

ACTIVITE 6 : Supervision systèmes et réseau avec NAGIOS Core sous Ubuntu :

Lien de la vidéo de mise en place : <https://www.youtube.com/watch?v=scLDRjyxNI0>
Site officiel : <https://www.nagios.org/>

Documentation
: <https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/3/en/toc.html>

L'iso de système Ubuntu 20.04.2 LTS : <https://ubuntu.com/download/server>

Introduction :

Nagios est une application permettant la surveillance système et réseau. Elle surveille les hôtes et services spécifiés, alertant lorsque les systèmes dysfonctionnent et quand ils passent en fonctionnement normal. C'est un logiciel libre sous licence GPL.

L'interface web permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies.

Les sondes (appelés greffons ou plugins), une centaine de mini programmes que l'on peut compléter en fonction des besoins de chacun pour superviser chaque ressource disponible sur l'ensemble des ordinateurs ou éléments réseaux du système informatique.

PS : une version Long-term support ou LTS (en français Support à long terme) désigne une version spécifique d'un logiciel dont le support est assuré pour une période de temps plus longue que la normale.

TIPS : Pour changer le clavier en fr, tapez la commande : `dpkg-reconfigure keyboard-configuration`
puis, entrée, entrée, entrée et entrée.

Topologie :

Une machine Ubuntu-20.04 LTS équipée de deux interfaces réseaux :

hostname : nagios

Carte 1 : En Bridged ou NAT

Carte 2 : static d'adresse 172.20.0.31/24 et en segment LAN "stadiumcompany"

Installer le paquet ifupdown (`apt install ifupdown`) pour configurer les interfaces réseaux :

Ouvrez la session avec le compte de l'utilisateur créé au moment de l'installation de la machine, changez d'identité à l'aide de la commande :

```
sudo su
```

```
apt install ifupdown -y
```

```
ip a : Pour Vérifier les noms de vos interfaces "ensXY"
```

```
nano /etc/network/interfaces
```

```
-----  
auto lo  
iface lo inet loopback
```

```
auto ens33  
iface ens33 inet dhcp
```

```
auto ens38  
iface ens38 inet static  
address 172.20.0.31/24  
-----
```

Après avoir enregistré votre fichier :

```
service networking restart
```

```
nano /etc/hostname
```

```
-----  
nagios  
-----
```

```
nano /etc/hosts (effacer la partie inférieur IPv6)
```

```
-----  
127.0.0.1      nagios.stadiumcompany.com  nagios  localhost  
172.20.0.31    nagios.stadiumcompany.com  nagios  
-----  
-
```

Validation :

```
ip a
```

carte 1 : adresse obtenue depuis le dhcp de l'école(bridged) ou de
vmware(nat)

carte 2 : 172.20.0.31/24

ping 1.1.1.1 -> ok : histoire de vérifier la passerelle / défaut

ping google.fr -> ok : histoire de vérifier le DNS de la machine.

Prérequis :

Suivez ces étapes pour installer les packages prérequis :

```
apt update && apt upgrade -y  
apt install -y autoconf gcc libc6 make wget unzip apache2 php libapache2-mod-  
php7.4 libgd-dev
```

Téléchargez la source :

```
cd /tmp  
wget -O  
nagioscore.tar.gz https://github.com/NagiosEnterprises/nagioscore/archive/nagios-  
4.4.6.tar.gz
```

Décompressez le zip téléchargé :

```
tar xzf nagioscore.tar.gz
```

Compilez les fichiers :

```
cd nagioscore-nagios-4.4.6/  
./configure --with-httpd-conf=/etc/apache2/sites-enabled  
make all
```

Créez l'utilisateur et le groupe :

Cela crée l'utilisateur et le groupe nagios. L'utilisateur www-data (correspondant à apache) est également ajouté au groupe nagios.

```
make install-groups-users  
usermod -a -G nagios www-data
```

Installez les binaires (exécutables)

Cette étape installe les fichiers binaires, les CGI et les fichiers HTML.

```
make install
```

Installez le Service / Daemon

Cela installe les fichiers de service ou de démon et les configure également pour le démarrage automatique

```
make install-daemoninit
```

Les informations sur le démarrage et l'arrêt des services seront expliquées plus loin.

Installez le mode commande

Cela installe et configure le fichier de commande externe.

```
make install-commandmode
```

Installez les Fichier de configuration

Cela installe les fichiers de configuration * SAMPLE *. Celles-ci sont nécessaires car Nagios a besoin de quelques fichiers de configuration pour lui permettre de démarrer.

```
make install-config
```

Installez les fichier de configuration d'Apache

Cela installe les fichiers de configuration du serveur Web Apache et configure les paramètres Apache.

```
make install-webconf  
a2enmod rewrite  
a2enmod cgi
```

Configure Firewall

Vous devez autoriser le trafic entrant du port 80 sur le pare-feu local pour pouvoir accéder à l'interface Web de Nagios Core.

```
ufw allow Apache  
ufw reload
```

Create nagiosadmin User Account

Vous devrez créer un compte utilisateur Apache pour pouvoir vous connecter à Nagios.

La commande suivante créera un compte utilisateur appelé nagiosadmin et vous serez invité à fournir un mot de passe pour le compte.

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Redémarrez Apache2 :

```
systemctl restart apache2.service
```

```
systemctl status apache2.service
```

Démarrez Nagios

```
systemctl start nagios.service  
systemctl status nagios.service
```

Test Nagios

Nagios est maintenant en cours d'exécution, pour confirmer cela, vous devez vous connecter à l'interface Web de Nagios.

Pointez votre navigateur Web vers l'adresse IP ou le FQDN de votre serveur Nagios Core :

depuis une VM dans le même segment LAN : <http://172.20.0.31/nagios> ou depuis la machine physique <http://@ens33/nagios> ou depuis un DC ou un client du domaine à l'aide de l'URL :

<http://nagios.stadiumcompany.com/nagios>

Vous serez invité à entrer un nom d'utilisateur et un mot de passe. Le nom d'utilisateur est nagiosadmin (vous l'avez créé à une étape précédente) et le mot de passe est celui que vous avez fourni précédemment.

Une fois que vous vous êtes connecté, l'interface Nagios vous est présentée.

Félicitations, vous avez installé Nagios Core !

Installer les plugins Nagios

Nagios Core a besoin de plugins pour fonctionner correctement. Les étapes suivantes vous guideront tout au long de l'installation des plugins Nagios.

Ces étapes installent nagios-plugins 2.2.1.

Veuillez noter que les étapes suivantes installent la plupart des plugins fournis dans le package Nagios Plugins. Cependant, certains plugins nécessitent d'autres bibliothèques qui ne sont pas incluses dans ces instructions.

Veuillez consulter les articles de la base de connaissances pour obtenir de apt instructions d'installation détaillées:

Prérequis :

Installer les packages prérequis :

```
apt install -y libmcrypt-dev libssl-dev bc gawk dc build-essential snmp libnet-  
snmp-perl gettext
```

Télécharger la source :

```
cd /tmp
```

```
wget --no-check-certificate -O nagios-plugins.tar.gz https://github.com/nagios-  
plugins/nagios-plugins/archive/release-2.2.1.tar.gz
```

Décompressez :

```
tar xzf nagios-plugins.tar.gz
```

Compilez + Installez

```
cd nagios-plugins-release-2.2.1/  
./tools/setup  
./configure  
make  
make install
```

```
#####  
#####
```

Activer la supervision des machines et autres matériels réseaux :

Editer le fichier nagios.cfg :

```
nano -c /usr/local/nagios/etc/nagios.cfg
```

Afin de superviser les machines Windows, décommenter (enlever le #) la ligne 38

```
·      cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

Afin de superviser les machines switchs et routeurs, décommenter (enlever le #) la ligne 41

```
·      cfg_file=/usr/local/nagios/etc/objects/switch.cfg
```

Afin de superviser les machines imprimantes, décommenter (enlever le #) la ligne 44

```
·      cfg_file=/usr/local/nagios/etc/objects/printer.cfg
```

Enregistrer le fichier

Ajouter et Superviser des Ordinateurs Windows :

Editer le fichier windows.cfg :

```
nano -c /usr/local/nagios/etc/objects/windows.cfg
```

Dans la section « HOST DEFINITIONS », aller à la ligne 24, section <define host> et écrire en face de 'host_name' le nom de la machine 'DC', dans alias le pseudonyme que l'on veut donner à la machine, et dans address l'adresse ip de la machine tel que :

```
define host{  
    use windows-server  
    host_name DC  
    alias AD-DS  
    address 172.20.0.10  
}
```

Il faut créer autant de <define host{...} > que de machine Windows Serveur à superviser tel que :

Rajoutez le bloc suivant pour déclarer la machine SDC :
exemple :

```
define host{
    use windows-server
    host_name SDC
    alias My secondary Windows Server
    address 172.20.0.11
}
```

Important : Ne pas oublier de changer le *host_name* des différents services (dans les blocs 'define service' un peu plus bas dans le même fichier) en supprimant "*winserver*" et en ajoutant les noms de chaque serveurs (dans notre cas DC, SDC).

65 : Bloc de supervision de l'agent de supervision NSClient

79 : Bloc de supervision du temps depuis lequel la machine tourne sans interruption.

92 : Bloc de supervision du charge système, une mesure de la quantité de travail

105 : Bloc de supervision de l'utilisation de la mémoire.

118 : Bloc de supervision de l'espace disque

131 : Bloc de supervision du service de publication World Wide Web : w3svc

143: Bloc de supervision d'Explorer

On peut ajouter plusieurs serveurs sur le même service, il suffit de séparer leurs noms par une virgule, on peut aussi surveiller d'autre service en ajoutant des blocs service.

service nagios restart

Vérifiez l'ajout de machines dans les menus hosts et map de la console Web nagios.

#####

Ajouter et superviser des serveurs Linux :

Editer le fichier localhost.cfg pour ajouter des serveurs Linux :

nano -c /usr/local/nagios/etc/objects/localhost.cfg

Dans la section « HOST DEFINITIONS », aller à la ligne 24, section <define host> et écrire dans host_name le nom de la machine Linux, dans alias le pseudonyme que l'on veut donner à la machine, et dans « address » l'adresse ip de la machine tel que :

```
define host{
    use          linux-server
```

```

host_name    Nagios
alias        Serveur de supervision
address      172.20.0.31
}

```

Juste après ce premier bloc, ajoutez le bloc suivant :

```

define host{
    use          linux-server
    host_name    Zimbra
    alias        Serveur de messagerie
    address      172.20.0.15
}

```

Changez localhost dans members du bloc define hostgroup par Nagios,Zimbra

Important : Ne pas oublier de changer le host_name en supprimant "localhost" et en ajoutant les noms de chaque serveurs pour chaque « define service ». On peut ajouter plusieurs serveurs sur le même service, il suffit de séparer leurs noms par une virgule.

```

define service{
    use          local-service
    host_name    Nagios, Zimbra
    service_description    PING
    check_command    chek_ping.....
}

```

Configuration de la notification par mail :

Installer les paquets sendmail, mailutils et ssmtp :

```

apt install sendmail
apt install mailutils
apt install ssmtp

```

Configuration du SSMTP:

```
nano -c /etc/ssmtp/ssmtp.conf
```

Modifier la ligne 10:

```
mailhub=mail.stadiumcompany.com
```

Enregistrer

Configuration de l'adresse de messagerie du compte root :

```
nano -c /etc/ssmtp/revaliases
```


Rajouter la ligne :

```
root:adminNagios@stadiumcompany.com
```

Attention :

La machine nagios doit pouvoir résoudre le nom : mail.stadiumcompany.com :

1- Allumez votre contrôleur de domaine stadiumcompany.com : 172.20.0.10 ou autre

2- Renseigner à nagios son serveur DNS 172.20.0.1

```
nano /etc/resolv.conf
```

```
nameserver 172.20.0.10
```

```
nameserver 1.1.1.1
```

```
search stadiumcompany.com
```

Testez la résolution de nom depuis nagios :

```
nslookup mail.stadiumcompany.com
```

Redémarrer le service nagios : service nagios restart ==

· Testez l'envoi du mail :

```
echo "Contenu du mail" | mail -s "Sujet 1" admin@stadiumcompany.com
```

Ou à votre adresse mail perso :

```
echo "Contenu du mail" | mail -s "Sujet 1" MailPerso
```

·

Vérifiez l'obtention du mail dans la boîte de messagerie
admin@stadiumcompany.com

Modification du fichier contact.cfg

```
nano /usr/local/nagios/etc/objects/contacts.cfg
```

```
define contact{
    contact_name          nagiosadmin
    alias                 Admin Alerte Nagios
    email                 admin@stadiumcompany.com
    service_notification_period 24x7
    service_notification_options w,u,c,r,f,s
    service_notification_commands notify-service-by-email
    host_notification_period 24x7
    host_notification_options d,u,r,f,s
    host_notification_commands notify-host-by-email
}
```

#####Explication#####

#####contact_name = nom du contact.

alias = description du contact.

email = adresse mail du contact.

service_notification_period 24x7 = période d'envoi des notification pour les services (applications) 7j/j 24h/24.

service_notification_options w,u,c,r,f,s = notifie les options choisis pour les services (w : informe les états de service WARNING, u : informe sur les états de service UNKNOWN, c : informe les états de service CRITICAL, r : informe le service RECOVERY (états OK), f : informe lorsque le service démarre et arrête FLAPPING, n : ne pas notifier le contact sur tout type de notifications de service).

Service_notification_commands notify-service-by-email = choix d'être notifier par email sur l'état des services.

Host_notification_period 24x7 =période d'envoi des notifications pour les hôtes (pc) 7j/j 24h/24

Host_notification_options d,u,r,f,s = notifie les options choisis pour les hôtes (d: informe sur le statut DOWN de l'hôte, u : informe sur le statut UNREACHABLE de l'hôte,r : informe sur l'hôte RECOVERY (états allumé), f : informe au démarrage de l' hôte et arrête FLAPPING, s : Envoie des notifications lorsque l'hôte ou le service prévu les temps d'arrêt commence et se termine, n(none) : Ne pas notifier le contact sur tout type de notifications d'hôtes.

Host_notification_commands notify-host-by-email = choix d'être notifier par email sur l'état des services.

#####

#####

Redémarrn :

service nagios restart

Autoriser l'envoi de notification :

chown -R nagios:www-data /usr/local/nagios/var/rw

Aller dans le dossier /usr/local/nagios/etc/objects/ :

cd /usr/local/nagios/etc/objects/

et rajouter les lignes suivant dans chaque sections « define host{ } » et dans chaque sections « define service{ } » des fichiers /usr/local/nagios/etc/objects/windows.cfg ,/usr/local/nagios/etc/objects/localhost.cfg et /usr/local/nagios/etc/objects/switch.cfg:

```
contact_groups    admins
contacts          nagiosadmin
```

Aller dans `/usr/local/nagios/etc/objects/templates.cfg` et rajouter les lignes suivant dans chaque sections « define host{ } » et dans chaque sections « define service{ } » des machine que l'on veut superviser (linux, windows, etc..) :

```
contact_groups    admins
contacts          nagiosadmin
```

Aller dans le fichier `commands.cfg` :

```
nano -c /usr/local/nagios/etc/objects/commands.cfg
```

et aller à la ligne 29 et 37 et modifier le fichier pour que `/usr/bin/mail` soit présent (compléter uniquement par `/usr`):

```
# notify-host-by-email' command definition
define command {
    command_name    notify-host-by-email
    command_line    /usr/bin/printf "%b" "***** Icinga *****\n\n \Notification
Type:$NOTIFICATIONTYPE$\n \Host: $HOSTNAME$\n \State: $HOSTSTATE$\n
\Address: $HOSTADDRESS$\n \Info: $HOSTOUTPUT$\n\n \Date/Time:
$LONGDATETIME$\n" \ | /usr/bin/mail-s \""" $NOTIFICATIONTYPE$ Host Alert:
\ $HOSTNAME$ is $HOSTSTATE$ """ \ $CONTACTEMAIL$
}
```

```
# 'notify-service-by-email' command definition
define command {
    command_name    notify-service-by-email
    command_line    /usr/bin/printf "%b" "***** Icinga *****\n\n \Notification Type:
$NOTIFICATIONTYPE$\n\n \Service: $SERVICEDESC$\n \Host: $HOSTALIAS$\n
\Address: $HOSTADDRESS$\n \State: $SERVICESTATE$\n\n \Date/Time:
$LONGDATETIME$\n\n \Additional Info:\n\n \ $SERVICEOUTPUT$\n" \
| /usr/bin/mail-s \""" $NOTIFICATIONTYPE$ Service Alert:
\ $HOSTALIAS$/ $SERVICEDESC$ is $SERVICESTATE$ """ \ $CONTACTMAIL$
}
```

Redémarrer le service nagios :

```
service nagios restart
```