

Sujet :

Mise en place d'un système de supervision Open source.

RAPPORT DE STAGE

(période du 24/11/2014 au 19/12/2014)

Elaboré par :

Ludovic LE BLOND

Encadré par :

Mr MAUBIAN Stéphane

Société d'accueil:

ALCATEL-LUCENT GUIPAVAS

Table des matières

Cahier des charges

Titre du projet :

Mise en place d'un système de supervision Open source.

Travail demandé:

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

Plan du travail :

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

-Coûts financiers les plus réduits possibles.

-Récupération des informations permettant la détection des pannes, l'indisponibilité des serveurs et de leurs services.

-Des renseignements supplémentaires de monitoring sur la charge CPU, Espace disque, mémoire disponible, input/output, etc....

-Gestion des alertes.

-Notification par mail ou SMS en cas de problème.

-Générer des rapports sur le fonctionnement des serveurs par mois.

-Générer des graphes (cartographie du réseau,...)

-Une interface graphique claire pour l'interaction utilisateur/Logiciel.

Introduction générale

Actuellement toutes les 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 maîtrise devient primordiale. Ils doivent fonctionner pleinement et en permanence pour garantir la fiabilité et l'efficacité exigées, 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 informés 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.

1. 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.

3.1 Les offres éditeurs

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**.

3.2 Les offres libres

Il existe des solutions de supervision libres et professionnelles. Parmi les plus répandues, reconnues du moment nous pouvons citer Nagios, Zabbix, BigBrother2 et OpenNMS.

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.

3.3 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 ma 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.

	Zabbix	Nagios
Présentation	<p>Open source, libre</p> <ul style="list-style-type: none"> -Multiplateformes -Homogène -Interface web utilisateur en PHP, base de données SQL (MySQL, Oracle...) -Configuration centralisée sur une même interface graphique.) <p>Peut monitorer de 3 manières:</p> <ul style="list-style-type: none"> -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). 	<ul style="list-style-type: none"> -Open source, Libre. -Conçu pour les plateformes Unix. -Modulaire -Interface web en PHP, base de données SQL. -Configuration plus ou moins complexe <p>Peut monitorer de 3manières:</p> <ul style="list-style-type: none"> -L'utilisation des journaux d'exploitation par l'envoi des évènements issus des fichiers log en temps réel vers un serveur centrale offrant les informations nécessaires à la supervision. -Supervision active des services et infrastructure qui nous permet de garder l'historique des performances
Fonctionnalités	<ul style="list-style-type: none"> -Offre une interface web de consultation et d'administration. 	<ul style="list-style-type: none"> -Offre une interface web basée sur les CGL avec gestion des droits pour la consultation.
Fonctionnalités	<ul style="list-style-type: none"> -Peut générer des graphes. -Peut lever des alertes en envoyant des mails. -Supervise des équipements SNMP. -Gère les pannes et les performances 	<ul style="list-style-type: none"> -Génère des rapports de surveillance. -Il a la possibilité demonitorer 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...)

		<ul style="list-style-type: none"> -Surveillance des services réseaux. -Arrêt temporaire de la supervision locale ou globale. -Génère des graphes par l'interfaçage avec RRDTools.
Architecture	<p>Architecture généralement basée sur:</p> <ul style="list-style-type: none"> -Serveur Zabbix, le cœur et moteur de l'application programmé en C. -Agent Zabbix pour la collection des informations locales. -Une interface web d'administration et consultation des données. -Une base de données SQL. 	<p>Architecture généralement basée sur:</p> <ul style="list-style-type: none"> -Le moteur de l'application qui sert à ordonnancer les tâches de supervision écrit en C. -Une interface web réalisée à l'aide des GCI, décrivant la vue d'ensemble du système et les anomalies possibles. -Plusieurs plugins qui peuvent être complétés en fonction des besoins.
Avantages	<ul style="list-style-type: none"> -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. 	<ul style="list-style-type: none"> -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 répartir la supervision entre plusieurs administrateurs. -Offre la possibilité de développer ses propres modules.
Inconvénients	<ul style="list-style-type: none"> -L'agent Zabbix communique 	<ul style="list-style-type: none"> -Configuration complexe mais

les données en claire nécessité de sécuriser les données. -Peu d'interfaçage avec d'autres solutions commerciales. -Communauté de développeurs limitée.	peut s'améliorer en ajoutant Centreon. -Interface peu ergonomique et intuitive.
---	--

Tableau 2. 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 plus ergonomiques et compréhensibles.

4. 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.

J'ai proposé des solutions et leurs études à mon maître 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.

Chapitre II: Présentation de l'outil de supervision Nagios

Dans ce présent chapitre, Je commence par définir la notion de la supervision et ses objectifs ensuite, analyser de près les fonctionnalités de la solution proposée, son architecture, et les différents services qu'elle offre et finir par énumérer les différents fichiers de configurations sur quoi se base cette solution.

1. La supervision

1,1 Définition

La supervision de réseaux peut être définie comme l'utilisation de ressources réseaux adaptées dans le but d'obtenir des informations (en temps réel ou non) sur l'utilisation ou la condition des réseaux et de leurs éléments

afin d'assurer un niveau de service garanti, une bonne qualité et une répartition optimale et de ceux-ci.

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

1.2 Objectifs

L'objectif d'une supervision de réseaux peut ainsi se résumer en trois points :

.Etre réactif en alertant l'administrateur (e-mail ou sms) en cas de dysfonctionnement d'une partie du système d'information.

.Etre pro actif en anticipant les pannes possibles.

.Cibler le problème dès son apparition afin d'agir rapidement de la façon la plus pertinente possible.

2.Nagios

2.1 Présentation

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.

2.2 Fonctionnalités

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

- .La supervision des services réseaux (SMTP, http...), des hôtes et des ressources systèmes (CPU, charge mémoire...)
- .La détermination à distance et de manière automatique l'état des objets et les ressources nécessaires au bon fonctionnement du système grâce à ses plugins.
- .Représentation colorisée 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.)