République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et De la Recherche Scientifique

Université Abderrahmane MIRA De Béjaia

Faculté Des Sciences Exactes

Département D'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Etude et mise en place d'un outil de monitoring et supervision des réseaux informatique: Cas d'étude SONELGAZ

Réalisé par :

M elle GHILI Amel

M elle MEZEMATE Yasmina

Promoteur : M r OUZEGGANE Redoine

Membre du jury :

Président : M r SLIMANI Hachem

Examinatrice : M elle CHERFA Hamida

Promotion : 2015-2016

Remerciements

On remercie dieux tout puissant de nous avoir donné la force, la santé, le courage et la patience de pouvoir accomplir ce travail qui est pour nous le point de départ d'une merveilleuse aventure.

Nous tenons particulièrement à remercier notre promoteur M^r^ Ouzeggane Redoine de nous avoir encadrées. Nous avons eu l'honneur et le privilège de travailler sous son assistance et de profiter de ses qualités humaines, professionnelles et de sa grande expérience. Il nous guider tout au long de ce travail et nous apporter les réponses nécessaires au bon déroulement de notre travail.

De plus Nous tenons également à remercie les membre du jury M^r^ slimani hachem et M^elle^ charfa hamida ainsi que les responsables de sonelgaz de nous avoir acceptés en tant que stagiaires et de nous avoir permis de vivre cette expérience enrichissante et pleine d'intérêt sur le plan professionnel et personnel en particulièrement notre encadreur M^r^idri bachir de nous avoir fait découvrir le fonctionnement d'un service informatique en entreprise et qui a su nous conseiller.

Dédicaces

Je dédiée mon travail :

A mes chers parents qui m'ont beaucoup aidés et qui se sont sacrifiés pour mon bien et qui m'ont encouragé et soutenu au long de ma vie et durant mon cursus que dieu vous préserve et vous procure la santé et la longue vie afin que à mon tour vous combler.

A mes sœurs et frères en leurs souhaitant un avenir plein de bonheur et de succès.

A ma famille sans exception qui me souhaite un avenir prospère sans oublier mes chers amis.

Enfin à toutes les personnes qui m'ont apporté de l'aide.

GHILI Amel

Dédicaces

Je dédiée mon travail :

A mes chers parents qui m'ont beaucoup aidés et qui se sont sacrifiés pour mon bien et qui m'ont encouragé et soutenu au long de ma vie et durant mon cursus que dieu vous préserve et vous procure la santé et la longue vie afin que à mon tour vous combler.

A mes sœurs et frères en leurs souhaitant un avenir plein de bonheur et de succès.

A ma famille sans exception qui me souhaite un avenir prospère sans oublier mes chers amis.

Enfin à toutes les personnes qui m'ont apporté de l'aide.

MEZEMATE Yasmina

Tables des matières

Chapitre 02 : Etat de l'art sur les systèmes de supervision

Chapitre 03 : Présentation et mise en place de l'outil Nagios

Liste des tableaux

Listes des figures

Liste des sigles

ACL	Access Control List
AIX	Aix-en-Provence
BMC	*Bicycle Manufacturing Company*
CGI	Common Gateway Interface
CIM	Common Information Modem
CMDB	Configuration Management DataBase
DMTF	Distributed Management Task Force
GPL	gaz de pétrole liquéfié
HP	hypertext
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IHM	Interactions homme-machine
IPMI	Intelligent Plateforme Management Interface
ITIL	Information technology infrastructure library
JMX	Java Management Interface
LDAP	Lightweight Directory Access Protocol
MIB	Management information base
MMS	Multimedia Messaging Service
MRTG	Multi Router Traffic Grapher
NNTP	Network News Transfer Protocol
PNG	Portable Network Graphics
POP3	Post Office Protocol
RRDTOOL	*Round-Robin database tool*
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
Tcp/ip	*General Public License*
XDR	External Data Representation
XML	L'*Extensible Markup Language*
WMI	Windows Management Instrumentation

Introduction générale

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

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

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

Ainsi, la supervision des réseaux s'avère nécessaire et indispensable. Elle permet entre autre d'avoir une vue globale du fonctionnement et des problèmes pouvant survenir sur un réseau mais aussi d'avoir des indicateurs sur la performance de son architecture.

Dans ce cadre, le présent rapport se base sur trois axes principaux :

- Présenter les notions de base de la supervision informatique et de ses logiciels les plus utilisés actuellement.
- Etudier la solution choisie parmi plusieurs en énumérant ses fonctionnalités et apports.
- la réalisation, et la mise en place de cette solution.

Chapitre 1 Présentation du cadre de stage

Chapitre 2 Etat de l'art sur les systèmes de supervision

Chapitre 3 Présentation et mise en place de l'outil Nagios

1. Introduction

Ce chapitre se focalise sur la présentation de l'entreprise accueillante et l'étude détaillée de l'existant où on cernera la problématique de notre sujet et nous présenterons la solution adoptée pour ce dernier.

2. Présentation de la société SONELAGAZ

Sonelgaz, ou **Société nationale de l'électricité et du gaz**, est une compagnie chargée de la production, du transport et de la distribution de l'électricité et du gaz en Algérie **[9].**

❖ **Identité visuelle (logo)**

Cette figure représente le logo de sonelgaz :

Figure 1 : Logo de sonelgaz **[9]**

❖ **Historique**

Elle a été créée en 1969, en remplacement de l'entité précédente Électricité et gaz d'Algérie (EGA), et on lui a donné un monopole de la distribution et de la vente de gaz naturel dans le pays, de même pour la production, la distribution, l'importation, et l'exportation d'électricité. En 2002, le décret présidentiel n° 02-195, la convertit en une Société par actions SPA entièrement détenue par l'État. En 2010, on parle de *Groupe Sonelgaz*.

En 2002, la loi n° 02-01 du 5 février 2002 ouvre le secteur de la production d'énergie électrique à la concurrence et met fin à son monopole. En 2003, elle produisait 29 milliards de kilowattheures par an, vendait 4,6 milliards de mètres cubes de gaz par an. En 2006, elle employait environ 28 000 personnes **[9].**

3. Etude de l existant

3.1 Description de l existant

Cette architecture représente le réseau de sonelgaz.

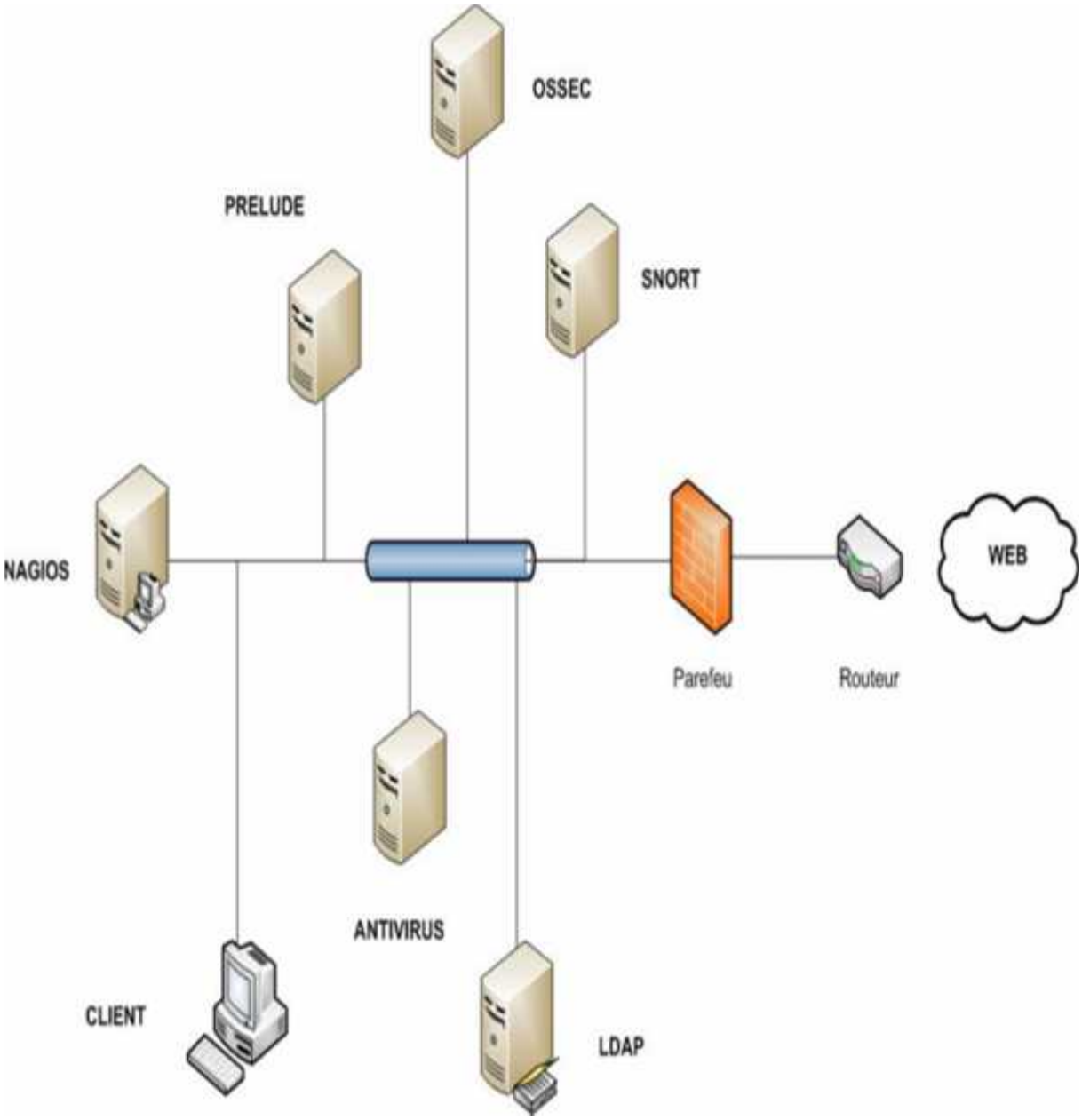


Figure 2 : architecture du réseau de sonelgaz[9]

3.2 Critique de l'existant

Ayant un très grand nombre de serveurs à gérer, l'administrateur est incapable de vérifier leurs disponibiliteé (en ligne ou pas), de déterminer la qualité des services qu'ils offrent, ni détecter la défaillance des équipements (charge CPU, Etat mémoire, surcharge du disque….), ni les surcharges et pénurie temporaire des ressources. Le seul moyen de détecter ces anomalies ne peut se faire que par la réception des différentes plaintes et réclamations des clients.

Se souciant de sa réputation et concerné par la satisfaction et le confort de ses clients, la société veut à tout prix éviter la confrontation à des clients mécontents d'où éviter le risque de les perdre, et ce en travaillant à offrir une meilleure qualité de services à ses clients en anticipant les pannes et en évitant les arrêts de longue durée gênant les services qui peuvent causer de lourdes conséquences aussi bien financières qu'organisationnelles.

Le but de ce projet est donc de trouver une solution optimale pour la gestion des serveurs et le monitoring de ses équipements en premier lieu, offrir la possibilité de devenir « pro actif » face aux problèmes rencontrés en un second lieu, et finalement et le plus important, de pouvoir détecter et interpréter en un simple coup d'œil les causes et origines des problèmes rencontrés afin de les fixer le plus rapidement possible.

3.3 Solution proposée

La gestion des serveurs distants et le monitoring de ses équipements étant le plus grand souci de l'administrateur, nous avons jugé nécessaire de mettre en évidence un outil pour contrôler le fonctionnement du réseau, d'étudier les données collectées et de définir des seuils d'alertes qui peuvent servir pour le déclenchement des alertes lors de détection des problèmes.

Il s'agit donc et sans doute d'une mise en place d'un système de supervision qui pourra grâce aux différentes fonctionnalités qu'il offre, anticiper les pannes en suivant méticuleusement le fonctionnement du système et en surveillant le statut des serveurs, des divers services réseaux et d'offrir des renseignements supplémentaires voir charge CPU, espace disque, mémoire disponible, etc.

Un système de supervision offrira à l'administrateur la possibilité de réagir le plus rapidement possible face aux pannes qui peuvent intervenir afin d'éviter un arrêt de production de longue durée.

4. Etude de choix

De nombreuses plateformes de supervision existent aujourd'hui. Certaines se contentent de gérer à temps réels l'état du réseau et préserve une vue globale sur le fonctionnement de son architecture, d'autres permettent également de connaître l'état des différents services, et d'autres qui offrent la possibilité de ressortir de nombreuses statistiques du réseau permettant une analyse assez fine.

4.1 Les outils non libres

S'assurant que la supervision est un marché porteur, les sociétés se pressent de plus en plus à investir dans des produits permettant la supervision et une meilleure gestion des réseaux. Deux familles apparaissent, celle proposant des solutions généralistes pour la supervision des Réseaux , des serveurs, des applications, des sites web,… comme les logiciels Patrol (BMC), d'Unicenter (Computer Associate), de la gamme openview (HP)...

D"autres offrent une supervision des domaines plus spécifiques citant comme logiciel panorama (Altaworks) qui gère uniquement l'aspect sécurité ou PathWAI (Candle) qui se penche principalement sur la supervision des applications. Ces solutions n'ont qu'un seul point commun : **un prix élevé [10].**

4.2 Les outils libres

Il existe des solutions de supervision libres et professionnelles. Parmi les plus répandues, reconnues du moment nous pouvons citer :

- **NAGIOS**

Créé en 1999 par Ethan Galstad, Nagios est un logiciel qui permet de superviser un système d'information. Il est considéré comme étant la référence des solutions de supervision open source. Il dispose de nombreuses fonctions telles que l'héritage multiple, les dépendances, l'escalade de notifications, les Template de services et d'hôtes, le support des surveillances actives et passives, etc. L'interface web est la partie graphique, 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'activités **[2].**

❖ **CENTREON**

Anciennement appelé Oreon1, Centreon est un logiciel de supervision des applications, systèmes et réseaux, basé sur les concepts de Nagios. C'est une solution complète destinée aux administrateurs et exploitants du service de supervision. Il apporte de nombreuses fonctions telles que la consultation de l'état des services et des machines supervisées, la métrologie, le reporting, l'accès aux événements de supervision, la gestion avancée des utilisateurs via des listes de contrôle d'accès (ACL), etc. Il s'appuie sur les technologies Apache et PHP pour l'interface web, MySQL pour le stockage des données de configuration et de supervision.

❖ **ZABBIX**

Zabbix est un logiciel libre qui permet de surveiller l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources. Le « serveur ZABBIX » peut être décomposé en trois 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. Il repose sur du C/C++, PHP pour la partie front end et MySQL/PostgreSQL/Oracle pour la partie BDD **[2].**

❖ **ZENOSS**

Tout comme Nagios, Zenoss est un outil qui se base sur une application Web qui va surveiller les nœuds de votre réseau et générer des rapports importants pour des décideurs informatiques. Publié sous la licence GNU General Public License (GPL) version 2, Zenoss fournit une interface Web qui permet aux administrateurs système de la surveillance de la disponibilité, de l'inventaire, de la configuration, des performances et des événements **[2].**

❖ **.GANGLIA**

Ganglia est beaucoup plus spécifique, c'est réellement un outil de supervision complémentaire destiné à la supervision d'un système en cluster. Il est basé sur une conception hiérarchique ciblée à des fédérations de grappes. Il exploite des technologies largement utilisées telles que XML pour la représentation des données, XDR pour compact, le transport de données portable et RRDtool pour le stockage des données et la

visualisation. Il utilise des structures de données et d'algorithmes soigneusement conçues pour atteindre de très faibles frais généraux par nœud et haute concurrence **[2].**

❖ **CACTI**

Cacti est un logiciel libre de mesure de performances réseau et serveur basé RRDTool dédié à la métrologie. Il ne fait pas de supervision en tant que tel. Il ne fait pas de corrélation d'incidents ni d'alertes en cas d'incident (bien que des plugins existent, ce n'est pas son but premier. Les possibilités de configuration très avancées font que celui-ci est souvent utilisé en complément de solutions de supervision tel que Nagios, notamment, pour assurer la partie métrologie lorsque les exigences sont fortes. Il permet de représenter sous forme de graphiques n'importe quelle donnée quantifiable collectée soit par le biais de protocoles réseaux tels que SNMP ou soit par des scripts personnalisés par l'utilisateur **[2].**

❖ **MUNIN**

Munin est un outil de surveillance système et réseau open source qui s'appuie sur l'outil RRDTool. Il présente ses résultats sous forme de graphiques disponibles via une interface web. Il possède une structure de plugins particulièrement simple qui permet d'enrichir rapidement l'outil. Des plugins sont actuellement disponibles pour les systèmes d'exploitations suivants: GNU/Linux, FreeBSD, NetBSD, Solaris et AIX. L'architecture du système Munin est constituée d'un serveur principal appelé Munin-master, récupérant les informations à intervalle régulier et de plusieurs nœuds appelés Munin-node. Le nœud doit être installé sur le(s) serveur(s) à surveiller **[2].**

Avantage de ces outils

L’avantage de ces logiciels libres est la gratuité, la disponibilité du code source et la liberté d’étudier et de modifier le code selon nos besoins et de le diffuser. De plus, il existe une communauté importante d’utilisateurs et de développeurs qui participent à l’amélioration des logiciels et apportent une assistance par la mise en ligne des documentations et les participations aux forums **[10].**

4.3 Choix du logiciel

Les différentes solutions commerciales déjà présentées (HPOpenview, Patrol, BigBrother, etc..) nécessitent un investissement important pour leur mise en place, et pour des raisons propres à l'entreprise, toutes ces solutions sont à écarter de mon liste de choix.

Parmi les solutions les plus connues, recommandées et surtout Libres, on citera Nagios et Zabbix. Voici un tableau comparatif des deux logiciels choisis **[11].**

	Zabbix	**Nagios**
Présentation	-Open source, libre -Multiplateformes -Homogène. -Moteur en C, interface web utilisateur en PHP, base de données SQL (MySQL, Oracle…) -Configuration centralisée sur une même interface graphique. ➔Peut monitorer de 3 manières : -LANCEMENT d‟un processus sur les machines à monitorer pour collecter des données locales, grâce à l'agent Zabbix (obtenir des infos sans utiliser SNMP). -Requêtes SNMP. -Check externes qui sert à tester les services réseaux (rien à installer sur l‟équipement surveillé, tests limités à des pings ou test de protocoles).	-Open source, Libre. -Conçu pour les plateformes Unix. -Modulaire. -Moteur en C, perl, sharp…, interface web en PHP, base de données SQL. -Configuration plus ou moins complexe ➔Peut monitorer de 3 manières : -L‟utilisation des journaux d‟exploitation par l‟envoie des évènements issus des fichiers log en temps réel vers un serveur central offrant les informations nécessaires à la supervision. -Supervision active des services et infrastructure qui nous permet de garder l‟historique des performances.

Fonctionnalités	-Offre une interface web de consultation et d‟administration. -Peut générer des graphes. -Peut lever des alertes en envoyant des mails. -Supervise des équipements SNMP. -Gère les pannes et les performances	-Offre une interface web basée sur les CGL avec gestion des droits pour la consultation. -Génère des rapports de surveillance. -Il a la possibilité de monitorer à distance à travers un firewall. -Il peut définir des serveurs esclaves qui prennent le relais si le serveur maitre tombe en panne. -Surveillance des ressources des serveurs (CPU, mémoire…) -Surveillance des services réseaux. -Arrêt temporaire de la supervision locale ou globale. -Génère des graphes par l‟interfaçage avec RRDTools.
Architecture	Architecture généralement basée sur : -Serveur Zabbix, le coeur et moteur de l‟application programmé en C. -Agent Zabbix pour la collection des informations locales.	Architecture généralement basée sur : -Le moteur de l‟application qui sert à ordonnancer les tâches de supervision écrit en C. -Une interface web réalisée à l‟aide des

	-Une interface web d‟administration et consultation des données. -Une base de données SQL.	GCI, décrivant la vue d‟ensemble su système et les anomalies possibles. -Plusieurs plugins qui peuvent être complétés en fonction des besoins.
Avantages	-Multiplateforme. -Utilise peu de ressources -Plus léger grâce à son homogénéité (Pas de plug-in à ajouter). -Mise à jour facile. -Configuration et utilisation aisée. -Interface vaste mais claire	-Des plugins qui étendent les possibilités de Nagios. -Une très grande communauté qui participe activement au développement. -Un moteur performant -solution complète permettant le reporting, la gestion des pannes et d‟alarmes, gestion des utilisateurs… -Des plugins permettent aux utilisateurs de développer facilement ses propres vérifications de services. -Possibilité de repartir la supervision entre plusieurs administrateurs. -Offre la possibilité de développer ses propres modules.
Inconvénients	-L‟agent Zabbix communique les données en claire➔ nécessité de sécuriser les données.	-Configuration complexe mais peut s‟améliorer en ajoutant Centreon. -Interface peu ergonomique

	-Peu d‟interfaçage avec d‟autres solutions commerciales. -Communauté de développeurs limitée.	et intuitive.

Tableau 01 : Tableau comparatif de zabix et nagios**[11]**

Parmi ces solutions libres, les deux logiciels Zabbix et Nagios sont les plus répandus et les plus utilisés. Par rapport à notre projet, se sont les deux solutions les plus adaptées permettant de satisfaire pratiquement tous les besoins de la société, par les différentes fonctionnalités qu'elles offrent. Et compte tenu de ce critère Zabbix et Nagios restent à égalité et il me sera impossible de les départager.

Une des particularités captivantes de Nagios est sa modularité, on a ainsi estimé que Nagios a été plus adapté aux besoins de notre projet que Zabbix. En effet, grâce à ses plugins, Nagios possède une architecture facilement adaptable à l'environnement. Ces derniers pouvant être ajoutés, modifiés ou même personnalisés et permettent de spécifier les tâches pour aboutir au résultat voulu.

De plus Nagios est une solution stable, dispose d'une grande communauté de développeurs et il est utilisé aussi bien dans les petites et moyennes infrastructures que dans les grands parcs informatiques et utilisé surtout par plusieurs entreprises de renommé, tels que Yahoo (100 000 serveurs), Yellow pipe Web Hosting (7000 serveurs) …

Bien que ce dernier soit réputé par sa configuration fastidieuse, il peut être couplé à Centreon un logiciel qui lui servira de couche applicative afin de faciliter la configuration et d'établir des interfaces IHM plus ergonomiques et compréhensibles.et pour cella notre choix s'est porté sur NAGIOS.

5. Conclusion

Ce chapitre a été conçu pour familiariser l'environnement du travail en présentant l'entreprise d'accueil et l'architecture réseau dont elle dispose.

Les problèmes que rencontre la société se sont imposés suite à l'étude de l'existant et à sa critique, ce qui nous a permis de cerner la problématique de notre projet. Nous allons par la suite proposé des solutions et leur étude à notre encadreur de stage et finalement nous avons posé notre choix sur la solution que nous jugeons la plus convenable à la société et à la formation que nous estimons acquérir qui est le logiciel de supervision libre « Nagios ». Dans le chapitre suivant, nous allons présenté quelques outils et protocoles de surveillance.

1. Introduction

Les systèmes d'information sont tous différents de par leur taille, leur nature, leur criticité. Ils ont cependant pour point commun d'être le théâtre d'incidents, à un moment ou à un autre. Un des rôles des administrateurs est justement de gérer cela. Ils doivent concevoir l'architecture du système d'information de telle manière qu'une panne ait un impact minimal sur le reste du système.

Les administrateurs ont un objectif clair : le maintien en production du système d'information. Cependant, tous les éléments ne sont pas logés à la même enseigne en ce qui concerne la criticité. Certaines parties sont vitales pour l'entreprise, comme les **serveurs**. Sans outils de supervision, il est quasi impossible pour un administrateur de garder en tête ces différents niveaux de criticité. L'outil de supervision peut ainsi aider à mettre des priorités sur les interventions des administrateurs et leur permettre de se concentrer sur l'essentiel. C'est pourquoi les administrateurs réseaux et systèmes font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi informé (par email, par SMS) en cas de problème. Un tel système assure une gestion proactive du système et améliore la disponibilité effective des applications et des services opérant sur les serveurs. Mieux elle permet d'anticiper et de prévoir les éventuels besoins en termes d'équipements pour une gestion optimale du système d'information.

2. La supervision informatique

La supervision est la « surveillance du bon fonctionnement d'un système ou d'une activité ».Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques. Elle répond aux préoccupations suivantes **[1].**

- Technique : surveillance du réseau, de l'infrastructure et des machines.
- Applicative : surveillance des applications et des processus métiers.
- Contrat de service : surveillance du respect des indicateurs contractuels.
- Cétier : surveillance des processus métiers de l'entreprise.

Nous ajouterons les actions réflexes à cette surveillance du système. Ce sont les réactions automatisées en fonctions d'alertes définies.

En cas de dysfonctionnement, le système de supervision permet d'envoyer des messages sur la console de supervision, ou bien d'envoyer un courriel à l'opérateur et ce 24H/24 et 7j/7 dans certaines entreprises.

Mais si la supervision n'est pas active 24X7 le dysfonctionnement se produit en dehors des heures de bureau, et en l'absence de système approprié, l'alerte n'est pas reçue par l'opérateur, et les utilisateurs des applications ne sont pas prévenus du dysfonctionnement C'est pourquoi il peut être utile de compléter le superviseur par un logiciel de gestion des alertes, qui envoie automatiquement un courriel, un SMS, ou un appel téléphonique à un opérateur sous astreinte.

3. Les types de surveillance

Parmi les types de surveillance **[2].**

3.1 Supervision system

La supervision système porte principalement sur les trois types principaux de ressources système :

- le processeur.
- la mémoire.
- le stockage.
- commutateurs : utilisation des ressources, métrologie.
- serveurs : utilisation des ressources.

3.2 Supervision réseau

La supervision réseau porte sur la surveillance de manière continue de la disponibilité des services en ligne, du fonctionnement, des débits, de la sécurité mais également du contrôle des flux.

3.3 Supervisons des applications

La supervision des applications (ou supervision applicative) permet de connaître la disponibilité des machines en termes de services rendus en testant les applications hébergées par les serveurs.

À titre d'exemple, un serveur web peut avoir une supervision système et réseau avec des signaux au vert, et la machine ne sera pourtant pas disponible au sens du service web si apache n'est pas présent ou n'est pas en mesure de servir des pages web.

La supervision applicative passe donc par des mesures faites aussi sur le flux de service. On parle alors de validation fonctionnelle. On utilise souvent un sous-ensemble des tests ayant permis la recette d'une application pour n'en prendre que les tests qui sont représentatifs de l'activité sans pour autant générer une charge trop importante ou modifier les données applicatives.

La supervision applicative ne peut se faire sans considérer la sécurité applicative.

4. La supervision des réseaux

4.1 Définition de la supervision des réseaux

La supervision réseau (ou monitoring) comprend un ensemble de protocoles, matériels et logiciels informatiques permettant de suivre à distance l'activité d'un réseau informatique. Ces solutions permettent également de cartographier le réseau.
La supervision est particulièrement adaptée pour des réseaux de plus de 50 machines et pour les prestataires de services.
Le principe général est le suivant :
– Des agents (ou sondes) sont placés sur les équipements à surveiller
– Un ou plusieurs serveurs centralisent les informations pour les afficher de manière cohérente aux techniciens ou aux administrateurs.
Il convient de distinguer la supervision qui utilise des technologies quasi temps réel de la gestion de parc informatique qui utilise des technologies moins dynamiques (inventaires de machines, gestion des stocks, …)**[1].**

4.2 Les fonctionnalités de la supervision réseau

Les principales fonctions que doivent implémenter les systèmes de supervision et d'administration sont les suivantes **[3].**

4.2.1 Gestion de la sécurité

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

4.2.2 Gestion de la comptabilité

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

4.2.3 Gestion des anomalies

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 cela 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 récurrent. 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.

4.2.4 Gestion des configurations

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 système d'exploitation, 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.

4.2.5 Gestion des performances

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 nous peuvons 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 régler 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.

4.3 Les moyens pour la supervision

Les deux règles d'or de la supervision sont d'être le moins intrusif possible et le plus indépendant possible des éléments supervisés afin de garantir un regard extérieur non biaisé.

Deux grandes méthodes de supervision sont utilisées avec plusieurs variantes :

Les méthodes active et passive, détaillées dans des paragraphes suivants **[12].**

4.3.1 Supervision active

La supervision active est la plus classique. Elle consiste en l'envoi de requêtes d'interrogation et de mesure par la plateforme de supervision. Cette méthode est composée de trois étapes **[12].**

- le serveur envoie une requête vers la ressource supervisée.
- La ressource repend à la requête du serveur.
- Le serveur analyse l'information et détermine un état pour la ressource.

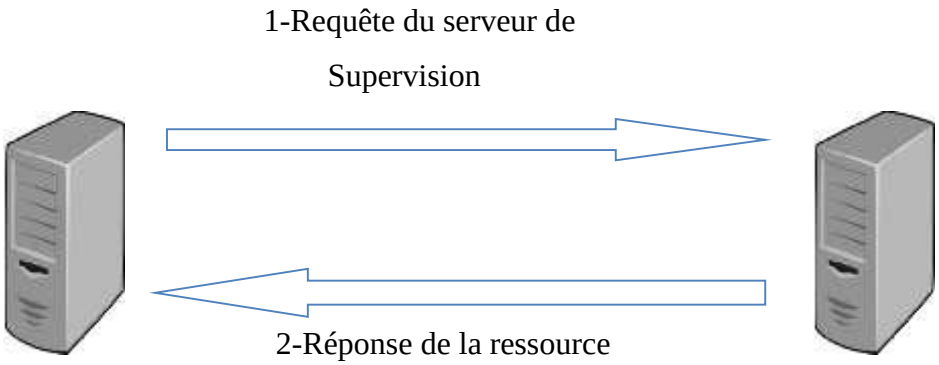


Figure 3 : Echange de message entre le serveur de Supervision et la ressource supervisée **[12].**

Cette méthode est la plus utilisée. Elle a l'avantage d'être fiable : les vérifications se font de manière régulière et en mode question-réponse.

Les deux protocoles de supervision active sont :

- Le protocole SNMP est le standard en matière de supervision active .il est largement adopté et utilisé.
- Le protocole WMI (Windows Management Instrumentation) est un standard de supervision pour les Systems Microsoft Windows.

4.3.2 Supervision passive

La supervision passive l'est du point de vue du serveur de supervision : ce sont les Ressources supervisées qui transmettent des alertes au serveur de supervision: **[12].**

- La ressource supervisée vérifie son état et transmet de manière autonome le résultat au serveur de supervision.
- Le serveur de supervision reçoit l'alerte et la traite.

L'échange est unidirectionnel.

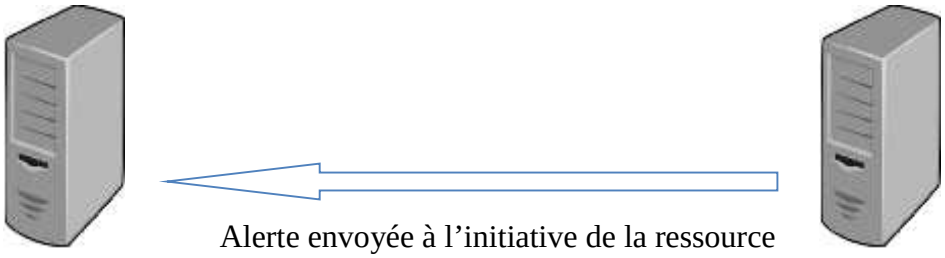


Figure 4 : Echange de message entre le serveur de

Supervision et la ressource supervisé **[12].**

La méthode passive possède plusieurs intérêts. D'abord elle est moins consommatrice de ressources du point de vue serveur de supervision et réseau. Le principal point noir de la supervision passive concerne la fraicheur des informations :rien ne permet de garantir que la ressource supervisée est dans un état correct si aucune alerte n'est reçue .les ressources n'envoient que très rarement des messages pour signaler un état correct.

4.4 Quelques standards de la supervision

Le monde de la supervision et du management des infrastructures en général possèdent ses normes et standards, pour la plupart émergeants, dont sont présentés ici les plus significatifs.

Ces standards sont pour la plupart gérés par la DMTF **[5].**

4 .4.1 IPMI (Intelligent Platform Management Interface)

L'Interface de gestion intelligente de matériel, (ou IPMI, Intelligent Platform

Management Interface) est un ensemble de spécifications d'interfaces communes avec du matériel informatique (principalement des serveurs) permettant de surveiller certains composants (ventilateur, sonde de température, …).

4 .4.2 JMX (Java Management Interface)

JMX (Java Management Extensions) est une API pour Java permettant de gérer le fonctionnement d'une application Java en cours d'exécution. JMX a été intégré dans J2SE à

partir de la version 5.0. (Attention, JMX est, par défaut, désactivé en version 5.0. Utiliser : java -Dcom.sun.management.jmxremote).Nous pouvons voir JMX comme une espèce de SNMP pour Java.

4 .4.3 CIM (Common Information Model)

Standard de description des données administratives développé par le DMTF (Desktop Management Task Force).

4 .4.4 ITIL (Information Technology Infrastructure Library)

ITIL (Information Technology Infrastructure Library) est un ensemble de bonnes pratiques (en anglais, « best practice » NB: cette expression s'écrit au singulier en anglais, mais au pluriel en français) pour la gestion d'un système d'information (informatique), édictées par l'Office public britannique du Commerce.

Sont en particulier abordés les sujets ci-dessous :

- une production informatique ?
- Comment améliorer l'efficacité du système d'information ?
- Comment réduire les risques ?
- Comment augmenter la qualité des services informatiques ?

Assez populaire en Europe à la fin des années 1980, ITIL s'est implanté sur le marché nord-américain, via des entreprises proches de l'informatique, comme Andersen Consulting (appelée désormais BearingPoint), Ernst & Young, Hewlett-Packard, ou PricewaterhouseCoopers.

Les recommandations ITIL positionnent des blocs organisationnels et des flux d'informations. De nombreux logiciels d'exploitation informatique sont conformes à ces recommandations.

4 .4.5 CMDB (Configuration Management DataBase),

Est une base de données unifiant les composants d'un système informatique. Elle permet de comprendre l'organisation entre ceux-ci et de modifier leur configuration. La CMDB est un composant fondamental d'une architecture ITIL.

Une CMDB contient des informations sur les principaux composants du système d'information (appelés configuration items ou CI) et des détails sur les relations importantes entre eux. Un CI est une instance d'une entité disposant d'attributs modifiables : par exemple un ordinateur, un processus ou un employé. Un facteur de succès clé lors de l'implémentation d'une CMDB est la capacité à récupérer automatiquement des informations concernant les CIs (auto-discovery) et à suivre les changements au fur et à mesure.

Les CMDBs contiennent des métadonnées et par conséquent leur utilisation peut entrer en conflit avec le concept de dépôt de métadonnées tel que déployé dans les grandes organisations informatiques. La gestion des configurations en tant que processus traite de la manière dont les données sont mises à jour, ce qui est justement une faiblesse des dépôts de métadonnées. Les CMDBs apportent alors la gestion des historiques. De plus, elles s'intègrent dans le processus ITIL plus global et apportent une cohérence à la gestion du système d'information.

4.5 Certains protocoles utilisés par les Systèmes de supervision

4.5.1 Le protocole SNMP

- **Définition du protocole SNMP**

SNMP signifie Simple Network Management Protocol (traduisez *protocole simple de gestion de réseau*). Il s'agit d'un protocole qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau **[6].**

- **Principe de fonctionnement du protocole SNMP**

Le système de gestion de réseau est basé sur deux éléments principaux : un superviseur et des agents. Le superviseur est la console qui permet à l'administrateur réseau d'exécuter des requêtes de management. Les agents sont des entités qui se trouvent au niveau de chaque interface connectant l'équipement managé au réseau et permettant de récupérer des informations sur différents objets.

Les Switchs, les hubs, les routeurs et les serveurs sont des exemples d'équipements contenant des objets manageables. Ces objets manageables peuvent être des informations

matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont directement liés au comportement en cours de l'équipement en question. Ces objets sont classés dans une sorte de base de données appelée **MIB** ("*Management Information Base*"). SNMP permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB.

L'architecture de gestion du réseau proposée par le protocole SNMP est donc basée sur trois principaux éléments : **[6]**

- Les équipements managés (managed devices) sont des éléments du réseau (ponts, hubs, routeurs ou serveurs), contenant des "objets de gestion" (*managed objects*) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques ;
- Les agents, c'est-à-dire une application de gestion de réseau résidant dans un périphérique et chargé de transmettre les données locales de gestion du périphérique au format SNMP ;
- Les systèmes de management de réseau (*network management systems* notés NMS), c'est-à-dire une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration.

4.5.2 Le protocole ICMP

⟩ Définition

Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite des protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.

ICMP se situe au même niveau que le protocole IP bien qu'il ne fournisse pas les primitives de service habituellement associées à un protocole de couche réseau. Son utilisation est habituellement transparente du point de vue des applications et des utilisateurs présents sur le réseau **[7].**

4.6 Quelques outils simples de surveillance des réseaux

On ne peut pas réellement parler de supervision, mais quand même de surveillance en utilisant des petits outils simples qui, une fois combinés à l'aide de langages de scripts permettent de réaliser des choses très intéressantes. D'autres part, ces petits outils sont la base des plus grosses solutions de supervision, il semble donc intéressant d'appréhender leur fonctionnement **[8].**

4.6.1 Ping

Voilà un outil très simple, qui remplit une tâche très importante. C'est en effet ce programme qui va nous permettre, en utilisant le protocole ICMP, de savoir si une machine destination est accessible (dans le cas contraire, connaître approximativement la raison via le code d'erreur ICMP) et de mesurer la latence existante entre les deux extrémités. L'implémentation est simple, Ping envoi une requête ICMP Echo et attend en retour une requête ICMP Echo Reply. Ping est par exemple souvent utilisé pour réaliser une alerte qui prévient l'administrateur d'une machine quand celle-ci n'est plus joignable. **[8].**

4.6 .2 Outils SNMP

Il existe bien évidemment des programmes simples destinés à utiliser le protocole SNMP. Leurs noms indiquent quelle requête ils peuvent envoyer, par exemple : snmpget, snmpgetnext, snmpinform, snmpset etc...Chacune de ses commandes permet de réaliser la requête en utilisant une des trois versions du protocole SNMP. Elles sont énormément utilisées dans le cadre de scripts qui stockent les valeurs obtenues afin de réaliser des statistiques ou des alertes. (exemple d'utilisation fournis en Fig 1).

4.6.3 MRTG

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

conséquent qui permet sur une même page de surveiller un réseau et de garder les traces des anciennes données. **.**

4.6 .4 RRDTOOL

Du même auteur que MRTG, RRDTOOL est un peu considéré comme une évolution de ce dernier. La gestion de stockage des données a surtout été entièrement revue pour améliorer les performances, pour cela l'auteur a utilisé une technique nommée "Round Robin", d'où le nom "RRDTOOL"(Round Robin Database TOOL). Les graphiques se sont également améliorés offrant plus de possibilités, et l'interfaçage entre la récupération de donnée et la génération des images est devenu plus modulaire permettant de réaliser des scripts dans beaucoup de langages différents. RRDTOOL est maintenant un outil incontournable pour générer des graphiques, il est donc utilisé dans quasiment tous les logiciels de supervision open-source **[8].**

5. Conclusion

La supervision est devenue indispensable dans le système d'information. Elle est à la base du bon fonctionnement d'une architecture réseau et permet de réagir rapidement en cas de problèmes ou pannes. Elle se base à l'heure actuelle principalement sur le protocole SNMP qui depuis de nombreuses années a quand même du mal à évoluer. Le chapitre suivant attaquera une étude approfondie de la solution proposée.

1. Introduction

Les systèmes d'information sont tous différents de par leur taille, leur nature, leur criticité. Ils ont cependant pour point commun d'être le théâtre d'incidents, à un moment ou à un autre. Un des rôles des administrateurs est justement de gérer cela. Ils doivent concevoir l'architecture du système d'information de telle manière qu'une panne ait un impact minimal sur le reste du système.

Les administrateurs ont un objectif clair : le maintien en production du système d'information. Cependant, tous les éléments ne sont pas logés à la même enseigne en ce qui concerne la criticité. Certaines parties sont vitales pour l'entreprise, comme les **serveurs**. Sans outil de supervision, il est quasi impossible pour un administrateur de garder en tête ces différents niveaux de criticité. L'outil de supervision peut ainsi aider à mettre des priorités sur les interventions des administrateurs et leur permettre de se concentrer sur l'essentiel.

C'est pourquoi les administrateurs réseaux et systèmes font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être aussi informé (par email, par SMS) en cas de problème. Un tel système assure une gestion proactive du système et améliore la disponibilité effective des applications et des services opérant sur les serveurs. Mieux elle permet d'anticiper et de prévoir les éventuels besoins en termes d'équipements pour une gestion optimale du système d'information.

2. La supervision informatique

La supervision[1] est la « surveillance du bon fonctionnement d'un système ou d'une activité ».Elle permet de surveiller, rapporter et alerter les fonctionnements normaux et anormaux des systèmes informatiques. Elle répond aux préoccupations suivantes :

- technique : surveillance du réseau, de l'infrastructure et des machines ;
- applicative : surveillance des applications et des processus métiers ;
- contrat de service : surveillance du respect des indicateurs contractuels ;
- métier : surveillance des processus métiers de l'entreprise.

[1] http://blog.adminrezo.fr/wp-content/uploads/2013/05/supervision-des-reseaux-v1.pdf

On ajoutera les actions réflexes à cette surveillance du système. Ce sont les réactions automatisées en fonctions d'alertes définies.

En cas de dysfonctionnement, le système de supervision permet d'envoyer des messages sur la console de supervision, ou bien d'envoyer un courriel à l'opérateur et ce 24h/24 et 7j/7 dans certaines entreprises.

Mais si la supervision n'est pas active 24/7 le dysfonctionnement se produit en dehors des heures de bureau, et en l'absence de système approprié, l'alerte n'est pas reçue par l'opérateur, et les utilisateurs des applications ne sont pas prévenus du dysfonctionnement C'est pourquoi il peut être utile de compléter le superviseur par un logiciel de gestion des alertes, qui envoie automatiquement un courriel, un SMS, ou un appel téléphonique à un opérateur sous astreinte.

3. Les types de surveillance

Parmi les types[2] de surveillance **:**

3.1 Supervision system

La supervision système porte principalement sur les trois types principaux de ressources système :

- le processeur .
- la mémoire.
- le stockage.
- commutateurs : utilisation des ressources, métrologie.
- serveurs : utilisation des ressources.

3.2 Supervision réseau

La supervision réseau porte sur la surveillance de manière continue de la disponibilité des services en ligne — du fonctionnement, des débits, de la sécurité mais également du contrôle des flux.

[2] https://fr.wikipedia.org/wiki/Supervision

3.3 Supervisons des applications

La supervision des applications (ou supervision applicative) permet de connaître la disponibilité des machines en termes de services rendus en testant les applications hébergées par les serveurs.

À titre d'exemple, un serveur web peut avoir une supervision système et réseau avec des signaux au vert, et la machine ne sera pourtant pas disponible au sens du service web si apache n'est pas présent ou n'est pas en mesure de servir des pages web.

La supervision applicative passe donc par des mesures faites aussi sur le flux de service. On parle alors de validation fonctionnelle. On utilise souvent un sous-ensemble des tests ayant permis la recette d'une application pour n'en prendre que les tests qui sont représentatifs de l'activité sans pour autant générer une charge trop importante ou modifier les données applicatives.

La supervision applicative ne peut se faire sans considérer la sécurité applicative.

4. La supervision des réseaux

4.1 Définition de la supervision des réseaux[3]

La supervision réseau (ou monitoring) comprend un ensemble de protocoles, matériels et logiciels informatiques permettant de suivre à distance l'activité d'un réseau informatique. Ces solutions permettent également de cartographier le réseau.
La supervision est particulièrement adaptée pour des réseaux de plus de 50 machines et pour les prestataires de services.
Le principe général est le suivant :
– Des agents (ou sondes) sont placés sur les équipements à surveiller
– Un ou plusieurs serveurs centralisent les informations pour les afficher de manière cohérente aux techniciens ou aux administrateurs.
Il convient de distinguer la supervision qui utilise des technologies quasi temps réel de la gestion de parc informatique qui utilise des technologies moins dynamiques (inventaires de machines, gestion des stocks, …).

[3] http://blog.adminrezo.fr/wp-content/uploads/2013/05/supervision-des-reseaux-v1.pdf

4.2 Les fonctionnalités de la supervision réseau

Les principales fonctions[4] qui doivent implémenter les systèmes de supervision et d'administration sont les suivantes.

4.2.1 Gestion de la sécurité

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

4.2.2 Gestion de la comptabilité

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

4.2.3 Gestion des anomalies

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 cela 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 récurrent. 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.

4.2.4 Gestion des configurations

La gestion des configurations effectue un suivi des différentes configurations des éléments

[4] www.junet.ci/telechargement/**memoire**_Abbe.**pdf**

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 système d'exploitation, 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.

4.2.5 Gestion des performances

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 régler 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.

4.3 Les moyens pour la supervision

Les deux règles d'or de la supervision sont d'être le moins intrusif possible et le plus indépendant possible des éléments supervisés afin de garantir un regard extérieur non biaisé.

Deux grandes méthodes de supervision sont utilisées avec plusieurs variantes :

Les méthodes active et passive, détaillées dans des paragraphes suivants.[5]

[5] FONTAINE.L et LEGROS.B,EDITION ENI,CENTREON, octobre 2012,imprimé en France, pp.18

4.3.1 Supervision active

La supervision active [6] est la plus classique. Elle consiste en l'envoi de requêtes d'interrogation et de mesure par la plateforme de supervision. Cette méthode est composée de trois étapes :

- le serveur envoie une requête vers la ressource supervisée.
- La ressource repend à la requête du serveur.
- Le serveur analyse l'information et détermine un état pour la ressource.

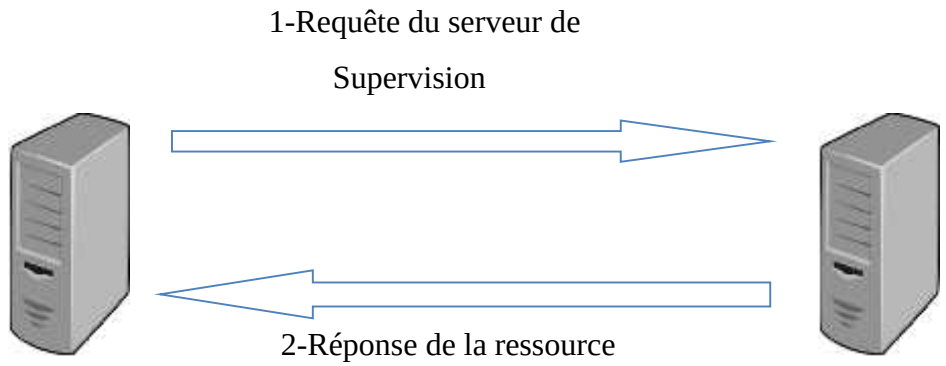


Figure 1 : Echange de message entre le serveur de Supervision et la ressource supervisée

Cette méthode est la plus utilisée. Elle a l'avantage d'être fiable : les vérifications se font de manière régulière et en mode question-réponse.

Les deux protocoles de supervision active sont :

- Le protocole SNMP est le standard en matière de supervision active .il est largement adopté et utilisé.
- Le protocole WMI (Windows Management Instrumentation) est un standard de supervision pour les Systems Microsoft Windows.
-

[6] FONTAINE.L et LEGROS.B,EDITION ENI,CENTREON, octobre 2012,imprimé en France, pp.19

4.3.2 Supervision passive

La supervision passive[7] l'est du point de vue du serveur de supervision : ce sont les

Ressources supervisées qui transmettent des alertes au serveur de supervision:

- La ressource supervisée vérifie son état et transmet de manière autonome le résultat au serveur de supervision.
- Le serveur de supervision reçoit l'alerte et la traite.

L'échange est unidirectionnel.

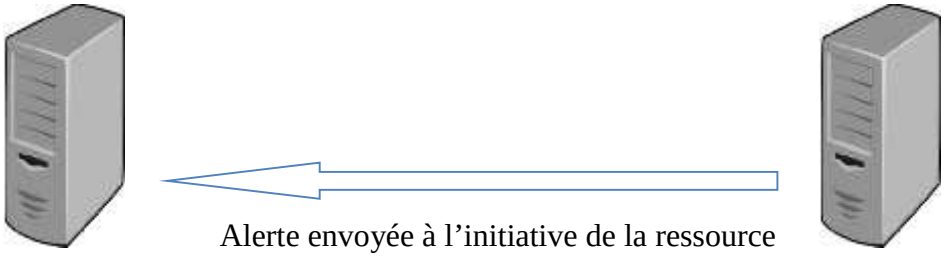


Figure 2 : Echange de message entre le serveur de

Supervision et la ressource supervisé

La méthode passive possède plusieurs intérêts. D'abord elle est moins consommatrice de ressources du point de vue serveur de supervision et réseau. Le principal point noir de la supervision passive concerne la fraicheur des informations :rien ne permet de garantir que la ressource supervisée est dans un état correct si aucune alerte n'est reçue .les ressources n'envoient que très rarement des messages pour signaler un état correct.

4.4 Quelques standards de la supervision

Le monde de la supervision et du management des infrastructures en général possèdent ses normes et standards, pour la plupart émergeants, dont sont présentés ici les plus significatifs.

[7] FONTAINE.L et LEGROS.B,EDITION ENI,CENTREON, octobre 2012,imprimé en France, pp.20

Ces standards sont pour la plupart gérés par la DMTF.[8]

4 .4.1 IPMI (Intelligent Platform Management Interface)

L'Interface de gestion intelligente de matériel, (ou IPMI, Intelligent Platform

Management Interface) est un ensemble de spécifications d'interfaces communes avec du matériel informatique (principalement des serveurs) permettant de surveiller certains composants (ventilateur, sonde de température, …).

4 .4.2 JMX (Java Management Interface)

JMX (Java Management Extensions) est une API pour Java permettant de gérer le fonctionnement d'une application Java en cours d'exécution. JMX a été intégré dans J2SE à partir de la version 5.0. (Attention, JMX est, par défaut, désactivé en version 5.0. Utiliser : java -Dcom.sun.management.jmxremote). On peut voir JMX comme une espèce de SNMP pour Java.

4 .4.3 CIM (Common Information Model)

Standard de description des données administratives développé par le DMTF (Desktop Management Task Force).

4 .4.4 ITIL (Information Technology Infrastructure Library)

ITIL (Information Technology Infrastructure Library) est un ensemble de bonnes pratiques (en anglais, « best practice » NB: cette expression s'écrit au singulier en anglais, mais au pluriel en français) pour la gestion d'un système d'information (informatique), édictées par l'Office public britannique du Commerce.

Sont en particulier abordés les sujets ci-dessous :

- une production informatique ?
- Comment améliorer l'efficacité du système d'information ?
- Comment réduire les risques ?

[8] http://www.monitoring-fr.org/supervision/standards/

- Comment augmenter la qualité des services informatiques ?

Assez populaire en Europe à la fin des années 1980, ITIL s'est implanté sur le marché nord-américain, via des entreprises proches de l'informatique, comme Andersen Consulting (appelée désormais BearingPoint), Ernst & Young, Hewlett-Packard, ou PricewaterhouseCoopers.

Les recommandations ITIL positionnent des blocs organisationnels et des flux d'informations. De nombreux logiciels d'exploitation informatique sont conformes à ces recommandations.

4 .4.5 La CMDB (Configuration Management DataBase),

Est une base de données unifiant les composants d'un système informatique. Elle permet de comprendre l'organisation entre ceux-ci et de modifier leur configuration. La CMDB est un composant fondamental d'une architecture ITIL.

Une CMDB contient des informations sur les principaux composants du système d'information (appelés configuration items ou CI) et des détails sur les relations importantes entre eux. Un CI est une instance d'une entité disposant d'attributs modifiables : par exemple un ordinateur, un processus ou un employé. Un facteur de succès clé lors de l'implémentation d'une CMDB est la capacité à récupérer automatiquement des informations concernant les CIs (auto-discovery) et à suivre les changements au fur et à mesure.

Les CMDBs contiennent des métadonnées et par conséquent leur utilisation peut entrer en conflit avec le concept de dépôt de métadonnées tel que déployé dans les grandes organisations informatiques. La gestion des configurations en tant que processus traite de la manière dont les données sont mises à jour, ce qui est justement une faiblesse des dépôts de métadonnées. Les CMDBs apportent alors la gestion des historiques. De plus, elles s'intègrent dans le processus ITIL plus global et apportent une cohérence à la gestion du système d'information.

4.5 Les protocoles utilisés par les Systems de supervision

4.5.1 Le protocole SNMP [9]

⟩ Définition du protocole SNMP

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

⟩ Principe de fonctionnement du protocole SNMP

Le système de gestion de réseau est basé sur deux éléments principaux : un superviseur et des agents. Le superviseur est la console qui permet à l'administrateur réseau d'exécuter des requêtes de management. Les agents sont des entités qui se trouvent au niveau de chaque interface connectant l'équipement managé au réseau et permettant de récupérer des informations sur différents objets.

Switchs, hubs, routeurs et serveurs sont des exemples d'équipements contenant des objets manageables. Ces objets manageables peuvent être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont directement liés au comportement en cours de l'équipement en question. Ces objets sont classés dans une sorte de base de données appelée **MIB** ("*Management Information Base*"). SNMP permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB.

L'architecture de gestion du réseau proposée par le protocole SNMP est donc basée sur trois principaux éléments :

- Les équipements managés (managed devices) sont des éléments du réseau (ponts, hubs, routeurs ou serveurs), contenant des "objets de gestion" (*managed objects*)

[9] http://www.commentcamarche.net/contents/537-le-protocole-snmp

pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques ;

- Les agents, c'est-à-dire une application de gestion de réseau résidant dans un périphérique et chargé de transmettre les données locales de gestion du périphérique au format SNMP ;
- Les systèmes de management de réseau (*network management systems* notés NMS), c'est-à-dire une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration.

4.5.2 Le protocole ICMP

⁾ Définition

Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite des protocoles Internet. Il est utilisé pour véhiculer des messages de contrôle et d'erreur pour cette suite de protocoles, par exemple lorsqu'un service ou un hôte est inaccessible.

ICMP se situe au même niveau que le protocole IP bien qu'il ne fournisse pas les primitives de service habituellement associées à un protocole de couche réseau. Son utilisation est habituellement transparente du point de vue des applications et des utilisateurs présents sur le réseau.[10]

4.6 Quelques outils simples de surveillance des réseaux

On ne peut pas réellement parler de supervision, mais quand même de surveillance en utilisant des petits outils simples qui, une fois combinés à l'aide de langages de scripts permettent de réaliser des choses très intéressantes. D'autres part, ces petits outils sont la base des plus grosses solutions de supervision, il semble donc intéressant d'appréhender leur fonctionnement.[11]

[10] https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol

[11] http://www.o00o.org/monitoring/outils.html

4.6.1 Ping

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

4.6 .2 Outils SNMP

Il existe bien évidemment des programmes simples destinés à utiliser le protocole SNMP. Leurs noms indiquent quelle requête ils peuvent envoyer, par exemple : snmpget, snmpgetnext, snmpinform, snmpset etc...

Chacune de ses commandes permet de réaliser la requête en utilisant une des trois versions du protocole SNMP. Elles sont énormément utilisées dans le cadre de scripts qui stockent les valeurs obtenues afin de réaliser des statistiques ou des alertes. (exemple d'utilisation fournis en Fig 1).

4.6.3 MRTG

MRTG est un outil réalisé en Perl et en C dans le but de surveiller la charge des liens réseaux. Il génère des pages html contenant des images au format PNG qui représentent graphiquement l'état en temps réel de la ressource surveillée. Le principe est simple : un script Perl recherche les données via le protocole SNMP et envoi celles-ci à un programme C qui va les stocker et générer les graphiques.

A la base l'auteur avait dans le but de surveiller le trafic passant par des routeurs, mais MRTG se basant sur SNMP, les possibilités se sont étendues à toute variable. Encore mieux, on peut aussi créer un script qui surveillera n'importe quelle type de donnée non disponible dans SNMP. On possède ainsi un système de surveillance déjà conséquent qui permet sur une même page de surveiller un réseau et de garder les traces des anciennes données. .

4.6 .4 RRDTOOL

Du même auteur que MRTG, RRDTOOL est un peu considéré comme une évolution de ce dernier. La gestion de stockage des données a surtout été entièrement revue pour améliorer les performances, pour cela l'auteur a utilisé une technique nommée "Round Robin", d'où le

nom "RRDTOOL"(Round Robin Database TOOL).
Les graphiques se sont également améliorés offrant plus de possibilités, et l'interfaçage entre la récupération de donnée et la génération des images est devenu plus modulaire permettant de réaliser des scripts dans beaucoup de langages différents. RRDTOOL est maintenant un outil incontournable pour générer des graphiques, il est donc utilisé dans quasiment tous les logiciels de supervision open-source. .

5. Conclusion

La supervision est devenue indispensable dans le système d'information. Elle est à la base du bon fonctionnement d'une architecture réseau et permet de réagir rapidement en cas de problèmes ou pannes. Elle se base à l'heure actuelle principalement sur le protocole SNMP qui depuis de nombreuses années a quand même du mal à évoluer. Dans le chapitre suivant, nous présentons les besoins fonctionnels et non fonctionnels.

1. Introduction

Ce chapitre se focalise sur la présentation de l'entreprise accueillante et l'étude détaillée de l'existant où on cernera la problématique de mon sujet et on présentera la solution adoptée pour ce dernier.

2. présentation de la société SONELAGAZ

Sonelgaz[12], ou **Société nationale de l'électricité et du gaz**, est une compagnie chargée de la production, du transport et de la distribution de l'électricité et du gaz en Algérie.

❖ **Identité visuelle (logo)**

❖ **Historique**

Elle a été créée en 1969, en remplacement de l'entité précédente Électricité et gaz d'Algérie (EGA), et on lui a donné un monopole de la distribution et de la vente de gaz naturel dans le pays, de même pour la production, la distribution, l'importation, et l'exportation d'électricité. En 2002, le décret présidentiel nº 02-195, la convertit en une Société par actions SPA entièrement détenue par l'État. En 2010, on parle de *Groupe Sonelgaz*.

En 2003, elle produisait 29 milliards de kilowattheures par an, vendait 4,6 milliards de mètres cubes de gaz par an. En 2006, elle employait environ 28 000 personnes. En 2002, la loi n° 02-

12

01 du 5 février 2002 ouvre le secteur de la production d'énergie électrique à la concurrence et met fin à son monopole.

3. Etude de l existant

3.1 Description de l existant[13]

13

3.2 Critique de l'existant

Ayant un très grand nombre de serveurs à gérer, l'administrateur est incapable de vérifier leurs disponibilité (en ligne ou pas), de déterminer la qualité des services qu'ils offrent, ni détecter la défaillance des équipements (charge CPU, Etat mémoire, surcharge du disque….), ni les surcharges et pénurie temporaire des ressources. Le seul moyen de détecter ces anomalies ne peut se faire que par la réception des différentes plaintes et réclamations des clients.

Se souciant de sa réputation et concerné par la satisfaction et le confort de ses clients, la société veut à tout prix éviter la confrontation à des clients mécontents d'où éviter le risque de les perdre, et ce en travaillant à offrir une meilleure qualité de services à ses clients en anticipant les pannes et en évitant les arrêts de longue durée gênant les services qui peuvent causer de lourdes conséquences aussi bien financières qu'organisationnelles.

Le but de ce projet est donc de trouver une solution optimale pour la gestion des serveurs et le monitoring de ses équipements en premier lieu, offrir la possibilité de devenir « pro actif » face aux problèmes rencontrés en un second lieu, et finalement et le plus important, de pouvoir détecter et interpréter en un simple coup d'œil les causes et origines des problèmes rencontrés afin de les fixer le plus rapidement possible.

3.3 Solution proposée

La gestion des serveurs distants et le monitoring de ses équipements étant le plus grand souci de l'administrateur, j'ai jugé nécessaire de mettre en évidence un outil pour contrôler le fonctionnement du réseau, d'étudier les données collectées et de définir des seuils d'alertes qui peuvent servir pour le déclenchement des alertes lors de détection des problèmes.

Il s'agit donc et sans doute d'une mise en place d'un système de supervision qui pourra grâce aux différentes fonctionnalités qu'il offre, anticiper les pannes en suivant méticuleusement le fonctionnement du système et en surveillant le statut des serveurs, des divers services réseaux et d'offrir des renseignements supplémentaires voir charge CPU, espace disque, mémoire disponible, etc.

Un système de supervision offrira à l'administrateur la possibilité de réagir le plus rapidement possible face aux pannes qui peuvent intervenir afin d'éviter un arrêt de production de trop longue durée.

4. Etude de choix

De nombreuses plateformes de supervision existent aujourd'hui. Certaines se contentent de gérer à temps réels l'état du réseau et préserve une vue globale sur le fonctionnement de son architecture, d'autres permettent également de connaître l'état des différents services, et d'autres qui offrent la possibilité de ressortir de nombreuses statistiques du réseau permettant une analyse assez fine.

4.1 Les offres éditeurs

S'assurant que la supervision est un marché porteur[14], les sociétés se pressent de plus en plus à investir dans des produits permettant la supervision et une meilleure gestion des réseaux. Deux familles apparaissent, celle proposant des solutions généralistes pour la supervision des Réseaux , des serveurs, des applications, des sites web,… comme les logiciels Patrol (BMC), d'Unicenter (Computer Associate), de la gamme openview (HP)...
D‟autres offrent une supervision des domaines plus spécifiques citant comme logiciel panorama (Altaworks) qui gère uniquement l'aspect sécurité ou PathWAI (Candle) qui se penche principalement sur la supervision des applications. Ces solutions n'ont qu'un seul point commun : **un prix élevé**.

4.2 Les offres libres

Il existe des solutions de supervision libres et professionnelles. Parmi les plus répandues, reconnues du moment nous pouvons citer [15]:

- **NAGIOS**

Créé en 1999 par Ethan Galstad, Nagios est un logiciel qui permet de superviser un système d'information. Il est considéré comme étant la référence des solutions de supervision open source. Il dispose de nombreuses fonctions telles que l'héritage multiple, les dépendances, l'escalade de notifications, les Template de services et d'hôtes, le support des surveillances actives et passives, etc. L'interface web est la partie graphique, via un serveur

[14] http://pfmh.uvt.rnu.tn/573/1/Mise_en_place_d%E2%80%99un_syst%C3%A8me_de_supervision_Open_source..pdf
[15]

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'activités[3].

❖ **CENTREON**

Anciennement appelé Oreon1, Centreon est un logiciel de supervision des applications, systèmes et réseaux, basé sur les concepts de Nagios. C'est une solution complète destinée aux administrateurs et exploitants du service de supervision. Il apporte de nombreuses fonctions telles que la consultation de l'état des services et des machines supervisées, la métrologie, le reporting, l'accès aux événements de supervision, la gestion avancée des utilisateurs via des listes de contrôle d'accès (ACL), etc. Il s'appuie sur les technologies Apache et PHP pour l'interface web, MySQL pour le stockage des données de configuration et de supervision.

❖ **ZABBIX**

Zabbix est un logiciel libre qui permet de surveiller l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources. Le « serveur ZABBIX » peut être décomposé en trois 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. Il repose sur du C/C++, PHP pour la partie front end et MySQL/PostgreSQL/Oracle pour la partie BDD.

❖ **ZENOSS**

Tout comme Nagios, Zenoss est un outil qui se base sur une application Web qui va surveiller les nœuds de votre réseau et générer des rapports importants pour des décideurs informatiques. Publié sous la licence GNU General Public License (GPL) version 2, Zenoss fournit une interface Web qui permet aux administrateurs système de la surveillance de la disponibilité, de l'inventaire, de la configuration, des performances et des événements

❖ **.GANGLIA**

Ganglia est beaucoup plus spécifique, c'est réellement un outil de supervision complémentaire destiné à la supervision d'un système en cluster. Il est basé sur une

conception hiérarchique ciblée à des fédérations de grappes. Il exploite des technologies largement utilisées telles que XML pour la représentation des données, XDR pour compact, le transport de données portable et RRDtool pour le stockage des données et la visualisation. Il utilise des structures de données et d'algorithmes soigneusement conçues pour atteindre de très faibles frais généraux par nœud et haute concurrence.

- **CACTI**

Cacti est un logiciel libre de mesure de performances réseau et serveur basé RRDTool dédié à la métrologie. Il ne fait pas de supervision en tant que tel. Il ne fait pas de corrélation d'incidents ni d'alertes en cas d'incident (bien que des plugins existent, ce n'est pas son but premier. Les possibilités de configuration très avancées font que celui-ci est souvent utilisé en complément de solutions de supervision tel que Nagios, notamment, pour assurer la partie métrologie lorsque les exigences sont fortes. Il permet de représenter sous forme de graphiques n'importe quelle donnée quantifiable collectée soit par le biais de protocoles réseaux tels que SNMP ou soit par des scripts personnalisés par l'utilisateur.

- **MUNIN**

Munin est un outil de surveillance système et réseau open source qui s'appuie sur l'outil RRDTool. Il présente ses résultats sous forme de graphiques disponibles via une interface web. Il possède une structure de plugins particulièrement simple qui permet d'enrichir rapidement l'outil. Des plugins sont actuellement disponibles pour les systèmes d'exploitations suivants: GNU/Linux, FreeBSD, NetBSD, Solaris et AIX. L'architecture du système Munin est constituée d'un serveur principal appelé Munin-master, récupérant les informations à intervalle régulier et de plusieurs nœuds appelés Munin-node. Le nœud doit être installé sur le(s) serveur(s) à surveiller.

- **Avantage de ces outils**

L'avantage[16] de ces logiciels libres est la gratuité, la disponibilité du code source et la liberté d'étudier et de modifier le code selon nos besoins et de le diffuser. De plus, il existe une communauté importante d'utilisateurs et de développeurs qui participent à l'amélioration des logiciels et apportent une assistance par la mise en ligne des documentations et les participations aux forums.

4.3 Choix du logiciel

Les différentes solutions commerciales déjà présentées (HPOpenview, Patrol, BigBrother, etc..) nécessitent un investissement important pour leur mise en place, et pour des raisons propres à l'entreprise, toutes ces solutions sont à écarter de mon liste de choix.

Parmi les solutions les plus connues, recommandées et surtout Libres, on citera Nagios et Zabbix. Voici un tableau[17] comparatif des deux logiciels choisis.

	Zabbix	**Nagios**
Présentation	-Open source, libre -Multiplateformes -Homogène. -Moteur en C, interface web utilisateur en PHP, base de données SQL (MySQL, Oracle…) -Configuration centralisée sur une même interface graphique. ➔Peut monitorer de 3 manières : -LANCEMENT d"un processus sur les machines à monitorer pour collecter des données locales, grâce à l"agent	-Open source, Libre. -Conçu pour les plateformes Unix. -Modulaire. -Moteur en C, perl, sharp…, interface web en PHP, base de données SQL. -Configuration plus ou moins complexe ➔Peut monitorer de 3 manières : -L"utilisation des journaux d"exploitation par l"envoie des évènements issus des fichiers log en temps réel vers un serveur centrale

[16] http://pfmh.uvt.rnu.tn/573/1/Mise_en_place_d%E2%80%99un_syst%C3%A8me_de_supervision_Open_source..pdf

[17]

	Zabbix (obtenir des infos sans utiliser SNMP). -Requêtes SNMP. -Check externes qui sert à tester les services réseaux (rien à installer sur l'équipement surveillé, tests limités à des pings ou test de protocoles).	offrant les informations nécessaires à la supervision. -Supervision active des services et infrastructure qui nous permet de garder l'historique des performances.
Fonctionnalités	-Offre une interface web de consultation et d'administration. -Peut générer des graphes. -Peut lever des alertes en envoyant des mails. -Supervise des équipements SNMP. -Gère les pannes et les performances	-Offre une interface web basée sur les CGL avec gestion des droits pour la consultation. -Génère des rapports de surveillance. -Il a la possibilité de monitorer à distance à travers un firewall. -Il peut définir des serveurs esclaves qui prennent le relais si le serveur maitre tombe en panne. -Surveillance des ressources des serveurs (CPU, mémoire…) -Surveillance des services réseaux. -Arrêt temporaire de la supervision locale ou globale. -Génère des graphes par l'interfaçage avec RRDTools.
Architecture	Architecture généralement basée sur : -Serveur Zabbix, le coeur et moteur de l'application programmé en C. -Agent Zabbix pour la collection des informations locales.	Architecture généralement basée sur : -Le moteur de l'application qui sert à ordonnancer les tâches de supervision écrit en C. -Une interface web réalisée à l'aide des

	-Une interface web d‟administration et consultation des données. -Une base de données SQL.	GCI, décrivant la vue d‟ensemble su système et les anomalies possibles. -Plusieurs plugins qui peuvent être complétés en fonction des besoins.
Avantages	-Multiplateforme. -Utilise peu de ressources -Plus léger grâce à son homogénéité (Pas de plug-in à ajouter). -Mise à jour facile. -Configuration et utilisation aisée. -Interface vaste mais claire	-Des plugins qui étendent les possibilités de Nagios. -Une très grande communauté qui participe activement au développement. -Un moteur performant -solution complète permettant le reporting, la gestion des pannes et d‟alarmes, gestion des utilisateurs… -Des plugins permettent aux utilisateurs de développer facilement ses propres vérifications de services. -Possibilité de repartir la supervision entre plusieurs administrateurs. -Offre la possibilité de développer ses propres modules.
Inconvénients	-L‟agent Zabbix communique les données en claire➔ nécessité de sécuriser les données. -Peu d‟interfaçage avec d‟autres solutions commerciales. -Communauté de développeurs limitée.	-Configuration complexe mais peut s‟améliorer en ajoutant Centreon. -Interface peu ergonomique et intuitive.

Tableau 01 : Tableau comparatif

Parmi ces solutions libres, les deux logiciels Zabbix et Nagios sont les plus répandus et les plus utilisés. Par rapport à mon projet, se sont les deux solutions les plus adaptées permettant

de satisfaire pratiquement tous les besoins de la société, par les différentes fonctionnalités qu'elles offrent. Et compte tenu de ce critère Zabbix et Nagios restent à égalité et il me sera impossible de les départager.

Une des particularités captivantes de Nagios est sa modularité, on a ainsi estimé que Nagios a été plus adapté aux besoins de mon projet que Zabbix. En effet, grâce à ses plugins, Nagios possède une architecture facilement adaptable à l'environnement. Ces derniers pouvant être ajoutés, modifiés ou même personnalisés et permettent de spécifier les tâches pour aboutir au résultat voulu.

De plus Nagios est une solution stable, dispose d'une grande communauté de développeurs et est utilisé aussi bien dans les petites et moyennes infrastructures que dans les grands parcs informatiques et utilisé surtout par plusieurs entreprises de renommé, tels que Yahoo (100 000 serveurs), Yellow pipe Web Hosting (7000 serveurs) …

Bien que ce dernier soit réputé par sa configuration fastidieuse, il peut être couplé à Centreon un logiciel qui lui servira de couche applicative afin de faciliter la configuration et d'établir des interfaces IHM plus ergonomiques et compréhensibles.et pour cella notre choix s'est porté sur NAGIOS.

5. Conclusion

Ce chapitre a été conçu pour familiariser l'environnement du travail en présentant l'entreprise d'accueil et l'architecture réseau dont elle dispose.

Les problèmes que rencontre la société se sont imposés suite à l'étude de l'existant et à sa critique, ce qui nous a permis de cerner la problématique de notre projet. Nous allons par la suite proposé des solutions et leur étude a notre encadreur de stage et finalement nous avons posé notre choix sur la solution que nous jugeons la plus convenable à la société et à la formation que nous estimons acquérir qui est le logiciel de supervision libre « Nagios ». Le chapitre suivant attaquera une étude approfondie de la solution choisie.

1. Introduction

Dans ce dernier chapitre, nous commençons par analyser de prés les fonctionnalités de la solution adoptée, son architecture, et les différents services qu'elle offre et enfin énumérer les différents fichiers de configurations sur quoi se base cette solution.

2. Nagios

2.1 Présentation de nagios

Nagios est un logiciel libre distribué sous licence GPL qui permet de superviser un système d'information complet. Utilisé par de nombreuses sociétés, il fait l'objet de contribution et recherche très actives.

Etant le successeur de NetSaint dont la première version date de 1999, ce logiciel est considéré comme une évolution de ce dernier auquel a été ajoutée, entre autre, la gestion du protocole SNMP. Il apparaît sous le nom de Nagios le 10 mai 2002 aux conditions de la GNU General Public License.

Cet outil repose sur une plate-forme de supervision, fonctionnant sous Linux et sous la plupart des systèmes Unix. Il centralise les informations récoltées périodiquement par le fonctionnement modulaire dont il est caractérisé, ce qui le rend beaucoup plus attractif que ses produits concurrents. En revanche sa configuration peut se révéler complexe.[4].

2.2 Avantage de nagios

Les avantages de Nagios sont [14] :

- Surveillance des services réseaux (SMTP, POP3, HTTP, NNTP, PING, etc.).
- Surveillance des ressources des hôtes (charge processeur, utilisation des disques, etc.).
- Système simple de plugins permettant aux utilisateurs de développer facilement leurs propres vérifications de services.
- Notifications des contacts quand un hôte ou un service a un problème et est résolu (via email, pager, ou par méthode définie par l'utilisateur)
- Possibilité de définir des gestionnaires d'évènements qui s'exécutent pour des évènements sur des hôtes ou des services, pour une résolution des problèmes
- Interface web, pour voir l'état actuel du réseau, notification et historique des

problèmes, fichiers log, etc. (voir la figure 6)

- Plugins existant pour utiliser MRTG ou RRDTool

2.3 Configuration de nagios

La configuration est assez complexe et nous allons donc détailler les principaux points à connaître pour la compréhension du bon fonctionnement de Nagios [13] .

- Définition des Hôtes :

Un hôte pour Nagios représente un serveur "physique", une station de travail, un périphérique, un équipement, qui se trouve sur le réseau.

- Définition des Services :

La définition d'un service identifie un service tournant sur un hôte. Le terme "service" est très générique. Il peut s'appliquer à un service (tel que POP, SMTP, HTTP, etc.) ou bien tout autre type de mesures associées à l'hôte (temps de réponse à un ping, nombre d'utilisateurs connectés, usage des disques).

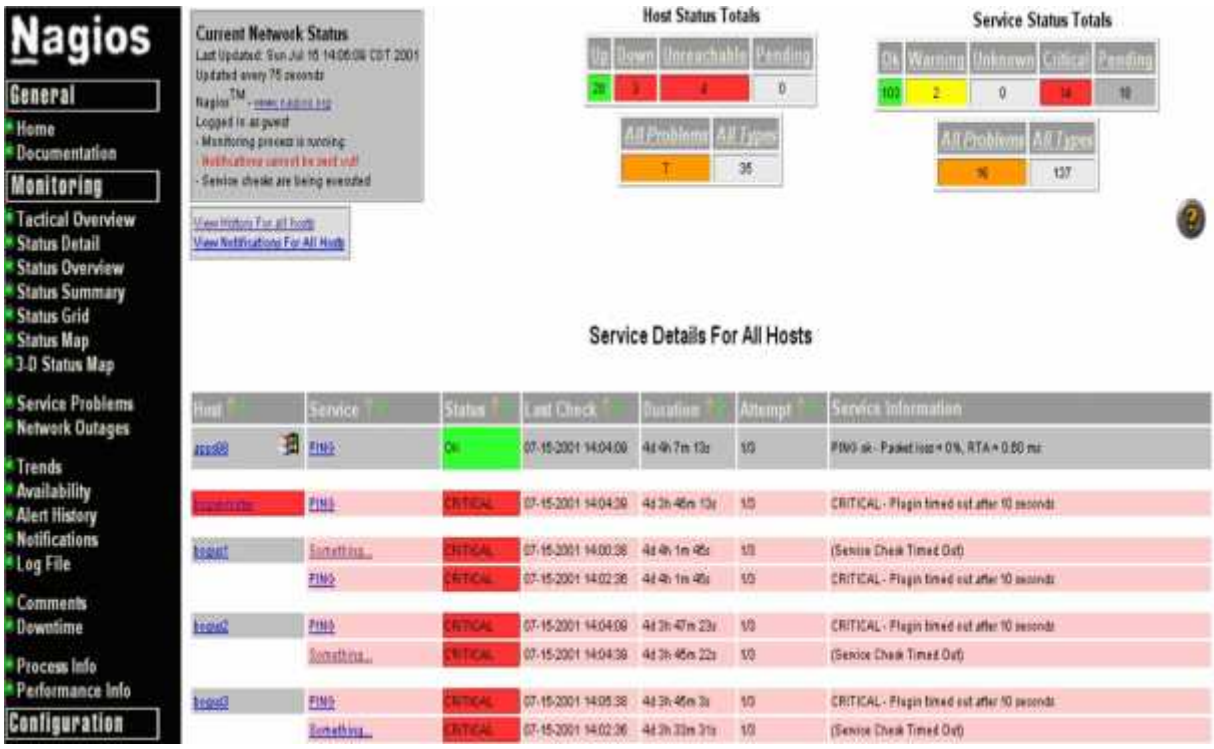


Figure 6: Interface graphique de Nagios [10]

2.4 Fonctionnalité de nagios

Les fonctionnalités de Nagios sont très nombreuses, parmi les plus communes nous pouvons citer les suivantes [10] :

- La supervision des services réseaux (SMTP, http…), des hôtes et des ressources systèmes (CPU, charge mémoire…)
- La détermination à distance et de manière automatique l'état des objets et les ressources nécessaires au bon fonctionnement du système grâce à ses plugins.
- Représentation coloriée des états des services et hôtes définies.
- Génération de rapports.
- Cartographie du réseau.
- Gestion des alertes.
- Surveillance des processus (sous Windows, Unix…).
- Superviser des services réseaux : (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP, etc.)
- La supervision à distance peut utiliser SSH ou un tunnel SSL.
- Les plugins sont écrits dans les langages de programmation les plus adaptés à leur tâche (Bash, C++, Python, Perl, PHP, C#, etc.)

Toutes ces fonctionnalités sont assurées grâce la gestion et supervision du réseau et ses différentes entités d'une manière centralisée. La figure 7 modélise cet aspect :

Figure 7 : Centralisation d'informations par Nagios [10]

2.5 Architecture de nagios

L'architecture de Nagios se base sur le paradigme serveur-agent. D'une manière spécifique, un serveur faisant office de point central de collecte des informations tandis que les autres machines du réseau exécutent un agent chargé de renvoyer les informations au serveur.

L'architecture globale de Nagios peut être décomposée en 3 parties coopératives entre elles [3] :

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

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

- **Des exécutants :** ce sont les plugins dont un grand nombre est fourni de base, responsables de L'exécution des contrôles et tests sur des machines distantes ou locales et du renvoie des résultats au noyau du serveur Nagios13

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

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

Il est possible de coupler Nagios à une base de données MySQL ou Postgres, lorsque le nombre d'objets à superviser devient conséquent. La figure 8 représente l'architecture de Nagios.

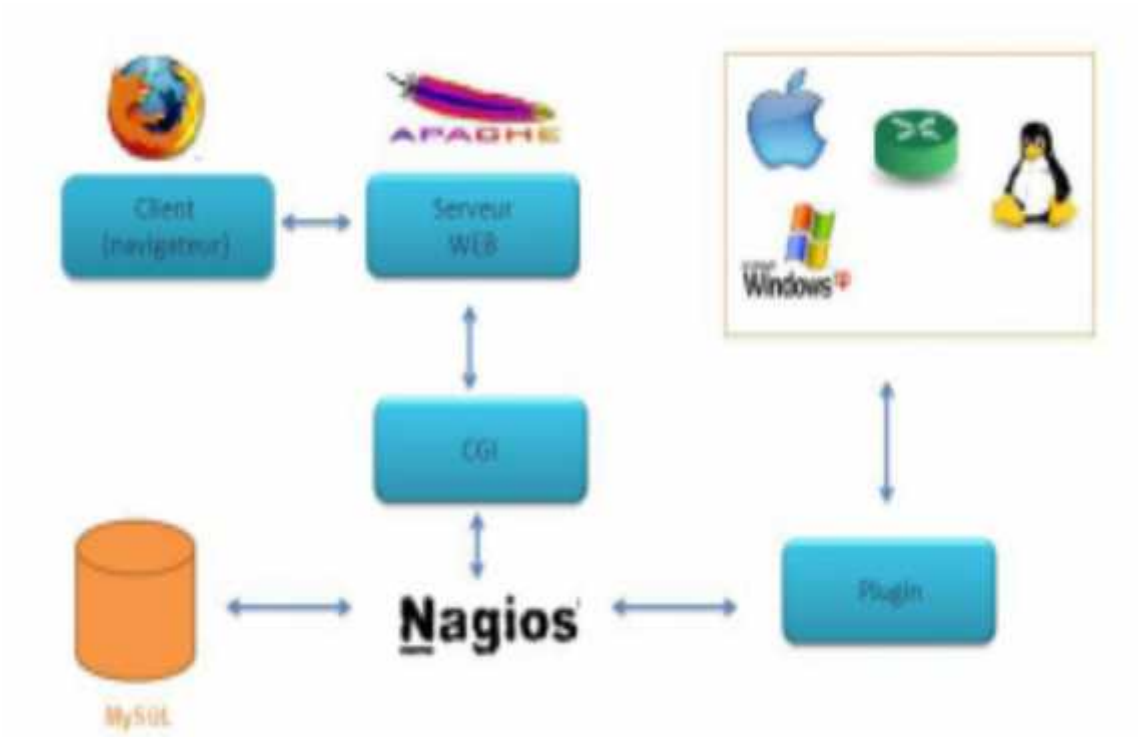


Figure 8 : Architecture de Nagios [10]

2.6 Plugin

Les plugins sont des programmes exécutables ou des scripts (perl, Shell, etc..) qui peuvent être lancés depuis une ligne de commande pour tester un hôte ou un service.

Le résultat de l'exécution d'un plugin est utilisé par Nagios pour déterminer le statut des hôtes ou des services sur le réseau. Le développement des plugins pour Nagios est fait sur Source Forge. La page du projet de développement de plugins pour Nagios (où vous trouverez toujours la dernière version des plugins) se trouve à http://sourceforge.net/projects/nagiosplug/ [10].

Les plugins développés pour Nagios doivent respecter un certain format d'affichage de retour afin de garantir leur intégration. Tous les plugins qui respectent les consignes minimales de développement pour ce projet contiennent une documentation interne. Cette documentation peut être affichée en exécutant le plugin avec le paramètre "**-h**" ("**--help**" si les paramètres longs sont activés)**.**

Par exemple, si nous voulons savoir comment fonctionne le plugin **check_http** (vérification de l'état du serveur web) ou quels paramètres il accepte, vous devez saisir dans la ligne de commande:

#. /**check_httpd --help**

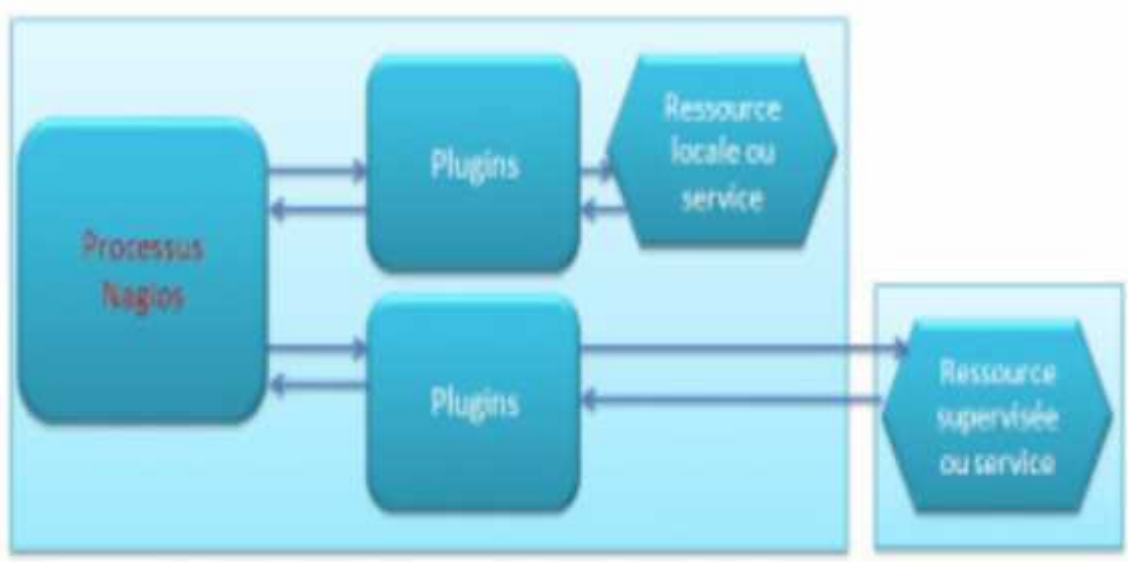


Figure 9 : Principe de fonctionnement des plugins [10]

3. Mise en place de NAGIOS XI

A – Réseau à superviser

Le réseau que nous devons superviser est celui-ci :

Il sera composé :

- D'un serveur "Windows Server 2003" qui permettra la gestion des utilisateurs du réseau : Stockage des données et identifications des utilisateurs
- D'un serveur "Nagios" qui s'occupera de la supervision du réseau, de la centralisation et de l'analyse des informations du réseau
- D'un poste client "Windows XP"
- D'un poste client "Linux"
-D'une imptémente

B – Que superviser?

Avant tout, il faut définir les informations qui seront récupérées par Nagios, sur chaque équipement du réseau.

Sur le serveur "2003 serveur", Nagios récupéra :

- La version du pluging qui envoie les informations au serveur Nagios : Si cette version n'est pas la dernière, un e-mail sera envoyé à l'administrateur réseau.
- La charge CPU du serveur. Dans notre cas, si la charge dépasse les 90 %, un e-mail sera envoyé à l'administrateur réseau.
- La durée depuis le dernier démarrage du serveur.
- La taille et l'occupation des disques durs. Dans notre cas, lorsque 90 % de l'un des disques durs est occupé, un e-mail sera envoyé à l'administrateur réseau.

Sur les postes clients, Nagios récupéra :

- La version du pluging qui envoie les informations au serveur Nagios : Si cette version n'est pas la dernière, un e-mail sera envoyé à l'administrateur réseau.
- La taille et l'occupation des disques durs. Dans notre cas, lorsque 90 % de l'un des disques durs est occupé, un e-mail sera envoyé à l'administrateur réseau.
- Pour Windows XP: La taille du dossier "C:\Documents and Settings" qui stocke les données des utilisateurs en local. Si ce dossier a une taille supérieure à 2Go, un e-mail sera envoyé à l'administrateur réseau pour qu'il puisse vider ce répertoire.

Si Internet n'est plus disponible, un SMS sera envoyé à l'administrateur réseau.

Si le routeur ne répond plus (le réseau ne peut donc plus marcher), envoie d'un SMS à l'administrateur réseau.
Nagios doit avoir un historique des paquets rejetés par le firewall (voir les règles d'autorisations / refus dans le paragraphe précédent)

4. Pré-requis

A – Choix d'une machine virtuelle

Après réflexion, nous avons décidé d'utiliser une machine virtuelle sur laquelle nous avons installé Nagios. Une machine virtuelle permet d'utiliser plusieurs systèmes d'exploitation sur une même machine simultanément.
Les avantages d'utiliser une machines virtuelle sont assez nombreux, et correspondent bien aux besoins de notre projet.
Tout d'abord cela nous permet d'avoir un PC de moins dans notre réseau, ce qui est assez agréable d'utilisation étant donné que nous en avons déjà trois (plus les câbles, le hub, le routeur...).
Etant donné que le pc sur lequel est installé la machine virtuelle est notre pc, cela nous a permis de travailler très facilement en dehors des séances de stage.
Ensuite, il est beaucoup plus aisé de faire des sauvegardes d'une machine virtuelle que d'une machine physique.
Au niveau sécurité, la mobilité de la machine est très intéressante : Si la machine physique tombe en panne, on peut mettre la machine virtuelle très rapidement sur une autre machine physique ; les délais de coupure en cas de panne sont réduits.
Dans une société où les équipements réseaux sont très nombreux, les machines virtuelles peuvent faire gagner de la place dans les locaux.
Il existe plusieurs logiciels permettant de créer des machines virtuelles. Un des plus connus est Vmware. Nous n'avons pas retenu ce logiciel pour éviter que l'utilisation de notre serveur Nagios nécessite une licence Vmware, qui est payante.
Notre choix c'est porté sur VirtualBox, développé par InnoTeck. C'est un logiciel à licence gratuite fonctionnant sur les machines hôtes Windows, Linux et Mac OS X, et qui peut supporter Windows (dont Vista) et Linux comme systèmes invités. De plus, VirtualBox est très simple d'utilisation avec une interface intuitive.(voir la figure dessous)

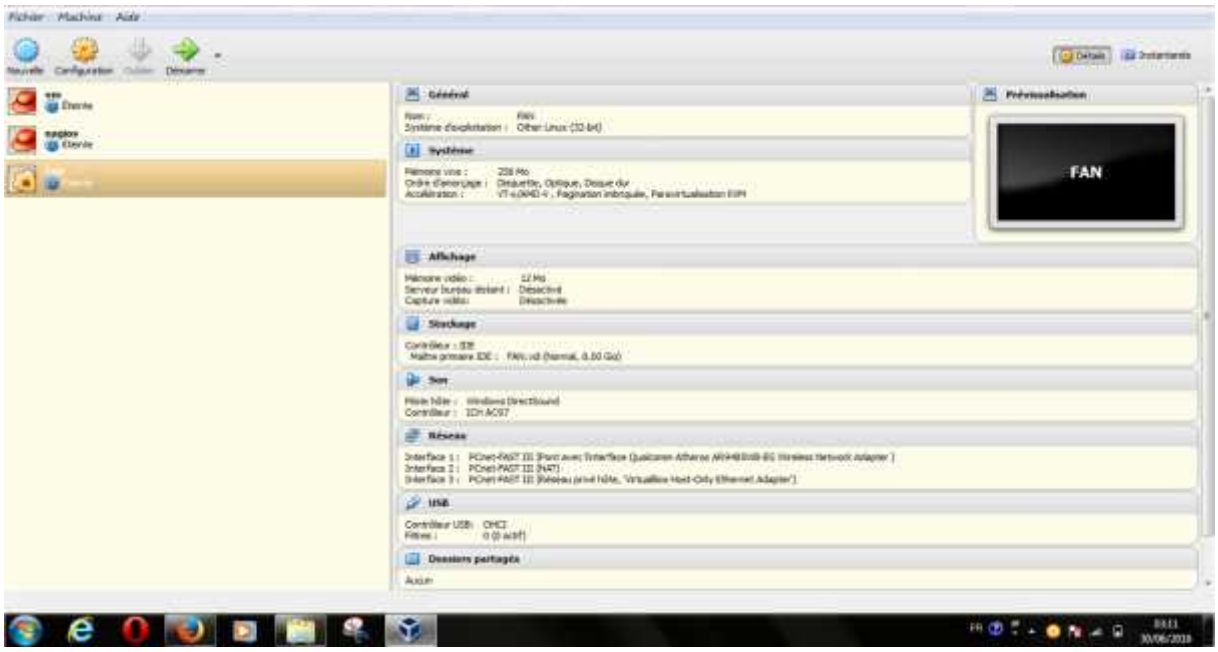


Figure 10 : Interface de VirtualBox

B. Installation de fan

L'installation de FAN est identique à celle d'un CentOS classique. Celle-ci est plutôt rapide, intuitive et ne nécessite pas de commentaire. Une fois terminée elle pèse environ 1Go.

Voici les étapes de l'installation :

Figure11 : Début d'installation

Figure12 : Choix de la langue

Figure13 : Choix du clavier

Figure14 : Choix d'une région

Figure15 : Administrer le système

Figure16 : Formatage du système de fichier

Figure17: L'installation de bash

Figure18: L'installation de Vconfig

Figure19: L'installation de net-snmp-libs

Figure20: L'installation de dokuwiki

Figure21: L'installation de nareto-database

Figure22: l'installation terminée

C. Installation de NSClient et NRPE

- Pour la supervision des serveurs Windows, nous allons installer le greffon NSClient sur la machine distante et vérifier la présence de la commande « check_nt » parmi les plugins installé de Nagios.
- Pour la supervision des serveurs Linux, je vais installer le greffon « NRPE-2.1.12 » sur la machine distante et vérifier la présence de la commande « check_nt » parmi les plugins installé de Nagios [10] .

D. Manipulation

Création des hôtes à superviser

- Récuperation d'adresse du serveur

  Etape :

  - introduire le login et le mot de passe

  - ensuite taper la commande ifconfig(voire la figure ci-dessous).

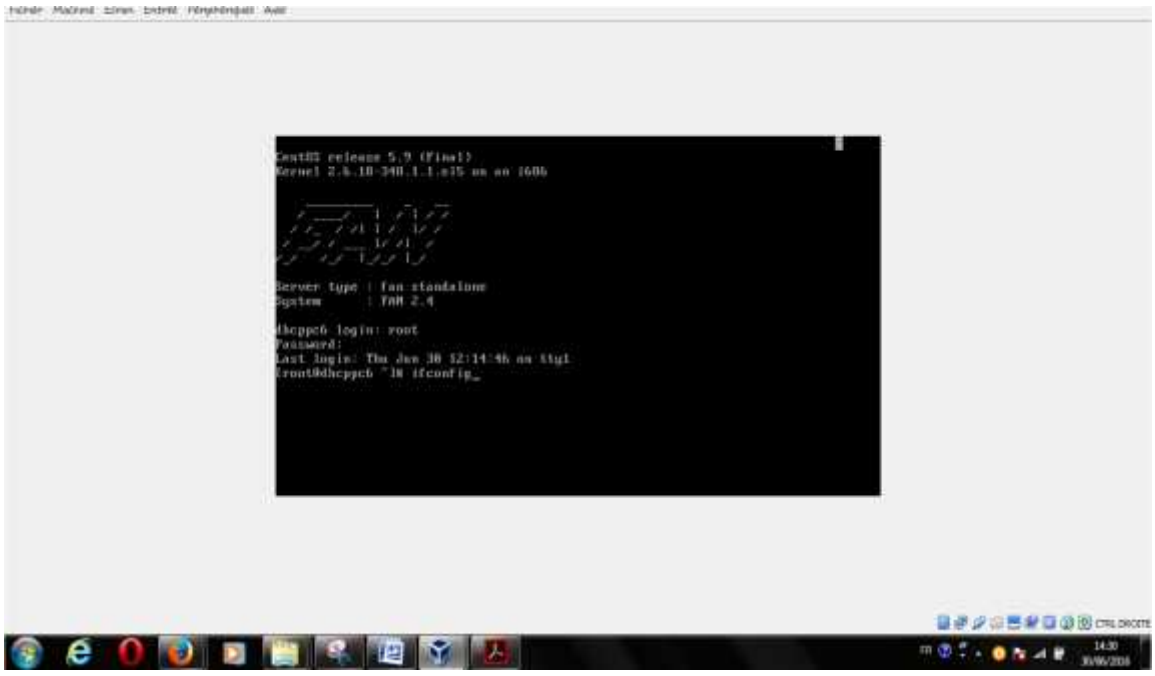


Figure 23 : Interface de récupération d'adresse de serveur

Une fois connect2 au serveur nous aurons la figure suivante :

Figure 24: Interface de FAN

Nous cliquons sur centreon nous aurons la figure qui suit et nous introduisons le login et le mot de passe :

Figure 25 : S'authentifier pour accéder à centreon

Nous aurons cette figure

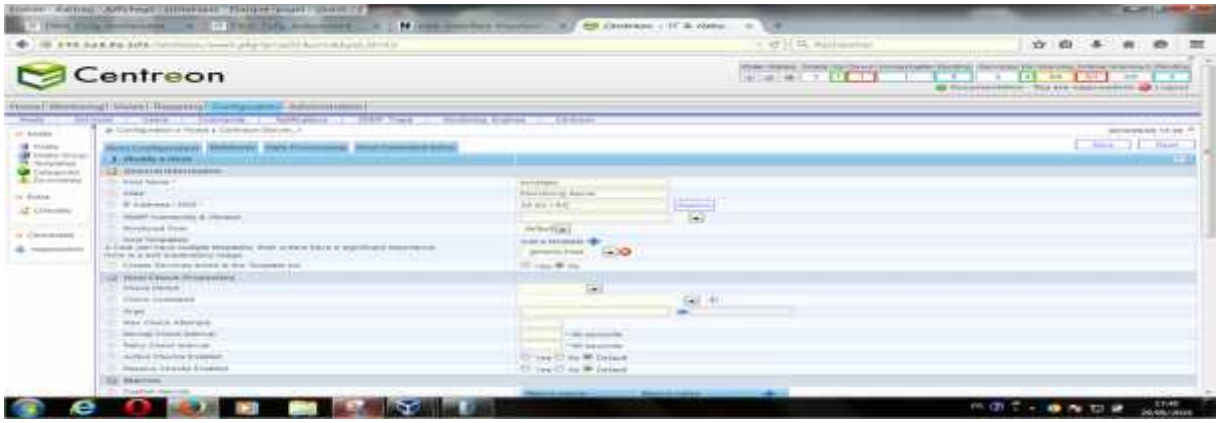
Nous cliquons sur configuration.

Figure 26: Interface de centreon

Puis nous allons sur hosts pour ajouter des hôtes à superviser.

Figure 27: Création d'un hôte

Nous remplissons les champs(nom d'hôte, adresse ip, la période de supervision) puis nous cliquons sur save nous aurons la figure ci après.



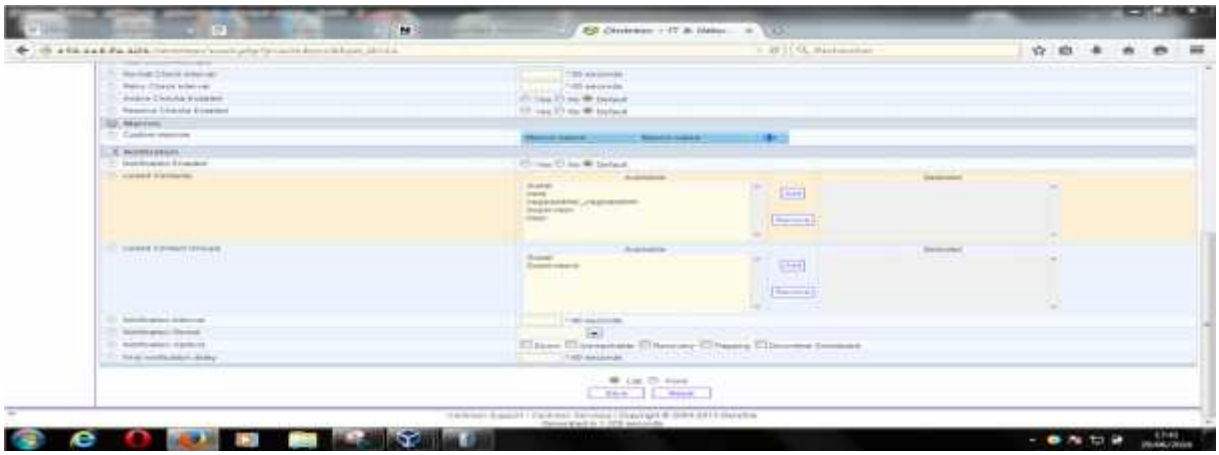


Figure28 : Remplir les champs

Nous cliquant sur monitoring engines puis cocher les champs qui convient puis cliquer sur Export pour exporter l'hôte ajouté sur interface de nagios.

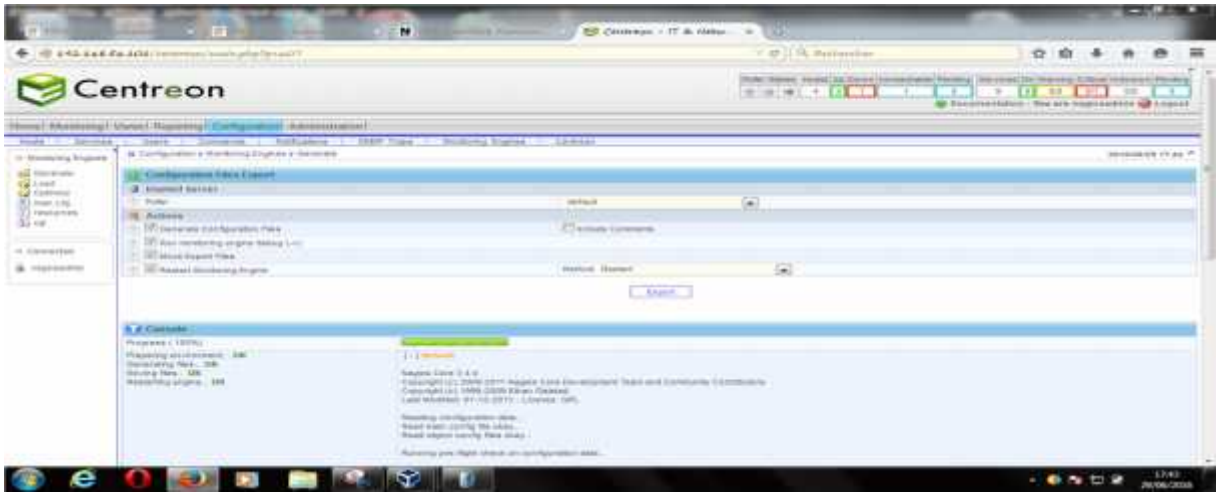


Figure 29: Export de l'hôte sur l'interface NAGIOS

Les hotes supervisés apparaitre sur l'interface nagios

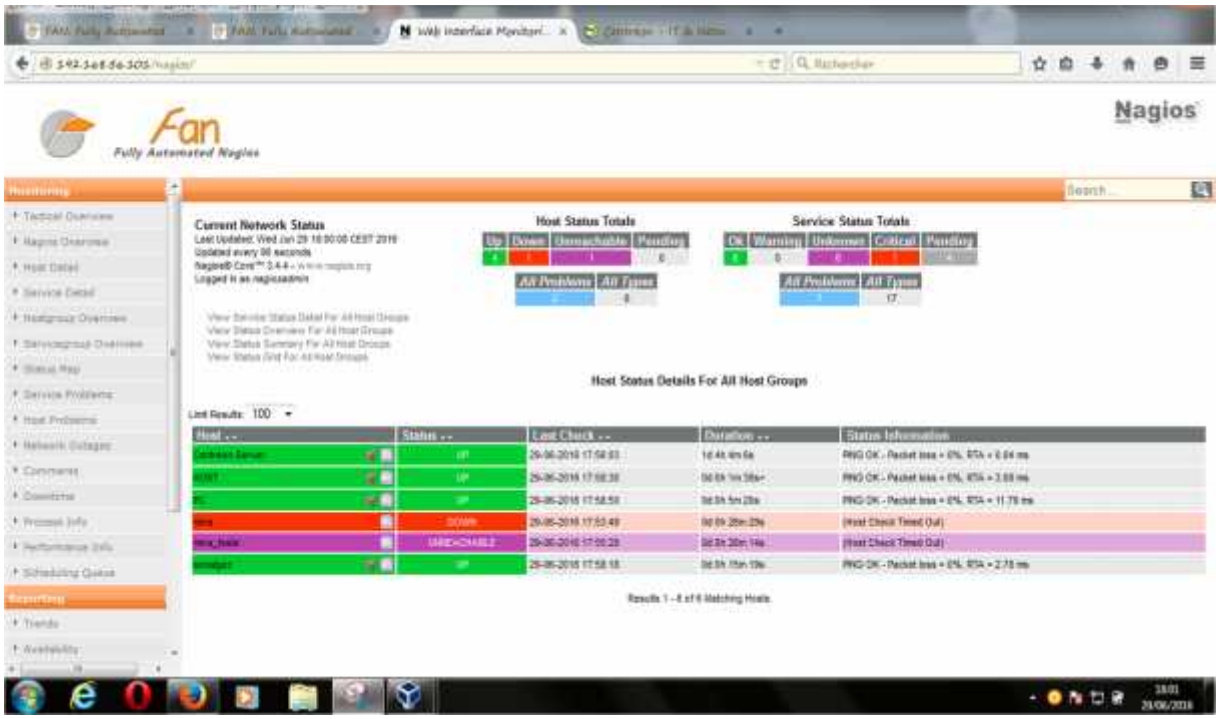


Figure 30: Interface des hôtes supervisées

5. Conclusion

Dans ce chapitre on a décrit l'aspect de notre solution, énuméré ses fonctionnalités et modélisé son architecture.

Ensuite une partie a été consacrée pour la définition des différents fichiers de configuration générés par la solution de supervision Nagios, précédée par l'énumération des différents plugins de base responsable de l'exécution des tests

Conclusion générale

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

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

L'association de Nagios et de Centreon a permis la constitution d'une solution de monitoring à la fois puissante et efficace.

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

Ce stage ma permis d'acquérir maintes connaissances dans le monde de la supervision des réseaux informatiques, et surtout la maitrise de l'environnement Unix.

Références bibliographiques et webografiques

Webographie

[1] http://blog.adminrezo.fr/wp-content/uploads/2013/05/supervision-des-reseaux-v1.pdf. AVRIL 2016

[2] https://fr.wikipedia.org/wiki/Supervision. AVRIL 2016

[3] M.GBEGBE Raymond :www.junet.ci/telechargement/**memoire**_Abbe.**pdf** . AVRIL 2016

[4]YVES Gallen : http://psnmp.sourceforge.net/rapport-enseirb2002/rapport.pdf. AVRIL2016

[5] http://www.monitoring-fr.org/supervision/standards/. MAI 2016

[6] http://www.commentcamarche.net/contents/537-le-protocole-snmp. MARS 2016

[7] https://fr.wikipedia.org/wiki/Internet_Control_Message_Protocol . AVRIL 2016

[8] http://www.o00o.org/monitoring/outils.html. MARS 2016

[9] https://fr.wikipedia.org/wiki/Sonelgaz. MAI 2016

[10]OTHMAN ,Souli :http://pfmh.uvt.rnu.tn/573/1/Mise_en_place_d%E2%80%99un_syst%C3%A8me_de_supervision_Open_source..pdf . AVRIL 2016

[11]REYNIER Serge :http://snakejulien69.free.fr/Etudes/BTS%20IG%20-%20ARLE/Projet%20-%20cacti%20-/Doc/supervision.pdf MARS 2016

Bibliographie

[12] Loic FONTAINE & Bruno LEGROS ,2012 Centreon –Maitrisez la supervision de votre système d'information. Edition ENI .

[13] Olivier JAN ,2008.NAGIOS et la supervision Open Source –De l'installation à l'optimisation. Edition EPSILON .

[14] Andrea DALLE Vacche & Stefano Kewan LEE ,2013.Mastering Zabbix.Packet Publishing Ltd.

Résumé

Les réseaux sont de partout à l'heure actuelle. Ils sont devenus indispensables au bon fonctionnement général de nombreuses entreprises et administrations. Tout problème ou panne peut avoir de lourdes conséquences aussi bien financières qu'organisationnelles. La supervision des réseaux est alors nécessaire et indispensable. Elle permet entre autre d'avoir une vue globale du fonctionnement et problèmes pouvant survenir sur un réseau mais aussi d'avoir des indicateurs sur la performance de son architecture. De nombreux logiciels qu'ils soient libres ou propriétaires existent sur le marché. La plupart s'appuie sur le protocole SNMP.

Dans une première partie nous allons faire une présentation de la supervision et tout ce qui touche au monitoring de réseau. Dans une seconde partie, nous verrons le fonctionnement du protocole le plus utilisé actuellement : le protocole SNMP. Ensuite nous ferons une présentation des différents logiciels existants à l'heure actuelle. Enfin nous essaierons d'avoir une vision sur l'avenir de la supervision.

Mots clés : Supervision réseau, Surveillance,Monitoring,SNMP.

Abstract

Networks are everywhere today. They have become essential to the overall functioning of many companies and administrations. Any problem or failure can have serious consequences both financial and organizational. The network supervision is necessary and indispensable. It allows among others to have an overall view of the functioning and problems that can occur on a network but also to have indicators on the performance of its architecture. Many software whether free or owners are on the market. Most uses SNMP.

In the first part we will make a presentation of the supervision and everything related to network monitoring. In the second part we will see the operation of the protocol as used currently: SNMP. Then we will make a presentation of the different existing software at present. Finally we will try to have a vision on the future of supervision.

Key Words: Network supervision,Monitoring,SNMP.