

Table des matières

1. Téléchargement et installation des plugins Nagios.....	1
2. Ping sur les différentes machines.....	2
3. Serveur Web Debian.....	2
4. Poste Windows (10) Client (NRPE)	4
5. Serveur Windows	6

Pour ce TP je serais en binôme avec Lucas LEGER. Nous ferons donc 1 compte rendu pour 2 mais nous ferons les manipulations chacun de notre côté

1. Téléchargement et installation des plugins Nagios

Avant de commencer les différentes commandes demandées dans le TP il faut que nous installions des plugins donnés par Nagios ou Centreon afin de pouvoir effectuer des pings et des requêtes TCP. Pour se faire nous devons télécharger les plugins sur internet et les décompresser sur notre serveur de supervision :

```
yum install wget gcc
cd /tmp
wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
tar -xvf nagios-plugins-2.3.3.tar.gz
cd nagios-plugins-2.3.3
./configure
make
make install
```

Il faut aussi installer des dépendances (certains paquets sont déjà installés de base) :

```
yum install -y gcc glibc glibc-common make gettext automake autoconf wget openssl-devel net-
snmp net-snmp-utils epel-release
yum install -y perl-Net-SNMP
yum install -y postgresql-devel
yum install -y libdbi-devel
yum install -y openldap-devel
yum install -y mariadb-devel mariadb-libs
yum install -y bind-utils
yum install -y samba-client
yum install -y fping
```

```
yum install -y openssh-clients  
yum install -y lm_sensors
```

2. Ping sur les différentes machines

Ping de la machine Windows Server :

```
[root@localhost libexec]# /usr/local/nagios/libexec/check_ping -H 192.168.6.2 -w 3,60% -c 5,80% -p5  
PING OK - Paquets perdus = 0%, RTA = 0.87 ms|rta=0.872000ms;3.000000;5.000000;0.000000  
pl=0%;60;80;0
```

Ping de la machine Windows (10) Client :

```
[root@localhost libexec]# /usr/local/nagios/libexec/check_ping -H 192.168.6.1 -w 3,60% -c 5,80% -p5  
PING OK - Paquets perdus = 0%, RTA = 0.87 ms|rta=0.866000ms;3.000000;5.000000;0.000000  
pl=0%;60;80;0
```

Ping de la machine Linux :

```
[root@localhost libexec]# /usr/local/nagios/libexec/check_ping -H 192.168.7.1 -w 3,60% -c 5,80% -p5  
PING OK - Paquets perdus = 0%, RTA = 0.87 ms|rta=0.869000ms;3.000000;5.000000;0.000000  
pl=0%;60;80;0
```

Nous pouvons aussi vérifier que la commande fonctionne bien en éteignant une machine par exemple :

```
[root@localhost libexec]# /usr/local/nagios/libexec/check_ping -H 192.168.7.1 -w 3,60% -c 5,80% -p5  
CRITICAL - Plugin timed out
```

3. Serveur Web Debian

Vérification du CPU :

Seuil warning à 80% d'utilisation et critique à 90%

```
[root@localhost ~]#I/usr/lib/centreon/plugins//centreon_linux_snmp.pl --plugin=os::linux::  
snmp::plugin --mode=cpu --hostname=192.168.7.1 --snmp-version='2c' --snmp-community='publi  
c' --warning-core='80' --critical-core='90' --verbose  
OK: 1 CPU(s) average usage is 1.00 % - CPU '0' usage : 1.00 % | 'total_cpu_avg'=1.00%;;0;  
100 'cpu'=1.00%;0:80;0:90;0:100  
CPU '0' usage : 1.00 %
```

Vérification de la mémoire :

Seuil warning à 80% d'utilisation et critique à 90%

```
[root@localhost ~]# /usr/lib/centreon/plugins//centreon_linux_snmp.pl --plugin=os::linux::snmp::plugin --mode=memory --hostname=192.168.7.1 --snmp-version='2c' --snmp-community='public' --warning-usage='80' --critical-usage='90' --verbose
OK: Ram Total: 3.84 GB Used (-buffers/cache): 481.85 MB (12.26%) Free: 3.37 GB (87.74%), Buffer: 30.30 MB, Cached: 415.88 MB, Shared: 8.32 MB | 'used'=505253888B;;;0;4122542080 'free'=3617288192B;;;0;4122542080 'used_prct'=12.26%;0;80;0;90;0;100 'buffer'=31772672B;;;0; 'cached'=436084736B;;;0; 'shared'=8728576B;;;0;
```

Vérification du storage :

Seuil warning à 80% d'occupation et critique à 90%

```
[root@localhost ~]# /usr/lib/centreon/plugins//centreon_linux_snmp.pl --plugin=os::linux::snmp::plugin --mode=storage --hostname=192.168.7.1 --snmp-version='2c' --snmp-community='public' --warning-usage='80' --critical-usage='90' --verbose
OK: All storages are ok | 'count'=6;;;0; 'used_run'=1196032B;0;329803366;0;371028787;0;412254208 'used_/'=4901646336B;0;20185533644;0;22708725350;0;25231917056 'used_dev/shm'=0B;0;1649016832;0;1855143936;0;2061271040 'used_run/lock'=4096B;0;4194304;0;4718592;0;5242880 'used_run/user/116'=90112B;0;329803366;0;371028787;0;412254208 'used_run/user/1000'=57344B;0;329803366;0;371028787;0;412254208
Storage '/run' Usage Total: 393.16 MB Used: 1.14 MB (0.29%) Free: 392.02 MB (99.71%)
Storage '/' Usage Total: 23.50 GB Used: 4.57 GB (19.43%) Free: 18.93 GB (80.57%)
Storage '/dev/shm' Usage Total: 1.92 GB Used: 0.00 B (0.00%) Free: 1.92 GB (100.00%)
Storage '/run/lock' Usage Total: 5.00 MB Used: 4.00 KB (0.08%) Free: 5.00 MB (99.92%)
Storage '/run/user/116' Usage Total: 393.16 MB Used: 88.00 KB (0.02%) Free: 393.07 MB (99.98%)
Storage '/run/user/1000' Usage Total: 393.16 MB Used: 56.00 KB (0.01%) Free: 393.10 MB (99.99%)
```

Vérification du fonctionnement d'Apache via TCP :

Le but est de voir si Apache fonctionne en vérifiant si le port 80 est ouvert ou fermé.

```
[root@localhost ~]# /usr/lib64/nagios/plugins/check_tcp -H 192.168.7.1 -p 80
connect to address 192.168.7.1 and port 80: Connection refused
[root@localhost ~]# /usr/lib64/nagios/plugins/check_tcp -H 192.168.7.1 -p 80
TCP OK - 0.001 second response time on 192.168.7.1 port 80|time=0.000732s;;;0.000000;10.000000
```

On peut voir que quand le service est éteint le port est fermé. Cependant si le service fonctionne alors nous pourrions voir le port ouvert.

4. Poste Windows (10) Client (NRPE)

Pour les différentes commandes en NRPE nous pouvons trouver les infos sur le site suivant :

<https://docs.nslclient.org/reference/>

Il faut aller dans l'onglet références -> Check commands et dedans nous avons les différents modules installés avec NSClient++

Dans ces modules nous pouvons trouver les commandes à passer ci-dessous (surligné en vert) pour vérifier ce que l'on a besoin sur la machine distante

En cliquant sur la commande on peut accéder à des exemples d'utilisation avec des syntaxes

Vérification du stockage sur le disque C en commande NRPE :

Seuil de Warning à 80% d'occupation

Seuil Critique à 90% d'occupation

```
[root@localhost libexec]# /usr/lib64/nagios/plugins/check_centreon_nrpe3 -H 192.168.6.1 -c  
check_drivesize -a "warn=free<20%" "crit=free<10%" drive=c  
CHECK_NRPE: Invalid packet version received from server.  
OK All 1 drive(s) are ok|c: free=7.60047GB;3.88743;1.94371;0;19.43718 'c: free %'=39%;20;10;0;100
```

Nous pouvons tester le bon fonctionnement de la commande en mettant un seuil de warning à 20% par exemple :

```
[root@localhost libexec]# /usr/lib64/nagios/plugins/check_centreon_nrpe3 -H 192.168.6.1 -c  
check_drivesize -a "warn=free<80%" "crit=free<10%" drive=c  
CHECK_NRPE: Invalid packet version received from server.  
WARNING c:: 11.838GB/19.437GB used|c: free=7.59949GB;15.54974;1.94371;0;19.43718 'c: free  
%=39%;80;10;0;100
```

Vérification de la quantité de mémoire en commande NRPE :

Seuil de Warning à 80% d'occupation

Seuil Critique à 90% d'occupation

```
[root@localhost libexec]# /usr/lib64/nagios/plugins/check_centreon_nrpe3 -H 192.168.6.1 -c  
check_memory -a "warn=free < 20%" "crit=free < 10%"  
CHECK_NRPE: Invalid packet version received from server.  
OK: committed = 1.343GB, physical = 1.184GB|committed=1.78181GB;0.62491;0.31245;0;3.12456  
'committed %'=57%;20;10;0;100 'physical'=835.28906MB;409.51015;204.75507;0;2047.55078 'physical  
%=41%;20;10;0;100
```

Vérification de la charge CPU en commande NRPE :

Seuil de Warning à 80% d'occupation

Seuil Critique à 90% d'occupation

```
[root@localhost libexec]# /usr/lib64/nagios/plugins/check_centreon_nrpe3 -H 192.168.6.1 -c  
check_cpu -a filter=none "warn=load > 80" "crit=load > 90"  
  
CHECK_NRPE: Invalid packet version received from server.  
  
OK: CPU load is ok.'core 0 5m'=0%;80;90 'total 5m'=0%;80;90 'core 0 1m'=0%;80;90 'total 1m'=0%;80;90  
'core 0 5s'=1%;80;90 'total 5s'=1%;80;90
```

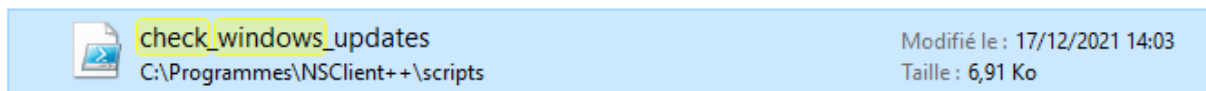
Vérification des mises à jour en commande NRPE :

Il n'existe pas de plugin permettant de vérifier si des mises à jour sont disponibles. Il faut donc télécharger ou créer un script qui permettra de répondre aux attendus

Pour se faire nous nous sommes aidés du site suivant :

<https://exchange.nagios.org/directory/Plugins/Operating-Systems/Windows-NRPE/Check-Windows-Updates-using-Powershell/details>

Sur ce site nous devons télécharger le script donné et le déplacer dans le répertoire "scripts" de notre NSClient :



Une fois le script mis dans le bon répertoire il faut lancer un Powershell en mode administrateur et lancer la commande suivante pour passer la sécurité :

```
set-executionpolicy bypass
```

Il faut vérifier dans le nsclient.ini que le module "CheckExternalScripts" est bien activé :

```
CheckExternalScripts = enabled
```

Ensuite dans le même fichier nsclient.ini y ajouter les lignes suivantes :

```
[/settings/external scripts/scripts]  
check_updates=cmd /c echo scripts\check_windows_updates.ps1; exit $LastExitCode /  
powershell.exe -command -
```

La 1^{ère} ligne fait le lien vers l'emplacement de notre script et la 2^{ème} ligne permet d'associer une commande au lancement du script

Maintenant que tout est bien configuré il faut redémarrer le service nsclient dans un cmd en mode administrateur :

```
cd "%Program Files%\NSClient++"  
net stop nscp && net start nscp
```

Nous pouvons maintenant passer la commande de check_update en mode NRPE :

```
[root@localhost libexec]# /usr/lib64/nagios/plugins/check_centreon_nrpe3 -H 192.168.6.1 -c  
check_updates  
  
CHECK_NRPE: Invalid packet version received from server.  
  
Updates: 3 critical, 1 optional  
  
Outil de suppression de logiciels malveillants Windows x64 - v5.96 (KB890830)  
2021-11 Mise à jour pour Windows 10 Version 21H2 sur systèmes x64 (KB4023057)  
2021-12 Mise à jour cumulative pour Windows 10 Version 21H2 pour les systèmes x64 (KB5008212)  
/critical'=3;0;0
```

5. Serveur Windows

Nous allons désormais faire quelques tests sur notre machine Windows Server.

Vérification du CPU :

```
[root@localhost plugins]# /usr/lib/centreon/plugins//centreon_windows_snmp.pl --plugin=os:  
:windows::snmp::plugin --mode=cpu --hostname=192.168.7.1 --snmp-community=public --snmp-ve  
rsion=2 --warning-average=80 --critical-average=90  
OK: 1 CPU(s) average usage is 1.00 % - CPU '0' usage : 1.00 % | 'total_cpu_avg'=1.00%;0:80  
;0:90;0;100 'cpu'=1.00%;;0;100
```

Vérification de la mémoire :

```
[root@localhost plugins]# /usr/lib/centreon/plugins//centreon_windows_snmp.pl --plugin=os:  
:windows::snmp::plugin --mode=memory --hostname=192.168.7.1 --snmp-community=public --snmp  
-version=2 --warning-memory=80 --critical-memory=90  
OK: Ram Total: 3.84GB Used: 1.31GB (34.07%) Free: 2.53GB (65.93%) | 'used'=1404485632B;0:3  
298033664;0:3710287872;0;4122542080
```

Vérification du storage :

```
[root@localhost plugins]# /usr/lib/centreon/plugins//centreon_windows_snmp.pl --plugin=os:  
:windows::snmp::plugin --mode=storage --name="C:" --hostname=192.168.7.1 --snmp-community=  
public --snmp-version=2 --warning-usage=80 --critical-usage=90  
OK: All storages are ok | 'count'=5;;0; 'used_/run'=1183744B;0:329803366;0:371028787;0:41  
2254208 'used_/'=4901830656B;0:20185533644;0:22708725350;0:25231917056 'used_/dev/shm'=0B;  
0:1649016832;0:1855143936;0:2061271040 'used_/run/lock'=4096B;0:4194304;0:4718592;0:524288  
0 'used_/run/user/1000'=102400B;0:329803366;0:371028787;0:412254208
```

Vérification du fonctionnement du IIS sur le port 80 :

```
[root@localhost plugins]# /usr/lib64/nagios/plugins/check_tcp -H 192.168.6.1 -p 80  
TCP OK - 0,001 second response time on 192.168.6.1 port 80|time=0,001332s;;0,000000;10,00  
0000
```