Table de Matières

Liste des Figures

Liste des Tableaux

Introduction générale

Actuellement aucune entreprise ne peut se passer d'outils informatiques, et très souvent un réseau informatique de taille plus ou moins importante est mis en œuvre.
Le nombre des machines dans ces réseaux peut parfois devenir extrêmement élevé, La maintenance ainsi que la gestion de ces parcs informatiques deviennent alors des enjeux cruciaux, d'autant plus qu'une panne du réseau peut parfois avoir des conséquences catastrophiques.

C'est pourquoi les administrateurs réseau font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi informé (par email, par SMS) en cas de problème. Grâce à un tel système, les délais d'interventions sont fortement réduits.

Plusieurs logiciels réalisent ces tâches, comme par exemple Websense, Tivoli, Observer,Hp Openview, Ciscoworks, Patrol et d'autres, mais certains sont payants.
Dans ce domaine, un logiciel fait office de référence: Nagios. En effet Nagios est très performant et possède une prise en main assez intuitive. Il s'installe sur une machine possédant un système d'exploitation Linux, mais peut superviser aussi bien des machines Linux que Windows. Cet outil permet également une supervision des équipements réseaux (Routeur, Switch), ce qui est primordial pour l'utilisation que l'on va en faire.

De plus, Nagios est un outil Open source: Chaque société peut l'adapter comme elle lui semble. Ainsi, la société ne payera pas de licence: elle ne payera que les frais de formation, d'installation et de maintenance.

Enfin un autre avantage: Une grosse communauté est réunie autour de ce logiciel, ce qui facilite les recherches de documentations et de réponses à nos questions.
Notre projet consiste donc à superviser un réseau grâce à l'outil Nagios. Ce rapport résumera les trois étapes de notre projet : Compréhension, installation, et utilisation de Nagios.

Ce rapport comporte 5 chapitres:

Dans un premier chapitre intitulé «Présentation du cadre du projet», nous allons présenter l'organisme d'accueil et le contexte du projet et ses objectifs.

Le deuxième chapitre concerne «Présentation de l'outil de supervision Nagios», dans ce chapitre nous allons présenter notre outil de supervision Nagios.

Le troisième chapitre «Installation du système de supervision», nous allons montrer les étapes de l'installation avec des imprime écran.

Le quatrième chapitre , «Les complément de nagios» Dans ce chapitre nous vais présenter tout outils ou compléments que nous 'envisageons ajouter à Nagios 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.

Et le dernier chapitre « Mise en place de system de supervision» Au sein de ce dernier chapitre, nous vont présenter l'environnement de travail et enfin quelques captures écrans des interfaces de Nagios/Centreon

Chapitre I : Présentation du cadre du projet

1. Présentation de l'organisme d'accueil

La CNAM a été crée par la loi N° 71/2004 portant institution d'un régime d'assurance maladie. Il s'agit d'un établissement public à caractère administratif doté de la personnalité civile et de l'autonomie financière. Elle s'engage à assurer tous les services dans le domaine de la santé, prodigués par les prestataires contractants, en vertu des normes et conditions énoncées par les textes législatifs et réglementaires ainsi que les conventions sectorielles établies à cet effet, elle a le droit de payer les prestataires de services dans le domaine de santé, selon les tarifs, les normes et les procédures énoncés aux conventions sectorielles, créer une structure informatique afin de garantir la couverture adéquate pour chaque service dans le cadre de l'assurance maladie, ainsi que le rassemblement des données médicales et financières afférentes à la gestion de ce domaine, en collaboration et en coordination avec les prestataires de services. Procurer les données et les informations nécessaires relatives aux services dans le domaine de santé prodigués dans le cadre du système d'assurance maladie et de les mettre à la disposition des prestataires, ce qui serait de nature à mieux rationaliser les dépenses et à mieux les contrôler. La CNAM effectue aussi le contrôle médical, conformément aux normes et évaluations réglementées par la législation en vigueur ainsi que les références médicales et les protocoles des soins énoncés dans les conventions sectorielles, et ce avec le respect en premier lieu des principes fondamentaux relatifs aux professions médicales et paramédicales, aux professions de pharmaciens biologistes, notamment d'exercice privé, ainsi que le respect du libre choix du malade du prestataire de service. Au niveau de la CNAM prestataires privés sont soumis à des obligations comme la non-sélection des assurés sociaux et le respect du principe de l'égalité de traitement entre eux, la garantie de la qualité de service, l'information publique de leur conventionnement avec la CNAM, l'application des tarifs conventionnels fixés par les conventions sectorielles ainsi que la rationalisation des dépenses afin de mieux contrôler les coûts dans le cadre des conventions sectorielles. Cette dernière est réalisé par la prescription de médicaments au moindre coût et la participation aux campagnes de sensibilisation des assurés pour maîtriser leurs comportements, de procurer les meilleures conditions de travail afin de procéder à un meilleur contrôle dans le domaine de la santé. Un autre service est présent au niveau de la caisse, l'affiliation, qui assure la liberté d'affiliation à la convention sectorielle réglementant les rapports entre la Caisse et les prestataires de services. En effet, la CNAM ne peut refuser une demande d'affiliation d'un prestataire de service qui exerce sa profession selon la législation en vigueur et qui respecte les dispositions de la convention sectorielle.

2. Organigramme de la CNAM

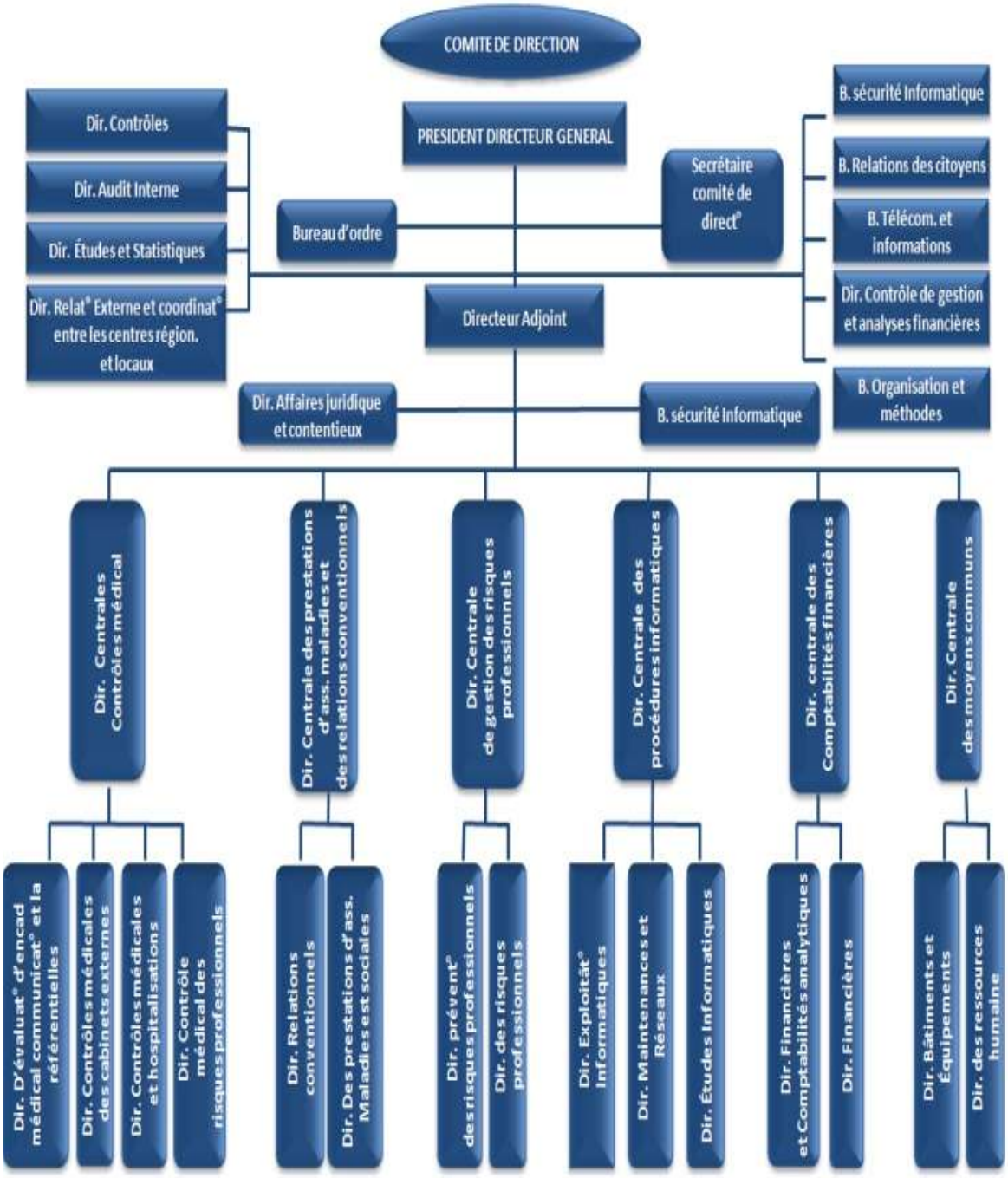

Figure 1 : Organigramme de la Caisse national d'assurance maladie (CNAM)

3. Cadre du projet

Dans le cadre de l'obtention d'un diplôme du mastère professionnel en sécurité des systèmes d'information à L'Institut Supérieur de Gestion de Tunis, il m'a était demandé d'élaborer un rapport suite à un stage de six mois. C'est dans ce cadre et pour l'année universitaire 2012/2013 que j'ai effectué le présent projet au sein de la Caisse National d'Assurance Maladie qui porte sur la mise en place d'une application de monitoring réseaux informatique (Nagios).

4. Travail demandé

Recherche, Implémentation et configuration d'une solution Open Source qui vise à superviser à distance les différents serveurs de la société avec gestion des alertes dans un environnement Multi plate formes.

5. Plan du travail

Le but principal du projet est de pouvoir établir, choisir ou installer une station de surveillance des serveurs qui remplissent les conditions suivantes :

- Récupération des informations permettant la détection des pannes, l'indisponibilité des serveurs et de leurs services.
- Des renseignements supplémentaires de monitoring sur la charge CPU, Espace disque, Mémoire disponible, input/output, etc.…
- Gestion des alertes.
- Notification par mail ou SMS en cas de problème.
- Générer des rapports sur le fonctionnement des serveurs par mois.
- Générer des graphes (cartographie du réseau,…).
- Une interface graphique claire pour l'interaction utilisateur/Logiciel.

6. Description de l'existant

Ce présent travail s'est déroulé dans un environnement comportant un parc informatique composé de machines et de serveurs régionaux locaux et distants.

C.N.A.M possède un grand nombre de serveurs en Tunisie qui nécessite une solution de supervision de ces énormes réseaux.

Chaque centre CNAM soit régional ou local possède :

- Un serveur avec système d'exploitation Redhat Entreprise5 il faut aussi qu'il doit être équipé d'un serveur de domaine et de partage samba, aussi une machine virtuelle windows 2003 pour le serveur antivirus Kaspersky Admin Kit.
- Un Switch ou plusieurs administrable avec configuration du VLAN selon le centre et les nombre des directions.
- Modem et routeur fourni par Tunisie Telecom.
- Les Pc des personnelles sous le domaine par exemple jerba.cnam et authentifie par (nom.prenom) de l'agent.
- Des onduleurs pour l'armoire des réseaux branché avec câble USB au serveur pour la suivi de l'état de la batterie.

Et pour la salle informatique (voir fig 12), on a plusieurs serveurs et équipements dont les plus importants sont :

- Les deux serveurs base de données cnam1 et cnam2 avec l'OS solaris 10 avec SGBD Oracle 10g
- les serveurs FTP, DNS, WEB, sauvegarde
- deux Switch niveau 3
- deux firewalls

7. Critique de l'existant

Ce présent travail s'est déroulé dans un environnement comportant un parc informatique composé de machines et de serveurs régionaux locaux et distants.

C.N.A.M possède un grand nombre de serveurs en Tunisie qui nécessite une solution de supervision de ces énormes réseaux.

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 (charge CPU, Etat mémoire, surcharge du disque….), ni les surcharges et pénurie temporaire des ressources. Le seul moyen de détecter ces anomalies ne peut se faire que par la réception des différentes plaintes et réclamations des agents de centres régionaux ou locaux distants. Nombreux sont les problèmes que rencontre un centre lors d'une panne d'équipement causant une coupure globale au niveau du réseau. D'une part, Celle-ci contrariait les assurés en créant un retard au niveau du service au guichet, mais aussi un retard pour fixer ce problème puisqu'il fallait contacter la direction informatique afin de régler cette défaillance technique et cela prenait assez de temps. D'autre part, il existe en Tunisie 65 centres CNAM qui ont besoin d'être constamment suivis mais le

manque d'informaticiens ne permet pas de remplir cette tache. Enfin, les liaisons entre les centres fournis par Tunisie télécom rendent compte de plusieurs problèmes de débit. Lors d'une réclamation auprès du fournisseur de la ligne celui-ci se détache de cette responsabilité en assurant que la ligne ne présente aucun problème et nous n'avons pas assez de preuves techniques pour lui prouver le contraire.

Se souciant de sa réputation et concerné par la satisfaction et le confort des assurés sociaux ainsi que les professionnels de santé conventionnés, la CNAM veut à tout prix minimiser tout arrêt éventuel de ses services vu la gravité de son impact de point de vu social, et ce en travaillant pour offrir une meilleure qualité de services en anticipant les pannes et en évitant les arrêts de longue durées.

Le but de ce projet est donc de trouver une solution optimale pour la gestion des serveurs et la supervision de ses équipements en premier lieu, offrir la possibilité de devenir « pro actif » face aux problèmes rencontrés du second lieu, et finalement le plus important est 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.

8. Solution proposée

La gestion et la supervision des serveurs et des équipements réseaux distants représentent un souci important pour l'administrateur. De ce fait, nous avons jugé nécessaire de mettre en place un outil pour contrôler le fonctionnement du réseau, d'étudier les données collectées et de définir des mécanismes déclenchant 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 et en surveillant le statut des serveurs, des divers services réseaux et d'offrir des renseignements supplémentaires voir charge CPU, espace disque, mémoire disponible, etc.

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.

9. 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 a permis de cerner la problématique de notre projet. Nous avons par la suite proposé des solutions à leur étude et à notre encadreur pour finalement poser notre choix sur la solution que nous jugeons la plus convenable à la CNAM et à la formation que nous estimons acquérir qui est le logiciel de supervision libre « Nagios ».

Chapitre II : Présentation de l'outil de supervision « Nagios »

1. Introduction

Dans ce présent chapitre, nous commençons par définir la notion de la supervision et de ses objectifs, ensuite est d'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 configurations sur quoi ce base cette solution.

2. Supervision

2.1 Définition

La supervision des réseaux peut être définie comme l'utilisation de 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 celles-ci.

La mise en place d'une supervision réseau, à donc pour principale vocation de collecter à intervalle régulier les informations nécessaires sur l'état de l'infrastructure et des entités qui y sont utilisés, de les analyser et de les rapporter.

2.2 Objectifs

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.

3. Présentation de Nagios

Nagios est un logiciel de supervision de réseau libre sous licence GPL qui fonctionne sous Linux. Il a pour fonction de surveiller les hôtes et services spécifiés, alertant l'administrateur des états des machines et équipements présents sur le réseau.

Bien qu'il fonctionne dans un environnement Linux, ce logiciel est capable de superviser

Toutes sortes de systèmes d'exploitation (Windows XP, Windows 2000, Windows 2003 Server, Linux, Mac OS entre autres) et également des équipements réseaux grâce au protocole SNMP.

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

Ce logiciel est composé de trois parties:

-Le moteur de l'application qui gère l'ordonnance, les supervisions des différents équipements.

-Les Plugins qui servent d'intermédiaire entre les ressources que l'on souhaite superviser et le moteur de Nagios. Il faut bien noter que pour accéder à une certaine ressource sur un Hôte, il faut un plugin coté Nagios et un autre coté hôte administré.

-L'interface web qui permet d'avoir une vue d'ensemble des états de chaque machine du Parc informatique superviser et ainsi pouvoir intervenir le plus rapidement possible en Ciblant la bonne panne.

4. Fonctionnalités

Figure 2 : Centralisation d'informations par Nagios

Les fonctionnalités de Nagios sont très nombreuses, parmi les plus communes que nous pouvons cités sont 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 l'état des objets et les ressources nécessaires au bon fonctionnement du système grâce à ses plugins.
- Représentation coloriée des états des services et hôtes définies.
- Génération de rapports.
- Cartographie du réseau.
- Gestion des alertes.
- Surveillance des processus (sous Windows, Unix…).
- Superviser des services réseaux : (SMTP, POP3, HTTP, ICMP, SNMP, DAP, etc.)
- La supervision à distance peut utiliser SSH ou un tunnel SSL.
- Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche (Bash, C++, Python, Perl, PHP, C#, etc.)

5. Architecture

L'architecture de Nagios se base sur le paradigme serveur-agent. D'une manière spécifique, un serveur fessant 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 3 parties coopératives entre elles :

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

C'est le principe de répartition des contrôles au mieux dans le temps qui nous évites la surcharge du serveur et des machines à surveiller.

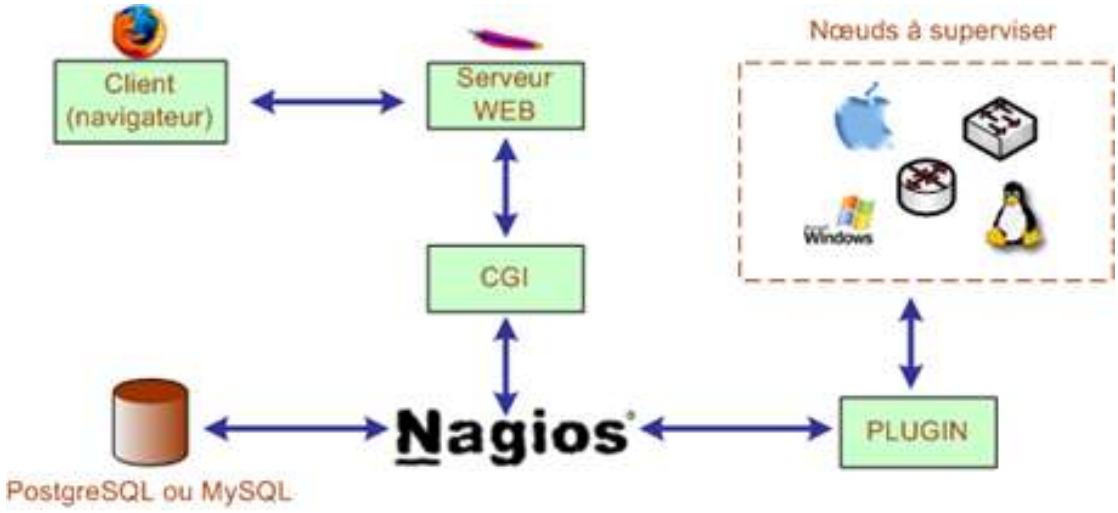

Figure 3 : Architecture Nagios

➢ **Des exécutants** : ce sont les plugins dont un grand nombre est fourni de base, responsables de l'exécution des contrôles et tests sur des machines distantes ou locales et du renvoie des résultats au noyau du serveur Nagios

➢ **Une IHM :** C'est une interface graphique accessible par le web conçue pour rendre plus exploitable les résultats. Elle est basée sur les CGI (Common Gateway Interface) fournis par défaut lors de l'installation de Nagios qui interprètent les réponses des plugins pour les présenter dans l'interface.

Cette interface sert à afficher de manière claire et concise une vue d'ensemble du système d'information et l'état des services surveillés, de générer des rapports et de visualiser l'historique. D'une manière générale avoir la possibilité de détecter en un simple coup d'œil, les services ou hôtes ayant besoin d'une intervention de leur administrateur.

- **Avantages**
  - Des plugins qui étendent les possibilités de Nagios.
  - Une très grande communauté qui participe activement au développement.
  - Un moteur performant.
  - Solution complète permettant le reporting, la gestion des pannes et d'alarmes, gestion des utilisateurs…
  - Des plugins permettent aux utilisateurs de développer facilement ces propres vérifications de leurs services.
  - Possibilité de repartir la supervision entre plusieurs administrateurs.
  - Offre la possibilité de développer ses propres modules.
- **Inconvénients**
  - Configuration complexe mais peut s'améliorer en ajoutant Centreon.
  - Interface peu ergonomique et intuitive.

6. Plugins

Nagios fonctionne grâce à des plugins écris en Perl ou en C. Sans eux, il est totalement incapable de superviser et se résume 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'envoie de requêtes vers les hôtes ou services choisis lors d'un appel du processus de Nagios, 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 sont assurés d'une part par les fichiers de configurations (définitions des commandes) et d'autre part par le code retour d'un plugin. Cette relation peut se résumer par le tableau suivant :

Code retour	Etat	Signification
1	Ok	Tout va bien
2	Warning	Le seuil d'alerte est dépassé
3	Critical	Le service à un problème
4	Unkown	Impossible de connaître l'état du service

Tableau 1 : Signification des codes de retours

Nagios est livré avec un « package » de greffons standards regroupant les plus utilisés. Pour une utilisation basique et simple, ils devraient être suffisants. En voilà quelques exemples:

- **check_http :** Vérifie la présence d'un serveur web.
- **check_load :** Vérifie la charge CPU locale.
- **check_ping :** Envoie une requête Ping à un hôte.
- **check_pop :** Vérifie la présence d'un serveur POP3.
- **check_procs :** Compte les processus locaux.
- **check_smtp :** Vérifie la présence d'un serveur SMTP.
- **check_snmp :** Envoie une requête SNMP (passée en argument) à un hôte.
- **check_ssh :** Vérifie la présence d'un service SSH.
- **check_tcp :** Vérifie l'ouverture d'un port TCP (passé en argument).
- **check_users :** Compte le nombre d'utilisateurs sur la machine locale.

Il est possible de créer son propre plugin et l'interfacer avec Nagios tout en respectant les conventions des codes de retours précédemment expliqués.
La vivacité de la communauté Open Source et celle de Nagios 2 en particulier permet de disposer d'un grand nombre de plugins supplémentaires.
Comme on peut le constater, les plugins peuvent fonctionner soit en effectuant des tests en local, à distance par le biais de divers moyen comme l'installation des agents NRPE sous linux ou NSClient sous Windows ou autres.

7. 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 et comprend l'ensemble des directives globales de fonctionnement.
- **Cgi.cfg** contient un certain nombre de directives qui affectent le mode de fonctionnements des CGI. Il peut être intéressant pour définir les 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 son nom, son adresse IP, le 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 de définir les paramètres des alertes (fréquences des notifications, moyens pour contacter ces personnes, plages horaires d'envoi des alertes...).

8. Conclusion

Le présent chapitre a été introduit avec une brève présentation de la notion de supervision et ses enjeux. Ensuite nous avons décrit l'aspect de notre solution, énuméré ses fonctionnalités et modélisé son architecture. Finalement une partie a été consacrée pour la définition des différents fichiers de configurations générés par la solution de supervision Nagios, précédé par l'é/numération des différents plugins de base responsable de l'exécution des tests nécessaires.

Chapitre III: Installation du système de supervision

1. Présentation Fan

Le but de FAN est de fournir une distribution incluant les outils les plus utilisés de la communauté Nagios. FAN est un CD-ROM distribué au format ISO.
Ajouté à ceci, un large panel d'outils est inclus dans cette distribution facilitant ainsi la mise en œuvre d'une plate-forme de supervision efficace.

2. Distribution

FAN est basé sur CentOS. Tous les « packages » CentOS étant disponibles, vous conservez tous les avantages de cette distribution avec les outils Nagios pré-installés et configurés pour vous.
Outils intégrés au projet :

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

3. Installation de CentOS

L'installation de FAN est identique à celle d'une distribution CentOS v5.6 classique. Celle-ci est plutôt rapide, intuitive et ne nécessite pas de commentaire. Une fois terminée elle occupe environ 1Go.
Depuis la version 2.2, FAN peut s'installer pour réaliser une supervision mono serveur (installation en mode standard) que pour une supervision distribuée (installation en mode distribuée).

3.1. Etapes d'Installation FAN(CentOS)

Voici les étapes de l'installation (qui sont identiques pour les 4 modes d'installation) :

Figure 4 : choix de Mode d'installation de Fan

Figure 5 : de choix de configuration clavier/disque d'installation/région

Figure 6 : de création de mot de passe pour l'accès à l'interface d'administration

3.2. Configuration interface réseau

Afin de pouvoir profiter de notre nouvelle plate-forme, il faut tout de même la configurer un minimum. Le minimum est la configuration réseau (adresse IP, routes, DNS…).
Les commandes suivantes permettent de configurer les interfaces réseau du serveur :

```
# system-config-network
```

Ou encore :

```
# vi /etc/sysconfig/networking/devices/ifcfg-eth0
# Realtek RTL8191SE Wireless LAN 802.11n PCI-E NIC
DEVICE=eth0
ONBOOT=yes
HWADDR=00:0c:29:72:44:a3
TYPE=Ethernet
NETMASK=255.255.255.224
IPADDR=10.10.10.152
GATEWAY=10.10.10.158
```

```
# service network restart
```

Juste après l'installation, tous les outils de supervisions sont installés et configurés (jusque là vous me direz, c'est le but ? ;)
Pour les plus pressés d'entre vous, vous pouvez accéder à la page d'accueil du projet (depuis un poste sur le réseau) : **http://ip-serveur/**

Figure 7 : Premier interface fan

Cette page d'accueil regroupe les différents services proposés pas FAN, il suffit de cliquer sur Nagios par exemple pour accéder à l'interface correspondante. Comme indiqué, le login/mot de passe par défaut est : **nagiosadmin/nagiosadmin**

4. Logiciels présents

4.1. NAgios

Nagios™ (anciennement appelé **Netsaint**) est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services que vous spécifiez, vous alertent ainsi des anomalies détectées et lorsqu'ils reviennent dans l'état nominal. . C'est un logiciel libre sous licence **GPL v2**.

C'est un programme modulaire qui se décompose en trois parties :

- Le moteur de l'application en charge d'ordonnancer les tâches de supervision l'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies les plugins, un ensemble de programmes que l'on peut compléter ou modifier en fonction des besoins de chacun pour superviser chaque service ou ressource disponible sur l'ensemble des ordinateurs ou éléments réseaux du si Offrant les possibilités suivantes :
- Superviser des protocoles réseaux : (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP, etc.) superviser les ressources des serveurs (charge du processeur, occupation des disques durs, utilisation de la mémoire paginée) et ceci sur les systèmes d'exploitations les plus répandus superviser via le protocole SNMP, notamment pour des équipements réseaux (Switch, Firewall), la supervision à distance en utilisant par exemple SSH ou un tunnel SSL.
- Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche : Scripts Shell (Bash, ksh, etc.) C++, Perl, Python, Ruby, PHP, C#, etc.
- La vérification des services se fait en parallèle, possibilité de définir une hiérarchie réseau pour différencier une panne serveur et un serveur injoignable, la notification d'alertes est entièrement paramétrable grâce à l'utilisation de plugins (alerte par email, SMS, etc.).
- Acquittement des alertes par les exploitants de la supervision.
- Gestion des escalades pour les alertes.
- Limitation de la visibilité, les utilisateurs peuvent avoir un accès limité à quelques éléments capacité de gestion des oscillations (nombreux passages d'un état normal à un état d'erreur dans un temps court) chaque test renvoie un état particulier :

  1. OK (tout va bien)
  2. WARNING (le premier seuil d'alerte est dépassé)
  3. CRITICAL (le second seuil d'alerte est dépassé ou alors le service a un problème)

4. UNKNOWN (impossible de connaître l'état du service)

Figure 8 : Premier interface nagios sur Fan

4.2. Centreon

Centreon fournit une interface de visualisation de la supervision différente de celle de **Nagios.**

Elle permet de rendre la consultation plus accessible à moyen de filtres de recherche, des graphes de métrologie, de reporting, d'une meilleure gestion des ACLs. Cette interface à l'avantage d'être plus dédiée à des personnes recherchent moins d'informations techniques, cependant elle ne remplace pas totalement l'interface de Nagios.

En juillet 2007, le logiciel **Oreon** change de nom pour devenir **Centreon.**

Ses fonctionnalités :

- Une interface multi-utilisateur intuitive et personnalisable.
- Une interface de configuration évoluée pour configurer le périmètre à superviser.
- Des aides à la configuration.
- Une gestion de l'ensemble des fichiers de configuration de Nagios (cgi, nagios.cfg...).
- Un module de chargement de configuration de Nagios.
- Une compatibilité Nagios 1.x, Nagios 2.x, Nagios 3.x.
- Un test de validité des configurations avec le debugger de Nagios.
- Des fiches d'identités serveurs/équipements réseaux regroupant les informations de base sur ces types de ressourcent.
- Des représentations graphiques élaborées et personnalisables sur la métrologie.

- Une gestion des accès très fine, comprenant les ressources comme les pages de l'interface.
- Un système de modules qui permet l'inclusion d'autres applications dans Centreon, par exemple le module syslog.
- Un compte-rendu complet sur les incidents.
- Un système de calcul de la qualité de service en temps réel avec alerte en cas de diminution de la qualité de service.
- Une map Java pour une vision simplifiée de l'état du système d'information.

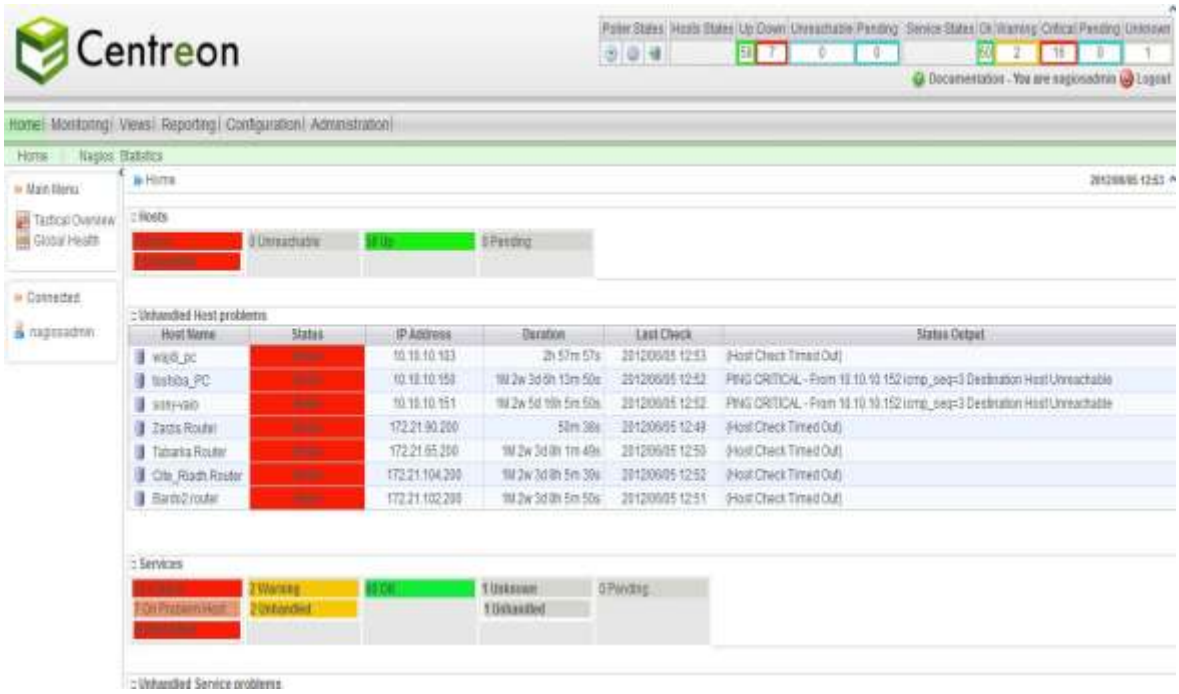

Figure 9 : Premier interface Centreon

4.3. Nagvis

Nagvis est un module de cartographie. Il permet de créer des vues « métiers » de la supervision. Il est possible de coupler Nagvis à un schéma réseau et ainsi mettre en relation les données de Nagios en temps réel sur le schéma. Nagvis utilise la base NDOUtils pour récupérer les données de supervision.

Il supporte aussi les moteurs évènements Mklivestatus, ndo2fs, merlin Son principal atout réside dans son système de Drag and Drop pour venir configurer ses cartes.

Figure 10 : Exemple de schéma Nagvis

4.4. Utilisation de Centreon

Centreon est une belle couche d'administration Web à ajouter à votre serveur Nagios (si vous êtes allergiques à la ligne de commande Unix). Cependant la prise en main de Centreon peut s'avérer difficile vu l'absence de guide utilisateur digne de ce nom...

Avant de commencer, il faut vous assurer d'avoir **une configuration Nagios/Centreon** en état de marche...

Nous allons donc dans ce billet dérouler un cas d'école: l'ajout d'un "host" de **type serveur** Linux et d'un "service" HTTP pour la **supervision** d'un serveur Web Apache.

c. Ajout d'un "host"

Nous allons ajouter un host de type serveur Linux à notre configuration Nagios.

On va pour cela dans le menu **Configurer** / **Hosts** et on clique sur le bouton **Add**:

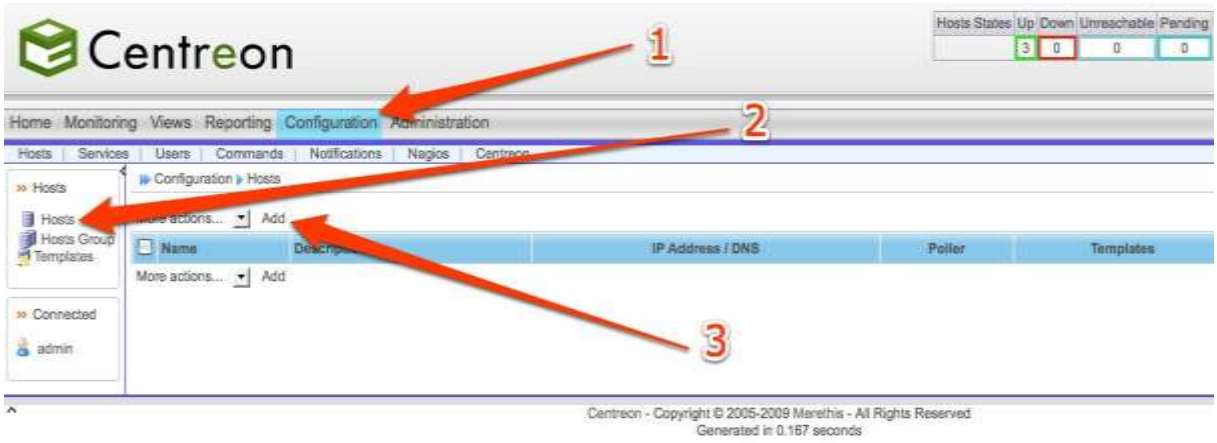

Figure 11: Ajout d'un host étape 1

Ensuite, on entre les caractéristiques propres du serveur (1):

- Son nom ("host name"): www
- Sa description ("Alias"): Serveur Web
- Son adresse IP/DNS: www.mondomaine.com

On clique ensuite sur le bouton + pour ajouter un template associé a cet "host" (2). Pour rappel, un template est la centralisation de caractéristiques communes à des machines.

Puis on sélectionne le template (3): **Servers-Linux**

Enfin, on clique sur le bouton **Save** (4).

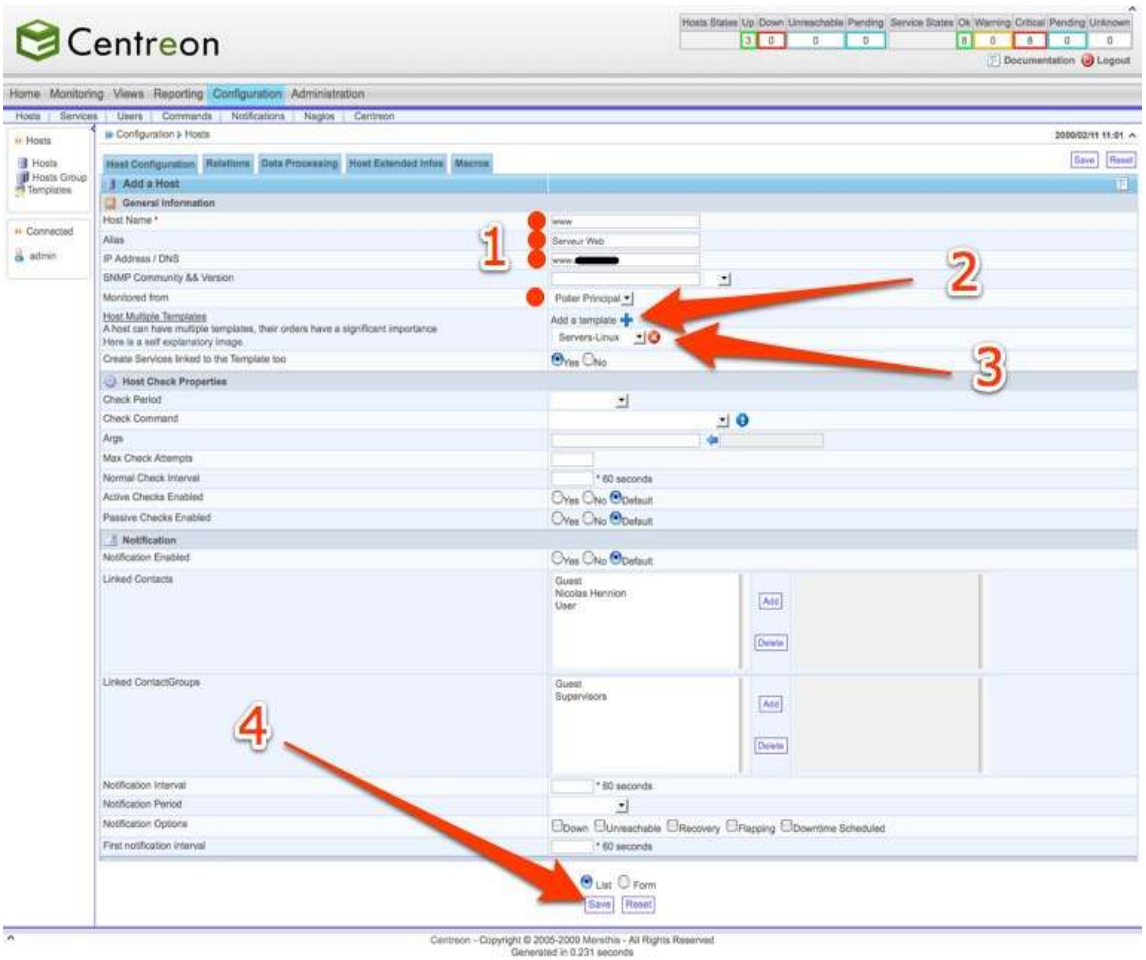

Figure 12: Ajout d'un host étape 2

A ce stade, l'host" www est dans la configuration de Centreon.

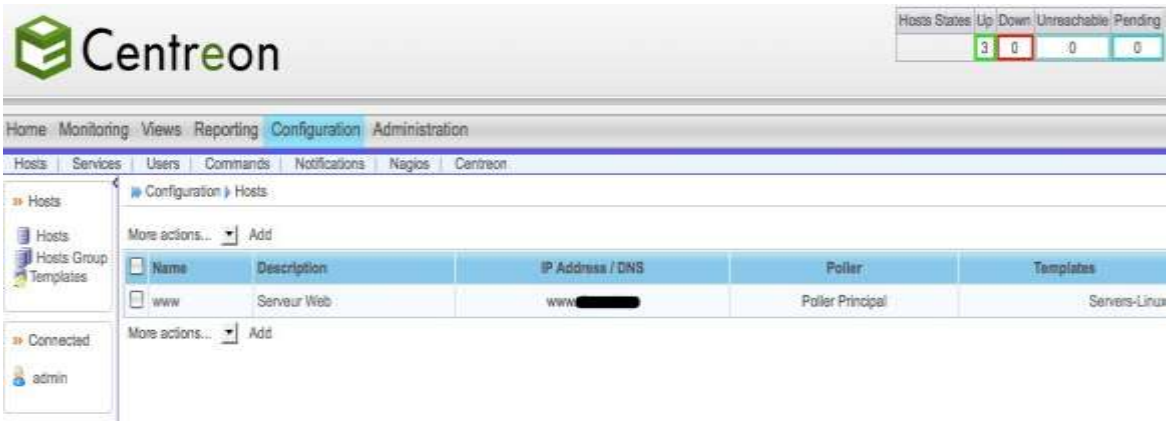

Figure 13: Ajout d'un host étape 3

d. Ajout d'un service

Nous allons ajouter un host de type Nous allons poursuivre notre exemple par l'ajout d'un "service" pour superviser un serveur Web hébergé sur notre "host" www. Pour cela, il faut se rendre dans les menus Configuration / Service.

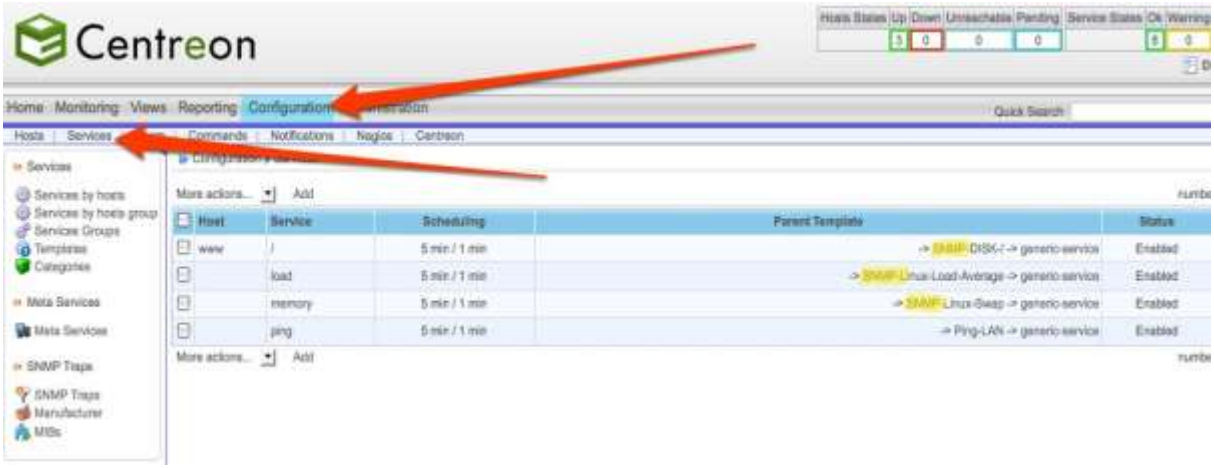

Figure 14: Ajout d'un service étape1

Comme on peut le voir, Centreon à créé des services par défaut (associé au Template par défaut) permettant de superviser par SNMP certains services (disque, charge, swap) de notre serveur. Pour que cela fonctionne, il faut bien évidemment qu'un **serveur SNMP soit lancé et configuré** sur la machine "host" www. Dans notre exemple, nous voulons seulement surveiller la présence d'un serveur Web, nous allons donc supprimer ces services de notre configuration Nagios:

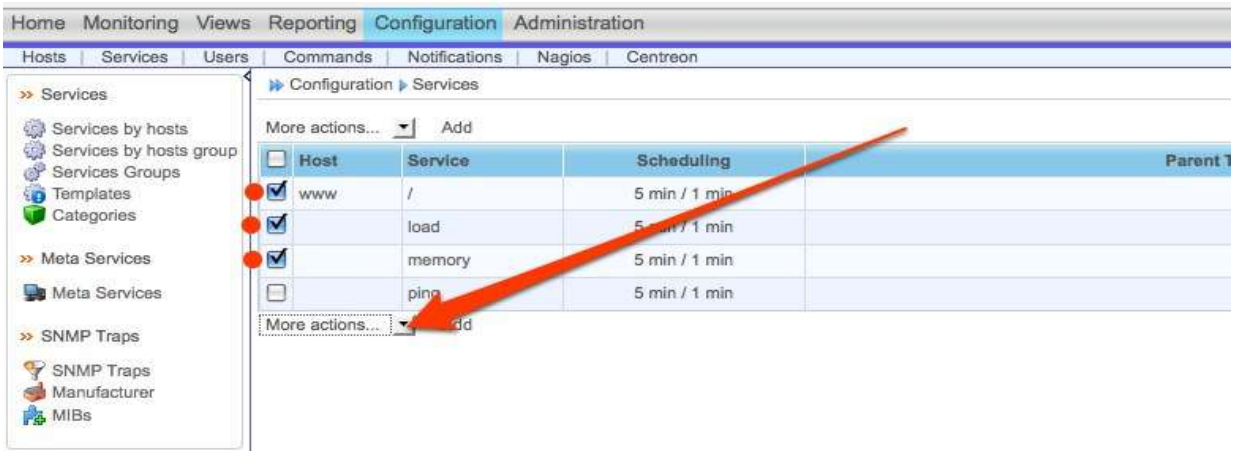

Figure 15:Ajout d'un service étape 2

Puis:

Figure 16: Ajout d'un service étape 3

On peut ensuite ajouter notre nouveau service en cliquant sur le bouton **Add**:

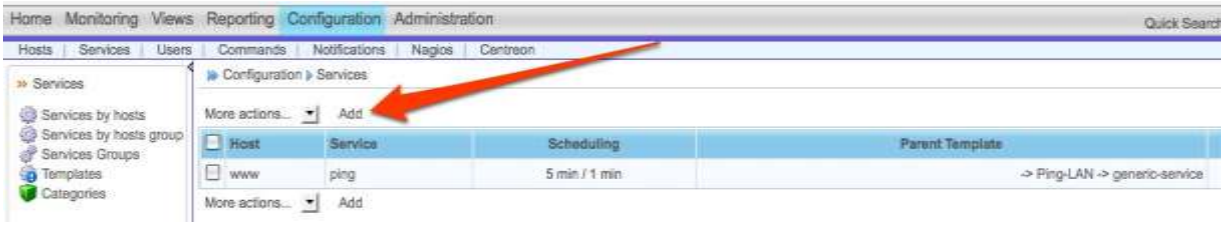

Figure 17: Ajout d'un service étape4

Nous allons commencer par saisir:

- le nom du service: Serveur HTTP (1)
- le template associé: generic-service (2)

Il est possible de voir le contenu d'un template en cliquant sur le bouton à droite du menu déroulant:

Figure 18: Ajout d'un service étape 5

Ce qui va afficher:

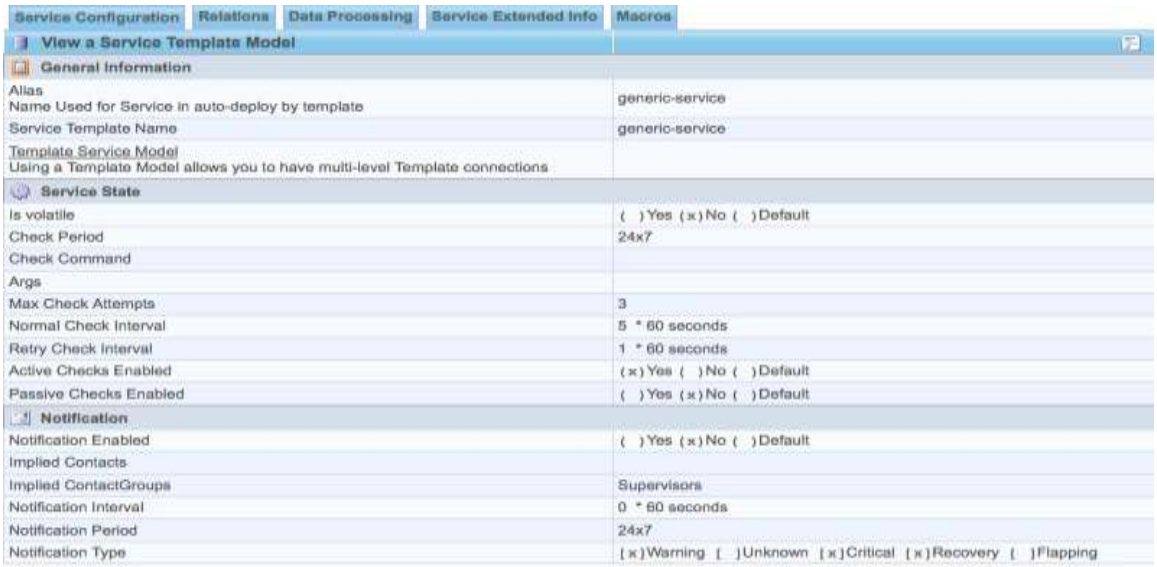

Figure 19: Ajout d'un service étape 6

- Le plugin à appeler pour ce service: **check_http** (3)

On clique ensuite sur le menu Relations (4) pour associer notre "service" au "host"

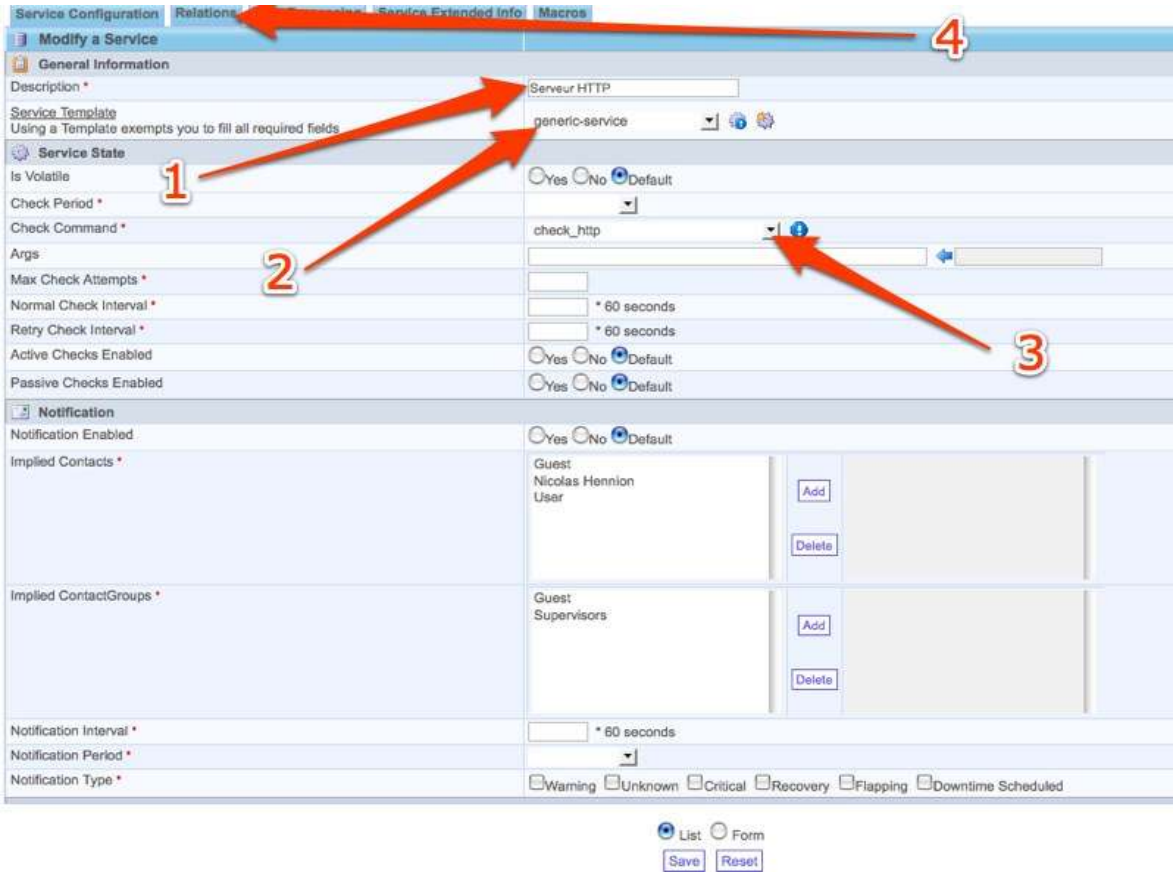

Figure 20: Ajout d'un service étape7

On ajoute donc le "host" www à la liste des hosts associés à ce service:

Figure 21: Ajout d'un service étape 8

On finalise en cliquant sur le bouton Save:

Figure 22: Ajout d'un service étape 9

Le service est maintenant présent dans la configuration de Centreon.

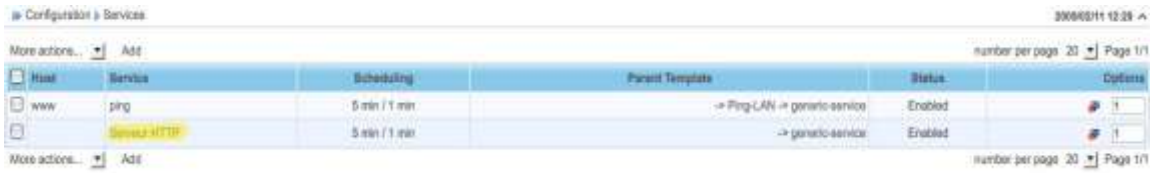

Figure 23: Ajout d'un service étape 10

Notre configuration n'est pas encore supervisé, Centreon ne fait pas la supervision, c'est Nagios qui s'occupe de ces tâches. Il faut donc exporter la nouvelle configuration sur notre serveur Nagios.

4.5. Exportation de la configuration vers Nagios

Il faut pour cela, aller dans le menu Configuration / Nagios / Génération (1 / 2) puis cliquer sur les boutons:

- "Move export files": pour déplacer physiquement les fichiers de configuration dans l'arborescence Nagios.
- "Restart Nagios": pour demander à Centreon de redémarrer Nagios pour que la configuration soit prise en compte. Puis cliquer sur Export (3)

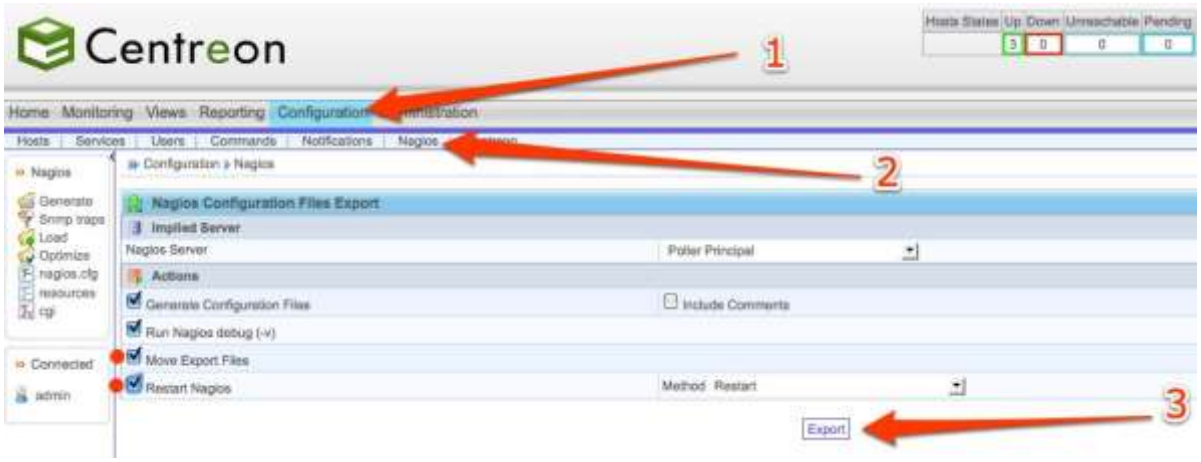

Figure 24:Ajout d'un service étape 11

Si tout ce passe bien, vous ne devriez pas avoir de message d'erreur mais seulement:

Figure 25: Ajout d'un service étape 12

Quelques minutes après l'exportation, la nouvelle configuration apparaitra dans l'interface de Centreon:

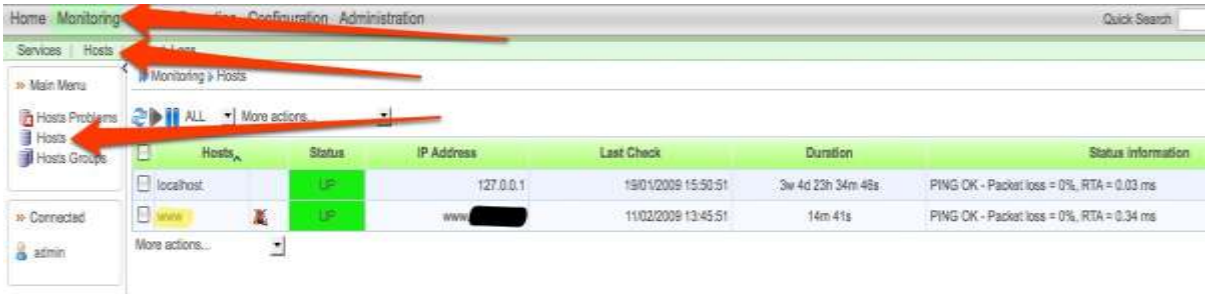

Figure 26: Ajout d'un service étape13

Chapitre IV: Les compléments de Nagios

1. Introduction

Dans ce chapitre nous vais présenter tout outils ou compléments que nous 'envisageons ajouter à Nagios 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.

2. NDOutils

2.1. Utilités

Il faut d'abord savoir que lorsque les greffons effectuent des tests, ils retournent au processus/ordonnanceur Nagios, deux types de données qui sont les états des hôtes et leurs services, ainsi que les données de performances qui par la suite seront enregistrées dans des fichiers plats.

Pour obtenir une information Nagios est obligée de lire et traiter ces fichiers en entier. Aussi chaque rafraichissement d'une page web depuis l'interface de Nagios implique une analyse complète de ces fichiers.

NDOutils vient alors optimiser l'exploitation de ces données en les exportant vers une base de données MySQL, ce qui a les avantages suivantes :

- Stockage des données à long terme.
- Permettre à un logiciel tiers comme « Centreon » d'accéder de manière optimisée aux données d'états et performances de Nagios et de partager ses données.
- Optimisation de l'exploitation des données et amélioration des performances il est plus rapide de rechercher des informations dans une base de données structurée, plutôt que dans un fichier de journalisation qu'il faut parcourir entièrement à chaque utilisation.

2.2.Présentation

NDOutils est un greffon chargé de transmettre les données remontées par Nagios (configuration des serveurs supervisés, les états des hôtes, les données de performance…) vers une base de données MySQL plutôt que de ne les garder que dans les fichiers plats.

De cette façon, les données seront plus souples à gérer. Grace à la possibilité de stockage à long terme, les données sont facilement exploitées et l'information devient aisément transformable de la manière que l'on souhaite.

NDOutils interagi avec Nagios indépendamment de Centreon.

2.3. Architecture

NDOutils se compose de deux modules :

- **Ndomod :** lancé automatiquement avec Nagios et responsable de l'exportation des données extraits des fichiers plats pour les déposer dans un socket (Unix, tcp).
- **Ndo2db :** démon nécessitant un script d'initialisation et responsable de l'ouverture de socket (Unix ou TCP) et place les données trouvées dans une base de donnée MySQL.

3. Centreon

3.1. Utilités

Sans aucun doute, Nagios est considéré comme étant une solution très puissante. Cependant, on peut lui reprocher d'être très compliquée à configurer vu le nombre important de fichiers dont elle dispose.

La modification manuelle de ces fichiers de configurations, à chaque ajout une hôte, un service, une commande.., augmentera le risque d'affronter beaucoup plus d'erreur.

On a donc choisi de coupler Nagios à Centreon pour remédier à ce problème en évitant la Modification à la main de ces fichiers textes. Centreon n'ayant pas seulement le grand avantage de gérer automatiquement les nombreux fichiers de configuration de Nagios mais aussi une interface multiutilisateurs, intuitive et personnalisable avec intégration des droits d'accès en plus d'un compte rendu graphique plus pratique et élégant que celui offert par Nagios.

3.2. Présentation

Centreon est une couche applicative Web venant se greffer à Nagios pour offrir une administration moins rudimentaire basée sur deux fonctionnalités principales :

- **Une seconde interface de monitoring :** Centreon propose une interface plus sobre, ainsi qu'une façon différente de traiter les données remontées par Nagios.
- **Puissante interface de configuration :** Centreon autorise en effet à l'utilisateur de modifier intégralement la configuration de Nagios depuis son navigateur internet, plutôt qu'en modifiant manuellement les fichiers éparpillés sur le disque.

Cet outil utilise ses propres bases de données MySQL crées automatiquement lors de son installation pour récupérer toutes les données d'états et de performances de Nagios pour les traiter et les afficher dans sa propre interface graphique.

Cet outil construit ses propres graphiques grâce aux RRD Tools, des bases de données particulièrement adaptées à la construction graphique.

3.3. Architecture

❖ **Centreon et Base de données**

Centreon interagit principalement avec la base de données MySQL pour remonter les données fournies par Nagios et stockées dans la base grâce à NDO.

Lors de son installation Centreon crée automatiquement trois schémas dans la base de Lors de son installation Centreon ainsi que trois schémas dans la base de données MySQL :

➢ **Centstatus:** C'est la base dans laquelle NDOUtils stocke les données extraites des fichiers plats de Nagios et sur laquelle Centreon pointe pour pouvoir remonter les mêmes données.

Ces données sont visualisées dans l'interface monitoring de Centreon.

➢ **Centstorage:** Traite et stocke les données de performances remontés de Nagios via NDOUtils vers la base de données MySQL, avant leurs intégration en base RRD. Responsable de la création des parties métrologiques de Centreon qui sont le reporting et la génération des Graphs.

Ces données sont visualisées dans la partie « Reporting » et « Views » de Centreon.

➢ **Centreon:** Collecte les informations de configuration, et stocke les fichiers objets de Nagios (Host, Services, Périodes, etc...). Grâce aux fonctions d'Import/Export, Centreon peut générer de nouveaux fichiers de configuration pour Nagios.

❖ **Centreon et démons :**

Pour un fonctionnement sain, Centreon a besoin que ses deux démons soient lancés :

➢ **Centstorage :** Centstorage est l'outil qui exploite les données remontées par Nagios pour Centreon. C'est un programme écrit en Perl, associé à Centreon. A chaque modification du fichier de données perfdata, centstorage met à jour deux bases de données « Centstorage » et « RRD ».

➢ **Centcore :** Dans le cas où l'architecture adoptée est distribuée (serveur centrale pour la Supervision et d'autres serveurs fils), Centcore permettra à cette architecture de bien communiquer ensemble, en se chargeant de la transmission des données entre ses différents serveurs. Aussi Responsable du déploiement de la configuration de Centreon vers Nagios.

4. NRPE pour la supervision des serveurs Linux

4.1. Présentation

NRPE (**N**agios **R**emonte **P**lugin **E**xécuter) est un agent de supervision qui vous permet de récupérer les informations à distance lors de la supervision d'un serveur Linux. Il a le grand

avantage d'exécuter les commandes dans la machine à superviser ce qui lui permet ainsi de répartir les charges.

Il est livré avec un ensemble de commandes check définis par défaut dans son fichier de Configuration et nécessite l'installation des plugins Nagios aussi.

- **NRPE** : Ce programme tourne en tâche de fond sur la machine distante et traite les requêtes d'exécution venant du plugin **check_nrpe** sur l'hôte Nagios.

Lorsqu'il reçoit une requête d'un hôte autorisé, il exécute la ligne de commande associée (les Paramètres) avec la commande reçue et envoie le résultat de l'exécution.

- **check_nrpe :**

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

4.2. Architecture

NRPE se base sur une architecture client/serveur (Figure 11). La partie cliente nommée **check_nrpe**, doit être disponible sur le serveur Nagios et on doit vérifier son existence parmi les plugins délivrés avec Nagios-plugins sinon l'installer. La partie serveur NRPE est à installer sur chacune des machines Windows à surveiller.

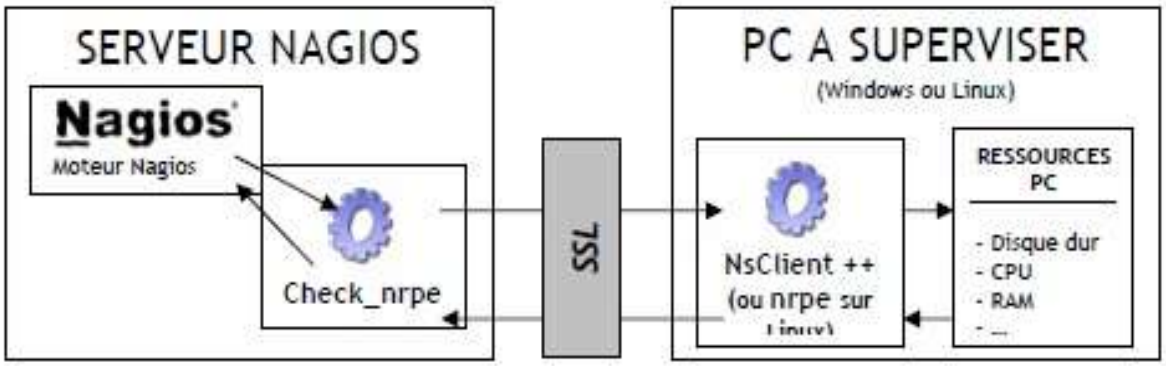

Figure 27 : Mécanisme du NRPE

Lorsque Nagios veut connaître une information sur un PC, il exécute le plugin check_nrpe. Celui envoie une requête au PC. Sur le PC, le programme NsClient++ (ou nrpe si linux) Reçoit la requête, va chercher les informations dans les ressources du PC et renvoie le résultat au serveur Nagios.

Usage :

Pour aller chercher les informations sur un PC grâce à check_nrpe, Nagios exécute une Commande ayant la syntaxe suivante :

Check_nrpe -H <adresse de l'hôte à superviser> **-c** <nom de la commande à exécuter sur le serveur>

Puis sur les postes à superviser, dans le fichier de configuration (NSC.ini pour Windows,

Nrpe.conf pour Linux), on doit définir la commande à exécuter pour chaque nom de commande.

Exemple pour Linux:

Command [check_cpu]=/usr/local/nagios/libexec/check_load -w 15, 10,5 -c 30, 25,20

Procédure de fonctionnement :

- Le serveur Nagios demande l'exécution d'un plugin sur la machine distante.
- Le daemon NRPE hébergé sur la machine distante, reçoit la requête d'exécution du plugin.
- Le plugin est exécuté sur la machine distante.
- Le daemon NRPE de la machine distante envoie le résultat du plugin au serveur Nagios.
- Le serveur Nagios interprète les résultats reçus.

4.3. Compilation

On a compilé NRPE et le plugin check_nrpe avec les commandes suivantes:

. /configure

Make all

Les binaires seront placés dans le répertoire src/.

NOTE: Comme le plugin check_nrpe plugin et le démon nrpe tournent sur deux machines Différentes. (Le plugin sur l'hôte Nagios et check_nrpe sur la machine distante), il nous faudra compiler le démon nrpe sur la machine cible distante.

4.4. Installation

Le plugin check_nrpe doit être placé sur l'hôte Nagios avec les autres plugins. Dans le répertoire /**usr/local/nagios/libexec**.

4.5. Exécution sous XINETD

On ajoute la ligne suivante à notre fichier **/etc/services** :

Nrpe 5666 /tcp # NRPE

On ajoute des entrées pour le démon NRPE par création du fichier "nrpe" dans le répertoire **/etc/xinetd.d** ; et nous devons donner le code ci-dessous:

Service nrpe

{

Flags = REUSE

Socket type = stream

Wait = no

Use = nagios

Server = <chemin d'accès à nrpe>

Server_args = - c </usr/local/Nagios/etc/>

log_on_failure += USERID

Disable = no

only_from = 127.0.0.1 <ip_nagios_machine>

}

→ Enfin on redémarre xinetd avec les commandes suivantes :

/etc/rc.d/init.d/xinetd restart

Configuration sur l'hote NAGIOS

Pour pouvoir utiliser check_nrpe depuis Nagios, il fait modifier son fichier de configuration.

Nous avons défini la commande suivante:

Define command {

command_name check_nrpe

Command line /usr/local/nagios/libexec/check_nrpe -H $HOSTADDRESS$ -c $ARG1$

}

Pour tout service utilisant l'ensemble plugin/démon NRPE et désirant exploiter leurs résultats,

Nous sommes obligées de définir la section "vérification du service" de cette manière :

Define service {

host_name Serveur_fujutsu_simens_primaryg_tx200s3

Service_description mémoire utilisée

```
        Use                         generic-service
        check_command               check_df
        max_check_attempts          5
        normal_check_interval       3
        retry_check_interval        1
        Check_period                24x7
        first_notification_delay    60
        Notification_options        w
}
```

Il va falloir créer et éditer plusieurs fichiers de configuration avant de pouvoir surveiller quoique ce soit. Ce travail est décrit ci-dessous.

4.5.1. Fichier de configuration principal

Le fichier de configuration principal : ***/usr/local/nagios/etc/nagios.cfg*** contient un certain nombre de directives qui affectent la manière dont Nagios fonctionne.

Ce fichier est lu par le processus Nagios et par les CGIs.

On va maintenant indiquer des chemins et des informations qui seront indispensable au fonctionnement de Nagios :

Le code écrit.	**Explication.**
log_file=/usr/local/nagios/var/nagios.log	On défini dans cette variation déterminante le chemin d'accès au fichier journal principal de Nagios.
cfg_file=/usr/local/nagios/etc/commands.cfg	Nous devons donner pour cette variable les fichiers de configuration des objets que Nagios doit utiliser pour la supervision.
cfg_file=/usr/local/nagios/etc/contacts.cfg	
cfg_file=/usr/local/nagios/etc/hosts.cfg	
cfg_file=/usr/local/nagios/etc/services.cfg	
nagios_user=Nagios	Par ceci on détermine qui est le propriétaire du processus Nagios.
nagios_group=nagios	
temp_file=/usr/local/nagios/var/nagios.tmp	C'est un fichier que Nagios crée périodiquement durant la mise à jour des données, des données d'état etc..
log_archive_path=/usr/local/nagios/var/archives	C'est le répertoire où on veut enregistrer les fichiers journaux
use_syslog=1	On journalise ici les messages via l'utilitaire système Syslog.

execute_service_checks=1	On impose à Nagios d'effectuer les contrôles des services et des hôtes.
execute_host_checks=1	
enable_notifications=1	On cherche par cette option si Nagios envoie ou non une notification.
enable_event_handlers=1	Par cette option on oblige Nagios à activer les gestionnaires d'événement.

Tableau 2 : Explication des ajouts sur Nagios.cfg

4.5.2. Définitions de quelques hôtes

Fichier Hosts.cfg :

Le code écrit.	**Le code écrit.**
define host{	**define host{**
host_name serveur_siemens_primaryg_tx200S3	**host_name Serveur_mail_cnam**
alias Serveur linux	**alias Serveur linux**
address x.xxx.xxx.xxx	**address xxx.xxx.xxx.xxx**
check_command check-host-alive	**check_command check-host-alive**
max_check_attempts 5	**max_check_attempts 5**
notification_interval 13	**notification_interval 13**
notification_period 24x7	**notification_period 24x7**
notification_options d,u,r	**notification_options d,u,r**
contact_groups admin	**contact_groups admin**
}	**}**

Tableau 3 : Exemple de définition d'un hôte à superviser.

Explication du code écrit :

***Host_name* :** C'est le nom court qui permet d'identifier l'hôte, La macro $**HOSTNAME$** contient ce nom court.

***Alias*:** C'est un nom long ou une description de l'hôte permettant de l'identifier plus facilement.

La macro **$HOSTALIAS$** contient cet alias/description.

Address : Cette directive définit l'adresse de l'hôte. C'est normalement une adresse IP, La macro **$HOSTADDRESS$** contient cette adresse.

***Parents* :** Cette directive définit une liste de noms courts d'hôtes "parents" de cet hôte, séparés par des virgules. Les hôtes parents sont généralement des routeurs, des commutateurs, des

firewalls, etc. se trouvant entre l'hôte de supervision et les hôtes distants. Le plus proche de l'hôte distant est considéré comme le parent de cet hôte.

Check_command **:** Cette directive définit le nom court de la commande à utiliser pour déterminer si l'hôte est hors service ou non. Typiquement, cette commande lance un "**Ping**" vers l'hôte pour voir s'il est "vivant". La commande doit retourner un état **OK** (0) sinon Nagios supposera que cet hôte est hors service.

Max_check_attempts : Cette directive définit le nombre de fois ou Nagios relancera la commande de contrôle de l'hôte si celle-ci retourne un état différent d'OK. Si on positionne cette valeur à 1 entraînera Nagios à générer une alerte sans re-contrôler l'hôte.

contact_groups : Ceci est une liste de noms courts de groupes de contacts qui devront être notifiés lorsqu'il y aura des problèmes avec cet hôte. Les multiples groupes de contacts devront être séparés par des virgules.

notification_interval **:** Cette directive définit le nombre d'unités de temps à patienter avant de re-notifier un contact que l'hôte est toujours hors service ou inaccessible.

notification_period **:** Cette directive définit le nom court de la période durant laquelle les notifications d'événements concernant cet hôte peuvent être émises vers les contacts. Si un hôte est hors service, inaccessible, ou se rétablit en dehors de la période de notification, aucune notification ne sera envoyée.

notifications_options **:** Cette directive définit quand les notifications pour cet hôte doivent être

Envoyées. Les options valides sont une combinaison d'une ou plusieurs des valeurs suivantes : : **d** = envoi de la notification pour un état **DOWN**, **u** = envoi de la notification pour un état **UNREACHABLE, r** = envoi de la notification pour le retour à la normale (état **OK**) et **f** =envoi d'une notification lorsque l'hôte commence ou arrête d'osciller. Si nous spécifions la valeur **n (none)**, aucune notification ne sera envoyée. Exemple: avec les valeurs **d,r** dans ce champ, les notifications seront envoyées quand l'hôte sera **DOWN** et quand il sortira de cet état pour un état OK.

4.5.3. Définition de quelques Services

Fichier Services.cfg :

Le code écrit.	Le code écrit.
define service { **host_name** **service_description PING** **is_volatile 0** **check_period 24x7** **max_check_attempts 3** **normal_check_interval 5** **retry_check_interval 1** **contact_groups admin** **notification_interval 900** **notification_period 24x7** **notification_options c,r** **check_command check_ping !3000.0,20%!5000.0,95%**	**define service {** **host_name** **serveur_siemens_primaryg_tx200S3** **use** **generic-service** **service_description charge CPU** **check_command** **check_nrpe!check_load** **}**

Tableau 4 : Exemple des services à superviser.

Explication du code écrit :

***service_description* :** Cette directive définit la description du service qui peut contenir des espaces, tirets, et deux-points. Deux services associés au même hôte ne peuvent pas avoir la même description. Les services sont identifiés uniquement avec les directives host_name et **service_description**.

***check_command* :** Cette directive est utilisée pour spécifier le nom court de la commande que Nagios exécutera pour déterminer l'état du service.

***max_check_attempts* :** Cette directive définit le nombre de fois que Nagios réessayera de contrôler le service si celui-ci retourne un état différent de **OK**. Si on positionne une valeur de 1 à cette variable, Nagios générera une alerte sans nouvel essai.

***normal_check_interval* :** Cette directive définit le nombre d'unités de temps à attendre avant d'ordonnancer le prochain contrôle régulier du service.

***retry_check_interval*:** Les services sont réordonnancés à cet intervalle quand ils sont passés dans un état différent de **OK**.

***check_period* :** Cette directive définit le nom court de la période de temps durant laquelle un contrôle actif peut être effectué.

***notification_interval* :** Cette directive définit le nombre d'unités de temps à patienter avant de notifier à nouveau un contact que le service est toujours hors service ou inaccessible.

***notification_period* :** Cette directive définit le nom court de la période durant laquelle les notifications d'événements concernant ce service peuvent être émises vers les contacts.

notification_options **:** Cette directive définit quand les notifications pour ce service doivent être envoyées. Les options valides sont une combinaison d'une ou plusieurs des valeurs suivantes **: w =** envoi de la notification pour un état **WARNING, u** = envoi de la notification pour un état **UNKNOWN, r** = envoi de la notification pour le retour à la normale (état **OK**) et **f** = envoi d'une notification lorsque le service commence ou arrête d'osciller.
Si nous spécifions la valeur n (none), aucune notification ne sera envoyée. .
contact_groups **:** C'est une liste de noms courts de groupes de contacts, séparés par des virgules, qui doivent être notifiés des problèmes ou rétablissements de ce service.

4.5.4. Définition de quelques Commandes

Fichier commands.cfg :

Le code écrit.	Explication.
define command{ **command_name check_http** **command_line $USER1$/check_http -H $HOSTADDRESS$** **}**	***command_line*****:** Cette directive définit ce qu'exécute Nagios lorsque la commande est utilisée pour un contrôle de service ou d'hôte, pour une notification, ou pour un gestionnaire d'événement. Avant que la ligne de commande ne soit exécutée, toutes les macros sont remplacées par leur valeur.
define command{ **command_name check_ftp** **command_line $USER1$/check_ftp -H $HOSTADDRESS$** **}**	
define command{ **command_name check_ping** **command_line $USER1$/check_ping –H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5** **}**	

Tableau 5 : Exemples de commandes à superviser.

5. Conclusion

Le but de ce chapitre était de présenter les compléments que nous avons choisir à Nagios. Certains ont été choisis pour leur nécessité comme les greffons NRPE, et d'autres participaient surtout à l'amélioration de la manipulation et l'utilisation de Nagios, et surtout facilité de sa configuration.
Le chapitre suivant entamera l'aspect technique de notre projet, de la mise en place jusqu'aux Exemples d'utilisations.

Chapitre V: Mise en place du système de supervision

1. Environnements de mise en place :

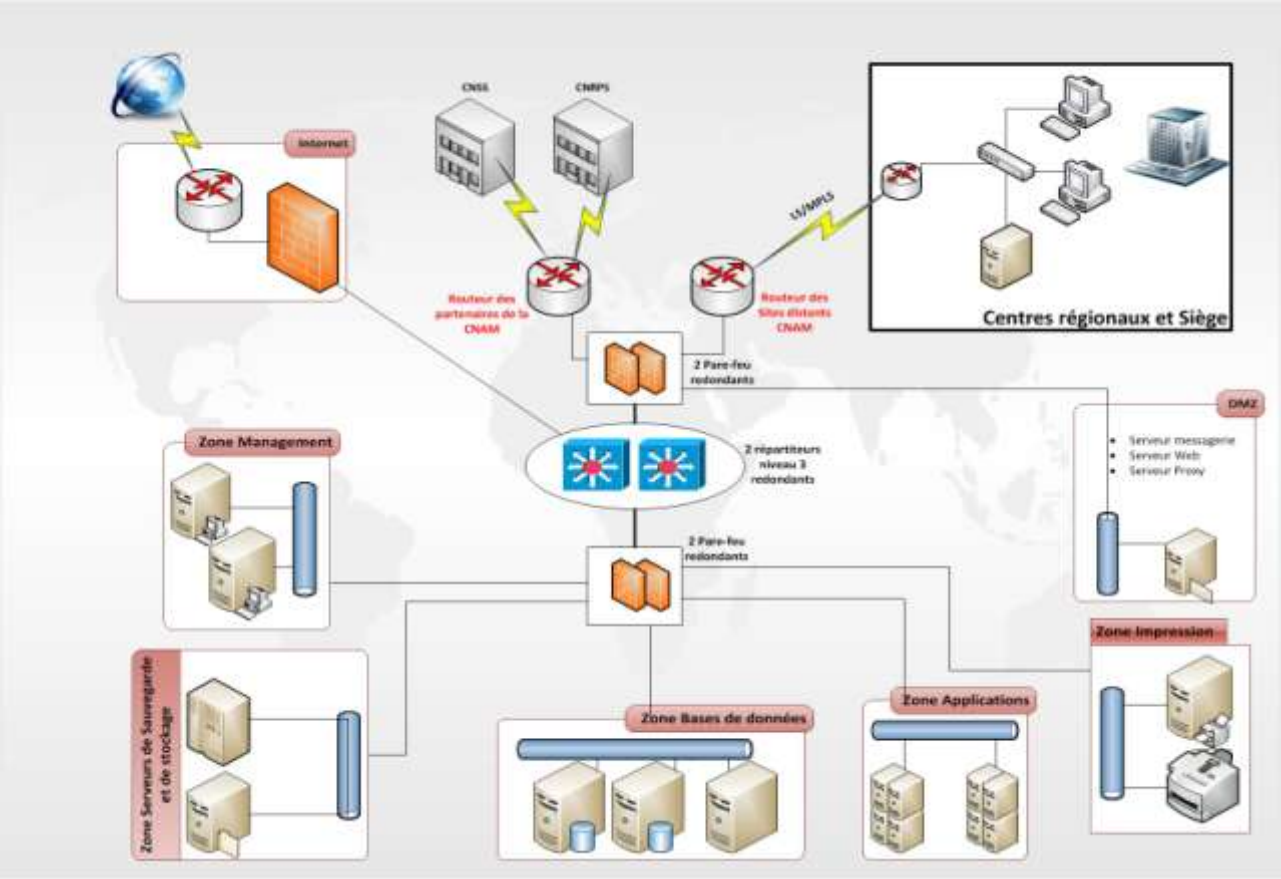

Figure 28 : Architecture de la CNAM

Ci-dessus, l'architecture simplifié du réseau de l'entreprise CNAM en Tunisie qu'ils sont besoin d'une solution pour la supervision de cette énorme architecture. Dans ce cas nous avons besoin d'une installation d'un serveur nagios pour superviser les ressources et les équipements réseaux locaux et des cites régionaux distant.

1.1 Environnement matériel

- **Phase de test :**

En cours de cette phase, j'ai installé une machine virtuelle sur une machine de test pour se familiariser avec la solution choisie et pour décortiquer toutes les fonctionnalités possibles offerte par cette solution. J'ai réussi à faire quelques essais sur des serveurs de tests. A ce stade là, je suis prêt à passer à la phase de production pour atteindre les objectifs de ce projet.

- **Phase de production :**

Avant de commencer cette phase, la CNAM j'ai mis en disposition un serveur de marque Fujitsu-Siemens et de modèle « Primergy TX200S3 » pour y installer nagios.

Les caractéristiques techniques de ce serveur est résumé dans le tableau suivant :

Caractéristique technique	Capacité
Nombre de processeurs physiques	2 processeurs
Mémoire	2 Go
Type de processeurs	Intel Xeon Quad-Core 3.0 GHz
Alimentation d'énergie	600 Watts
Mémoire interne maximale	16 GO
Nombre de disques	3 * 146 Go (SAS)
Contrôleur RAID	Oui (Contrôleur SAS)
RAID supportés	RAID 0 – 1 – 5 - 6
Nombre de carte réseaux	2 cartes réseaux (Gigabit) + 1 carte réseau de management
Alimentation redondante	Oui (double alimentation)
Ventilation redondante	Oui (double ventilation)

Tableau 6 : caractéristique technique du serveur Siemens

J'ai installé le système d'exploitation CentOS V5.6 sur ce serveur avec tous les outils nécessaires pour faire fonctionner notre solution (La procédure d'installation est décrite en détail dans le chapitre précédent). Les outils installés sont les suivants :

- L'outil de supervision Nagios-3.2.3.
- Les greffons de Nagios, Nagios-plugins-2.13
- La couche applicative associée à Nagios pour faciliter sa configuration et son administration Centreon-2.2.10
- Le plugin NRPE-2.13 pour la supervision des serveurs Linux.
- Nagvis pour la cartographie des adresses routeurs.

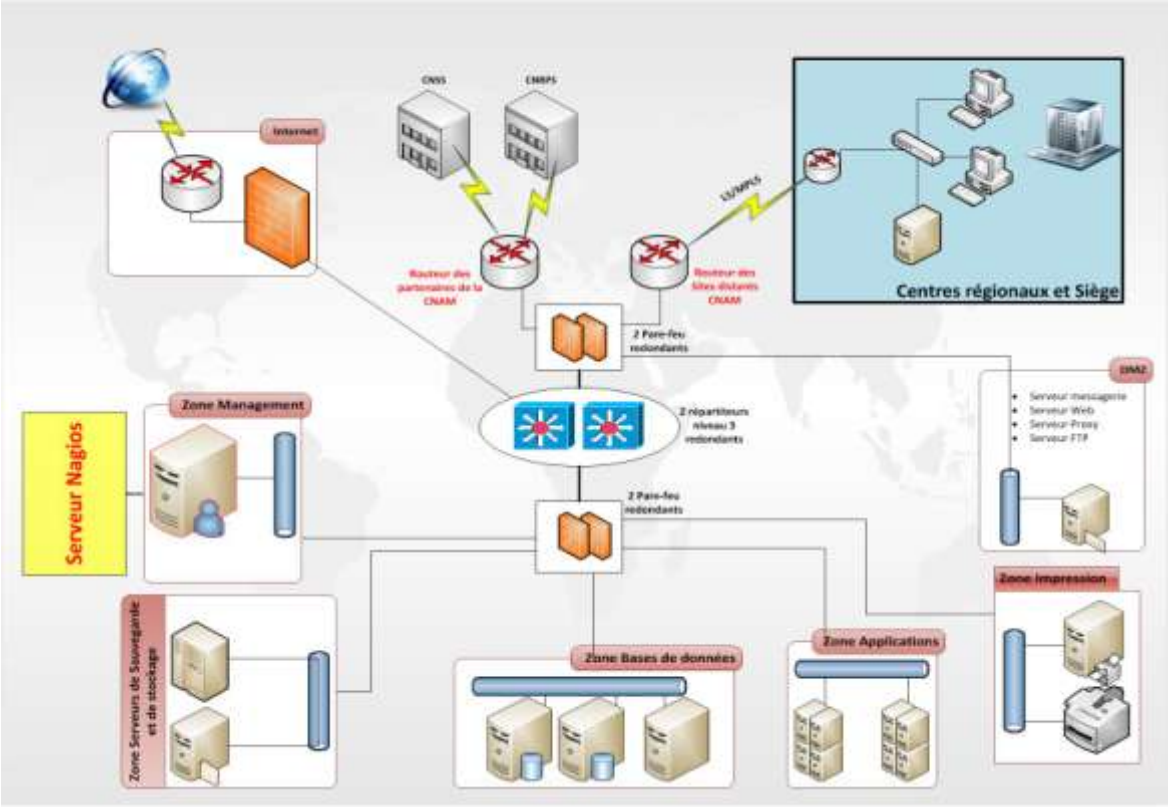

Figure 29 : Architecture de la solution de la supervision du réseau de la CNAM

Dans la zone de management j'ai installé un serveur Nagios pour éteindre l'objectif de la supervision dans le réseau de la CNAM, dans un premier lieu pour la supervision des serveurs locaux, comme tel que serveur de messagerie ou serveur de base de données en utilisant des regèles et des protocoles à superviser, dans un deuxième lieu pour superviser des équipements réseaux des centres et siège à distance tel que les routeurs les serveurs de d'applications etc.

1.2 Mise en place du serveur Nagios

Ci-dessus dans le dans le schéma précédent nous avons fait la mise en place du serveur dans sa zone (La zone de Management) pour éteindre l'objectif de la supervision.

a. Dégagement des besoins :

- Au niveau des centres régionaux on va superviser les serveurs et les routeurs aussi les débits réel entrant sortant avec les routeurs
- Coté site Central : Nous avons fait la supervision de quelques serveur tel que serveur de messagerie, serveur de base de données, serveur web …

b. Quels Services à superviser au niveau ?

Au niveau des centres régionaux :

Dans les centres régionaux les système d'exploitations installée sur les serveurs des centres sont de type linux RED HAT 5 dans lequel nous avons supervisé les services et les états des périphériques et aussi les autres équipements réseaux (Switch, Routeur) dans le tableau suivants :

Services	Etat
• Ping • SSH • SMB • Serveur anti virus Kaspersky • GFA (system de gestion d'appel au guichet CNAM)	• Etat CPU • Etat mémoire • Etat disque • Etat RAID • Vlan switch • Débit réel entrant sortant de routeur

Tableau 7: Les services et Les états supervisé

Ainsi la supervision d'état des routeurs par le service PING.

- Au niveau du Site central

Dans ce niveau on a réussit à faire la supervision de quelques services locaux des serveurs central par exemple

Serveur	Service supervisé
Serveur mail	Ping, Smtp, pop3
Serveur Web	Http,Https, Service Apache Tomcat port 8080
Serveur Base de données	Ping, Service Oracle à traves le port 1521

Tableau 8 : Tableau des serveurs supervisé

→ **Remarque** : on est arrivé à faire la supervision des ces services décrite dans les tableaux précédent grâce à des services locaux et des plugins installés par défauts dans la libraire de Nagios, aussi à travers l'installation de l'agent NRPE dans les serveurs distant à superviser ainsi avec le paquetage spéciale du serveur Fujitsu-Siemens « Primergy TX200S3 » avec le pack « *ServerView Linux Agent* » et aussi avec le paramétrage et la configuration nécessaire du pare-feu et proxy.

❖ **Installation de NRPE**[1]

Pour la supervision des serveurs Linux, je vais installer le greffon « NRPE-2.2 » sur la machine distante et vérifier la présence de la commande « check_nrpe » parmi les plugins installé de Nagios. Les étapes d'installation seront plus détaillées dans **l'Annexe A.**

❖ **Installation de *ServerView Linux Agent*** [2]

2. Interface de Nagios/Centreon

➢ **Tactical Overview**

La figure 13 est la première vue après l'authentification, elle nous propose l'essentiel des Informations importantes qui sont : l'état de fonctionnement du système d'information supervisé, le nombre d'alertes actuelles, etc.

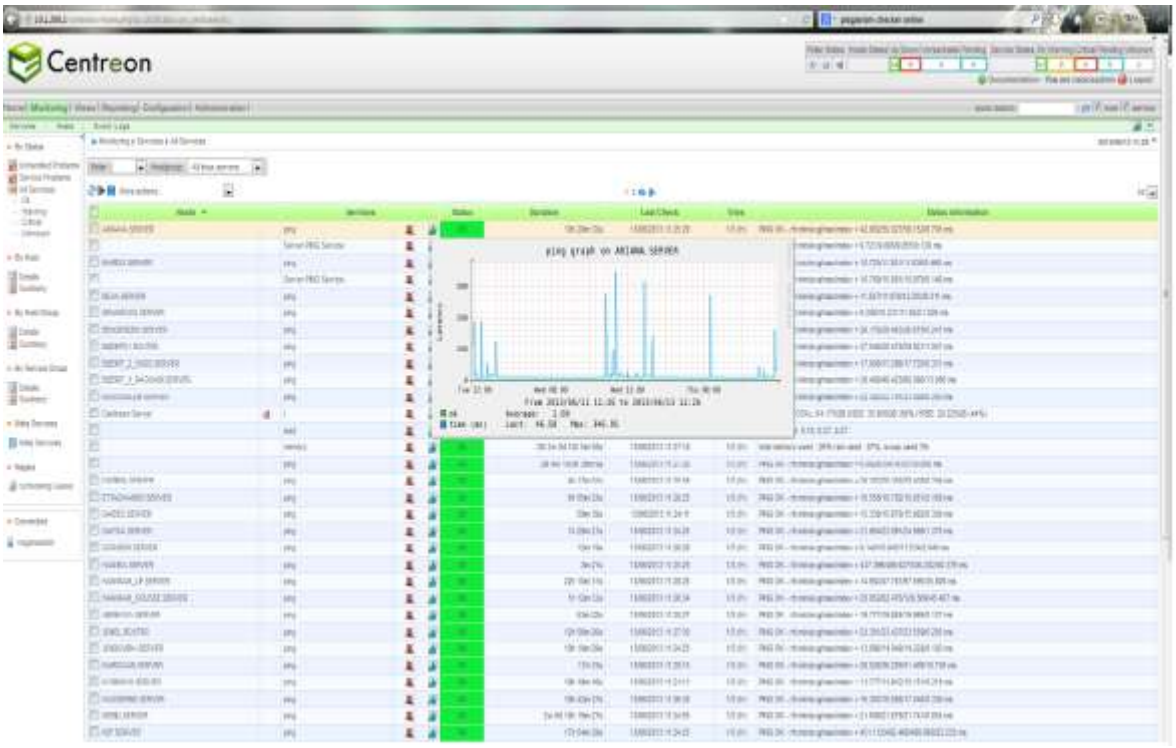

Figure 30 : Interface de Vue Globale

[1] VoirAnnexe A

[2] Voir Annexe B

- **Santé globale**

Cette vue nous permet d'avoir en représentation dite en "camembert", un état de santé globale de notre supervision.

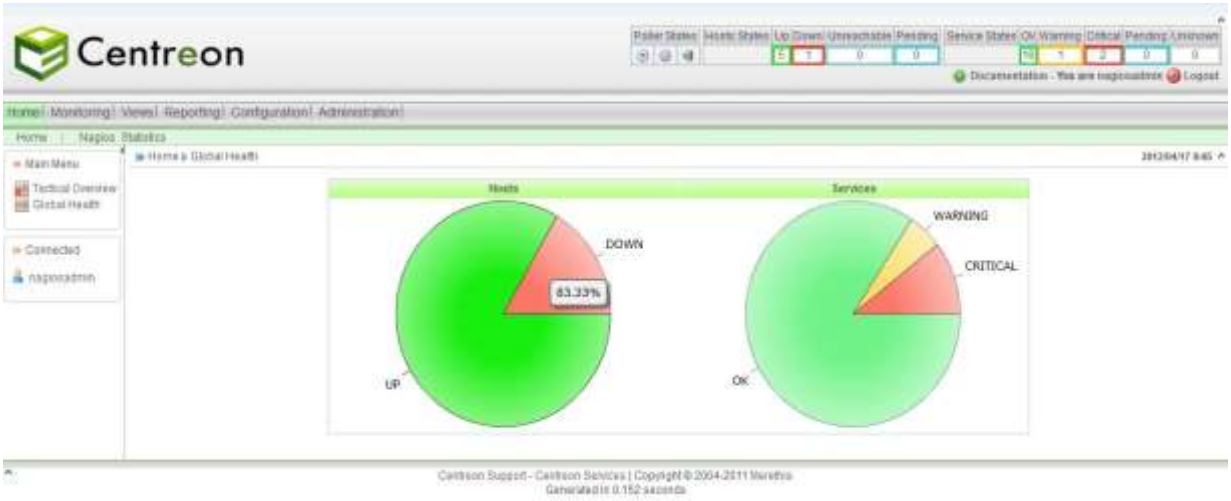

Figure 31 : Interface de la santé globale

- ***Graphique de performance***

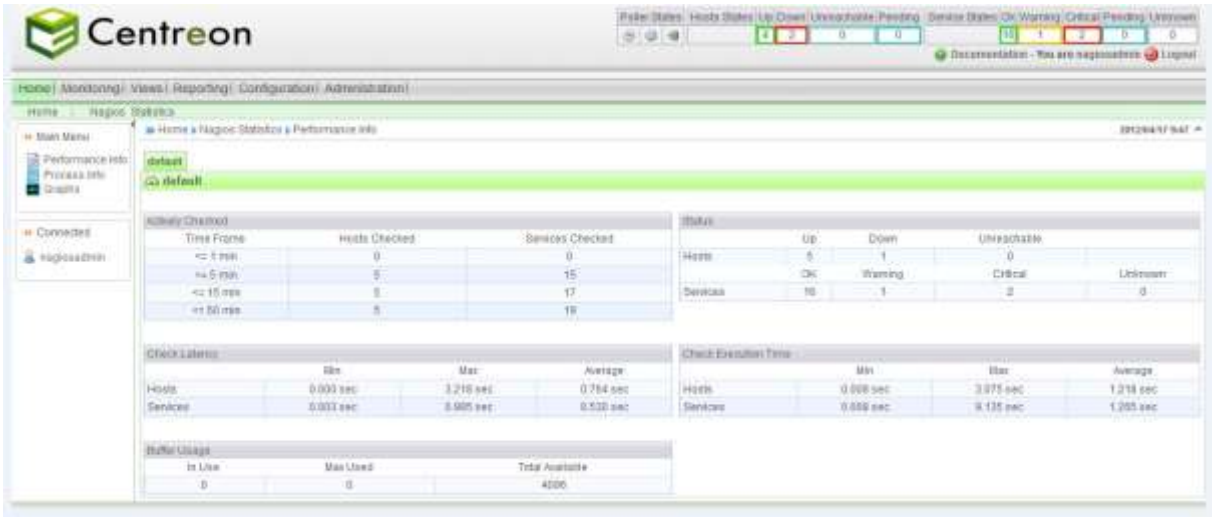

Figure 32 : Interface de graphiques de performance

➢ Monitoring

Cette vue va nous permettre d'accéder à nos hôtes et nos services supervisés.

- ***Les hôtes***

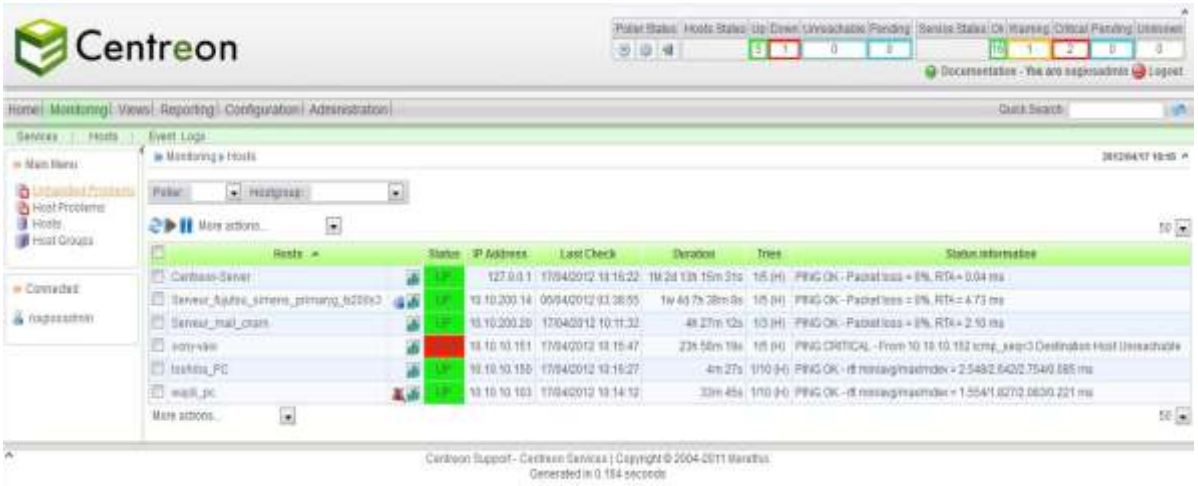

Figure 33 : Interface des hôtes supervisées

- ***Les services***

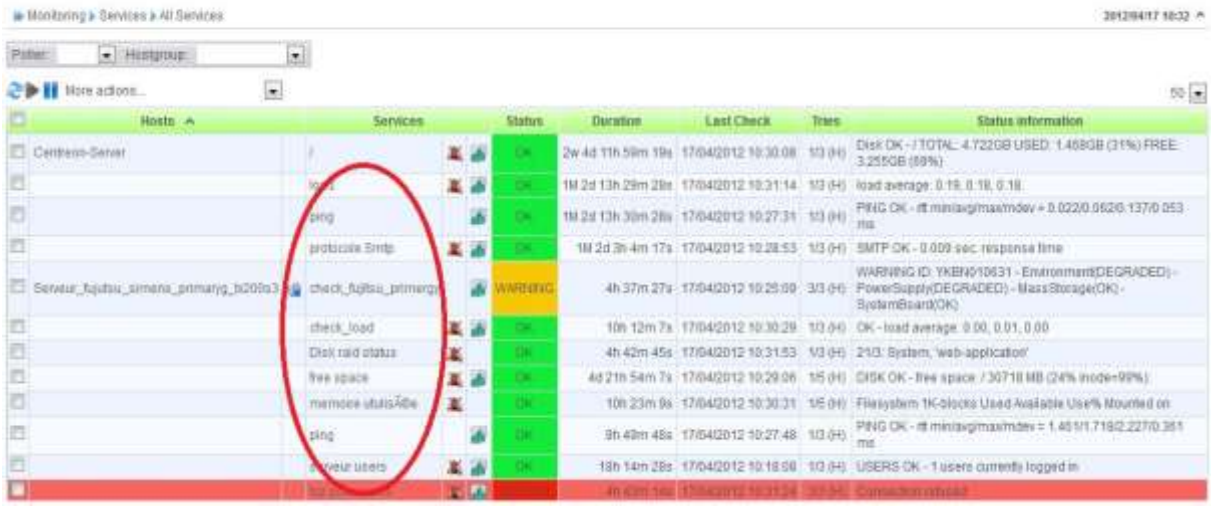

Figure 34 : Etat des services supervisés dans Centreon

- **Event logs**

Dans cette vue, nous aurons accès à tout l'historique des journaux d'évènements Concernant Centreon (Nagios).

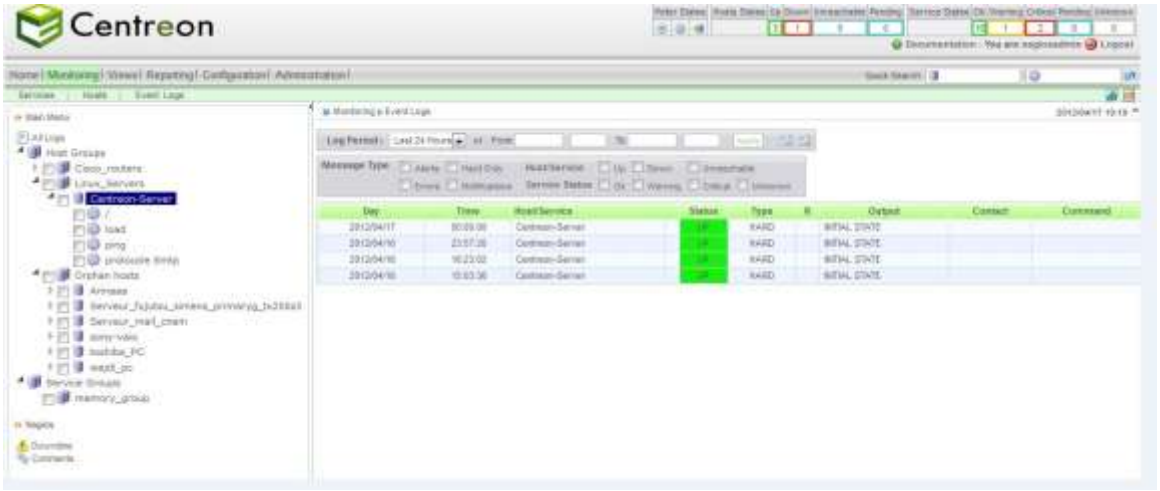

Figure 35 : Interface des journaux d'évènements

- **Views**

Cette vue permet de voir, de créer, de paramétrer des Templates de graphiques pour les exploiter ensuite pour vos hôtes et services.

Figure 36 : Interface de Views

➢ Reporting

Cette vue vous permet d'avoir des statistiques de fiabilité de chaque hôte sur une période de temps

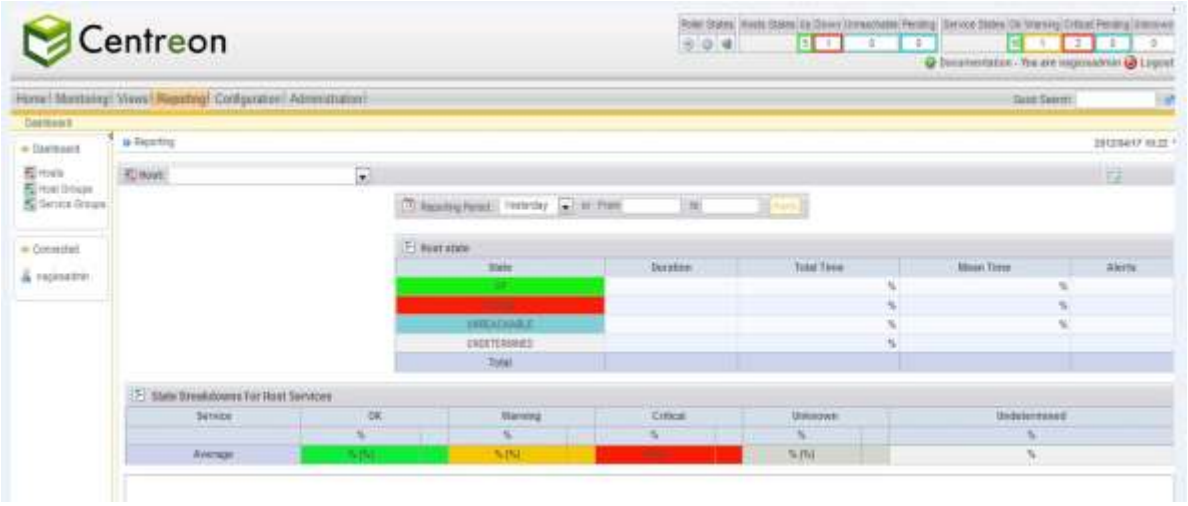

Figure 37: Interface des rapports

❖ Etape1 : Ajout des commandes dans l'interface suivante de Centreon :

Dans l'interface Configuration/Commandes, On doit ajouter les commandes checks qui nous Permettront de relever les informations de supervision voulues depuis le serveur distant

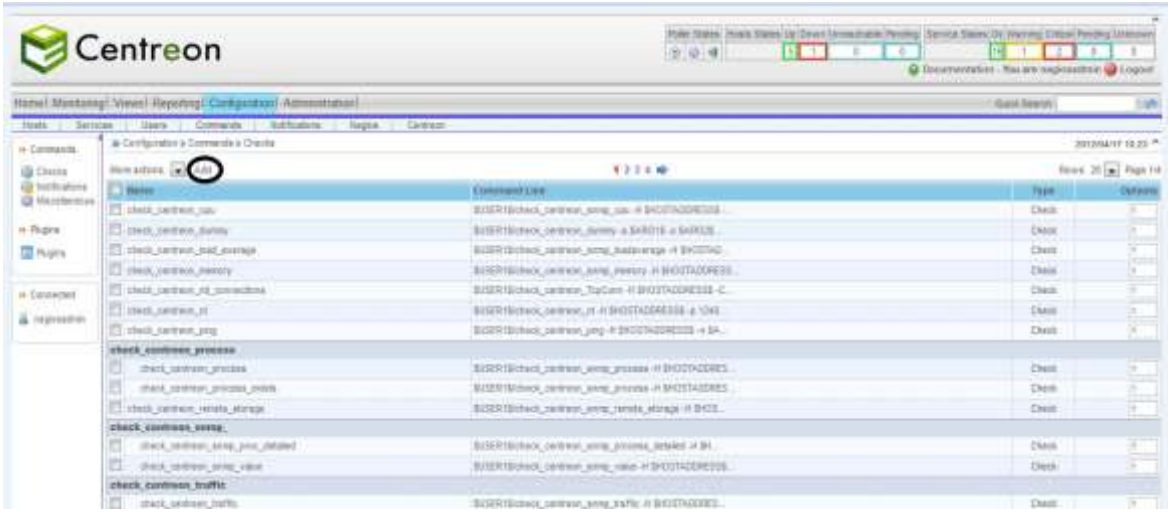

Figure 38 : Interface des services supervisés dans Nagios

L'appuie sur « **add** » nous ramène à l'interface suivante pour la définition des commandes:

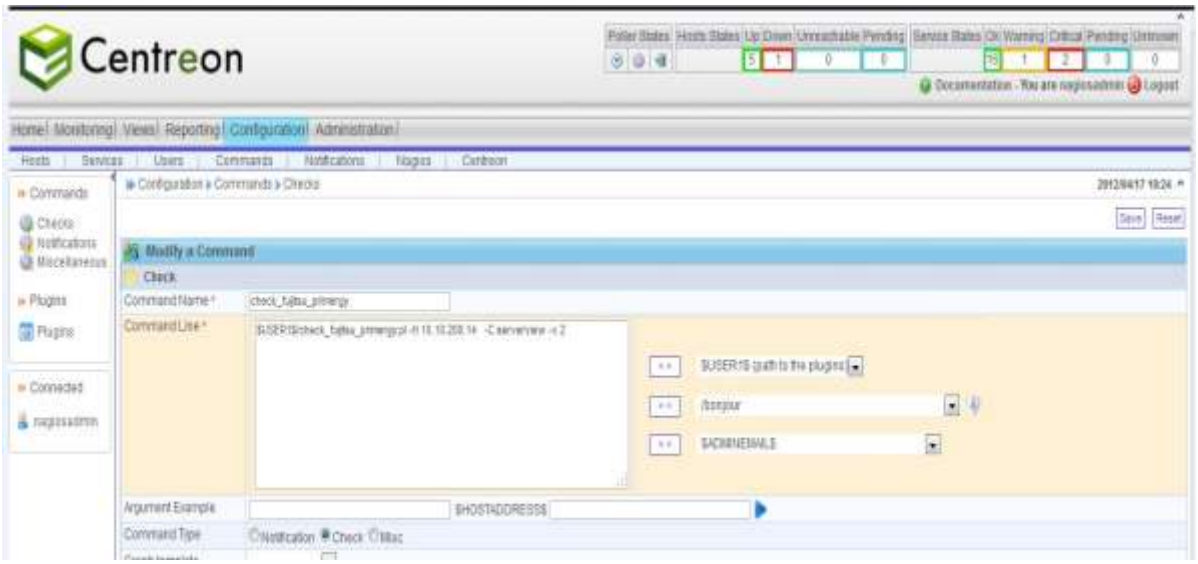

Figure 39 : Interface de définition des commandes

De la même manière toutes ces commandes seront définies :

Commandes	Syntaxes	Significations
Check_nrpe	**$user$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$**	**Permet de récupérer les informations à distance lors de la supervision**
Check_raid_status	**$USER1$/ /check_nrpe -H 10.10.200.14 -c check_amCLI**	**Permet de déterminer l'état des discs raid, le nom, espace disque, vitesse de rotation, numéro du Port**
Check_users	**$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_users**	**Permet de déterminer les utilisateurs actif sur le serveur à distant**
Check_df	**$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_df**	**Permet de déterminer l'espace mémoire utilisée du disc**
Check_load	**$USER1$//check_nrpe -H $HOSTADDRESS$ -c check_load**	**Permet de déterminer la vitesse du chargement du Serveur distant**
Check_ fujitsu_primergy	**$USER1$/check_fujitsu_primergy.pl -$HOSTADDRESS$ -C serverview -v 2**	**Permet de déterminer La charge Cpu, Mémoire Utilisée, vitesse de ventilation,**

		vitesse d'alimentation courant …

Tableau 9 : Exemples des commandes avec check_nrpe

❖ Etape2 : Associer chaque commande à un Template de service :

L'option « Add » nous renvoie vers une interface ou nous devons définir notre « Service Template » et l'associer à sa commande relative.
Ainsi on définit les Templates propre à chaque commande crée dans la partie 1.

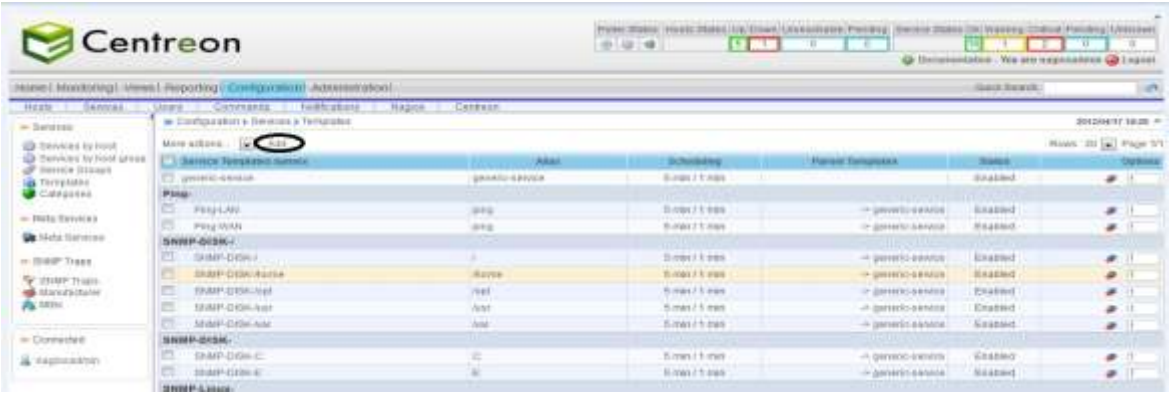

Figure 40 : Interface d'ajout de services supervisés dans Nagios

❖ Etape3 : Exportation de la configuration vers Nagios

En fait lorsque nous modifions la configuration dans Centreon, nous ne faisons que modifier L'état de la base Centreon. Les modifications ne sont pas encore prises en compte par les différents collecteurs Nagios.
Pour effectuer cette mise à jour, il faut se rendre au menu **Configuration / Nagios** puis cliquer sur les
Boutons:

- **"Move export files":** pour déplacer physiquement les fichiers de configuration dans L'arborescence Nagios.
- **"Restart Nagios":** Pour le redémarrage de Nagios afin que la configuration soit prise en Compte.
- Puis cliqué sur **"Export"**

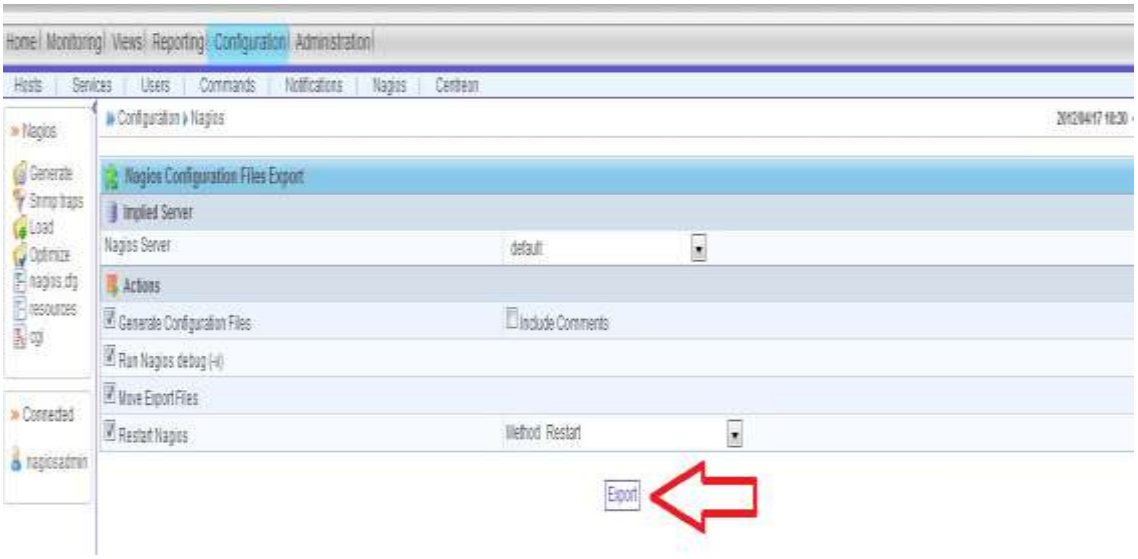

Figure 41 : Interface d'exportation

Si tout se passe bien, nous ne devrions pas avoir de messages d'erreurs, Quelques minutes après l'exportation, l'hôte ajouté apparaitra dans l'interface « Monitoring » de Centreon, accompagné de ses services.

La même hôte et ses services apparaissent dans l'interface de Nagios après l'exportation de Centreon Vers Nagios :

Figure 42 : Interface des services supervisés dans Nagios

3. Utilisation des Templates pour l'ajout et la supervision des serveurs Linux

Puisque NRPE à la particularité d'exécuter les commandes réclamer par le serveur Nagios dans la machine Linux distante à superviser, on doit avoir cet ensemble de commandes définies dans le fichier de configuration **nrpe.cfg** de la machine à superviser.

Ligne ajoutée	Significations
command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c 10	Permet de déterminer le nombre d'utilisateurs connectés.
command[check_load]=/usr/local/nagios/libexec/check_load -w 15,10,5 -c 30,25,20	Permet de déterminer la charge CPU
command[check_root]=/usr/local/nagios/libexec/check_disk -w 20% -c 10% -p /dev/mapper/VolGroup00-LogVol00	Permet de déterminer l'espace disc restant sur la partition
command[check_df]=/bin/df	Permet de déterminer l'espace mémoire utilisée du disc
command[check_amCLI]=/usr/sbin/amCLI –l –All	Permet de déterminer l'état des discs raid, le nom, espace disque, vitesse de rotation, numéro du Port
command[check_script]=/usr/local/nagios/libexec/amcli_script	Même que la précédence mais à travers un script

Tableau 10 : Exemple de configuration de quelques commandes NRPE

➢ **Remarques :**

• Les plugins check_users, check_load, etc.…Sont déjà présents dans le répertoire **/usr/local/nagios/libexec** à l'installation des plugins dans la machine distante

- La commande **amCLI** est installée suite à un package *« ServerView Linux Agent »* du **serveur siemens primaryg** dans le même répertoire.
- **check_fujitsu_primergy.pl** est un script perl est placé dans le répertoire **/usr/lib/nagios/plugins** dans le serveur nagios ont lui donnant tout les droit d'exécution

  sudo chmod +x /usr/lib/nagios/plugins/check_fujitsu_primergy.pl

Ces commandes seront appelés depuis le serveur nagios seulement par leur nom indiqué entre < > Et de la manière suivante :

Check_nrpe –H <@machine distante> **-c** <nom de la commande>

4. Notification par mail

En plus d'être informé visuellement par l'interface de Centreon ou Nagios, on peut paramétrer l'envoi des mails pour indiquer la perte d'un hôte ou d'un service. Cela permet d'avoir des informations supplémentaires, et d'avoir un historique de l'activité durant la nuit lorsque l'on ouvre sa boite mail le matin

Nagios possède déjà les commandes de notification **« host-notify-by-email »** et **« service-notify-byemail »** dans la partie **configuration> commands>notifications** qui seront paramétrées à des hôtes ou services lors de leur création, ainsi on gardera la même configuration à chaque nouvel ajout.

Il nous reste qu'à informer le système des utilisateurs et groupes d'utilisateurs à notifier lors de l'apparition d'un problème et de sélectionner la durée de notification.

5. Conclusion

Dans ce chapitre nous avons penchés sur l'aspect pratique de notre projet, en détaillant les étapes de la mise en place et l'utilisation de notre solution, et nous avons ainsi prouver l'apport important de Centreon à Nagios, qui est principalement, la facilité de la configuration, mais aussi la livraison de comptes rendus et d'analyses plus rapidement et d'une manière beaucoup plus précise pour le seul but de gagner et optimiser la gestion de son temps.

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 expliqué dans notre étude, la supervision est un des moyens indispensables pour favoriser la croissance de rendement d'une entreprise. Le propos de ce projet était de choisir une solution qui répondait aux besoins organisationnels et financiers de l'entreprise et il n'y'avait pas mieux pour combler ce besoin que Nagios.

L'association de Nagios et de Centreon a permis la constitution d'une solution de monitoring à la fois puissante et efficace.
Centreon agit comme un intermédiaire entre l'administrateur et les fichiers de configurations de Nagios.

Il enregistre dans une base de données les configurations effectuées par l'administrateur, puis il modifie les fichiers de configuration de Nagios en fonction du contenu de la base de données. Ce qui a permis de simplifier grandement le travail de l'administrateur, contrairement à l'utilisation de Nagios seul.

Ce stage nous a permis de nous familiariser avec le système d'exploitation linux dont la maîtrise est nécessaire pour travailler dans les réseaux informatiques. La mise en place du service de surveillance Nagios permet actuellement à l'administrateur, à l'ensemble du service informatique, ainsi qu'aux dirigeants d'être informé de la santé du réseau en temps réel.
Depuis la mise en place de Nagios, certains problèmes réseau ont été traités plus rapidement.

Références nétographiques

1. Site officiel de Nagios :
   http://www.nagios.org/
2. Documentation complète sur les fichiers de Nagios :
   http://www.nagios.sourceforge.net/ :
3. Le site du support du nagios
   http://www.nagios.org/support/
4. Le site officiel de Centreon
   http://www.centreon.com/
5. Manuel d'utilisation de Centreon
   http://wiki.monitoring-fr.org/centreon/manuel-utilisation/start
6. Un site d'installation de Nagios et Centreon
   http://dokuwiki.ruusan.org/administration/nagios
7. Un tutoriel pour l'installation et la configuration de POSTFIX
   http://wiki.monitoring-fr.org/infra/postfix
8. Blog de Nicolar
   http://blog.nicolargo.com/nagios-tutoriels-et-documentations

Annexe A : Installation NRPE

Vous pouvez superviser les machines Linux/Unix en utilisant le plugin NRPE afin de superviser les attributs/ressources locaux comme l'utilisation disque, la charge CPU, l'utilisation mémoire, etc. sur une hôte distant.

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

a. Côté serveur Nagios

- Télécharger la dernière version de nrpe, puis la décompressez et l'installez

```
wget http://freefr.dl.sourceforge.net/sourceforge/nagios/nrpe-2.12.tar.gz
tar zxvf nrpe-2.12.tar.gz
cd nrpe-2.12
./configure --prefix=/usr/local/nagios/ --enable-ssl --with-log-facility --enablecommand-
args --enable-threads=posix --with-trusted-path=
/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/nagios/bin:/usr/local/nagios/libexec
make
make install
cp sample-config/nrpe.cfg /usr/local/nagios/etc/
```

✓ Vérifier que la définition du plugin est bien présente dans le fichier de configuration des commandes (**/usr/local/nagios/etc/objects/commands.cfg**):

```
######
#NRPE
######
#'check_nrpe' command definition
define command{
command_name check_nrpe
command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$

}
```

✓ Configurer NRPE pour qu'il soit gérer comme un démon et qu'il démarre automatiquement au démarrage de la machine. Ensuite, redémarrer nagios

b. Côté machine linux à surveiller

✓ - Téléchargez la dernière version de NRPE et de nagios-plugins :

```
Mkdir ~/download
```

```
Cd ~/download
wget http://surfnet.dl.sourceforge.net/sourceforge/nagios/nrpe-2.12.tar.gz
```

```
wget
http://heanet.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.14.tar.gz
```

✓ Ajouter un utilisateur pour nagios

Adduser nagios

c. Installation de NRPE :

```
Cd ~/download
tar zxvf nrpe-2.12.tar.gz
cd nrpe-2.12
./configure
make all
make install
```

d. Installation de nagios plugins :

```
tar zxvf nagios-plugins-1.4.14.tar.gz
cd nagios-plugins-1.4.14
./configure
make install
```

Placer le fichier de configuration de NRPE sous le répertoire de nagios

```
mkdir /usr/local/nagios/etc
cd nrpe-2.12
cp sample-config/nrpe.cfg /usr/local/nagios/etc/
```

✓ Donnez les droits sur les fichiers pour l'utilisateur nagios

```
chown -R nagios:nagios /usr/local/nagios/
```

✓ Ajout de script de démarrage de NRPE, lui donner les droits nécessaire et le gérercomme un démon, qu'il démarre automatique au démarrage de la machine.

```
cd nrpe-2.12
cp init-script.debian /etc/init.d/nrpe
chmod 755 /etc/init.d/nrpe
update-rc.d nrpe defaults
```

✓ Si vous avez un firewall sur la machine que vous souhaitez surveiller, il est nécessaire d'ajouter une règle à votre firewall afin que NRPE puisse se communiquer avec le serveur nagios

```
iptables –A INPUT -p tcp --dport 5666 -j ACCEPT
```

e. Configuration

✓ Editer le fichier **/usr/local/nagios/etc/nrpe.conf** sur la machine à surveiller

```
# Adresse IP de votre machine
server_address=xx.xx.xx.xx
# Adresse autorisant NRPE (yy.yy.yy.yy --> IP du serveur Nagios)
allowed_hosts=127.0.0.1,yy.yy.yy.yy
# Autorisation du passage d'argument durant les checks dans NRPE dont_blame_nrpe=1
```

✓ Côté serveur nagios, éditer le fichier commands.cfg (**/usr/local/nagios/etc/objects/commands.cfg**) afin de définir une commande pour utiliser le plugin « **check_nrpe** ».

```
# NRPE avec SSL
define command{
command_name check_nrpe
command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

La dernière étape consiste à modifier les fichiers de configuration de Nagios pour intégrer le monitoring du serveur Linux. Il faut dans un premier temps éditer votre fichier de configuration des hosts (**localhost.cfg** par défaut) et y ajouter votre machine Linux.

```
define host {
use generic-host jerba.cnam linux
alias jerba server
address  172.21.89.1
}
```

Puis ajouter les services offerts par NRPE dans le même fichier (**localhost.cfg**)

```
# Charge CPU
define service{
use generic-service
14
host_name linux
service_description CPU Load
check_command check_nrpe!check_load
}
# Memoire
define service {
use generic-service
host_name linux
service_description Memory
check_command check_nrpe!check_mem
}
```

✓ Ajout d'autres plugins exécutables par NRPE

✓ Check Memory

- Téléchargez l'exécutable de cet plugin :

```
Cd ~/download
Wget http://www.monitoringexchange.org/attachment/preview/Check-Plugins/Operating-Systems/Linux/check_memory/check_memory.pl
cp check_memory.pl /usr/local/nagios/libexec/
chmod +x /usr/local/nagios/libexec/check_memory.pl
cd /root/download/nagios-plugins-1.4.14/perlmods/
make
make install
```

Vérifiez si les modules perl de nagios sont bien installées dans **/usr/local/nagios/perl**.

Puis tester le fonctionnement à l'aide de cette commande

```
perl -Mlib=/usr/local/nagios/perl/lib/ /usr/local/nagios/libexec/check_memory.pl -w 30 –c 15
```

Ajoutez la ligne suivante dans « **/usr/local/nagios/etc/nrpe.cfg** »

```
command[check_mem]=perlMlib=/usr/local/nagios/perl/lib//usr/local/nagios/libexec/check_memory.pl -w 30 -c 15
```

Redémarrez NRPE et nagios côté client et serveur.

- Vous pouvez tester du côté serveur.

```
usr/local/nagios/libexec/check_nrpe -H 10.10.200.14  -c check_mem
```

Annexe B : Installation du ServerView Linux Agent

ServerView Linux Agent est un logiciel qui surveille le matériel, ainsi qu'il détecte et informe sur des anomalies (par journal des événements et des interruptions SNMP), en installant dans le serveur qu'il PRIMERGY à surveiller.
Il fournit également ServerView console les informations sur le serveur contrôlé par en utilisant le protocole SNMP.

- Comment faire pour démarrer le script d'installation ?

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
LinuxSVAgent/
# ./insagt
```

➢ ***Pré-requis :***

Les pré-requis à l'installation sont donc :

PC System	Operational Conditions
Mémoire Utilisée	32MB ou plus
Disque dur	30MB plus d'espace libre (/lib 3MB/var 3MB/etc 3MB/sbin 1MB/usr 20MB)
Carte Réseau	carte Réseau Obligatoire (On Board LAN est également possible)
Écran	Monitor SVGA (800×600) ou plus of resolution (recommended: 1024×768)
Souris	Required Required (On Board LAN is also possible)
Système d'exploitation	Red Hat Enterprise Linux 5 (for Intel64) (Abbreviation:RHEL5(Intel64))
Protocole	TCP/IP est nécessaire pour exécuter
Service	SNMP (service and trap) doit être actionné
Package(RPM)	• net-snmp , net-snmp-utils , compat-libstdc++ , gcc ,• glibc • glibc-devel • binutils • libstdc++ • make • gawk ,• rpm • compat-libstdc++