République Tunisienne
*****
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
*****
Université Virtuelle de Tunis

RAPPORT DU PROJET DE FIN D'ÉTUDES

Pour l'obtention du diplôme de

Mastère Professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR)

Mise en place d'un outil de supervision système et réseau open source

Réalisé par :

Abir Trabelsi

Encadrants

Dr Hanen Idoudi

Mr Anouar KETAT

Année Universitaire 2014-2015

Dédicaces

Je dédie ce travail à :

À mes parents Abdelkrim et Fatima

Pour votre amour…

Pour tous vos sacrifices…

Pour tous l'enseignement que vous m'avez transmis…

En témoignage de mon éternelle reconnaissance.

À mon mari Nejmeddin

Pour ton amour…

Pour ton soutien et tes sacrifices…

À mes petits Amen Allah et Meniyar

Que dieu vous protège

Et à tous ceux qui m'ont soutenu et me soutient encore.

Remerciements

J'exprime mes profondes gratitudes et respectueuses reconnaissances à

Mon encadreur : **Dr Hanen Idoudi**

Pour sa bonne volonté d'accepter de m'encadrer, pour tout le temps

Qu'elle m'a accordée et pour tous les conseils qu'elle m'a prodigué.

Je remercie aussi mon encadreur au sein de la société

Mr Anouar KETAT

Pour ses directives précieuses, et pour la qualité de ses suivis durant toute

La période de mon projet.

Sommaire

Liste des figures

Liste des Tableaux

Introduction générale

Actuellement, les systèmes d'informations dans les entreprises deviennent de plus en plus importants mais aussi complexes. Le besoin de maintenance et de gestion de ces systèmes est rapidement devenu une priorité. Plusieurs logiciels de surveillance et de supervision de réseaux ont été développés pour vérifier l'état du réseau en temps réel et pour être informé au plutôt de tout incident réseau. Grâce à ces logiciels, les délais d'interventions sont fortement réduites et les anomalies peuvent être aussitôt prises en main sans que les utilisateurs du réseau en question soient affectés ou remarquent des erreurs.

Dans ce cadre, nous envisageons de mettre en place une console d'administration réseau pour la société tunisienne de sidérurgie. Cette console permettra de superviser et de contrôler le réseau et l'état des équipements informatiques.

Ce rapport présente l'ensemble des étapes suivies pour développer l'application. Il contient quatre chapitres organisés comme suit :

Le premier chapitre intitulé « Présentation et cadre général du projet » est consacré à la présentation de l'organisme d'accueil et du problématiques. Il contient ensuite l'étude et la critique de l'existant suivis de la proposition de la solution adéquate et enfin donner la solution retenue.

Le second chapitre sera intitulé « Etat de l'art » présente un rappel du principe de supervision avant de passer à l'étude comparative des outils de supervision existants et la fixation du choix de l'outil à mettre en place.

Le troisième chapitre a pour objectif de présenter l'étude théorique de la solution de monitoring adoptée pour ce travail, son architecture et son principe de fonctionnement.

Le dernier chapitre intitulé « Mise en place de la solution adoptée » présente l'environnement de travail ainsi que les outils logiciels que nous avons utilisés pour la réalisation de notre projet. Il illustre aussi le travail réalisé et quelques tests.

Chapitre1 : Présentation et cadre général du projet

Introduction :

Nous allons introduire dans ce premier chapitre l'organisme d'accueil ainsi que le cadre de notre projet. Par la suite, nous passerons à l'étude préalable qui est une étape primordiale dans le déroulement du projet.

1. Présentation générale de l'organisme d'accueil :

1.1.Présentation de Netuse :

Netuse est une Société de Services et Ingénierie Informatiques créée en 2007. Elle aide ses clients à innover, à se transformer et à devenir plus performants. En coopération avec ses clients, Netuse contribue à l'élaboration de leur orientation stratégique, à sa mise en œuvre et les aide à tirer le meilleur parti de la technologie. Pour eux, il prend en charge la gestion de leurs processus opérationnels et de leurs infrastructures informatiques.

En associant ses compétences en matière d'entreprise, de technologie et de gestion des opérations, Netuse propose des services véritablement intégrés, ce qui constitue son expertise la plus précieuse.

Netuse, s'est entourée de partenaires les leaders mondiaux dans leurs domaines sélectionnés pour leurs technologies : Microsoft, VMware, Citrix, McAfee, GFI, Websense et Wyse.

1.2.Les métiers de Netuse :

Netuse propose à ses clients une gamme complète de prestations organisées autour de quatre métiers :

- Le conseil en stratégie et transformation : qui a pour mission de contribuer à l'amélioration des performances économiques des entreprises grâce à une connaissance approfondie de leurs métiers et de leurs processus.

- L'intégration de systèmes et de solutions d'infrastructure IT, qui permet de planifier, de concevoir, de diriger et de supporter du plus petit aux plus grands projets d'infrastructure IT.
- L'infogérance / Outsourcing : qui consiste à proposer des contrats d'assistance technique pour les petites et moyennes entreprises de façon à prendre en charge tous les aspects qui garantissent le bon fonctionnement de l'ensemble du système informatique de nos clients.
- Support IT à forte valeur ajoutée : Les équipes de support, formées et certifiées sur les technologies de nos partenaires éditeurs, apportent leur expertise et leur soutien quotidien aux clients dans la résolution de leurs incidents de production, mais aussi dans l'évolution de leurs infrastructures IT.

2. Cadre général du projet :

Les systèmes d'information jouent un rôle capital dans le succès des organismes en assurant une exploitation efficiente et une gestion efficace pour maintenir leurs avantages sur les différents concurrents. L'échange des informations et leur diffusion à temps sont parmi les priorités de tout responsable de système d'information.

Ces systèmes sont exposés à des pannes, à des baisses de performance et à d'autres problèmes opérationnels.

En effet, les systèmes d'informations deviennent de plus en plus complexes et la surveillance et la localisation des problèmes deviennent de plus en plus ardues pour l'administrateur réseaux et systèmes. Le service informatique ainsi que l'administrateur doivent connaître à tout moment l'état de chaque équipement et service sur le réseau pour une très grande réactivité. C'est pourquoi ils ont recours à une technique de suivi, c'est à dire « la supervision».

Dans ce contexte s'introduit notre projet qui consiste à mettre en place un outil de supervision système et réseau pour le client « EL FOULADH »afin d'être prévenu en cas d'incident via divers moyens de communication (SMS, E-mails…) .

3. Etude préalable :

Il s'agit d'une étude de l'existant suivie de critiques permettant au projet de présenter une amélioration résumant l'ensemble des solutions retenues.

3.1.Etude de l'existant :

Nous allons étudier l'environnement informatique d'**ELFOULADH** et notamment :

- L'infrastructure Système (serveurs, système de fichiers et base de données) ;
- L'infrastructure Réseau (Réseau LAN et Réseau WAN).

L'accès WAN est assuré par une ligne LS 1Méga configuré sur un routeur « CISCO 1841ic 1 T Wic 1 ADSL » et à travers un firewall « CISCO Pix 515E »

Le parc informatique de la société ELFOULEDH est composé d'un ensemble de 9 serveurs avec des systèmes d'exploitation hétérogènes, (Windows, Linux et SUN Solaris), d'environ 300 postes de travail aillant aussi des OS hétérogène et de différents constructeurs (Acer, DELL, HP…) et de 250 imprimantes réseaux et locaux.

Nom du Serveur	Système	Service offert
SRV-PDC	Windows 2003 server entreprise Edition	contrôleur de domaine primaire.
SRV-SDC	Windows 2003 server entreprise Edition	contrôleur de domaine secondaire
SRV-GMAO	Windows 2003 server standard Edition	serveur d'application de GMAO
SERDH	Windows 2003 server SP2 R2	serveur d'application « **Gestion de personnel** +comptabilité»
NTS	Windows NT 4 SP6	Un serveur d'application
SUN	SUN SOLARIS	serveur de bases de données **(Oracle)**

Internet et Messagerie	Linux	serveur de messagerie (**Postfix)** et proxy (**SQUID**)
SRV-Sécurité	Windows 2003 server standard Edition	serveur d'antivirus (Trend Micro)
NTS2	Windows 2000 server SP4	serveur de réplication du serveur NTS
	Windows 2003 Server Standard Edition	Serveur des caméras de vidéosurveillance

Tableau 1: Liste des serveurs

3.2.Critique de l'existant :

Lors de l'étude que nous avons faite dans la section précédente, nous avons relevé les problèmes suivants :

- Aucun outil de supervision système et réseau n'est mis en place au sein de l'entreprise.
- Un taux important de temps est gaspillé lors du diagnostic des pannes ce qui influe sur la qualité du service et donc le bon fonctionnement de l'entreprise.
- Plus le nombre des équipements et des services augmente plus les tâches de l'administrateur deviennent trop compliquées et il n'arrive pas à les assurer convenablement.
- Vu l'absence d'un outil de supervision, l'administrateur n'est pas alerté en cas de problèmes de fonctionnements anormaux.

3.3.Solutions proposées :

Suite aux inconvénients cités dans le paragraphe précédent, nous proposons la mise en place d'un outil de supervision système et réseau qui assurent les fonctionnalités suivantes :

- Diagnostiquer l'état du réseau.
- Vérifier la disponibilité des serveurs en surveillant les ressources et les performances systèmes (CPU, Disques surs et partitions,RAM,…)
- Surveiller les différents services (Oracle, la connexion au listner, Le service d'annuaire LDAP Les services de messagerie (POSTFIX, SMTP) .
- Déclencher des alertes lors de détection des pannes.
- Générer des graphes, des cartographies et des rapports.

- Avoir une interface graphique compréhensible pour l'interaction entre l'utilisateur et le logiciel.
- N'avoir aucun impact sur les performances et désencombrer le réseau lors de la remontée des informations.

Deux alternatives sont possibles : soit les solutions commerciales soit les solutions open source.

3.4.Solution retenue :

Le responsable du projet nous a confirmé son choix pour la mise en place d'un outil de supervision réseau open source.

Conclusion :

Ce chapitre nous a permis de mieux comprendre les besoins et les attentes du client. Le chapitre suivant sera consacré à effectuer le choix de l'outil à mettre en place.

Chapitre2 : Etat de l'art

Introduction :

Dans ce chapitre, nous allons définir précisément le concept de supervision et la manière dont il a été normalisé par l'ISO, ensuite nous procédons à une étude comparative des outils de supervision et à préciser le choix de l'outil retenu.

1. Principe de la supervision :

La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l'état des réseaux et de leurs composants. Ces données seront ensuite traitées et affichées afin de mettre ma lumière sur d'éventuels problèmes. La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir via un système d'alerte (email ou SMS par exemple) les administrateurs. Cette définition de la supervision est décrite plus en détail dans la norme ISO7498/4. Plusieurs actions sont ainsi réalisées : Acquisition de données, analyse, puis visualisation et réaction. [1]

Un tel processus est réalisé à plusieurs niveaux d'un parc de machines : Au niveau interconnexions (Réseau), au niveau de la machine elle-même (Système) et au niveau des services offerts par cette machine (Applications).

- **Supervision réseau :** Par le terme réseau on entend ici l'aspect communication entre les machines. Le rôle est de s'assurer du bon fonctionnement des communications et de la performance des liens (débit, latence, taux d'erreurs). C'est dans ce cadre que l'on va vérifier par exemple si une adresse IP est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau.
- **Supervision système :** La surveillance se cantonne dans ce cas à la machine elle-même et en particulier ses ressources. Si l'on souhaite par exemple contrôler la mémoire utilisée ou la charge processeur sur le serveur voire analyser les fichiers de logs système.
- **Supervision applicative :** Cette technique est plus subtile, c'est elle qui va nous permettre de vérifier le fonctionnement d'une application lancée sur une machine.

Cela peut être par exemple une tentative de connexion sur le port de l'application pour voir si elle retourne ou demande bien les bonnes informations, mais aussi de l'analyse de logs applicatifs. [1]

2. La norme ISO 7498/4 :

Le concept de supervision a été normalisé par l'ISO (International Organization for Standardization). Voici les différentes fonctions qui ont été défini par l'ISO :

2.1.Gestion des performances

Elle doit pouvoir évaluer les performances des ressources du système et leur efficacité. Elle comprend les procédures de collecte de données et de statistiques. Elle doit aboutir à l'établissement de tableaux de bord. Les informations recueillies doivent aussi permettre de planifier les évolutions du réseau. [2]

Les performances du réseau sont évaluées à partir de quatre paramètres :

- le temps de réponse
- le débit
- le taux d'erreur par bit
- la disponibilité

2.2.Gestion des configurations (Management Configuration)

La gestion de configuration permet d'identifier, de paramétrer et de contrôler les différents objets du réseau. Les procédures requises pour gérer une configuration sont : [2]

- · la collecte d'information
- · le contrôle d'état
- · la sauvegarde historique de configurations de l'état du système.

2.3.Gestion de la comptabilité (Accounting Management)

Son rôle est de connaître les charges des objets gérés ainsi que leurs coûts de communication. Des quotas d'utilisation peuvent être fixés temporairement ou non sur chacune des ressources

réseaux. De plus, la gestion de la comptabilité autorise la mise en place de systèmes de facturation en fonction de l'utilisation pour chaque utilisateur. [2]

2.4.Gestion des anomalies (Fault Management)

La gestion des fautes permet la détection, la localisation et la correction d'anomalies passagères ou persistantes. Elle doit également permettre le rétablissement du service à une situation normale. [2]

2.5.Gestion de la sécurité (Security Management)

La gestion de la sécurité contrôle l'accès aux ressources en fonction des politiques de droits d'utilisation établies. Elle veille à ce que les utilisateurs non autorisés ne puissent accéder à certaines ressources protégées.

Elle a également pour rôle de mettre en application les politiques de sécurité. [2]

3. Le protocole SNMP :

3.1.Présentation :

SNMP (Simple Network Management Protocol) est le protocole de gestion de réseaux proposé par l'IETF. Il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux.
SNMP est un protocole relativement simple. Pourtant l'ensemble de ses fonctionnalités est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications : les bases de données, les serveurs, les logiciels, etc. [3]

Les buts du protocole SNMP sont de :

- connaître l'état global d'un équipement (actif, inactif, partiellement opérationnel...)
- gérer les évènements exceptionnels (perte d'un lien réseau, arrêt brutal d'un équipement...) ;
- analyser différents métriques afin d'anticiper les problèmes futurs (engorgement réseau...) ;
- agir sur certains éléments de la configuration des équipements.

3.2.Les différentes versions du SNMP :

Depuis la création de SNMP, ce protocole a connu des améliorations importantes. Cependant les précédentes versions (la V1 et la V2C) sont encore les versions les plus utilisées actuellement.

Un support de SNMP V3 a récemment été lancé car il est plus sécurisé si on le compare à ses prédécesseurs.

- SNMP V1 : C'est la première version du protocole. La sécurité de cette version est minimale car elle basée uniquement sur la chaîne de caractère appelée "communauté". Cette version du protocole est définie dans les RFC 1155 et 1157. [4]
- SNMP V2C : C'est un protocole révisé, qui comprend les améliorations de SNMP V1 dans différents domaines tels que les types de paquets, les éléments de structure MIB et les requêtes protocolaires MIB. Cependant ce protocole utilise la structure d'administration de SNMP V1 (à savoir "communauté") d'où le terme SNMP V2C.
- SNMP V3 : Aussi connu sous le nom de version sécurisée de SNMP. SNMP V3 facilite la configuration à distance des entités SNMP. [4]

Ces trois versions sont les principales, même si des versions intermédiaires ont vu le jour (SNMPSec, SNMP V2, SNMP V2U, SNMP V2P), celles-ci ne présentent que des mises à jours mineures plutôt que de véritables améliorations.

Actuellement les versions les plus utilisées (par ordre d'utilisation) sont : SNMP V1, SNMP V3 puis SNMP V2C.

Malgré tout la version SNMP V1 persiste encore sur les périphériques, plusieurs facteurs expliquent ce phénomène :

- Les infrastructures déployées en V1 ne sont plus modifiées, tout simplement car cela fonctionnait suffisamment à l'époque, du coup aucune modification n'y est appliquée.
- Les autres versions de SNMP ont été implémentées tardivement par les différents constructeurs.
- SNMP V1 demande très peu de ressources sur des petits équipements tels qu'une imprimante ou un hub. [4]

3.3.Architecture :

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

- Les agents SNMP : ce sont les équipements (réseau ou serveur) qu'il faut superviser.
- Le superviseur SNMP : c'est une machine centrale à partir de laquelle un opérateur humai²n peut superviser en temps réel toute son infrastructure, diagnostiquer les problèmes et finalement faire intervenir un technicien pour les résoudre.
- La MIB : ce sont les informations dynamiques instanciées par les différents agents SNMP et remontées en temps réel au superviseur.

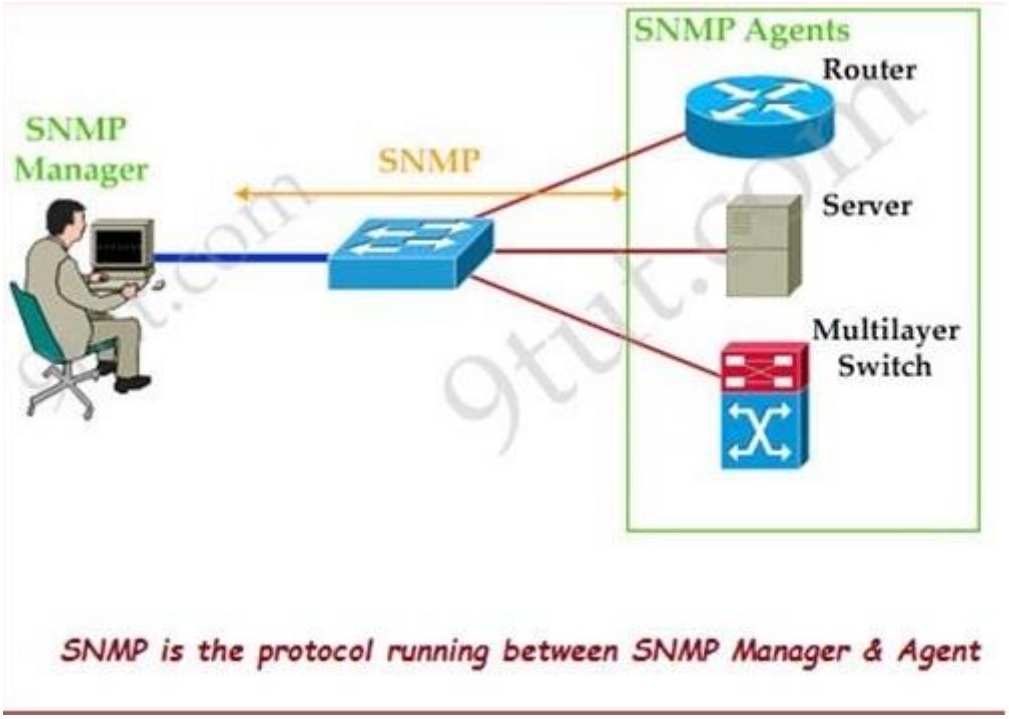

Figure 1: Architecture SNMP

3.4.Le manager

Rappelons que le Manager se trouvera sur un machine d'administration (un poste de travail en général). Il reste un client avant tout, étant donné que c'est lui qui envoie les différentes requêtes aux agents. Il devra disposer d'une fonction serveur, car il doit également rester à l'écoute des alertes que les différents équipements sont susceptibles d'émettre à tout moment.

Si l'on se base sur le schéma précédent, l'administrateur peut observer correctement le comportement de ses différents équipements en réseau.

Le Manager dispose d'un serveur qui reste à l'écoute sur le port UDP 162 ainsi que d'éventuels signaux d'alarme appelés des "traps". Le Manager peut tout autant être installé sur une machine.

3.5.L'agent snmp :

L'agent est un programme qui fait partie de l'élément actif du réseau. L'activation de cet agent permet de recueillir la base de données d'informations et la rend disponible aux interrogations.

Les principales fonctions d'un agent SNMP :

- Collecter des informations de gestion sur son environnement local.
- Récupérer des informations de gestion tel que dé_ni dans la MIB propriétaire.
- Signaler un évènement au gestionnaire.

Par ailleurs même si la principale fonction de l'agent est de rester à l'écoute des éventuelles requêtes du Manager et y répondre s'il y est autorisé, il doit également être capable d'agir de sa propre initiative, s'il a été configuré.

Par exemple, il pourra émettre une alerte si le débit d'une interface réseau, atteint une valeur considérée par l'administrateur comme étant critique. Plusieurs niveaux d'alertes peuvent ainsi être définis, selon la complexité de l'agent (température du processeur, occupation disque dur, utilisation CPU...)

3.6.MIB :

Chaque agent SNMP maintient une base de données décrivant les paramètres de l'appareil géré. Le Manager SNMP utilise cette base de données pour demander à l'agent des renseignements spécifiques. Cette base de données commune partagée entre l'agent et le Manager est appelée Management Information Base (MIB).

Généralement ces MIB contiennent l'ensemble des valeurs statistiques et de contrôle définis pour les éléments actif du réseau. SNMP permet également l'extension de ces valeurs standards avec des valeurs spécifiques à chaque agent, grâce à l'utilisation de MIB privées.

Un fichier MIB est écrit en utilisant une syntaxe particulière, cette syntaxe s'appelle SMI 3, basée sur ASN.1 tout comme SNMP lui-même.

En résumé, les fichiers MIB sont l'ensemble des requêtes que le Manager peut effectuer vers l'agent. L'agent collecte ces données localement et les stocke, tel que défini dans la MIB. Ainsi le Manager doit être conscient de la structure (que celle -ci soit de type standard ou privée) de la MIB afin d'interroger l'agent au bon endroit.

La structure d'une MIB est une arborescence hiérarchique dont chaque noeud est défini par un nombre ou un Object IDentifier (OID). Chaque identifiant est unique et représente les caractéristiques spécifiques du périphérique géré. Lorsqu'un OID est interrogé, la valeur de retour n'est pas un type unique (texte,entier,compteur,tableau...) Un OID est donc une séquence de chiffres séparés par des points. [4]

Une MIB est un arbre très dense, il peut y avoir des milliers d'OID dans la MIB.

Voici un exemple de structure MIB :

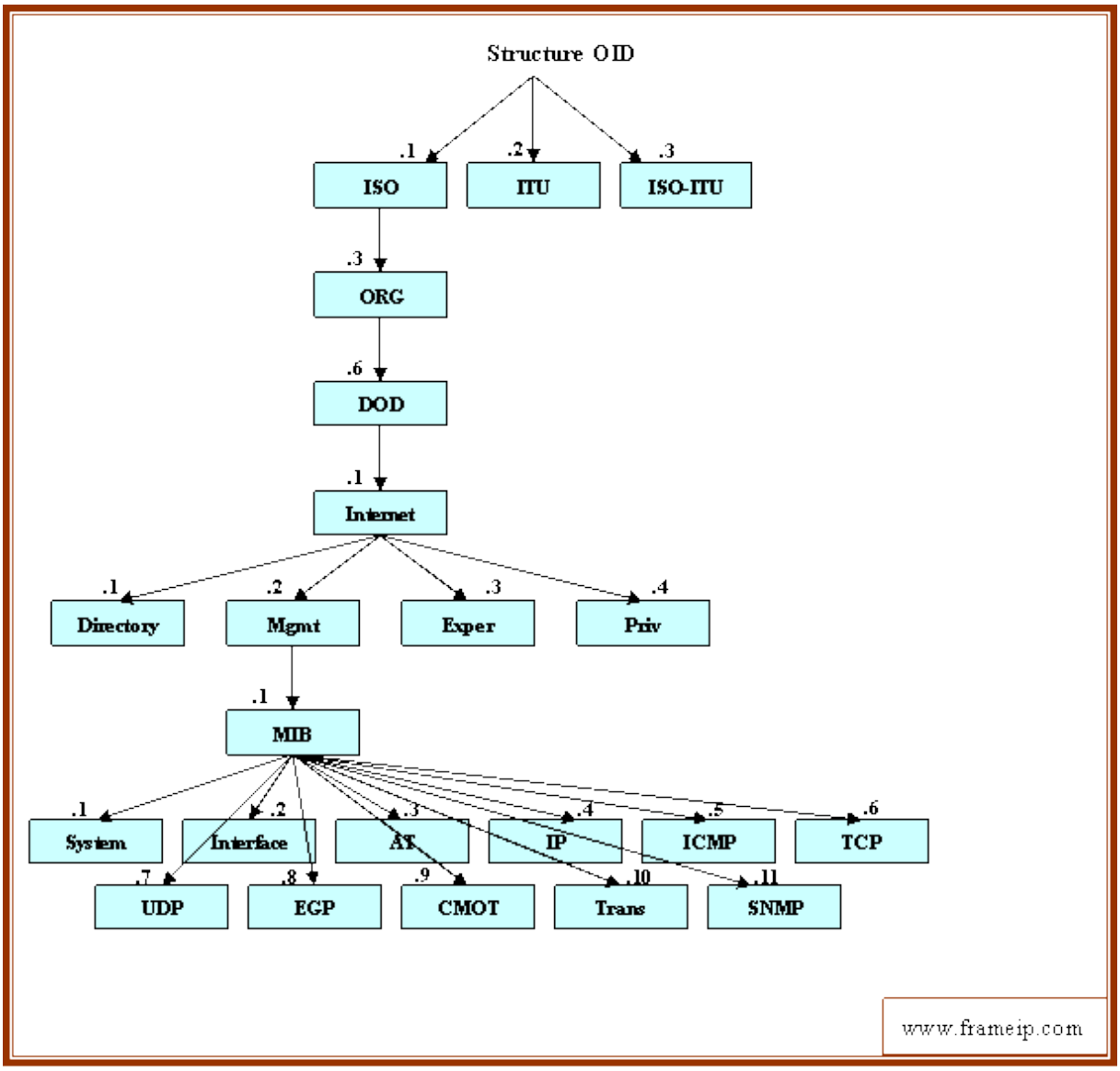

Figure 2 : Strcuture OID

Ainsi, pour interroger les différentes variables d'activité sur un appareil, il faudra explorer son arborescence MIB. Celle-ci est généralement fournie par le constructeur mais il est aussi possible d'utiliser un explorateur de MIB tel que « Getif MIB Browser ».

Ensuite, pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne l'emplacement de la variable à consulter dans la MIB. On aura par exemple sur un commutateur Nortel Passport l'OID .1.3.6.1.4.1.2272.1.1.20 désignant le taux de charge du CPU.

3.7.Les requêtes SNMP :

Le mécanisme de base du **protocole SNMP** est constitué d'échanges de type requête/réponse appelé PDU pour Protocol Data Unit. En fonction de la version du protocole SNMP utilisé, différentes commandes sont possibles. La structure des paquets utilisés par le protocole SNMP V1, est définie dans la RFC 1157. Les requêtes SNMP vont contenir une liste d'OID (Object identifier) à collecter sur l'agent SNMP.

Les types de requêtes du manager SNMP vers l'agent SNMP sont :

- **Get Request** : Le manager interroge un agent sur les valeurs d'un ou de plusieurs objets d'une MIB.

- **Get Next Request** : Le manager interroge un agent pour obtenir la valeur de l'objet suivant dans l'arbre des objets de l'agent. Cette interrogation permet de balayer des objets indexés de type tableau.
- Get Bulk Request : Introduite avec la version 2 du protocole SNMP, cette requête permet de mixer la commande GET et GETNEXT pour obtenir des blocs entiers de réponses de la part de l'agent.
- **Set Request** : Le manager positionne ou modifie la valeur d'un objet dans l'agent. [4]

Les réponses ou informations de l'agent vers le manager sont :

- **Get Response** : L'agent répond aux interrogations du manager.
- **Trap** : L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du manager.
- **Notification** : Introduite avec la version 2 du protocole SNMP. L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du manager.
- **Inform** : Introduite avec la version 2 du protocole SNMP. L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent attend un d'acquittement de la part du manager et il y aura une retransmission en cas de non réponse. [4]

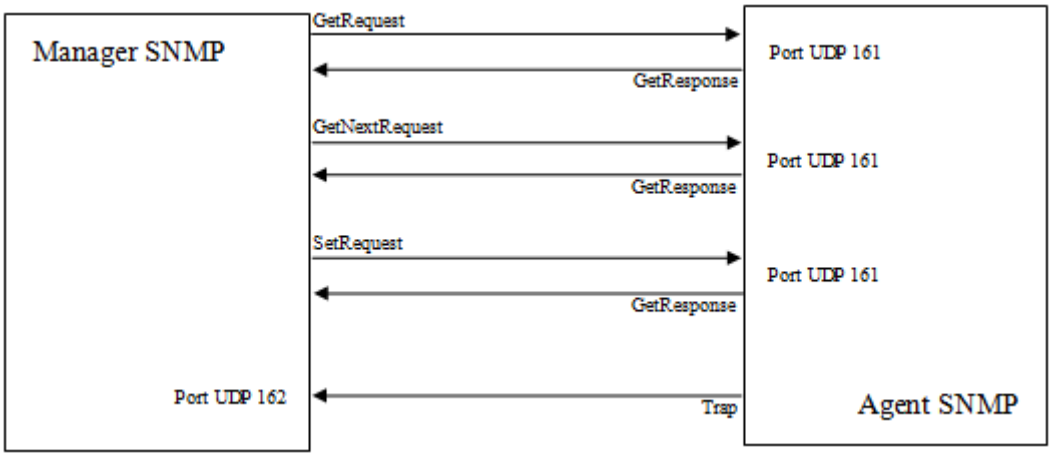

Figure 3 : Les échanges entre le manager et l'agent SNMP

2. Etude comparative des outils de supervision open source :

Nous allons présenter les principaux outils de supervision réseau open source que nous avons choisi vu la diversité de ces outils tout en dégageant leurs avantages et inconvénients :

3.1. Cati :

✓ **Présentation de l'outil :**

C'est un logiciel de supervision réseau basé sur RRDTool. Il peut être considéré comme un successeur à MRTG et également comme une interface à RRDTool. Cacti permet de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP ou encore grâce à des scripts (Bash, PHP, Perl, VBs…) pour avoir par exemple l'espace disque restant ou bien la mémoire utilisée, la charge processeur ou le ping d'un élément actif. Les données sont récoltées auprès des différents agents SNMP (ou auprès des scripts locaux) grâce à un script php. Pour de meilleures performances un exécutable, nommé cactid, peut également effectuer les interrogations. [5]

✓ **Avantages :**

- Configuration : Avec l'utilisation des templates pour les machines, les graphiques, et la récupération des données tout se configure aisément et entièrement via l'interface web. Import/ Export très simple des templates au

format XML. On peut aussi très facilement utiliser des options poussées de RRDTOOL.

- Performance : Avec le choix du moteur de récolte des données, On peut opter pour la performance ou la simplicité
- Gestion des utilisateurs
- Communauté sur le web, présence d'une dizaine de plugins permettant d'étendre les fonctionnalités

✓ **Inconvénients :**

- Pas de gestion d'alarmes, sauf avec un plugin nommé Thold.
- Pas de gestion de panne et absence d'une cartographie de réseau.
- Un développement lent tout comme NetMRG.

3.2. Zabbix

✓ **Présentation de l'outil :**

Zabbix est un outil de supervision, ambitionnant de concurrencer Nagios et MRTG. Il permet de superviser réseau, systèmes (processeur, disque, mémoire, processus,…). Zabbix permet offre des vues graphiques (générés par RRDtool) et des alertes sur seuil. Le « serveur ZABBIX » peut être décomposé en 3 parties séparées: Le serveur de données, l'interface de gestion et le serveur de traitement. Chacune d'elles peut être disposée sur une machine différente pour répartir la charge et optimiser les performances. Un agent ZABBIX peut aussi être installé sur les hôtes Linux, UNIX et Windows afin d'obtenir des statistiques comme la charge CPU, l'utilisation du réseau, l'espace disque… Le logiciel peut réaliser le monitoring via SNMP. Il est possible de configurer des « proxy Zabbix » afin de répartir la charge ou d'assurer une meilleure disponibilité de service. [5]

✓ **Avantages :**

- Une solution très complète : cartographie de réseaux, gestion poussée d'alarmes via SMS, Jabber ou Email, gestion des utilisateurs, gestion de pannes, statistiques et reporting.
- Une entreprise qui pousse le développement, et une communauté croissante

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

✓ **Inconvénients :**

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

3.3. Nagios :

✓ **Présentation de l'outil :**

Nagios (anciennement Netsaint) est un logiciel qui permet de superviser un système d'information. Nagios est, avant toute chose, un moteur gérant l'ordonnancement des vérifications, ainsi que les actions à prendre sur incidents (alertes, escalades, prise d'action corrective). L'interface web est la partie graphique visible, via un serveur web tel que Apache, et qui va permettre à l'administrateur d'avoir une vue d'ensemble de son réseau, de visualiser la supervision des équipements et de produire des rapports d'activité. [5]

✓ **Avantages :**

- Reconnu auprès des entreprises, grande communauté.
- Très puissant et modulaire.
- Plétore de plugins qui permettent d'étendre les possibilités (agents comme zabbix, reporting amélioré, etc...)
- Une solution complète permettant le reporting, la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau.

- Beaucoup de documentations sur le web.
- Performances du moteur.

✓ **Inconvénients :**

- Interface non ergonomique et peu intuitive.
- Configuration fastidieuse via beaucoup de fichiers.
- Pour avoir toute les fonctionnalités il faut installer des plugins, de base c'est assez limité.

3. Choix de l'outil

Pour la supervision informatique au sein de la société, nous avons choisi NAGIOS comme un outil de supervision à mettre en place.

Notre choix s'est basé sur les points forts de cet outil notamment sa modularité complète et sa capacité à gérer un parc important de machines.

- Sa modularité : Nagios laisse la supervision à des plug-ins, ou sondes, que va lui fournir l'utilisateur. Il se contente de les lancer et de gérer les informations recueillies par ce biais. Il permet également de définir des plug-ins qui vont alerter les utilisateurs en cas de problème, ce qui permet d'être inventif en matière d'avertissement. Lorsque quelque chose se passe mal, d'autres plug-ins peuvent tenter de corriger le problème. Il n'est pas possible de prévoir tous les cas de réparations possibles. Nagios laisse le soin de définir lui-même les commandes pour résoudre le problème sur son environnement. [6]
- Sa Capacité à gérer un parc important de machines : Sur ce point, trois critères principaux entrent en jeu :
  - ✓ les performances : En matière de performances, Nagios n'a rien à envier aux outils de supervision propriétaires. Il permet, avec un serveur modeste, de surveiller près de 10 000 éléments. Nagios propose des options pouvant sensiblement augmenter cette valeur.
  - ✓ la gestion de la configuration : Plus on a de points à surveiller, plus la configuration devient lourde, avec les risques, si elle devient trop dure à gérer, d'être laissée de côté. Nagios propose diverses solutions pour

faciliter la gestion d'un nombre élevé de points surveillés, et c'est même une de ses grandes forces.

- ✓ Les pertes massives : Dans le cas des grandes architectures, de petits problèmes peuvent vite devenir un véritable cauchemar. Partant d'une simple erreur, on atteint au final un nombre impressionnant d'alertes. Si l'outil de supervision ne gère pas ce genre de cas, les utilisateurs auront toutes les peines du monde à trouver, parmi toutes ces alertes, la cause initiale du problème. Nagios gère ces cas grâce aux relations de dépendances. Ces relations peuvent être physiques (par exemple pour les liens réseau) ou bien virtuelles (comme c'est le cas entre une application et sa base de données). Il permet de filtrer les alertes pour avoir uniquement celles qui apportent des informations sur la résolution du problème.

Conclusion :

Après avoir effectué le choix de l'outil de supervision open source convenable, nous allons l'étudier en profondeur pour faciliter sa mise en œuvre.

Chapitre3 : Etude technique détaillée de NAGIOS

Introduction :

Dans ce chapitre, nous commençons par présenter l'outil Nagios, son architecture et son principe de fonctionnement, ensuite nous présentons les compléments de notre solution qui sont les agents spécialisés en supervision à distance NSClient et NRPE ainsi que ses fichiers de configuration.

1. Présentation de NAGIOS :

Nagios (anciennement appelé Netsaint) est un logiciel libre sous licence GPL permettant principalement la surveillance système et réseau mais reste évolutif et assez flexible. Il se base sur la collecte déclenchée et personnalisée des informations que nous cherchons à analyser, il permet la surveillance d'un grand nombre de paramètres sur les machines du réseau. La principale particularité de cet outil est sa grande modularité qui lui permet de s'adapter aux besoins des utilisateurs. L'utilisateur pourra donc affiner les tests à effectuer selon ce qu'il veut surveiller.

A la différence de beaucoup d'autres outils de supervision, Nagios ne possède pas un mécanisme interne qui vérifie l'état d'une application, d'un hôte… A la place, il utilise des programmes externes appelés plugins.

2. Architecture de NAGIOS :

C'est un programme modulaire qui se décompose en trois parties : un ordonnanceur, une IHM (Interface Homme Machine) Et les sondes.

- ✓ **L'ordonnanceur** est le moteur de l'application qui vient ordonnancer et gérer les tâches, les vérifications, et les actions à prendre en cas d'incidents (alertes, types d'analyse et d'action corrective.
- ✓ **IHM (Interface Homme Machine)** représente la partie graphique, visible à travers un simple serveur Web tel Apache, permettant d'avoir une vue d'ensemble du système

d'information et des possibles anomalies afin de faciliter la communication entre l'administrateur réseau et l'ordonnanceur.

✓ Les sondes (un greffon/plugin) est un petit programme qui assure une ou plusieurs tâches particulières. Pour les plugins dédiés à Nagios. Il existe déjà plusieurs disponibles gratuitement sur internet, notamment sur le site http://exchange.nagios.org/.Chaque utilisateur pourra compléter et modifier en fonction de ses besoins pour superviser chaque service ou ressource disponible de la manière qu'il souhaite. C'est cette troisième composante de Nagios qui fait « sa force ». En effet les plugins peuvent être développés à l'aide de langages de programmations communs comme le C++, Perl ou PHP en fonction des aptitudes de l'utilisateur et suivant ses critères personnels de supervision afin d'appliquer les solutions adéquates à chaque situation.

3. Principe de fonctionnement de NAGIOS

Nagios est un moteur d'ordonnancement de vérifications diverses et variées. Ces dernières, dont le développement est séparé du noyau moteur, sont assurées par des plugins. La relation entre le moteur et les plugins est assurée d'une part par la configuration de Nagios afin que Nagios sache quelles vérifications lancer et sur quelles machines. D'autre part, cette relation est garantie par la sortie retournée du plugin sous la forme d'un code retour. Ce code sera accompagné éventuellement d'un petit message décrivant le déroulement de l'exécution (dans le but d'aider l'utilisateur à faire le bon diagnostic en cas de problème). Ce sont donc ces états qui seront ensuite remontés au moteur qui prendra les décisions et lancera les actions adéquates et préalablement programmées. Le code retour fourni par l'exécution du plugin est décrit dans le tableau ci-dessous.

Valeur Numérique	Statut du Service	Description du Statut
0	OK	Le plugin a été en mesure de vérifier le service et fonctionne correctement
1	WARNING	Le plugin a été en mesure de vérifier le service, mais ne semble pas fonctionner correctement
2	CRITICAL	Le plugin n'a même pas pu être vérifié

3	UNKNOWN	Arguments invalides dans la ligne de commande du plugin ou bien ce dernier a été incapable de vérifier l'état de l'hôte donné ou le service

Tableau 2: Correspoendace de retour-état

Le processus standard se déroule comme suit : Nagios exécutera un plugin dès qu'il a besoin de tester un service ou un hôte. Les plugins feront ce qu'il faudra pour exécuter le contrôle choisi et envoyer ensuite le résultat à la machine serveur de supervision. Nagios analysera le résultat reçu du plugin et prendra les mesures nécessaires prévus au préalable (informer l'administrateur via e-mail, sms…).

Ces greffons fonctionnent soit à distances (tests sur des protocoles réseaux tels que SMTP, FTP ou l'exécution à distance via SSH ou autre), soit en local sur la machine supervisée (par exemple vérification sur les disques) comme il montre la figure 4.

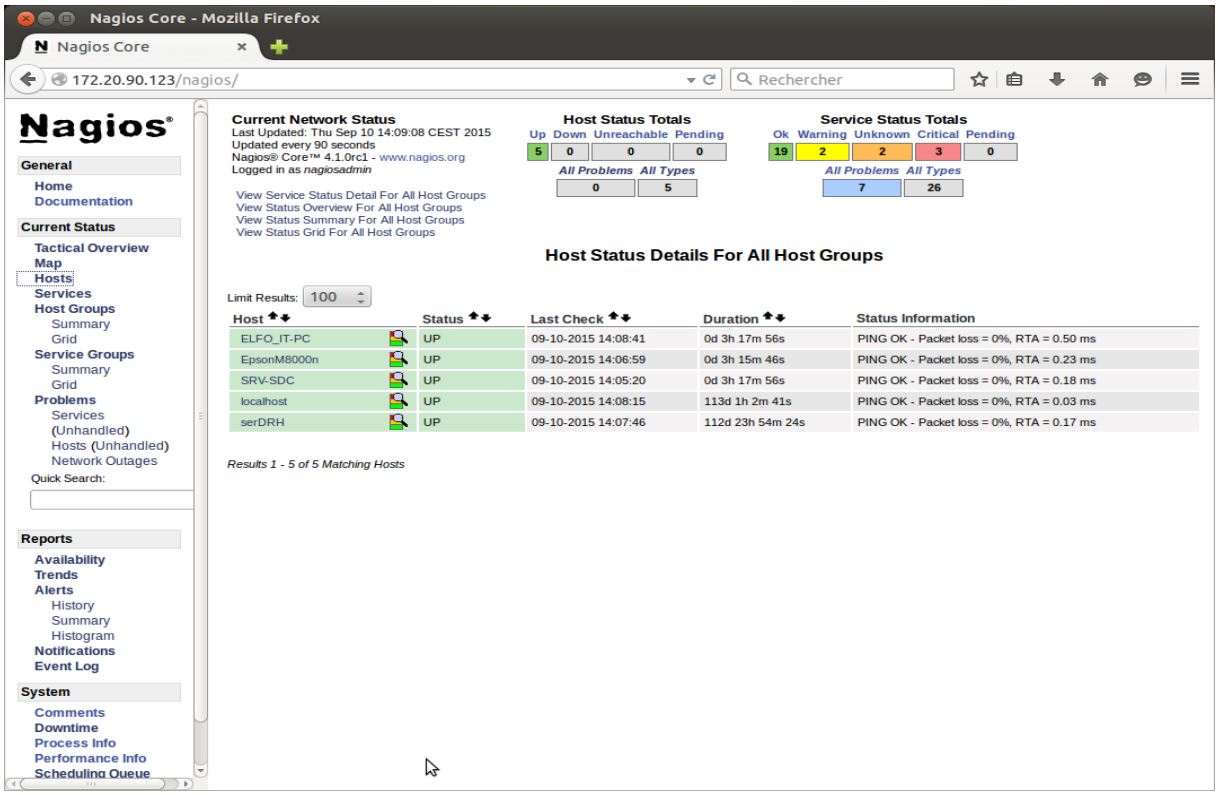

Figure 4 : Interface web de Nagios

4. Les plugins :

Nagios possède une importante communauté sur Internet. Grâce à celle-ci, de nombreux utilisateurs ont créés des plugins permettant à Nagios d'aller récupérer des informations sur des équipements du réseau (PC, routeurs, serveurs, …).

Les plugins n'utilisent pas tous le même protocole pour échanger les informations. Le protocole utilisé est dans la plupart des cas un facteur décisif sur le choix des plugins à utiliser.

Un seul plugin Nagios ne peut pas aller chercher toutes les informations sur les équipements du réseau: En effet, chaque plugin n'a accès qu'à certaines informations (exemple: un plugin peut aller chercher l'occupation du disque dur, et un autrel'occupation du processeur d'un PC). Pour superviser un parc informatique, il est donc nécessaire de mettre en place plusieurs plugins. De plus, certains plugins peuvent aller chercher des informations sur des clients uniquement sur certains systèmes d'exploitation (c'est le cas du plugin check_nt qui peut chercher des informations uniquement sur des équipements Windows).

Les principaux plugins utilisés par Nagios sont :

- ✓ check_disk : Vérifie l'espace occupé d'un disque dur
- ✓ check_http : Vérifie le service "http" d'un hôte
- ✓ check_ftp : Vérifie le service "ftp" d'un hôte
- ✓ check_mysql : Vérifie l'état d'une base de données MYSQL
- ✓ check_nt : Vérifie différentes informations (disque dur, processeur …) sur un système d'exploitation Windows
- ✓ check_nrpe: Permet de récupérer différentes informations sur les hôtes
- ✓ check_ping: Vérifie la présence d'un équipement, ainsi que sa durée de réponse
- ✓ check_pop: Vérifie l'état d'un service POP (serveur mail)
- ✓ check_snmp : Récupère divers informations sur un équipement grâce au protocole SNMP (Simple Network Management Protocol)

Il est possible de créer son propre plugin. Dans ce cas, il faudra les créer de la sorte que celui renvoie à Nagios :

- ✓ L'état du résultat (OK, CRITICAL, DOWN, UP, …)
- ✓ Une chaine de caractères (pour donner le détail du résultat)

5. Supervision passive et active

Nagios peut utiliser différentes méthodes dans le but de récolter les informations sur les machines du réseau. Une méthode dite active, et une autre passive. Les deux se basent sur l'exécution d'un daemon sur la machine à surveiller. Ces deux méthodes se combinent généralement pour une efficacité optimale de la supervision.

Nous rappelons que dans tout système d'exploitation multitâche, un démon est un programme informatique qui s'exécute en arrière-plan, et non sous le contrôle direct d'un utilisateur.

5.1. Les plugins actifs avec NRPE

A la différence des plugins locaux (ceux qui s'exécute sur la machine serveur, localhost, concernant ses propres ressources), le module/démon NRPE (Nagios Remote Plugin Executor) permet l'exécution de plugins dit actifs directement sur les machines à surveiller. Dans ce cas, la demande d'exécution du greffon actif est faite à l'initiative de la machine serveur Nagios.

La procédure interne est la suivante: Le serveur Nagios demande, via le client NRPE, l'exécution du plugin P sur la machine M. Le daemon NRPE hébergé sur la machine M, reçoit la requête d'exécution du plugin P. Ensuite l'exécution de ce plugin sur la machine M. Le daemon NRPE de la machine M récolte les informations suit à l'exécution du greffon P et envoi le résultat au serveur Nagios. Enfin le serveur Nagios interprète les résultats et lance le traitement adéquat.

Ce type de procédure permet d'assurer une surveillance distante .Il faudra toutefois ouvrir un port de communication pour permettre au NRPE de communiquer avec son client et récupérer les informations d'état concernant les machines déportées.

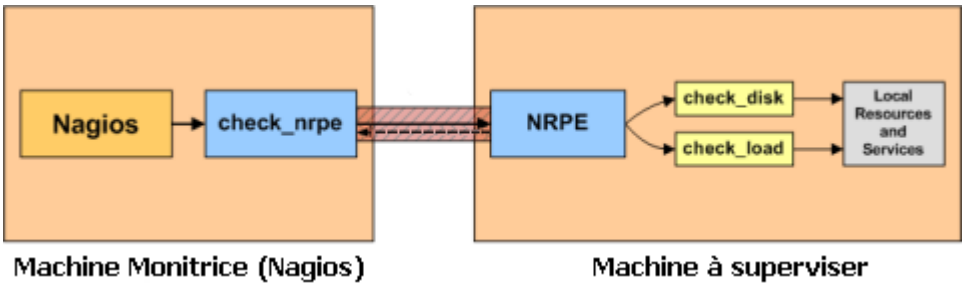

Figure 5 : Supervision active avec NRPE

Comme nous venons de le voir, NRPE est déclenché à l'initiative du serveur Nagios. Ce mode de fonctionnement présente des limites. Par exemple dans le cas où les machines à surveiller son derrière un réseau sécurisé ,NRPE ne permet que les connexions sortantes de celui-ci, ou encore si le processus à surveiller demande une fréquence d'exécution très courte. L'échange des informations n'est plus assuré. Dans ce cas nous avons recours aux greffons dits passifs.

5.2. Les plugins passifs avec NSCA

Le module NSCA propose l'exécution de plugins passifs sur les machines à surveiller. Leur exécution est déclenchée suite à des critères préalablement définis sur les machines distantes. Par exemple, le dépassement de 75% de la capacité de stockage, la détection d'une activité réseau anormale ou simplement des checks périodiques sous forme de mises à jour auto-déclenchées.

La procédure interne est la suivante : Le daemon NSCA sur une machine M lance l'exécution du plugin P suite à un critère de déclenchement vérifié. En effet le plugin P est exécuté sur la machine M. Le daemon NSCA de la machine M récolte les informations suite à l'exécution du greffon P et envoi le résultat au serveur Nagios. Enfin le serveur Nagios interprète les résultats et lance le traitement adéquat.

Nous remarquons bien que dans ce cas, la demande d'exécution du greffon est faite non pas l'initiative de la machine serveur Nagios mais à celle de la machine distance elle-même.

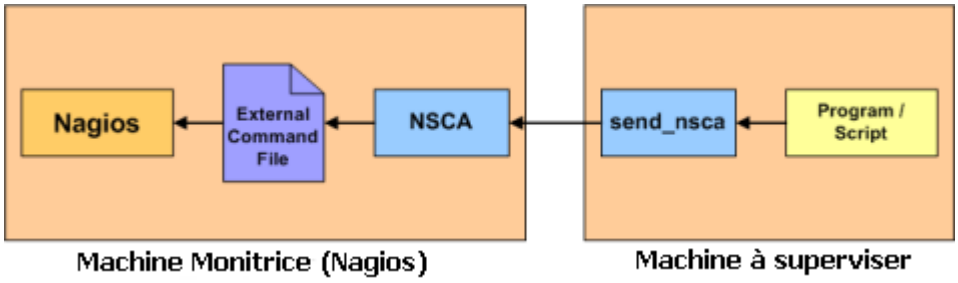

Figure 6 : Supervision active avec NSCA [4]

La figure 6 Présente la supervision active avec NSCA. Nous remarquons que la demande d'exécution du greffon est faite non pas par l'initiative de la machine serveur Nagios , mais par l'initiative de la machine distance elle-même (la machine à superviser) suite à un critère de déclenchement vérifié.

Dans la pratique, les vérifications sont rarement passives, nous avons eu recours à cette méthode dans certains cas où la sécurité impose d'interdire une connexion dans un sens, ou encore dans le cas de supervision hiérarchique, mais le plus souvent les vérifications sont actives.

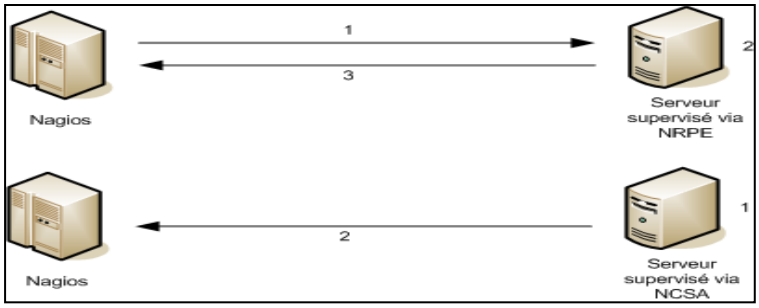

Figure 7 : Schéma comparatif NRPE-NSCA [5]

La figure 7 présente un schéma comparatif entre les plugins actifs NRPE et les plugins passifs NSCA

Dans ce projet, nous nous limiterons au cas de la supervision active.

6. Les fichiers de configurations :

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 fonctionnement des CGI. Il peut être intéressant pour définir 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 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 définit les paramètres des alertes (fréquences des notifications, moyens pour contacter ces personnes, plages horaires d'envoi des alertes...).

Conclusion :

Après avoir bien étudié l'outil de supervision open source choisi, nous allons passer dans le chapitre suivant à sa mise en place au sein de l'entreprise.

Chapitre4 : Mise en place de la solution de supervision adoptée

Introduction :

.Dans ce chapitre, nous décrirons en premier lieu le réseau sur lequel nous avons mis en place notre outil de supervision ainsi le fonctionnement de la machine de supervision NAGIOS et leur implémentation dans notre réseau. Après nous présenterons la mise en place de la machine cliente Windows qui simulera le rôle d'un serveur Windows et la configuration et la supervision d'une imprimante IP. Enfin nous développerons un plugin pour vérifier le lancement du processus apache.

1. Préparation du réseau :

Notre réseau comporte les équipements suivant :

- ✓ Un serveur Linux nommé ABIR sur lequel sera installé Nagios pour superviser notre réseau. Il aura pour adresse IP 172.20.90.123
- ✓ Un serveur Windows SRV-SDC qui sera supervisé. Il aura pour adresse IP 172.20.95.3
- ✓ Un serveur Windows serDRH qui sera supervisé. Il aura pour adresse IP 172.20.95.11
- ✓ Une imprimante réseau Epson Acluaser M8000N et qui aura comme adresse IP 172.20.95.105

Au niveau de l'installation, Nous nous sommes intéressés par les dernières versions existantes en 2015, et qui sont compatibles entre eux pour être communiqué ensemble et fournir une meilleure interprétation sur des équipements à superviser. Donc les versions des logiciels utilisés dans notre projet sont les suivants :

- ✓ L'outil de supervision nagios-4.1.0rc1.
- ✓ Les plugins de Nagios, nagios-plugins-2.0.3.
- ✓ L'agent NSClient++ pour la supervision des machines windows, nscp-0.4.3.

2. Serveur NAGIOS :

L'installation de Nagios ainsi sa configuration est relativement difficile comparée à des autres outils de supervision. Il faut avoir des connaissances concernant l'utilisation du terminal de linux et plus précisément d'Ubuntu (installation manuelle des paquets, modification des droits, créations des utilisateurs…).

Avant de commencer nous avons besoin d'installer Apache et PHP car nous visualiserons les données à travers une interface web. Il nous faudra également installer "**Net-SNMP**" afin de pouvoir lancer des requêtes snmp pour superviser des routeurs ou switchs par exemple. Nous avons installé aussi quelques librairies, en utilisant cette commande :

Sudo apt-get install fping libnet-snmp libdap –dev libmysql-dev libradiusclient-ng-dev

Après nous avons téléchargé les paquets d'installation des versions stables disponibles à partir du site de officiel de Nagios qui sont : le paquet de l'outil Nagios (Version 4.1.0) et le paquet contenant les plugins (Version 2.0.3).

Après le téléchargement, l'enchaînement classique d'installation manuelle des paquets sur linux se met en place avec la décompression, le désarchivage, la compilation, les make…Ci-dessous un exemple des commandes nécessaires à l'installation du Core Nagios.

tar xzf nagios-4.1.0.rc1.tar.gz

cd nagios-4.1.0.rc1

./configure

make all

make install

make install-init

ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios

Une fois les deux paquets installés, nous pouvons vérifier s'il ya un problème de localisation des fichiers ou une redondance de définition dans les fichiers de configuration en utilisant la commande suivante.

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

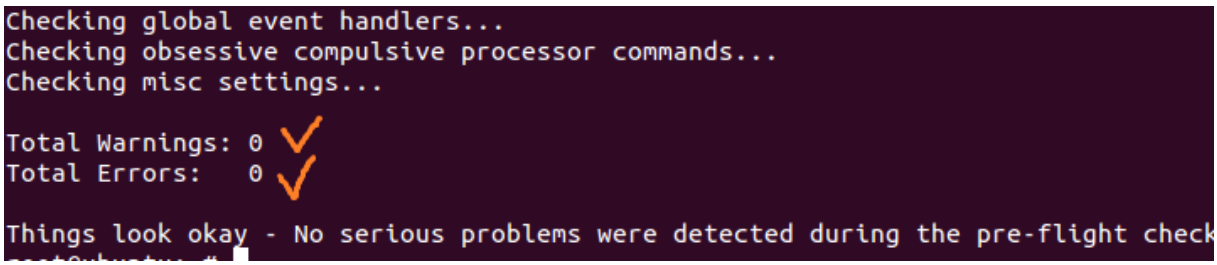

Figure 8 : ***Test des fichiers de configuration***

Les étapes d'installation du serveur NAGIOS sont détaillés dans l'annexe A

Il ne reste plus qu'à utiliser le navigateur Web saisir l'URL : *http://172.20.90.123/nagios/*, après avoir entré le nom d'utilisateur et le mot de passe nous accédons enfin à la page Web interne de Nagios comme s'est indiqué dans la figure 9.

Figure 9: Page d'accueil de Nagios

3. Machine Windows :

Pour surveiller les machines fonctionnant sous le système d'exploitation Windows nous avons besoin d'un daemon (responsable d'une tâche exécutée en arrière-plan) sous le nom de NSClient++.

3.1. Présentation du NSClient++ :

NSClient++ est un démon de surveillance simple et efficace pour les systèmes d'exploitation Windows. Il a été conçu spécialement pour Nagios, mais il n'en est pas dépendant. NSClient++ pourrait sans doute, être intégré dans n'importe quel logiciel de surveillance. La structure du démon consiste en un service simple qui charge les plugins d'une pile interne. Ces derniers peuvent alors demander des informations résultantes de l'exécution de ces plugins.

Il n'utilise pas le protocole de supervision SNMP. En fait, il utilise ses propres données puisque le système est un système Client-serveur, comme le montre la figure 10.

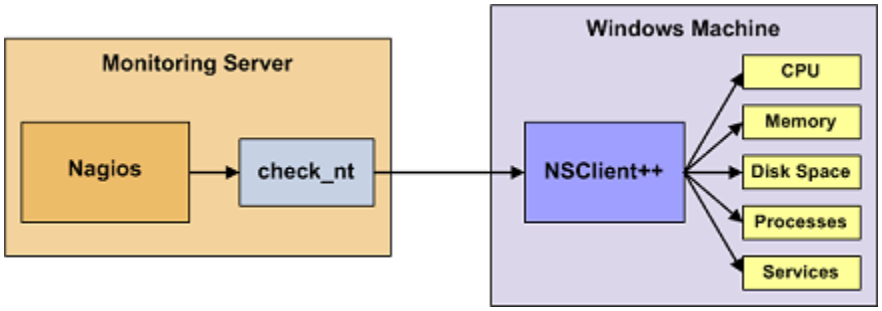

Figure 10: Architecture NSCLIENT

C'est un plugin qui permet de récupérer un nombre important d'informations. Il faut tout d'abord savoir que le logiciel Nsclient ++ est destiné aux machines Windows. Il existe également un plugin destiné aux machines linux, présenté si dessous. La partie cliente (nommée check_nt), doit être présente sur le serveur Nagios. La partie serveur (Nsclient++) est à installer sur chacune des machines Windows à surveiller. Ce plugin permet de retourner de nombreuses informations telles que la charge de la CPU, la mémoire utilisée, ou encore l'espace disque...)

3.2. Installation et Configuration :

L'agent possède un exécutable d'installation. Il s'installe par défaut dans le répertoire C:\Program Files\NSClient++. Nous avons téléchargé et installer la version 0.4.3 de NSClient.

Avant de lancer le service, il faut modifier le fichier de configuration nsclient.ini avec l'éditeur de texte classique de Windows. Il faut plus précisément dé-commenter quelques lignes nécessaires à son fonctionnement. Il faut aussi définir le mot de passe de la connexion entre les deux machines (password = nagios) et les utilisateurs apte à accéder aux informations retournées (allowed hosts = 172.20.90.123/20, qui est l'adresse de notre serveur de supervision Nagios).

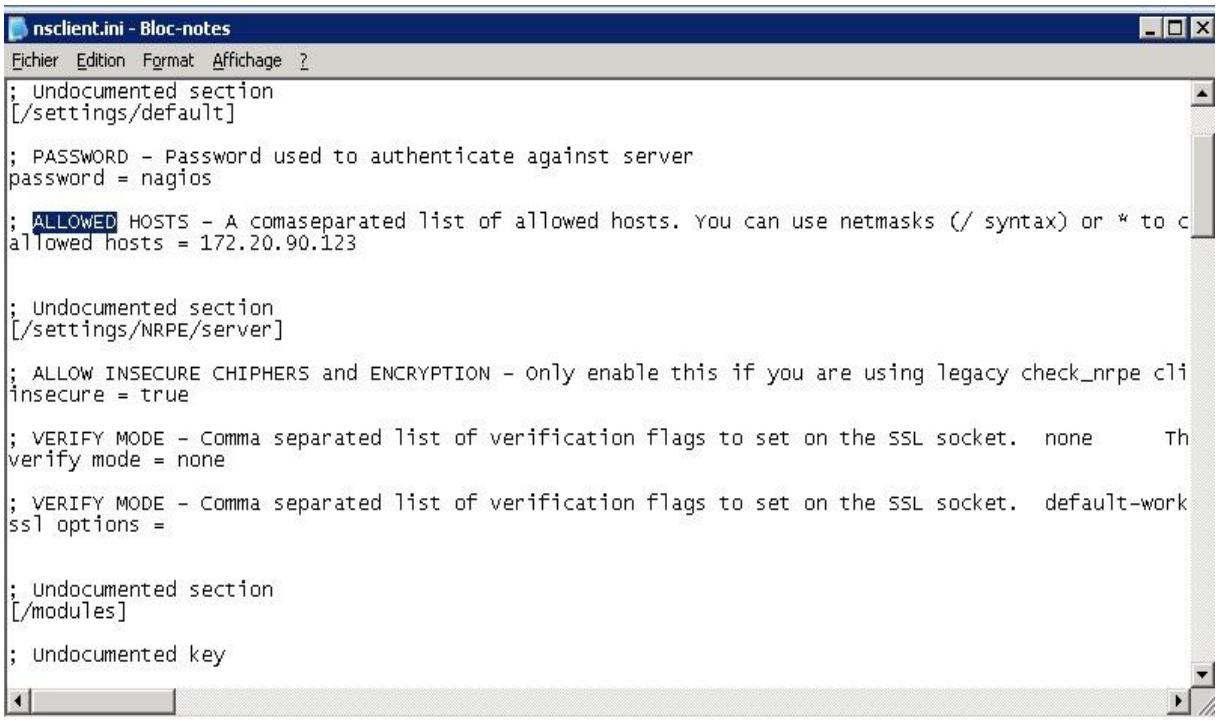

Figure 11 : Configuration du NSClient via le nsc.ini

La configuration continue sur la machine monitrice. Il faut maintenant déclarer la machine à travers son nom et son adresse IP dans le fichier de configuration /usr/local/nagios/etc/objects/windows.cfg

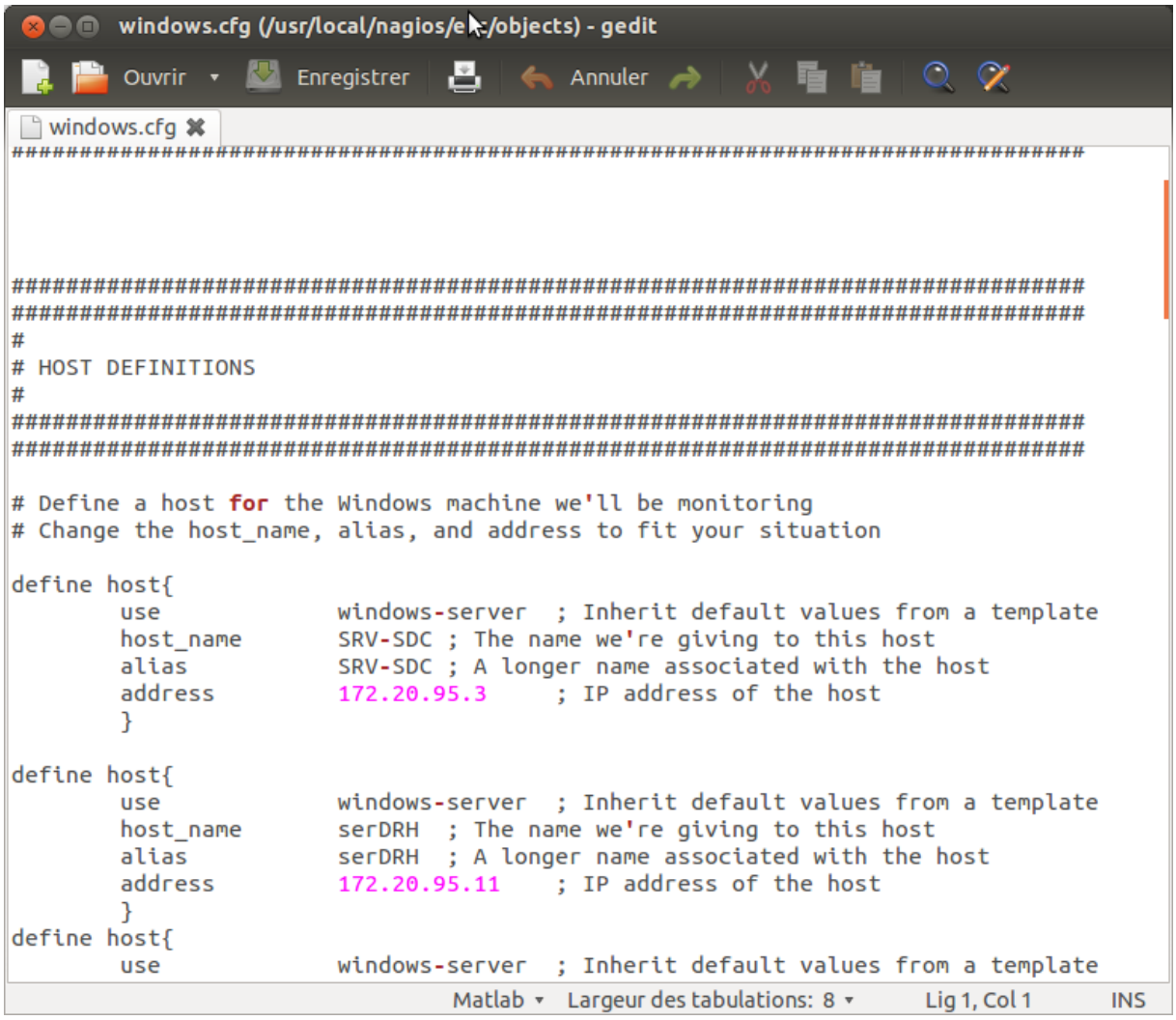

Figure 12 : Déclaration des serveurs Windows SRV-SDC et serDRH

Nous passons ensuite à la déclaration des vérifications que nous souhaitons faire dans le fichier Windows.cfg. Pour cela, un plugin sous le nom check_nt parmi ceux télécharger est dédié au cas des machines Windows. IL permet de faire appel aux checks existants dans la pile interne du service NSClient. Il faut donc indiqué le nom de la machine (host_name SRv-SDC), le service à hériter (use generic-services), et la commande du check_nt à combiner avec d'autres checks (check_command check_nt !CPULOAD) et refaire la même

configuration pour la machine serDRH. La déclaration se fait comme expliqué sur la figure13

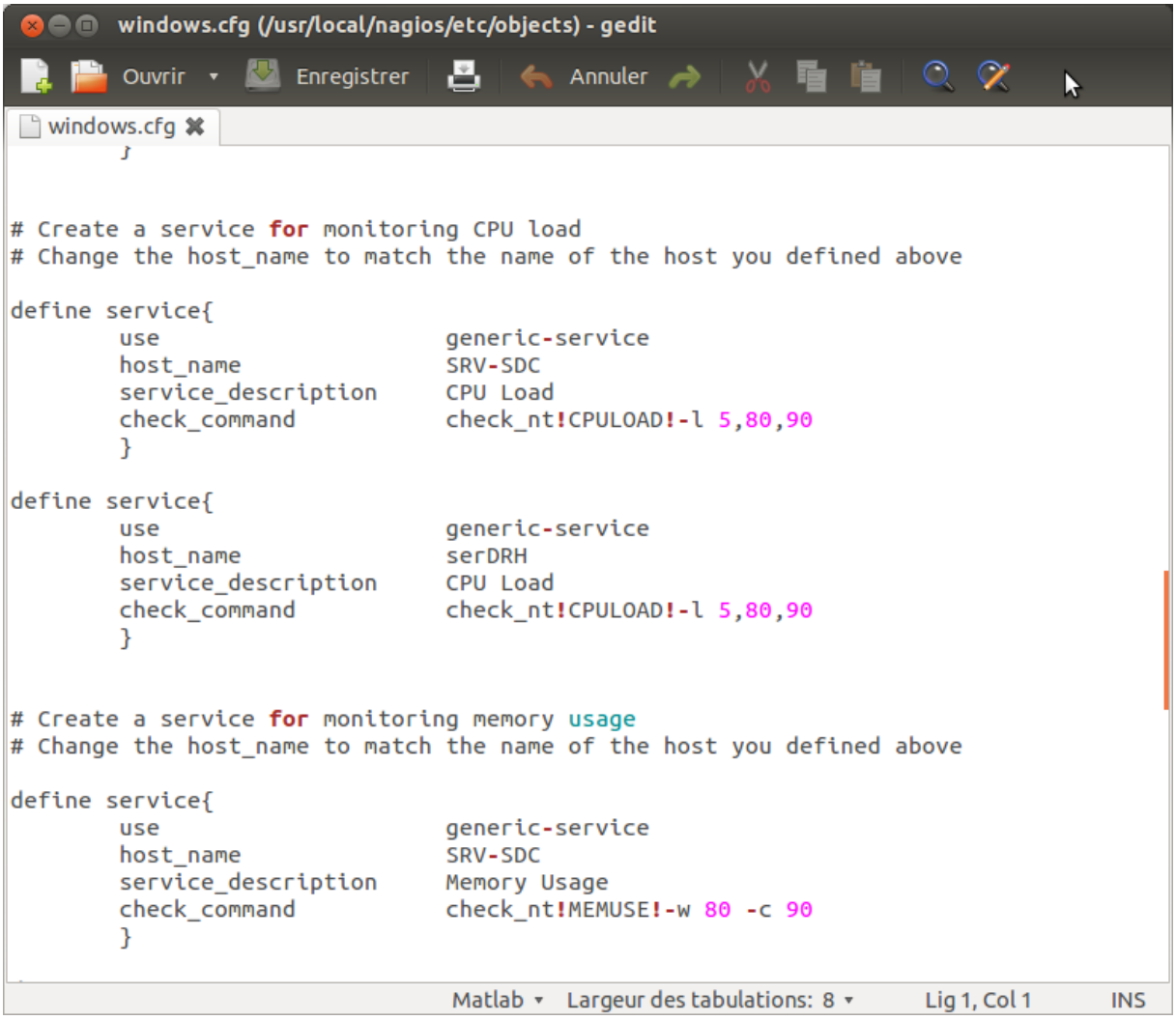

Figure 13 : Déclaration des checks de SRV-SDC et serDRH

3.3. Les tests :

Nous laissons le programme faire la collecte et le traitement des données pendant quelques minutes avant d'actualiser l'interface de Nagios.

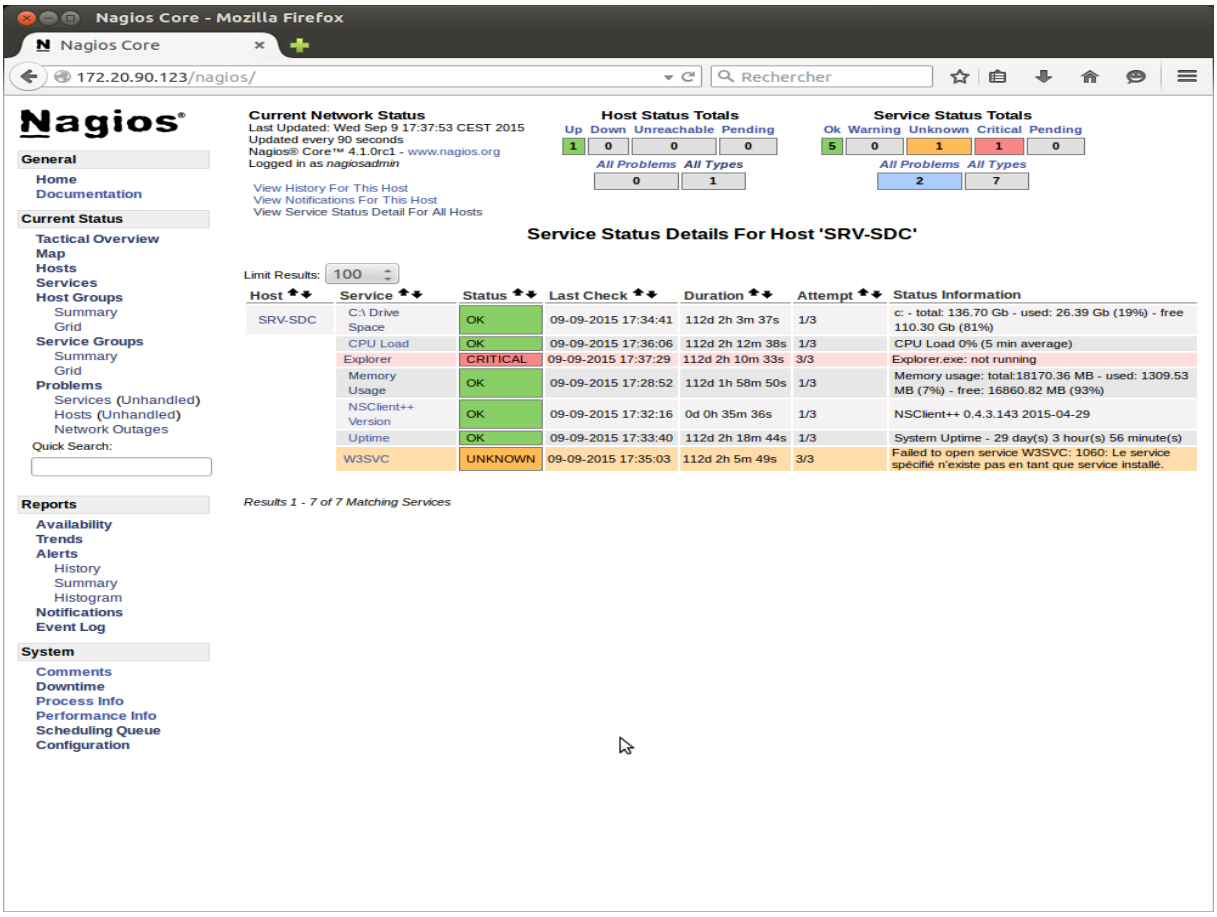

Figure 14 : Affichage des résultats des checks de SRV-SDC

L'administrateur possède à une heure précise à travers Nagios quelques informations additionnelles l'aidant à mieux anticiper les pannes :

Pour le serveur SRV-SDC, nous constatons comme illustré dans la figure10 que :

- L'état du l'espace disque est : OK. En fait pour un disque du 136.7Gb seulement 26.39Gb sont utilisés représentant 19% de la taille totale du disque et 110.30Gb sont libres ce qui est équivalant à 81%.
- L'état de la charge du processeur est : OK.
- L'Etat du service explorer est critique en fait il n'est plus démarré.
- L'état de l'utilisation de la mémoire est : ok. En fait la taille totale de la mémoire est 16Gb. Seulement 7% ce cette mémoire est utilisé.

- L'état du service UPTIME est OK. Le serveur n'a pas été arrêté depuis 30 jours et 54 minutes.

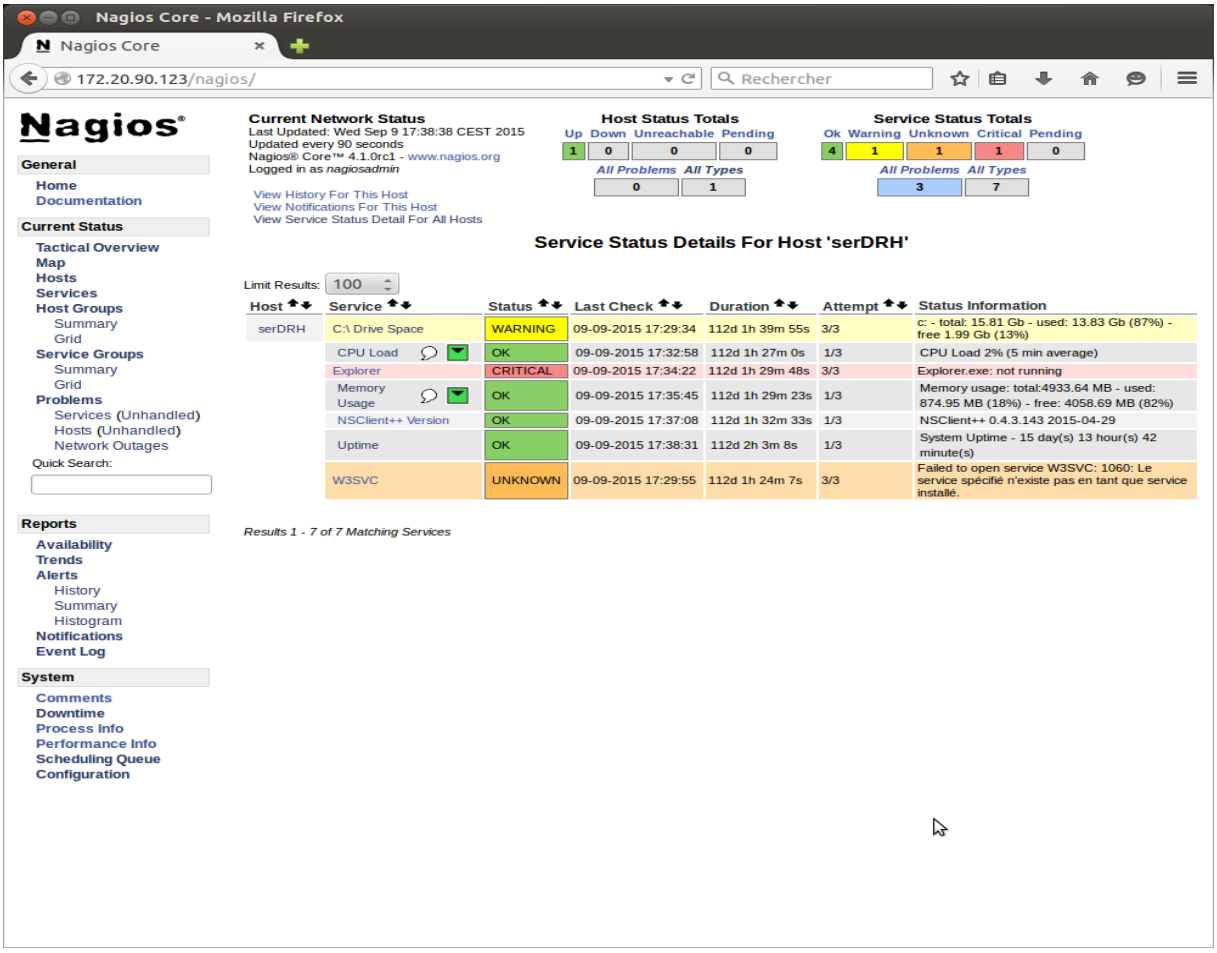

Figure 15 : Affichage des résultats des checks de serDRH

Pour le serveur serDRH, nous constatons que :

- L'état du l'espace disque est alarmant. En fait pour un disque du 15.81Gb , 13.83Gb sont utilisés représentant 87% de la taille totale du disque ce qui est très critique pour un serveur d'application.
- L'état de la charge du processeur est : OK.
- L'Etat du service explorer est critique en fait il n'est plus démarré.
- L'état de l'utilisation de la mémoire est : ok. En fait la taille totale de la mémoire est 4Gb. Seulement 17% ce cette mémoire est utilisé.

- L'état du service UPTIME est OK. Le serveur n'a pas été arrêté depuis 16 jours et 10 minutes.

4. Configuration d'une imprimante :

Nous passons à rappeler le principe général de la supervision d'une imprimante, avant de présenter sa définition dans les fichiers de configuration de Nagios.

4.1. Principe de la supervision d'une imprimante :

La supervision de l'état d'une imprimante réseau est simple. Les imprimantes compatibles JetDirect ont en général SNMP activé, ce qui permet à Nagios de les superviser en utilisant le plugin check_hpjd, comme elle est montrée dans la figure 16.

4.2. Définition d'une imprimante :

. Nous avons défini l'imprimante réseau que nous souhaiterons superviser dans le fichier de configuration /usr/local/nagios/etc/objects/printer.cfg

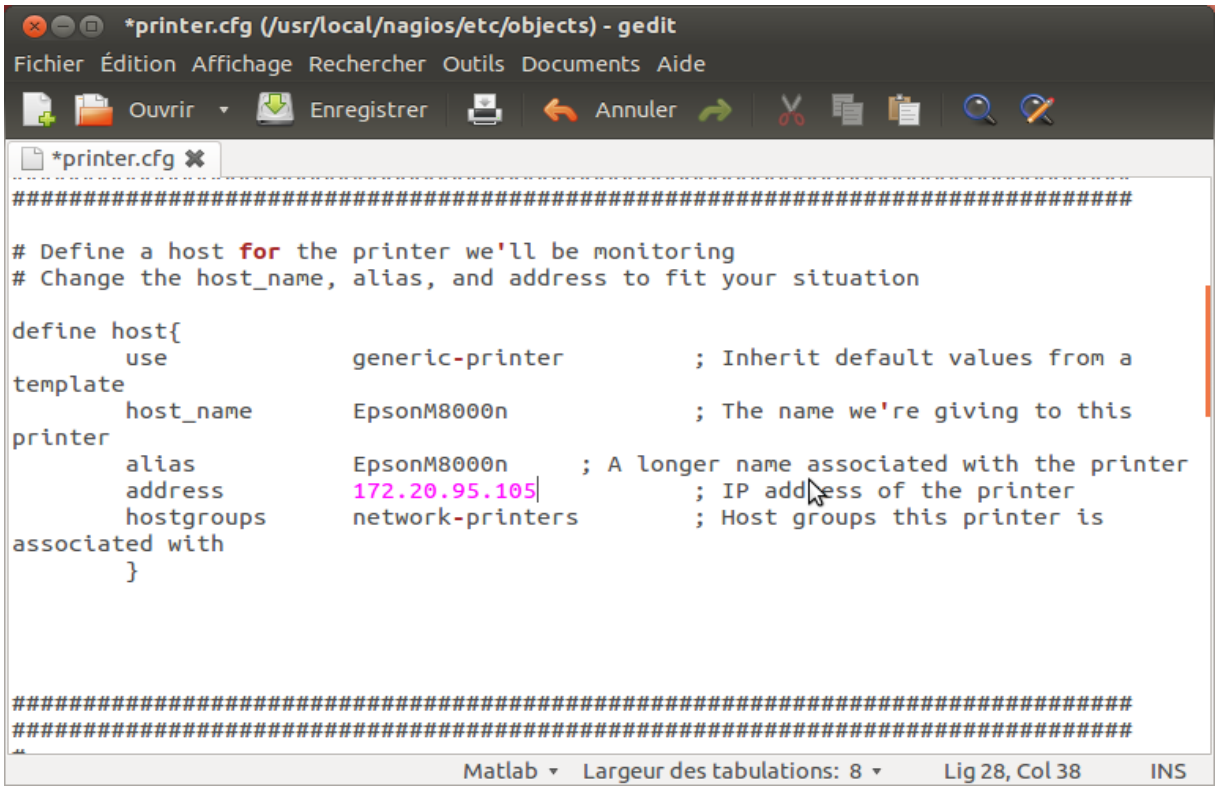

Figure 16: Définition de l'imprimante IP dans le fichier de configuration printer.cfg

4.3. Définition des services pour les imprimantes :

Ensuite, nous avons ajouté quelques définitions de services comme indiqué dans la figure17 (Dans le même fichier de configuration) pour superviser les différents aspects de notre imprimante.

- ✓ Le service PING permet de vérifier l'envoi des pings vers l'imprimante toutes les 10 minutes par défaut. C'est utile pour superviser le RTA(Le temps moyen qui a mis l'hôte pour répondre), les paquets perdus et la connectivité réseau.
- ✓ Le service printer status permet de vérifier l'état de l'imprimante. Le service utilise le plugin check_hpjd pour vérifier l'état de l'imprimante toutes les 10 minutes par défaut. La communauté SNMP utilisée dans cet exemple pour interroger l'imprimante est 'public'.

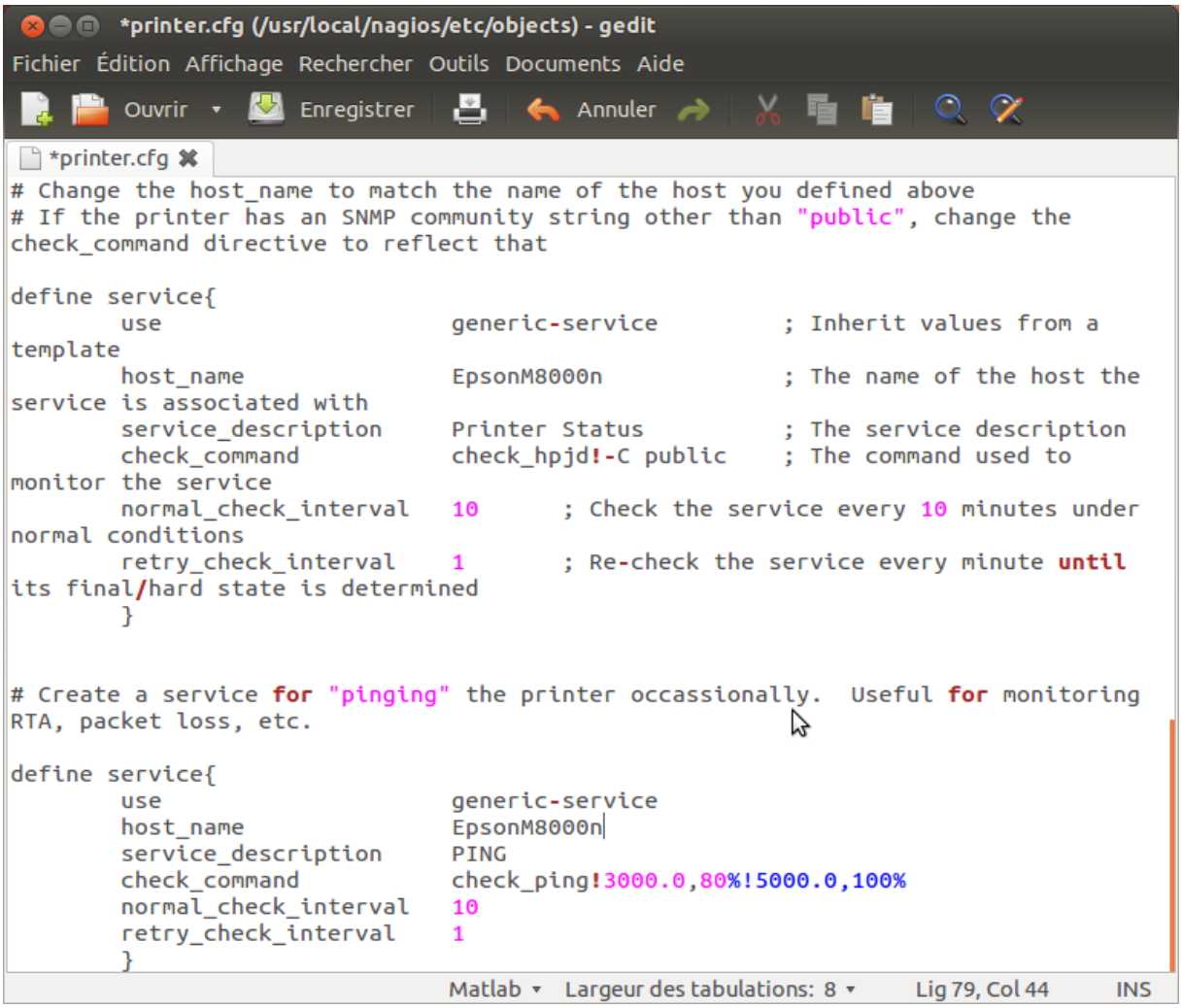

Figure 17: Définition des services de l'imprimante IP

Comme indiqué dans la figure18, l'administrateur peut constater à tout moment l'état de la connexion réseau de ces imprimantes IP ainsi que leurs statuts.

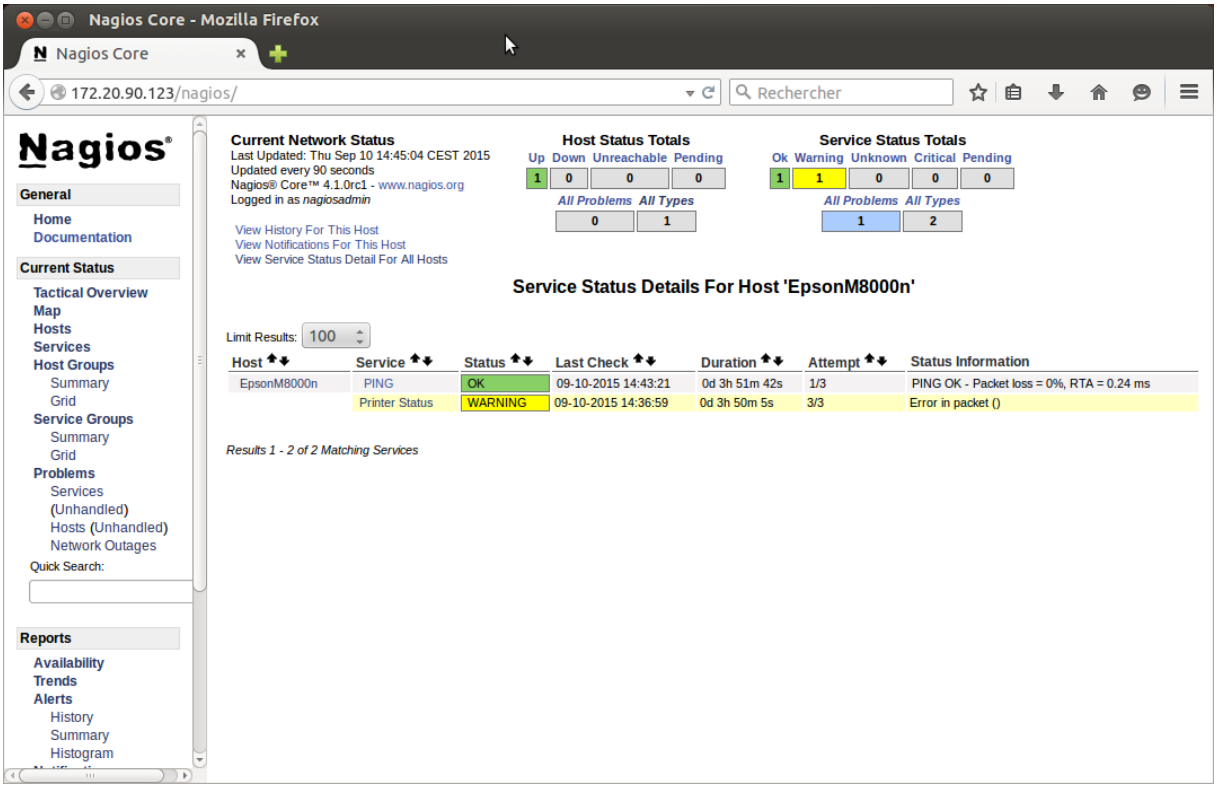

Figure 18: Résultat du check de l'imprimante IP

5. Alertes :

La solution de supervision doit faire gagner du temps aux administrateurs. La concision des alertes est un premier pas dans cette direction.

Les administrateurs n'aiment pas perdre de temps lorsqu'il s'agit d'alertes sur leurs serveurs ou éléments réseau. Ils veulent que l'information soit énoncée rapidement et clairement. L'alerte doit être suffisamment explicite pour permettre à l'administrateur de savoir d'où vient le problème.

Les informations généralement nécessaires sont les suivantes :

- ✓ Le nom de la machine sur laquelle le problème est survenu.
- ✓ L'élément qui est en faute sur la machine.
- ✓ La criticité de l'alerte.

- ✓ L'heure où le problème a été détecté.
- ✓ Un petit texte explicatif du problème (une ligne ou deux maximums).

5.1. Configuration des contacts :

La configuration commence par celle des contacts devant être avertis et, en tout premier lieu, par le moyen d'alerte souhaité.

Le contact que nous allons définir est l'administrateur. Il veut être averti par le biais d'un e-mail pour chaque problème. La configuration se fait au sein du fichier /etc/nagios/objects/contacts.cfg.

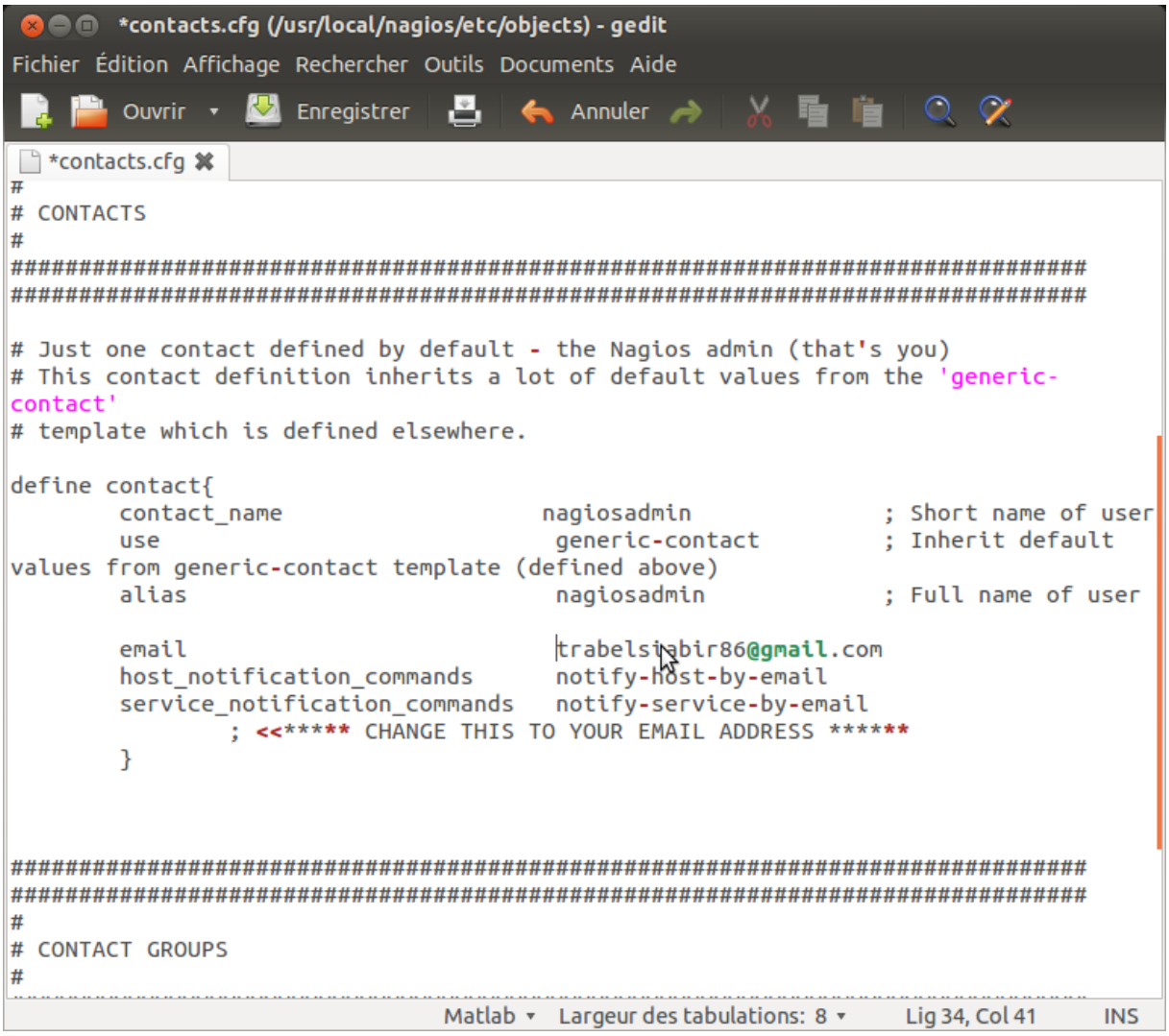

Figure 19: Configuration des contacts

5.2. Configuration des commandes :

Les alertes doivent porter sur les hôtes et les services qu'ils hébergent. Regardons, dans la configuration standard de Nagios, la définition des commandes envoyant un e-mail aux administrateurs. Elles figurent dans le fichier /etc/nagios/objects/commands.cfg :

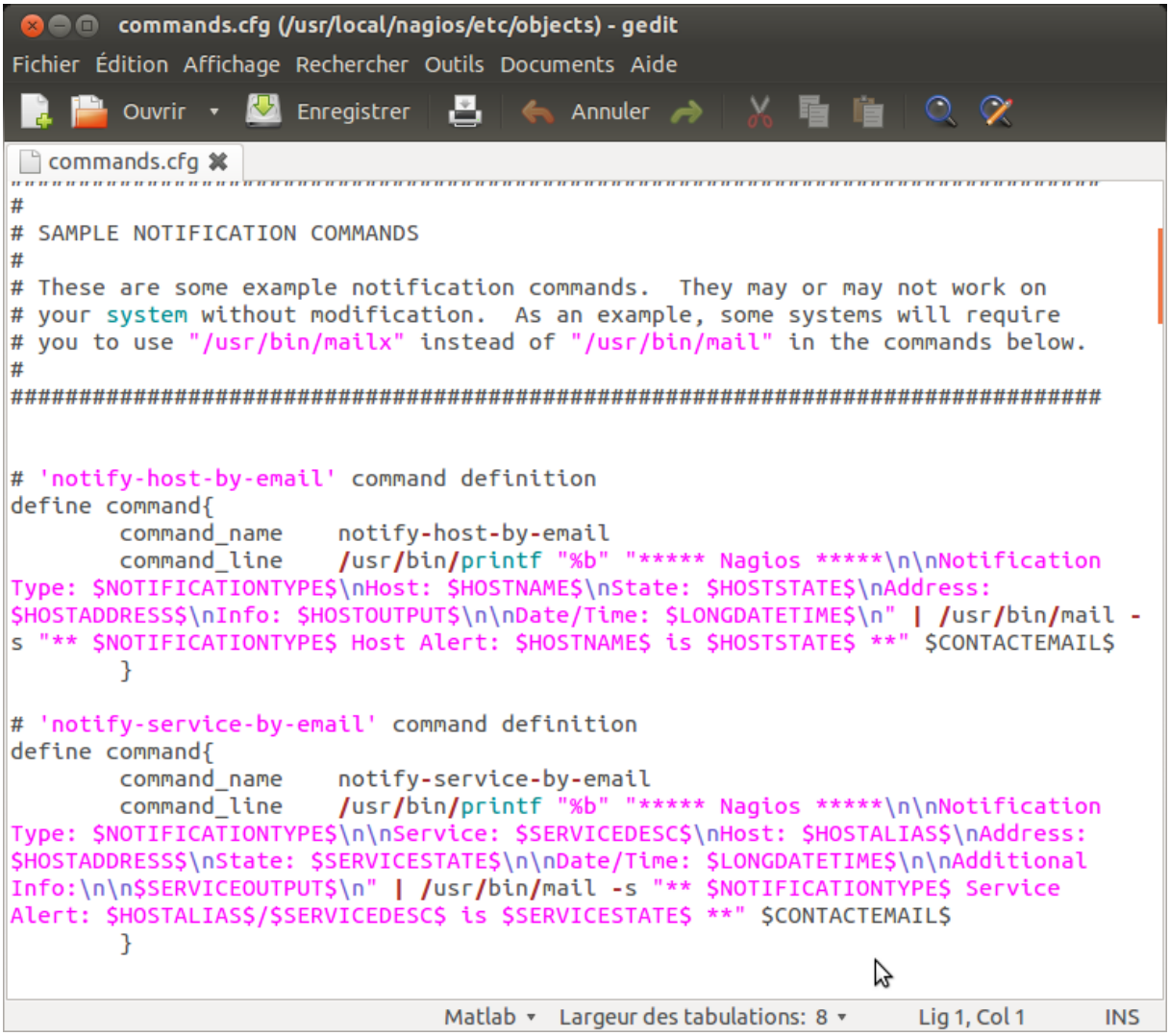

Figure 20: Commandes d'envoi par mail

Le fonctionnement de ces commandes est simple malgré leur longueur. Elles réalisent l'envoi de l'e-mail en deux étapes. Tout d'abord, elles génèrent le texte du message. Lors de l'appel à la commande pour l'envoi d'une notification, les macros sont modifiées par les valeurs du contexte de l'erreur.

Une fois ce texte généré, il est envoyé sur l'entrée standard de la commande /bin/mail. Cette dernière sert tout simplement à envoyer un e-mail. Le paramètre -s sert à paramétrer le titre, qui est également appelé avec des macros. Le dernier argument correspond à l'adresse du destinataire du message.

5.3. configuration du ssmtp

Un service d'envoi d'e-mail est nécessaire sur le serveur de supervision. À ce propos, sur la distribution installée ici, c'est le programme Sendmail qui est installé par défaut. Nous allons utiliser SSMTP (pour Simple SMTP).

On configure SSMTP en éditant le fichier texte /etc/ssmtp/ssmtp.conf comme indiqué dans la figure 21.

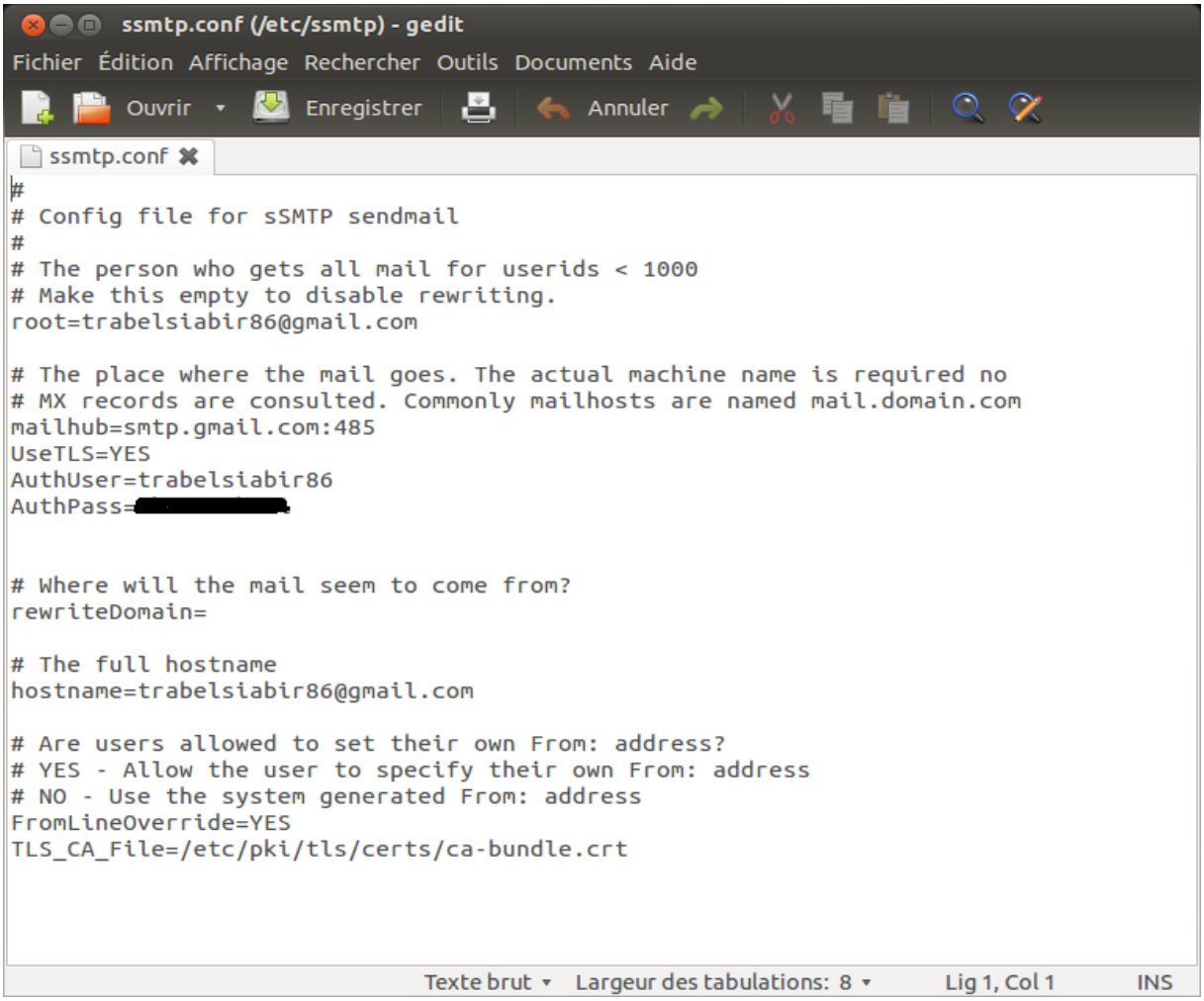

Figure 21: Configuration du ssmtp.conf

Puis on passe à la configuration du fichier /etc/ssmtp/revaliases :

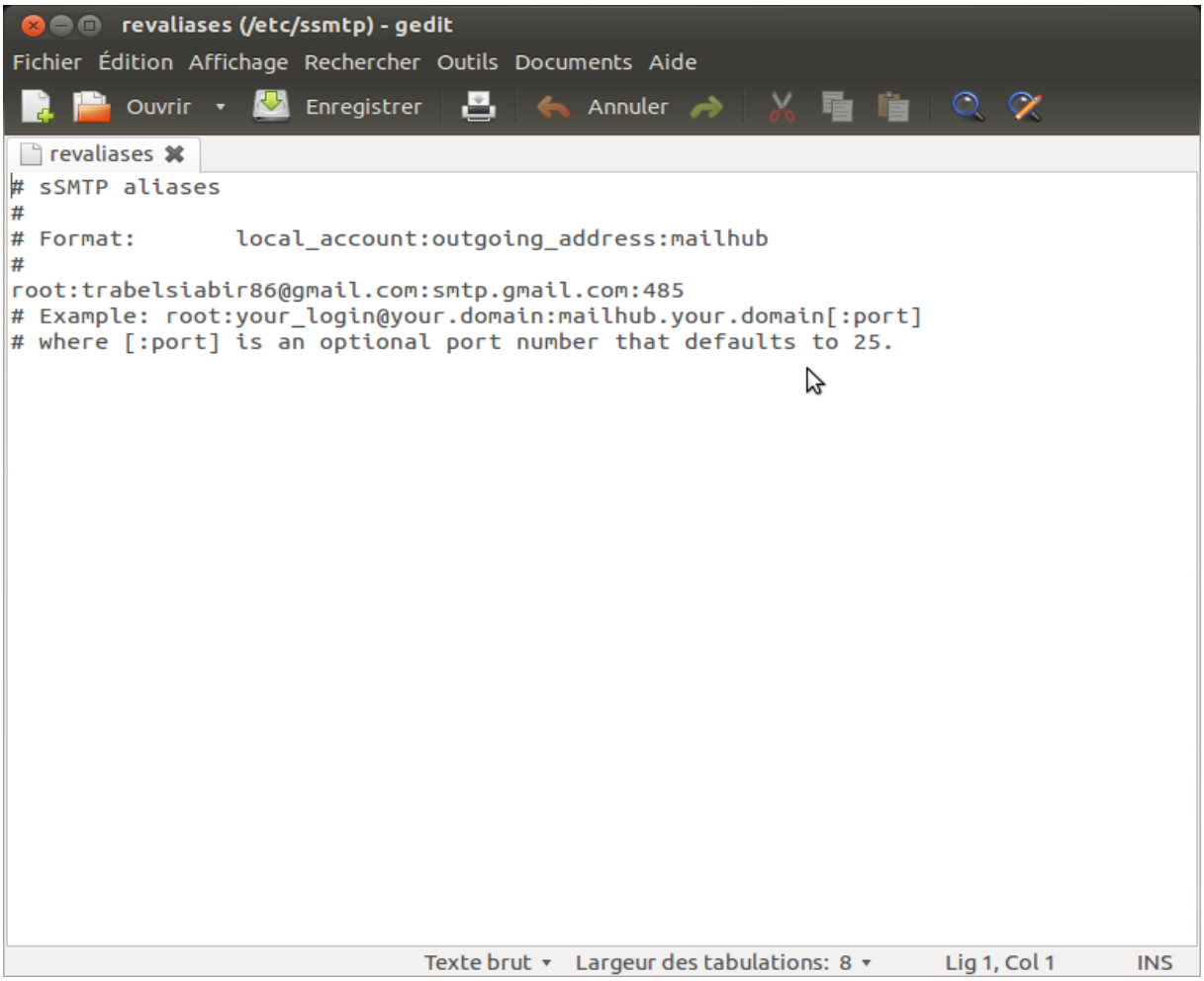

Figure 22: confiugration du revaliases

5.4. Configuration des périodes

Les périodes sont définies au sein du fichier suivant :/etc/nagios/objects/timeperiods.cfg.

La période qui nous intéresse ici est de 24 heures sur 24, 7 jours sur 7.

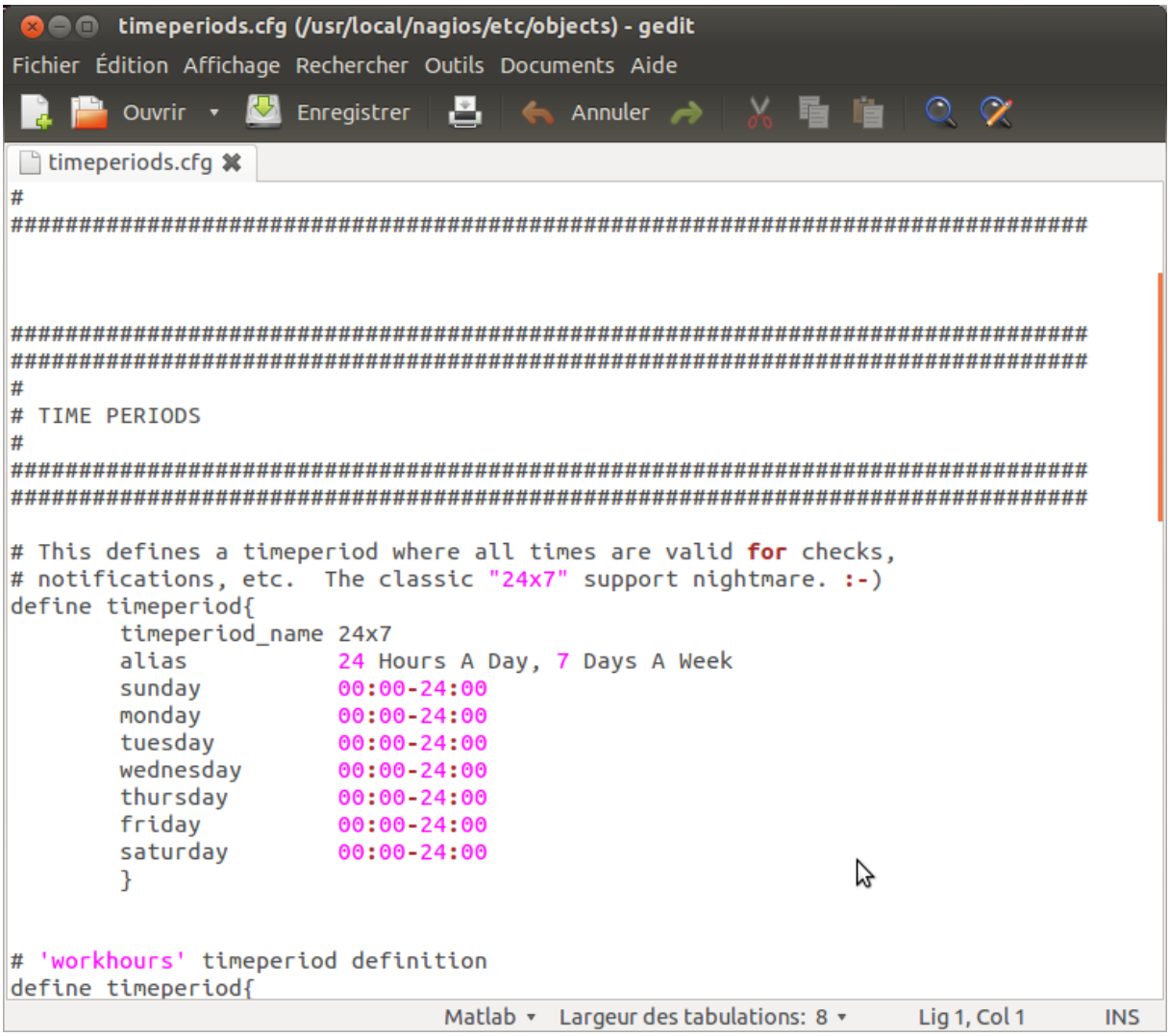

Figure 23 : configuration de période

Conclusion :

Nous avons essayé dans cette partie d'installer, de configurer et de tester Nagios dans la société ELFOULADH.

Conclusion générale

L'objectif de notre projet était de permettre à l'administrateur de l'entreprise de mieux superviser les équipements et les services de son réseau. En effet une solution de supervision permet de diminuer le taux lors de diagnostic des pannes et faciliter les tâches de l'administrateur réseaux.

Plus le nombre des équipements et des services informatiques augmente plus les tâches de l'administrateur deviennent trop compliquées et il n'arrive pas à les assurer convenablement ce qui engendre une perte du temps et un travail con accomplie.

Notre travail consistait à mettre en place un outil de supervision système et réseau. Dans un premier lieu, nous avons pu étudier l'existant et dégager ses limites afin de fixer la solution retenue après avoir réalisé une étude comparative entre les différentes solutions open source existantes sur le marché. Dans la partie réalisation, nous avons mis en place l'outil NAGIOS et le configurer sur les serveurs Windows et une imprimante réseau pour les mieux superviser et alerter l'administrateur par mail en cas de pannes.

Comme perspectives, nous proposons l'amélioration de ce travail par :

- La configuration des notifications par SMS.
- La supervision des services de bases de données
- La supervision des switchers dès que l'entreprise finisse la mise en place et la configuration des nouveaux switchers niveau3

Annexe A : Installation de Nagios

Nagios est un système d'exploitation linux installer sur le serveur ou nous aurons mise en place notre solution. Nous avons choisi d'utiliser la distribution Ubuntu Server Edition 14:04 pour le télécharger dans notre serveur.

Comme étant une première étape pour l'installation, Nous allons créer un utilisateur et un groupe dédié au processus Nagios (pour d'évidentes raisons de sécurité) et un autre groupe « nagcmd » permettant l'exécution des commandes externes à travers l'interface Web. Puis nous avons rajouté des utilisateurs Nagios et Apache à l'intérieur du groupe « nagcmd ».voici quelque commande nous utiliser comme une premier étape :

sudo useradd --system --home /usr/locale/nagios -M nagios

sudo groupadd --system nagcmd

sudo usermod -a -G nagcmd nagios

sudo usermod -a -G nagcmd www-data

Par la suite nous passons d'installer quelques bibliothèques. Nous allons installer apache2, php et gd, sont utiles pour la future interface de Nagios, make et gcc pour les compilations, et snmp pour superviser les routeurs, switch…, ainsi nous avons besoin d'installer quelque autre librairies. Nous avons utilisé donc la ligne de commande suivante :

sudo apt-get install apache2 libapache2-mod-php5 php5-gd php5 make gcc build-essential wget libgd-gd2-perl libgd2-dev libgd2-xpm libgd2-xpm-dev libnet-snmp-perl libssl-dev snmp daemon

Maintenant le temps de télécharger les paquets d'installation des versions stable disponible à travers le site officiel de Nagios http://Nagios.downlod.org , et qui sont le paquet de Nagios core (version 4.1.0rs1) et le paquet de nagois-plugins (version 2.0.3).

cd /tmp

wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.1.0rc1.tar.gz

wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz

Après avoir téléchargé les paquets, nous avons les décompresser.

tar xzvf Nagios-4.1.0rc1.tar.gz

tar xzvf nagios-plugins-2.0.3.tar.gz

Ensuite, il est très important de nous déplaçons dans le dossier extrait de l'archive de nagios et configurer la compilation:

sudo cd Nagios-4.1.0rc1

sudo ./configure \

> --with-nagios-group=nagios \

> --with-command-group=nagcmd \

> --with-mail=/usr/sbin/sendmail \

> --with-httpd_conf=/etc/apache2/conf-available

A la suite, Nous allons installer les scripts de démarrage pour que Nagios se lance automatiquement avec notre serveur de supervision :

Commencons a Compilé les codes sources.

sudo make all

Nous Installons ainsi le binaire suivant.

sudo make install

sudo chown -R nagios:nagios /usr/local/nagios/libexec/eventhandlers

Par la suite, nous avons testé les fichiers de configuration s'il y a un problème de localisation des fichiers ou une redondance de définition:

sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Pour rendre l'accès à notre interface Nagios plus sécurisé, nous avons créé à cette dernière un login (nagiosadmin) et un mot de passe (nagios).

sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

Nous sommes retournées sur le chemin que nous avons procédé à l'installation du plugin. Pour compilée les codes sources de plugins

cd ..

cd tmp/nagios-plugins-2.0.3

sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios --enable-perl-modules --with-enable-extra-opts

sudo a2enmod cgi

sudo vi /etc/apache2/sites-enabled/000-default.conf

sudo service apache2 restart

sudo /etc/init.d/nagios checkconfig

sudo /etc/init.d/nagios

Nous pouvons maintenant connecter à l'interface web de Nagios via l'adresse IP de notre serveur, Après l'authentification qui lui demandé notre nom utilisateur (nagiosadmin) et notre mot de passe que nous avons spécifié plus tôt.

Il ne reste que le lancement de serveur apache et le serveur Nagios avant qu'il se puise accéder à l'interface de notre moniteur.

Bibliographie

[1] : http://www.o00o.org/monitoring/bases.html

[2] : https://bencherifcheikh.wordpress.com/2012/08/08/le-protocole-snmp/

[3] : http://www.frameip.com/snmp/

[4] : http://ram-0000.developpez.com/tutoriels/reseau/SNMP/

[5] : https://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal

[6] : Livre Nagios3 pour la supervision et la métrologie

[7] : Livre Nagios au cœur de la supervision Open source