Dans le cadre de *SECURIDAY 2009*

SECURINETS

Présente

Atelier : Nagios

Formateurs : 1. Hajer Younes
2. Farah Ben Ahmed
3. Wael Mejri
4. Abdelbasset hadj taieb

1. Présentation :

Notre atelier nommé : « Nagios » se situe dans le cadre de la sécurisation des réseaux et des machines contre la menace des botnets.
Il s'agit d'un outil de supervision qui surveille les hôtes et services que nous spécifions. C'est un logiciel libre sous licence GPL.

Nagios est un programme modulaire qui se décompose en trois parties :
1) Le moteur de l'application responsable de l'ordonnancement des les tâches de supervision.
2) L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des anomalies possibles.
3) Les plugins, une centaine de mini programmes que l'on peut compléter en fonction des besoins de chacun pour superviser chaque service ou ressource disponible sur l'ensemble des ordinateurs ou éléments réseaux du SI.

L'architecture standard de Nagios peut donc être représentée de la manière suivante :

Fonctionnalités :

- La supervision des services réseau : (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, LDAP, etc.)
- La supervision des ressources des serveurs (charge du processeur, occupation des disques durs, utilisation de la mémoire paginée) et ceci sur les systèmes d'exploitations les plus répandus.
- Interfaçage avec le protocole SNMP.
- La supervision à distance en utilisant SSH ou un tunnel SSL.
- Les plugins (écrit avec les langages de programmation les plus adaptés à leur tâche : scripts shell (Bash, ksh, etc.), C++, Perl, Python, Ruby, PHP, C#, etc.)
- La vérification des services se faisant en parallèle.
- Possibilité de définir une hiérarchie dans le réseau pour pouvoir faire la différence entre un serveur en panne et un serveur injoignable.
- La remontée des alertes : elle est entièrement paramétrable grâce à l'utilisation de plugins (alerte par email, SMS, etc.).
- Acquittement des alertes par les administrateurs.

- Gestion des escalades pour les alertes.
- Limitation de la visibilité, les utilisateurs peuvent avoir un accès limité à quelques éléments.
- Capacité de gestion des oscillations (nombreux passages d'un état normal à un état d'erreur dans un temps court).
- Chaque test renvoie un état particulier :
  1. OK (tout va bien)
  2. WARNING (le seuil d'alerte est dépassé)
  3. CRITICAL (le service a un problème)
  4. UNKNOWN (impossible de connaître l'état du service)

2. Outils utilisés :

- ### FAN: FULLY AUTOMATED NAGIOS

Le but de FAN est de fournir une installation incluant les outils les plus utilisés de la communauté Nagios. FAN est un CDRom distribué au format ISO. Il est donc très facile à installer.
FAN est basé sur la distribution linux CentOS. Par ailleurs, tous les packages CentOS sont disponibles, de sorte que nous conservons tous les avantages de cette distribution avec les outils Nagios préinstallés et configurés.
Ajouté à ceci, un large panel d'outils est inclus dans la distribution facilitant ainsi la mise en œuvre d'une plateforme de supervision efficace.

- ### Les agents

Il est possible d'utiliser des agents de supervision permettant de récupérer des informations à distances. Il existe 2 types d'agents :

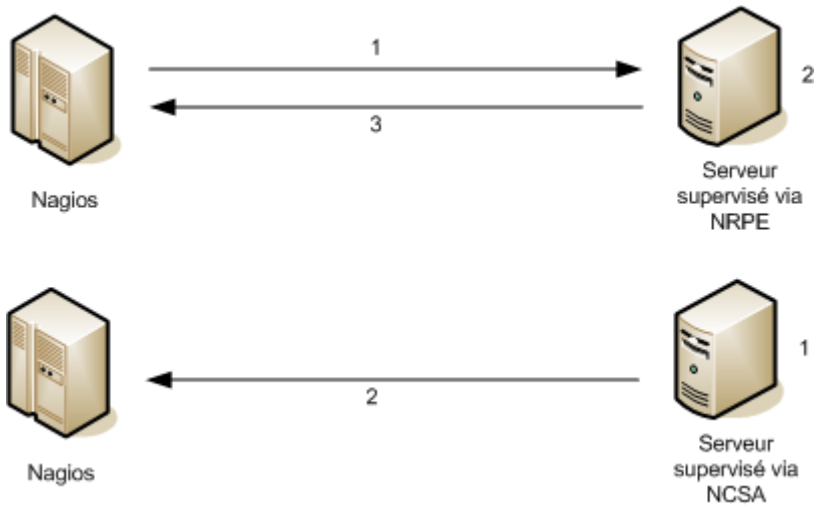
- Les agents NRPE
- Les agents NCSA

Le principe de fonctionnement des *agents nrpe (pour Nagios Remote Plugin Executor)* est simple : les plugins sont installés sur l'équipement à superviser, compilés en fonction de son architecture car c'est elle qui va les exécuter, ainsi que le démon nrpe faisant office de serveur. Sur la plateforme de supervision Nagios, le plugin *check_nrpe* fera alors office de client nrpe, récupérant les informations en interrogeant le démon nrpe sur l'équipement concerné.

Le plugin *check_nrpe* sur le serveur Nagios initiera une connexion vers l'agent nrpe de la machine cible et lui demandera alors l'exécution d'une vérification. L'agent nrpe lancera alors le plugin configuré en local pour obtenir l'information et retournera le code retour de l'exécution ainsi que sa sortie standard.

Les *agents ncsa (pour Nagios Service Check Acceptor)* diffèrent des agents nrpe car la vérification est planifiée en local sur l'équipement supervisé, exécutée, puis le résultat est

envoyé au serveur Nagios. De même que pour nrpe, l'architecture ncsa demande la présence du plugin *check_ncsa* sur la plateforme Nagios.



3. Suite de l'atelier :

- **INSTALLATION DE FAN**

L'installation de FAN est identique à celle d'un système CentOS classique (distribution de fedora core). Celle-ci est plutôt rapide et intuitive et ne nécessite pas de commentaire
La figure ci-dessous montre une capture-écran après avoir suivi les étapes d'installation.

```
CentOS release 5.2 (Final)
Kernel 2.6.18-92.1.6.el5 on an i686

localhost login: root
Password:
[root@localhost ~]# ps -A| grep nagios
 3541 ?        00:00:00 nagios
[root@localhost ~]# _
```

Ainsi le processus Nagios, indispensable au bon fonctionnement de la plate-forme tourne déjà.

- **PREMIÈRE CONFIGURATION**

Afin de pouvoir profiter de notre nouvelle plate-forme, il faut tout de même la configurer un minimum.
Le minimum est : La configuration réseau (adresse IP, routes, DNS…) et le nom de machin

➢ Interface réseau

La commande suivante permet de configurer les interfaces réseau du serveur :

 # system-config-network
Ou
 # vi /etc/sysconfig/networking/devices/ifcfg-eth0
 # Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
ONBOOT=yes
HWADDR=00:0c:29:72:44:a3
TYPE=Ethernet
NETMASK=255.255.255.0
IPADDR=192.168.1.21
GATEWAY=192.168.1.1

➢ Configurer les routes

 # route add –net 0.0.0.0 gw 10.166.200.252 netmask 255.255.255.0 (10.166.200.252 est la passerelle)
Au démarrage les autres routes ne seront pas prises en compte.
Pour cela il faut les inscrire dans un fichier texte :

 # touch /etc/sysconfig/network-scripts/route-eth0
#vi /etc/sysconfig/network-scripts/route-eth0
GATEWAY0=10.166.200.254
NETMASK0=255.255.0.0
ADDRESS0=10.174.0.0

➢ Redémarrer les interfaces réseau

 # ifup eth0 « après avoir configure via system-config-network »

➢ Sauvegarder/restaurer la configuration réseau

Sauvegarde
 # system-config-network-cmd -e > /tmp/network-config
Restauration
 # system-config-network-cmd -i -c -f /tmp/network-config
L'option -i indique l'import de données, l'option -c provoque la suppression de la configuration existante avant l'import et l'option -f spécifie que le fichier à importer est le suivant :

➢ Le DNS

 # vi /etc/resolv.conf
nameserver monDNS
nameserver DNSpublic
search mondomaine

➢ Le nom de la machine

 # vi/etc/sysconfig/network

HOSTNAME=Nagios (où Nagios est le nouveau nom :-)
Puis : ***# hostname Nagios*** (se re-loguer)
Pour ceux qui ne peuvent se passer d'interface graphique :

➢ Installer l'environnement graphique

 # yum --exclude=nautilus-sendto groupinstall "GNOME Desktop Environment" "X Window System"
 # startx
 # system-config-display (pour configurer l'affichage)

Ainsi, les outils de supervision sont installés et configurés.

On peut accéder à la page d'accueil du projet (depuis un poste sur le réseau) : http://ip-serveur/

A partir de la page d'accueil, on accède à l'interface Nagios ; le login/mot de passe par défaut est : nagiosadmin / nagiosadmin

- Nagios

A gauche de la fenêtre, on trouve les vues de monitoring permettent de connaître l'état des équipements et des services supervisés.

• CONFIGURATION DE NAGIOS

Le projet FAN fournit plusieurs choix de configuration. En effet l'administrateur de la plate-forme peut utiliser uniquement Nagios. On va détailler la configuration de la plate-forme en utilisant la méthode de configuration via fichier de texte de Nagios.

Où sont situés les principaux fichiers et répertoires ?

➢ Répertoires importants

·/etc/nagios
·/usr/lib/nagios
·/usr/share/nagios

➢ Définition des fichiers

 # ls /etc/nagios/
cgi.cfg : fichier de configuration des CGI.
localhost.cfg : définition de l'host « localhost » (autrement dit de Nagios).
ndomod.cfg : fichier de configuration de ndoutils.
resource.cfg : possibilité de définir des informations sensibles (identifiant, mot de passe…)
command-plugins.cfg : définition des commandes « check ».
nagios.cfg : fichier de configuration principal de Nagios.
ndomod-load.cfg : fichier de configuration de ndoutils (emplacement du « broker_module »).
send_nsca.cfg : fichier de configuration de nsca.
commands.cfg : définition des commandes (commandes de « check » et de notifications).
nagvis.ini.php : fichier de configuration de Nagvis par défaut.
nrpe.cfg : fichier de configuration du serveur nrpe.
htpasswd.users : stocke les utilisateurs et mot de passe (en crypté) ayant accès à Nagios.
ndo2db.cfg : fichier de configuration de ndoutils.
nsca.cfg : fichier de configuration du serveur nsca.

➢ Méthodologie

Afin d'ajouter un host avec des services à superviser, il faut configurer plusieurs fichiers.
Pour des raisons de simplification de configuration, nous pouvons créer un répertoire « conf.d » situé dans « /etc/nagios/ » où nous regrouperons l'ensemble des fichiers de configuration.
En fonction de notre architecture de supervision (multi-sites ou pas) nous pouvons créer un répertoire du nom du site ou de l'entreprise.
Toujours afin de faciliter la configuration, il peut être intéressant de créer des fichiers appelés
·serveurs_nomdusite.cfg ;
·imprimantes_ nomdusite.cfg ;
·switchs_ nomdusite.cfg ;
·routeurs_ nomdusite.cfg.
La définition des différents éléments se fera donc en fonction de son type.

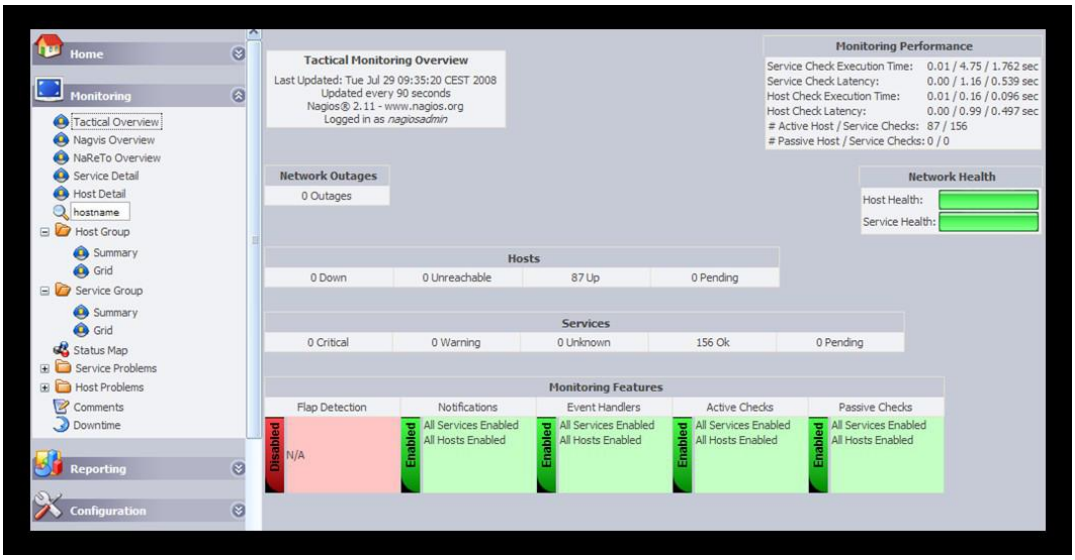
Partant du même principe il est conseillé de créer les fichiers suivants :
·**contacts.cfg** : définition des contacts ;
·**dependances.cfg** : gestion des dépendances ;
·**extinfo.cfg** : ajout de fonctionnalité graphique (icon…) ;
·**services.cfg** : définition des services ;
·**hostgroups.cfg** : définition des groupes d'hôtes ;
·**generic-host.cfg** : définition d'un template pour les hôtes ;
·**generic-service.cfg** : définition d'un template pour les services ;
·**time-period.cfg** : définition des périodes de notifications.

➢ Définir les besoins

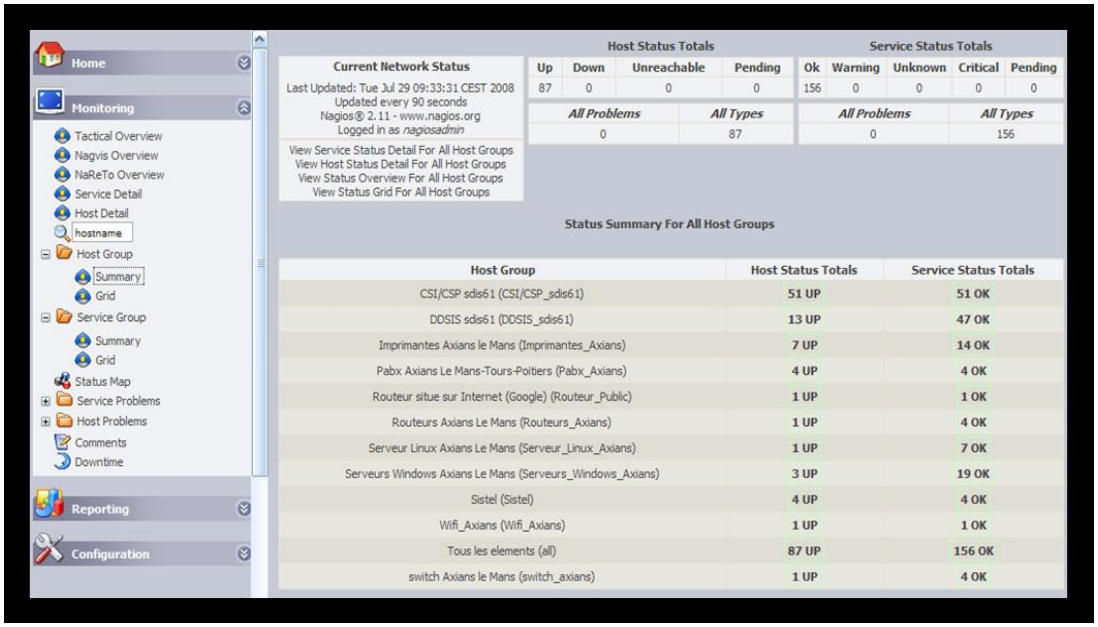
Avant la première ligne de commande, il faut bien entendu définir de façon très précise les besoins.
Il faut se poser les questions suivantes :

- Quel élément superviser ?
- Quel service doit être surveillé ?
- Qui va recevoir les mails ?
- Qui va utiliser la plate-forme et donc la modifier ?

Un exemple de configuration nous a fourni les résultats suivants :



Tactical Overview: 87 Hosts up et 156 services testés.



Host Group – Summary : affiche les “hostgroup” avec leurs statuts.

Conclusion

Nous avons vu ci-dessus les résultats d’une configuration minimaliste de Nagios. La configuration peut s’avérer difficile et fastidieuse, cela nécessite une grande rigueur d’organisation et de nommage. De plus, l’interface web de Nagios ne permet en aucun cas la modification de la plateforme. C’est pourquoi l’outil Centreon est très répandu dans la communauté.