Les outils d'administration et de supervision réseau

L'exemple de Nagios

Compte rendu

Thierry Briche

Matthieu Voland

Document réalisé sous LaTeX

Version 1.00
Décembre 2004

Table des matières

1 Introduction

1.1 Etat des lieux

La taille des réseaux ne cessant de grandir de jour en jour et l'importance de ceux-ci dans le monde de l'entreprise prenant une place prépondérante, le besoin de contrôler en temps réel leur qualité et leur état est rapidement devenu une priorité. C'est dans ce but qu'est apparu, il y a maintenant une vingtaine d'années, le concept de supervision de réseaux.

Nous présenterons dans ce document ce qu'est la supervision de réseaux ainsi que l'implémentation qui en a été faite. Pour ce faire nous définirons en premier lieu les concepts et les notions de la supervision de réseaux et nous présenterons ce que la normalisation a apporté en réponse à ces problématiques et plus particulièrement dans le monde IP. Nous étudierons ensuite l'exemple du plus en plus populaire Nagios, un logiciel libre dédié à la supervision de réseaux .

1.2 Problématique

Les réseaux ont vu un essor rapide accompagné par la découverte de nouvelles technologies. Les entreprises entrevoyant les possibilités offertes par ces nouveaux apports ont été amenées à les assimiler très vite, ce qui implique donc la cohexistence de milieux très hétérogènes aux divers niveaux de l'architecture d'interconnexion des systèmes ouverts (OSI : Open System Interconnection), aussi bien au niveau des protocoles de transports que des infrastructures physiques supportant ces réseaux.

Un des principaux enjeux de la supervision de réseaux est ainsi de réussir à offrir une solution unique permettant de gérer son réseau dans un milieu hétérogène indépendamment des contraintes physiques et techniques ; l'ampleur de ces réseaux pouvant varier grandement : que l'on parle d'un réseau d'un opérateur et fournisseur ou bien que l'on parle du réseau interne d'une petite entreprise, la supervision doit pouvoir apporter des outils performants, adaptables aussi bien à la taille des réseaux qu'à leur grande diversité technologique.

Un autre enjeu est l'automatisation du traitement de l'information. En effet, face à l'importance (taille et criticité) des réseaux dans tous les milieux professionnels, il reste difficile de prendre connaissance de toutes les informations et de réagir proactivement. Dès lors, l'automatisation de l'analyse des informations remontées par la supervision permet la mise en place de statistiques et de procédures pour la résolution des problèmes récursifs ou étendus.

2 La supervision / administration réseau

Avant de présenter le principal protocole ainsi que les outils actuels permettant de superviser un réseau, il paraît bon de définir précisément le concept de supervision et la manière dont il a été normalisé par l'ISO[1]. La normalisation ISO étant identique pour la supervision et l'administration, nous ne parlerons que de supervision.

2.1 Le concept de supervision réseau

La supervision réseau a pour but de surveiller le bon fonctionnement des réseaux.

Ce concept est né au début des années 1980, lors de l'explosion de la mise en place de réseaux informatiques dans les entreprises. La taille grandissante de ceux-ci ainsi que leur hétérogénéité posaient un réel problème de gestion et d'administration, multipliant les besoins en main d'oeuvre d'experts administrateurs. C'est donc à cette époque qu'ont été menées les premières réflexions sur un nouveau concept, celui de la supervision.

La supervision devait être capable de s'adapter à des milieux hétérogènes, d'automatiser le contrôle des réseaux et de générer un ensemble de statistiques donnant une meilleure vision du réseau, permettant par là-même d'anticiper les besoins de celui-ci.

La supervision peut ainsi se définir comme étant l'utilisation de ressources réseaux adaptées (matérielles ou logicielles) afin d'obtenir des informations sur l'utilisation et sur l'état des réseaux et de leurs composants (logiciels, matériels). Ces informations peuvent alors servir d'outils pour gérer de manière optimale (automatique si possible) le traitement des pannes ainsi que la qualité des réseaux (problèmes de surcharge). Elles permettent également de prévoir toute future évolution nécessaire.

La supervision est capable de diagnostiquer et bien souvent de réparer seule les pannes. Si ce n'est pas le cas, elle se charge d'alerter immédiatement les personnes concernées par l'incident. Elle est donc extrêmement réactive et représente un gain important en temps. De plus, par sa vision continue du réseau, elle anticipe souvent sur des problèmes ultérieurs. On parle alors de proactivité.

Ainsi, la supervision est à la fois réactive et proactive. C'est pourquoi, petit à petit, la supervision s'impose dans la plupart des entreprises possèdant un parc informatique conséquent.

[1] International Organization for Standardisation.

2.2 La norme ISO

L'ISO s'intéresse de près à la supervision. Et, dès 1988, l'organisme publie la norme ISO7498/4 [2] définissant les principales fonctions que doivent implémenter les systèmes de supervision et d'administration. Ces fonctions sont les suivantes :

2.2.1 Gestion des performances (Performance Management)

La gestion des performances analyse de manière continue les performances du réseau afin de le maintenir dans un état de performance acceptable. Cette gestion s'opère en trois étapes. Tout d'abord, des variables contenant des informations significatives quant aux performances du réseau sont récupérées. Parmi celles-ci on peut citer le temps de réponse d'une station utilisateur ou encore le taux d'occupation d'un segment réseau. Une fois ces variables obtenues, elles sont analysées. Si elles dépassent un seuil de performance fixé préalablement, une alarme est tout de suite envoyée à l'administrateur du réseau, pour règler le problème au plus vite. Ces variables de gestion de performances sont réactualisées à court intervalle de temps dans le but d'être le plus réactif possible au moindre embryon de baisse de performance.

La gestion des performances permet donc une évaluation du comportement des ressources et un contrôle de l'efficacité des activités de communication.

2.2.2 Gestion des configurations (Management Configuration)

La gestion des configurations effectue un suivi des différentes configurations des éléments présents sur le réseau. Elle stocke dans une base de données les versions des systèmes d'exploitation et des logiciels installés sur chaque machine du parc réseau. Par exemple pour un ordinateur du réseau, la base contiendra la version de son OS, du protocole TCP/IP, etc ...

La gestion des configurations permet donc une identification et un contrôle des systèmes ouverts. Elle collecte et fournit des informations sur les différents systèmes du réseau.

2.2.3 Gestion de la comptabilité (Accounting Management)

La gestion de la comptabilité a pour but de mesurer l'utilisation des ressources afin de réguler les accès et d'instaurer une certaine équité entre les utilisateurs du réseau. Ainsi 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] aussi connue sous le nom de OSI management Framework.

La gestion de la comptabilité permet donc un établissement des coûts d'utilisation ainsi qu'une facturation de l'utilisation des ressources.

2.2.4 Gestion des anomalies (Fault Management)

La gestion des anomalies détecte les problèmes réseaux (logiciels ou matériels). Elle essaie d'isoler le plus précisément le problème en effectuant divers tests. Quand celà est possible, elle règle elle-même automatiquement l'anomalie. Sinon, elle alerte les personnes concernées par le type du problème afin de solliciter leur intervention. La gestion des anomalies garde dans une base de données l'ensemble des problèmes survenus ainsi que leur solution, de manière à être encore plus efficace face à un incident réccurrent. Cette fonction de la norme ISO7498/4 demeure de loin la fonction la plus implémentée à ce jour.

La gestion des anomalies détecte donc et corrige les fonctionnements anormaux des éléments du réseau.

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 accèder à certaines ressources protégées.

La gestion de la sécurité met donc en application les politiques de sécurité.

2.2.6 Structure de gestion des réseaux (Network Management System)

Après avoir défini les fonctionnalités de la supervision réseau, l'ISO s'est attaché à décrire la structure de la gestion des réseaux (Network Management System).

L'ISO propose d'installer un agent de gestion sur chaque machine supervisée, comme le montre la figure suivante :

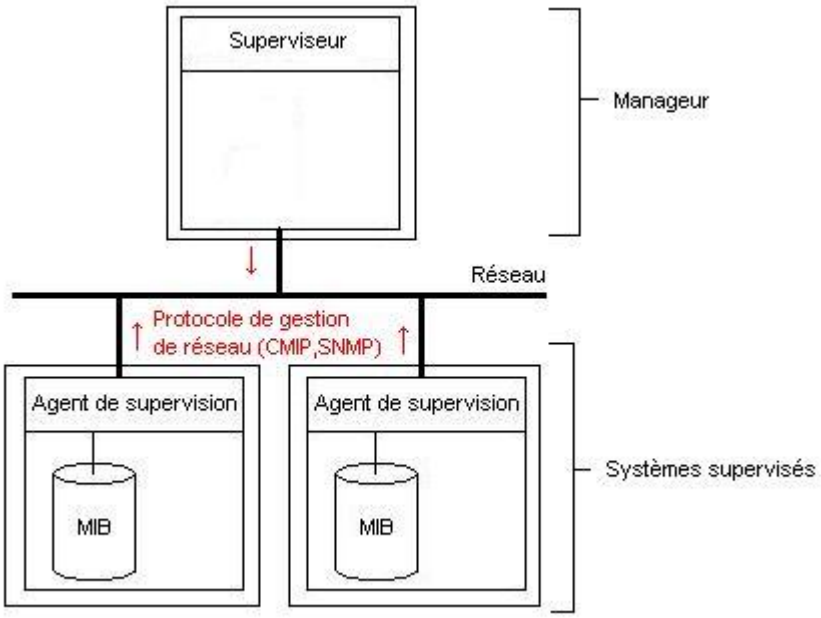

FIG. 1 – Network Management System (MNS).

Cet agent récupère périodiquement et stocke localement des informations sur la machine sur laquelle il tourne. Quand il détecte un problème, il le signale au service de gestion centralisé (installé sur le serveur de supervision). Le service de supervision, en fonction de la nature de l'anomalie, prend un ensemble de décisions (actions) dont une bonne partie est transmise à l'agent de gestion présent sur la machine en difficulté. L'agent exécute alors l'ensemble des actions réparatrices demandées par le superviseur afin de remettre la machine en état.

Toutefois, le service central de supervision ne reste pas inactif en attendant que ses agents lui rapportent des problèmes. Il peut en effet questionner régulièrement ses agents, par le biais de requêtes, pour connaître l'état complet d'une machine, et par addition, l'état de l'ensemble du réseau.

Les objets stockés dans les bases de données des agents sont normalisés au format ASN.1. Ces bases de données ont aussi été normalisées par l'ISO. Elles sont appelées bases de données MIB [3]. Nous ne détaillerons ni le format ASN.1, ni les bases de données MIB.

Pour transmettre les différents messages échangés entre l'agent de supervision et le superviseur, un protocole réseau de couche OSI 7 a été défini par l'ISO : le pro-

[3] Management Information Base.

tocole CMIP [4]. Nous ne détaillerons pas ce protocole, puisqu'aucune implémentation n'en a été faite à ce jour. En effet, les travaux de l'ISO sur la supervision restent trop complets et complexes à mettre en oeuvre. Ils ont toutefois eu le mérite de poser un cadre clair à la supervision réseau.

2.3 Le protocole SNMP

Jugeant les spécifications du protocole de transport CMIP proposé par l'ISO trop lourdes à mettre en oeuvre, l'IETF [5] a défini son propre protocole de gestion des réseaux : SGMP [6]. Celui-ci ne fut jamais réellement déployé mais donna naissance en 1988 au protocole SNMP [7].

Comme son nom l'indique, SNMP se veut être le plus simple possible. L'IETF estime en effet que le transport des données de supervision ne doit pas nuire aux performances du réseau. SNMP ne permet de superviser que les réseaux TCP/IP. Il est donc totalement adapté aux réseaux informatiques utilisant majoritairement cette technologie. D'ailleurs, SNMP s'est imposé, ces dernières années, comme étant le standard incontournable de la supervision pour l'ensemble des réseaux non téléphoniques.

Depuis 1988, SNMP a beaucoup évolué en passant de sa première version [8], complètement dépourvue de sécurité, à sa version numéro trois combinant une sécurité basée sur les usagers et sur le type des opérations. Toutefois, actuellement, SNMPv1 reste la version la plus employée, SNMPv3 n'étant en cours de déploiement que depuis 1999.

Dans un soucis de rapidité, le protocole SNMP ne transporte que des variables par le biais du protocole de transport UDP. Il sert à instaurer le dialogue entre les agents installés sur les machines supervisées et le serveur de supervision (voir structure NMS [9] 2.2.6 FIG.1). L'agent reçoit les requêtes sur le port 161 et le superviseur reçoit les alarmes sur le port 162. Le modèle d'échange entre le serveur et l'agent est basé sur deux types d'opérations, les requêtes et les alarmes :

- Lorsque le serveur veut demander quelque chose à l'agent ou lui imposer un ordre, il émet une requête en direction de l'agent. Celui-ci la traite et lui retourne une réponse.

- Lorsqu'un événement survient sur l'élément du réseau monitoré par l'agent,

[4] Common Management Information Protocol
[5] Internet Engineering Task Force.
[6] Simple Gateway Monitoring Protocol.
[7] Simple Network Management Protocol.
[8] RFC 1157.
[9] Network Management System.

ce dernier en informe immédiatement le superviseur par le biais d'une alarme de type trap ou inform. Dans le cas d'un inform, le serveur retourne une réponse à l'agent émetteur.

Ainsi, il existe trois messages SNMP différents : les requêtes, les réponses et les alarmes. Les requêtes SNMP sont les suivantes :

- GetRequest : recherche d'une variable sur un agent.
- GetNextRequest : recherche la variable suivante.
- GetBulk : recherche un ensemble de variables regroupées.
- SetRequest : change la valeur d'une variable sur un agent.

L'agent répond aux requêtes par un message GetResponse. En cas d'erreur, le message sera accompagné d'un des codes d'erreurs suivants :

- NoAccess : accès non autorisé.
- WrongLength : erreur de longueur.
- WrongValue : erreur de valeur.
- WrongType : erreur de type.
- WrongEncoding : erreur d'encodage.
- NoCreation : objet inexistant.
- ReadOnly : seule la lecture est autorisée.
- NoWritable : interdiction d'écrire.
- AuthorisationError : erreur d'authorisation.

Les alarmes sont envoyées par l'agent lorsqu'un évenment survient sur la ressource monitorée. Elles peuvent prendre les formes suivantes :

- ColdStart (0) : redémarrage du système à froid.
- WarmStart (1) : redémarrage du système à chaud.
- LinkDown (2) : le lien n'est plus opérationnel.
- LinkUp (3) : le lien est à nouveau opérationnel.
- AuthentificationFailure (4) : Tentative d'accès à l'agent avec un mauvais nom de communauté.
- EgpNeighborLoss (5) : la passerelle adjacente ne répond plus.
- EntrepriseSpecific (6) : alarme spécifique aux entreprises.

Le paquet SNMP, tel qu'il est définit dans la RFC 1157 (SNMPv1), est encodé au format ASN.1. Il possède les champs suivants :

Version SNMP - Communauté - PDU [10]

La communauté définit le domaine de gestion. Agents et superviseurs doivent être dans la même communauté pour pouvoir échanger. Le PDU contient les données du protocole de supervision. Il est construit de manière identique pour les requêtes

[10] Packet Data Unit.

et les réponses. Il diffère légèrement pour les alarmes (voir annexe 1).

Comme nous l'avons vu, le protocole SNMP permet l'échange de données de gestion entre un agent et un superviseur dans un réseau TCP/IP. Toutefois, il est aussi possible de monitorer des équipements n'utilisant pas TCP/IP ou n'ayant pas d'agent SNMP. Pour celà, un proxy SNMP doit être installé sur une machine TCP/IP. Ce proxy se charge de faire la translation entre les données d'un agent de supervision privée et SNMP. Il est ensuite capable de transmettre ces données à un superviseur SNMP. L'utilisation de ces proxies permet ainsi à SNMP de s'adapter facilement à des réseaux très hétérogènes et prouve la grande flexibilité de ce protocole.

En plus des proxies SNMP, l'IETF a aussi défini des sondes capables de collecter des informations de gestion sur un segment de réseau. Ces sondes font tampon entre les agents d'un segment et un superviseur en centralisant les données relatives à un segment réseau dans une base de données MIB. Les superviseurs ne dialoguent alors plus qu'avec les sondes. Celles-ci ajoutent donc un niveau hiérarchique à la supervision. Chaque sonde dite RMON [11] peut écouter des segments réseaux de type Ethernet, TokenRing, ATM ou encore FDDI.

2.4 Les logiciels de supervision

Les logiciels de supervision sont des solutions applicatives répondant au concept de supervision tel qu'il a été défini précédement. Ils s'appuient, pour la plupart, sur le protocole SNMP.

Ces outils ont principalement pour objectif de connaître à tout instant l'état des noeuds critiques (serveurs, switchs, routeurs) et l'état des services tournant sur les différents serveurs. Ils doivent également être capable d'analyser le trafic réseau afin de permettre une meilleure répartition des ressources réseaux. Pour celà, ils peuvent être déployés de différentes manières.

2.4.1 Déploiement des logiciels de supervision :

Ces outils peuvent être déployés de trois manières différentes : centralisée, hiérarchique ou distribuée.

Déploiement centralisé La supervision n'est assurée que par un seul ordinateur, avec éventuellement une ou plusieurs machines mirroir synchronisées. La visualisation des éléments du réseau (alarmes, état des noeuds, etc...) est alors centralisée en un point unique.

[11] Remote Monitoring.

Ce type de supervision reste tout de même sensible, car toute la gestion repose sur une seule station. Si celle-ci vient à tomber en panne, tout le processus de supervision est alors compromis. De plus la machine étant seule, elle doit être suffisament robuste pour pouvoir traiter l'ensemble des données de supervision du réseau. Enfin, la machine effectue la totalité des requêtes de supervision, ce qui a pour conséquence d'augmenter fortement le trafic réseau en provenance de cette machine.

Déploiement hiérarchique La supervision est assurée ici de manière hiérarchique. Un serveur de supervision central dialogue avec d'autres serveurs de supervision ne s'occupant chacun que d'un segment de réseau. Ces mêmes serveurs peuvent aussi avoir d'autres serveurs sous leur responsabilité. Ils sont à la fois clients et serveurs de supervision.

Ce type de déploiement est bien plus délicat à mettre en oeuvre qu'un simple déploiement centralisé mais offre une tolérance aux pannes bien plus élévée. En effet, si un serveur supervisant un segment tombe en panne, seul le segment concerné ne sera plus supervisé. De plus un tel déploiement permet d'avoir plusieurs visions du réseau : une vision globale, depuis le serveur central, une vision d'un segment depuis un serveur supervisant un segment, etc...

Toutefois, il ne faut pas occulter le fait qu'un déploiement hiérarchique reste plus coûteux en temps de réponse qu'un déploiement centralisé, les différents serveurs devant se synchroniser pour faire remonter les informations au niveau hiérarchique le plus haut.

Déploiement distribué Ce déploiement combine l'approche centralisée et l'approche hiérarchique. Chaque station de supervision tient à jour une base de données complète. Toutes les stations échangent donc entre elles les données de supervision, sans restriction. Celà permet même de spécialiser certaines machines sur un traitement de supervision précis (alarme, sécurité, performances, etc...). Toutefois, il convient de bien définir le degré de responsabilité et de coopération entre les machines.

2.4.2 Quelques outils de la supervision

Les plateformes complètes de supervision reposent toutes sur le protocole SNMP. En voici une liste non exhaustive :

- **HP Open View :** solution de supervision modulaire très complète développée par HP. Elle permet globalement de cartographier automatiquement et dynamiquement le réseau, de collecter les informations de supervision, de les mettre en correspondance, d'envoyer des alarmes, de maintenir une base de données simplifiée pour analyser l'historique des événements et enfin de

générer automatiquement des comptes rendus graphiques.

- **Big Brother :** superviseur simple de services fonctionnant sous Windows NT. Il est efficace mais ne permet de ne superviser qu'un nombre restreint de services (http, pop, nntp, smtp et quelques autres). De plus on ne peut lui ajouter de nouvelles fonctionnalités et il est incapable de remonter les alarmes autrement que graphiquement (pas d'envoie de mail ou de sms).

- **CiscoWorks 2000 :** outil de supervision propriétaire à Cisco, parfaitement adapté pour monitorer et configurer le matériel cisco. Attention ce superviseur matériel utilise les propriétés spécifiques du matériel de la marque cisco (CDP [12], etc...). Il n'est donc pas du tout adapté pour un autre type de matériel. En outre, il permet de configurer facilement et graphiquement le matériel CISCO sans connaissance des commandes de leurs IOS (permet même de configurer les VLAN et le Spanning Tree). Il s'installe sous Windows NT.

- **MRTG [13] :** outil de visualisation basé sur SNMP et permettant la réalisation d'un historique graphique des variables représentatives des performances du réseau et de ses éléments. MRTG est inclus dans Nagios.

- **Nagios :** voir 3

Parmi les logiciels les plus employés, nous retiendrons la plateforme HP OpenView et Nagios (anciennement NetSaint).

Maintenant que le concept de supervision est connu, nous allons vous présenter un outil de supervision libre et très utilisé : Nagios.

[12] Cisco Discovery Protocol.
[13] Multi Router Trafic Grapher.

3 Supervision : l'exemple de Nagios

Un des besoins les plus exprimés en matière de gestion de réseau est la surveillance des services. C'est donc dans une démarche de qualité de service, et de manière à pouvoir réagir dans les plus brefs délais, que de nombreuses solutions de supervision de services ont vu le jour, dont Nagios.

3.1 Présentation générale

3.1.1 Le concept

Nagios est un système de supervision de services, la version stable actuelle est la 1.2[14]. Il a été développé pour fonctionner sur une plateforme Linux ou éventuellement Unix avec un concept assez simple : les services de surveillance lancent par intermittence des contrôles de services et de stations que l'on définit, grâce à des greffons[15] externes.

3.1.2 Le fonctionnement

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

3.1.3 mode de licence

Nagios est distribué sous les termes de la *GNU General Public Licence* Version 2 comme publiée par la Free Software Foundation (FSF[16]). Cette licence donne la permission légale de copier, distribuer et/ou modifier Nagios sous certaines conditions.

3.1.4 Périmètre de l'outils

Nagios possède de nombreuses fonctionnalités, voici les principales :
- Surveillance des services réseaux(SMTP, POP3, http, NNTP, PING, etc)
- Surveillance des ressources des stations (serveur, routeur ...) comme la charge du processeur, des informations sur l'utilisation des disques durs, les processus en cours, les fichiers de log, ...
- Surveillance des données environnementales comme par exemple la température.

[14] Téléchargeable sur `http ://www.nagios.org/download`
[15] le terme "Greffon" est la traduction officielle du mot anglais "plugin"
[16] Fondation créée par Richard M. Stallman au début des années 80 visant à développer les logiciels libres. `http ://www.gnu.org/`

- Une conception simple de greffons permettant aux administrateurs de développer facilement leurs propres fonctionnalités de surveillance.
- Possibilité de définir des groupes de contacts à joindre en cas d'apparition de problème via différentes méthodes (le courrier électronique, les messages instantanés).
- Sectorisation des groupes de contacts par rapport aux problèmes rencontrés et définition de proçédures
- Définition de gestionnaires d'événements qui peuvent être exécutés afin d'automatiser la résolution de problèmes rencontrés.
- Surveillance des architectures des systèmes répartis ou redondants.
- L'interface de commandes externes permet des modifications à la volée du comportement de la surveillance et du retour d'informations à travers l'utilisation de gestionnaires d'événements, d'une interface web et d'applications tierces.
- L'historique de l'état du réseau est conservé même après un redémarrage
- Possibilité de plannifier des périodes d'inactivités des contrôles pour correspondre à une période d'inactivité physique d'un serveur.
- Retour d'informations disponible à travers n'importe quel navigateur, permettant de consulter l'état courant du réseau, l'historique des avertissements et les fichiers de log.
- Un schéma simple de gestion des autorisations permet de gérer facilement les droits de consultation des informations par les utilisateurs à travers un navigateur.

Nagios possède également une fonctionnalité importante : *l'héritage*. Cela permet de hierarchiser l'ensemble des hôtes supervisés. Concrêtement, si un hôte faisant la jonction entre la machine Nagios et le reste d'une branche ne fonctionne plus, Nagios ne générera pas d'alertes concernant les éléments de cette branches.

3.1.5 Architecture

Voici les éléments de l'architecture de Nagios :

- Un ordonnanceur : Nagios est d'abord un moteur gérant l'ordonnacement des vérifications, ainsi que les actions à prendre sur incidents (alertes, escalades, prise d'action corrective) ;
- Une IHM[17] : La partie visible à travers un simple serveur web, tel Apache, est basée sur des CGI[18] ;
- Des sondes : Les sondes de Nagios sont des petits scripts ou programmes qui sont la base des vérifications.

[17] IHM : Interface Homme-Machine
[18] CGI : Common Gateway Interface

3.2 Les greffons

3.2.1 Principe de base

Nagios est un moteur d'ordonnancement de vérifications diverses assurées par des greffons. La relation entre le moteur principal et les greffons se fait d'une part dans la configuration de Nagios, pour que Nagios sache quelles vérifications lancer sur, ou à destination, de quelles machines ou services ; d'autre part par le code retour ainsi que la sortie standart d'un greffon.Ces greffons fonctionnent soit en local sur la machine Nagios, soit effectuent des tests à distance.

Voici comment on peut schématiser le fonctionnement de base :

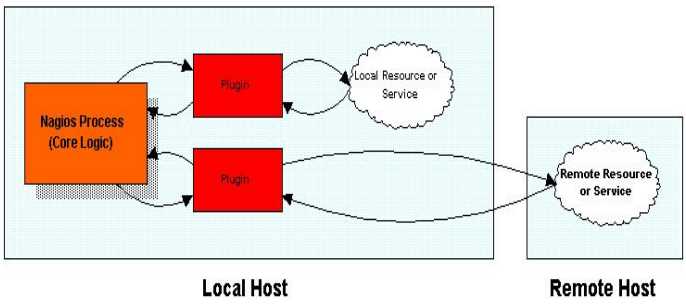

FIG. 2 – Illustration du principe de fonctionnement des greffons

Il est donc possible d'effectuer des tests de toutes sortes (fonctionnement de services, espace disque, charge, ...) sur la machine Nagios, ainsi que des tests simples (par exemple ping) sur une machine distante.

3.2.2 Fonctionnalités avancées

Afin de pouvoir effectuer des vérifications plus poussées sur une machine distante sans pour autant modifier la configuration de sécurité mise en place, les créateurs de nagios ont développé différent agents de transport et d'exécution de test. Cette possibilité reprend une fonction définie par la norme ISO 7498/4 : la Structure de gestion de réseaux (MNS).
Voici deux des principaux agents proposés par Nagios :

- **NRPE** *(Nagios Remote Plugin Executor)* : il constitue une méthode de surveillance dite active. En effet, l'initiateur et l'ordonnanceur des tests est la machine nagios : le plugin *check_nrpe* permet à la machine Nagios d'envoyer des instructions aux démon NRPE situé sur la machine distante.
- **NSCA** *(Nagios Service Check Acceptor)* : il s'agit là d'une méthode passive : le client NSCA est installé, configuré et lancé sur chaque hôte distant de sorte à envoyer des résultats de tests à la machine Nagios.

3.2.3 Ecriture de greffons

Le projet Nagios fournit en standart bon nombre de greffons de base, mais la simplicité de leur mode de fonctionnement permet à l'administrateur d'en écrire pour ses propres besoins.

3.3 Configuration des composants

3.3.1 Apache

Il est nécessaire d'intégrer dans le serveur web apache un certain nombre de directives. Ces directives vont permettre de régler différentes options (chemin d'accès, autentification, etc.). Il est donc possible pour réaliser ses opérations d'intervenir directement sur le fichier de configuration du serveur Apache, soit en intégrant un fichier de configuration propre à Nagios.

3.3.2 Authentification

L'accès à Nagios doit être restreint, car il peut montrer des informations importantes voir confidentielles. De plus, des actions peuvent être prises via l'interface Web comme par exemple l'acquiescement d'une alarme au redémarrage d'un serveur. La définition des règles d'authentification ayant été réalisé durant la configuration de apache, il suffit de renseigner le fichier */etc/nagios/htpasswd*. Cela se fait par le biais de l'utilitaire *htpasswd* fourni avec apache :

```
#htpasswd [-c] /etc/httpd/htpasswd nagios
New password: ******
Re-type new password: ******
Updating password for user nagios
```

L'utilisateur *nagios* utilisé correspond à un contact défini dans */etc/nagios/contacts.cfg* et non à l'utilisateur POSIX.

3.3.3 Nagios

Les fichiers de configuration de Nagios se trouve dans le répertoire */etc/nagios/*. Ces fichiers de configuration, à l'exception des fichiers *nagios.cfg* et *cgi.cfg*, utilisent une structure unique de définition des objets sur le principe suivant :

```
define {
param1 value
param2 value
...
paramn value
}
```

Le fichier de configuration principal :
Le fichier de configuration principal (par défaut, /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. Un fichier de configuration principal est généré automatiquement à titre d'exemple quand vous lancez le script *"configure"* avant de compiler les programmes.

Fichier de configuration des ressources :
Les fichiers des ressources sont utilisés pour stocker les macros définies par les utilisateurs. Ces fichiers peuvent aussi contenir d'autres informations (telles que la configuration des connexions de la base de données), bien que celles-ci dépendent de la manière dont est compilé Nagios. L'avantage de ces fichiers est de pouvoir y mettre des données sensibles de configuration qui ne seront pas accessibles à travers les CGIs.

Fichier de configuration des objets :
Le fichier de configuration des objets (historiquement appellé "host" dans les fichiers de configuration) définit les hôtes, services, groupes d'hôtes, contacts, groupes de contacts, commandes, etc ... C'est là que sont défini les éléments à surveiller.

Fichier de configuration des CGIs :
Le fichier de configuration des CGIs (par défaut, /usr/local/nagios/etc/cgi.cfg) contient un certain nombre de directives qui affectent le mode de fonctionnement des CGIs.

Fichier de configuration des informations étendues :
Le fichier de configuration des informations étendues est utilisé pour définir des informations supplémentaires pour les hôtes et les services qui doivent être utilisés par les CGIs.

Il est possible de tester la cohérence des fichiers de configuration à l'aide de la commande suivante :

```
#/usr/bin/nagios -v ../etc/nagios.cfg
```

3.4 Utilisation

3.4.1 L'interface d'administration

Nagios a basé l'entière intéraction entre les administrateurs et le programme via une interface web. Ceci pour répondre aux besoins d'accessibilité des administrateurs (claires, regroupées, graphiques, accessibles de n'importe quel endroit, etc.) mais aussi pour s'appuyer sur des technologies Unix éprouvées comme le serveur Web *apache* qui va prendre en charge une partie de la gestion des accès à l'interface.

L'interaction utilisateur via son navigateur et les processus Nagios sur la station de supervision vont se faire grâce à des CGIs (Common Gateway Interface) et permettre entre autre la présentation des informations de manière graphique. Cette interface va permettre également à l'administrateur d'utiliser des commandes appelées commandes externes (dont la sécurité est basée sur la gestion des droit Unix) afin d'intervenir à distance, améliorant ainsi la réactivité.

3.4.2 Des alarmes aux administrateurs

La traduction claire et graphique de l"état des noeuds en quasi temps-réel est une mesure indispensable de la supervision de réseau. Néanmoins elle n'est pas suffisante et l'une des fonctionnalités les plus intéressantes de Nagios est son interfaçage avec un serveur SMTP[19] ou de SMS[20]. Ainsi il est possible de prévenir instantanément les administrateurs au lieu d'attendre que ceux-ci effectuent des vérifications. Ils sont tenus au courant automatiquement de l'état des services et cela engendre une réactivité plus grande.

Une deuxième étape permise par Nagios est la classification des remontées d'informations aux différents administrateurs classés par secteur de compétences. Ainsi un expert du service défaillant sera alerté, ciblant les compétences nécessaires et réduisant proportionnellement les délais de remise en fonction. Ajouté à cette fonction, Nagios permet l'automatisation de l'escalade des actions et alertes enclenchées en réponse à une situation donnée, permettant une plus grande liaison et une meilleure synchronisation des réponses et procédures amenées à être mise en place dans la supervision des services d'un réseau.

3.4.3 Les statistiques et l'anticipation

Nagios offre un service efficace de mémorisation et de traduction graphique des événements advenus sur l'ensemble des services et stations du réseau. Cette fonction est indispensable pour mener une analyse approfondie des causes ayant menées aux différentes pannes survenues. Il semble évident que pour améliorer la proactivité et non la réactivité, une connaissance pointue des coûts et besoins de son réseau, proportionnelle aux ressources mise en place doit être maintenue et anticipée. Cela passe forcément par la mise en place d'outils générant des statistiques représentatives et adaptées à l'architecture de son réseau et de ses services.

[19] Simple Mail Transer Protocol
[20] Short Message Service

4 Conclusion

4.1 Bilan

Les réseaux sont devenus un pilier de l'économie mondiale. Les besoins et les enjeux de ces technologies ne cessant d'augmenter, la supervision est alors apparue pour apporter une garantie de fiabilité, de réactivité et d'adéquation des moyens mis en place. Néanmoins la grande disparité de ces technologies de réseau pose un certain nombre de problèmes : comment superviser toutes ces technologies, comment récupérer les informations, etc.

Les organismes de normalisations ont été les premiers à apporter une réponse en définissant un format commun des données, un modèle d'administration pour les adresser et des protocoles pour les communiquer. La mise en place d'une procédure de supervision de réseaux passe alors forcément par l'application concrète d'une de ces normes, sans laquelle il est impossible d'obtenir une réelle plus valu sur l'administration de son réseau. Le seul véritable standard actuel du monde IP élaboré à partir de ces normes est le protocole SNMP. Il constitue la base de la majorité des plateformes logicielles de supervision réseau dont Nagios, une des plus populaires.

Nagios réussit, grâce à son exploitation intelligente des capacités des technologies Unix, à proposer une plate-forme de supervision d'une grande variété de services, complète et facilement modulable.

Elle répond aux besoins de supervision de nombreux services basés sur des protocoles différents et a su présenter des fonctionnalités adaptées aux attentes concrètes de la supervision comme l'accessibilité et ses interactions à distance, l'automatisation des remontées d'alarmes jusqu'aux administrateurs, ou encore les comptes-rendus et historiques graphiques des événements du réseau.

4.2 Quel avenir ?

Nagios 2.0 est virutellement prêt mais la documentation n'étant pas à jour, sa sortie en est différé. Cette version intégrera notamment des améliorations dans la configuration. Parallèlement, un projet nommé OREON est en cours de développement. Ce projet a pour but de construire une solution complète basée sur Nagios.

Les organismes de normalisation de la supervision et les différents acteurs du réseau sont étroitement liés, ce qui permet le développement de normes qui répondent aux plus justes aux besoins des réseaux d'aujourd'hui et permettent d'anticiper les besoins futurs. Les outils commerciaux de supervision bénéficient alors directement des avancées des recherches menées au sein des consortiums par les constructeurs. La supervision avance ainsi à grand pas et sera certainement un pillier des réseaux de demain.

5 Ressources

5.1 Bibliographie

5.1.1 Ouvrages

Références

[1] ”Les réseaux”, Guy Pujolle, *édition Eyrolles, 3eme édition 2002*

[2] ”Théorie et pratique : Supervision avec Nagios”, *GNU Linux Magasine* No 65.

[3] ”Pratique de la gestion de réseau”, Nazim AGOULMINE, Omar CHERKAOUI, *Edition Eyrolles 2003*

[4] ”Nagios, un outil GPL de surveillance pour petits et grands réseaux hétérogènes”, Pierre-Antoine Angelini, *JRES 2003*

5.1.2 Références de sites internet

Sites web indépendants

`http ://www.snmplink.org` :
Un site contenant des informations sur SNMP et les MIB.

`http ://wwwsnmp.cs.utwente.nl/` :
Un site très complet sur les normes de supervision de réseaux.

`http ://www.et.put.poznan.pl/snmp/main/mainmenu.html` :
Un site qui introduit très simplement les différentes versions des normes SNMP.

Sites Web commerciaux et institutionnels

`http ://www.nagios.org` : le site officiel de Nagios
`http ://www.dmtf.org` : le site officiel du DMTF.
`http ://www.iso.org` : le site officiel de l’ISO.
`http ://www.ietf.org` : le site officiel de l’IETF.
`http ://www.snmp.org` : le site officiel du centre de recherche international sur SNMP.

5.2 Glossaire

A :

ASN.1 *(Abstract Syntaxe Notation number One)*
Notation formelle qui permet de spécifier très facilement et sans sacrifier à la généralité les informations manipulées par les protocoles de télécommunications, indépendamment des systèmes informatiques, des logiciels et des modes de transfert des données.

C :

CIM *(Common Information Model)*
Norme développée par le DMTF permettant de décrire des données, des applications ou des entités de telle manière que les administrateurs et les programmes de gestion puissent contrôler les différentes applications et dispositifs des différentes plates-formes de la même manière, assurant ainsi l'interopérabilité à travers le réseau.

CGI *(Common Gateway Interface)*
Interface standard installée sur les serveurs HTTP permettant entre autres l'envoi de variables d'entrée et d'environnement à tout programme serveur dont on demande l'exécution (utile par exemple pour la saisie de formulaires via le Web).

CMIP *(Common Management Information Protocol)*
Norme de supervision de réseaux définie par l'ISO qui permet de fournir les services liés au standard CMIS.

CMIS *(Common Management Information Services)*
Norme de supervision de réseaux définie par l'ISO qui présente les services utilisables par les entités de gestion. CMIS définie un ensemble de primitives et la structures des messages échangeables par CMIP.

D :

DMTF *(Distributed Management Task Force)*
Consortium industriel très actif dans la recherche et le développement de normes de supervision ainsi qu'à leur mise en place.

I :

ICMP *(Internet Control Message Protocol)*
Extension du protocole Internet qui permet la génération de messages d'erreurs, de tests et d'informations relatifs aux conditions de transmission sur le réseau.

IETF *(Internet Engineering Task Force)*
Groupe de travail qui développe les nouveaux standards pour l'Internet.

IOS *(Internetworking Operating System)*
Permet aux routeurs et commutateurs de fonctionner avec (IP, IPX) en réseau local, (X.25, RNIS, PPP, Frame Relay) en réseau étendu avec les protocoles de routage : RIP, IGRP.

ISO *(International Organisation for Standardization)*
Organisation internationale de standardisation regroupant les organismes similaires de 89 nations. L'ISO se charge des standards qui régissent l'Internet actuellement.

IT *(Information Technology)*
Se dit de l'ensemble des technologies (matérielles et logicielles) qui permettent la collecte, le stockage et l'exploitation des informations à des fins d'usage spécifique. Ces technologies sont en train de révolutionner les structures sociales, culturelles et économiques en générant de nouveaux comportements vis-à-vis de l'information et de l'intelligence, de la connaissance et de leur représentation, des métiers et de l'activité professionnelle.

M :

MIB *(Management Information Base)*
Base de données d'objets pouvant être consultée grâce à un système de supervision de réseau.

MRTG *(Multi Router Traffic Grapher)*
Logiciel Unix gratuit basé sur SNMP permettant la traduction graphique de données pertinentes récupérées sur des entités du réseau.

N :

NMS *(Network Management System)*
Système de gestion de réseau.

O :

OSI *(Open Systems Interconnection)*
Architecture à 7 couches qui normalise les niveaux de service et les types d'interactions entre les ordinateurs qui échangent des informations à travers un réseau. Elle décrit le flux des données entre la connexion physique et le réseau d'une part et le programme de l'utilisateur final d'autre part.

R :

RFC *(Request For Comment)*
Une série de documents techniques émanant de la communauté de recherche et du développement de l'Internet.

S :

SMS *(Short Message Service)*
Messages courts qui peuvent être envoyés et reçus sur des téléphones mobiles GSM.

SMTP *(Simple Mail Transfer Protocol)*
Protocole de gestion des courriers électroniques sur Internet.

SNA *(System Network Architecture)*
Architecture de réseau en couche introduit par IBM et qui servit, plus tard, de base au modèle OSI.

SNMP *(Simple Network Management Protocol)*
Protocole de supervision de réseaux conçu par l'IETF pour le monde IP. Il existe actuellement 3 versions.

6 ANNEXES

6.1 SNMP : Détail du Packet Data Unit

Il existe deux structures de PDU dans SNMP. La première est commune aux requêtes et aux réponses. Elle est constituée des champs suivants :

FIG. 3 – PDU SNMP (requêtes et réponses).

L'autre PDU est propre aux alarmes (trap). Il est construit de la manière suivante :

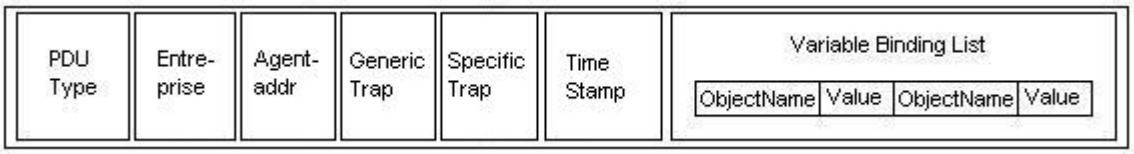

FIG. 4 – PDU SNMP (alarmes).

6.1.1 PDU Type

Il identifie le message transporté par le PDU. Ses valeurs possibles sont les suivantes :

- 0 : GetRequest
- 1 : GetNextRequest
- 2 : SetRequest
- 3 : GetResponse
- 4 : Trap

6.1.2 Request ID

Il permet de faire correspondre une requête avec une réponse.

6.1.3 Error Status

Il est utilisé par les réponses et les requêtes pour indiquer une erreur du type suivant :

- 0 : NoError
- 1 : tooBig
- 2 : noSuchName
- 3 : badValue
- 4 : readOnly
- 5 : genError

6.1.4 Error Index

Il indique, dans le cas d'une erreur, quelle variable a causé l'erreur.

6.1.5 Variable Binding List

Ce champ liste les variables. Pour chaque variable, il est constitué de l'identificateur unique de la variable dans la base MIB (ObjectName), associé à la valeur de la variable (Value).

6.1.6 Entreprise

Il est l'identifiant de l'agent ayant généré l'alarme.

6.1.7 Agent-addr

C'est l'adresse IP de l'agent ayant généré l'alarme.

6.1.8 Generic-Trap

Ce champ prend une des septs valeurs possibles de l'alarme :
- 0 : ColdStart : redémarrage du système à froid.
- 1 : WarmStart : redémarrage du système à chaud.
- 2 : LinkDown : le lien n'est plus opérationnel.
- 3 : LinkUp : le lien est à nouveau opérationnel.
- 4 : AuthentificationFailure : Tentative d'accès à l'agent avec un mauvais nom de communauté.
- 5 : EgpNeighborLoss : la passerelle adjacente ne répond plus.
- 6 : EntrepriseSpecific : alarme spécifique aux entreprises.

6.1.9 Specific-Trap

Ce champ est un code déterminant la nature de l'alarme. Il est spécifique à chaque agent propriétaire.

6.1.10 Time-Stamp

Ce champ donne le temps écoulé, en millisecondes, entre l'envoi de l'alarme et l'initialisation de l'agent.

6.2 Quelques outils et leur interface

6.2.1 Nagios

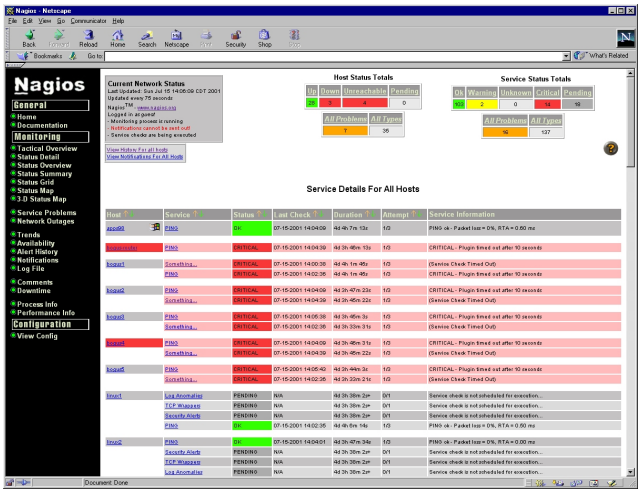

FIG. 5 – Nagios - Liste des états des services supervisés.

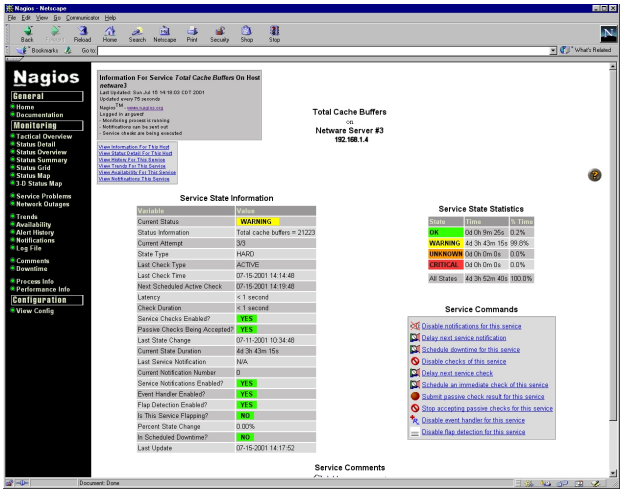

FIG. 6 – Nagios - Information détaillée sur l'état d'un service.

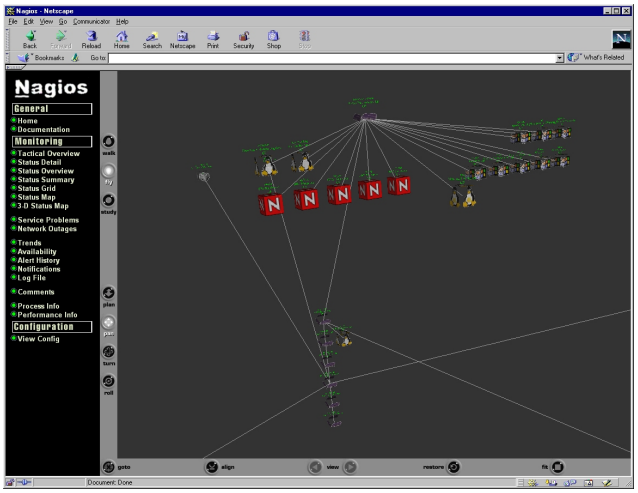

FIG. 7 – Nagios - Représentation graphique des machines supervisées.

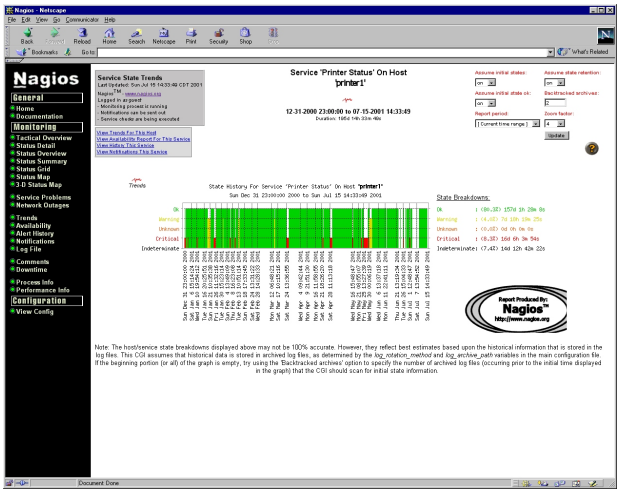

FIG. 8 – Nagios - Etat d'un service sur une machine pour une période donnée.

6.2.2 HP Open View

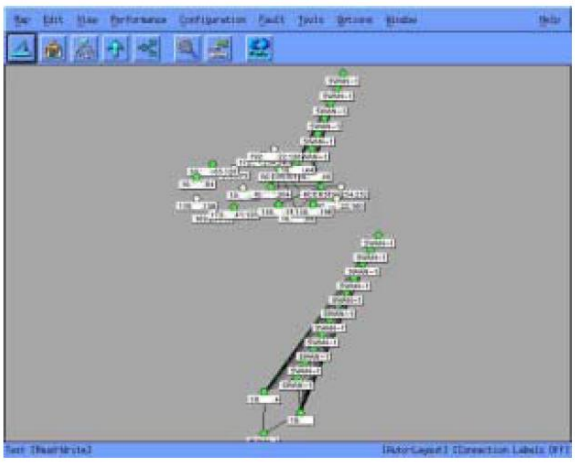

FIG. 9 – HP Open View - Vue d'ensemble après la première découverte.

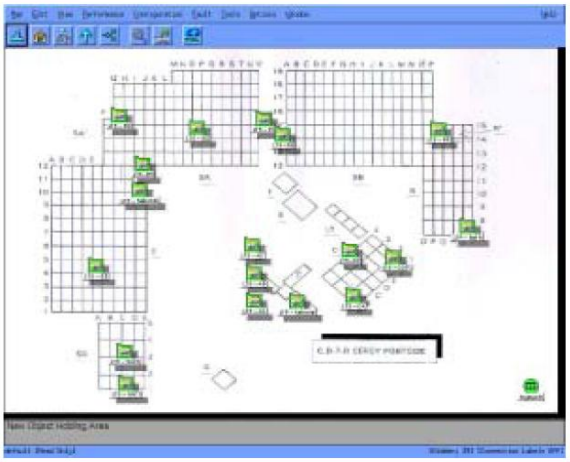

FIG. 10 – HP Open View - Vue par sectorisation géographique.

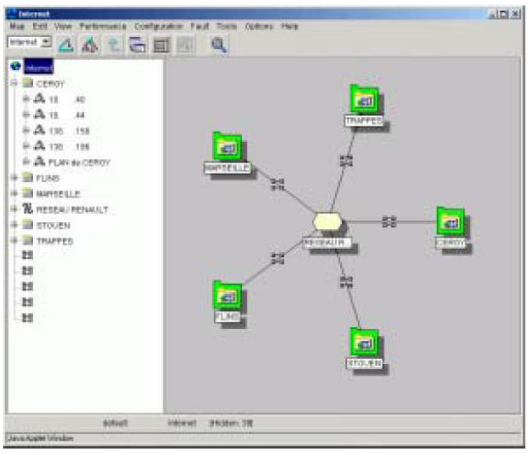

FIG. 11 – HP Open View - Vue par le web.

6.2.3 Big Brother

FIG. 12 – Big Brother - Tableau des états des services par serveur.

FIG. 13 – Big Brother - Page dynamique de remonté d'erreurs.

6.2.4 CiscoWorks

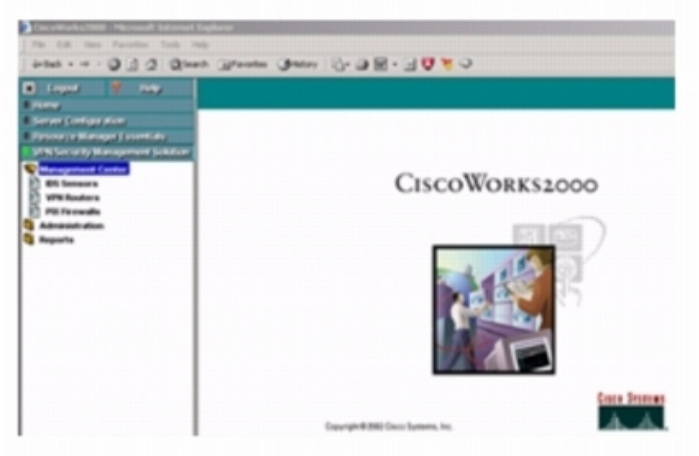

FIG. 14 – CiscoWorks - Page d'accueil.

6.2.5 MRTG

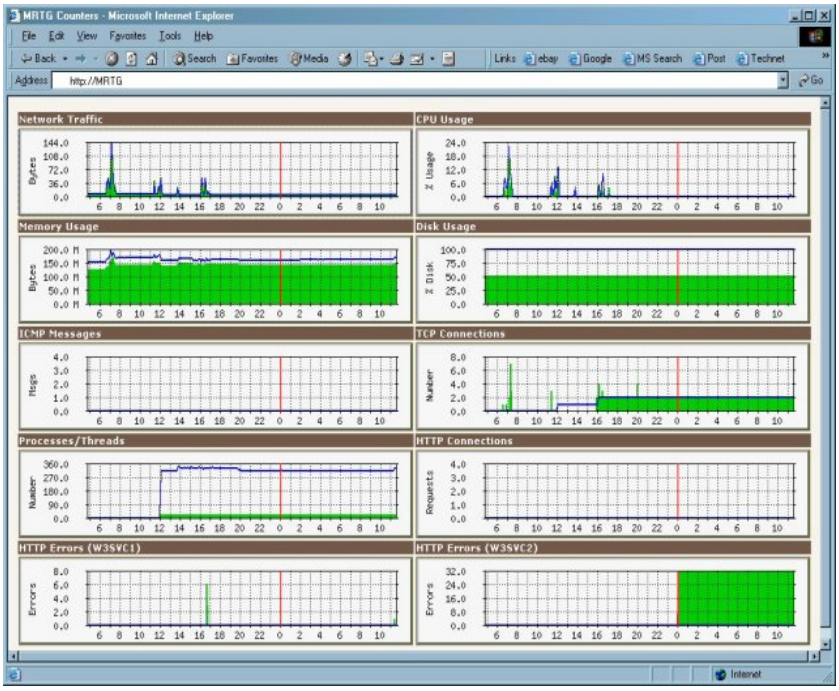

FIG. 15 – MRTG.

Table des figures