Chapitre II

Généralités

I. Le réseau local sans fil : Wi-Fi

Le Wi-Fi est une technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenue un moyen d'accès à haut débit à internet. Il est basé sur la norme IEEE 802.11.

Dans la pratique, le wifi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA), des objets communicants ou même des périphériques à une liaison haut débit (de 11 Mbit/s en 802.11b à 54 Mbit/s en 802.11a/g) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres). Dans un environnement ouvert, la portée peut atteindre plusieurs centaines de mètres voire plusieurs dizaines de kilomètres (pour la 'variante' WIMAX ou avec des antennes directionnelles) dans des conditions optimales.

I.1. Mode opératoires du réseau 802.11

Le Wi-Fi cible deux contextes d'utilisation distincts pour un réseau Wi-Fi ayant chacun des caractéristiques propres. Il s'agit du mode **infrastructure** et du mode **ad hoc** (sans infrastructure). Ces deux modes de fonctionnement permettent de définir la topologie du réseau sans fil. La figure ci-dessous représente brièvement les modes de fonctionnement d'un réseau Wi-Fi.

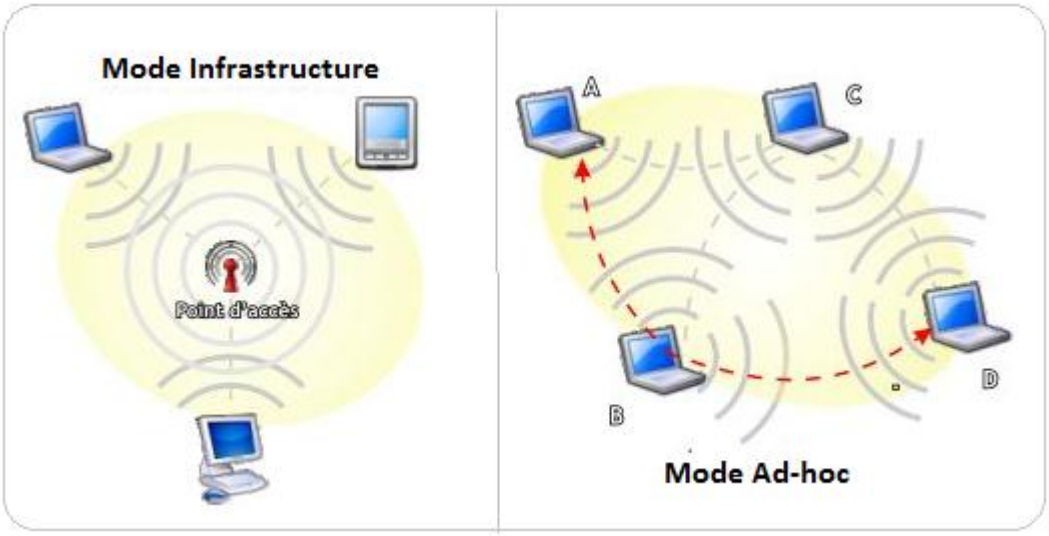

Figure II. 1: Mode opératoire du réseau Wi-Fi

I.2. Architecture du Wi-Fi

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, autrement dit :

- **La couche physique** (notée parfois couche PHY), propose trois types de codage de l'information,

- **La couche liaison de données**, constituée de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC).

La couche physique définit la modulation des ondes radio-électriques et les caractéristiques de la signalisation pour la transmission des données. Tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique. Elle possède notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et elle s'appuie dans sa fonction sur les règles de communication entre les différentes stations.

I.3. Les différentes normes Wi-Fi

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas

des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) et aussi pour préciser des éléments dans le but d'assurer une meilleure sécurité ou une meilleure interopérabilité. Vous trouvez dans la page suivante un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

Norme	***Nom***	***Description***
802.11a	**Wi-Fi5**	La norme 802.11 a permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	**Wi-Fi**	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radios disponibles.
802.11c	**Pontage 802.11 vers 802.1d**	Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données).
802.11d	**Internationalisation**	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11.
802.11e	**Amélioration de la qualité de service**	La norme 802.11e vise à donner des possibilités en matière de qualité du service au niveau de la couche liaison de données. Ainsi cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de manière à permettre une meilleure transmission de la voix et de la vidéo.
802.11f	**Itinérance (roaming)**	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau.
802.11g		La norme 802.11g est la plus répandue dans le commerce actuellement. Elle a une compatibilité descendante avec la norme802.11b.Et elle offre un haut débit: 54 Mbit/s théoriques, 26 Mbit/s réels sur la bande de fréquences des 2,4 GHz.

802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, d'où le h de 802.11h) et cherche à être en conformité avec la réglementation européenne en matière de fréquence. et d'économie d'énergie.
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11n	**WWiSE (World-Wide Spectrum Efficiency) ou TGn Sync**	La norme 802n est sortie en 2007 son débit théorique atteint les 540 Mbit/s (débit réel de 100Mbit/s) avec une portée de rayon de 90 mètres grâce aux technologies MIMO (multiple-input multiple-output) et OFDM (Orthogonal Frequency Division Multiplexing).
802.11s	**Réseau Mesh**	La norme 802.11s est en cours d'élaboration. Son débit théorique atteint aujourd'hui 1 à 2 Mbit/s, et son but est d'implémenter la mobilité sur les réseaux de type ad hoc.

Tableau II. 1: Les différentes normes Wi-Fi

I.4. Les équipements Wi-Fi

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil Wifi :

- **Les adaptateurs sans fil ou cartes d'accès :** Il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs Wi-Fi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte compact flash, ...). D'ailleurs nous appelons station tout équipement possédant une telle carte. Il est important de souligner que les composants Wi-Fi deviennent des standards sur les portables.).
- **Les points d'accès :** Notés AP pour Access point, parfois appelés bornes sans fil. Ils permettent de fournir au réseau filaire un accès (auquel ils sont raccordés) aux différentes stations avoisinantes équipées de cartes Wi-Fi. Cette sorte de hub est l'élément nécessaire pour déployer un réseau centralisé en mode infrastructure. Certains modèles proposent des fonctions de modem ADSL et d'autres, fonctions comme un pare-feu.

- **Les autres :**

  - **Smart Display** : écrans mobiles, soutenus par Microsoft.

  - **Chaînes Wi-Fi** : offrant la capacité de lire les MP3 directement sur le disque dur d'un ordinateur grâce à l'interface Ethernet sans fil intégrée. Elle préfigure toute une génération de produits, capables de lire, outre les CD audio, les radios qui émettent en MP3 sur internet.

  - **Assistant personnel:** les PDA intégrant le Wi-Fi sont parfois plus avantageux qu'un portable pour lire les mails, importer des documents voir surfer sur le net.

  - **Rétroprojecteurs:** pour des présentations avec portables mobiles.

  - **Caméra vidéo:** transmet des images à distance à l'ordinateur qui les enregistre par la suite.

II. Sécurité des réseaux Wi-Fi :

Les ondes radio-électriques ont intrinsèquement une grande capacité à se propager dans toutes les directions avec une portée relativement grande. Il est ainsi, très difficile d'arriver à confiner les émissions d'ondes radio dans un périmètre restreint.

La principale conséquence de cette "propagation sauvage" des ondes radios est la facilité d'accès que peut avoir une personne non autorisée d'écouter le réseau. Il existe plusieurs niveaux de sécurité permettant d'une part, de gérer les droits d'accès au réseau Wi-Fi, et d'autre part, de garantir la confidentialité des échanges.

II.1. Infrastructure adaptée :

Dans cette perspective, la première action à effectuer consiste à positionner intelligemment les points d'accès selon la zone à couvrir. Il est préférable d'éviter les murs extérieurs et de choisir plutôt un emplacement central.

II.2. Eviter les valeurs par défauts :

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Toutefois, les paramètres par défaut agissent de façon que la sécurité soit minimale. Il est donc impératif de se connecter à l'interface d'administration pour définir un mot de passe

d'administration.

En outre, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID). Ainsi qu'il est vivement conseillé de modifier le nom de réseau par défaut et de désactiver la diffusion.

II.3. Chiffrement WEP ou WPA

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du WEP, qui est un protocole chargé du chiffrement des trames 802.11 utilisant l'algorithme symétrique RC4 avec des clés d'une longueur de 64 bits ou 128 bits.

Par ailleurs, pour obtenir un niveau de sécurité supérieur, il convient d'utiliser le cryptage WPA ou WPA2.

II.4. Filtrage des adresses MAC

Chaque adaptateur réseau possède une adresse physique qui lui est propre (appelée adresse MAC). Cette adresse est représentée par 12 chiffres hexadécimaux groupés par paires et séparés par des tirets. Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. En activant ce MAC Adresse Filtering (Filtrage des adresses MAC), même si cette précaution est un peu contraignante, nous pouvons limiter l'accès au réseau à un certain nombre de machines. En contrepartie, cette démarche ne règle pas le problème de la confidentialité des échanges.

II.5. Amélioration de l'authentification

Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs (en anglais AAA pour Authentication, Authorization, and Accounting) il est possible de recourir à un serveur RADIUS (Remote Authentication Dial-In User Service). Le protocole, est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

III. Supervision du Wi-Fi

La supervision de réseaux peut être définie comme l'utilisation de ressources réseaux adaptées dans le but d'obtenir des informations (en temps réel ou non) par interrogation périodique ou par remontée non sollicitée de l'informations de la part des équipements de réseau, 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.

La mise en place d'une supervision réseau a comme principale vocation la collection, à intervalle régulier, des informations nécessaires sur l'état de l'infrastructure et des entités qui y sont utilisées, de les analyser et de les rapporter.

Il existe des protocoles réseau qui permettent de récupérer des informations sur le parc informatique. Les deux plus importants qui possèdent des rôles très différents mais qui ont un point en commun : Ils sont tous deux largement utilisés par les logiciels de supervision.

- **ICMP (Internet Control Message Protocol) :** est un protocole de couche réseau qui vient palier à l'absence de message d'erreur du protocole IP (Internet Protocol). C'est un protocole très simple, qui n'a pas pour fonction directe la supervision d'un réseau mais qui est utilisé comme source d'information sur la qualité du réseau ou sur la présence d'une machine.

- **SNMP (Simple Network Management Protocol) :** SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau). C'est un protocole qui permet comme son nom l'indique, de gérer les équipements réseaux ainsi que les machines informatiques. Ce protocole est donc utilisé par les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau. Par soucis de simplicité et donc de rapidité, SNMP ne transporte que des variables et s'appuie sur le protocole UDP (User Datagram 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 .

➢ 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 créée par un agent en cas d'évènement et utilise un message dit de type trap ou de type inform pour prévenir le serveur. Ce message SNMP transite via le port 162 UDP.

Dans notre cas, nous allons configurer le logiciel « Nagios » qui se base sur le protocole SNMP, pour pouvoir superviser le réseau Wi-Fi.

III.1. C'est quoi Nagios ?

Nagios est un logiciel libre distribué sous licence GPL. Il permet de superviser un système d'information complet utilisé par de nombreuses sociétés.

Etant le successeur de **NetSaint** ,Nagios est considéré comme une évolution de ce dernier avec l'ajout en principe de la gestion du protocole SNMP.

Cet outil repose sur une plate-forme de supervision, fonctionnant sous Linux et sous la plupart des systèmes Unix. Grace à son fonctionnement modulaire, il centralise les informations récoltées périodiquement. Chose qui le rend beaucoup plus attractif que les autres produits concurrents bien que, sa configuration se révéle complexe.

III.1.1. Fonctionnalités

Les fonctionnalités de Nagios sont très nombreuses, parmi les plus communes nous pouvons citer les suivantes :

- La supervision des services réseaux (SMTP, HTTP,…), des hôtes et des ressources systèmes (CPU, charge mémoire…),

- La détermination à distance et de manière automatique de l'état des objets et des ressources nécessaires au bon fonctionnement du système grâce à ses plugins. Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche (Bash, C++, Python, Perl, PHP, C#, etc.),
- Représentation coloriée des états des services et des hôtes définies,
- Génération de rapports,
- Cartographie du réseau,
- Gestion des alertes,
- Surveillance des processus (sous Windows, Unix…),
- La supervision à distance peut utiliser SSH ou un tunnel SSL.

Figure II. 2: Centralisation de l'information par Nagios

III.1.2. Architecture

L'architecture de Nagios se base sur le paradigme serveur-agent. Cet outil s'appuie spécifiquement sur un serveur faisant office de point central de collecte des informations tandis que les autres machines du réseau exécutent un agent chargé de renvoyer les informations au serveur.

L'architecture globale de Nagios peut être décomposée en trois parties coopératives que nous décrivons dans les points suivants :

- **Un noyau** : qui est le cœur du serveur Nagios, lancé sous forme de démon. Il est responsable de la collecte et de l'analyse des informations, de la réaction, de la prévention, de la réparation et de l'ordonnancement des vérifications (quand et dans quel ordre) ;

- **Des exécutants** : ce sont les plugins, responsables de l'exécution des contrôles et des tests sur des machines distantes ou locales et du renvoi des résultats au noyau du serveur Nagios ;

- **L'interface graphique :** accessible par le web, elle est conçue pour rendre plus exploitable les résultats. Cette interface est basée sur les CGI (Common Gateway Interface) fournis par défaut lors de l'installation de Nagios et qui interprètent les réponses des plugins pour les présenter dans l'interface par la suite.

Figure II. 3 : Architecture de Nagios

III.1.3. Plugins

Nagios fonctionne grâce à des plugins écris en Perl ou en C. Sans ces plugins Nagios incapable de superviser et il se réduit à un simple noyau.

Les plugins sont en fait, 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 des requêtes vers les hôtes ou les services choisis lors d'un appel du processus de Nagios. Et il se base sur la transmission du code de retour au serveur principal qui par son tour se charge d'interpréter les résultats et de déterminer l'état de l'entité réseau testée.

Il est possible de créer son propre plugin et de l'interfacer avec Nagios tout en respectant les conventions des codes de retour que nous allons expliquer par la suite.

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.

Le tableau suivant présente un résumé de cette relation:

Code retour	*Etat*	*Signification*
1	OK	Tout va bien
2	Warning	Le seuil d'alerte est dépassé
3	Critical	Le service a un problème
4	Unknown	Impossible de connaitre l'état de service

Tableau II. 2: Signification des codes de retour

Comme nous pouvons le constater sur la figure ci-dessous, les plugins fonctionnent en effectuant des tests en local et à distance par le biais de divers moyens comme l'installation des agents NRPE ou NSClient ou autres.

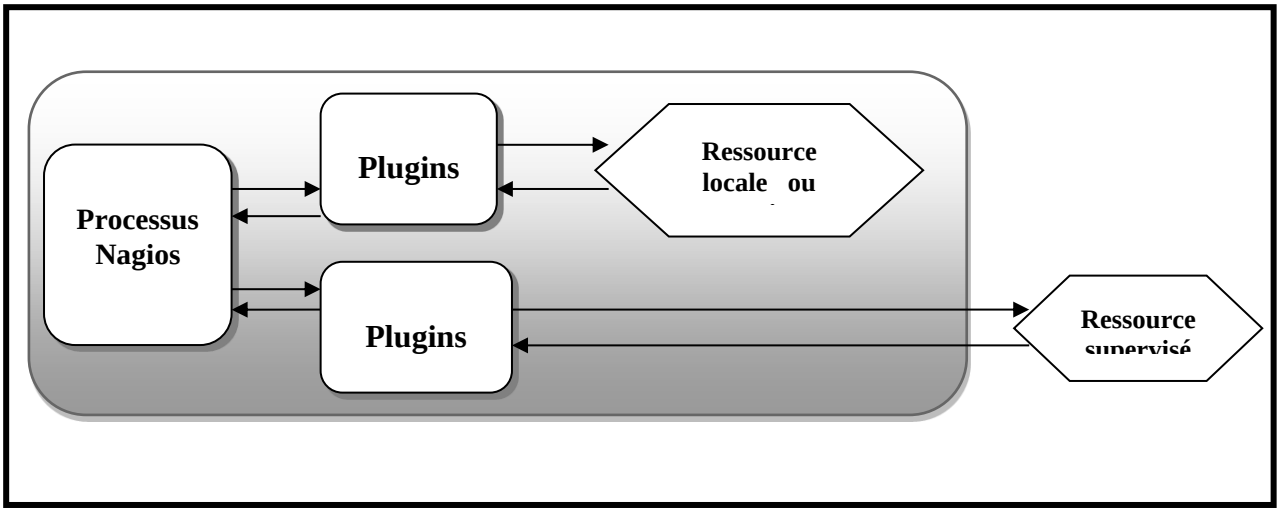

Figure II. 4: Principe du fonctionnement des plugins

III.1.4. Les fichiers de configuration

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

- **Nagios.cfg** est le fichier de configuration principal de Nagios. Il contient la liste

des autres fichiers de configuration comme il comprend l'ensemble des directives globales de fonctionnement ;

- **Cgi.cfg** contient un certain nombre de directives qui affectent le mode de fonctionnement des CGI. Il s'avère qu'il joue un rôle intéressant dans la définition des préférences concernant l'interface web de Nagios ;

- **Resource.cfg** permet de définir des variables globales réutilisables dans les autres fichiers. Etant inaccessible depuis les CGI qui génèrent l'interface, ce fichier peut être utilisé pour stocker des informations sensibles de configuration ;

- **Commands.cfg** contient les définitions des commandes externes, telles que celles qui seront utiles pour la remontée d'alerte ;

- **Checkcommands.cfg** contient les définitions des commandes de vérification prédéfinies et celles définies par l'utilisateur ;

- **Hosts.cfg** définit les différents hôtes du réseau à superviser. A chaque hôte est associé un nom, une adresse IP, et un test à effectuer par défaut pour caractériser l'état de l'hôte, etc ;

- **Services.cfg** associe à chaque hôte ou à chaque groupe d'hôtes l'ensemble des services qui doivent être vérifiés ;

- **Hostsgroups.cfg** définit des groupes d'hôtes pour regrouper des hôtes selon des caractéristiques communes. Un hôte peut appartenir à plusieurs groupes ;

- **Contacts.cfg** déclare les contacts à prévenir en cas d'incident et définit les paramètres des alertes (fréquences des notifications, moyens pour contacter ces personnes, plages horaires d'envoi des alertes...).

Chapitre III

Modularisation du logiciel « Nagios »

Dans ce dernier chapitre, nous allons présenter la procédure adoptée pour superviser notre réseau Wi-Fi contrôlé par un contrôleur Wi-Fi « Ruckus ».

I. Environnement de mise en place

I.1. Environnement matériel

Nous allons installer notre logiciel sur un serveur ayant les caractéristiques suivantes :

- Système d'exploitation linux : Fedora 14 ;
- Microprocesseur dual core;
- Connexion internet.

I.2. Environnement logiciel

- La solution de supervision Nagios ;
- Les greffons de Nagios, Nagios-plugins ;
- Le plugin NDOutils pour le stockage des données de Nagios dans la base de données MySQL ;
- Le plugin NSClient pour la supervision des serveurs Windows ;
- Le plugin NRPE pour la supervision des serveurs Linux ;
- le plugin PnP4Nagios, permet de générer des graphes sur les hosts et services surveillés par Nagios ;
- le plugin ruckus zone director pour superviser le réseau Wi-Fi

II. Mise en place de Nagios

II.1. Prérequis Nagios

En plus des plugins Nagios, nous sommes appelées à satisfaire certaines dépendances. Les prérequis d'installation sont donc :

- Dépendances LAMP : Apche2, PHP5, MySQL
- Librairies Perl
- Les librairies graphiques : GD, libgd libpng, libjpeg…
- Compilateur : gcc, gcc-gc++

II.2. Installation de Nagios

Les étapes d'installation et de configuration de « Nagios » et ses plugins Nagios-plugins NDOutils seront détaillées dans l'annexe.

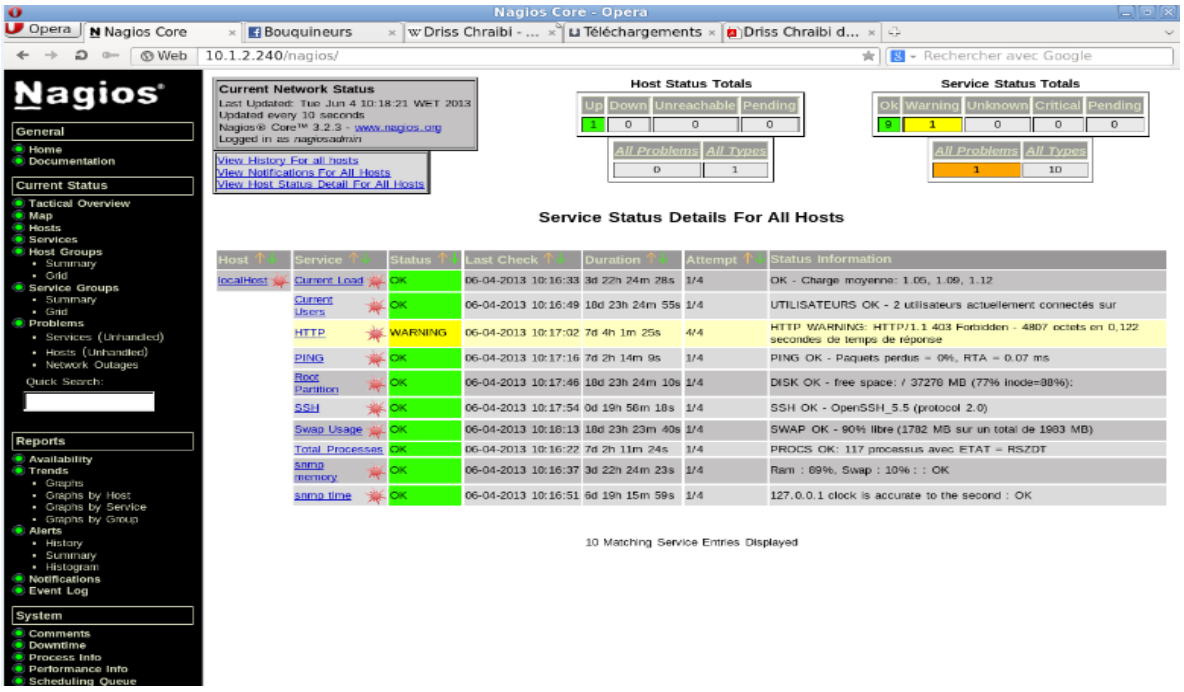

Figure III. 1 : Interface de Nagios

II.3. Installation de NSClient

Pour la supervision des serveurs Windows, nous allons installer le greffon NSClient sur la machine distante et vérifier la présence de la commande « check_nt » parmi les plugins installés de Nagios.

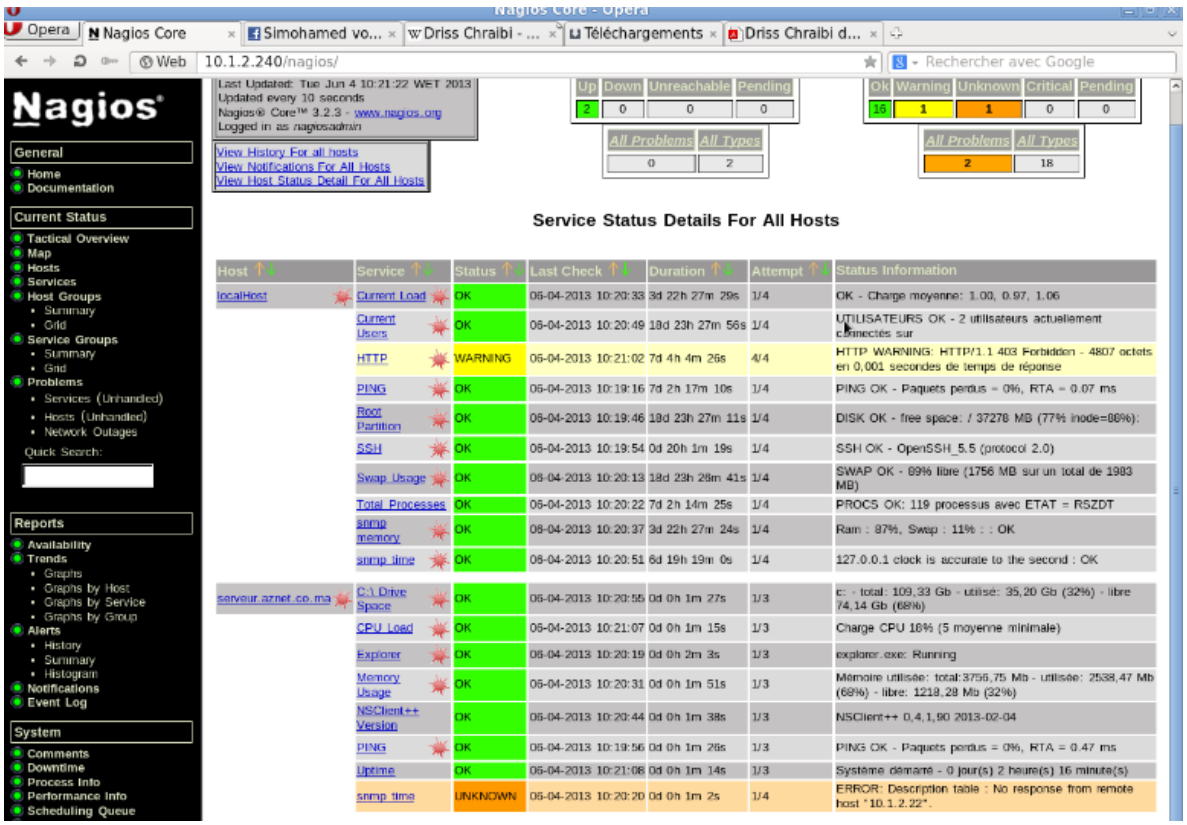

Figure III. 2 : supervision de Windows

II.4. Installation de NRPE

Pour superviser les serveurs Linux, nous allons installer le greffon « NRPE » sur la machine distante et vérifier la présence de la commande « check_nrpe » parmi les plugins installés de Nagios.

II.5. Installation PnP4Nagios

Afin d'avoir des graphes, nous avons choisit d'installer PnP4Nagios, le plugin permettant de générer des graphes sur les hosts et les services surveillés par Nagios.

Figure III. 3: Graphe associé à la supervision

III. Nagios et la supervision du réseau Wi-Fi

Afin de pouvoir superviser notre réseau Wi-Fi contrôlé par « Ruckus » nous allons dans un premier temps, télécharger le plugin check zone director.

Et ensuite, nous allons modifier le code écrit en langage de programmation « Perl » afin d'avoir une vue global sur notre réseau Wi-Fi.

Dans notre cas nous allons ajouter la fonctionnalité permettant l'affichage du nombre de point d'accès liés à notre contrôleur Wi-Fi.

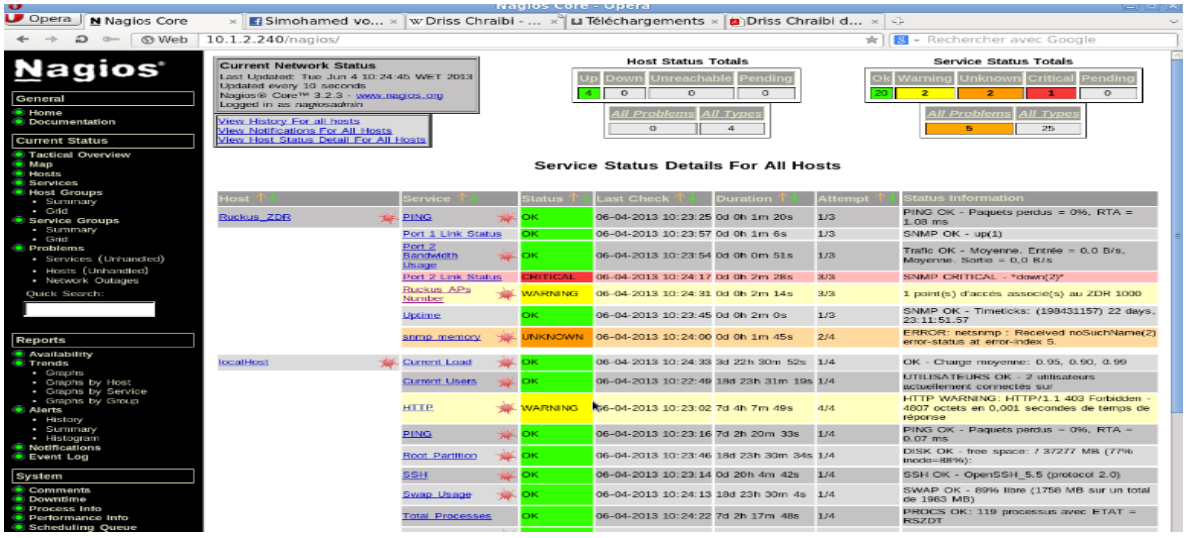

Figure III. 4 : la supervision du réseau Wi-Fi

Dans la phase suivante nous souhaitons associer notre supervision Wi-Fi au plugin

PnP4Nagios afin de générer des graphes et d'avoir une supervision en temps réel de notre Réseau Wi-Fi. Pour effectuer cette tâche nous allons associer notre plugin « check zone director » au plugin PnP, qui est un module permettant à Nagios de stocker, dans une base RRD et d'afficher via une interface Web , des données provenant des plugins Nagios , selon la procédure suivante :

PnP stocke ces templates dans deux endroits :

- /usr/local/pnp4nagios/share/templates.dist → Il s'agit des modèles inclus avec PNP ;
- /usr/local/pnp4nagios/share/templates → Il s'agit des modèles personnalisés.

Nous accédons ainsi à : /usr/local/pnp4nagios/share/templates pour créer notre propre Template qui doit respecter les conditions suivantes:

- Les modèles doivent avoir le code PHP valide.
- Les modèles ne doivent pas réaliser des sorties (echo, return, etc …).
- Les deux tableaux $opt[] et $def[] doivent y apparaître, Ces deux tableaux sont nécessaires pour l'exécution de la commande 'rrdtool graph'

Après la création de notre Template un fichier XML se génère automatiquement.

Figure III. 5 : Graphe associé à la supervision Wi-Fi