Monitoring d’infrastructure : Eyes Of Network

Monitoring d’infrastructure à l'aide de Eyes Of Network, basé sur Nagios Core.

- Eyes Of Network

Eyes Of Network

Introduction

Eyes Of Network est une solution Open Source réunissant de manière pragmatique
les processus ITIL et l'interface technologique permettant leur application. C'est une solution de supervision d'infrastructure comme Nagios. Celle-ci regroupe différentes solutions : Cacti, Nagios, Thruk, Nagvis ou encore Weathermap.

C'est une solution à base de Nagios. La configuration s'effectue uniquement en GUI comparé à Nagios qui s'effectue en ligne de commande. Les modifications via GUI vont faire pour nous les modifications en ligne de commande.





Développement

Cahier des charges

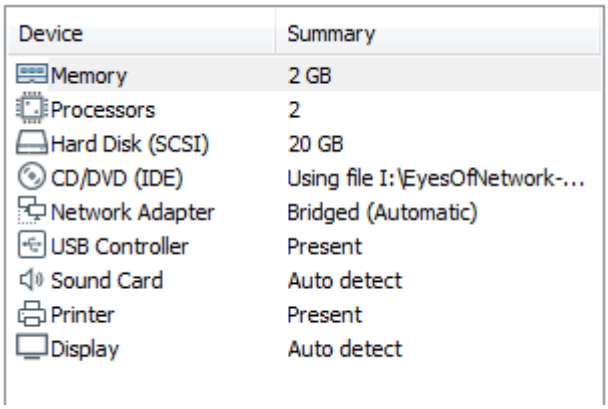
Pour ce TP, le but est de superviser de nombreux appareils : machines linux & Windows, Switch, Vidéoprojecteur, Routeur internet, imprimantes...

Ce service doit resté disponible, avec un accès réservé à l'administrateur, pour éviter tout accès non autorisé. En effet, on a à disposition ici de nombreuses informations sur l'infrastructure.

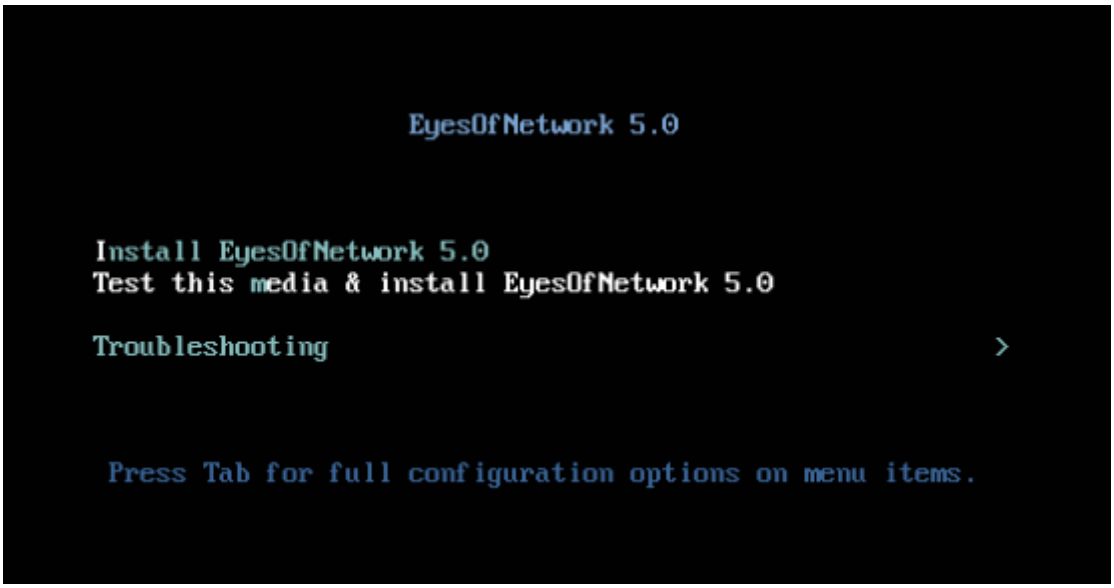
Répartition du travail

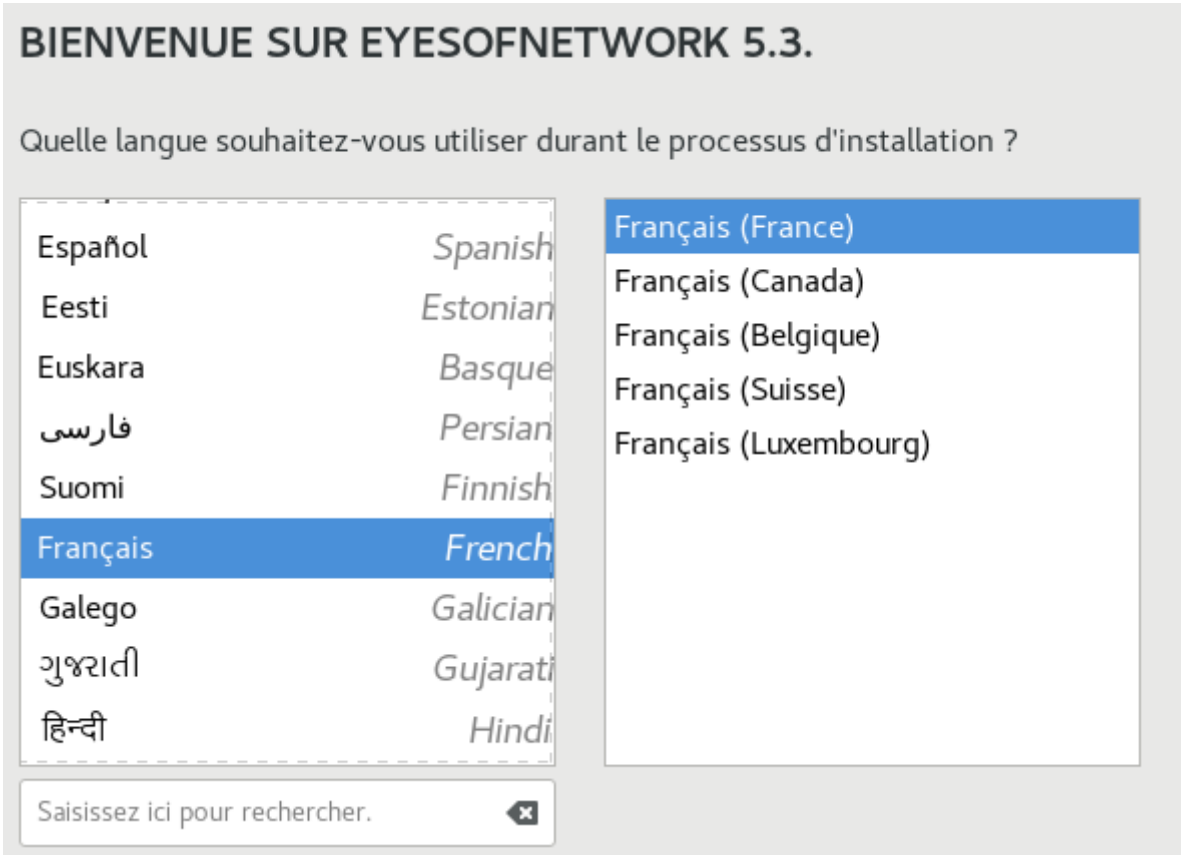
Ce projet a été réalisé à deux. Les tâches ont été divisées : La recherche de la méthode de supervision, configuration des équipements en SNMP, sécurisation...

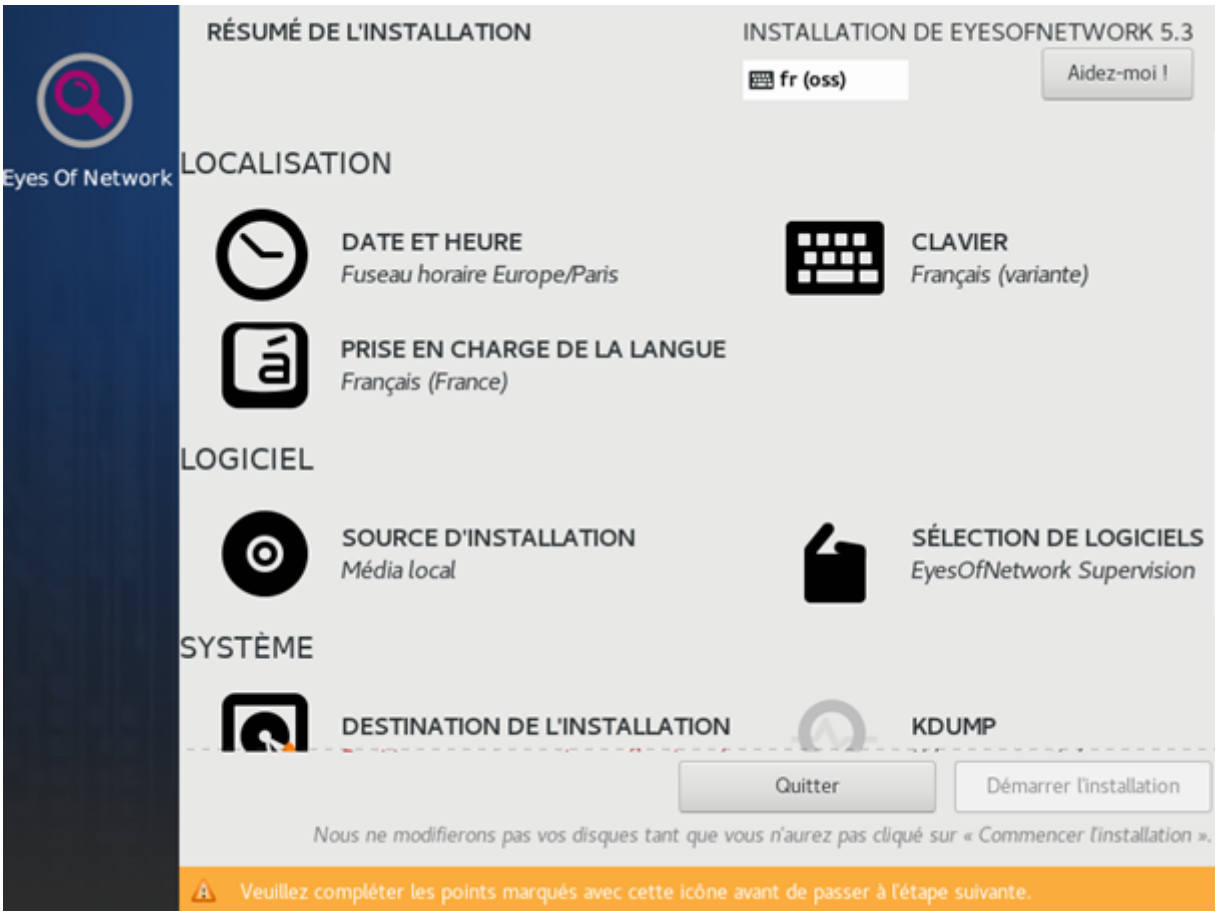
Configuration de la machine virtuelle



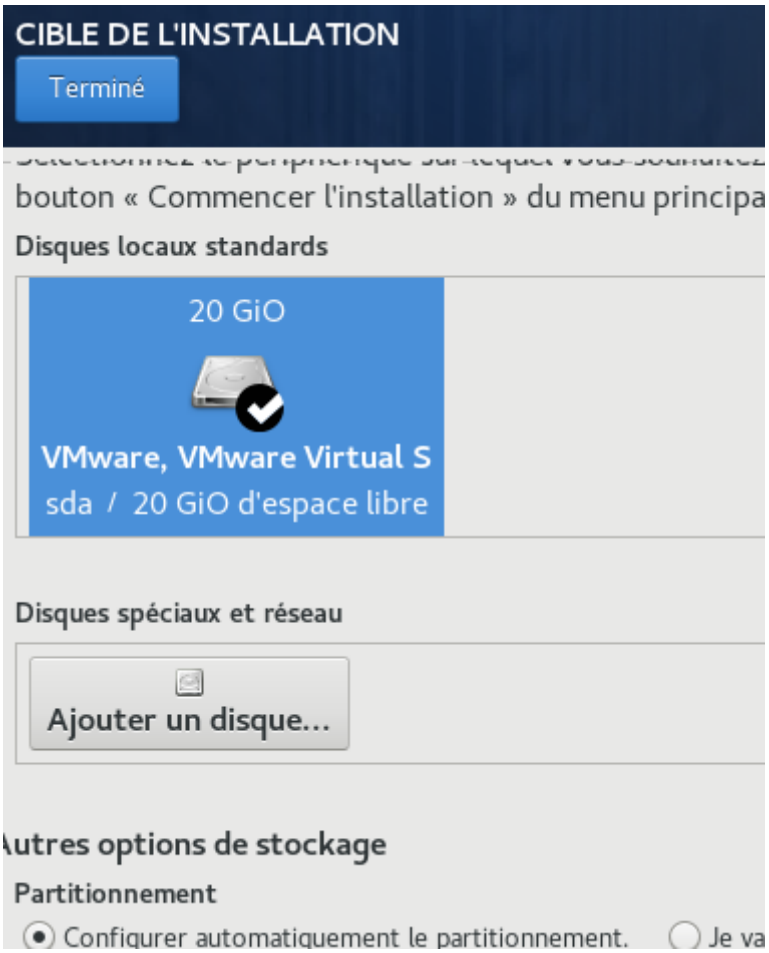
Installation de EoN



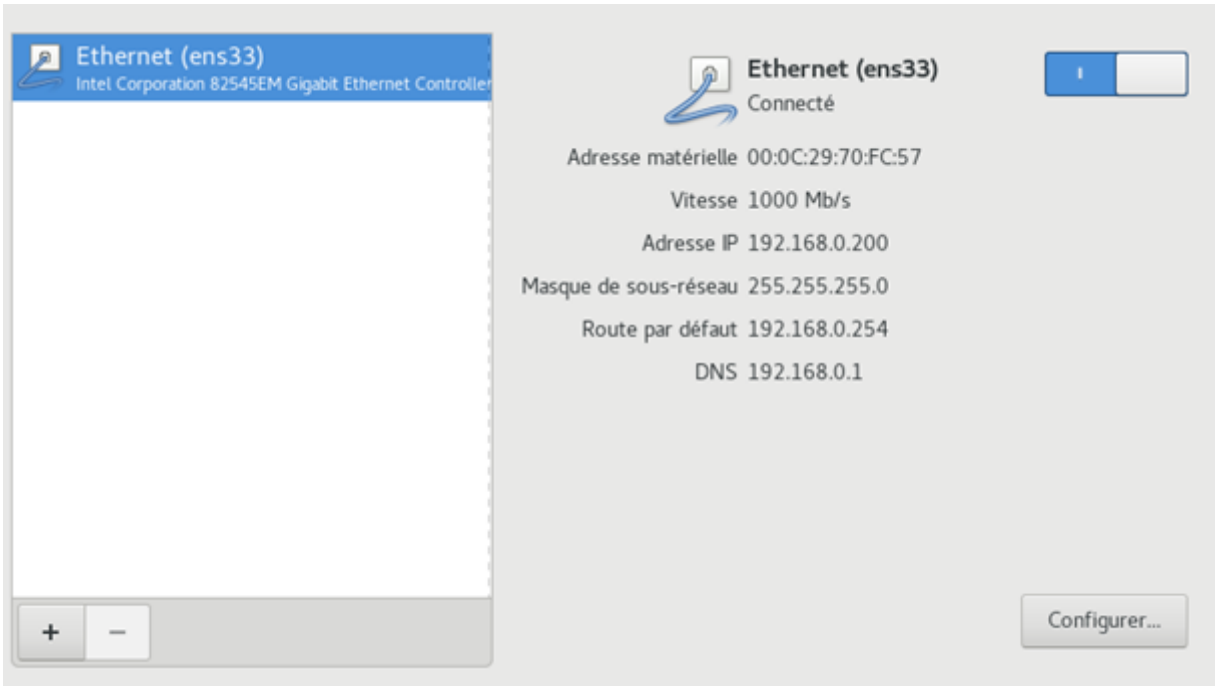


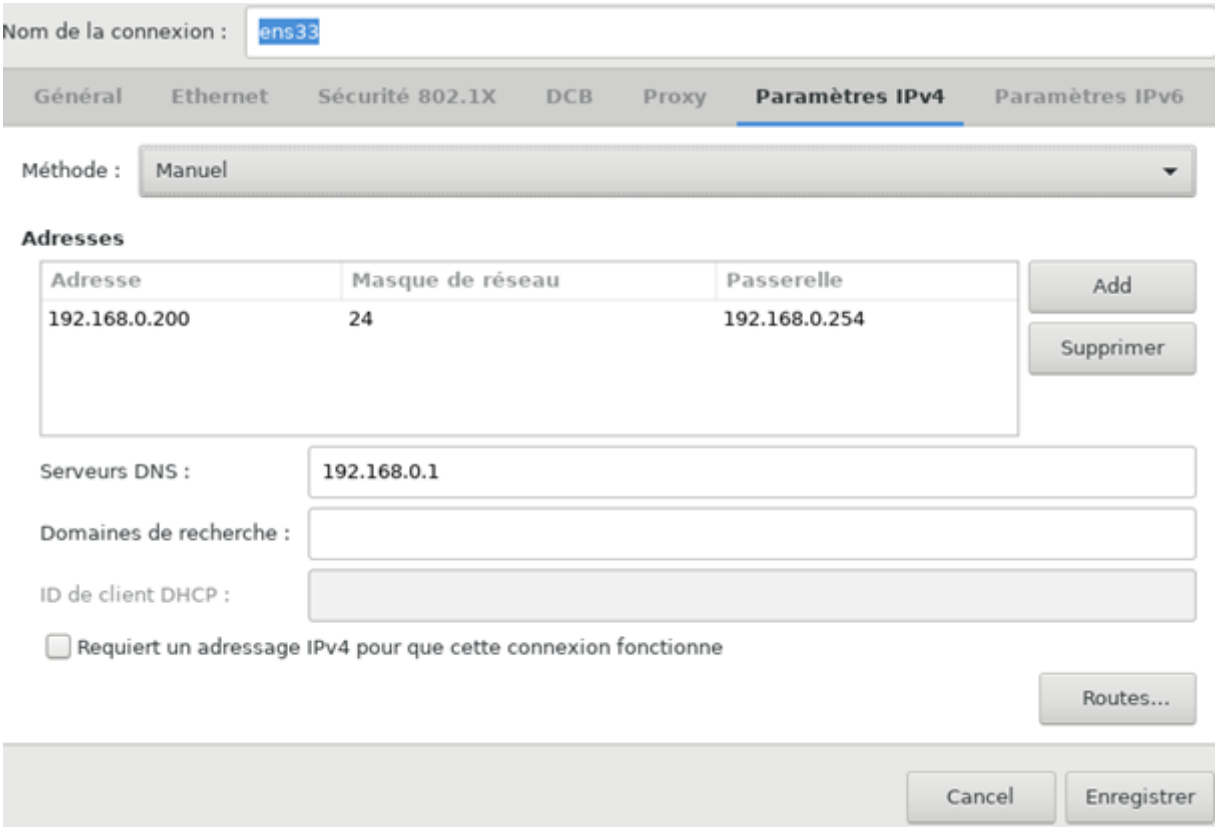


Pour la destination de l'installation :



On paramètre bien le réseau :



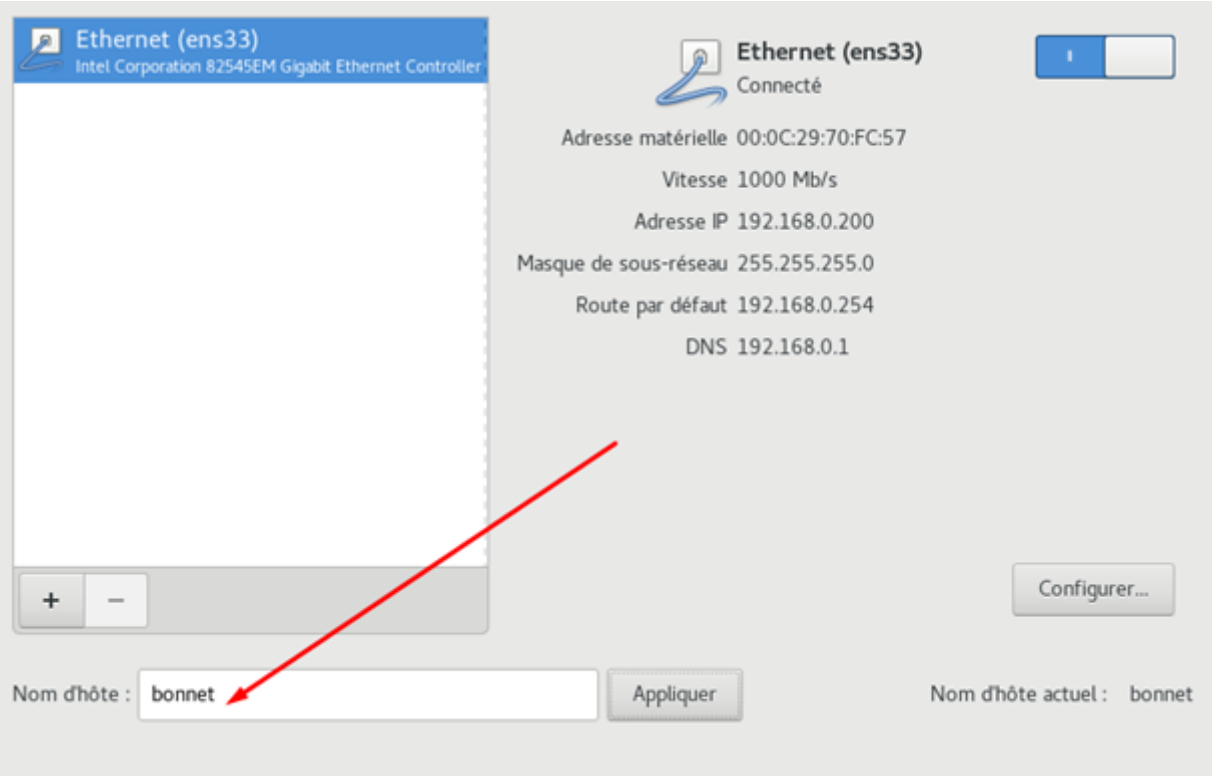


On coche cette case :



On n’oublie pas de l’activer en haut à droite.

On met le nom d’hôte



On se rend dans Sélection de logiciels :



On prend ce qu'on a besoin.

On clique sur démarrer.



On défini un mot de passe.

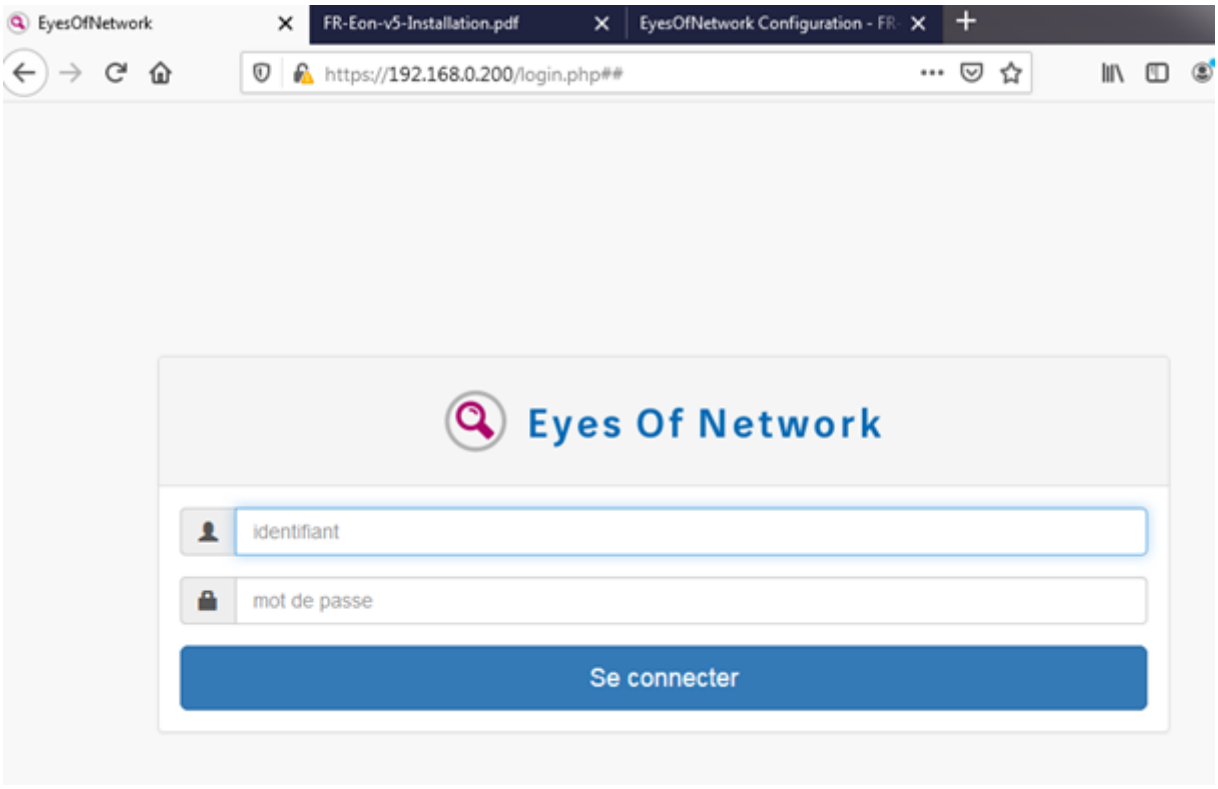


Fini !

Installation de Nano

sudo yum –y install nano

Accès en GUI via un navigateur web



Le compte par défaut est admin:admin.

Changement du nom de communauté SNMP

`nano/etc/snmp/snmpd.conf`

```
  GNU nano 2.3.1         Fichier : /etc/snmp/snmpd.conf                Modi

# the agent so that you can change the community names, and give
# yourself write access to the mib tree as well.
#
# For more information, read the FAQ as well as the snmpd.conf(5)
# manual page.

####
# First, map the community name "EyesOfNetwork" into a "security name"

#       sec.name  source          community
com2sec notConfigUser  default       BonnetSupervision

####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
group   notConfigGroup v1           notConfigUser
group   notConfigGroup v2c           notConfigUser
```

```
systemctl restart snmpd
```

Ensuite, on fait de même dans snmptrapd.conf.

```
nano /etc/snmp/snmptrapd.conf
```

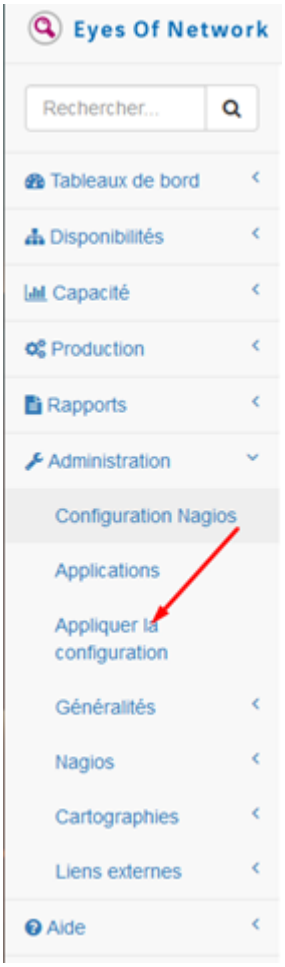
```
ignoreauthfailure yes
authCommunity log,execute,net BonnetSupervision
traphandle default /srv/eyesofnetwork/snmptt/bin/snmptthandler
```

```
systemctl restart snmptrapd
```

Dans l'interface web, Administration – Configuration Nagios – Nagios Resources

On modifie la variable *$user2$* par le nom de la communauté.

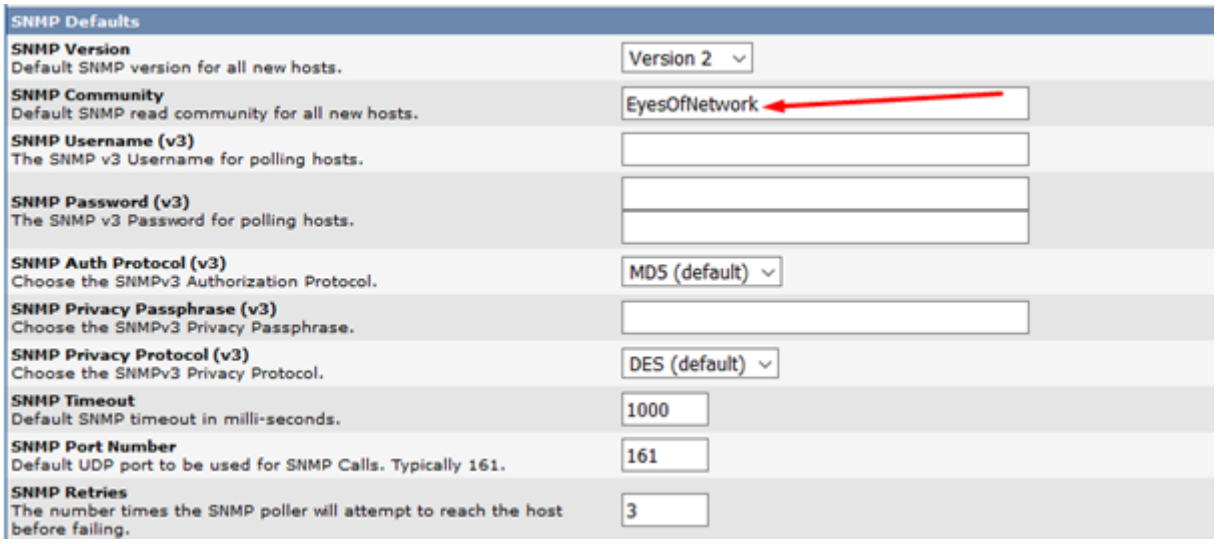
On clique sur « *Update Ressource Configuration* » puis on applique.



On restart nagios.

On va dans Admin – Lien externes – Cacti et dans settings.



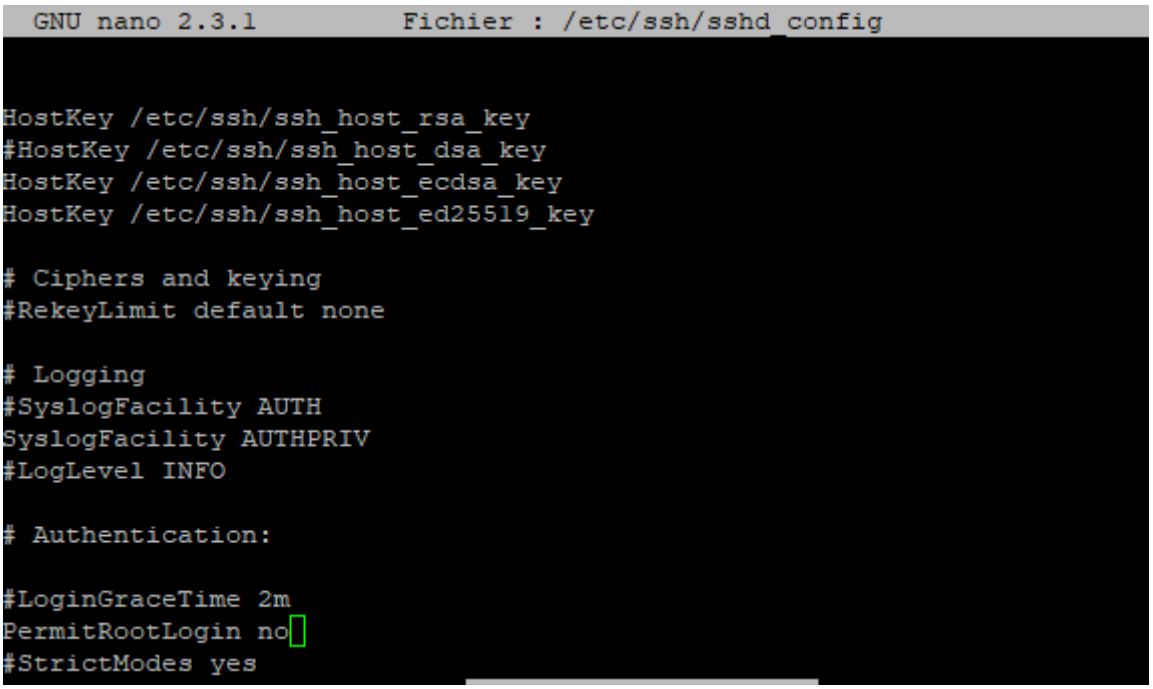


On remplace par le nom de communauté puis on enregistre.

Sécurisation

On supprime l’accès root direct en SSH.

nano /etc/ssh/sshd_config



On change la ligne *#PermitRootLogin yes* par « *PermitRootLogin no* ».

```
systemctl restart sshd
```

On crée alors un compte de maintenance :

```
useradd maintenance -g wheel
passwd maintenance
```

(Ici, le groupe wheel est l'équivalent de sudo)

En se connectant via notre utilisateur créé, on peut passer en root en rentrant « su - ».

Configuration du rsyslog

Par défaut Cacti n’affiche que les logs locaux. On modifie rsyslog.conf

```
nano /etc/rsyslog.conf
```

Sous la ligne *$ModLoad imuxsock*, on ajoute :

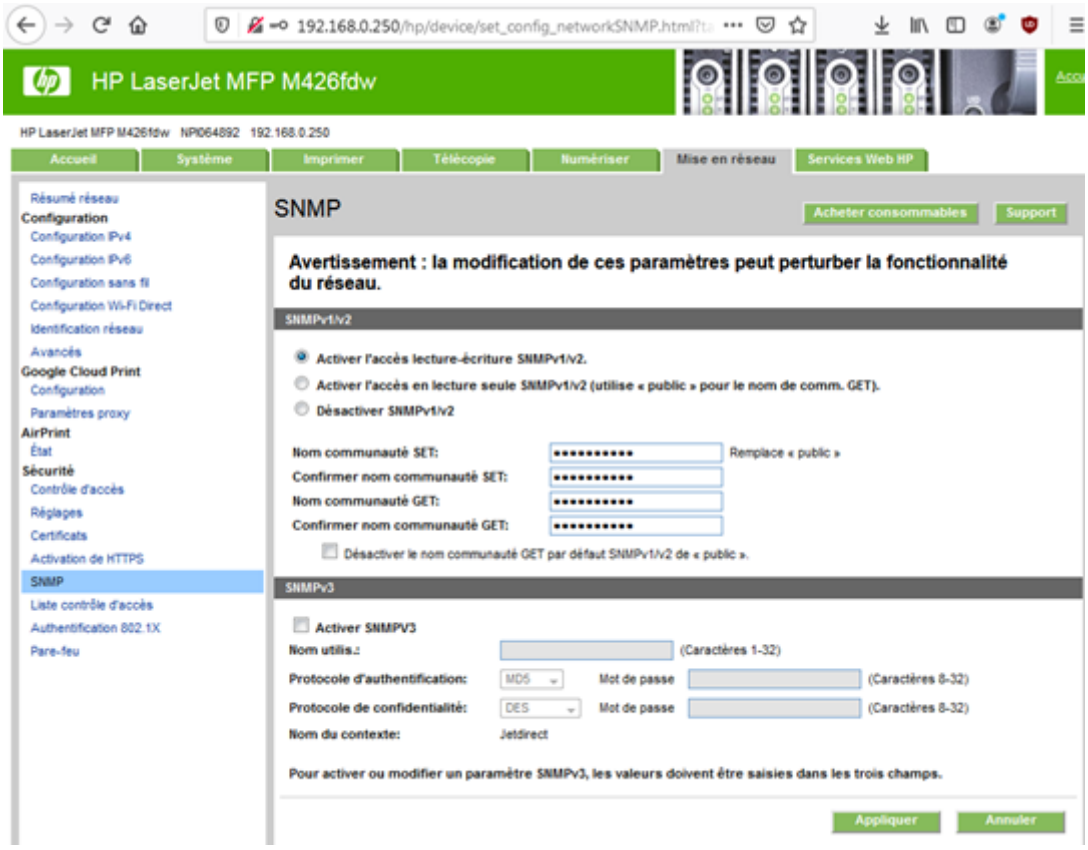
> #Provides UDP syslog reception
>
> *$ModLoad imudp*
>
> *$UDPServerRun 514*
>
> *#Provides TCP syslog reception*
>
> *$ModLoad imtcp*
>
> *$InputTCPServerRun 514*

On redémarre rsyslog.

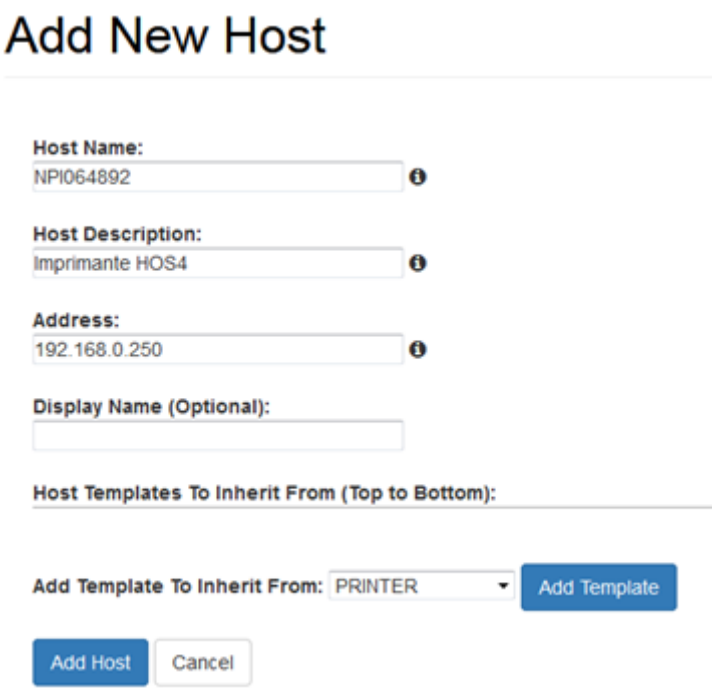
```
systemctl restart rsyslog
```

Monitoring

Monitoring d’une imprimante HP



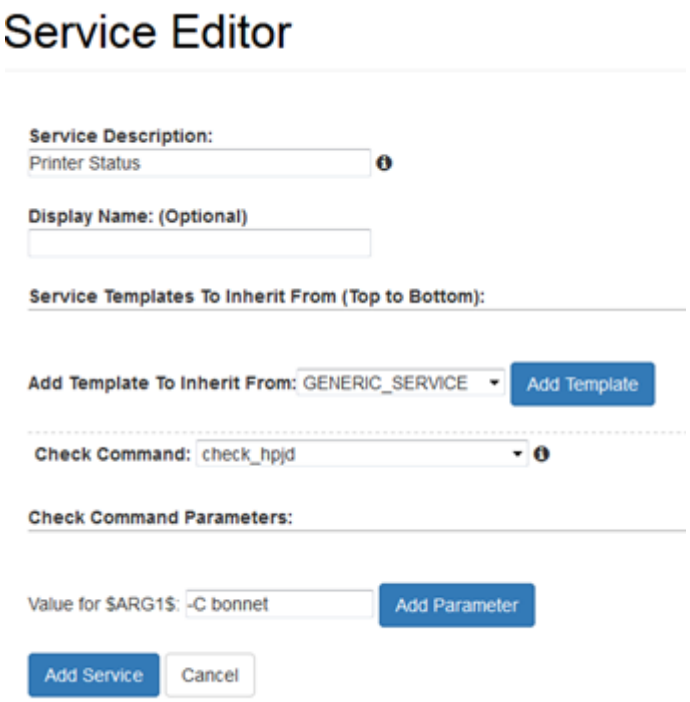
Configuration Nagios, Equipements, Ajouter



Dans Template, on choisit Printer.

On se rend aussi dans Services puis on créer un service.

On choisit le check_hpjd et generic service

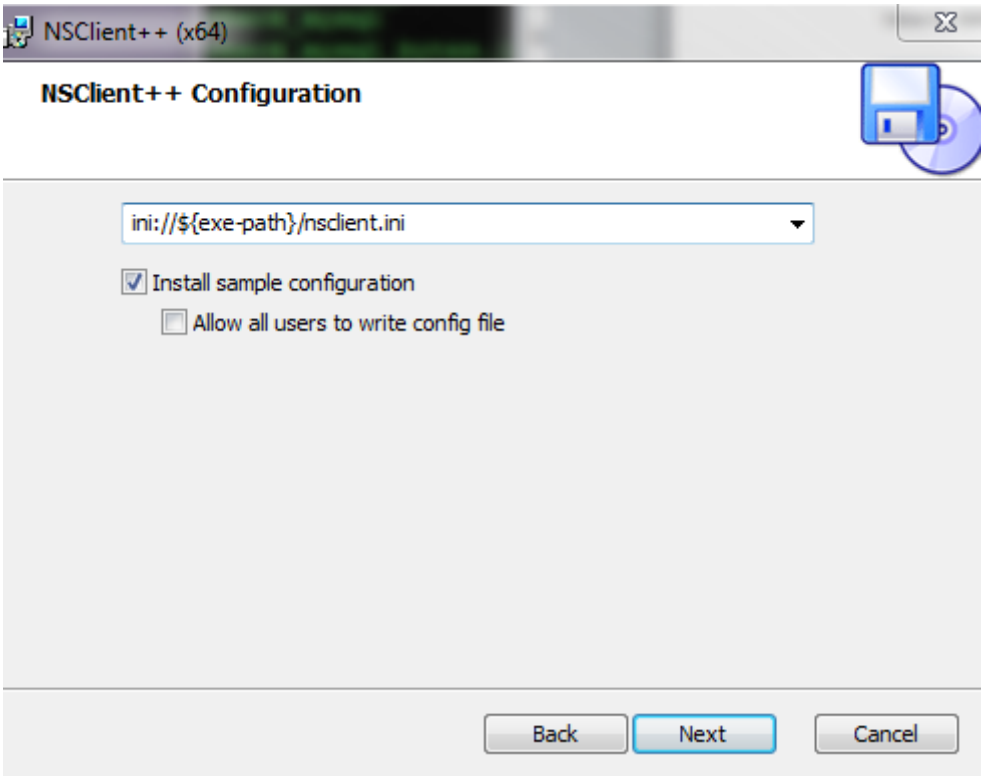


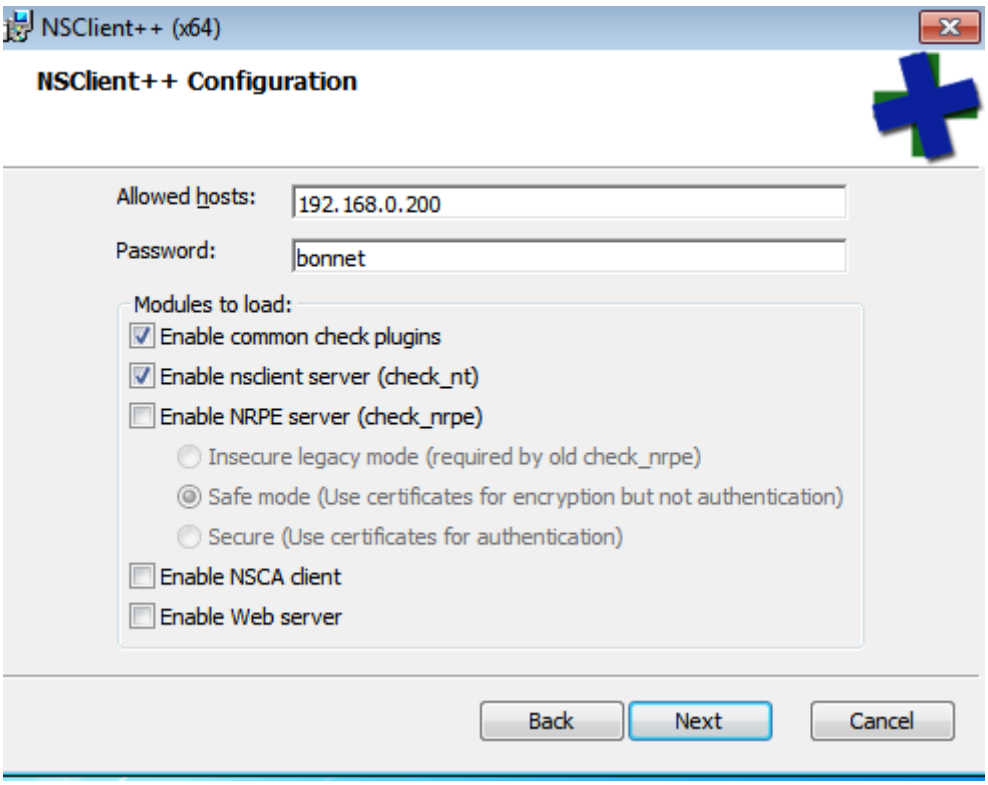
On met la communauté défini précédemment.

Monitoring d’un hôte Windows

https://sourceforge.net/projects/nscplus/files/nscplus/

On télécharge et installe nsclient++ sur notre machine windows que l’on souhaite superviser.

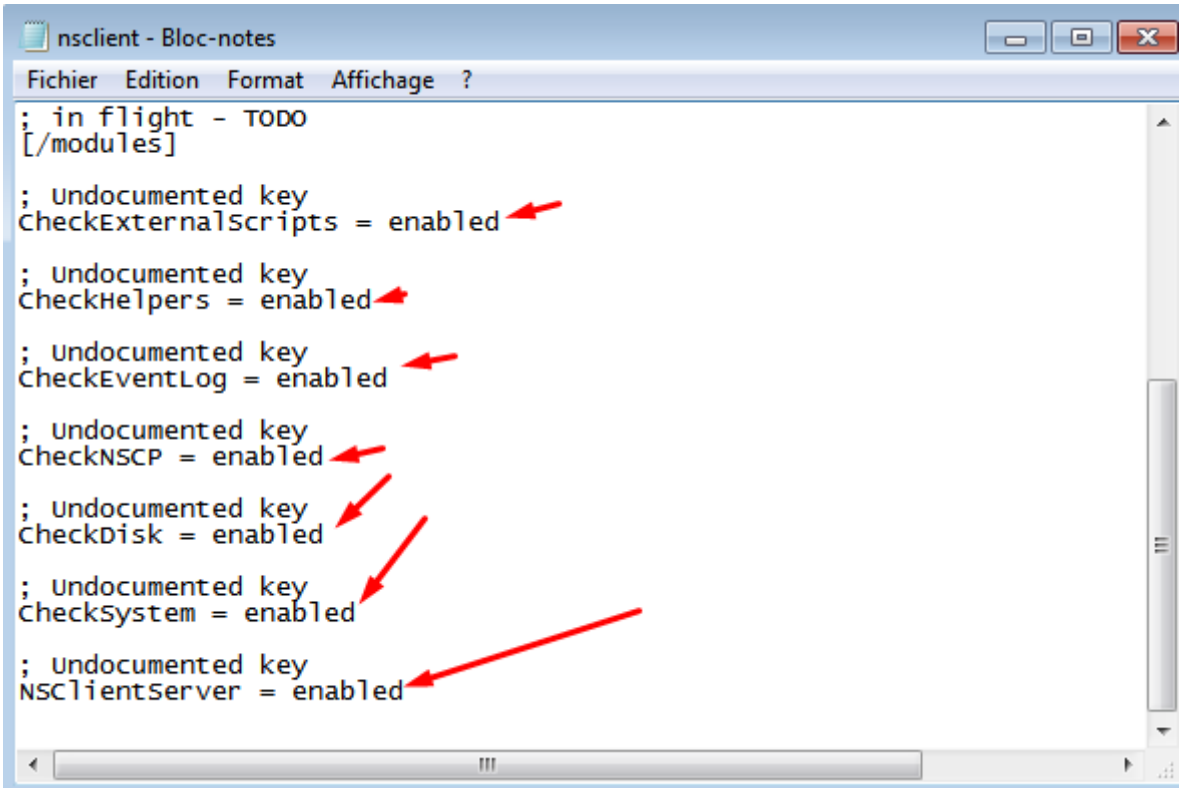




On rentre l'ip du serveur Nagios.

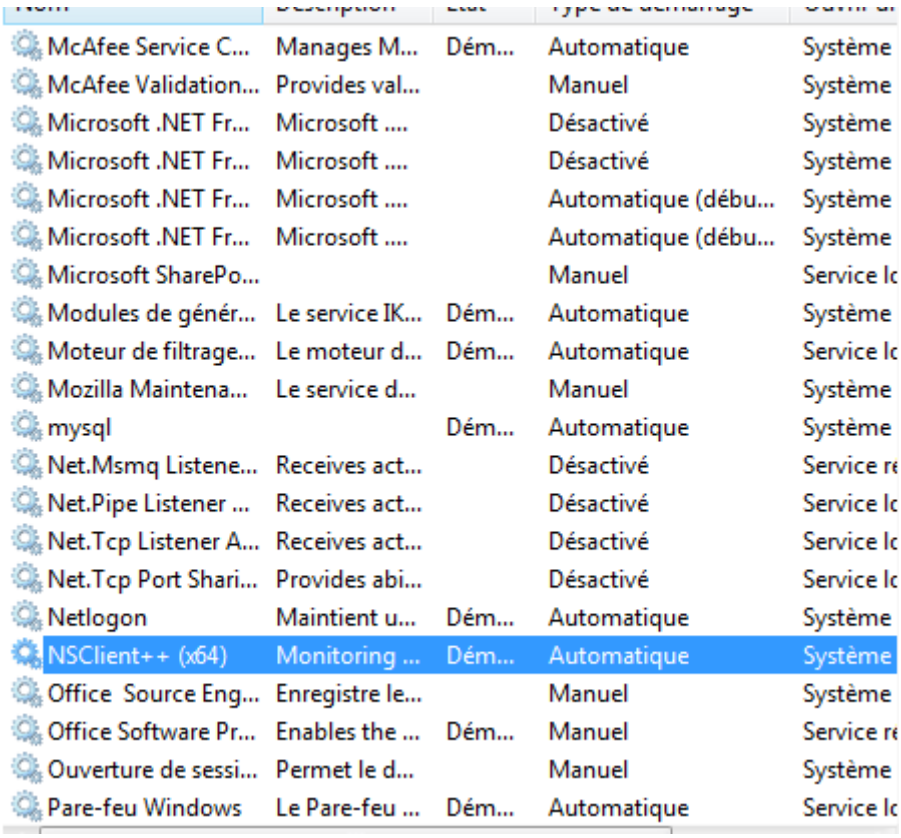
On installe.

On se rend dans le dossier d'installation et on modifie le fichier nsclient.ini.

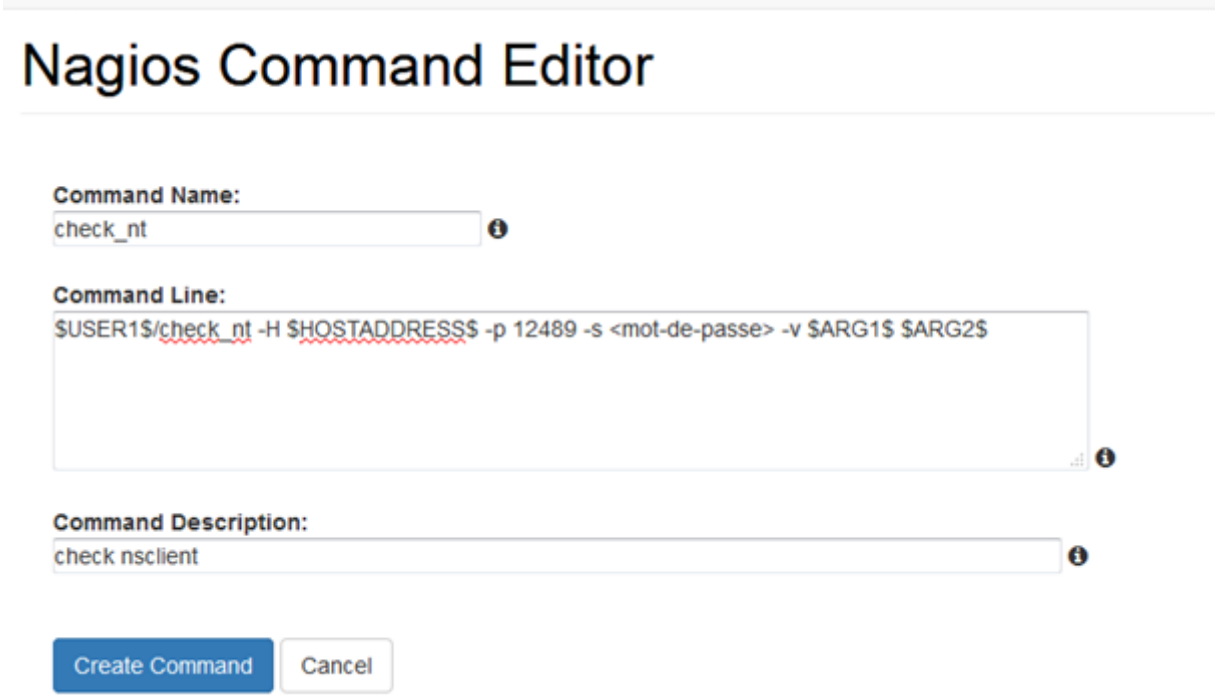


On redémarre.

On vérifie dans services.msc si le service nsclient++ est bien présent et démarré.

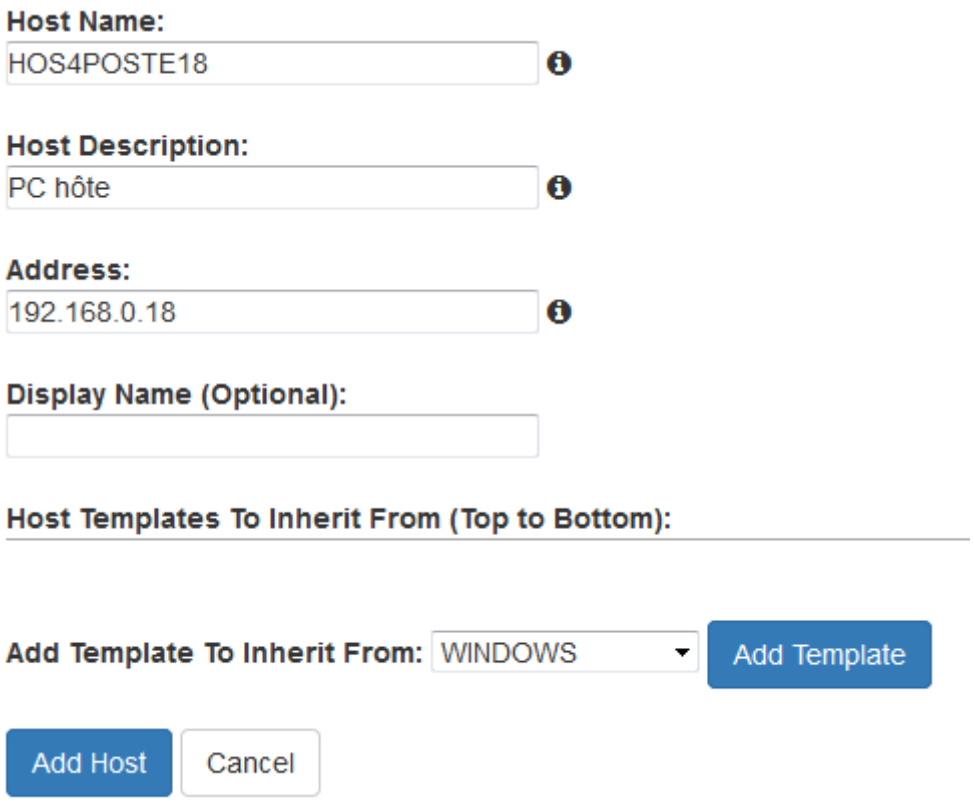


On se rend ensuite dans Eyes Of Network, Administration et Configuration Nagios > Commandes.
On ajoute une commande check_nt

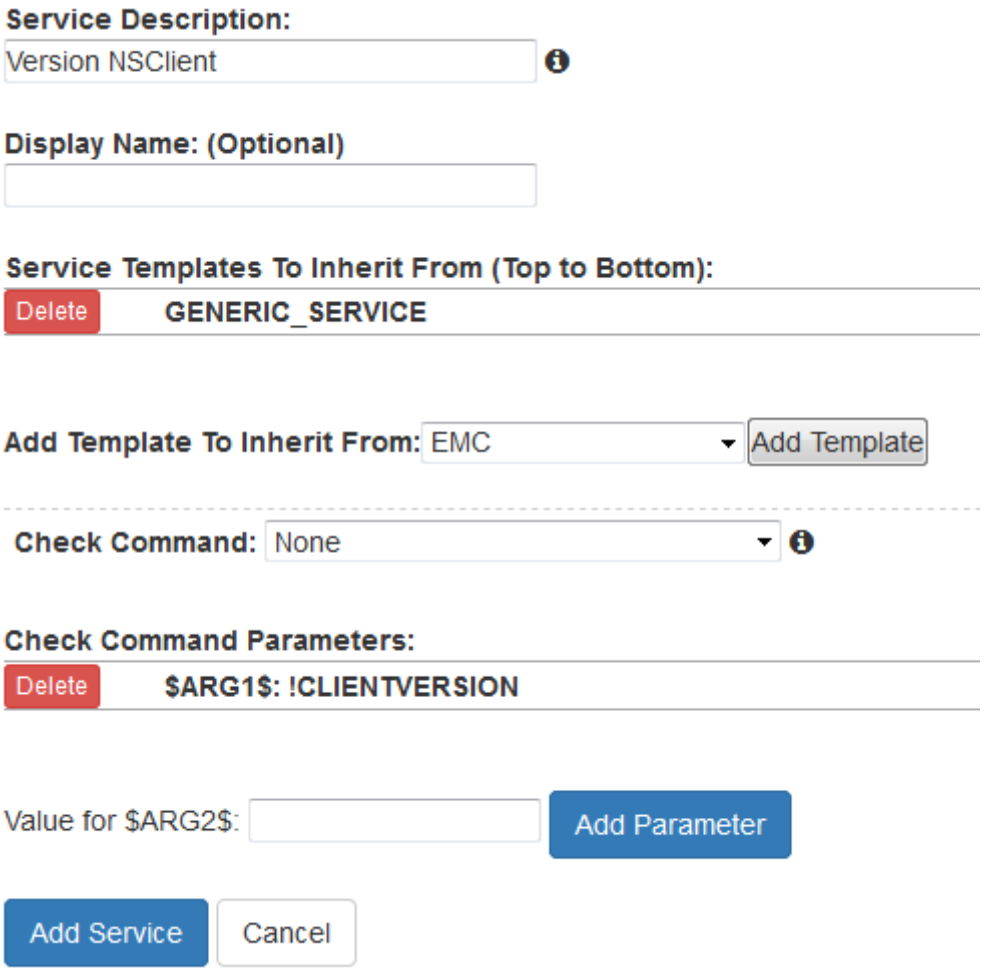


On remplace <mot-de-passe> par le mdp rentré dans NSClient.

Equipements > Ajouter



On ajoute ensuite des services.

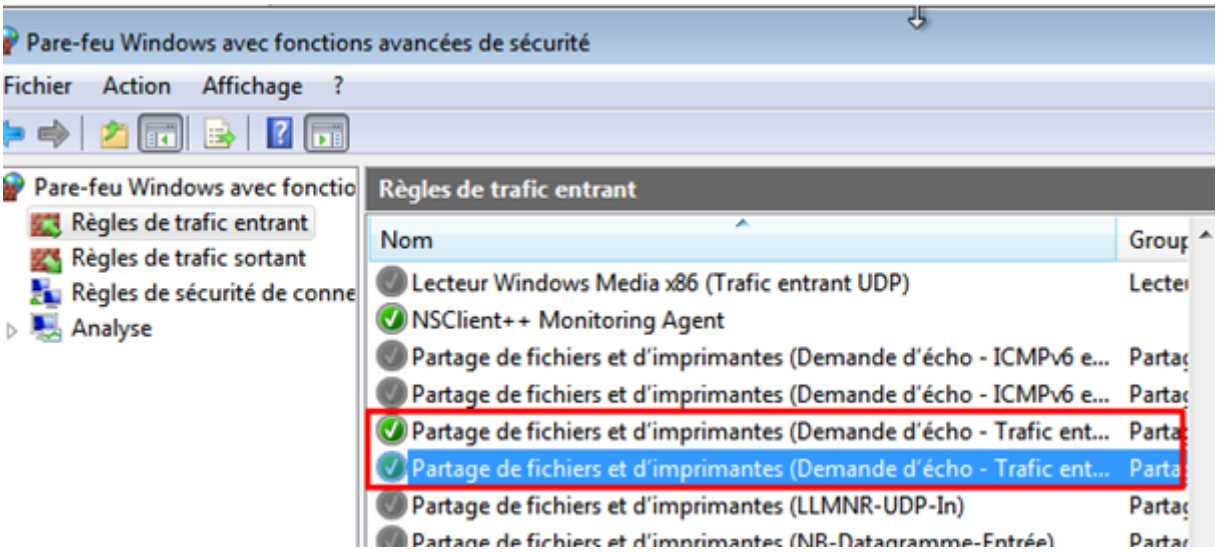


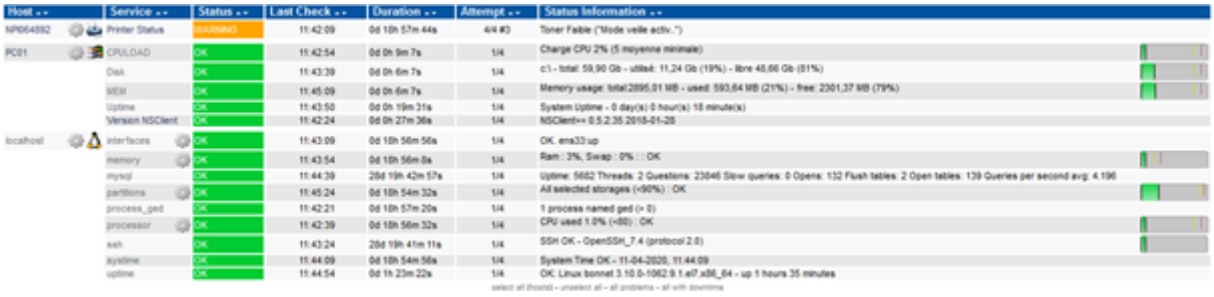
On fait la meme chose pour ce que l'on veut monitorer :

- CLIENTVERSION
- UPTIME

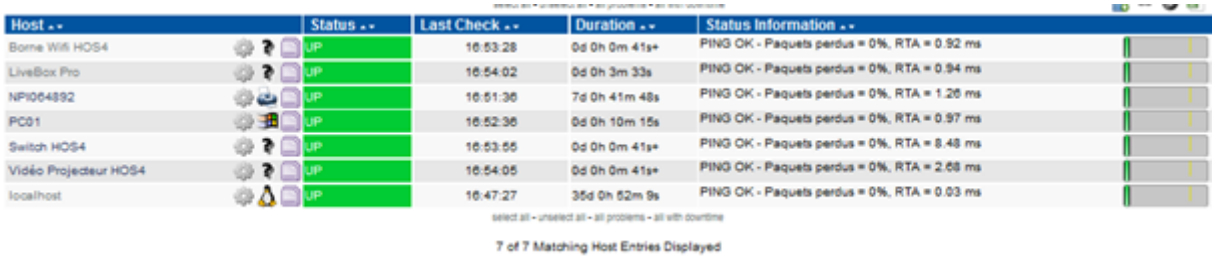
```
- CPULOAD!-l 5,80,90
- MEMUSE!-w 80 -c 90
- USEDDISKSPACE!-l c -w 80 -c 90
- SERVICESTATE!-d SHOWALL -l W3SVC
- PROCSTATE!-d SHOWALL -l Explorer.exe
```

Si l'hôte est considéré comme "down" :





Pour avoir la réponse PING d'autres équipements, on ajoute un équipement et on rentre l'ip à chaque fois. On applique.



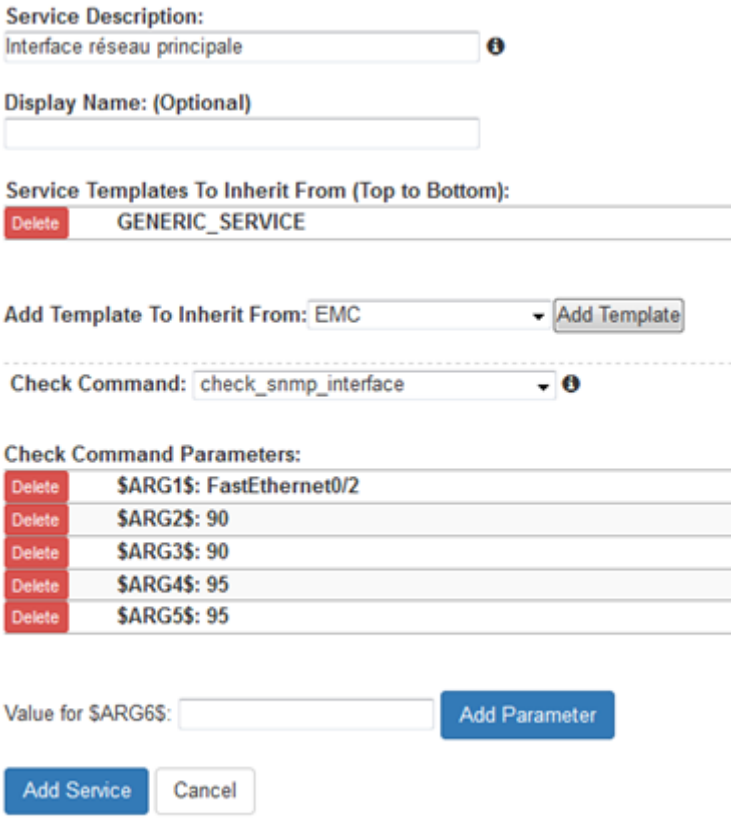
Monitoring d'un switch cisco

On ajoute l'hote puis cisco en template



```
snmp-server community public RO
snmp-server community <public> RO
snmp-server community bonnet RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstar
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-fail-vlan no-g
est-vlan
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps power-ethernet police
 --More--
```

On ajoute un service check_snmp_interface.



Si on a un unknown, il faut enlever l’argument « -k » dans la commande.