

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.



Nagios®

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.

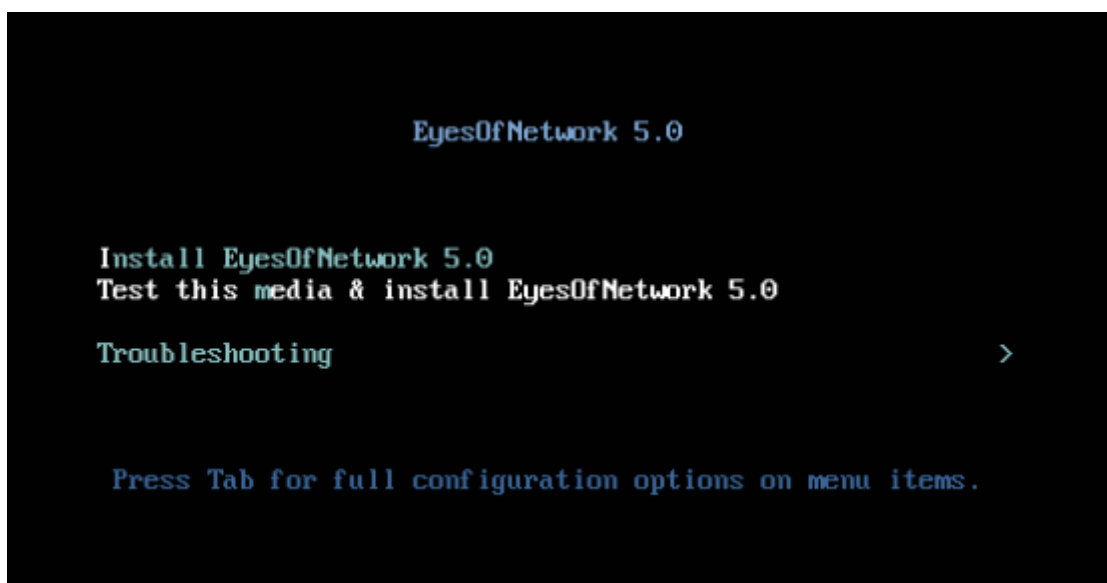
Répartition du travail

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

| Device | Summary |
|------------------|---------------------------------|
| Memory | 2 GB |
| Processors | 2 |
| Hard Disk (SCSI) | 20 GB |
| CD/DVD (IDE) | Using file I:\EyesOfNetwork-... |
| Network Adapter | Bridged (Automatic) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |


Installation de EoN




BIENVENUE SUR EYESOFNETWORK 5.3.

Quelle langue souhaitez-vous utiliser durant le processus d'installation ?

| | | |
|-----------------|---------------|-----------------------|
| Español | Spanish | Français (France) |
| Eesti | Estonian | Français (Canada) |
| Euskara | Basque | Français (Belgique) |
| فارسی | Persian | Français (Suisse) |
| Suomi | Finnish | Français (Luxembourg) |
| Français | French | |
| Galego | Galician | |
| ગુજરાતી | Gujarati | |
| हिन्दी | Hindi | |


Saisissez ici pour rechercher. 






Eyes Of Network

RÉSUMÉ DE L'INSTALLATION



INSTALLATION DE EYESOFNETWORK 5.3

 fr (oss) Aidez-moi !



LOCALISATION

| | |
|---|--|
|  DATE ET HEURE <i>Fuseau horaire Europe/Paris</i> |  CLAVIER <i>Français (variante)</i> |
|  PRISE EN CHARGE DE LA LANGUE <i>Français (France)</i> | |

LOGICIEL


| | |
|--|---|
|  SOURCE D'INSTALLATION <i>Média local</i> |  SÉLECTION DE LOGICIELS <i>EyesOfNetwork Supervision</i> |
|--|---|

SYSTÈME

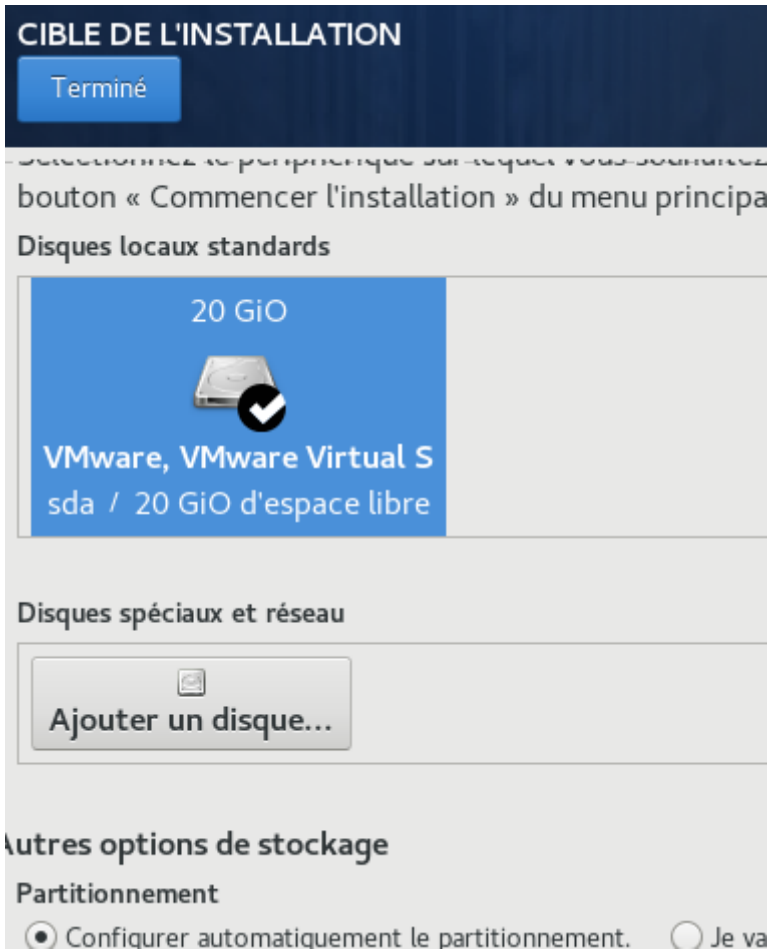
| | |
|--|--|
|  DESTINATION DE L'INSTALLATION |  KDUMP |
|--|--|

Quitter Démarrer l'installation

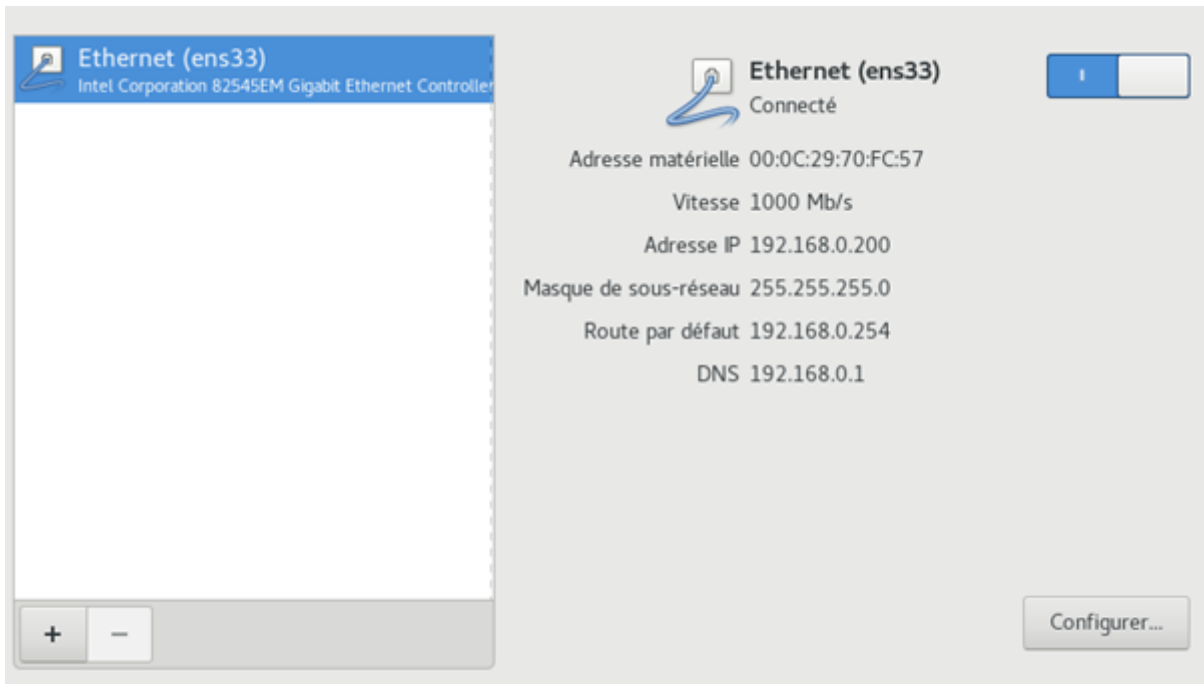
Nous ne modifierons pas vos disques tant que vous n'aurez pas cliqué sur « Commencer l'installation ».

 Veuillez compléter les points marqués avec cette icône avant de passer à l'étape suivante.

Pour la destination de l'installation :



On paramètre bien le réseau :



Nom de la connexion :

Général Ethernet Sécurité 802.1X DCB Proxy **Paramètres IPv4** Paramètres IPv6

Méthode : Manuel

Adresses

| Adresse | Masque de réseau | Passerelle |
|---------------|------------------|---------------|
| 192.168.0.200 | 24 | 192.168.0.254 |

Add
Supprimer

Serveurs DNS :

Domaines de recherche :

ID de client DHCP :

Requiert un adressage IPv4 pour que cette connexion fonctionne

Routes...

Cancel Enregistrer

On coche cette case :

Modification de ens33

Nom de la connexion :

Général Ethernet Sécurité 802.1X DCB Proxy Paramètres IPv4 Paramètres IPv6

Se connecter automatiquement à ce réseau si disponible

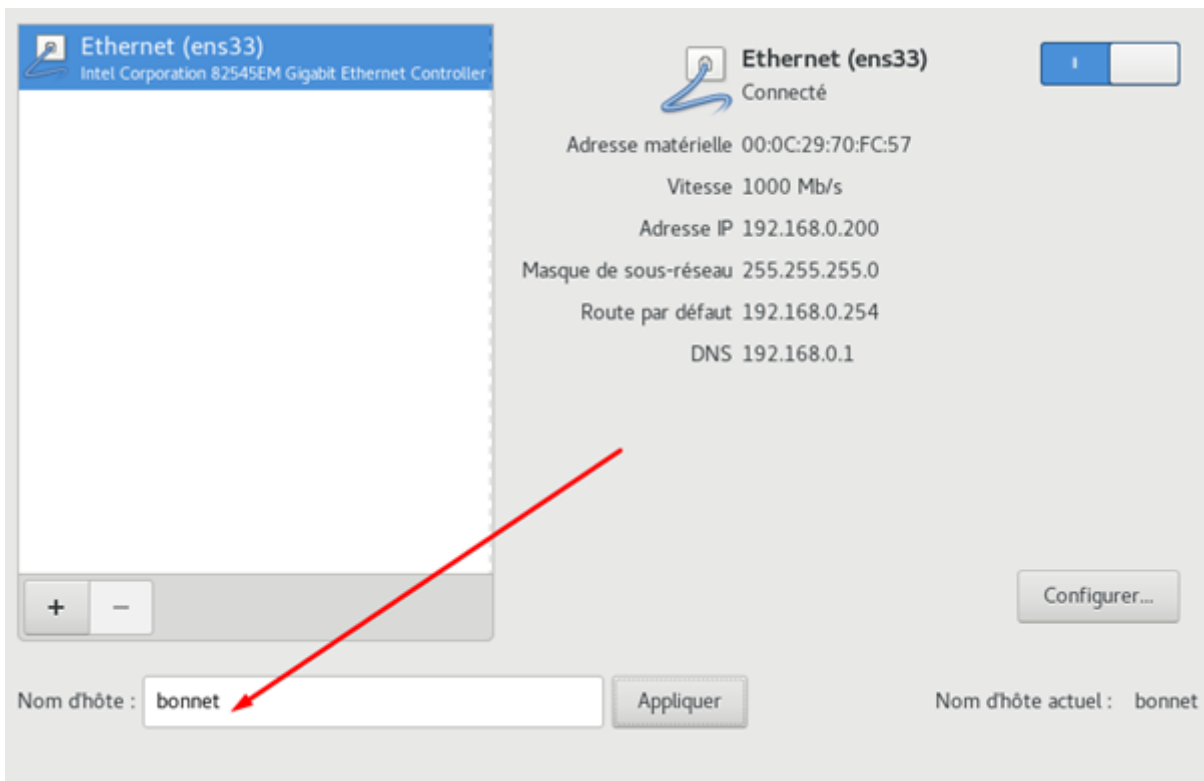
Connection priority for auto-activation: - +

Tous les utilisateurs peuvent se connecter à ce réseau

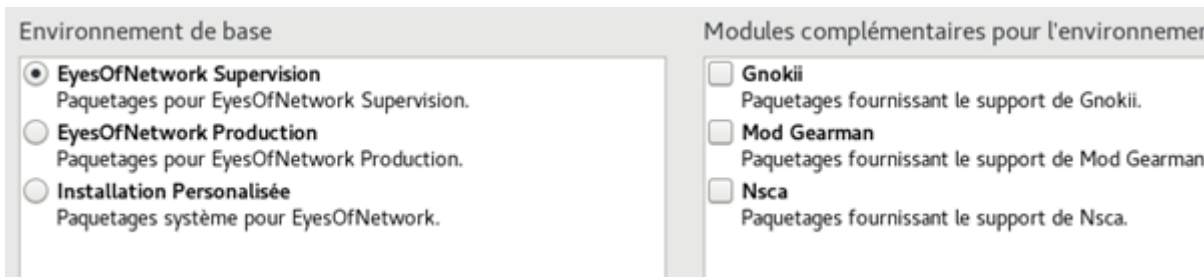
Se connecter automatiquement au VPN lorsque cette connexion est utilisée

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

On met le nom d'hôte

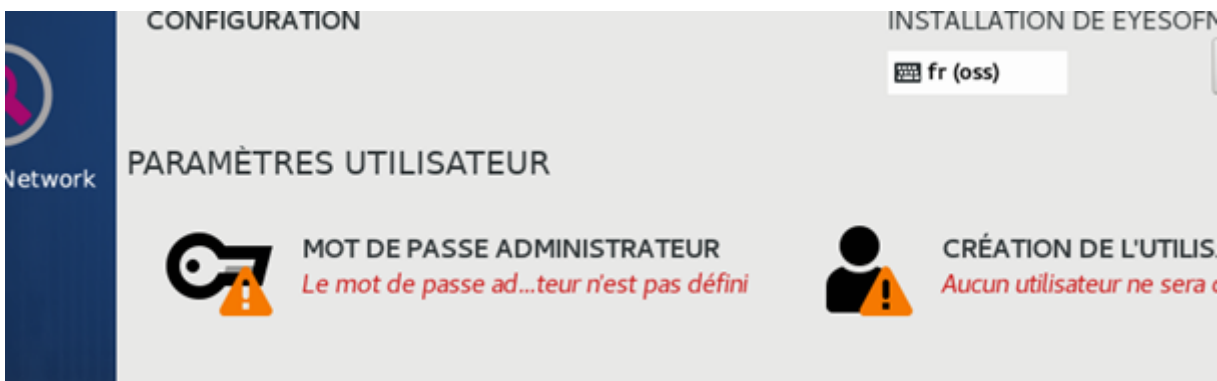


On se rend dans Sélection de logiciels :



On prend ce qu'on a besoin.

On clique sur démarrer.



On définit un mot de passe.

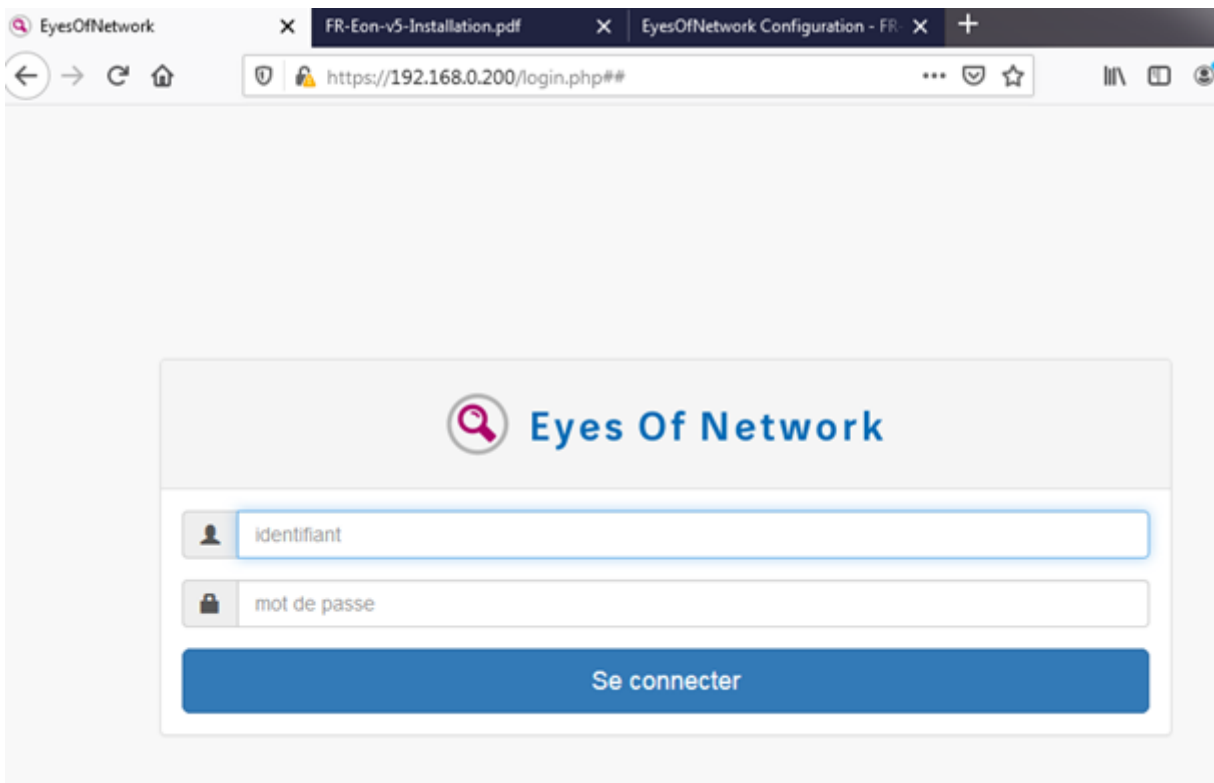


Fini !

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
```

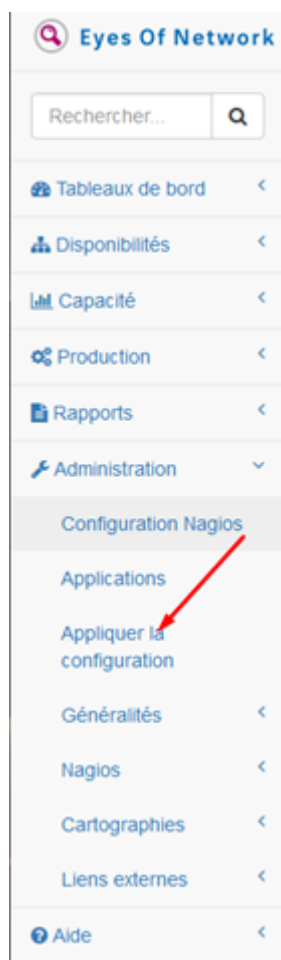
```
ignoreauthfailure yes  
authCommunity log,execute,net BonnetSupervision  
traphandle default /srv/eyesofnetwork/snmppt/bin/snmpthandler
```

```
systemctl restart snmptrapd
```

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

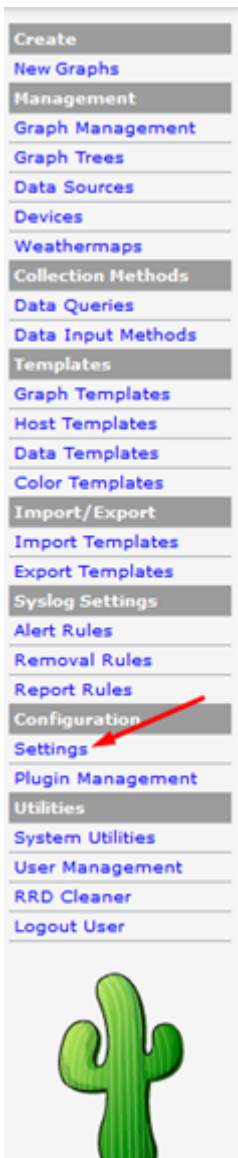
On modifie la variable `$user2$` par le nom de la communauté.

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



On restart nagios.

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



| SNMP Defaults | |
|--|----------------------|
| SNMP Version Default SNMP version for all new hosts. | Version 2 ▾ |
| SNMP Community Default SNMP read community for all new hosts. | EyesOfNetwork |
| SNMP Username (v3) The SNMP v3 Username for polling hosts. | <input type="text"/> |
| SNMP Password (v3) The SNMP v3 Password for polling hosts. | <input type="text"/> |
| SNMP Auth Protocol (v3) Choose the SNMPv3 Authorization Protocol. | MD5 (default) ▾ |
| SNMP Privacy Passphrase (v3) Choose the SNMPv3 Privacy Passphrase. | <input type="text"/> |
| SNMP Privacy Protocol (v3) Choose the SNMPv3 Privacy Protocol. | DES (default) ▾ |
| SNMP Timeout Default SNMP timeout in milli-seconds. | 1000 |
| SNMP Port Number Default UDP port to be used for SNMP Calls. Typically 161. | 161 |
| SNMP Retries The number times the SNMP poller will attempt to reach the host before failing. | 3 |

On remplace par le nom de communauté puis on enregistre.

Sécurisation

On supprime l'accès root direct en SSH.

```
nano /etc/ssh/sshd_config
```

```
GNU nano 2.3.1      Fichier : /etc/ssh/sshd config
HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
```

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

Add New Host

Host Name:
 ⓘ

Host Description:
 ⓘ

Address:
 ⓘ

Display Name (Optional):

Host Templates To Inherit From (Top to Bottom): _____

Add Template To Inherit From:

Dans Template, on choisit Printer.

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

On choisit le check_hpjd et generic service

Service Editor

Service Description:

Printer Status ⓘ

Display Name: (Optional)

Service Templates To Inherit From (Top to Bottom):

Add Template To Inherit From: GENERIC_SERVICE ▼ Add Template

Check Command: check_hjpd ▼ ⓘ

Check Command Parameters:

Value for \$ARG1\$: -C bonnet Add Parameter

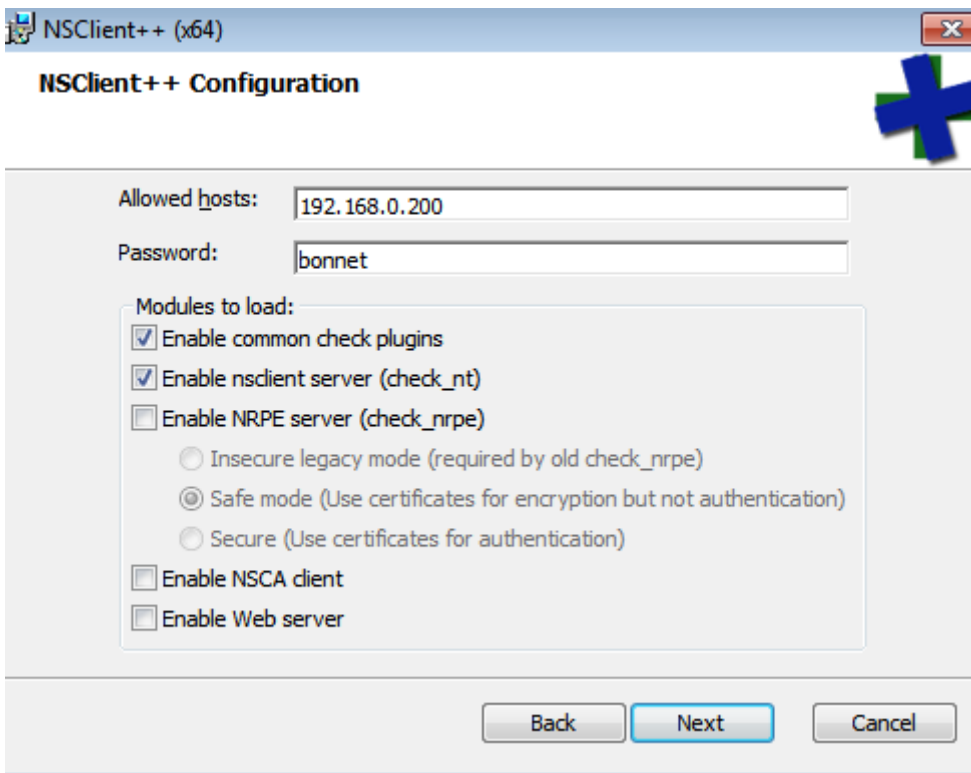
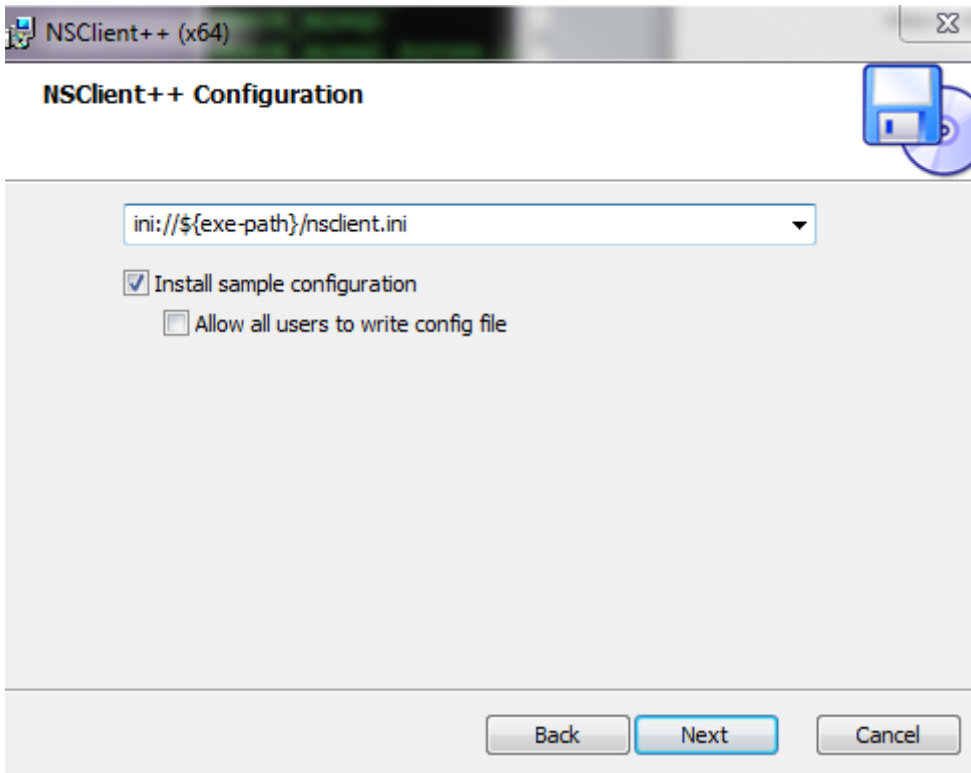
Add ServiceCancel

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.

```
nsclient - Bloc-notes
Fichier Edition Format Affichage ?
; in flight - TODO
[/modules]

; Undocumented key
CheckExternalScripts = enabled

; Undocumented key
CheckHelpers = enabled

; Undocumented key
CheckEventLog = enabled

; Undocumented key
CheckNSCP = enabled

; Undocumented key
CheckDisk = enabled

; Undocumented key
CheckSystem = enabled

; Undocumented key
NSClientServer = enabled
```

On redémarre.


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

| Nom | Description | État | Type de démarrage | Contrôle |
|-------------------------|------------------|----------------------|-------------------|------------|
| McAfee Service C... | Manages M... | Dém... | Automatique | Système |
| McAfee Validation... | Provides val... | | Manuel | Système |
| Microsoft .NET Fr... | Microsoft ... | Désactivé | | Système |
| Microsoft .NET Fr... | Microsoft ... | Désactivé | | Système |
| Microsoft .NET Fr... | Microsoft ... | Automatique (débu... | | Système |
| Microsoft .NET Fr... | Microsoft ... | Automatique (débu... | | Système |
| Microsoft SharePo... | | | Manuel | Service lc |
| Modules de génér... | Le service IK... | Dém... | Automatique | Système |
| Moteur de filtrage... | Le moteur d... | Dém... | Automatique | Service lc |
| Mozilla Maintena... | Le service d... | | Manuel | Système |
| mysql | | Dém... | Automatique | Système |
| Net.Msmq Listene... | Receives act... | | Désactivé | Service re |
| Net.Pipe Listener ... | Receives act... | | Désactivé | Service lc |
| Net.Tcp Listener A... | Receives act... | | Désactivé | Service lc |
| Net.Tcp Port Shari... | Provides abi... | | Désactivé | Service lc |
| Netlogon | Maintient u... | Dém... | Automatique | Système |
| NSClient++ (x64) | Monitoring ... | Dém... | Automatique | Système |
| Office Source Eng... | Enregistre le... | | Manuel | Système |
| Office Software Pr... | Enables the ... | Dém... | Manuel | Service re |
| Ouverture de sessi... | Permet le d... | | Manuel | Système |
| Pare-feu Windows | Le Pare-feu ... | Dém... | Automatique | Service lc |


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

Nagios Command Editor


Command Name:

check_nt 

Command Line:

`$USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -s <mot-de-passe> -v $ARG1$ $ARG2$` 

Command Description:

check nsclient 

Create Command

Cancel

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

Equipements > Ajouter

Host Name:

HOS4POSTE18 

Host Description:

PC hôte 

Address:

192.168.0.18 

Display Name (Optional):

Host Templates To Inherit From (Top to Bottom):

Add Template To Inherit From: WINDOWS 

Add Template

Add Host

Cancel

On ajoute ensuite des services.

Service Description:


Version NSClient 

Display Name: (Optional)

Service Templates To Inherit From (Top to Bottom):

Delete

GENERIC_SERVICE

Add Template To Inherit From: EMC  Add Template

Check Command: None  

Check Command Parameters:

Delete

\$ARG1\$: !CLIENTVERSION

Value for \$ARG2\$: Add Parameter

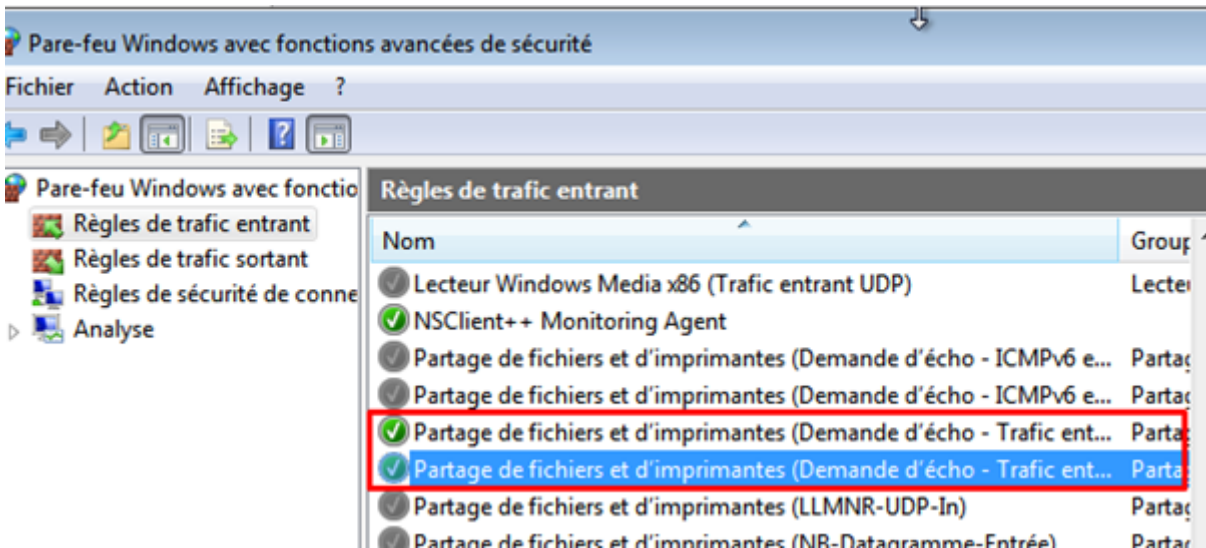
Add Service

Cancel

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" :



| Host | Service | Status | Last Check | Duration | Attempts | Status Information |
|-----------|-----------------|--------|------------|-----------------|----------|--|
| NPI064892 | Printer Status | OK | 11:42:09 | 0d 18h 57m 44s | 4/4 #3 | Toner Fable ("Mode veille activ.") |
| PC01 | CPULOAD | OK | 11:42:54 | 0d 0h 9m 7s | 1/4 | Charge CPU 2% (5 moyenne minime) |
| | Disk | OK | 11:43:39 | 0d 0h 6m 7s | 1/4 | c1 - total: 59,90 Gb - utilisé: 11,24 Gb (19%) - libre: 48,66 Gb (81%) |
| | Mem | OK | 11:45:09 | 0d 0h 6m 7s | 1/4 | Memory usage: total:2095,01 MB - used: 593,64 MB (21%) - free: 2301,37 MB (79%) |
| | Uptime | OK | 11:43:50 | 0d 0h 19m 21s | 1/4 | System Uptime - 0 day(s) 0 hour(s) 19 minute(s) |
| localhost | Verken NSClient | OK | 11:42:24 | 0d 0h 27m 36s | 1/4 | NSClient++ 9.5.2.35 2010-01-28 |
| localhost | interfaces | OK | 11:43:09 | 0d 18h 56m 56s | 1/4 | OK, ens33 up |
| | memory | OK | 11:43:54 | 0d 18h 56m 8s | 1/4 | Ram - 3% Swap - 0% : OK |
| | mysql | OK | 11:44:39 | 20d 19h 42m 57s | 1/4 | Uptime: 5662 Threads: 2 Questions: 23648 Slow queries: 0 Opens: 132 Flush tables: 2 Open tables: 139 Queries per second avg: 4.196 |
| | partitions | OK | 11:45:24 | 0d 18h 54m 32s | 1/4 | All selected storages (>90%): OK |
| | processes | OK | 11:42:21 | 0d 18h 57m 20s | 1/4 | 1 process named gcc (- 0) |
| | processor | OK | 11:42:39 | 0d 18h 56m 32s | 1/4 | CPU used 1.0% (<80): OK |
| | ssh | OK | 11:43:24 | 20d 19h 41m 11s | 1/4 | SSH OK - OpenSSH_7.4 (protocol 2.0) |
| | system | OK | 11:44:09 | 0d 18h 54m 56s | 1/4 | System Time OK - 11-04-2020, 11:44:09 |
| | uptime | OK | 11:44:54 | 0d 1h 23m 22s | 1/4 | OK: Linux bonnet 3.10.0-1062.9.1.el7.x86_64 - up 1 hour 35 minutes |

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

| Host | Status | Last Check | Duration | Status Information |
|-----------------------|--------|------------|---------------|--|
| Borne Wifi HOS4 | UP | 16:53:28 | 0d 0h 0m 41s+ | PING OK - Paquets perdus = 0%, RTA = 0.92 ms |
| LiveBox Pro | UP | 16:54:02 | 0d 0h 3m 33s | PING OK - Paquets perdus = 0%, RTA = 0.94 ms |
| NPI064892 | UP | 16:51:36 | 7d 0h 41m 48s | PING OK - Paquets perdus = 0%, RTA = 1.26 ms |
| PC01 | UP | 16:52:36 | 0d 0h 10m 15s | PING OK - Paquets perdus = 0%, RTA = 0.97 ms |
| Switch HOS4 | UP | 16:53:55 | 0d 0h 0m 41s+ | PING OK - Paquets perdus = 0%, RTA = 8.48 ms |
| Vidéo Projecteur HOS4 | UP | 16:54:05 | 0d 0h 0m 41s+ | PING OK - Paquets perdus = 0%, RTA = 2.68 ms |
| localhost | UP | 16:47:27 | 35d 0h 52m 9s | PING OK - Paquets perdus = 0%, RTA = 0.03 ms |

7 of 7 Matching Host Entries Displayed

Monitoring d'un switch cisco

On ajoute l'hôte puis cisco en template

| Host | Service | Status | Last Check | Duration | Attempts | Status Information |
|--------------|-----------|--------|------------|--------------|----------|---|
| Switch yeast | memory | OK | 16:55:06 | 0d 0h 5m 46s | 1/4 | Processor 79% Device load 0%/10/27% 70% : OK |
| | processes | OK | 16:55:10 | 0d 0h 5m 46s | 1/4 | CPU: 0.0.0 : OK |
| | status | OK | 16:55:17 | 0d 0h 5m 36s | 1/4 | 1 ps OK : OK |
| | uptime | OK | 16:55:23 | 0d 0h 5m 36s | 1/4 | OK: Cisco IOS Software - up 13 days 22 hours 54 minutes |

```

snmp-server community public RO
snmp-server community <public> RO
snmp-server community bonnet RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
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.

Service Description:
 ⓘ

Display Name: (Optional)

Service Templates To Inherit From (Top to Bottom):
Delete GENERIC_SERVICE

Add Template To Inherit From: Add Template

Check Command: ⓘ

Check Command Parameters:

| | |
|---------------------|---------------------------|
| Delete | \$ARG1\$: FastEthernet0/2 |
| Delete | \$ARG2\$: 90 |
| Delete | \$ARG3\$: 90 |
| Delete | \$ARG4\$: 95 |
| Delete | \$ARG5\$: 95 |

Value for \$ARG6\$: Add Parameter

Add Service Cancel

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