Nagios, un outil GPL de surveillance pour petits et grands réseaux hétérogènes

Pierre-Antoine Angelini
IFSIC, Campus de Beaulieu, Université de Rennes 1, Avenue du Général Leclerc, 35042 Rennes Cedex
Pierre-Antoine.Angelini@ifsic.univ-rennes1.fr Date : 26 Septembre 2003

Résumé

De nos jours, le moindre réseau comprend au moins une dizaine de services, externalisés ou non, et souvent cruciaux. La facilité de mise en oeuvre de serveurs et de services, aussi bien dans le monde Unix que Windows, le coût toujours décroissant des matériels, incitent à la mise en œuvre d'architecture réseau s'appuyant sur de nombreux petits serveurs dédiés. La réutilisation, dans ce contexte, de matériels un peu dépassés, mais adaptés à des tâches légères, participe à ce mouvement. Mais surveiller tous ces serveurs et services demande un outil adapté. D'autre part, le rôle central de l'outil informatique, dans toutes les composantes de nos institutions, exige des administrateurs qu'ils soient en mesure d'informer très rapidement leurs utilisateurs d'une anomalie. Ce document explique en quoi et comment Nagios[1] est susceptible de les aider dans cette tâche, tout en constituant une solution techniquement et financièrement viable.

Mots clefs

Surveillance, réseaux hétérogènes, sécurité, cryptage, help-desk.

1 Etat du marché des moniteurs de réseau et services

Pour qui souhaite surveiller l'activité de serveurs, services, matériels sur un réseau hétérogène, le choix est très rapidement restreint : soit des solutions très basiques, soit des logiciels propriétaires, souvent basés sur SNMP et/ou le déploiement de clients spécifiques. Les serveurs sont implémentés sur tous types de systèmes d'exploitation (avec une certaine domination du monde Windows).
Beaucoup, parmi ceux-ci, sont dotés de fonctionnalités limitées en ce qui concerne le test précis d'un service (test de la réponse à une requête spécifique SQL ou HTTP, par exemple). SNMP sait parfois remonter des informations dans ce domaine, mais au prix d'un développement souvent ardu.

2 Nagios

Parmi tous ces outils, Nagios [1], développé par Ethan Galstad, se détache du lot en raison de : salicence GPL (coût nul), son ouverture, sa relative pérennité depuis 1999 (la plupart des produits similaires ont des difficultés à survivre). De plus, une ergonomie agréable (via une interface graphique bien pensée) et une documentation en français en facilitent l'usage.
Mise en garde : Nagios n'est pas un outil d'inventaire logiciel et/ou matériel, et n'est pas, nativement, destiné à traiter des données SNMP, même s'il sait le faire, via des modules complémentaires.

3 Domaine d'application

Nagios est destiné à toute personne ayant la responsabilité d'un environnement informatique, notamment quand l'indisponibilité d'un service a de fortes répercutions sur la qualité du service apporté (e-mail, accès Internet, serveur de SGBD, serveur web, matériels réseaux, etc) et sur l'humeur de leurs utilisateurs ☺. Il n'a pas vocation à remplacer un outil de surveillance existant et satisfaisant, mais plutôt alors à le complèter . C'est un outil simple d'emploi, accessible depuis un navigateur, qui permet de délivrer une information de qualité sur l'état du réseau à des utilisateurs sans privilèges. Dans le cas de l'IFSIC, les étudiants peuvent vérifier si un service est effectivement indisponible, sans compétences techniques particulières et sans avoir recours aux administrateurs.

La surveillance d'un ensemble de machines pourra s'effectuer avec des niveaux très divers, suivant les besoins et compétences :

- **simple** : ping sur les machines surveillées et remontée d'alerte en cas d'absence de réponse dans un délai défini, via une page web
- **élaboré** : rajout du test de services (serveurs web, serveur de SGBD, serveur DNS, etc), avec remontée des résultats obtenus via email ou pager. C'est actuellement le statut du serveur Nagios de l'IFSIC.
- **sophistiqué** : rajout de fonctions d'administration plus complexes (rétroaction de Nagios vis à vis d'une défaillance : relance automatique d'un service « tombé », escalade des alertes en cas d'absence de réaction des responsables dans un temps donné). C'est le statut du serveur en cours de montage.

[1] Anciennement Netsaint.

- **complexe** : serveurs redondants, cryptage des communications entre serveurs et clients, surveillance de milliers de machines/services.

4 Installation et pré-requis matériel

Serveur : L'installation requiert un serveur Unix, de préférence Linux, puisque c'est la plateforme de développement de Nagios. Les dernières distributions (RedHat, Mandrake) s'installent facilement. La documentation décrit l'installation de Nagios pas à pas et le site de Nagios comporte une base de FAQ très riche. Un novice doit ainsi pouvoir monter un serveur doté de fonctions de base. L'un des attraits de Nagios réside dans la possibilité de réutiliser des matériels anciens. Un PII 233 mhz, doté de 256 mo de mémoire, fera un serveur tout à fait honorable, pour le test d'une cinquantaine de machines et de services. Le serveur de l'IFSIC (PIII 1.3 GHZ, 512MO) teste plus de 200 services et machines.

Clients (Windows et Unix): Outre les tests de type « ping », ne nécessitant aucune modification du client, un greffon[2] est associé à chaque type de test (check_disk, check_proc, etc). Certains sont quasi-universels (Netsaint_statd[3]). Leur installation sur chaque machine est fonction des tests choisis. Les tests peuvent être activés depuis le serveur (contrôles actifs) via «NRPE[4]» ou envoyés depuis le client (contrôles passifs[5]), via NSCA[6]. Le déploiement de ces greffons sur les clients n'est pas prévu dans Nagios et est laissé à l'initiative de l'installateur.

5 Administration

Nagios connaît trois types d'objets : les hôtes, les services installés sur les hôtes, les utilisateurs. Aux deux premiers, il appliquera des fonctions définies par les fichiers de configuration, parmi lesquelles : type de surveillance, périodicité, action en cas d'anomalie, etc. Il est à noter que la configuration de Nagios repose sur une syntaxe objet qui facilite l'écriture des fichiers de configuration pour les gros parcs. Il sait s'interfacer avec des produits très connus, tel MRTG [2], pour suivre le débit de liens surveillés ou WEBMIN [3], pour simplifier son administration. Un outil additionnel, nmap2nagios, fabrique les fichiers de configuration de Nagios. Il s'appuie sur les fichiers XML issus d'une exploration du réseau avec Nmap [4].

Les utilisateurs (lambda ou administrateurs) ont accès aux résultats, en fonction de leurs privilèges, via l'interface Web. Entre autres :

- Tactical view : vue synthétique de l'ensemble des résultats, qui, d'un coup d'œil, met en évidence un problème
- Services/Host/Network : vue synthétique de l'ensemble des services, hôtes ou matériels réseau
- Status Map : représentation en 2D du réseau.
- Status overview screen : représentation des groupes (de services, d'hôtes) définis par l'administrateur, avec le statut individuel de chaque objet

Toutes les fonctions d'administration (acquittement d'une alerte, suppression d'une alarme, consultation des logs, etc) à l'exception de la modification de la configuration, sont accessibles, en standard, à travers l'interface Web. L'intégration de Nagios dans WEBMIN permet l'administration des configurations via un navigateur.
Des fonctions de mise en page permettent d'obtenir des graphes divers : disponibilité d'un hôte/service sur une période de temps donnée, état du serveur Nagios, etc . Les « accros de la connexion » pourront installer une interface WAP ☺.

6 Conclusion

Nagios est un produit qui sait s'adapter à vos besoins, moyennant un investissement raisonnable (temps, budget). Vous êtes interessés ? Le site de Nagios comporte une section « démo » qui permet de le découvrir sans recourir à une installation.

Références

[1] NAGIOS : http://www.nagios.org
[2] MRTG : http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
[3] WEBMIN: http://www.webmin.com
[4] NMAP : http://www.nmap.org

[2] Les greffons (plugins) font partie d'un paquetage disponible via le site de Nagios, mais indépendant de celui-ci. Leur traduction en français est en cours.
[3] Netsaint-statd fait partie des modules complémentaires (Addons) .Ecrit en perl, il sait exécuter et récupèrer le résultat de toutes fonctions systèmes.
[4] NRPE (Nagios Remote Plugin Executor) permet l'exécution d'un greffon installé localement sur un hôte distant, via un canal crypté.
[5] notamment pour passer les firewall et routeurs
[6] NSCA (Nagios Service Check Acceptor) permet d'envoyer les résultats d'un test sur le serveur Nagios, à travers un canal crypté.