Date – Date	**jeudi 16 octobre 2003**
Marque – Brand	
Ecrit par – Written by	**M. Grégory Bernard**
Destinataires – Recipients	
Copie – Copy	

Objet - Subject

Présentation de l'outil d'administration de réseau Nagios™

Très chers,

Vous trouverez dans les pages suivantes une explication détaillée du fonctionnement de l'outil de monitorage de réseau Nagios™. Cet outil basé sur une licence GPL de version 2 et fonctionne originellement sur la plate-forme Linux.

La courte étude qui vous est proposée à pour but d'analyser le produit Nagios™ en se servant d'une grille simple et performante (quoi, pourquoi, comment).

Pour toutes questions relatives à l'utilisation ou à la mise en œuvre de ce produit, n'hésitez pas à me contacter à l'adresse nagios@todo.biz

Bonne lecture.

Grégory Bernard
Directeur

21, rue Jean Jacques Rousseau – 75001 Paris – Tél : 01 40 26 43 14
E-Mail : nagios@todoo.biz – Web : http://www.todoo.biz/

ToDoo S.A.R.L au capital de 7.650 € – R.C. Paris B 439 872 540

Avant propos :

Je tenais tout d'abord à remercier Ethan Galstad et la communauté de développeurs qui ont participé à la mise au point de Nagios™. Cet outil contribue en grande partie à la qualité des services Internet de ma société, et il me permet de passer des week-end agréables tout en étant prévenu du moindre incident sur mon téléphone portable.

Nagios™ est devenu au fur et à mesure de ses différentes améliorations successives un partenaire simple à consulter et remarquablement fiable et efficace.

1. Le Pourquoi ?

Avec l'explosion des systèmes d'information répartis au milieu des années 90, les administrateurs de réseaux et des systèmes ont dû apprendre à gérer la supervision des services et des serveurs de façon plus active.

La décentralisation des systèmes d'information, la transparence des réseaux et la simplification des systèmes ont permis à des entreprises de taille moyenne d'acquérir des systèmes précédemment réservés à de très grandes entreprises ou à des administrations.

Cette démocratisation a introduit de nouveaux besoins de gestion et d'administration des systèmes. Souvent proposée par les opérateurs dans le cadre de leurs offres commerciales, la supervision des réseaux et des services peut aujourd'hui être prise en charge par les entreprises à moindre coût.

Le produit Nagios™ est né dans ce contexte. La première version du logiciel a été créée en Mars 1999 par Ethan Galstad (nagios@nagios.org) avec comme objectif « d'assurer la surveillance des hôtes et des services en vous prévenant lorsque les choses vont mal ».

Basé sur linux, cet outil a principalement été développé pour fonctionner sous des systèmes Unix. Afin de le faire fonctionner, il est nécessaire de posséder : un système Unix et un compilateur C.

Le système Nagios™ se distingue de tous ses concurrents par sa politique de licence ouverte (licence GNU General Public Licence). Celle-ci a permis une distribution massive de ce produit et son utilisation par un public de novice ou d'expert qui à largement contribué à son amélioration rapide au cours des huit différentes versions qui se sont succédées depuis trois ans.

Ce produit a souvent été intégré à de nouveaux produits de gestion de réseaux et services (http://telemetrybox.org ou http://linux-ha.org/) composé d'un assemblage d'outils Open Source. Il semble possible d'en faire une utilisation assez extensive (on citera entre autre : le monitoring de la température, des capacités des disques ainsi que des services).

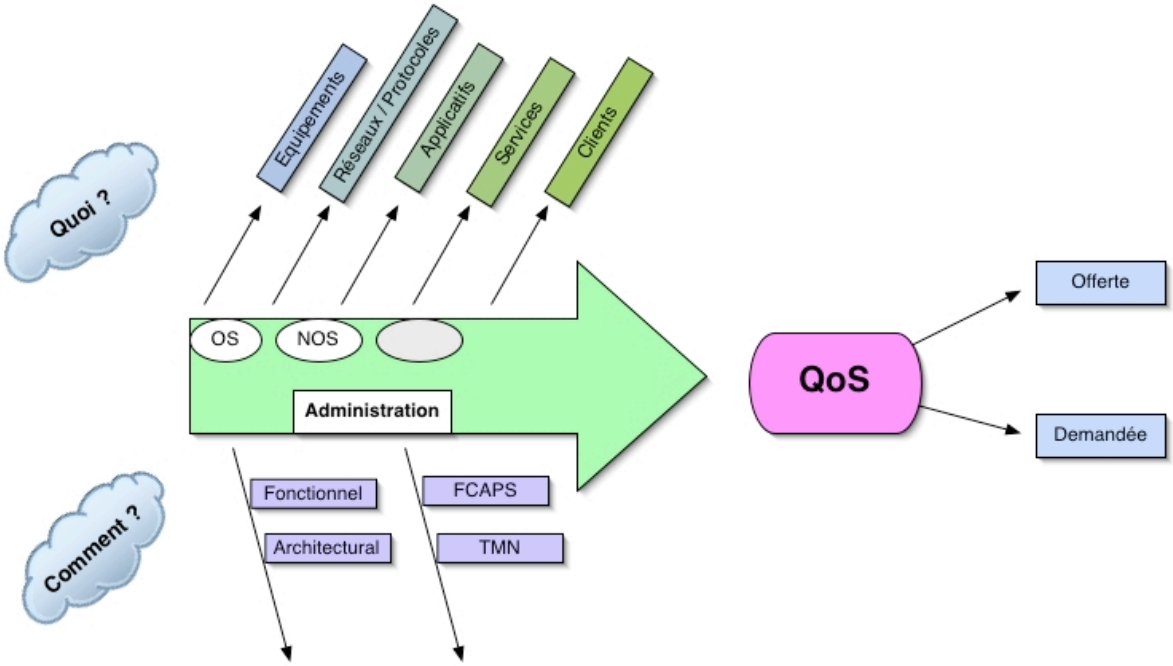
Lenny Liebmann éditorialiste pour la revue InternetWeek défini ainsi le produit : « Les produits tels que Nagios™ et Webmin, disponibles gratuitement, ont été mis au point par la même communauté de développeurs que ceux qui ont faits de Linux une alternative aussi viable dans le domaine des serveurs. »

Jeff Davis D'Amareda Hess Corp. à Houston qui gère plusieurs dizaines de serveur Linux faisait remarquer : « Il est particulièrement difficile de justifier des coûts d'acquisition de système de gestion de réseau qui coûtent plus cher que vos systèmes. La plupart des systèmes de gestion de réseaux propriétaires sont simplement trop chers pour nous !».

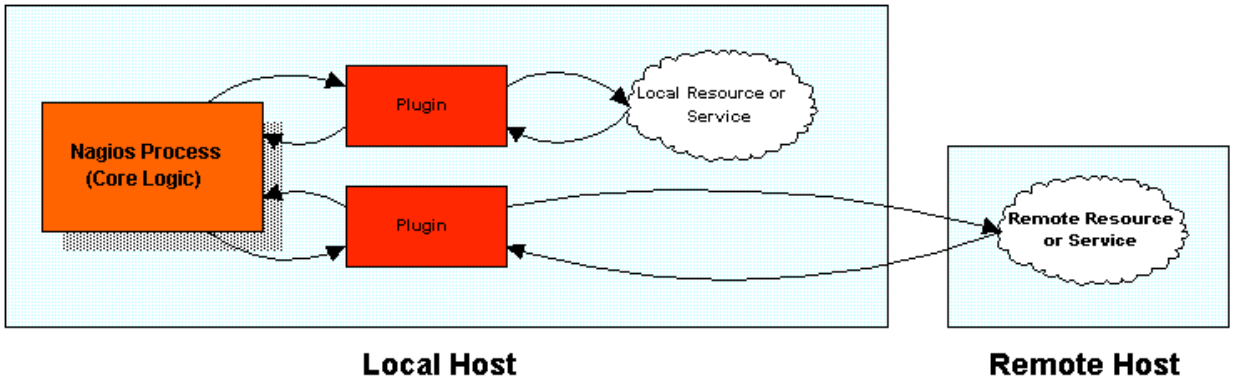
Nous allons donc étudier plus dans le détail les différents mécanismes mis en œuvre dans ce produit et découvrir quels services peuvent être pris en charge par Nagios™.

2. Le quoi gérer ?

Une division en couche nous a été proposée pour aborder la problématique du « quoi gérer ?» (cf. schéma ci-dessous). Nagios™ adopte une grille d'analyse simplifiée et inspiré de la division en couche proposée par TCP/IP.



Nagios™ fait ainsi une synthèse par le plus petit commun multiple disponible sur chacun des équipements dont il se charge de vérifier le fonctionnement. Nagios™, à la différence d'autres outils de monitoring n'intègre pas d'outil de maintenance en son corps, il se base sur différents "adaptateurs". Suivant le schéma figurant ci-dessous :



Approche de la gestion des couches basses par Nagios™:

Le principe retenu par Nagios™ est celui de différents adaptateur (pour la plupart écris en PERL et en C) qui communiquent une information standardisée au Process Nagios™. Un guide de développement des plugin Nagios™ est proposé sur le site SourceForge.net il permet de rapidement se familiariser avec les codes à retourner pour s'assurer de la compatibilité des adaptateurs développés avec le processus maître.

Une procédure de validation classique des développements est ensuite proposée (comme c'est le cas pour la plupart des projets Open-Source).

Il existe à ce jour 70 adaptateurs différents dont la plupart sont écrits en C et quelques-uns en PERL. Une cinquantaine d'autres adaptateurs sont à l'état de développement et n'ont pas encore été testés.

L'installation des adaptateurs est assez simple pour la plupart des systèmes UNIX qui possèdent les outils GCC permettant de compiler les sources. Après l'installation, les différentes librairies sont placées dans un répertoire de destination du type libexec.

Les adaptateurs écrit en C se servent des différentes librairies permettant de supporter le transport des requêtes (netutils.h). L'accès aux sources des différents adaptateurs permet, pour ceux qui en ont les compétences, d'apporter des modifications « maison » ;

Les adaptateurs sont appelés depuis le fichier nagios.cfg. Ce dernier comprend des lignes de commandes qui se servent des librairies compilées dans le répertoire libexec pour tester les « services » et transmettre la réponse au serveur Nagios™.

Il serait un peu rébarbatif de dresser la liste complète des différents adaptateur mis à la disposition des utilisateurs. Nous essaierons donc de les regrouper en catégorie logique suivant la nomenclature suivante :

1. Equipements.
    a. « check_disk.c » permet de tester l'espace disque disponible sur les partitions testés. Basé sur une utilisation de la commande /bin/df
    b. « get_load_average.c » permet de tester la charge d'un système en temps réel. Basé sur la commande unix uptime ou getloadaverage.
    c. « check_swap.c » permet de tester le swap disque.
    d. « check_ups.c » permet de tester les systèmes d'onduleurs et de déterminer leur état.
    e. « check_hpjd.c » permet de tester les imprimantes HP qui utilisent Jet Direct.
    f. « check_temptraxf » permet de tester la température à l'aide d'un module externe Temptrax.

2. Réseaux/Protocoles.
    a. « check_ping.c » permet de vérifier qu'un hôte est vivant sur un réseau, basé sur ICMP.
    b. « check_mrtgtraf.c » ce plugin va vérifier les taux de transfert d'un routeur, switch, il est basé sur les logs au format MRTG.
    c. « check_nw.c » permet de tester les réseaux NetWare.
    d. « check_udp.c » permet de tester les le bon fonctionnement de la couche transport en se basant sur UDP.

3. Applicatifs :
    a. « check_by_ssh.c » permet d'encapsuler des requêtes en se servant de ssh comme support.
    b. « check_radius.c » permet de tester les serveurs radius.

4. Services.
    a. Il existe plus d'une dizaine de adaptateur dans cette catégorie. Nous citerons parmi ceux-ci : « check_dns.c », « check_ftp.c », « check_http.c », « check_imap.c », « check_ldap.c », « check_mysql.c », « check_pgsql.c », « check_pop.c », « check_real.c ». L'ensemble de ces noms sont assez explicites pour comprendre la fonction qu'ils peuvent avoir. Le principe est toujours le même : formaliser une requête dans le protocole et vérifier l' état de l'hôte distant.

5. Clients.
    a. « check_Nagios™.c » permet de valider le bon fonctionnement des clients Nagios™ dans le cadre d'une architecture distribuée.

21, rue Jean Jacques Rousseau – 75001 Paris – Tél : 01 40 26 43 14
E-Mail : nagios@todoo.biz – Web : http://www.todoo.biz/

ToDoo S.A.R.L au capital de 7.650 € – R.C. Paris B 439 872 540

b. « check_nt.c » permet de tester les serveurs ou client NT.

Il existe de nombreux autres adaptateurs qui sont encore en cours de développement et qui permettent de faire des tests aussi variés que :

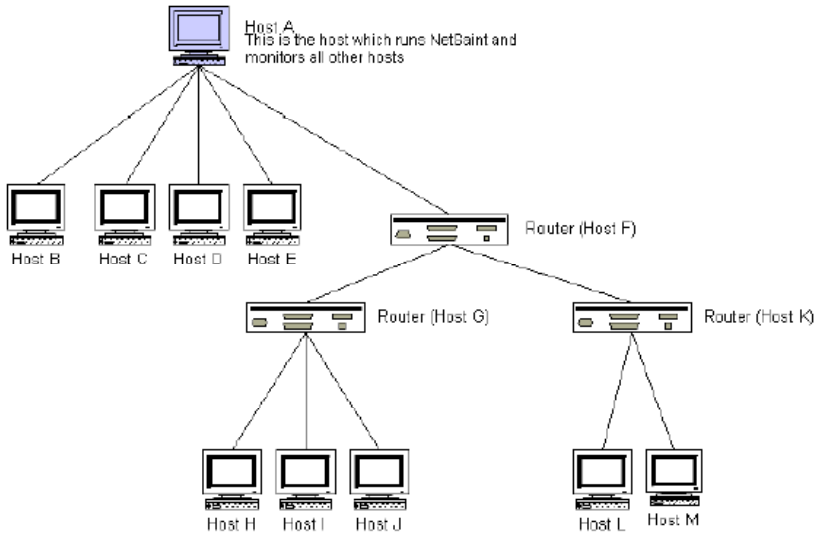
- Test des architectures réseaux utilisant BGP.
- Test des réseaux IPX.
- …

Une documentation extensive ainsi qu'un « readme » est fournie pour les utilisateurs intéressés par ces nouveaux développements et souhaitant y prendre part.

Gestion de la couche réseau :

Bien que Ping puisse permettre de détecter certains problèmes sur des réseaux distants, Nagios™ fait rapidement la différence entre les hôtes locaux et les hôtes distants en adoptant deux stratégies distinctes pour chaque cas de figure :

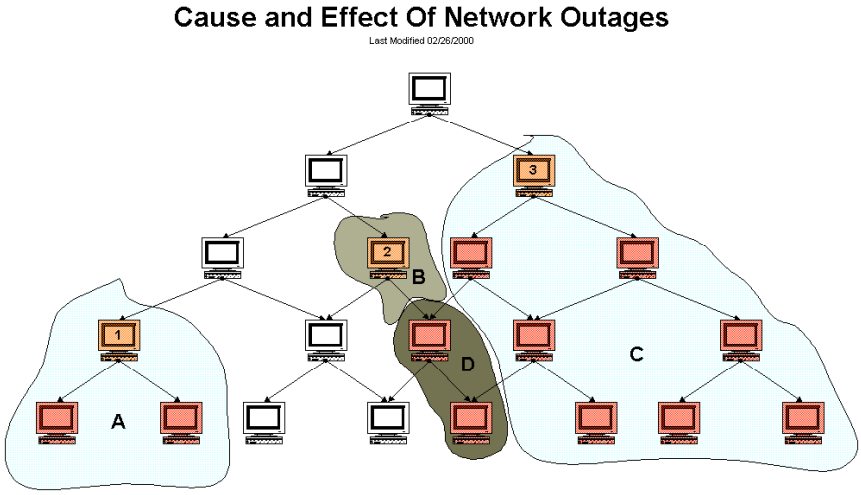
Les hôtes locaux utilisent un script de connexion directe « check_host » alors que les hôtes distants vont se baser sur des techniques de hiérarchies d'hôtes, permettant ainsi d'établir deux états : « host_unreacheable » et « host_down ».



En se basant sur les hiérarchies d'hôtes, le script va pouvoir établir une cartographie de la sévérité des problèmes rencontrés et permettre d'établir un diagnostique précis visant à permettre une prise de décision rapide pour la résolution du problème rencontré.

21, rue Jean Jacques Rousseau – 75001 Paris – Tél : 01 40 26 43 14
E-Mail : nagios@todoo.biz – Web : http://www.todoo.biz/

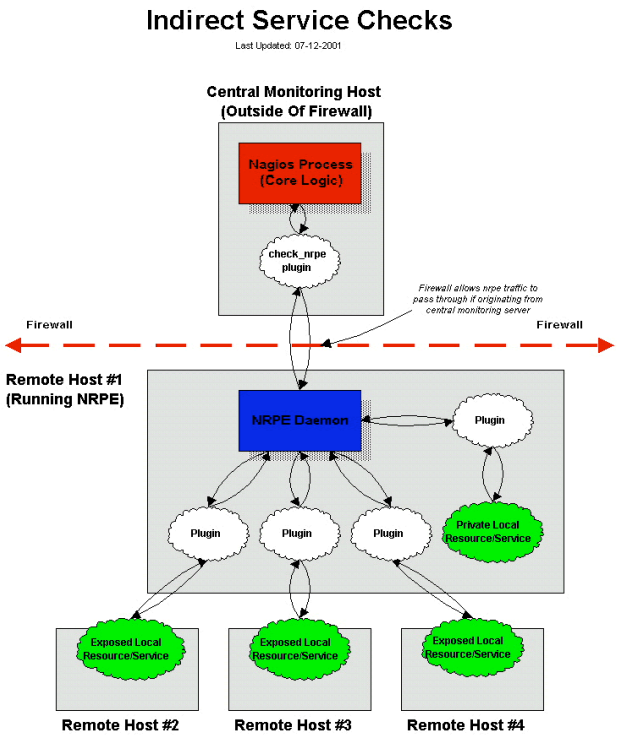
ToDoo S.A.R.L au capital de 7.650 € – R.C. Paris B 439 872 540



La gestion des réseaux distants :

Dans un soucis d'efficacité, Nagios™ prend en compte les architectures déportées et permet un monitoring efficace, même lorsque les réseaux administrés se situent derrière un firewall.

En permettant l'accès à un daemon fonctionnant sur le client grâce au module NRPE et NRPEP (avec un ajout de l'encryption triple DES), Nagios™ permet d'assurer une surveillance distante malgré la présence de firewall. Il faudra toutefois ouvrir un port de communication non privilégié pour permettre à NRPE de communiquer avec son client et récupérer les informations d'état concernant les serveurs déportés.



Monitoring déporté :

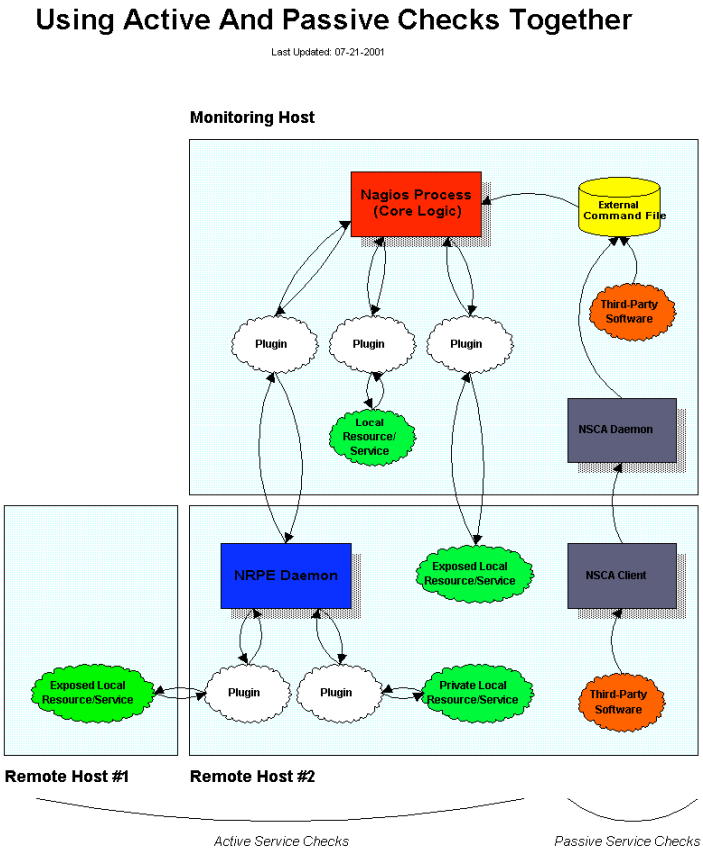
Une nouveauté intéressante est aussi l'architecture de « passive_check » proposé par Nagios™ en alternative aux commandes « active_check ».
Afin de permettre un accès aux applications distantes situées derrières un firewall (et sans ouvrir de port de communication, à la différence du système NRPE), Nagios™ peut utiliser les commandes « passive_check » ces commandes permettent aux différentes applications gérées de soumettre par un système de « external command file ». Les résultats des commandes externes sont ensuite mis dans la même file d'attente que les services actifs avant d'être traités.

Sécurité, le Monitoring Passif :

Afin de pouvoir soumettre les résultats de « passive service check » un module serveur « NSCA » devra être installé sur le serveur central et un client « NSCA_client » sur la machine surveillée.

Le module appelé « NSCA_client » ne fait que transmettre les résultats collectés en local au serveur NSCA suivant un protocole simple. Afin de s'assurer de la confidentialité des résultats soumis, il est possible d'utiliser l'une des méthodes d'encryptions suivantes (DES, 3DES, CAST, xTEA, Twofish, LOKI97, RJINDAEL, SERPENT, GOST, SAFER/SAFER+, etc.).

Il est ainsi possible d'utiliser ensemble des systèmes de contrôle actif et passif suivant les besoins de votre organisation et la structure de votre réseau.



Monitoring redondant :

Afin d'assurer une qualité au niveau même de l'outil de supervision, il est intéressant de s'assurer de son fonctionnement constant.

Nagios™ prévoit ainsi des cas de figure où l'un des nœuds ou se trouve le serveur Nagios™ principale tombe, isolant ainsi le réseau du reste des segments, rendant impossible toute supervision. Pour parer ces cas de figure, il est possible de configurer un ou plusieurs autres serveurs qui devront prendre le relais dans les cas suivants :

- Le serveur esclave doit prendre le relais si :
  - Le process Nagios™ du maître s'arrête.
  - Si le serveur maître est mort.
  - Si le serveur devient injoignable (routeurs ou routes injoignables)

- Le serveur esclave doit prendre le relais sur son réseau local si :
  - Le maître devient injoignable alors qu'il fonctionnait et qu'un ou les deux routeurs d'interconnexions sont down.

- Enfin le serveur maître doit arrêter de superviser tout le réseau et ne plus superviser que son réseau local si :
  - L'hôte esclave devient injoignable dû à un ou plusieurs routeurs ne fonctionnant plus et le serveur de secours était joignable.

L'interface graphique de monitoring :

Host	Service	Status	Last Updated	Attempt	Service Information
closet	PING	OK	Tue Mar 28 09:26:52 CST 2000	1/3	PING ok - Packet loss = 0%, RTA = 12.10 ms
cofh-405-lj4000	Printer Status	OK	Tue Mar 28 09:26:54 CST 2000	1/3	Printer ok - ("READY")
cofh-415-lj4	Printer Status	OK	Tue Mar 28 09:26:56 CST 2000	1/3	Printer ok - ("00 READY")
cofh-475-lj4m	Printer Status	OK	Tue Mar 28 09:26:59 CST 2000	1/3	Printer ok - ("00 READY")
	PING	WARNING	Tue Mar 28 09:27:01 CST 2000	1/3	PING problem - Packet loss = 0%, RTA = 62.50 ms
dbase	PING	WARNING	Tue Mar 28 09:27:03 CST 2000	1/3	PING problem - Packet loss = 0%, RTA = 85.70 ms
dev	PING	OK	Tue Mar 28 09:27:06 CST 2000	1/3	PING ok - Packet loss = 0%, RTA = 1.20 ms
devone	PING	OK	Tue Mar 28 09:27:08 CST 2000	1/3	PING ok - Packet loss = 0%, RTA = 0.90 ms
es-eds	SMTP	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:10 2000
	POP3	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:13 2000
	PING	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:15 2000
	IPX PING	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:17 2000
	Processor Load	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:20 2000
	Total Cache Buffers	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:22 2000
	Dirty Cache Buffers	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:24 2000
	Long Term Cache Hits	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:27 2000
	LRU Sitting Time	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:29 2000
	Connections	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:31 2000
	SYS Volume	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:34 2000
	DC Volume	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:36 2000
	INSTALL Volume	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:38 2000
	USER Volume	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:41 2000
	SNMP	PENDING	N/A	0/3	Service check scheduled for Tue Mar 28 09:27:43 2000

Les entreprises ont de plus en plus de services à gérer sur leurs réseaux, aussi bien au niveau des services réseaux, (SMTP, POP, http, NNTP, …). Qu'au niveau des hôtes eux-mêmes (charge des processeurs, utilisation des disques).

21, rue Jean Jacques Rousseau – 75001 Paris – Tél : 01 40 26 43 14
E-Mail : nagios@todoo.biz – Web : http://www.todoo.biz/

ToDoo S.A.R.L au capital de 7.650 € – R.C. Paris B 439 872 540

Nagios™ offre :

- Supervision de services réseau (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Supervision des ressources des hôtes (charge du processeur, utilisation du disque, etc.).
- Un système de plugins permettant aux développeurs de facilement développer des modules de surveillance "maison".
- Contrôle parallélisé des services.
- Possibilité de définir une hiérarchie dans les hôtes grâce aux hôtes "parents", permettant la détection et la distinction entre les hôtes en panne et ceux qui ne sont plus accessibles.
- Notifications à des contacts de l'apparition ou de la disparition de problèmes sur les hôtes ou les services (via email, pager, ou toute méthode définie par l'utilisateur).
- Possibilité de définir des gestionnaires d'événements qui sont lancés automatiquement lors de l'apparition d'événements concernant les hôtes ou les services, pour une résolution préventive des problèmes.
- Rotation automatique des fichiers journaux.
- Support de la supervision redondante
- Interface web optionelle pour visualiser l'état du réseau, les notifications et l'historique des problèmes, les fichiers journaux, etc.

3. Le comment ?

La façon la plus simple semble être de se reporter à la documentation qui vient d'être traduite en Français par Christian Vanguers et Pierre-Antoine Angelini

Il est possible de la télécharger directement en cliquant ici : http://heanet.dl.sourceforge.net/sourceforge/nagios-i18n/nagios-doc-FRENCH-1.0alpha1.tar.gz

La mise en œuvre du produit nécessite une bonne connaissance du système Linux, bien que la procédure soit assez standardisée (make, make clean…). Une bonne connaissance d'Apache pourra aussi vous éviter de faire des erreurs en laissant à la vue de tous l'état de votre réseau…

Afin de réaliser une installation efficace, il est nécessaire de bien comprendre les mécanismes qui sont mis en œuvre dans la gestion des ressources par Nagios™. Il ne sert à rien de se lancer dans une installation complexe alors que ce dont vous avez besoin se limite à un test de ping sur deux ordinateurs.

Les étapes de mise en œuvre du service Nagios™ :

1. Lecture assidue des concepts soutenant la construction de l'outil Nagios™.
2. Établissement d'un plan du réseau sous forme de diagramme.
3. Détermination des objets à prendre en charge sur chaque équipement actif.
4. Regroupement des objets en entité logique :
    a. Choix d'une politique de supervision par groupe d'objet.
    b. Détermination des interactions entre objets.
    c. Détermination des seuils d'alertes et des groupes à alerter.
5. Détermination des politiques de supervisions par type de service :
    a. Fixation des seuils par type de services
    b. Examen des cas particuliers (par machines ou services).
6. Écriture des règles dans les fichiers de configuration.
7. Installation des adaptateurs pour le monitoring déporté.
8. Démarrage du service et correction des erreurs dans les fichiers de configuration.

Quelques conseils pratiques :

L'accès aux tableaux de supervision peut constituer un outil précieux à exploiter pour des pirates. Il convient donc de prendre des mesures adaptés pour se protéger. L'accès aux statistiques doit normalement être protégé par un mot de passe du type htpasswd.

Pour des administrateurs qui souhaitent avoir un accès à leur tableaux de supervision depuis l'extérieur de leur réseau sans laisser le serveur Nagios™ à la vue de tous, le plus simple est d'utiliser ssh et le « port forwarding ».

Une commande du type :

sudo ssh -L 80:nagios.monreseau.fr:80 greg@mon_serveur_ssh.monreseau.fr

vous permettra d'accéder à un serveur Nagios™ dont les ports 80 sont inaccessibles depuis l'extérieur. Pour ce faire vous devez être root sur votre machine car les ports < à 1024 ne peuvent être manipulés que par root…

Il vous suffit ensuite sur votre machine local d'ouvrir un navigateur et de tapper : http://localhost/ pour accéder à votre tableau de supervision de façon entièrement sécurisée.

En espérant que ces quelques explications vous seront utiles.