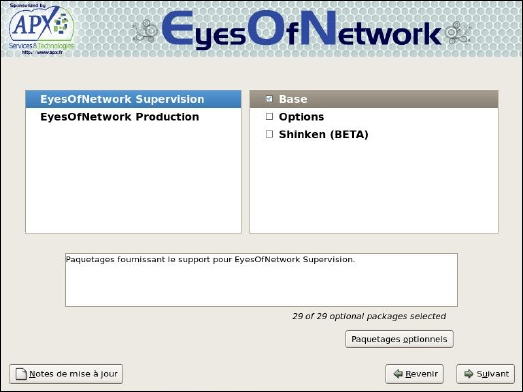
-**OPTIONS :** contient les agents les plus utilisés par la communauté.

-**SHINKEN** (BETA) : installe Shinken en plus de Nagios.

**Production :**

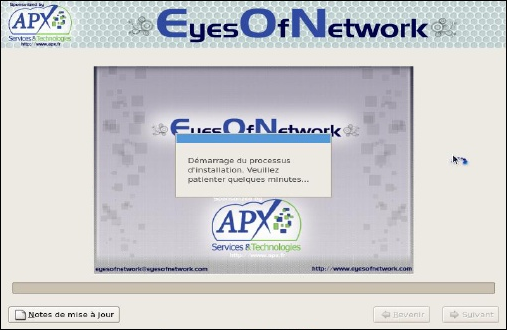
-**GESTION DES INCIDENTS :** installe **GLPI**.

**INVENTAIRE:** installe FUSION et OCS inventory (inventaire de parc et déploiement de logiciel àdistance).



*Figure 5.4: choix des paquets*

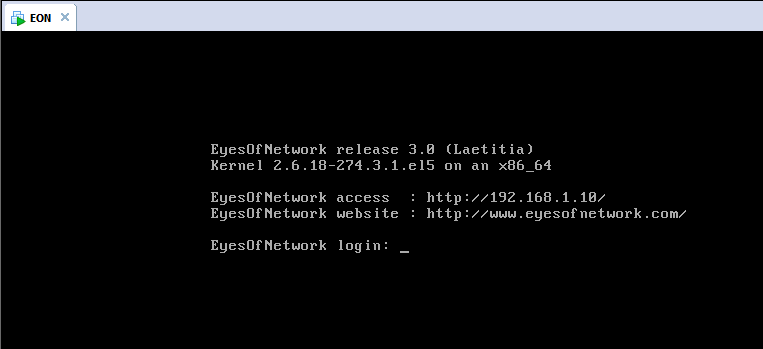
Une fois les paquets choisis, EON s’installe pour une durée approximative de 20 minutes (paramétrage réseau Compris).



*Figure 6.4: démarrage du processus d’installation d’EON*

A la fin de l’installation et lorsque on lance la solution (EON) Il affiche une adresse DHCP

Comme suit :



*Figure 7.4: démarrage du d’EON*

Ici, On va configurer configuré l’interface réseau de notre serveur ce qui nous permet de connecté à ce lui sans adresse DHCP.

Nous allons donc Configuré le fichier ifcfg-eth0.

Taper la commande **vi /etc/sysconfig/network-scripts/ifcfg-eth0** pour acceder aufichier ifcfg-eth0.et taper les paramètres suivants :

**DEVICE=eth0               ## Nom de l'interface**

**BOOTPROTO=static          ## Passer en mode static et non DHCP**

**BROADCAST=192.168.0.255   ## Adresse de broadcast**

**HWADDR=AA:BB:CC:DD:EE:FF  ## MAC ADRESSE de la carte reseau**

**IPADDR=192.168.0.10       ## Adresse IP de la machine**

**NETMASK=255.255.255.0     ## Masque sous-reseau**

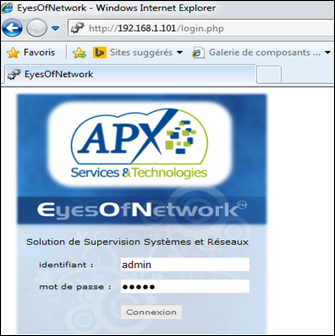
**NETWORK=192.168.0.0       ## Adresse reseau**

**ONBOOT=yes                ## Monter l'interface au boot**

**NM\_CONTROLLED="no"﻿        ## Pas de contrôl via NetworkManager**

* + - 1. **Interfaces de Eyes Of Network**

La première étape à faire avant d’accéder à l’interface d’Eyes of Network c’est d’ouvrir un navigateur web et écrire dans la barre de navigation « http://Addresse du serveur »Une page d’authentification s’affiche demandant le nom de l’utilisateur ainsi que le mot de passe comme l’indique :



*Figure 8.4: fenêtre d’authentification*



*Figure 9.4: interface graphique d’EyesOfNetwork*

**4.4 Installation du protocole SNMP**

**4.4.1 Installation et paramétrage du SNMP sous linux**

Pour installer un manager SNMP, nous pouvons utiliser Net-SNMP. L'application Net-SNMP est un ensemble de programmes console permettant de tout faire avec le protocole SNMP. L'avantage d'utiliser des programmes console est que vous pouvez facilement écrire des petits scripts de vérification que vous pourrez intégrer dans **Nagios**.

Nous allons donc installer les paquets SNMP: **Snmp** et **snmpd**

Sous un système CentOS**:** ouvrir une console et taper la commande :

**yum -y install net-snmp**

Ensuite nous allons éditer le fichier snmpd.conf avec la commande :

**vi /etc/snmp/snmpd.conf**

Et rentrer les paramètres suivant:

**com2sec notConfigUser default EyesOfNetwork**

Ici on autorise en lecture et écriture la communauté EyesOfNetwork

Valider les changements (ctrl+x, o, entrer).

Nous allons aussi éditer le fichier /etc/default/snmpd.

**iv /etc/default/snmpd**

Chercher la ligne, et remplacez 127.0.0.1 par l'adresse IP de l'interface réseau utilisée pour communiquer avec le serveur de supervision (généralement l’IP de notre machine).

**SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1'**

Redémarrer le service SNMP :

**iv /etc/init.d/snmpd restart**

Pour tester SNMP sur le serveur linux, on rentre la commande :

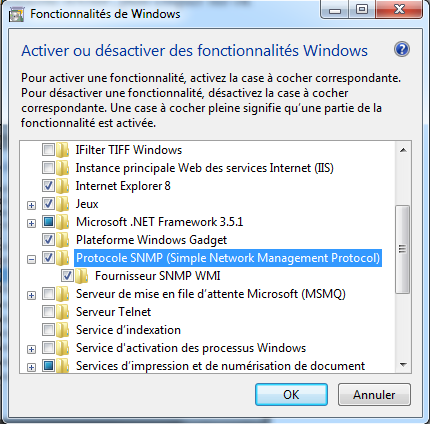
**snmpwalk -v 2c -c EyesOfNetwork localhost**

Pour tester que cela fonctionne du serveur de supervision, on rentre la commande :

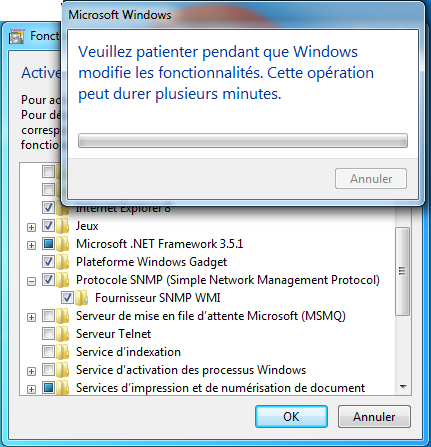
**snmpwalk -v 2c -c EyesOfNetwork ip\_du\_poste\_supervisé**

**4.4.2 Installation et paramétrage du SNMP sous Windows**

Aller dans le **panneau de configuration**> **programmes**> **Activer ou désactiver des fonctionnalités Windows** Cocher ensuite la case correspondant au Protocole SNMP, puis cliquer sur ok.

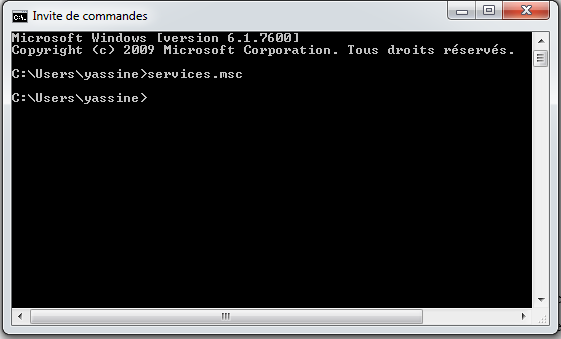


*Figure 10.4: Activation du Protocole SNMP*

****

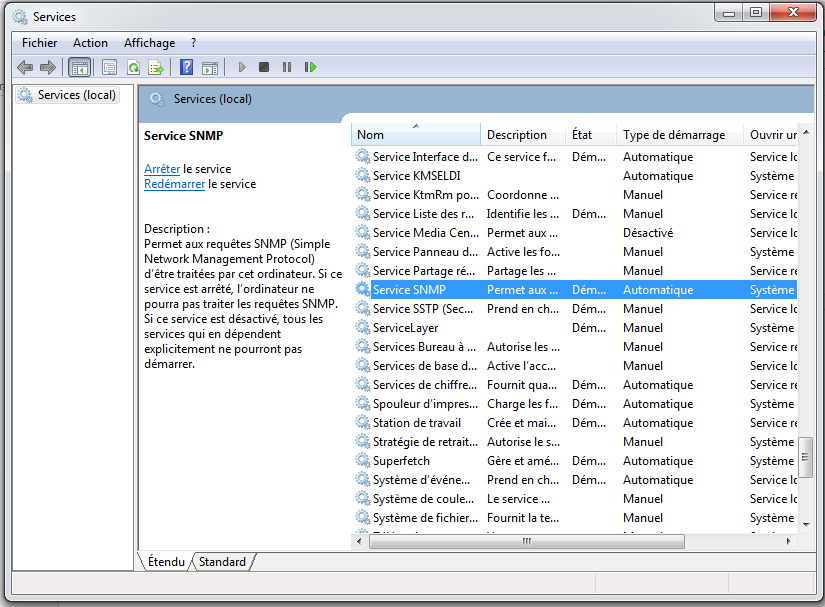
*Figure 11.4: Windows modifie les fonctionnalités*

En suite Ouvrir le panneau des services en lançant la commande services.msc.



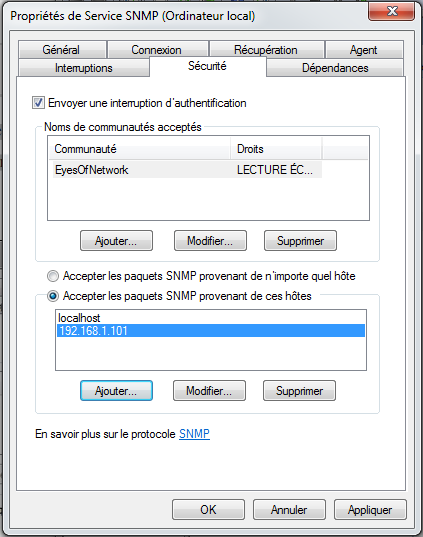
*Figure 12.4: invite des commandes*

Cette fenêtre ouverte, chercher le service SNMP et faire un clic droit/propriété pour accéder à la configuration.



*Figure 13.4: panneau des services*

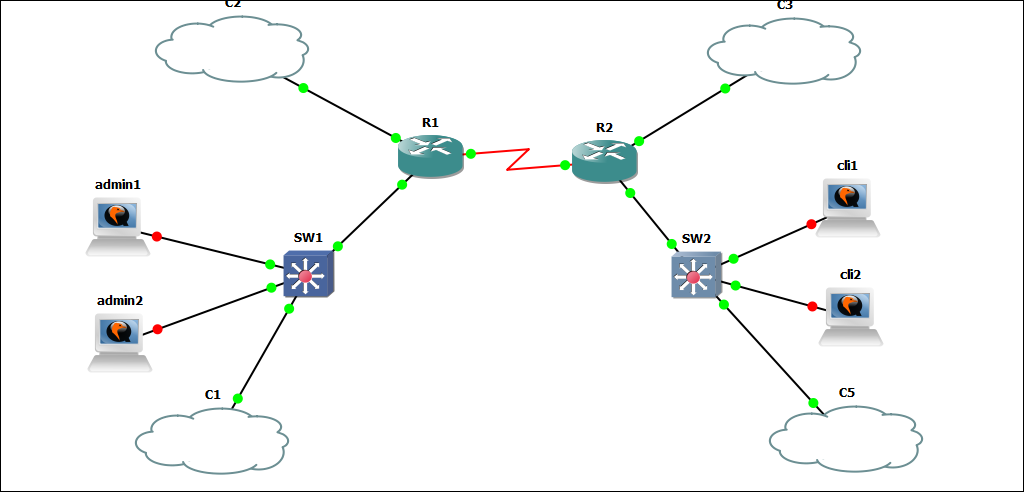
Aller dans l’onglet sécurité, ici l’on va renseigner la communauté que possède notre serveur de supervision et lui accorder les droits en lecture et écriture. Nous allons aussi renseigner l’IP de notre serveur de supervision ici, 192.168.1.10.



*Figure 14.4: propriétés de service SNMP*

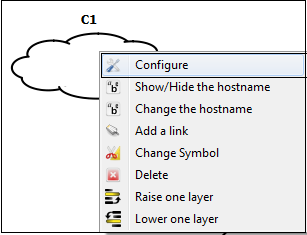
* + 1. **Architecture réseaux sous GNS3**

La première étape à faire est d’ouvrir le logiciel GNS3 avec l’option exécuter tan ’que administrateur. Ensuite On va faire une architecture réseaux composé de 4 machines, 2 switches et 2 routeurs Tous connecté a des Cloud. Comme suit :



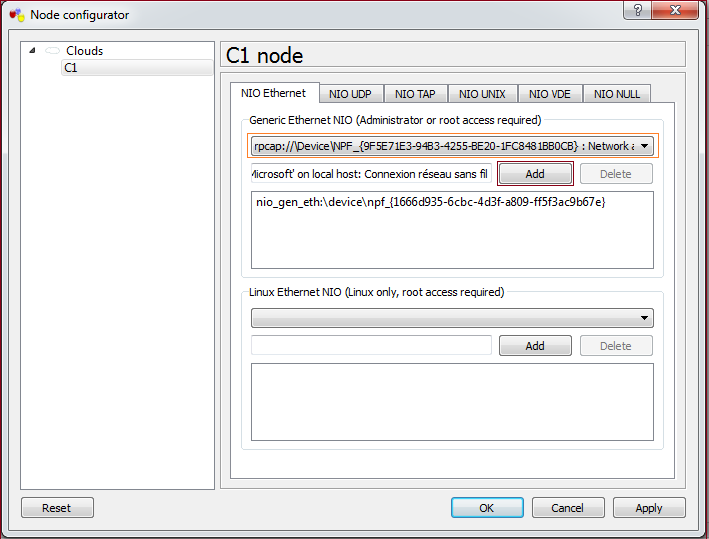
*Figure 15.4:**Architecture réseaux*

Dans GNS3 faire glisser et déposer un routeur à partir du menu de gauche, puis un nuage, travers lequel gns3 sera connecté à un hôte VMware Workstation ensuite Bouton droit sur le nuage et sélectionner Configure.



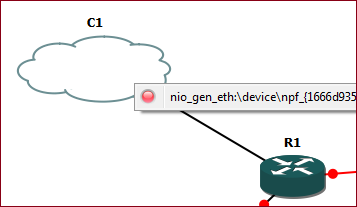
*Figure 16.4:**configuration de nuage 1*

Depuis l’Onglet NIO Ethernet choisissez la carte réseau qui est précédemment attribué à l’hôte dans VMware Workstation et cliquer sur Ad.



*Figure 17.4:**configuration de nuage 2*

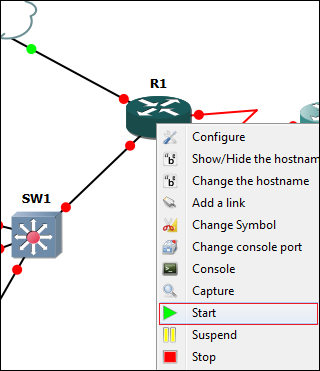
Enfin interconnecter l'interface du routeur (par exemple Fa0 / 0) avec le nuage:



*Figure 18.4:**interconnecter l'interface du routeur avec le nuage*

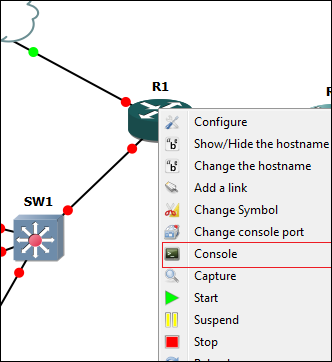
Maintenant on va configurer les équipements un par un, on commence par le routeur 1.

Bouton droit sur l’équipement à configurer et on clique sur Start.

****

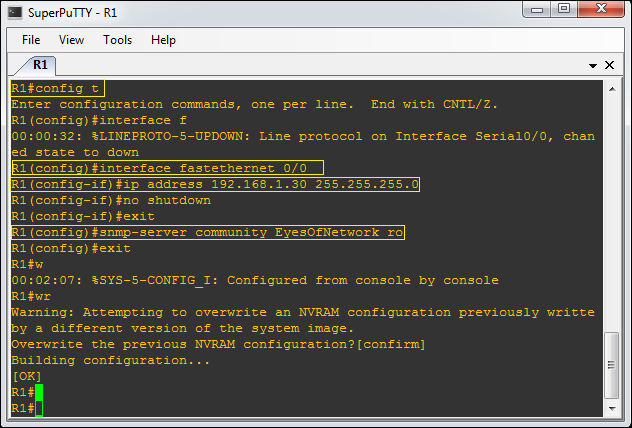
*Figure 19.4: Start routeur 1*

Puis sur console ou on tape les commandes de configuration.



*Figure 20.4: console*

Ici, on ajoute une adresse IP pour le router 1 et paramétrer Le SNMP de lui comme suit :



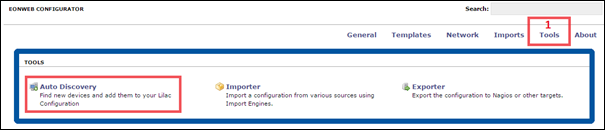
*Figure 21.4: configuration du routeur 1*

* 1. **Interface de configuration : Interface web d’EON**

**4.5.1 Scan du réseau**

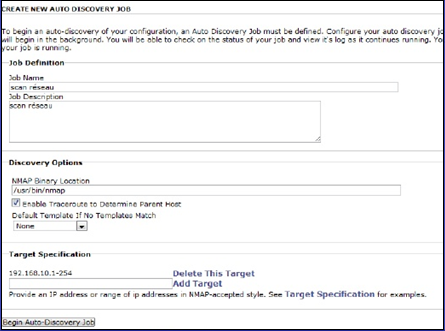
Pour pouvoir scanner le réseau, il faut connecter sur l’interface web d’EON.

Dans **ENOWEB CONFIGIRATOR,** cliquez sur «**Tools**» puis «**Auto Discovery**»



*Figure 22.4 : Auto-discovery*

Ensuite dans la fenêtre suivante nous allons remplir les champs suivant :



*Figure 23.4: Paramétrage Auto-discovery*

**Job Name** : nom du travail

**Job description** : description du travail

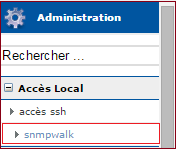
**Nmap binary location** : emplacement de l’exécutable Nmap (laisser par défaut)

**Target spécification** : adresse que l’on souhaite superviser, exemple : 192.168.10.x/32 ou 192.168.10.x-x/32Cliquez ensuite sur « add target » puis sur « Begin auto-discovery job ».

Le processus démarre, il faut maintenant attendre la fin du processus pour pouvoir exporter les hôtes dans Nagios.

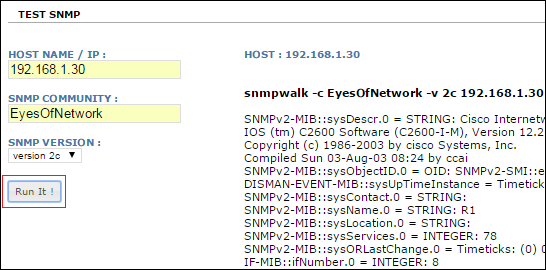
**4.5.2 superviser des hôtes**

On a besoin de vérifier la détection de Eyes Of Network à l’équipement routeur 1 , il faut connecter sur l’interface web d’EON et clique sur l’onglet administration puis à gauche sur Snmpwalk.



*Figure 24.4 : configuration du routeur 1*

Ici, taper l’adresse IP de l’équipement dans le champ **HOST NAME / IP** et le nom de la communité (Eyes Of Network) dans le champ **SNMP COMMUNITY**et enfin sur run.



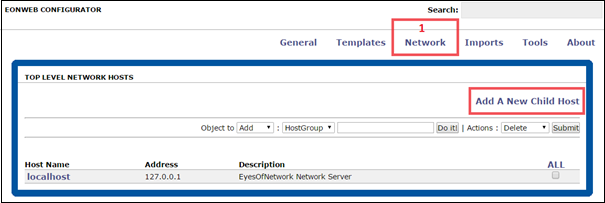
*Figure 25.4 : test SNMP*

Maintenant dans l’onglet Nagios on clique sur configuration.



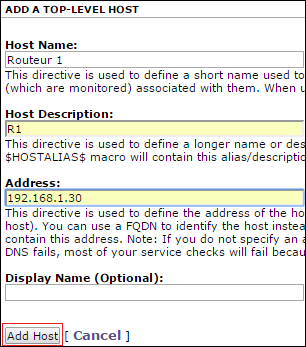
*Figure 26.4: test SNMP*

Dans **ENOWEB CONFIGIRATOR,** cliquez sur **«Network »** puis **«add a new child host»**.

****

*Figure 27.4:superviser une Hôte*

Remplissez ensuite les champs suivants :

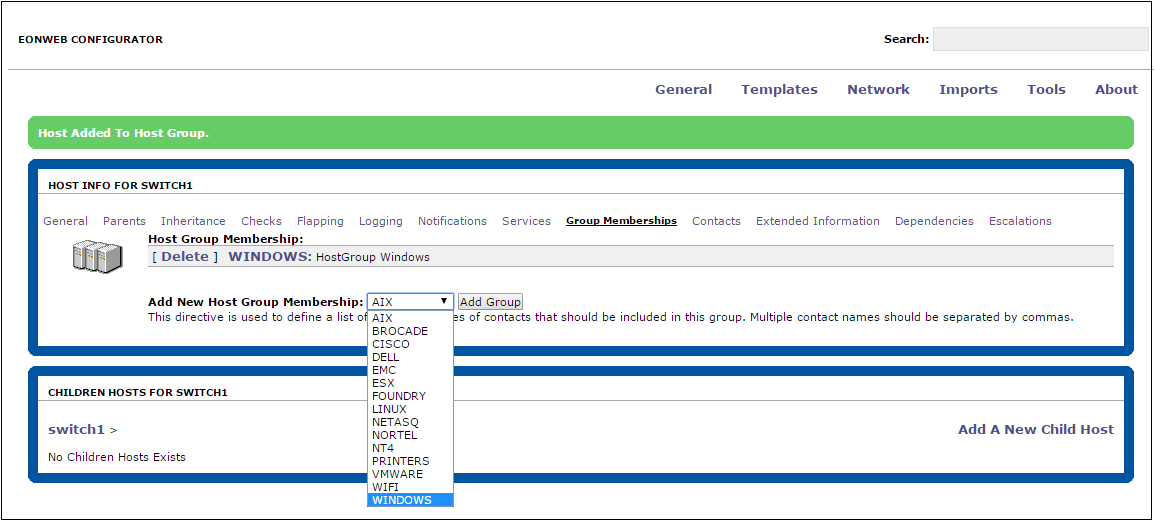


*Figure 28.4: Ajout d’une hôte*

**Host Name :** Nom **de l’hôte (ne doit pas contenir d’espace)**

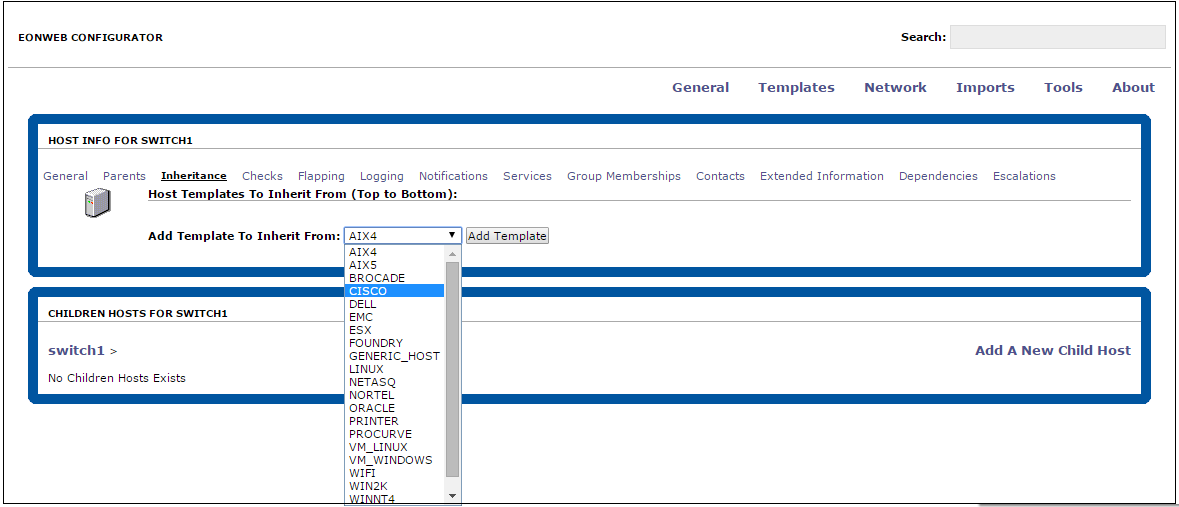
**Host Description :** Description de l’hôte**Address :** adresse ip, nom d’hôte ou adresse internet Cliquez sur **« Add host »** pour l’ajouter.

Une fois le périphérique ajouté, nous devons l’affecter à un groupe par exemple si c’est un équipement Cisco, on effectue cette action :



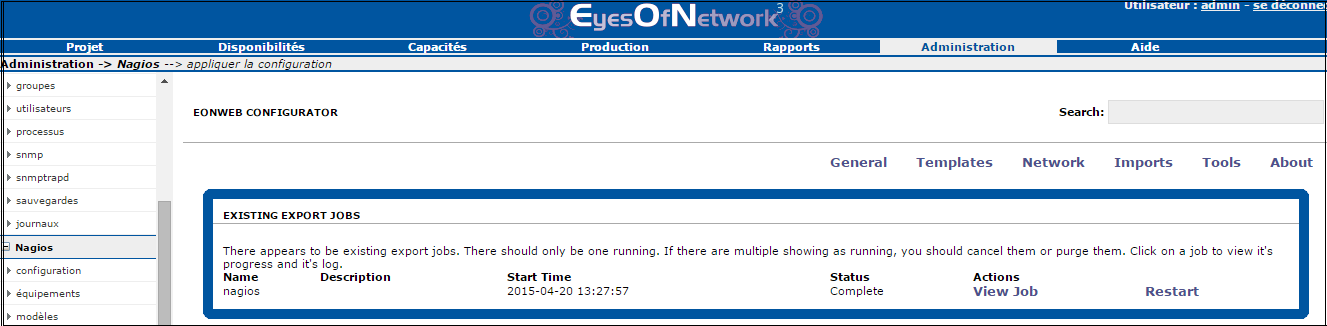
*Figure 29.4:GroupMembership*

Dans notre cas on choisit inheritance, puis Cisco et on clique sur add Template.



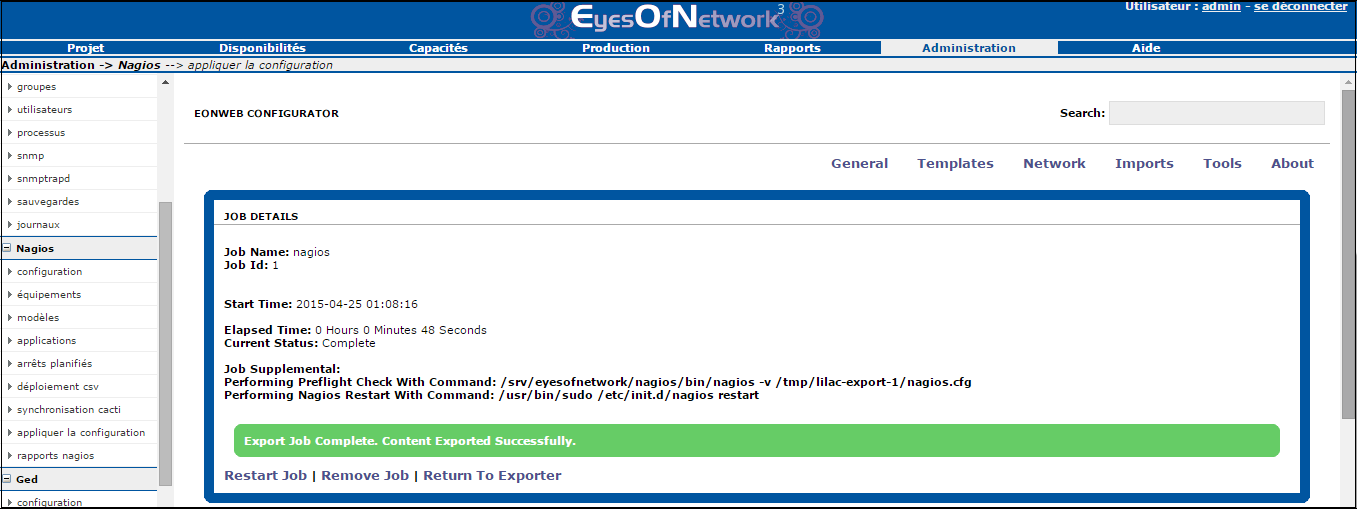
*Figure 30.4:Inheritance*

Par la suite on clique sur appliquer la configuration à gauche et on clique sur restart :



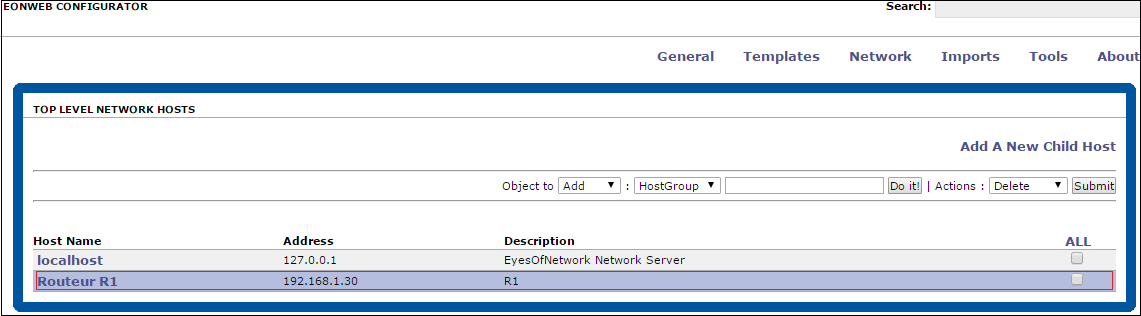
*Figure 31.4:application de la configuration*

Nous devons obtenir le résultat suivant :



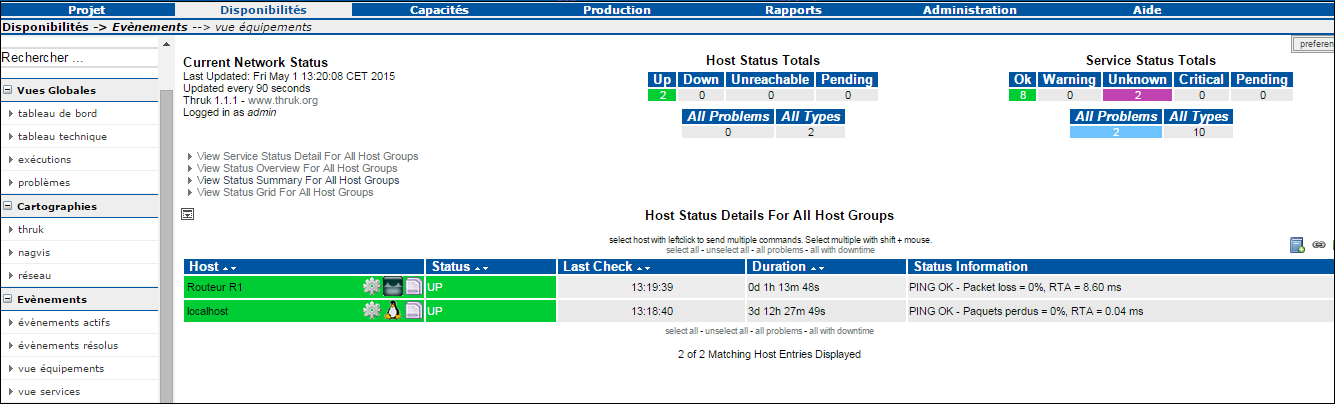
*Figure 32.4:succès de l'application de la configuration*

Par la suite on clique sur équipement dans l’onglet Nagios pour voir notre équipement (Routeur 1).



*Figure 33.4:équipement*

Et en fin on clique sur disponibilité puis sur vue d’équipement dans l’onglet Evènement pour obtenir l’état de notre équipement.



*Figure 34.4:etat d’équipement*

pour ajouter plus d’équipement Nous cliquons sur **«add A New Child Host»** , On remplit les champs hostname, host description, adresse et display Name. Ensuite on clique sur add host puis cliquez sur « Inheritance » pour choisir un template à associer à l’hôte, cliquez sur «Tools» puis sur «Exporter» Et enfin sur «Restart» pour pouvoir charger la configuration dans Nagios.

* + 1. **Superviser un serveur Windows**

Suivez les étapes précédente choisissez le Template Win2K lors du choix des Templates.

* + 1. **Superviser un serveur linux**

Suivez les étapes précédentes**,** puis choisissez le Template Linux lors du choix des Templates.

* + 1. **Superviser les actifs**

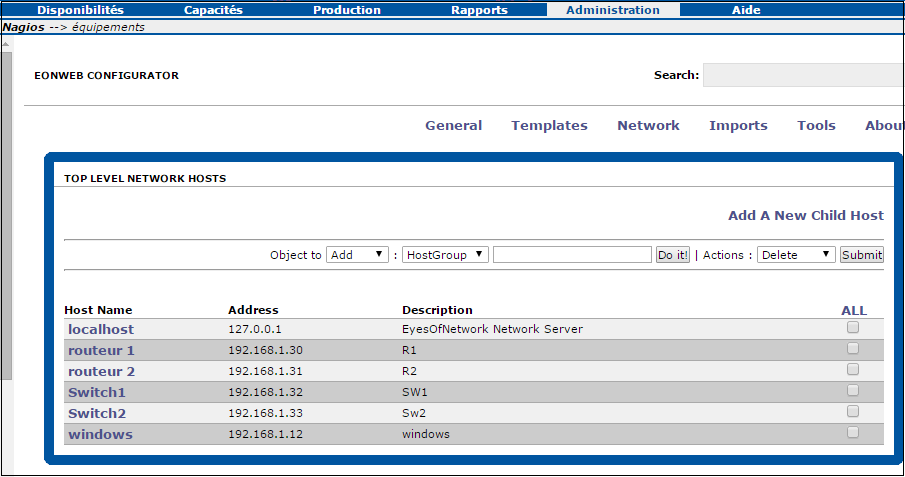
Superviser un actif :

Suivez les étapes précédentes**,** puis choisissez le Template Generic\_Host lors du choix des Templates.

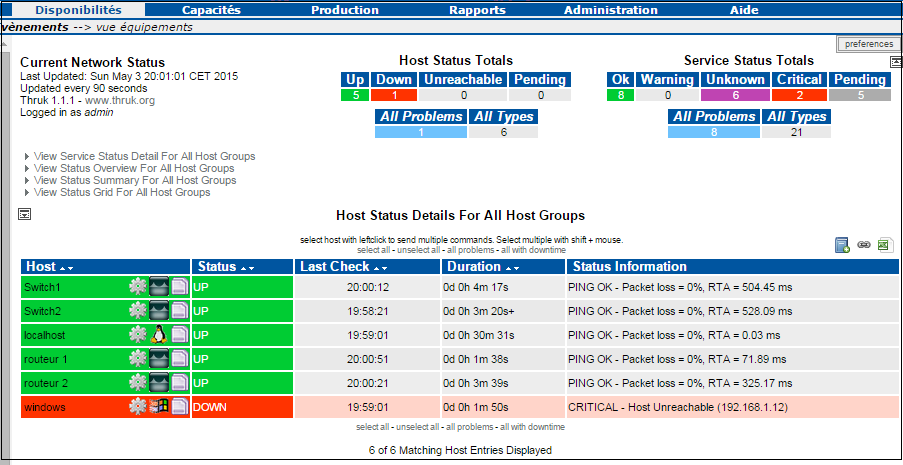
Superviser une imprimante :

Suivez les étapes précédentes, puis choisissez le Template Printer du choix des Templates.

On va répéter les étapes président avec les autres équipements pour obtenir le résultat suivant :



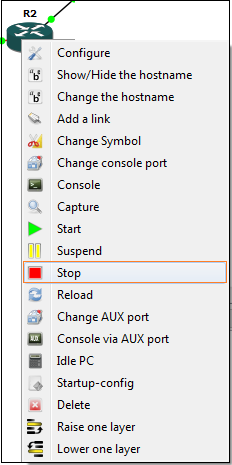
*Figure 35.4’équipements*

**

*Figure 36.4:etat d’équipements*

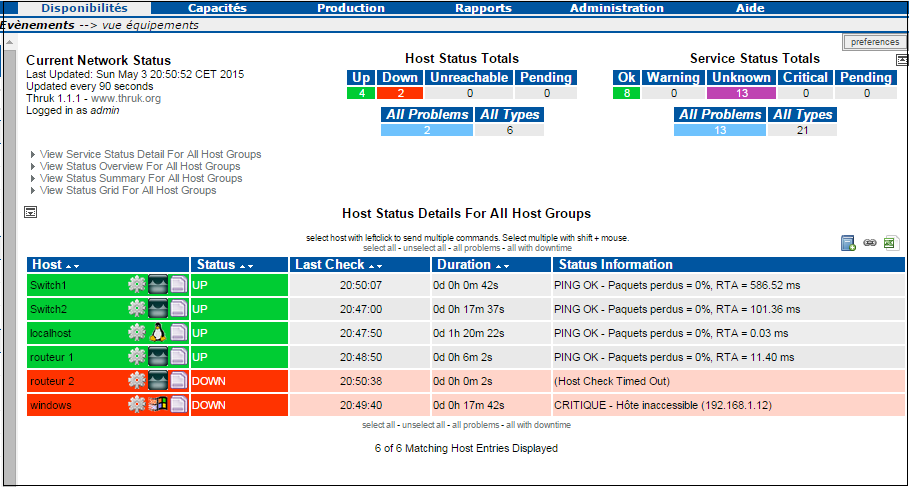
On peut tester la détection de notre solution a l’état des équipements.

Par exemple d’arrêté le routeur2 :



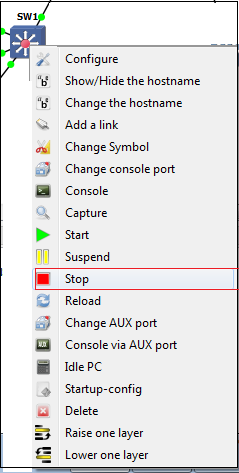
*Figure 37.4:* *arrête de routeur2*

On obtenir le résultat suivant :



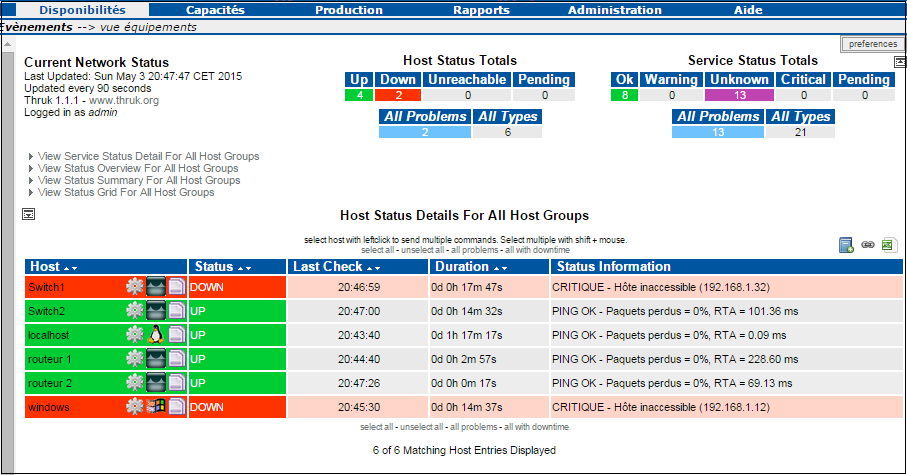
*Figure 38.4:* *douteur2 est en panne*

Ensuite on va voir le résultat avec le switch1 :



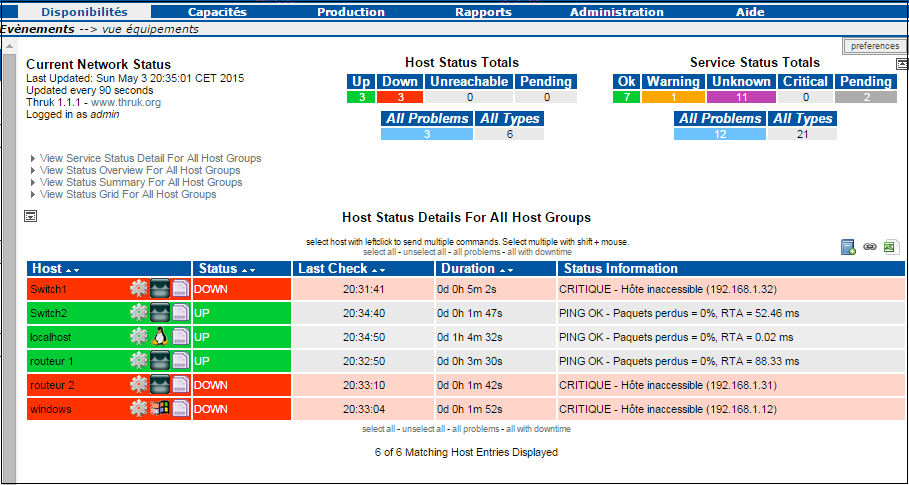
*Figure 39.4:* *arrête de switch1*

Le résultat est la suivante :



*Figure 40.4:* *switch1 est en panne*

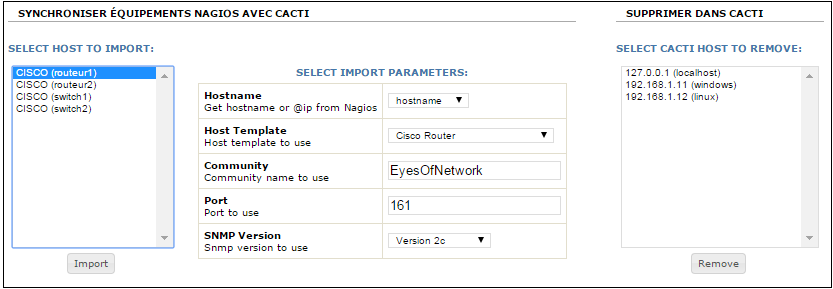
Maintenant on va arrêtée les deux équipements (routeur2 et le switch1) pour avoir le résultat.



*Figure 41.4:* *routeur2 et Switch 1 en pannes*

* 1. **synchronisation avec Cacti**

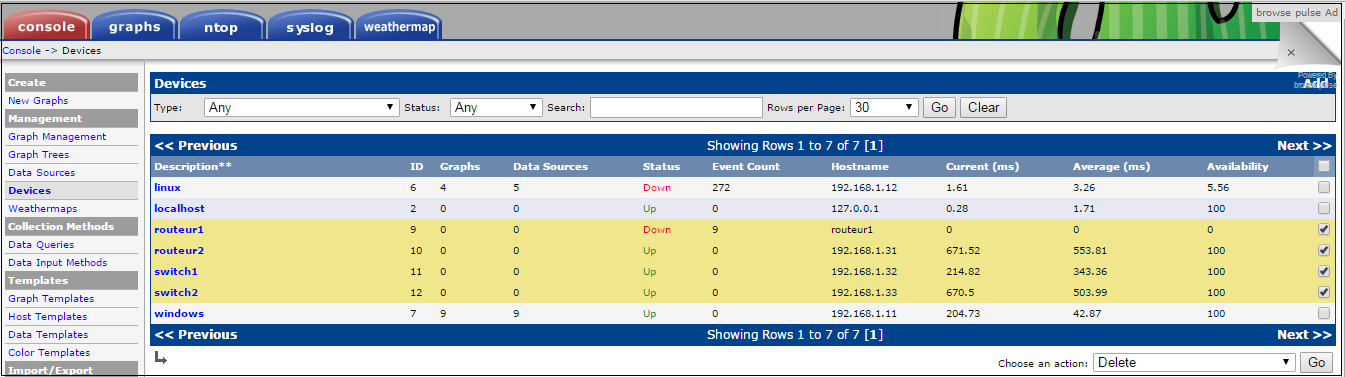
Il faut ensuite faire la synchronisation avec Cacti, en cliquant sur l’onglet synchronisation Cacti à gauche sous Nagios :



*Figure 42.4:Synchroniser Cacti avec Nagios*

On choisit l’équipement à importer, on entre la communauté dans le champ community et on clique sur import, voici le résultat dans Cacti on accède à l’interface graphique de Cacti en cliquant sur **administration>liens externes>Cacti** à gauche.

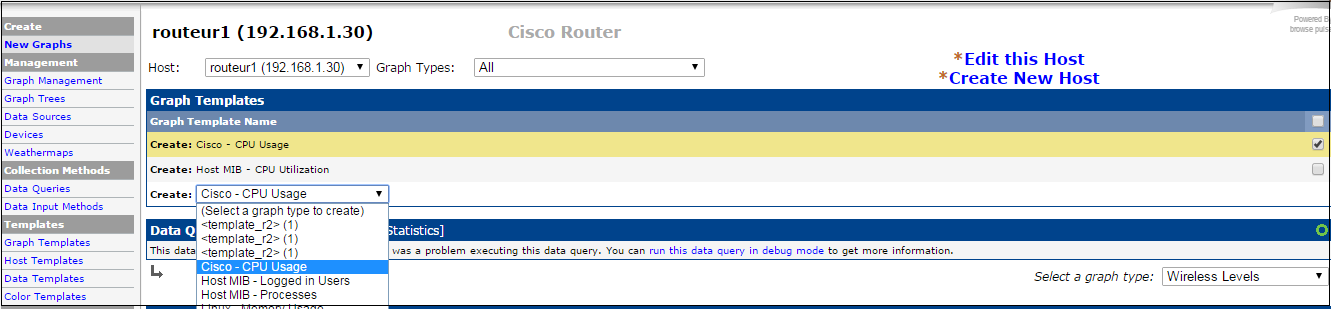
Nous cliquons sur devices pour voir les équipements :



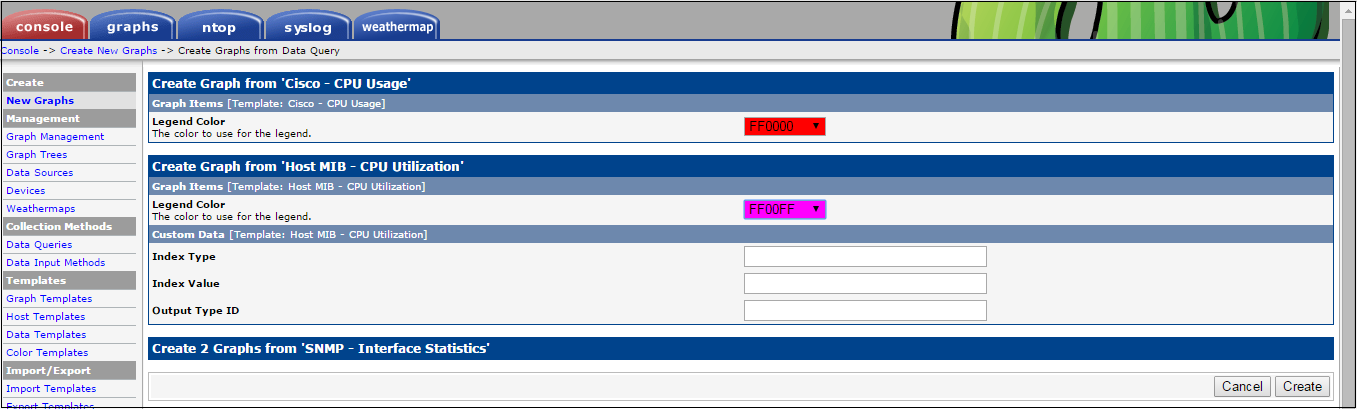
*Figure 43.4: Paramétrage Cacti*

Nous voyons bien que notre équipement myhost a été ajouté avec succès.

On peut créer un graphe en choisissant un Template generic et ajouter nous-même l’OID .correspondant au paramètre qu’on veut visualiser  voici comment faire :

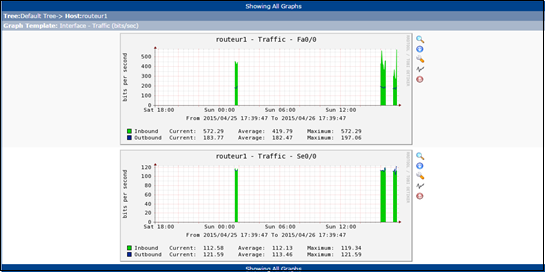


*Figure 44.4: Generic OID Template*



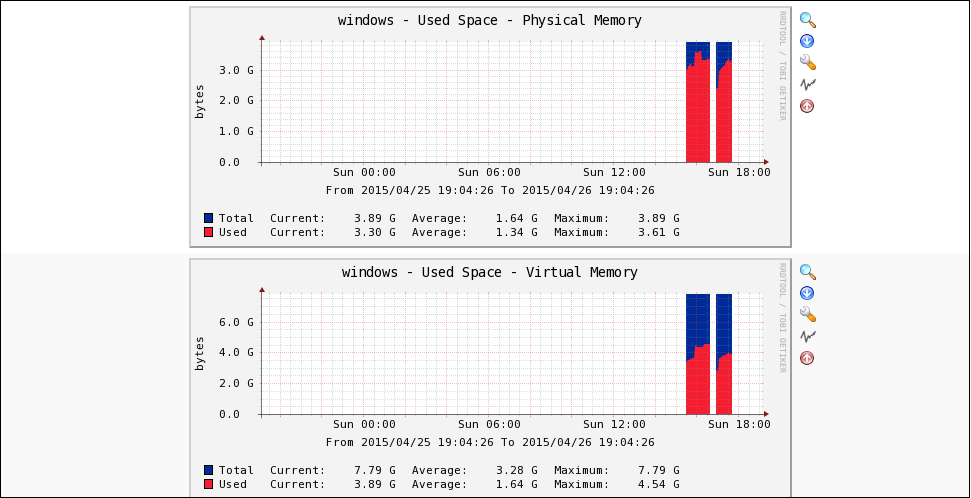
*Figure 45.4: ajout d'OID*

Voici des exemples des graphes que nous avons créés :



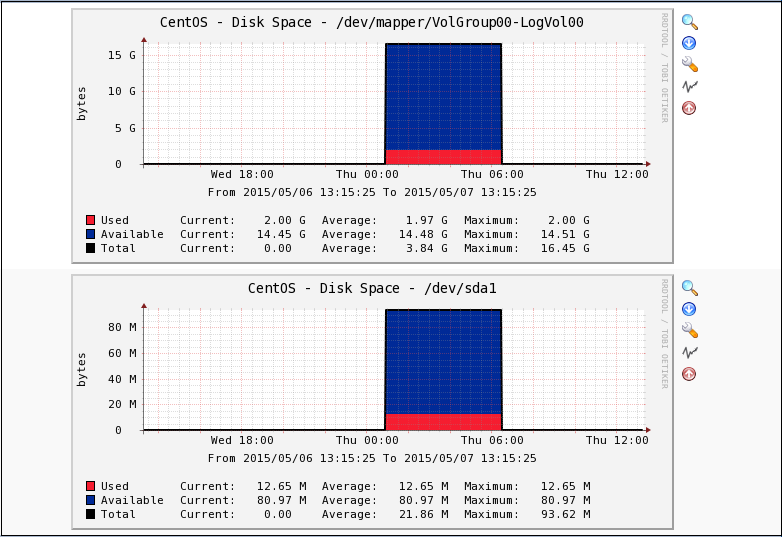
*Figure 46.4:Graphes de trafic sur les interfaces du routeur1*

Ce graphe défini les trafics sur les interfaces du routeur1 lors de sa connexion avec les autres équipements.



*Figure 47.4:Graphes d’espace mémoires utilisé sur Windows*

Ce graphe défini l’espace mémoires utilisé sur Windows de la mémoire physique et la mémoire virtuel.



*Figure 48.4:Graphes d’espace mémoires utilisé sur CentOS*

Ce graphe défini l’espace mémoires utilisé sur les partitions du CentOS.

La partie en bleu définie : l’espace mémoire libre

La partie en rouge définie : l’espace mémoire utilusé

* 1. **Exemple d’utilisations**

Les alertes remontées aux administrateurs sont au cœur même des outils de supervision. Nous allons voir comment assurer leur précision et leur pertinence. Nous avons déjà évoqué la nécessité d’impliquer au maximum dans le projet les administrateurs. Ils sont les seuls à pouvoir définir les règles de supervision de leurs environnements. L’un des objectifs du chef de projet est de leur faire accepter l’outil. Pour cela, la solution doit faciliter leur travail. Les informations doivent leur arriver déjà filtrées. Dans le cas contraire, ils perdent du temps. Le seuil de tolérance est variable suivant les administrateurs On peut considérer qu’une vingtaine d’alertes par jour est acceptable pour une grande majorité. Au-dessus, certains vont commencer à se plaindre. Cette limite est notre marge haute. Si l’on arrive à faire mieux, il ne faut pas s’en priver. Or la solution de supervision doit faire gagner du temps aux administrateurs. La concision des alertes est un premier pas dans cette direction.

**4.5.1 Paramétrage** **de Postfix**

Ouvrir le fichier main.cf qui se trouve dans l'arborescence **:**

**vi /etc/postfix/main.cf**

Ajouter les lignes suivantes

**Smtp\_sasl\_security\_options = noanonymous**

**relayhost = [smtp.gmail.com]:587**

**smtp\_use\_tls = yes**

**smtp\_tls\_CAfile = /etc/postfix/cacert.pem**

**smtp\_sasl\_auth\_enable = yes**

Enregistrer le changement au sein du fichier.

Créer/etc/postfix/sasl/passwd

Créer un repertoire sasl under /etc/postfix et créer un fichier passwd avec les paramètres suivants :

**[smtp.gmail.com]:587** [**yassine.rhimi12@gmail.com:password**](mailto:yassine.rhimi12@gmail.com:password)

Enregistrer et sortir.

Paramétrages des droits d’accès

**#chmod 600 /etc/postfix/sasl/passwd**

Création lookup table via postmap

**#postmap /etc/postfix/sasl/passwd**

Création du proper CA certificat

Change le répertoire /etc/pki/tls/certs

**#cd /etc/pki/tls/certs**

Création de la clé et test du certificat sur un seul fichier

**#make hostname.pem**

Sur l’écran s’affiche le traitement de donnée en suite faut remplir les cases vides comme suite:

umask 77 ; \

PEM1='/bin/mktemp /tmp/openssl.XXXXXX' ; \

PEM2='/bin/mktemp /tmp/openssl.XXXXXX' ; \

/usr/bin/openssl req -utf8 -newkey rsa:1024 -keyout $PEM1 -nodes -x509 -days 365 -out$PEM2 -set\_serial 0 ; \

cat $PEM1 > hostname.pem ; \ echo "" >> hostname.pem ; \

cat $PEM2 >> hostname.pem ; \

rm -f $PEM1 $PEM2

Generating a 1024 bit RSA private key

............................++++++

.....++++++

writing new private key to `/tmp/openssl.z12084?

---

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter `.', the field will be left blank.

---

Country Name (2 letter code) [GB]:

State or Province Name (full name) [Berkshire]:

Locality Name (eg, city) [Newbury]:

Organization Name (eg, company) [My Company Ltd]:

Organizational Unit Name (eg, section) []:

Common Name (eg, your name or your server's hostname) []:

Email Address []:

**#cp /etc/pki/tls/certs/hostname.pem /etc/postfix/cacert.pem**

Restart the postfix service.

**#service postfix restart**

POUR le test mettez //

**Echo ‘Test mail from postfix’ | mail –s’Test Postfix’** [**yassine.rhimi12@gmail.com**](mailto:yassine.rhimi12@gmail.com)

* 1. **Conclusion**

Ce dernier chapitre consiste à présenter les étapes d’installation d’EyesOfNetwork

Ainsi le mode d’utilisation en accédant aux informations fournies par Nagios par l’interface web de notre serveur EyesOf Network. Et d’autres participaient surtout à l’amélioration de la manipulation et l’utilisation d’Eyes Of Network, et surtout facilité de sa configuration.

Enfin de illustrer la remontée des alertes et les notifications par mails en cas de changement d’état d’équipements supervisés.

***Conclusion Générale***

Le domaine de la supervision est un domaine important de l’administration systèmes et réseaux. En constante évolution, les solutions libres de supervision ont prouvé qu’elles avaient leur place dans la sphère professionnelle.

Et comme nous l’avons déjà explicité dans nos étude, la supervision est un des moyens indispensables pour favoriser la croissance de rendement d’une entreprise. Le propos de ce projet est de choisir une solution qui répond aux besoins organisationnels et financiers de l’entreprise et il n’y avait pas mieux pour combler ce besoin qu’EyesOfNetwork .

L'association de Nagios et de Cacti a permis la constitution d'une solution de monitoring à la fois puissante et efficace. Ce stage nous’a permis d’acquérir des connaissances dans le monde de la supervision des réseaux informatiques, et notamment sur le principe et le fonctionnement du protocole SNMP, ainsi que sur le principe et les fonctionnalités des outils de supervision Cacti et Nagios.

Un chemin important a été parcouru pendant nos 4 mois de stage mais il est loin d’être terminé. Arrivé à ce point, chaque administrateur qui a nous en pratique les principes et méthodes décrites jusqu’ici a dans les mains une solution complète de supervision et de métrologie. Il connaît le rôle de chaque élément et, plus important encore, sait comment gérer un projet de mise en place d’une solution de supervision.

***Résumé***

Le présent document constitue une synthèse du projet de fin d’étude effectué au sein de Centre National d’informatique. Le projet consistait à reprendre un logiciel de supervision de réseau dont les principales fonctionnalités sont la découverte de la topologie des réseaux à partir des informations récupérables en interrogeant les équipements réseau avec le protocole SNMP, collecter les pannes et anomalies du système supervisé, et finalement présenter les données graphiquement .

La solution serait donc la mise en place de contrôles automatisés chez chacun de nos Clients, renvoyant des alertes emails en cas de problème. Cela nous permettrait d’être avertis en cas d’espace disque faible ou en cas de perte de connexion internet ou encore en cas de problème de sauvegarde, la liste n’est bien sûr pas exhaustive. Le coût de la mise en place D’un tel système devra être minime pour éviter les répercussions sur les contrats de maintenance.

logiciel de supervision

***Annexe***

*La MIB 54*

*Tableau comparatif entes les logiciels du supervisions55*

*Paramétrage de Nagvis55*

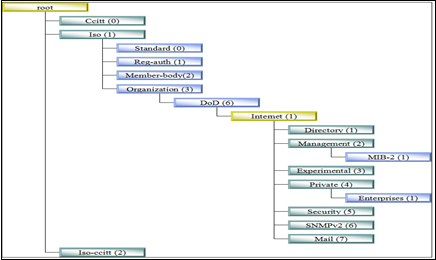
*Création d’une carte sous Nagvis56*

**La MIB**

Comme on a commencé à le voir dans le paragraphe le précédent, SNMP définit deux choses, le protocole, c'est-à-dire la façon dont est transportée l'information et les informations dynamiques, fournies par les différents agents SNMP. Ces informations sont spécifiées dans ce que l'on appelle la MIB (Management Information Base).

La MIB est un ensemble structuré d'informations organisé sous la forme d'un arbre hiérarchisé de la même manière que l'arborescence des domaines Internet. Chaque information dans cette hiérarchie est identifiée par son OID (Object Identifier). Par exemple, l'objet ifDescr est identifié par son OID 1.3.6.1.2.1.2.2.1.2.

Comme on peut le voir dans l'exemple, un OID est une séquence de nombres séparés par le caractère "." (Point).Le début de l'arborescence des OID défini dans les différentes RFC est le suivant :



La MIB est un arbre hiérarchisé très dense. Il existe plusieurs milliers d'OID dans la MIB. Il est par conséquent impossible de décrire tous ces OID dans un seul fichier MIB.

De même que pour le DNS, les différentes parties de la MIB sont définies dans différents fichiers MIB. Chaque fichier MIB a la responsabilité d'une branche particulière de la MIB.

**Tableau comparatif entre les logiciels du supervisions**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **description** | **FAN** | **Nagios** | **Shinken** | **EON** | **Cacti** | **Remarques** |
| licence |  |  |  |  |  |  |
| Disponible facilement | **10** | **10** | **10** | **10** | **5** | Une inscription est obligatoire pour spiceworks |
| installation |  |  |  |  |  |  |
| S’installe sous l’Unix | **10** | **10** | **10** | **10** | **0** | Spiceworks n’est disponible que sous Windows |
| Simple à installer | **8** | **4** | **4** | **8** | **10** | Spiceworks reste les plus rapides à installer, Nagios et Shinken sont plus complexe à installer |
| Compatible avec VMware | **10** | **10** | **10** | **10** | **10** |  |
| paramétrage |  |  |  |  |  |  |
| Simple à paramétrer | **8** | **4** | **4** | **8** | **10** | Spiceworks est le plus simple |
| L’outil est modulable | **8** | **10** | **10** | **8** | **2** |  |
| Accepte l’ajout des plugins | **8** | **10** | **10** | **10** | **2** | L’utilisation des plugins demande un temps d’adaptation sur le produit |
| fonctionnalité |  |  |  |  |  |  |
| Envoi des mails d’alertes | **8** | **8** | **8** | **8** | **10** | Bien définir les alertes mails savant de les activer |
| Supervise des hôtes | **10** | **10** | **10** | **10** | **10** |  |
| Supervise des actifs | **10** | **10** | **10** | **10** | **10** |  |
| Supervise des services | **10** | **10** | **10** | **10** | **10** |  |
| Supervise des éléments définis dans le cahier des charges | **5** | **10** | **10** | **10** | **5** | Certains plugins ne peuvent être ajoutés |
| Génère des rapports | **8** | **8** | **8** | **10** | **2** | Format des rapports |
| **Total** | **113** | **112** | **112** | **122** | **86** |  |

**Paramétrage de Nagvis**

Avant de paramétrer Nagvis il faut :

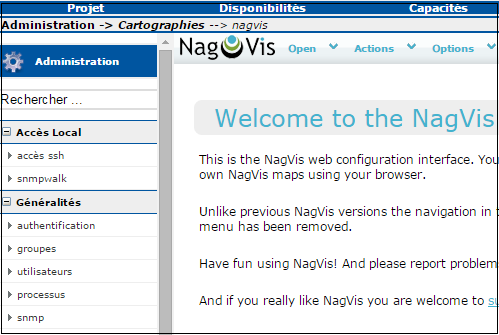
1. Paramétrer notre serveur EON avec tous les actifs que l’on souhaite voir sur la carte.

2. Faire un schéma réseau avec un outil comme Visio ou une photo de nos équipements et l’enregistrer en  png avec un nom sans espace.

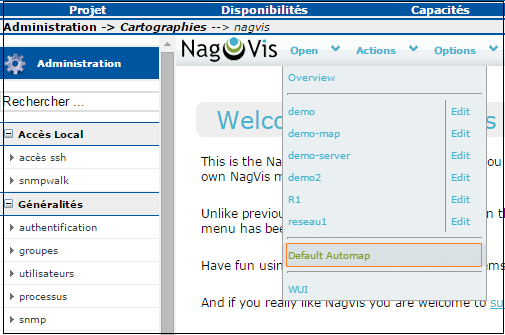
3. Redimensionner l’image en pixel (450\*600) afin d’avoir une meilleure visibilité.

**Création d’une carte sous Nagvis**

Aller dans l’interface d’EON, ensuite il faut cliquer sur l’onglet Disponibilités puis dans la colonne de gauche sur l’onglet Nagvis.

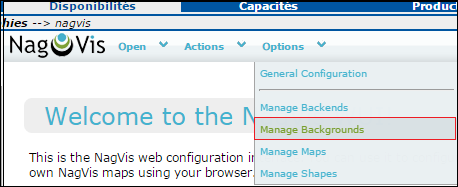


Une fois sur la page de Nagvis, l’on peut cliquer sur «OPEN » puis « WUI » pour pouvoir configurer  Nagvis.

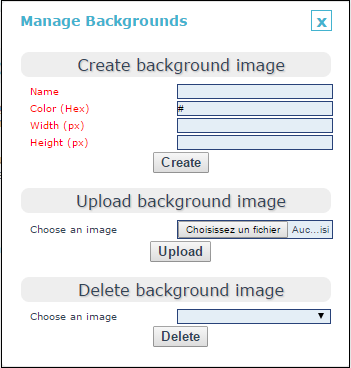


Après avoir cliqué sur WUI, un nouveau menu «**OPTION**» apparait.

Cliquer dessus puis sur manage background pour insérer dans **Nagvis** notre schéma réseau.



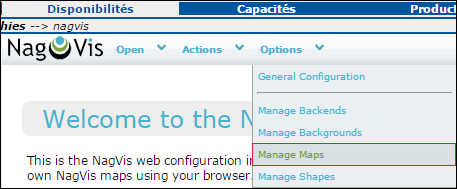
Nous avons donc la fenêtre suivante qui va apparaitre.



Ici, nous allons chercher l’image sur notre support en cliquant sur parcourir, l’image choisie, cliquez sur Upload.

L’image chargée dans notre serveur, nous allons maintenant créer la carte dans Nagvis.

Cliquez sur Options puis sur manage Maps.



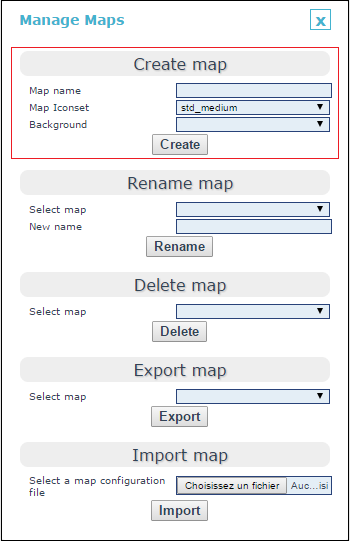
La fenêtre suivante apparait :

Ici, ce sont les trois premiers champs qui nous intéressent.

**Map name** = nom de la carte.

**Map iconset** = définit la taille des icônes sur la carte (petites, moyennes, grandes).

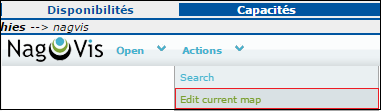
**Backgroud** =Choix de l’image de fond de la carte.



Cliquer maintenant sur << **create** >> la carte se créera.

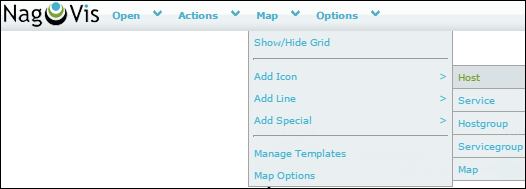
**Placer des indicateurs d’états sur notre carte**

Dans l’interface de Nagvis, connectez-vous sur votre carte, cliquez ensuite sur « **Action** » puis sur « **editcurrent map** ».



Les onglets **« map »** et option **« apparaissent. »**

Cliquez sur  **« map », « Add Icon** » et enfin **« Host »**.



Après avoir cliqué sur la carte, la fenêtre suivante va apparaitre.



Sélectionnez votre hôte dans le champ **« Host name »** puis cliquez sur  **« Save »**. Nous avons

Maintenant notre indicateur d’état sur la carte.

Vous pouvez ensuite placer le curseur de la souris dessus pour voir les informations de l’élément supervisé.

***Néographies***

[www.google.com](http://www.google.com)

<http://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol>

http://www.open-source-guide.com/Solutions/Infrastructure/Supervision-et-la-metrologie

<https://www.eyesofnetwork.com/?lang=fr>

http://www.centos.org/download/

<http://www.gns3.com/>

http://sourceforge.net/projects/gns-3/files/latest/download

http://www.lolokai.com/2011/06/10/virtualisation/configurer-nagios-pour-superviser-un-environnement-vsphere-4-esxi-vcenter-centos/

<http://www.cacti.net/>

<https://www.youtube.com/>

***Bibliographies***

<http://fr.scribd.com/doc/187761738/FR-Eon-v4-Configuration>

http://nagios.sourceforge.net/docs/3\_0/toc.html

Monitoring.fr

Nagios 3

Generation linux

***خلاصة***

**وورك " نات أوف إيز " الشبكات رصد حل وتنصيب دراسة في يتلخص المشروع هذا**

**مراقبة من المديرين يمكن والذي الشبكات مجال في للإعلامية الوطني المركز لمصلحة**

**للشبكة. المكونة والمعدات الأجهزة جميع**

**وذلك بتطبيق خدمات الايز اوف نات وورك الرئيسية وتتمثل في تغطية هيكل الشبكة عبر معلومات تسترد عن طريق تجاوب معداتها مع بروتكول "اس ان ام بي" ثم جمع كل خلل أو عطب للنظام المراقب وفي النهاية عرض النتائج بشكل بياني**.

**الكلمات المفاتيح :**

**وورك, , اس** **ان ام بي. نات أوف إيز**

***Résumé***

Ce document est un résumé du projet dans le Centre informatique national. Le projet était de reprendre des logiciels de surveillance de réseau dont les principales caractéristiques sont la découverte de la topologie du réseau a partir des informations récupérable en interrogeant les périphériques réseau avec le protocole SNMP, de recueillir les échecs et les anomalies du système supervisé, et enfin les données présentes graphiquement.

Mots clés :

Eyes Of Network,SNMP.

logiciels de surveillance

***Abstract***

This document is a summary of the project in National informatics Center. The project was to resume network monitoring software whose main features are the discovery of the network topology from the recoverable information by querying network devices with SNMP, collect the failures and anomalies supervised system, and finally present data graphically.

Keywords:

Eyes Of Network, SNMP.