Table des matières :

Nagios®

Lancement du projet Nagios, (C'est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services spécifiés, alertant lorsque les systèmes ont des dysfonctionnements et quand ils repassent en fonctionnement normal.

Le projet a commencé par l'explication et le fonctionnement de Nagios par communication téléphonique du responsable sécurité de chez Bitdefender (Mr. Renaud) qui m'a bien aidé pour le lancement de mon projet.

Installation des pré-requis :

Tout d'abord, Nagios sera installé sur un Centos 6.7 une distribution LINUX. Tout d'abord, Nagios sera installer sur un CentOS 6.7 une distribution LINUX, j'ai commencé par installer les paquets nécessaires au bon fonctionnement de l'application.

```
[root@localhost ~]# yum install gcc glibc glibc-common gd gd-devel httpd php ope
nssl openssl-devel_
```

J'ai commencé par crée un utilisateur du nom nagios et mdp (D3lpl@st). J'ai aussi crée un groupe nagcmd qui permettra l'exécution des commandes externes à l'aide de l'interface Web par l'administrateur. J'ai ajouté à ce groupe les utilisateurs « nagios » et « apache ».

Pour faciliter l'installation de nagios, au lieu de télécharger un fichier et de devoir l'extraire, nous somme allez direct prendre les paquets dans une liste de donnée « epel »

En voici la liste : https://dl.fedoraproject.org/pub/epel/6/x86_64/

Pour accéder à cette base de donnée, nous avons d'abord installé un navigateur web

```
[root@localhost ~]# yum install elinks -y_
```

```
[root@localhost ~]# elinks http://dl.fedoraproject.org/pub/epel/6/x86_64/_
```

Ensuite nous somme allez chercher le fichier epel-release-6-8.noarch.rpm dans la liste donnée. Nous l'avons enregistré dans le répertoire principal.

Ensuite il suffit de l'installer en local :

```
[root@localhost ~]# yum localinstall epel-release-6-8.noarch.rpm _
```

Nous somme quand même aller vérifier par précaution que epel était bien activer.

```
[root@localhost ~]# vim /etc/yum.repos.d/epel.repo _
```

```
[epel]
name=Extra Packages for Enterprise Linux 6 - $basearch
#baseurl=http://download.fedoraproject.org/pub/epel/6/$basearch
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-6&arch=$basearch
failovermethod=priority
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
```

Apres vérification, on peut tester que les paquets sont bien installer ou s'il y a un paquet disponible a être installer.

```
[root@localhost ~]# yum list nagios
Modules complémentaires chargés : fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: centos.crazyfrogs.org
 * epel: mirror.vutbr.cz
 * extras: centos.mirror.fr.planethoster.net
 * updates: centos.mirror.fr.planethoster.net
Paquets installés
nagios.x86_64                           3.5.1-1.el6                          @epel
```

(Capture prise après installation)

Installation de Nagios :

On peut maintenant installer nagios et les plugins de nagios

```
[root@localhost ~]# yum install nagios nagios-plugins-all_
```

Apres installation, on a vérifié que le fichier de conf était bien présent

```
[root@localhost ~]# cat /etc/nagios/nagios.cfg _
```

Histoire de ne pas avoir de problème de recherche d'un fichier, on a fait un `updatedb _` qui permet de mettre à jour les base de données de recherche.

Ensuite nous sommes allez chercher l'emplacement des fichiers plugins, étant donnée quand faisant la commande « locate check », il y avait une grande liste d'installation de paquet inutile et prenant place sur notre recherche, nous avons décidé de les retirer de la recheche avec un « grep –v »

Il y a ci-dessous 3 commande qui vont s'exécuter en même temps, pour les dissocier, elles sont séparer d'un « | »

```
[root@localhost ~]# locate check |grep -v yum |grep -v share_
```

Grâce a ce système de recherche, cela nous a facilité les recherches de plugins pour déterminer leur emplacement.

```
/usr/lib64/nagios/plugins/check_
```

Installation de NRPE :

Enfin, nous allons installer NRPE (Nagios Remote PluginExecutor) qui permet d'exécuter à distance des plugins sur d'autre machine. Cela va vous permettre de surveiller les paramètres de la machine a distance comme l'utilisation du disque, du CPU… il est possible aussi d'exécuter des scripts pour vérifier des mesures sur les machines Windows.

```
yum install nrpe_
```

```
================================================================================
 Paquet          Architecture      Version                 Dépôt           Taille
================================================================================
Installation:
 nrpe            x86_64            2.15-7.el6              epel            225 k
```

Comme nagios et les plugins de nagios, nrpe était la aussi disponible dans la list de paquet d'epel, ce qui facilite grandement l'installation.

Maintenant on lance Nagios

```
[root@localhost ~]# /etc/init.d/nagios start_
```

Ensuite on lance apache et on le configure pour qu'il se lance automatiquement à chaque fois.

```
[root@localhost ~]# /etc/init.d/httpd start_
```

```
[root@localhost ~]# start apache on boot_
```

```
[root@localhost ~]# chkconfig httpd on_
```

Maintenant on crée un admin nagios

```
[root@localhost ~]# htpasswd -c /etc/nagios/passwd nagiosadmin_
```

Mdp : D3lpl@st

Apres on vérifie qu'on a bien le fichier nagios.conf dans apache.

```
[root@localhost ~]# /etc/httpd/conf.d/nagios.conf_
```

```
cat nagios.conf _
```

Apres on vérifie que SELINUX est bien désactiver dans :

```
[root@localhost ~]# cat /etc/selinux/config_
```

```
[root@localhost ~]# cat /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted
```

S'il est activé, on le désactive et on reboot la machine.

Ensuite on vérifie que nos utilisateurs sont bien dans leur groupe destiné, si cela n'est pas le cas, il faut effectuer les commandes suivantes.

```
# groupadd nagios
# adduser nagios -g nagios
# passwd nagios
# usermod -G nagios nagios
# usermod -G apache,nagios apache
```

Pour vérifier le résultat final que tout fonctionne. Il suffit de faire une vérification pour constater possiblement des erreurs.

```
[root@localhost ~]# nagios -v /etc/nagios/nagios.cfg _
```

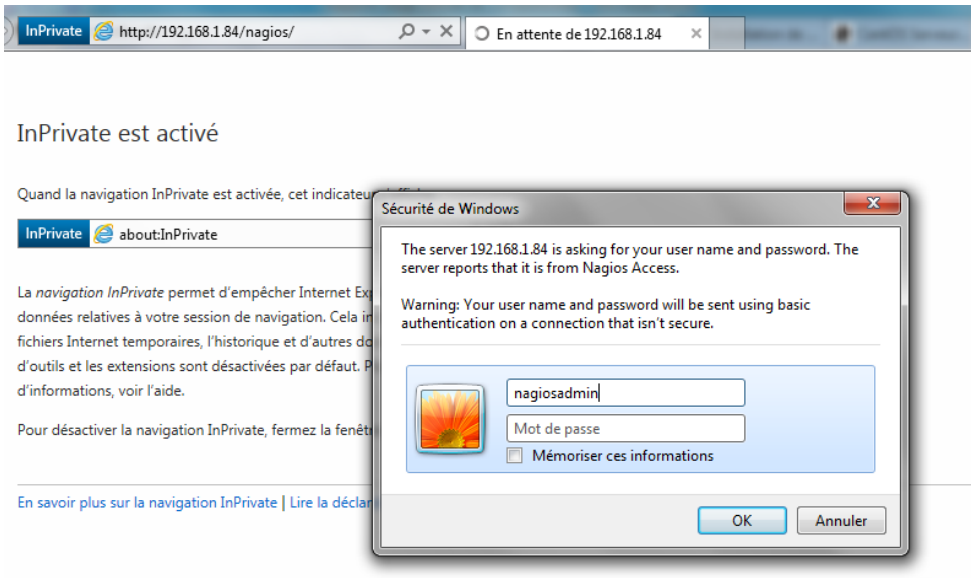
```
Total Warnings: 0
Total Errors:   0
```

Si on obtient ceci, alors tout fonctionne normalement.

Interface Web Nagios :

On peut aller test dans le navigateur avec l'adresse ip du serveur **http://ip/nagios**

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 00:0c:29:47:8a:08 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.84/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::20c:29ff:fe47:8a08/64 scope link
       valid_lft forever preferred_lft forever
[root@localhost ~]#
```



Il suffit de rentrer les identifiants d'administrateur. (Le mot de passe se trouve plus haut)

Exemple de notre interface web, ceci est la page hôte.

Il faut aussi ne pas oublier d'ajouter nagios dans les services et de régler pour qu'il se lance automatiquement.

```
[root@localhost ~]# chkconfig --add nagios_
```

```
[root@localhost ~]# chkconfig nagios on_
```

Configuration Plugins Nagios:

Enfin on configure les plugins de nagios

Il faut aller dans :

```
/etc/nagios/objects/commands.cfg
[root@localhost nagios]# vi commands.cfg_
```

Il faut aller a la fin du fichier et ajouter les lignes suivantes :

```
######
# NRPE
###### # 'check_nrpe' command definition
define command{
command_name check_nrpe
command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

On peut aller entre son mail pour recevoir les notifications en cas de problème .

```
/etc/nagios/objects/contacts.cfg
```

Il mot modifier le fichier :

```
# Vue partielle du fichier

define contact{
contact_name nagiosadmin ; Short name of user
use generic-contact ; Inherit default values
alias Nagios Admin ; Full name of user

email nagios@localhost ; <<***** Votre adresse mail ici ******
}
```

```
        email                           arthur.mariette@sts-sio-caen.info       ;
<<****** CHANGE THIS TO YOUR EMAIL ADDRESS ******
        }
```

Petite aparté, verifier bien que le service ssh est bien en marche, si cela n'est pas le cas, il y aura un problème de connexion refusé qui sera constaté dans le tableau des services nagios.

```
[root@localhost ~]# service sshd start
Démarrage de sshd :                                        [  OK  ]
[root@localhost ~]# service sshd status
openssh-daemon (pid  4628) en cours d'exécution...
[root@localhost ~]# _
```

SSH	OK	05-31-2016 15:55:34	0d 0h 3m 47s	1/4	SSH OK - OpenSSH_5.3 (protocol 2.0)

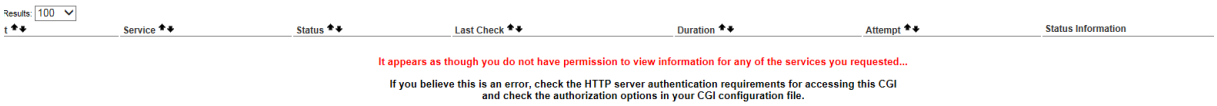
Ajout d'un utilisateur avec droit limité sur l'interface Web :

On crée d'abord l'utilisateur puis après on ira modifier c'est droit.

Pour ce test, l'utilisateur sera « usenul »

```
[root@localhost nagios]# htpasswd /etc/nagios/passwd usenul
New password:
Re-type new password:
Adding password for user usenul
[root@localhost nagios]# _
```

Vu que l'utilisateur n'a pas de droit, il n'a accès à aucun service



Maintenant on test avec un nouveau utilisateur auquel on va lui attribuer des droits limités, il sera autorisé seulement a voir tout les services et voir tout les hôtes.

```
[root@localhost nagios]# htpasswd /etc/nagios/passwd usenuladmin
New password:
Re-type new password:
Adding password for user usenuladmin
[root@localhost nagios]# _
```

Il faut maintenant éditer le fichie cgi.cfg pour pouvoir ajouter l'utilisateur, on fait une sauvegarde avant du fichier.

```
[root@localhost nagios]# cp cgi.cfg cgi2.cfg
[root@localhost nagios]# vi cgi.cfg_
```

Pour attribuer la totalité des droits, procédez comme pour les utilisateurs limités (ci dessus) et ajoutez (en plus) leur login à trois autres lignes du fichier de configuration (vers les lignes 144, 171 et 172) :

```
authorized_for_system_information=nagiosadmin,usenuladmin_
```

```
authorized_for_all_services=nagiosadmin,usenuladmin_
authorized_for_all_hosts=nagiosadmin,usenuladmin
```

Il faut maintenant redémarrer les services

```
[root@localhost ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
[root@localhost ~]# service nagios restart
Running configuration check...done.
Stopping nagios: .done.
Starting nagios: done.
```

On peut maintenant se connecter en tant que usenuladmin à l'interface de nagios, après verification, l'utilisateur usenuladmin dispose bien des droits d'administrateur.

Ajouter un utilisateur avec accès complet :

Pour attribuer les droit complet il faut déjà les ajouter les lignes demander au dessus si l'utilisateur de base ne l'est possède pas.

Si c'est est fait, il ne reste plus qu'a ajouter les lignes suivantes pour autoriés les droits total pour l'utilisateur « usenuladmin »

Il faut aller dans /etc/nagios/cgi.cfg et modifier les lignes 144, 171 et 172, il faut juste rajouter le nom utilisateur.

```
authorized_for_all_service_commands=nagiosadmin,usenuladmin
authorized_for_all_host_commands=nagiosadmin,usenuladmin
```

```
authorized_for_system_commands=nagiosadmin,usenuladmin_
```

Il faut maintenant redémarrer les services pour que la modification soit prise en compte.

```
[root@localhost ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
[root@localhost ~]# service nagios restart
Running configuration check...done.
Stopping nagios: .done.
Starting nagios: done.
```

Pour la suppression d'un utilisateur Nagios :

Pour cela il faut déjà retirer les lignes modifies dans le fichier « cgi.cfg »

Apres il faut supprimer la ligne qui concerne l'utilisateur dans le fichier. « passwd »

```
[root@localhost ~]# cat /etc/nagios/passwd
nagiosadmin:63oTkyZDGNDww
usenul:AdbE0lthq5UXA
usenuladmin:6s2Ug2JujlPhI
```

Il faudra ensuite redémarrer apache et nagios

Fin d'installation d'un Nagis, le projet est maintenant dévier vers le projet Centreon.

La partie suivante permet de gerer lui aussi les applications, système et réseaux, il est basé sur les concepts de Nagios. En effet après réflexion, nous avons décidé de modifier le projet de base pour lui ajouter le supperviseur centreon qui est plus performant.
