−Table des matières

Nagios

Introduction

Nagios est un outil libre de monitoring réseau. Anciennement appelé NetSaint (sortie en Mars 1999), une première version de Nagios apportant un changement majeur est sortie en février 2005. Nagios permet de surveiller des machines et des services. En cas de dysfonctionnement, il alerte des utilisateurs préalablement définis. Sa modularité lui permet de s'adapter aux besoins des administrateurs de réseaux informatiques soucieux de contrôler différents paramètres de leur infrastructure.

Nagios à été développé par Ethan Galstad et d'autres (http://www.nagios.org/).

Pourquoi superviser ?

Problématique des réseaux des entreprises :

- La taille des réseaux ne cesse de grandir.
- Besoin d'experts en Administration pour surveiller les réseaux.
- Décentralisation des systèmes d'information.
- L'évolution des méthodes de travail au sein même de l'entreprise.
- Enjeu économique : l'activité de toute entreprise dépend de la disponibilité de son système d'information.
- La disponibilité du réseau.
- Q.O.S (Contrôler la bonne santé du réseau).

La supervision permet de répondre à cette problématique.

Objectifs de la supervision

- Être réactif : en alertant les administrateurs en cas de dysfonctionnement d'un élément du système d'information.
- Être proactif : en permettant d'anticiper les futurs incidents.
- Être pertinent : aider à cibler le problème dès son apparition afin d'agir de la façon la plus claire possible.

Description

Afin de pouvoir paramétrer Nagios correctement, il est nécessaire de comprendre certaines notions :

Le protocole SNMP

Nagios utilise le protocole SNMP, basé sur UDP (port 161), pour remonter les informations stockées dans la table MIB (Management Information Base) des machines. Il fonctionne suivant le principe de client (Nagios) / serveur (l'équipement à contrôler). Il est donc nécessaire que l'équipement dispose d'un agent SNMP (c'est le cas pour la plupart des éléments d'un réseau : routeur, imprimantes,...) activé et configuré. Sur les serveurs de type Linux, il suffit d'installer le daemon snmpd de la suite Open-SNMP. Sur Windows, il est également possible d'installer le daemon Net-SNMP. Enfin, Mac OS X inclut un daemon SNMP (UCD-SNMP), il suffit de suivre cette procédure pour l'activer.

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

- **Les équipements managés** (managed devices) sont des éléments du réseau (ponts, switches, 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 à travers laquelle les administrateurs peuvent réaliser des tâches d'administration.

L'utilisation de SNMP

Une requête SNMP est un datagramme UDP habituellement à destination du port 161. Les schémas de sécurité dépendent des versions de SNMP (v1, v2 ou v3).
Dans les versions 1 et 2, une requête SNMP contient un nom appelé communauté, utilisé comme un mot de passe. Il y a un nom de communauté différent pour obtenir les droits en lecture et pour obtenir les droits en écriture. Dans bien des cas, les colossales lacunes de sécurité que comportent les versions 1 et 2 de SNMP limitent l'utilisation de SNMP à la lecture des informations car la communauté circule sans chiffrement avec ces deux protocoles.
Un grand nombre de logiciels libres et propriétaires utilisent SNMP pour interroger régulièrement les équipements et produire des graphes rendant compte de l'évolution des réseaux ou des systèmes informatiques (MRTG, Cacti, Nagios, Zabbix,...).

Le protocole SNMP définit aussi un concept de trap. Une fois défini, si un certain événement se produit, comme par exemple le dépassement d'un seuil, l'agent envoie un paquet UDP à un serveur. Ce processus d'alerte est utilisé dans les cas où il est possible de définir simplement un seuil d'alerte. Les traps SNMP sont envoyés en UDP/162.
Dans nombre de cas, hélas, une alerte réseau ne devrait être déclenchée qu'en corrélant plusieurs événements.

Autres utilisations et notions

Le protocole SNMP peut aussi être utilisé dans le domaine industriel. Dans ce cas, SNMP sert à transporter des informations ne concernant pas le réseau informatique. SNMP transporte alors des informations applicatives industrielles. Dans ce cas, SNMP ressemble à une sorte de base de données arborescente. Les messages SNMP sont engagés soit par le système de gestion de réseau (NMS), soit par des éléments de réseau :
SNMP Trap est un message qui est lancé par un élément de réseau et envoyé au système de gestion du réseau.
Par exemple, un routeur peut envoyer un message si l'une de ses alimentations redondantes tombe en panne ou une imprimante peut envoyer un trap SNMP quand elle manque de papier.

La MIB

SNMP MIB, ou Management Information Base, est un ensemble de variables qui sont partagées entre les NMS et des éléments de réseau (NE). La MIB est un modèle de données associé à SNMP :

- **SMI** (Structure of Management Information) : méta modèle
- **MIB** : Liste de variables reconnues par les agents. C'est une base de données contenant des informations sur les éléments du réseau à gérer. Une ressource à gérer correspond à un objet. La MIB c'est une collection structurée d'objets.

Chaque noeud du système doit maintenir une MIB qui reflète l'état des ressources gérées. Une entité d'administration peut accéder aux ressouces du noeud en lisant les valeurs de l'objet et en les modifiant (si toutefois cette entité a l'autorisation en lecture/écriture sur les valeurs de l'objet !).
La MIB est extensible, ce qui signifie que le matériel et le logiciel peuvent ajouter de nouvelles variables dans la MIB. Ces nouvelles définitions doivent êtres ajoutées à la fois à des éléments du réseau et dans le système de gestion du réseau.

Voici un exemple de répertoire par défaut des tables MIB sous Ubuntu:

```
toto@serveur:/usr/share/mibs/netsnmp$ ls
GNOME-SMI       NET-SNMP-AGENT-MIB     NET-SNMP-EXTEND-MIB  NET-SNMP-MONITOR-MIB  NET-SNMP-SYSTEM-MIB  NET-SNMP-VACM-MIB  UCD-DISKIO-MIB  UCD-IPFWACC-MIB
LM-SENSORS-MIB  NET-SNMP-EXAMPLES-MIB  NET-SNMP-MIB         NET-SNMP-PASS-MIB     NET-SNMP-TC          UCD-DEMO-MIB       UCD-DLMOD-MIB   UCD-SNMP-MIB
toto@serveur:/usr/share/mibs/netsnmp$ :/usr/share/mibs/netsnmp
```

Communauté SNMP et nom de communauté

Nous avons vu plus haut que dans la version 1 et 2 de SNMP, une requête contient un nom appelé “communauté” qui est utilisé comme un mot de passe pour accéder à la MIB des équipements du réseau.
Cette communauté SNMP est une relation entre un agent et les stations d'administration (que l'on nomme aussi NMS) qui définit l'authentification, le contrôle d'accès et les caractéristiques des agents proxys. Chaque communauté définie entre un agent et ses stations d'administration a un nom unique (pour l'agent) employé lors des opération GET et SET. Une station d'administration (Centreon par exemple) garde la liste des noms de communauté donnés par les différents agents.

Nous avons 3 aspects du contrôle d'accès à la MIB de chaque agent par les différentes stations d'administration :

- **Un service d'authentification** : Un agent peut souhaiter limiter les accès à la MIB aux stations d'administration.

SNMP fournit un schéma d'authentification simple : chaque message d'une station d'administration comporte le nom de la communauté. Ce nom fonctionne comme un mot de passe et le message est dit authentifié si l'émetteur connaît le mot de passe. C'est un peu léger, ce qui fait que les opérations SET et TRAP sont mises dans des communautés à part avec l'utilisation de cryptage et décryptage.

- **Une politique d'accès** : Un agent peut donner des privilèges aux différentes stations d'administration.

Il peut fournir plusieurs types d'accès en définissant plusieurs communautés. Ce contrôle d'accès a deux aspects qui forment le profil de la communauté SNMP:
- Une vue de la MIB : Un sous-ensemble des objets de la MIB. Différentes vues de la MIB peuvent être définies pour chaque communauté.
- Un mode d'accès SNMP : Un éléments de l'ensemble (read only.read-write). Il est défini pour chaque communauté.

- **Un service de mandataire (proxy)** : Un agent peut agir comme un proxy pour d'autres périphériques gérés (qui ne supportent pas par exemple TCP/IP). Nous avons alors cette notion de sécurité, d'où la création de communauté SNMP.

Pour chaque périphérique que représente le système de proxy, ce dernier doit maintenir une politique d'accès. Le proxy connaît quels sont les objets MIB utilisés pour gérer le système mandaté (la vue de la MIB et les droits d'accès).

Bien souvent,il y a une chaîne de communauté qui est utilisée pour l'accès en lecture seule à un élément du réseau. La valeur par défaut pour cette communauté chaîne est souvent “public”. A l''aide de cette communauté comme une chaîne de mots de passe, les NEM peuvent récupérer les données d'éléments de réseau.

Moins souvent, il y a aussi une lecture-écriture communauté chaîne. La valeur par défaut pour cette communauté est souvent “privé”.

En utilisant cette chaîne de communauté, les NEM peuvent réellement changer les variables MIB sur un élément du réseau.

Commande en SNMP

Lorsqu'un élément supporte SNMP, on peut récupérer n'importe quelle valeur. Pour récupérer ces valeurs, on peut utiliser le plugin check_snmp de nagios avec les OID exacts des valeurs de MIB à interroger (celles qui nous intéressent).

Pour interroger la MIB v2 d'un élément, afin de trouver un OID, il faut télécharger la MIB sur le site du constructeur de l'élément (ou parfois sur l'élément lui-même) pour comprendre à quoi correspond les valeurs qu'on interroge et il faut taper une commande de ce type.

```
snmpwalk -v 2c -c COMMUNAUTE_SECU @IP:161  1.3.6.1.4
```

L'outil sous Linux est snmpwalk, snmpget... pour lire les valeurs et pour récupérer les informations. Sous Windows, utiliser MIB Browser (en graphique) est une bonne solution. Il faut ouvrir le fichier de MIB préalablement téléchargé, cliquer sur la valeur qu'on veut dans la MIB et simplement lui donner l'adresse IP et la communauté SNMP de l'élément à interroger. En faisant un “get” ou un “Go”, on obtient la valeur du champ et l'OID. C'est cette valeur que l'on va par exemple utiliser dans la commande check_snmp de nagios pour remonter l'information désirée.

Avec snmpwalk, la succession de chiffres 1.3.6.1.4 limite l'interrogation à la MIB v2. Si on enlève les derniers chiffres, on a encore plus d'information.

Autre exemple avec la librairie de sauvegarde.

```
snmpwalk -v 2c -c COMMUNAUTE_RESEAU @IP:161  1.3.6.1.4

snmpwalk -v 2c -c COMMUNAUTE_RESEAU @IP:161 -Os enterprises.3764.1.10.10.1

snmpwalk -v 2c -c COMMUNAUTE_RESEAU @IP:161 -Os enterprises.3764.1.10.10.1.1.0
```

Fonctionnalités de Nagios

Nagios permet :

- La supervision réseau (SMTP, POP3, HTTP, NNTP, ping, ...) ;
- La supervision des ressources systèmes (charge du processeur, utilisation du disque, nombre d'utilisateurs connectés, nombre de process, ...) ;
- La supervision applicative ;
- La notification par différents moyens de communication (SMS, mail, wap, ...) ;
- L'exécution de commandes manuelles ou automatiques ;
- La représentation des états des ressources supervisées, par coloration ;
- La cartographie du système d'information supervisé ;
- Le reporting.

Pour chaque élément supervisé, il peut gérer :

- Des contacts (les personnes qui doivent être alertées en cas de dysfonctionnement) ou un groupe de contacts (administrateurs-unix par exemple);
- Des plages horaires ;
- Des plugins.

Il est possible d'utiliser le système de templates (modèles prédéfinis) pour déclarer les différentes machines et services à surveiller.

Nagios surveille les machines et leurs services réseaux grâce à des plugins. Il prévient certaines personnes en fonction de l'état à certaines périodes de temps, de certaines machines ou services.

Une vue d'ensemble des équipements supervisés est disponible via une interface web.

Nagios et ces plugins locaux

En paramétrage standard, SNMP ne remonte que des informations système basiques (états des disques durs, état d'une imprimante, utilisation de la mémoire d'un pc,...). Pour aller plus loin et surveiller des processus plus complexes, Nagios utilise un système de plugins locaux. Ces plugins sont dits “local” car ce sont des scripts localisés sur le serveur Nagios (sous Linux,généralement dans /usr/lib/nagios/plugins).

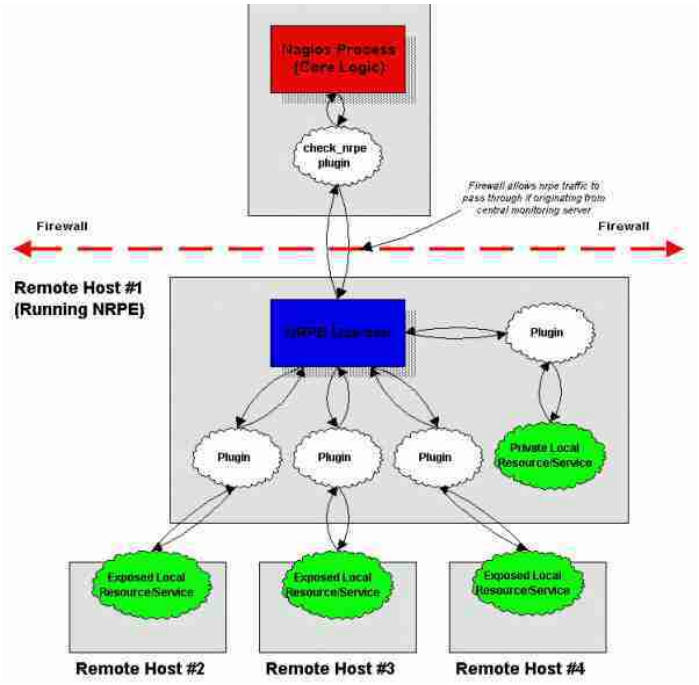
Ce script, lancé à la demande de Nagios, doit retourner un code dont la signification est la suivante :

- Code 0: OK - Tout va bien
- Code 1: WARNING - Alerte
- Code 2: CRITICAL - Alerte critique
- Code 3: UNKNOWN - Problème lors de l'exécution du plugin

En plus de ces codes, un plugins peut fournir d'autres informations (sous la forme d'une chaine de caractères) qui seront affichées à coté du statut de la machine.

Nagios et ses plugins actifs avec NRPE

A la différence des plugins locaux, le plugin NRPE permet l'exécution de plugins dit actifs directement sur les machines à surveiller. L'architecture est la suivante (schéma trouvé sur le site officiel de Nagios):

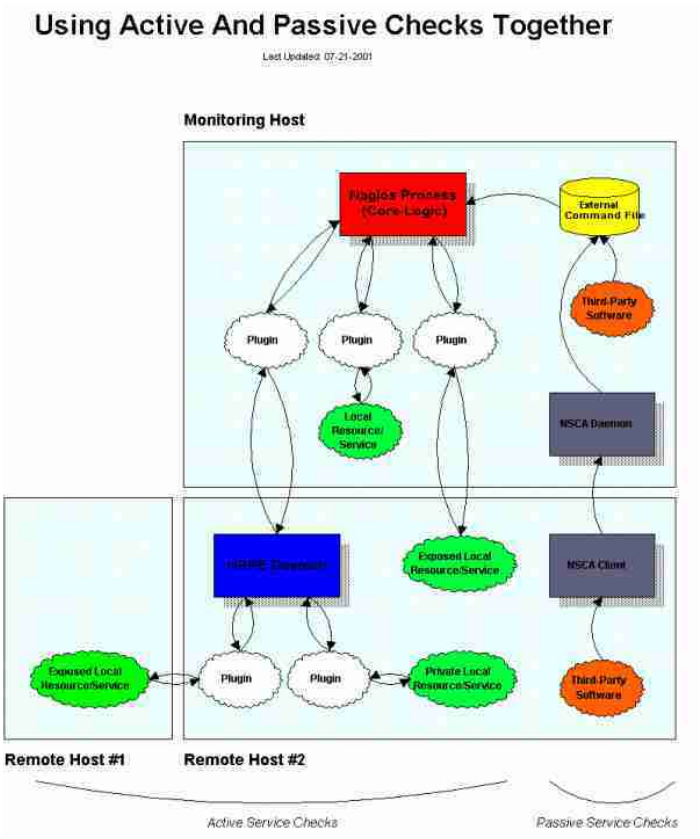


Avec NRPE, la demande d'exécution d'un plugin actif est faite à l'initiative du serveur Nagios. La procédure interne est la suivante:

- le serveur Nagios demande, via le client NRPE, l'exécution du plugin X sur la machine A
- le daemon NRPE, hébergé sur la machine A, reçoit la requête d'exécution du plugin X
- le plugin X est exécuté sur la machine A
- le daemon NRPE de la machine A envoie le résultat du plugin X au serveur Nagios
- le serveur Nagios interprète les résultats retournés par le plugin X

Les plugins passifs avec NSCA

Comme on vient de le voir NRPE est déclenché à l'initiative du serveur Nagios. Ce mode de fonctionnement peut poser problème, par exemple dans le cas où les machines à surveiller son derrière un réseau sécurisé par un Firewall ou si le processus à surveiller demande une fréquence d'exécution très courte. Le plugin NSCA répond à ce problème en proposant l'exécution de plugins passifs sur les machines à surveiller.



Ici, c'est donc le daemon NSCA qui va envoyer l'information au serveur Nagios. On peut comparer cette fonction à un TRAP SNMP.

Concernant les machines Windows

Les plugins NRPE et NSCA ne sont disponibles que pour Linux et Mac OS X. Si vous souhaitez surveiller des machines sous Windows (il vaut mieux les surveiller de près ces bêtes-là …) , il faut utiliser le plugin NSClient.

Etude de quelques plugins

Etant donné que nous utilisons Centreon pour interfacer Nagios, nous allons plutôt voir quelques exemples de plugins qui sont utilisés dans Centreon. Cliquer ici .

Sources

Largement inspiré du travail de documentation effectué sur le site Nicolargo:

D'ailleurs, Nicolargo a publié un manifique ebook sur Nagios que vous pouvez télécharger ici ou depuis son site

Liens ou documentations supplémentaires

Un étudiant de l'université de Caen a publié un beau rapport intitulé “Supervision d'une infrastructure répartie et virtualisée” que vous pouvez télécharger ici

http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2005ttnfa2006/lefebvre-maes/index.htm

Michauko : Installation de Nagios à partir de Rien

Michauko : Monitorer Linux avec Nagios

10 outils pour analyser son réseau

Distribution spécialement dédiée au monitoring

Pour toute question merci de nous contacter à l'adresse info@prolibre.com.

“La connaissance a plus de valeur et s’accroît rapidement lorsqu'elle est partagée et accessible librement…”