# Mise en production et déploiement

## TP 1:METTRE EN PLACE UN SERVEUR AVEC SYSLOG-NG (7 points)

Pour la lisibilité du document la partie **Serveur** sera en **rouge** et la partie **client** sera en **cyan**

## SERVEUR

•Apres avoir installé syslog-ng,on commence par configurer les paramètres IP dans /etc/network/interfaces

```
interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
##########################################
#                AJOUTER                 #
##########################################
auto eth0
iface eth0 inet static
address 192.168.1.10
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.1
gateway 192.168.1.1
```

```
syslog-ng
# If a variable is not set here, then the corresponding
# parameter will not be changed.
# If a variables is set, then every invocation of
# syslog-ng's init script will set them using dmesg.

# log level of messages which should go to console
# see syslog(3) for details
#
CONSOL_LOG_LEVEL=1

# Command line options to syslog-ng
#SYSLOGNG_OPTS="--no-caps"
```

•On decommante CONSOL_LOG_LVL=1 dans /etc/default/syslog-ng

```
update-rc.d -f rsyslog remove
dpkg  -P rsyslog
```

•On modifie le fichier /etc/syslog-ng/syslog-ng.conf on verifie qu'il n 'y a pas d'erreur grace a la commande :

```
/usr/sbin/syslog-ng -svf /etc/syslog-ng/syslog-ng.conf
```

## BONUS

•On ajoute l'IP du client et on la nome dans: /etc/hosts

```
hosts
127.0.0.1   localhost
127.0.1.1   user
192.168.1.11 client

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
user@user: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@user:/var/log/client/2020/10/19# ls
kern.log  messages  syslog
root@user:/var/log/client/2020/10/19#
```

•Apres avoir lancé la commande sur le client:

```
/usr/sbin/syslog-ng  -d
```

on obtient ces fichier sur le serveur

## CLIENT

•Apres avoir installé syslog-ng,on commence par configurer les paramètres IP dans /etc/network/interfaces

```
interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
##########################################
#                AJOUTER                 #
##########################################
auto eth0
iface eth0 inet static
address 192.168.1.11
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.1
gateway 192.168.1.1
```

```
syslog-ng
# If a variable is not set here, then the corresponding
# parameter will not be changed.
# If a variables is set, then every invocation of
# syslog-ng's init script will set them using dmesg.

# log level of messages which should go to console
# see syslog(3) for details
#
CONSOL_LOG_LEVEL=1

# Command line options to syslog-ng
#SYSLOGNG_OPTS="--no-caps"
```

•On decommante CONSOL_LOG_LVL=1 dans /etc/default/syslog-ng

```
update-rc.d -f rsyslog remove
dpkg  -P rsyslog
```

•On ajoute a /etc/syslog-ng/syslog-ng.conf

```
destination d_logger {udp("192.168.1.10" port(514)); };
log { source(s_src); destination(d_logger); };
```

puis on lance la commande:

```
/usr/sbin/syslog-ng  -d
```

```
user@user: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
    Compiling f_crit sequence [filter] at [/etc/syslog-ng/syslog-ng.conf:9]
      Compiling #unnamed single [log] at [/etc/syslog-ng/syslog-ng.conf:9]
  Compiling d_console reference [destination] at [/etc/syslog-ng/syslog-ng.conf:1]
    Compiling d_console sequence [destination] at [/etc/syslog-ng/syslog-ng.conf:6]
      Compiling #unnamed junction [log] at [/etc/syslog-ng/syslog-ng.conf:6]
        Compiling #unnamed single [log] at [/etc/syslog-ng/syslog-ng.conf:6]
Compiling #unnamed sequence [log] at [/etc/syslog-ng/syslog-ng.conf:1]
  Compiling s_src reference [source] at [/etc/syslog-ng/syslog-ng.conf:1]
  Compiling d_logger reference [destination] at [/etc/syslog-ng/syslog-ng.conf:1]
    Compiling d_logger sequence [destination] at [/etc/syslog-ng/syslog-ng.conf:1]
      Compiling #unnamed junction [log] at [/etc/syslog-ng/syslog-ng.conf:1]
        Compiling #unnamed single [log] at [/etc/syslog-ng/syslog-ng.conf:1]
Syslog connection established; fd='8', server='AF_INET(192.168.1.10:514)', local='AF_INET(0.0.0.0:0)'
Running application hooks; hook='1'
Running application hooks; hook='3'
syslog-ng starting up; version='3.5.6'
^Csyslog-ng shutting down; version='3.5.6'
Running application hooks; hook='4'
root@user:/home/user#
```

# Mise en production et déploiement

## TP 2: AUTOMATISATION POUR LA GESTION (8 points)

### AUTOMATISATION POUR LA GESTION

1) Automatiser la suppression des logs de plus de 90 jours, via une tâche automatique et un script shell.

logsup.sh

```
#!/bin/bash
rm -fr "/var/log/client/"`date '+%C%y/%m/%d' -d "-90 days"`
```

2) Créer un script permettant l'archivage et la compression des fichiers de log « message » et « syslog » (archive.sh) et l'exécuter tous les jours à 00h01, le fichier compressé (tar.gz) devras être enregistré dans /home/archives/$jour/$mois/$annee/[message|syslog]

archive.sh

```
#!/bin/bash -e
source="/home/archives/"`date '+%d/%m/%C%y' -d "-0 days"`
destination="/var/log/client/"`date '+%C%y/%m/%d' -d "-0 days"`
mkdir -p $source"/syslog" && tar -cvf "$source/syslog/syslog.tar.gz" "$destination/syslog"
mkdir -p $source"/messages" && tar -cvf "$source/messages/messages.tar.gz" "$destination/messages"
```

Une fois les 2 scriptes crés on automatise les taches sur la crontab:

```
# m h  dom mon dow   command
00 00 * * * bash /home/user/logsup.sh
01 00 * * * bash /home/user/archive.sh
```

3) Créer un script de déploiement de clients avec syslog **a.** Le script s'exécute sur le serveur syslog mais est à destination des clients

**b.** Il devra installer syslog-ng, modifier le fichier /etc/default/syslog-ng pour décommenter la ligne **CONSOLE_LOG_LEVEL=1**, restart le service, désinstaller le démon syslogd (**update-rc.d -f rsyslog remove | dpkg -P rsyslog**)

**c.** Il devra ajouter les lignes nécessaires a **syslog-ng.conf** et tester le bon fonctionnement de client avec le retour de la commande **/usr/sbin/syslog-ng -d**.

J'ai crer une nouvelle machine dont j'ai choisis l'adresse IP de facon statique ,puis j'ai lancer ce scripte qui a permis l'installation de syslog ainsi que son bon foctionnement.

autosyslog.sh

```
#!/bin/bash
ipclient2="192.168.1.12"
ipclient="192.168.1.11"
ipserveur="192.168.1.10"
confadd='destination d_logger {udp(\"'$ipserveur'\" port(514)); };\nlog { source(s_src); destination(d_logger); };'
ssh $ipclient2 "apt-get install syslog-ng"
ssh $ipclient2 "sed -i -e 's/#CONSOLE_LOG_LEVEL=1/CONSOLE_LOG_LEVEL=1/' /etc/default/syslog-ng"
ssh $ipclient2 "/etc/init.d/syslog-ng restart"
ssh $ipclient2 "update-rc.d -f rsyslog remove"
ssh $ipclient2 "dpkg -P rsyslog"
ssh $ipclient2 "[ `sed -n \"/$ipserveur/p\" /etc/syslog-ng/syslog-ng.conf` == "" ] && echo -e \"$confadd\">>/etc/syslog-ng/syslog-ng.conf"
ssh $ipclient2 "/usr/sbin/syslog-ng -d"
```

## *BONUS*

Pour utiliser ssh sans mot de passe, dans /etc/ssh/sshd_config de la nouvelle machine j'ai remplecer without_password par yes, puis j'ai redemarer le service
`service ssh restart`

on lance la commande `ssh-keygen` pour génerer une clé RSA puis `ssh-copy-id root@ipclient` qui permet d'envoyer la clé au client .On constate alors qu' on a la meme clé /root/.ssh/id_rsa.pub dans le serveur que dans /root/.ssh/autorizedkey du client

# Mise en production et déploiement

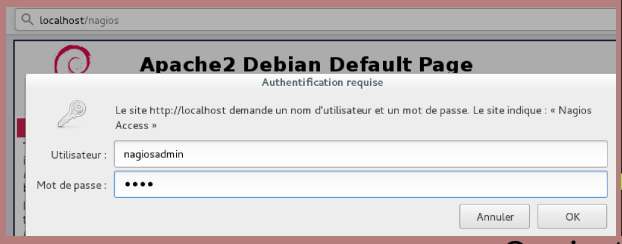
## TP3 :CENTREON/NAGIOS/GRAYLOG SUJET LIBRE
## (5 points+1 bonus)

## SERVEUR

J'ai créer un scripts pour installer nagios ainsi que tout les outils indisponsable a son bon fonctionement

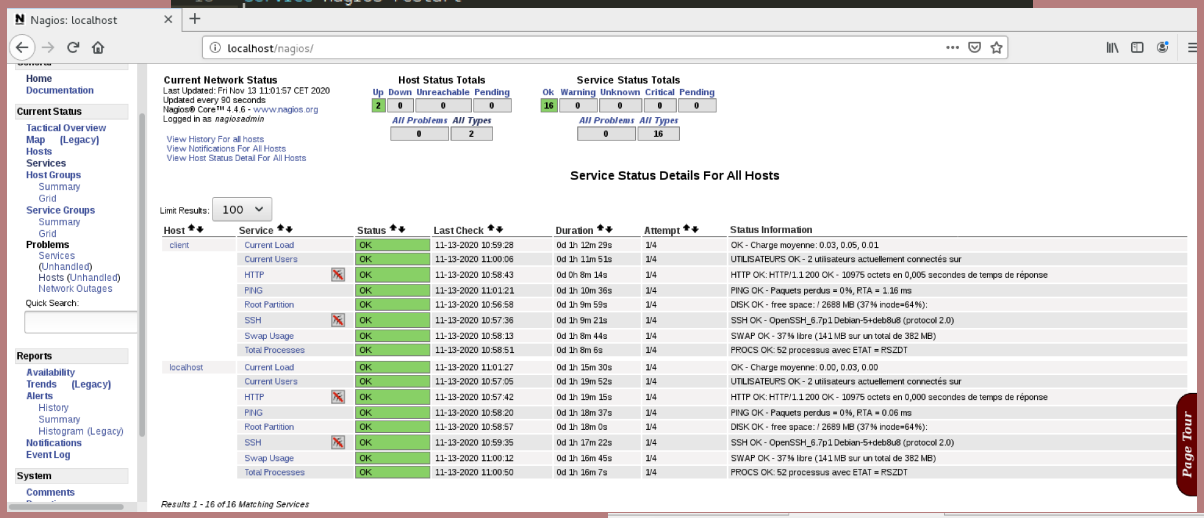
```
#!/bin/bash
apt-get update
yes | apt-get install php5
yes | apt-get install apache2
service apache start
useradd nagios
groupadd nagios
wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz
wget http://www.nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
tar -zxvf nagios-4.4.6.tar.gz
cd nagios-4.4.6
./configure
make all
make install
make install-init
make install-commandmode
make install-config
make install-webconf
echo "root" |htpasswd -c -i /usr/local/nagios/etc/htpasswd.users nagiosadmin
cd ..
tar -zxvf nagios-plugins-2.0.3.tar.gz
cd nagios-plugins-2.0.3
./configure --with-nagios --with-nagios-group=nagios
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
service apache2 restart
service nagios start
yes | apt-get install fcgiwrap
a2enmod cgi
yes | apt-get install nagios-plugins
cp /usr/lib/nagios/plugins/check_* /usr/local/nagios/libexec
clear
echo "instalation terminé"
```

On s'authentifie

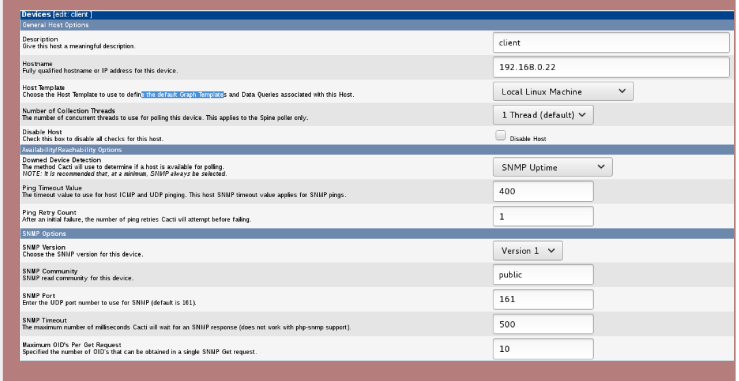



On ajoute la machine Client

```
#!/bin/bash
cd /usr/local/nagios/etc/objects/
cp localhost.cfg client.cfg
chmod 777 client.cfg
sed -i "33,46d" client.cfg #cela correspnd a la partie HOST GROUP DEFINITION
sed -i "s/localhost/client/" client.cfg
sed -i "s/127.0.0.1/192.168.0.22/" client.cfg
cd ..
echo -e "\ncfg_file=/usr/local/nagios/etc/objects/client.cfg">> nagios.cfg
service nagios restart
```




Par la suite j'ai installer cacti ,on ajoute notre client





Sur le client on install et on parametre SNMP