Labo 3 Nagios

Joel Schär, Yann Lederrey, Yohann Meyer

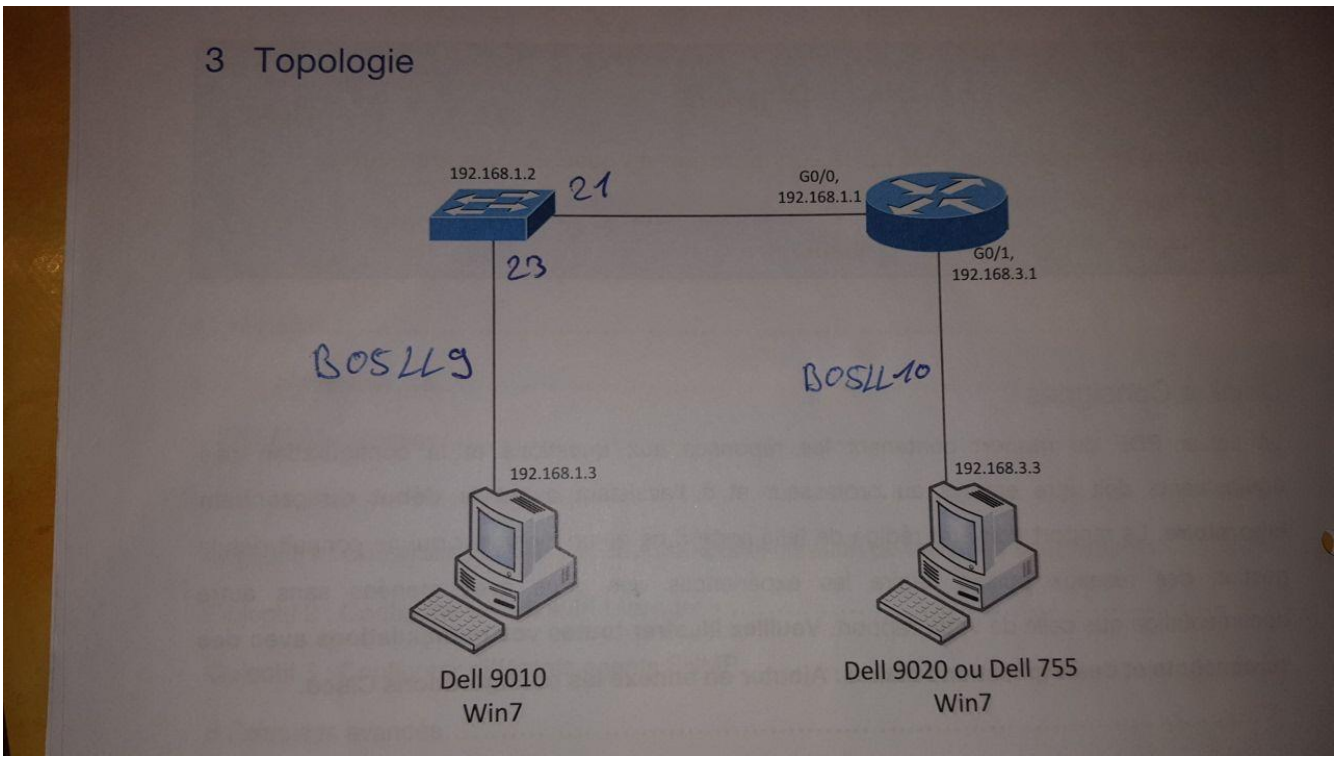
Objectif 1

On a fait la même chose que pour les derniers laboratoires.

Extrait du laboratoire SNMP

Configuration des machines

Il faut relier les équipements comme indiqué sur le schéma ci dessous. Les liaisons entre l'armoire de brassage et les machines Windows était le **B05LL09** et le **B05LL10**. Le schéma réseau ci dessous, illustre le montage réseau utilisé.



Il faut ensuite configurer les machines en leur attribuant les adresses ip indiquées dans le tableau ci- dessous.

Équipement	OS	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	CISCO	0 / 1	192.168.3.1	255.255.255.0	192.168.3.1
R1	CISCO	0 /0	192.168.1.1	255.255.255.0	192.168.1.1
S1	CISCO	21	192.168.1.2	255.255.255.0	192.168.1.1
S1	CISCO	23	192.168.1.2	255.255.255.0	192.168.1.1
Dell 9010	Win 10	NIC	192.168.1.3	255.255.255.0	192.168.1.1
Dell 9010	Ubuntu (VM)	NIC	192.168.1.4	255.255.255.0	192.168.1.1
Dell 9020	Win 10	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Pour ce qui est des machines Windows, il faut faire la configuration dans les paramètres réseau dédiée et reliée au montage.

Pour la machine virtuelle Ubuntu, il est nécessaire de régler la carte réseau en mode **Bridged Networking** dans les paramètres de configuration VMware et d'associer la carte virtuelle avec la carte physique correspondante. Définir ensuite les paramètres Ip dans les réglage réseau de la machine Linux.

Pour la configuration du router cisco il faut entrer les commandes suivantes dans le terminal.

```
> enable
> configure terminal
> interface GigabitEthernet 0/0
> ip address 192.168.1.1 255.255.255.0
> no shutdown
> exit
> interaface GigabitEthernet 0/1
> ip address 192.168.3.1 255.255.255.0
> no shutdown
> exit
> exit
> exit
```

Pour attribuer une adresse Ip au switch il faut entrer les commandes suivantes dans le terminal.

```
> enable
> configure terminal
> interface vlan1
> ip address 192.168.1.2 255.255.255.0
> no shutdown
> exit
> ip default-gateway 192.168.1.1
> exit
> exit
```

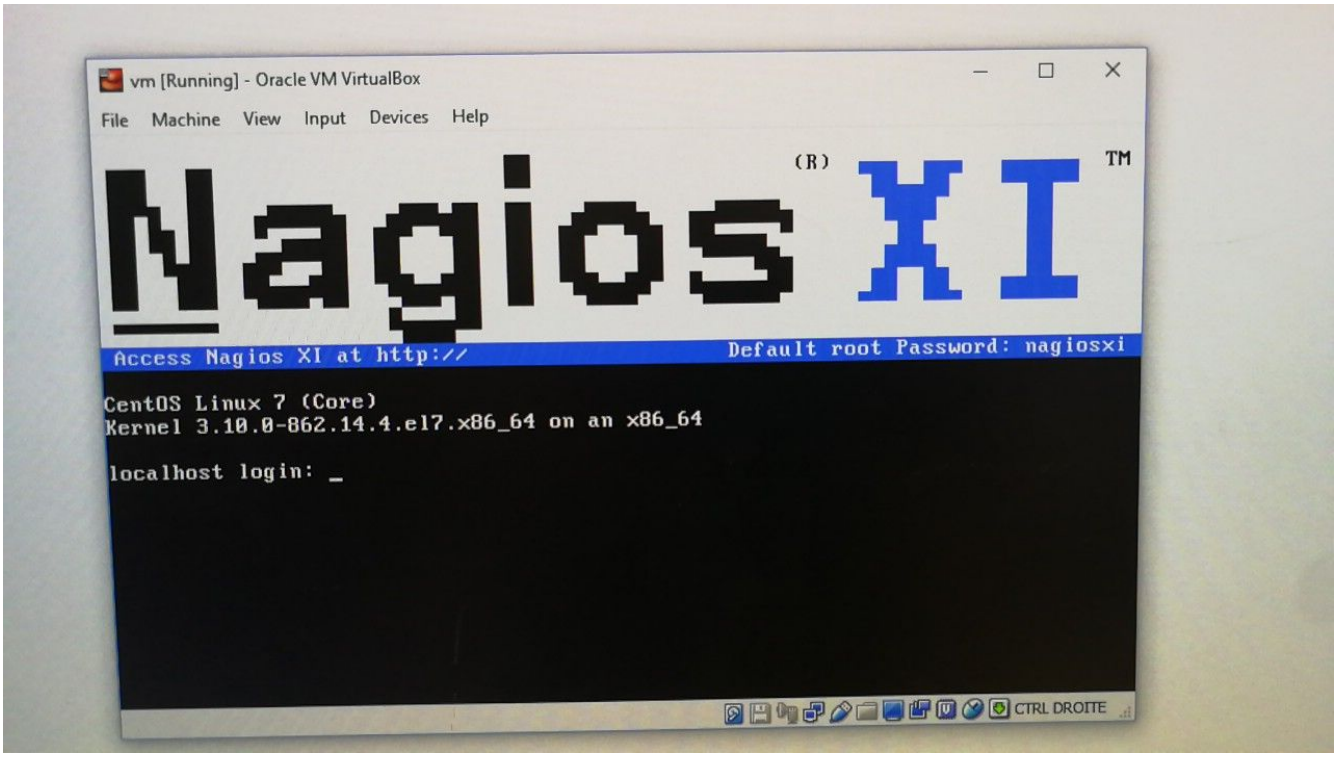
On obtient en finalité un réseau dans lequel toutes les machines peuvent être pingée entre elles.

Objectif 2

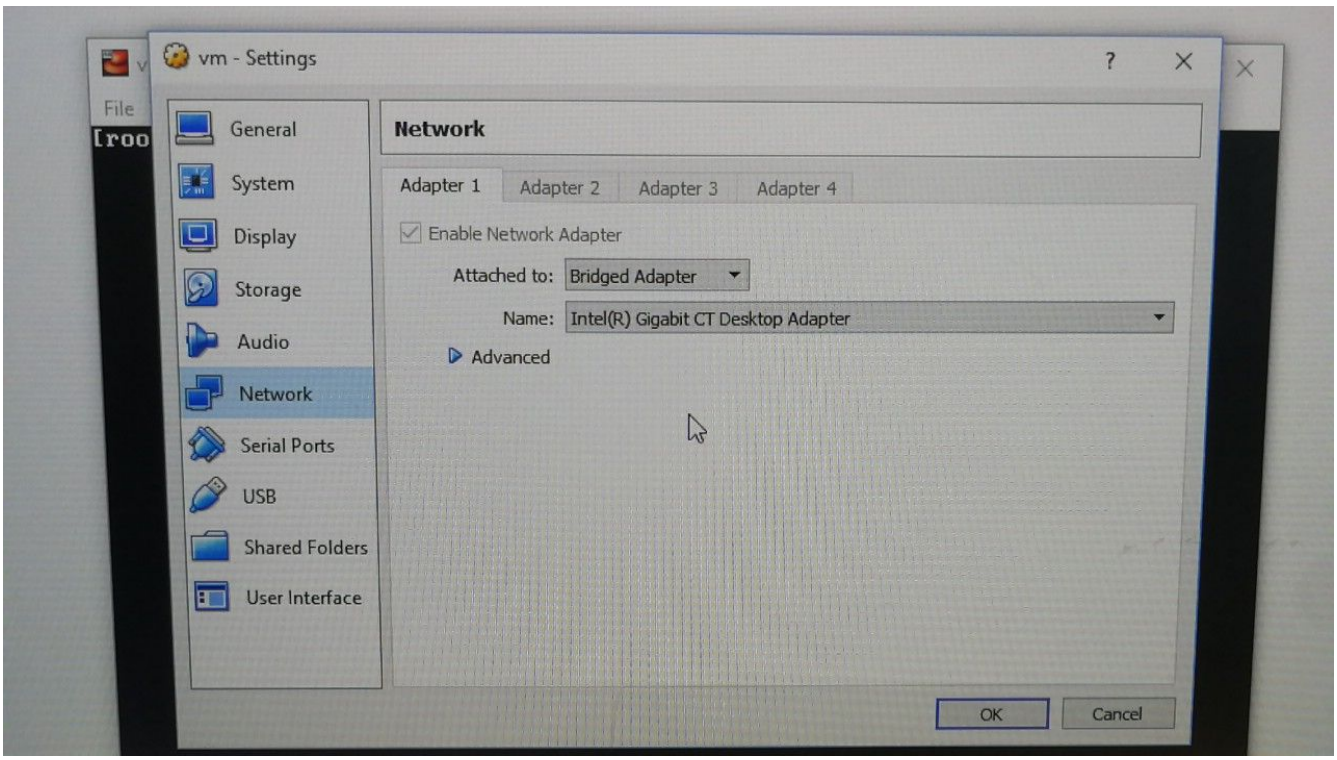
Tutoriel:

1. Télécharger la machine virtuel sur https://www.nagios.com/downloads/nagios-xi/vmware
2. double cliquez sur le fichier ova.
3. virtual box ouvre une page de settings, copiez les configurations suivantes.

4. faites un import.
5. Démarrez la vm se nommant "vm"
6. un login localhost est demandé :
    1. mot de passe : nagiosxi



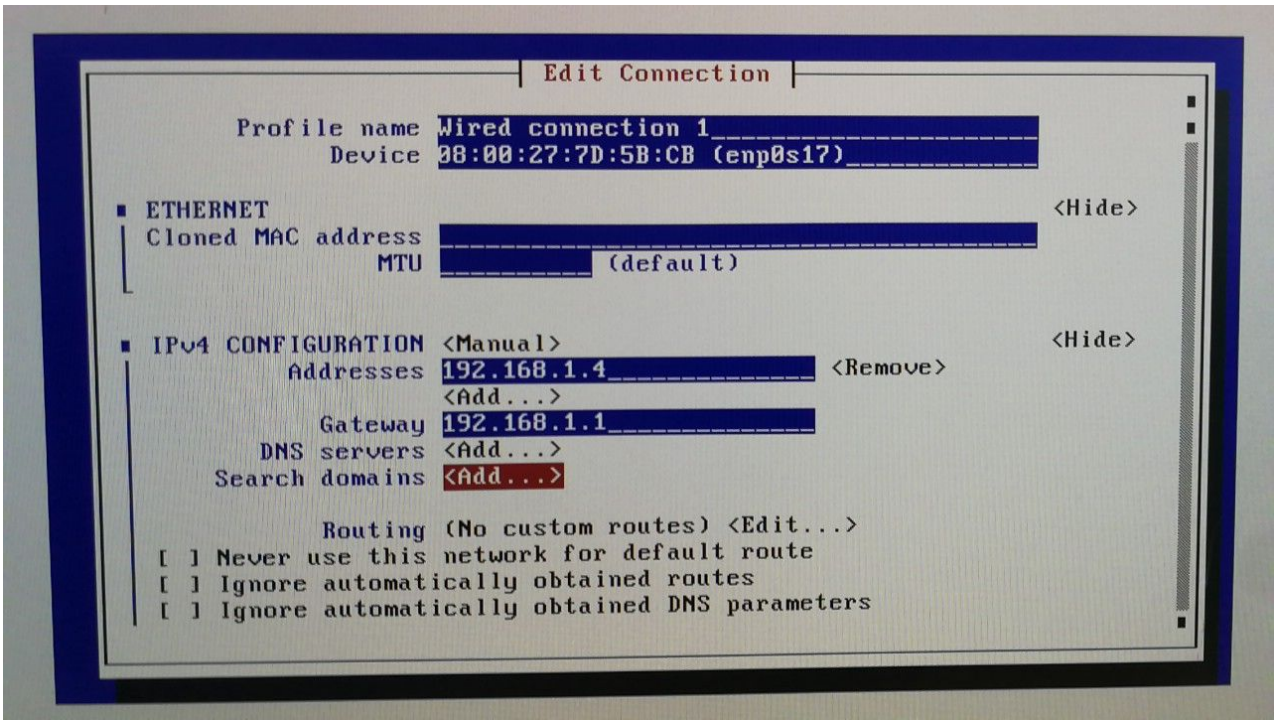
7. vérifiez que l'interface réseau de la machine virtuelle VirtualBox est en bridge.



8. vous pouvez changer la langue de votre clavier en effectuant la commande suivante : `vi etc/sysconfig/keyboard` , ensuite attribuez la valeur "fr_CH" à la variable "KEYTABLE". faites `:wx` pour sauver vos changements.
    1. si le fichier n'existe pas, faites `localectl set-keymap ch-fr`
9. Attribuez une adresse ip fixe à votre machine virtuelle, pour cela :
    1. Lancez la commande suivante afin d'installer l'outil permettant la configuration réseau.

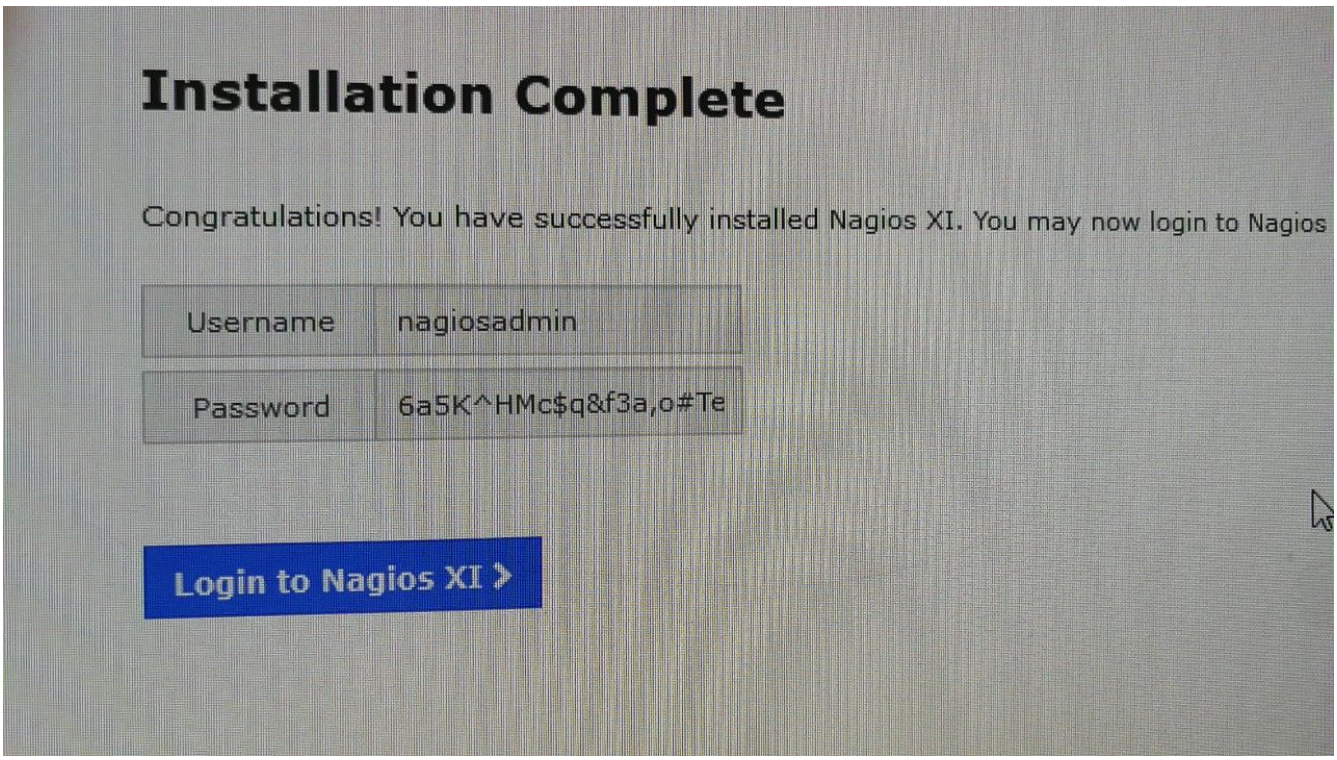
```
nmtui
```

3. allez dans Edit a connection
4. allez dans wired connection
5. configurez une adresse ip fixe dans IPv4 CONFIGURATION passez en manual



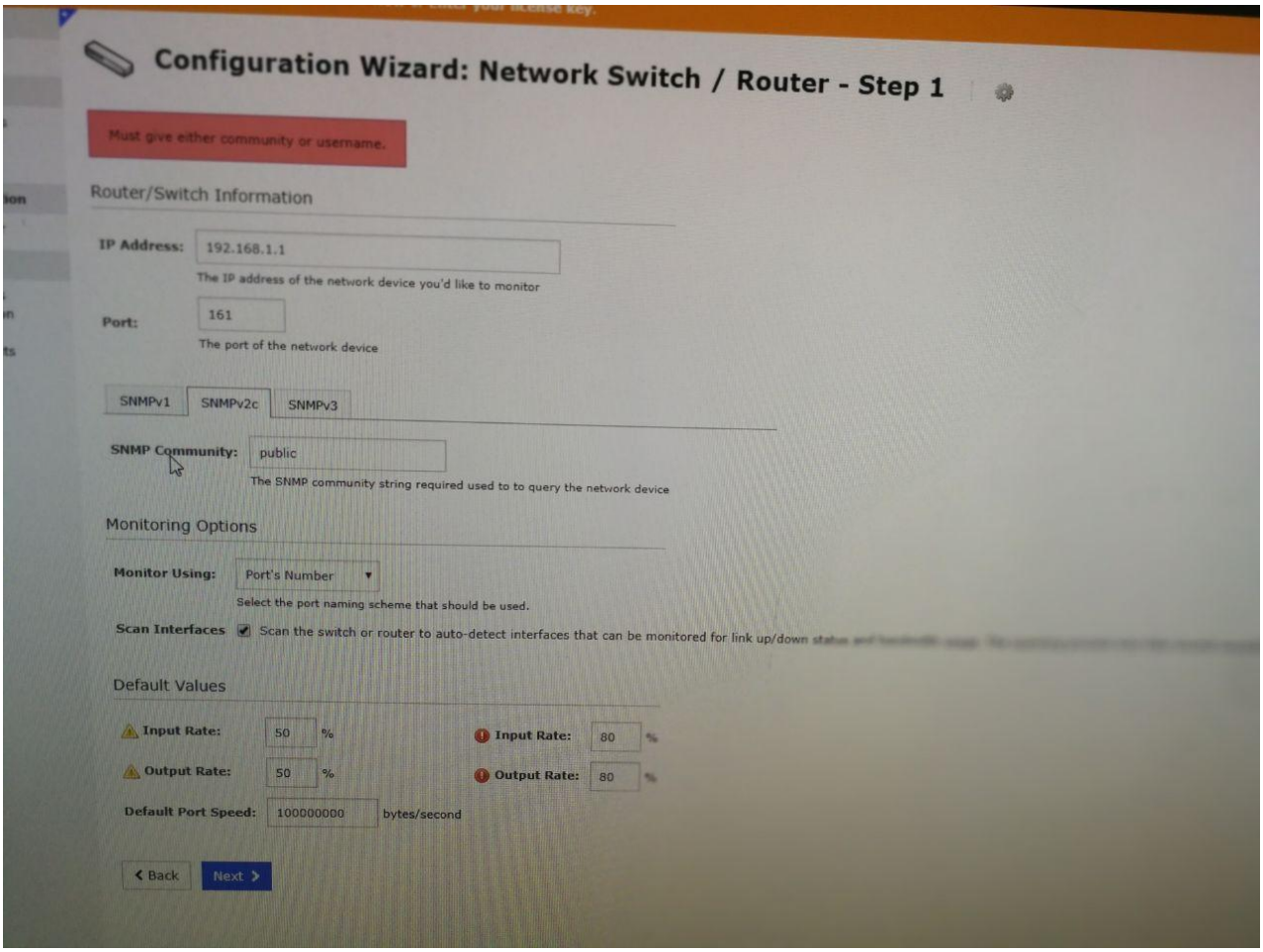
Objectif 3

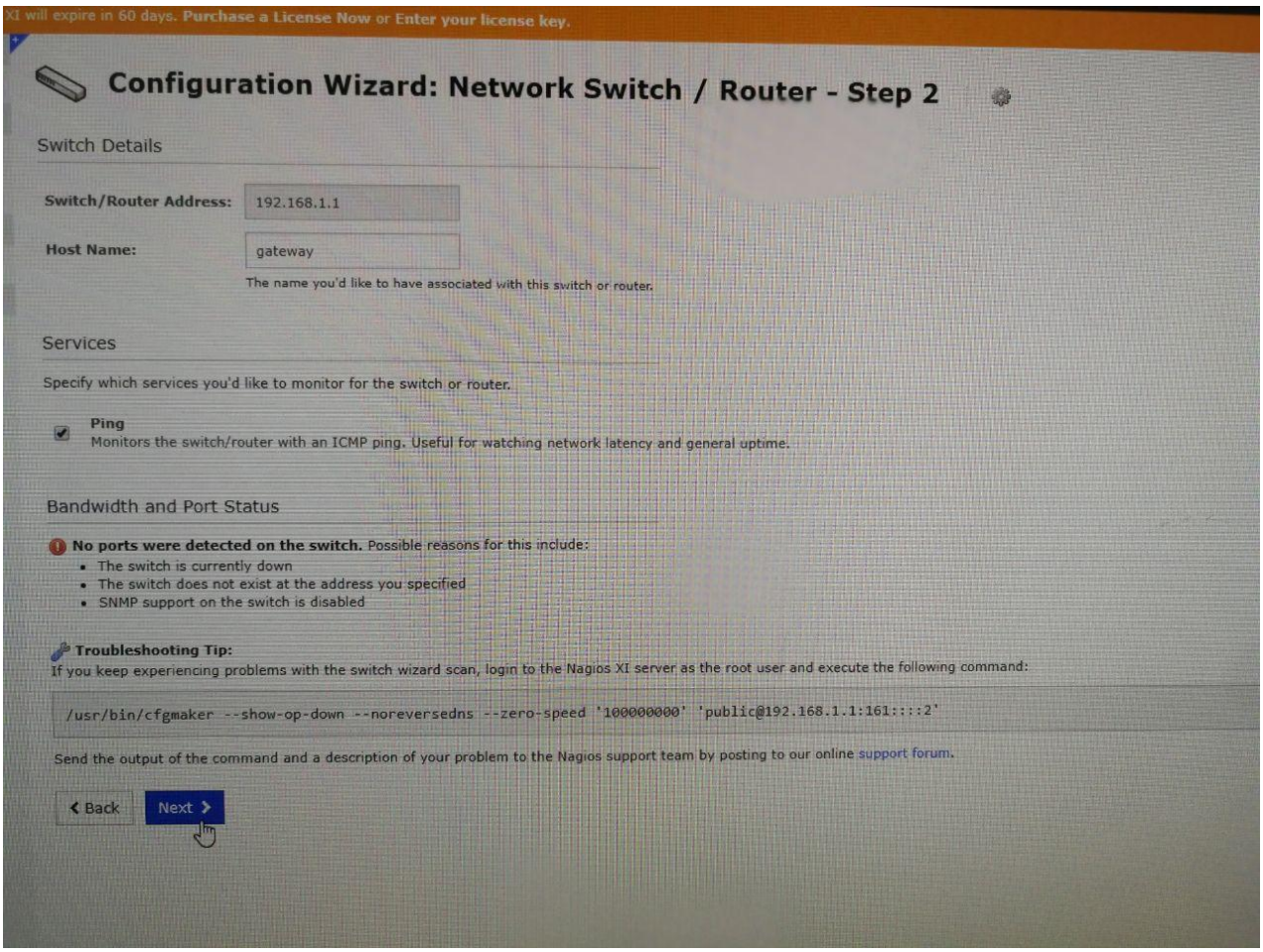
1. Allez sur http://<>/nagiosxi/install.php

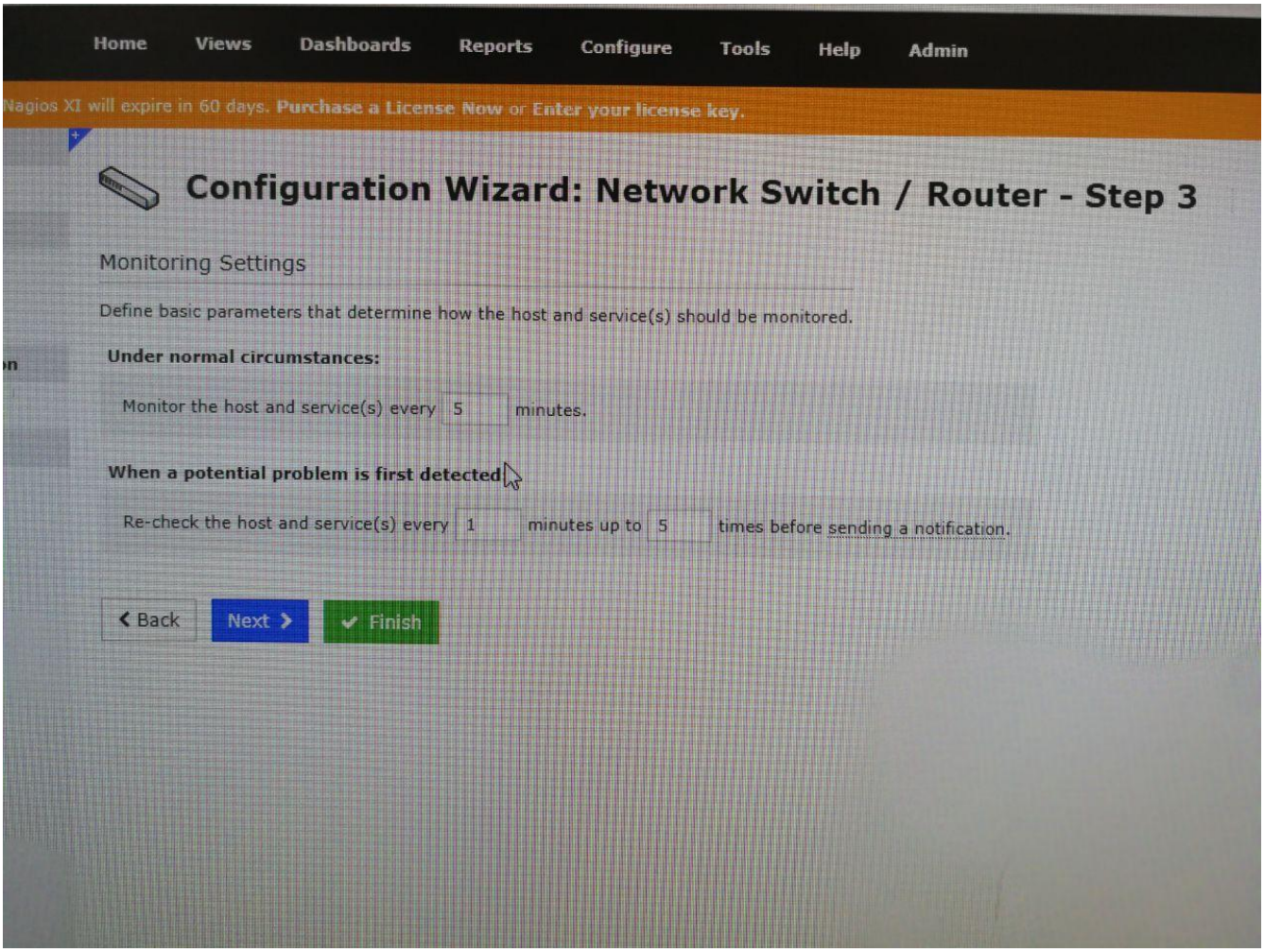


(mot de passe changé -> "admin")

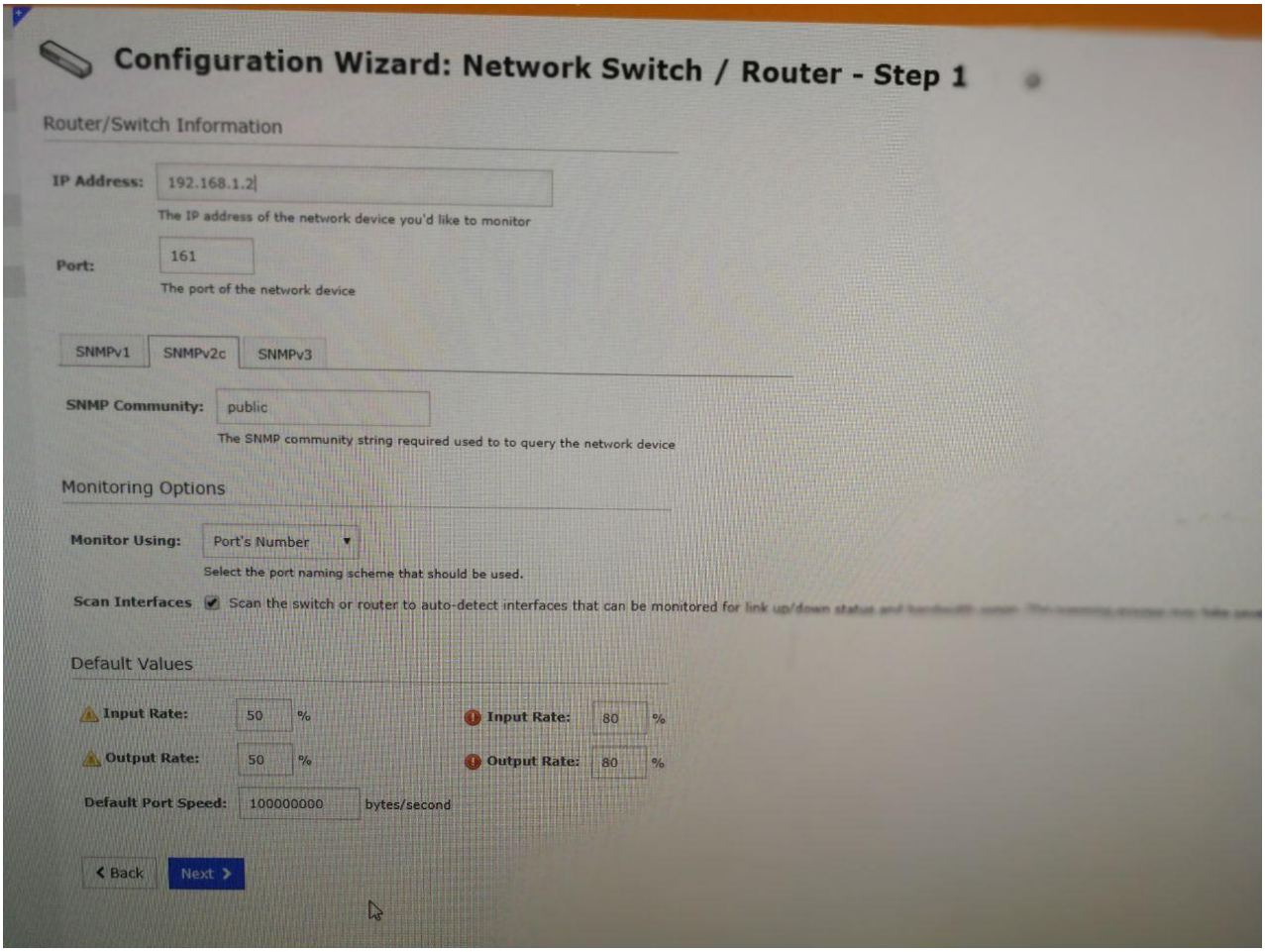
2. Loguez vous avec votre username, password.
3. Allez sur configure => configure wizard
4. chechez network switch routeur
5. configurez.
6. choisir l'ip de du router

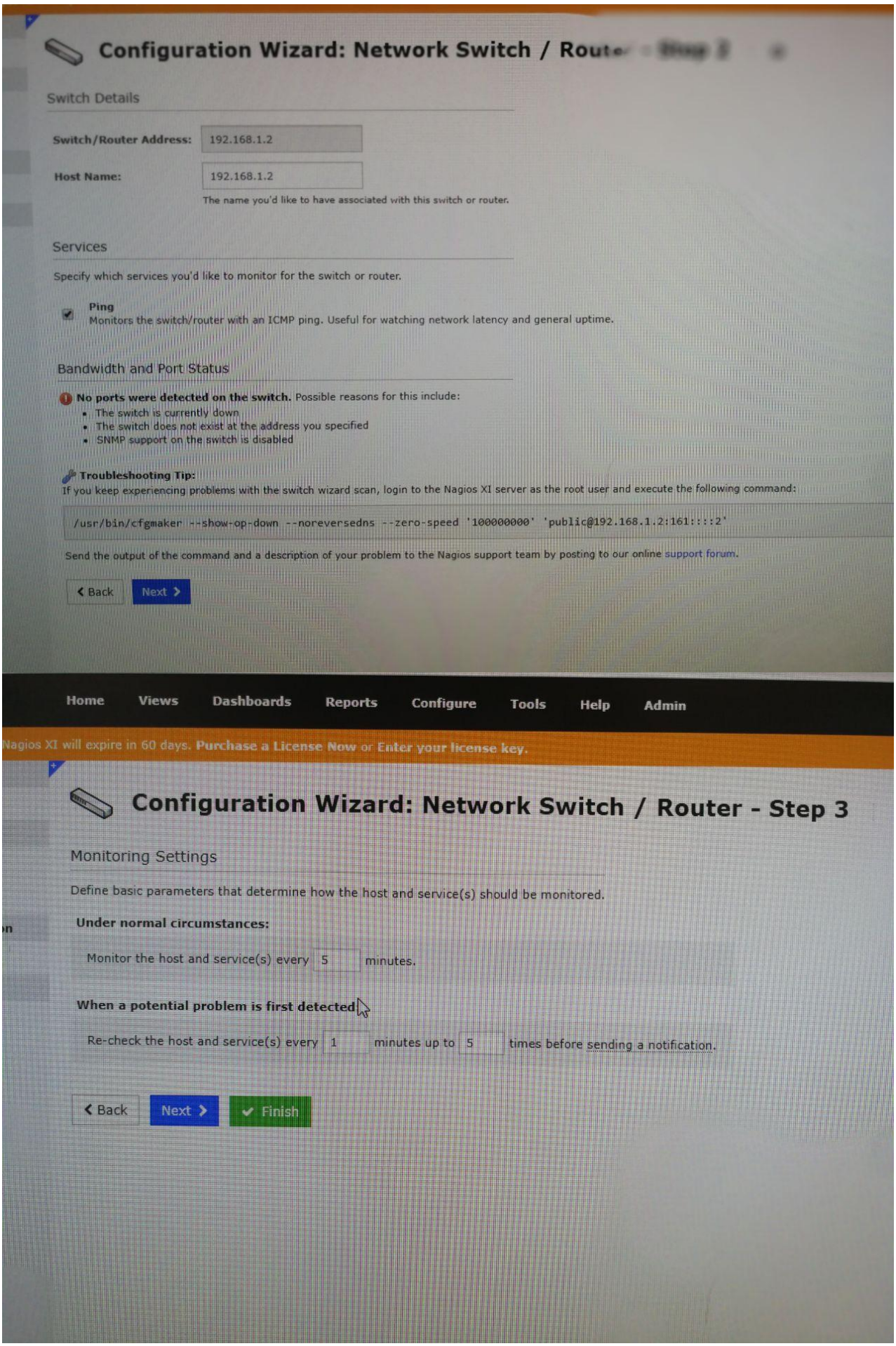



XI will expire in 60 days. Purchase a License Now or Enter your license key.
Configuration Wizard: Network Switch / Router - Step 2
Switch Details
Switch/Router Address:
192.168.1.1
Host Name:
gateway
The name you'd like to have associated with this switch or router.
Services
Specify which services you'd like to monitor for the switch or router.
Ping
Monitors the switch/router with an ICMP ping. Useful for watching network latency and general uptime.
Bandwidth and Port Status
No ports were detected on the switch. Possible reasons for this include:
The switch is currently down
The switch does not exist at the address you specified
SNMP support on the switch is disabled
Troubleshooting Tip:
If you keep experiencing problems with the switch wizard scan, login to the Nagios XI server as the root user and execute the following command:
/usr/bin/cfgmaker --show-op-down --noreversedns --zero-speed '100000000' 'public@192.168.1.1:161::::2'
Send the output of the command and a description of your problem to the Nagios support team by posting to our online support forum.
Back
Next



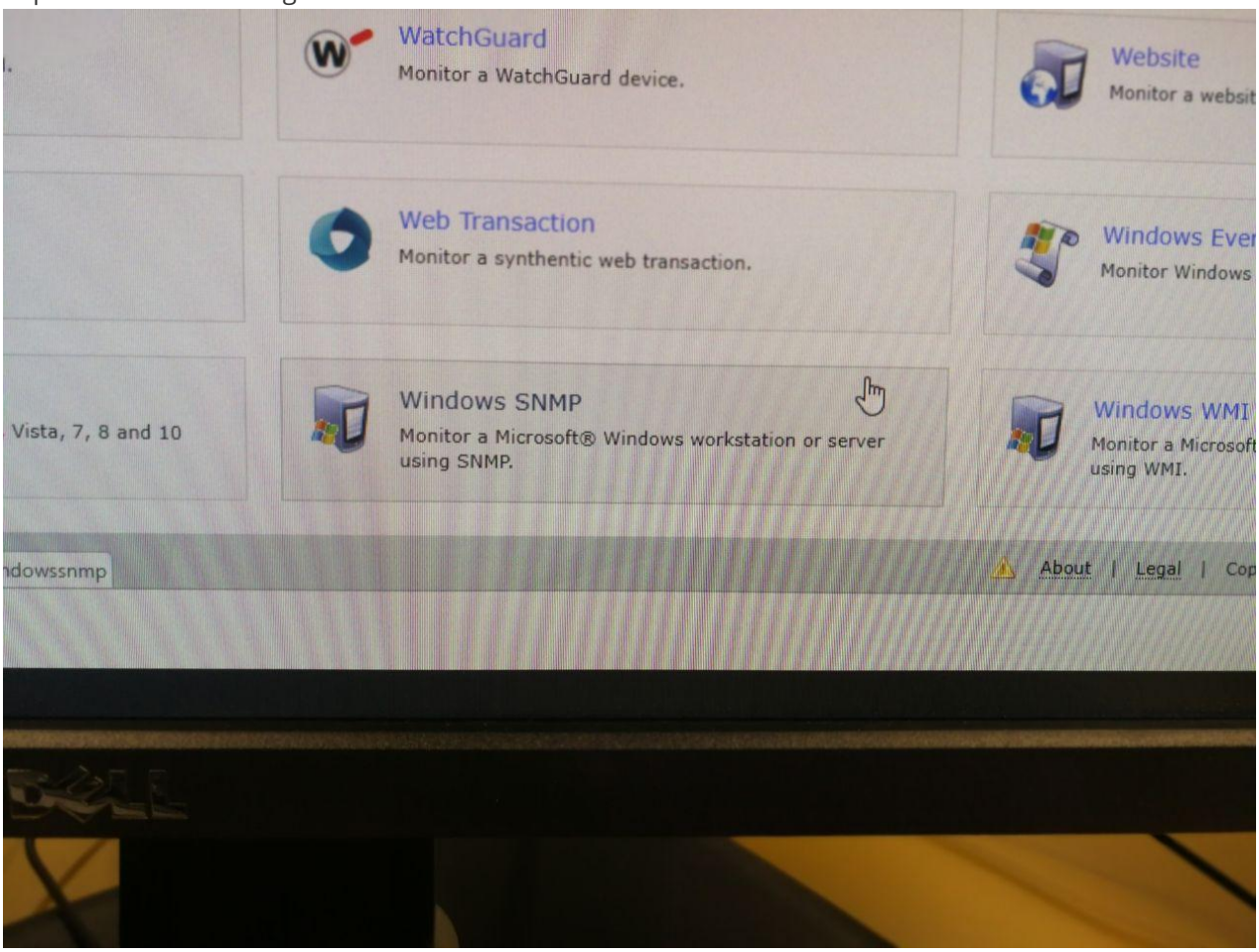
7. On fait la même manipe pour le switch


Configuration Wizard: Network Switch / Router - Step 1
Router/Switch Information
IP Address:
192.168.1.2
The IP address of the network device you'd like to monitor
Port:
161
The port of the network device
SNMPv1
SNMPv2c
SNMPv3
SNMP Community:
public
The SNMP community string required used to to query the network device
Monitoring Options
Monitor Using:
Port's Number
Select the port naming scheme that should be used.
Scan Interfaces
Scan the switch or router to auto-detect interfaces that can be monitored for link up/down status
Default Values
Input Rate:
50
%
Input Rate:
80
%
Output Rate:
50
%
Output Rate:
80
%
Default Port Speed:
100000000
bytes/second
Back
Next

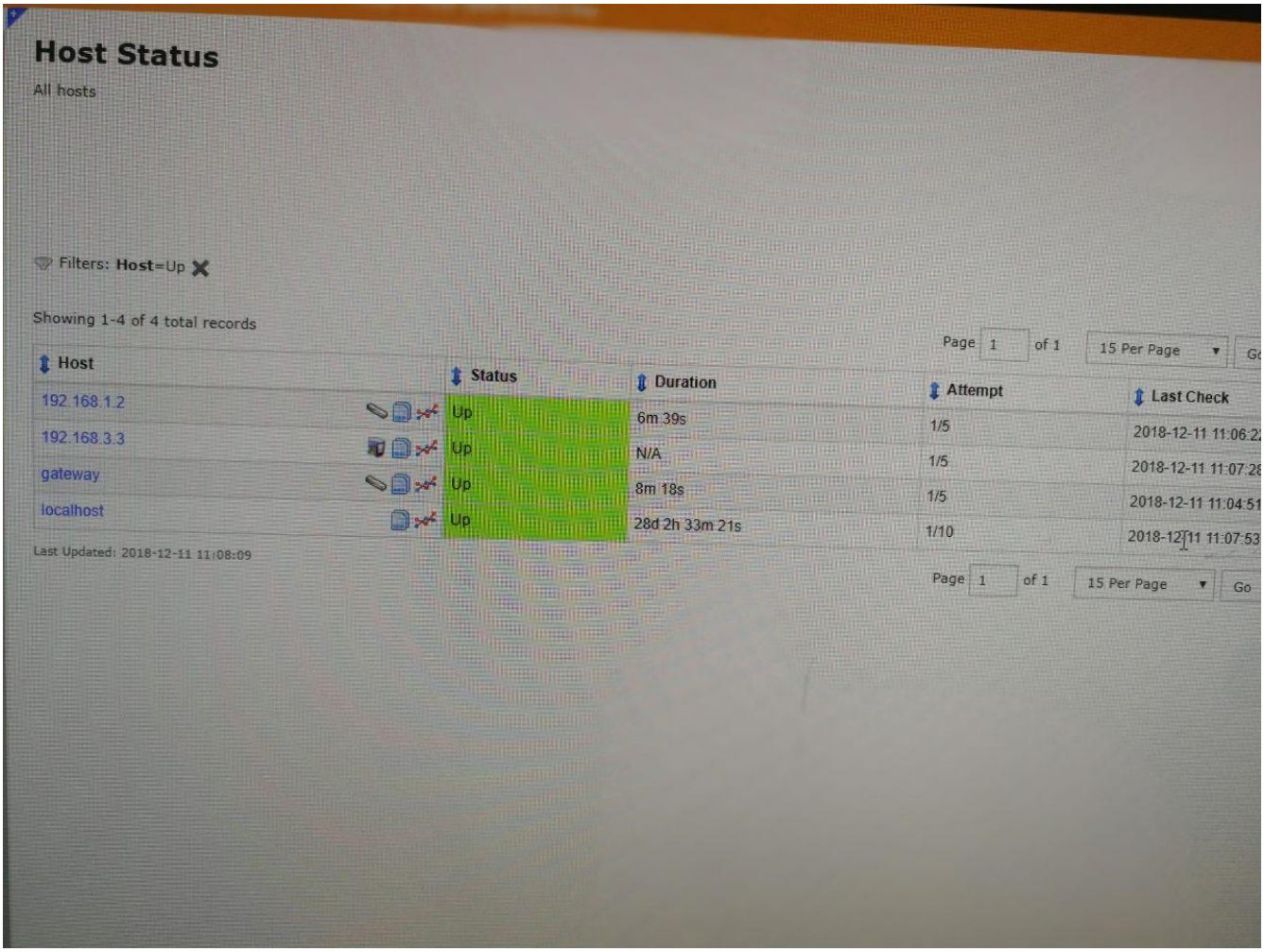

Configuration Wizard: Network Switch / Route
Switch Details
Switch/Router Address: 192.168.1.2
Host Name: 192.168.1.2
The name you'd like to have associated with this switch or router.
Services
Specify which services you'd like to monitor for the switch or router.
Ping
Monitors the switch/router with an ICMP ping. Useful for watching network latency and general uptime.
Bandwidth and Port Status
No ports were detected on the switch. Possible reasons for this include:
The switch is currently down
The switch does not exist at the address you specified
SNMP support on the switch is disabled
Troubleshooting Tip:
If you keep experiencing problems with the switch wizard scan, login to the Nagios XI server as the root user and execute the following command:
/usr/bin/cfgmaker --show-op-down --noreversedns --zero-speed '100000000' 'public@192.168.1.2:161::::2'
Send the output of the command and a description of your problem to the Nagios support team by posting to our online support forum.
Back
Next
Home
Views
Dashboards
Reports
Configure
Tools
Help
Admin
Nagios XI will expire in 60 days. Purchase a License Now or Enter your license key.
Configuration Wizard: Network Switch / Router - Step 3
Monitoring Settings
Define basic parameters that determine how the host and service(s) should be monitored.
Under normal circumstances:
Monitor the host and service(s) every 5 minutes.
When a potential problem is first detected
Re-check the host and service(s) every 1 minutes up to 5 times before sending a notification.
Back
Next
Finish

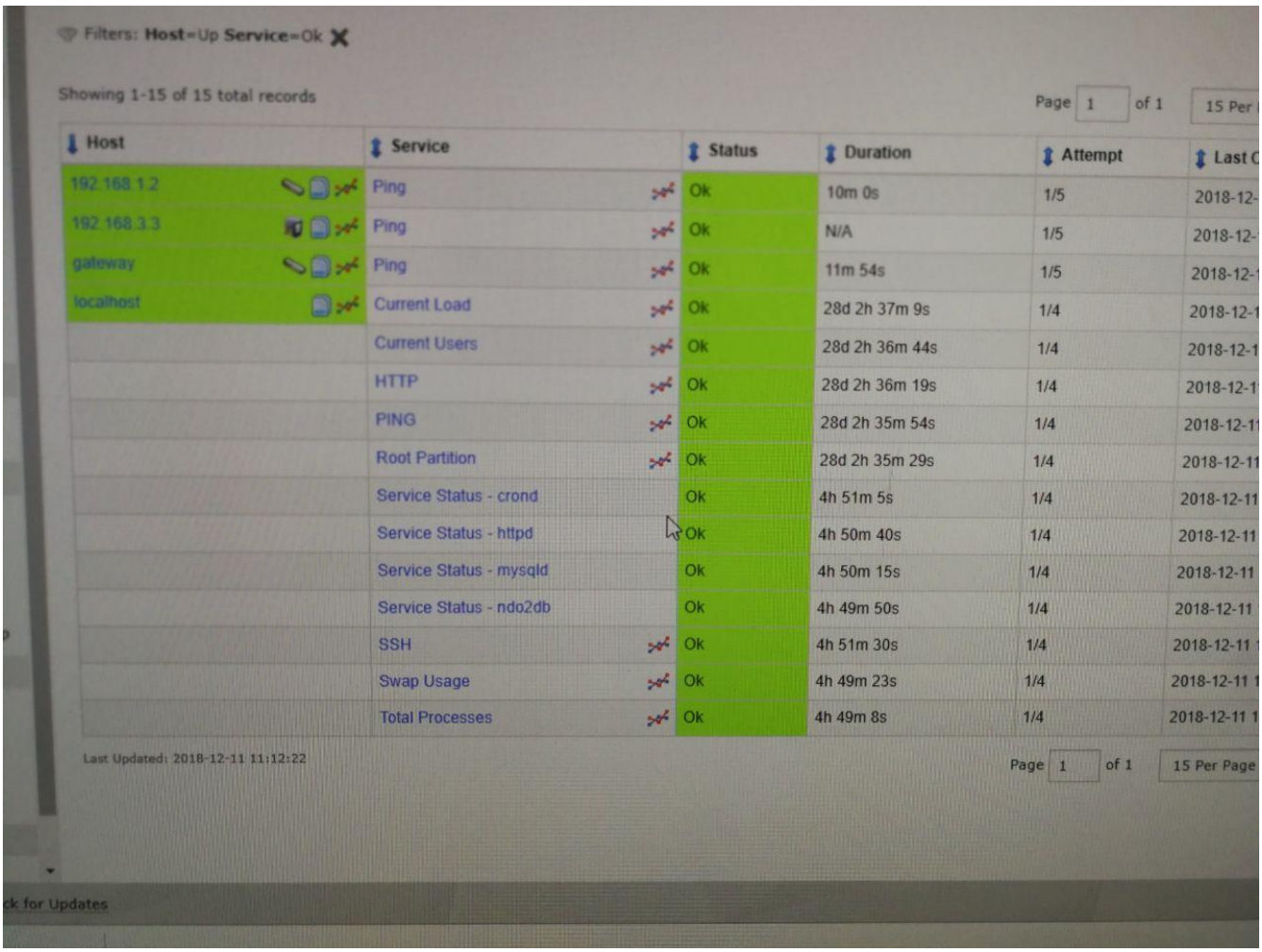
8. On fait la même manipe pour le Dell 9020

   Pour ce faire on va utiliser "windows SNMP" Il faut installer un agent disponible en téléchargement depuis la console de nagios.



On peut maintenant voir les différents hosts dans la consôle.


Host Status
All hosts
Filters: Host=Up
Showing 1-4 of 4 total records
Page 1 of 1 15 Per Page Go
Host
Status
Duration
Attempt
Last Check
192.168.1.2
Up
6m 39s
1/5
2018-12-11 11:06:22
192.168.3.3
Up
N/A
1/5
2018-12-11 11:07:28
gateway
Up
8m 18s
1/5
2018-12-11 11:04:51
localhost
Up
28d 2h 33m 21s
1/10
2018-12-11 11:07:53
Last Updated: 2018-12-11 11:08:09
Page 1 of 1 15 Per Page Go

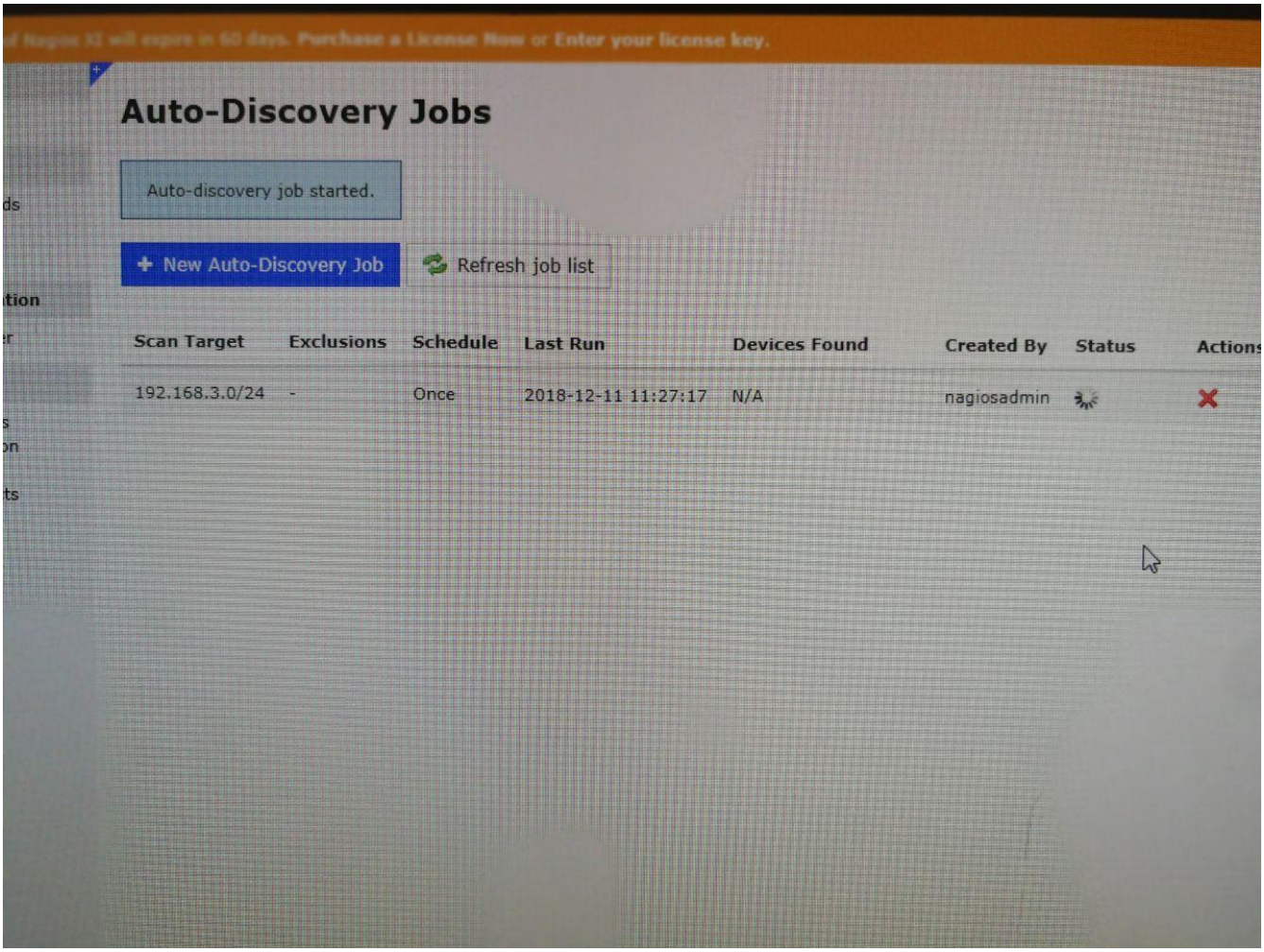


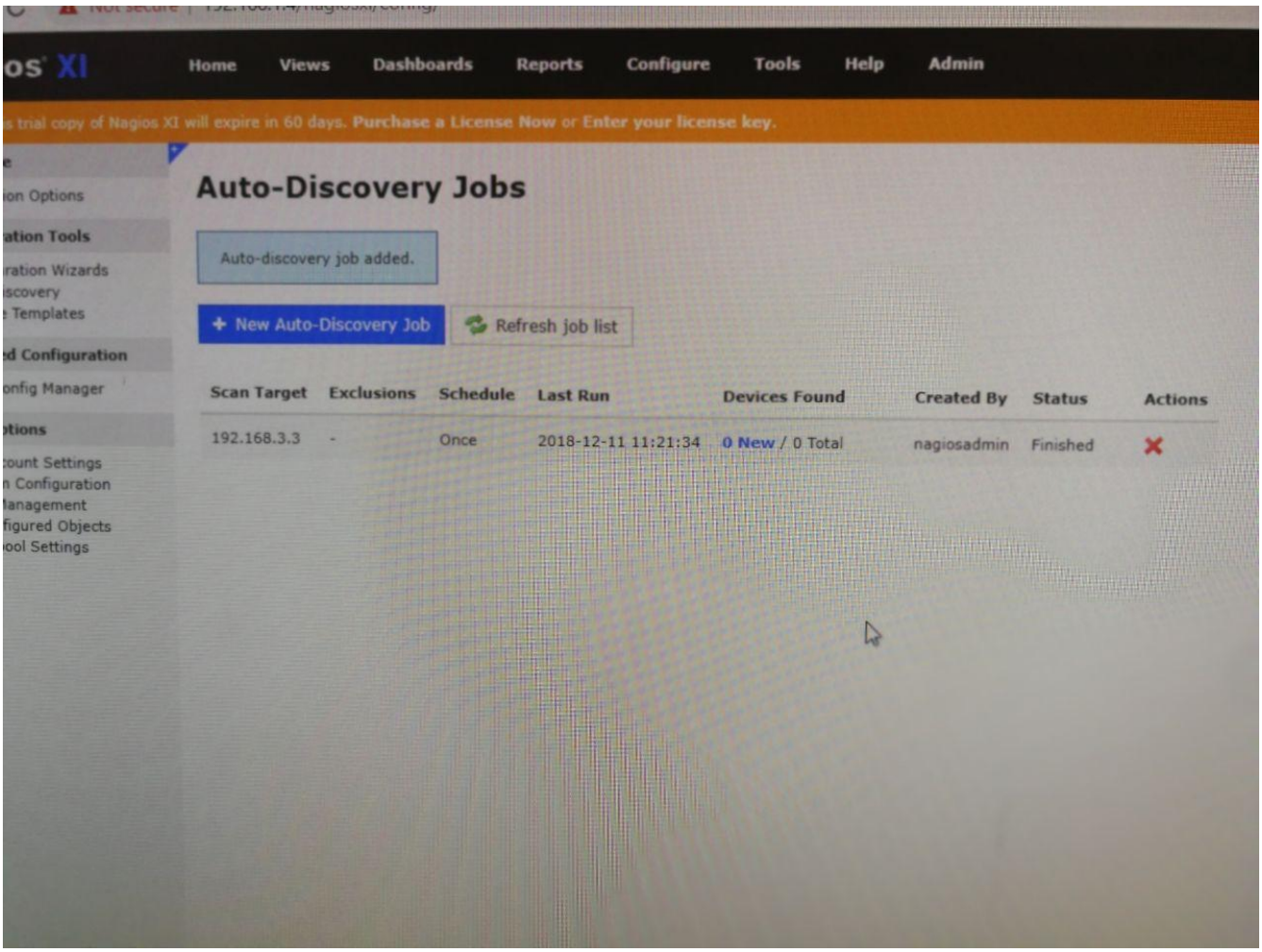
Question 3

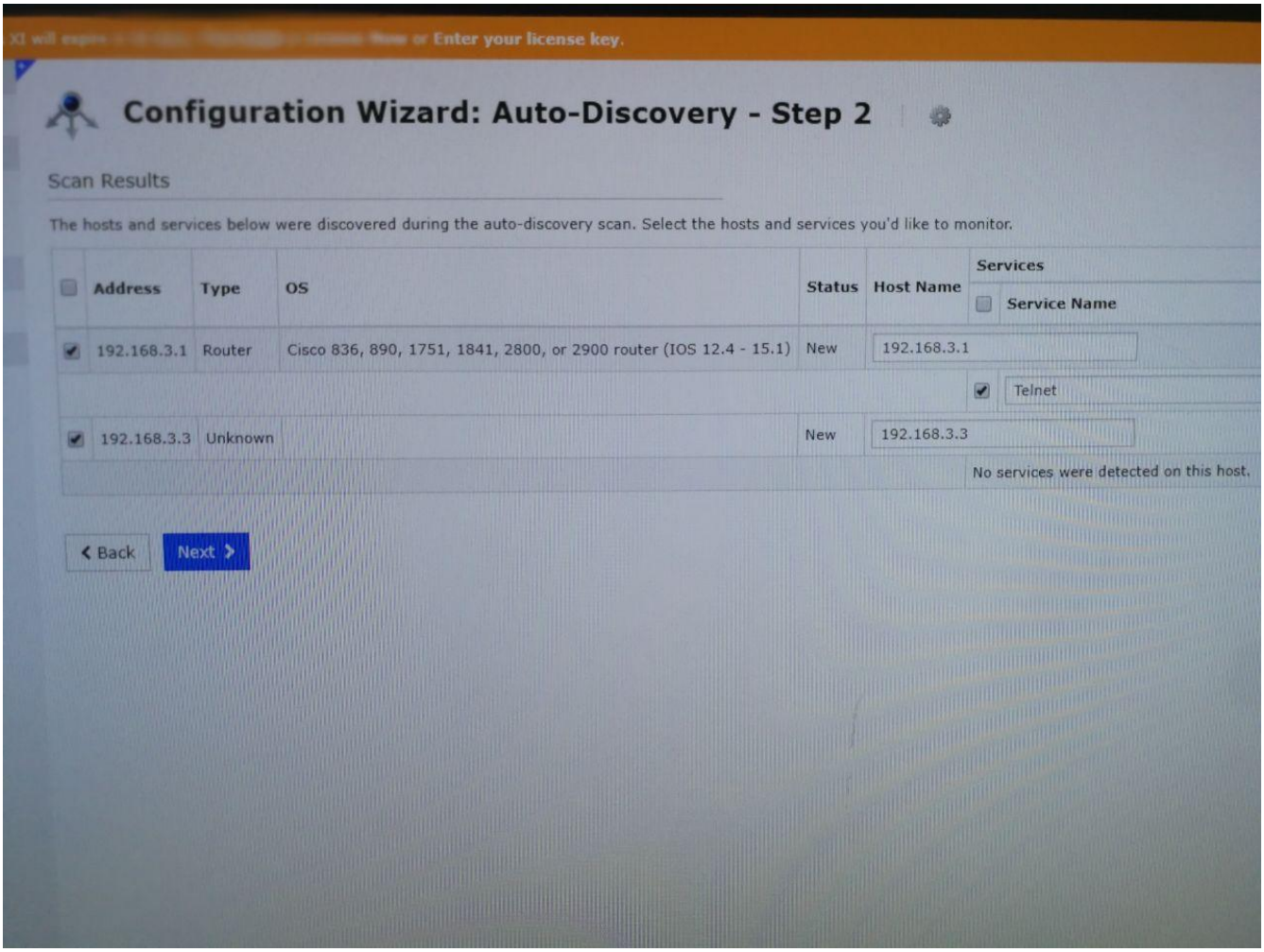
Deux moyens possible pour faire la découverte des hôtes est d'utiliser SNMP ou de faire un simple ping vers toutes les adresses IP.

Objectif 4

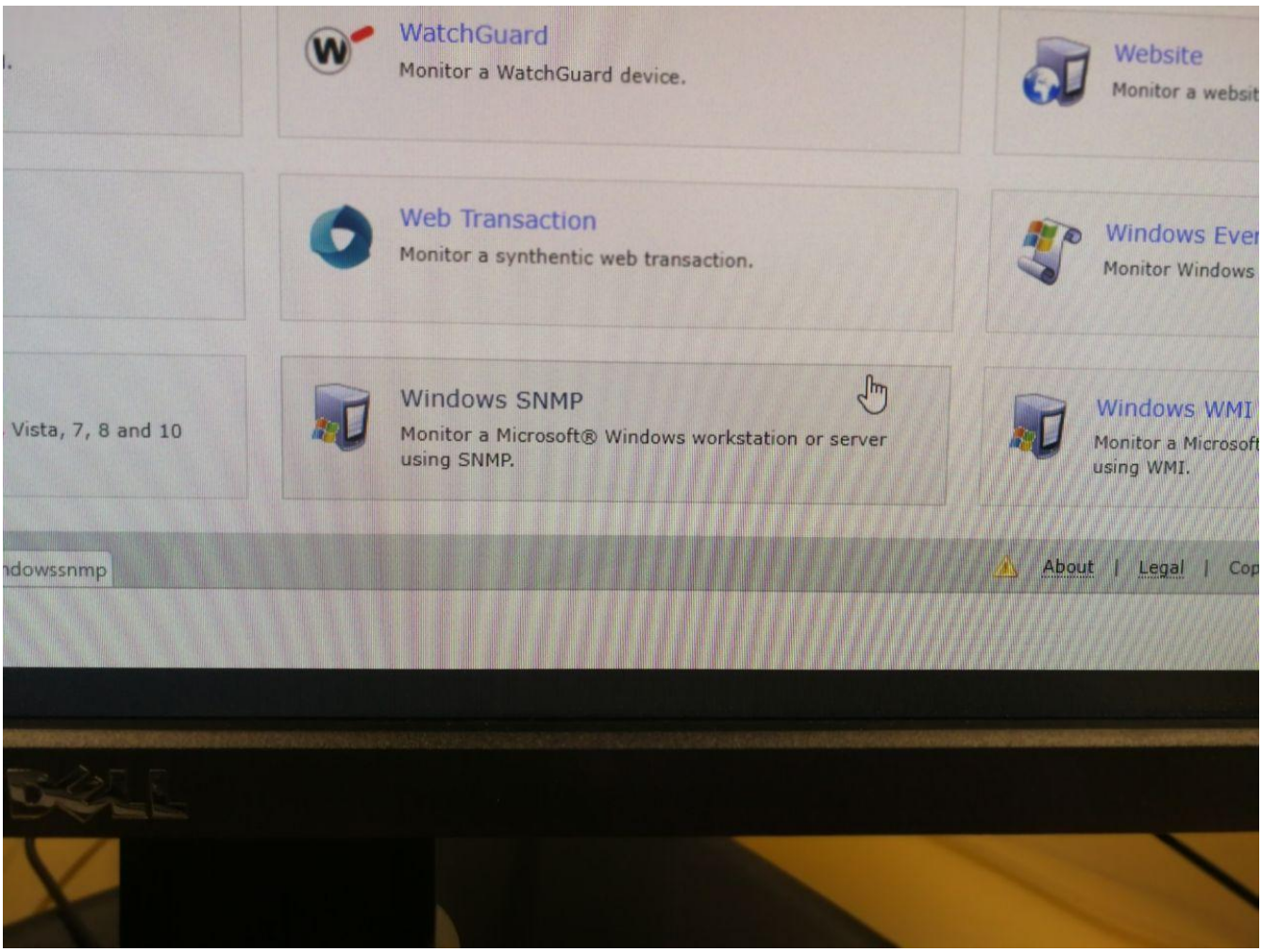
Pour l'auto découverte de la machine windows.


Purchase a License Now or Enter your license key.
Auto-Discovery Jobs
Auto-discovery job started.
New Auto-Discovery Job
Refresh job list
Scan Target
Exclusions
Schedule
Last Run
Devices Found
Created By
Status
Actions
192.168.3.0/24
-
Once
2018-12-11 11:27:17
N/A
nagiosadmin


os XI
Home
Views
Dashboards
Reports
Configure
Tools
Help
Admin
trial copy of Nagios XI will expire in 60 days. Purchase a License Now or Enter your license key.
ion Options
ation Tools
ration Wizards
iscovery
Templates
d Configuration
onfig Manager
tions
count Settings
n Configuration
lanagement
figured Objects
ool Settings
Auto-Discovery Jobs
Auto-discovery job added.
+ New Auto-Discovery Job
Refresh job list
Scan Target
Exclusions
Schedule
Last Run
Devices Found
Created By
Status
Actions
192.168.3.3
-
Once
2018-12-11 11:21:34
0 New / 0 Total
nagiosadmin
Finished

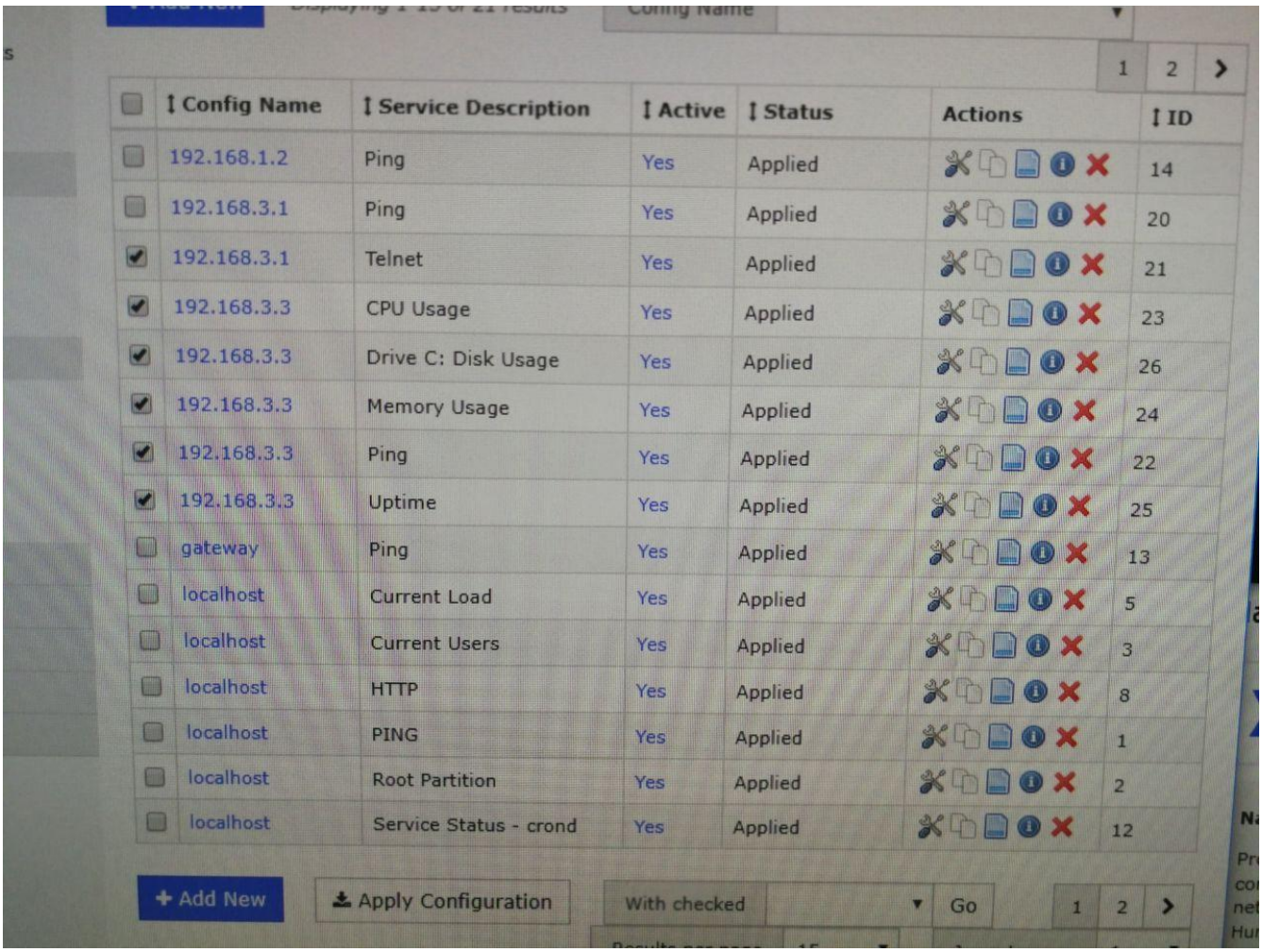


Une fois toutes la configuration faites, nous ne pouvions tout de même pas avoir accès aux données de la machine. Nous avons donc refait la configuration manuellement avec "windwos SNMP".



Question 4

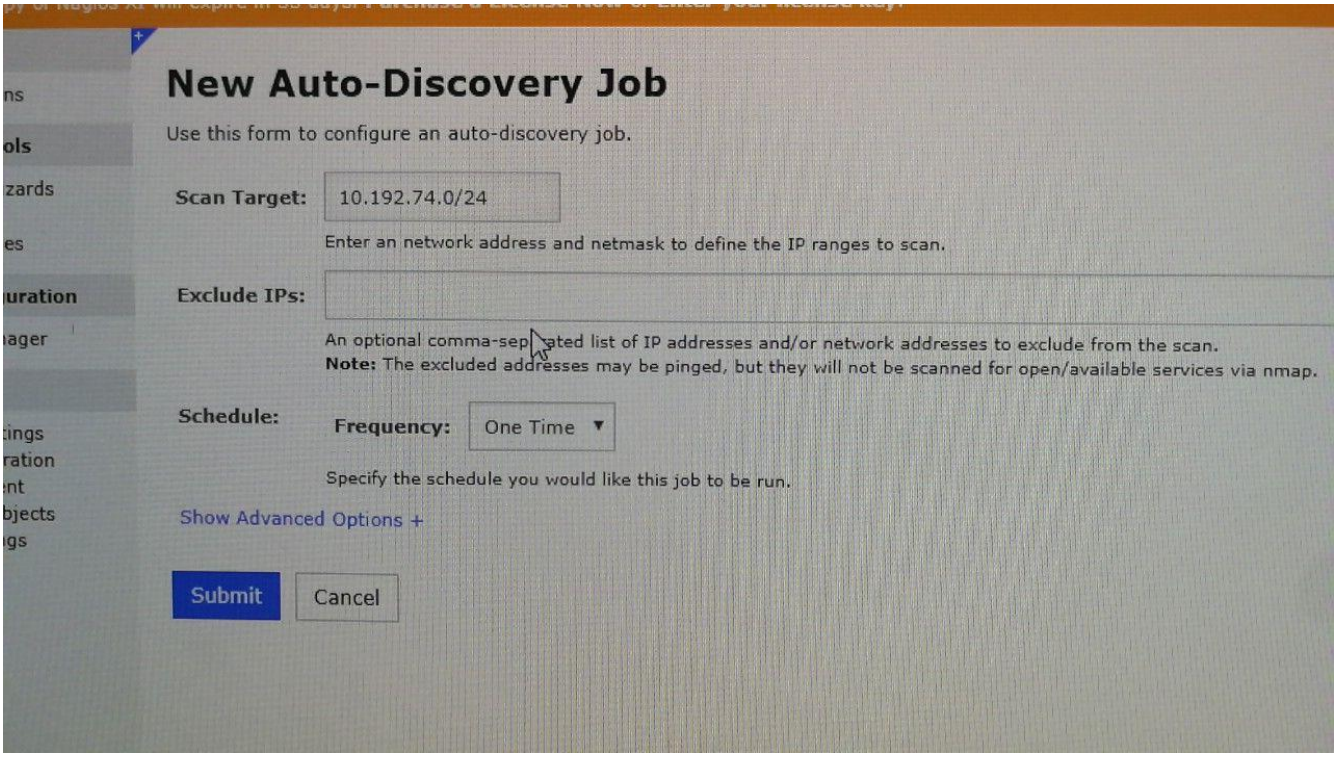
Il est possible de monitorer les services suivant.



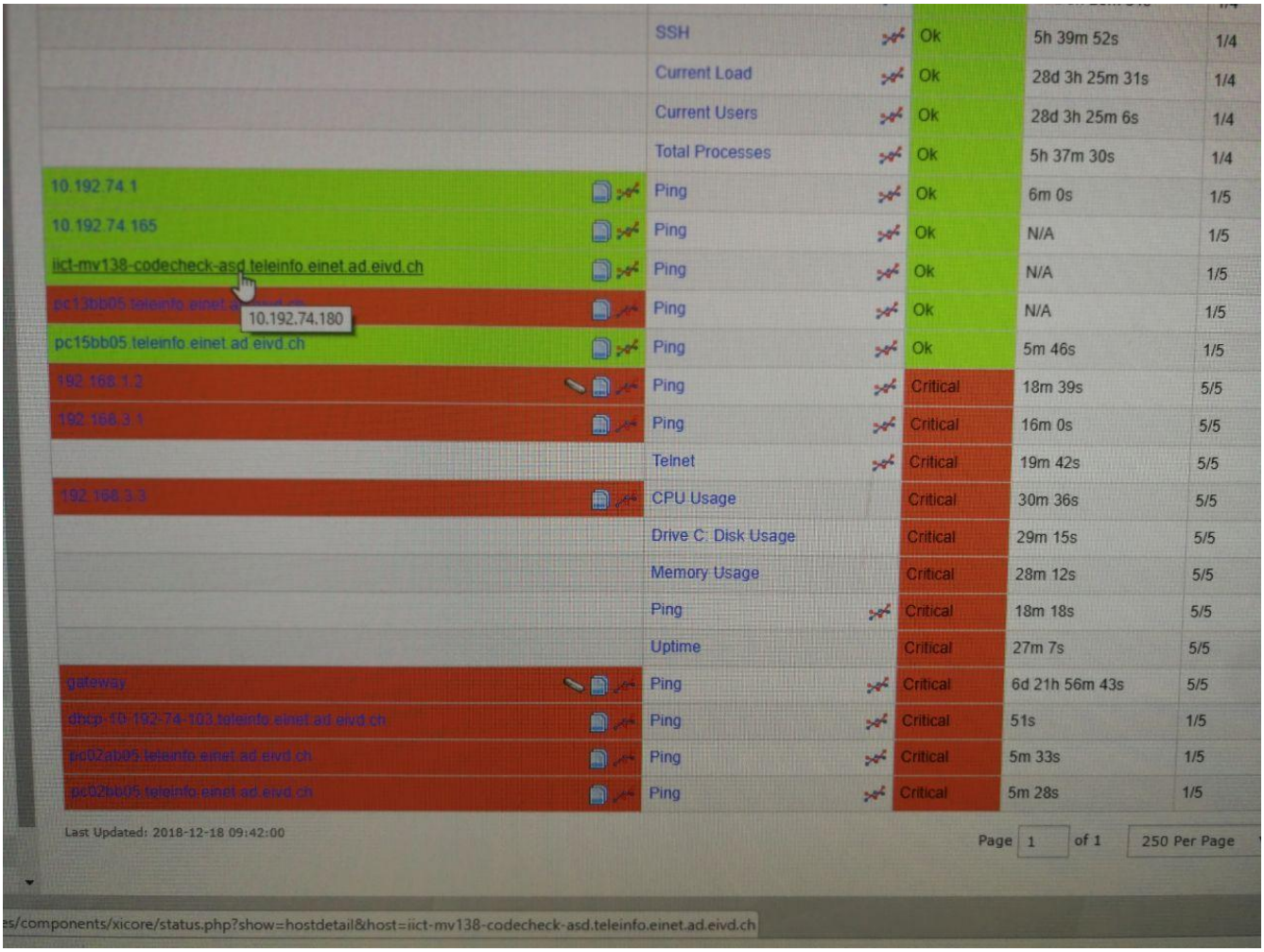
Config Name	Service Description	Active	Status	Actions	ID
192.168.1.2	Ping	Yes	Applied		14
192.168.3.1	Ping	Yes	Applied		20
192.168.3.1	Telnet	Yes	Applied		21
192.168.3.3	CPU Usage	Yes	Applied		23
192.168.3.3	Drive C: Disk Usage	Yes	Applied		26
192.168.3.3	Memory Usage	Yes	Applied		24
192.168.3.3	Ping	Yes	Applied		22
192.168.3.3	Uptime	Yes	Applied		25
gateway	Ping	Yes	Applied		13
localhost	Current Load	Yes	Applied		5
localhost	Current Users	Yes	Applied		3
localhost	HTTP	Yes	Applied		8
localhost	PING	Yes	Applied		1
localhost	Root Partition	Yes	Applied		2
localhost	Service Status - crond	Yes	Applied		12

Quesiton 5 - 6

Après avoir changé le réseau du serveur nagios sur le réseau de l'école est remis la carte réseau en mode DHCP. On peut faire une découverte de tous les devices du réseau.


New Auto-Discovery Job
Use this form to configure an auto-discovery job.
Scan Target:
10.192.74.0/24
Enter an network address and netmask to define the IP ranges to scan.
Exclude IPs:
An optional comma-separated list of IP addresses and/or network addresses to exclude from the scan.
Note: The excluded addresses may be pinged, but they will not be scanned for open/available services via nmap.
Schedule:
Frequency:
One Time
Specify the schedule you would like this job to be run.
Show Advanced Options +
Submit
Cancel


Scan Results
The hosts and services below were discovered during the auto-discovery scan. Select the hosts and services you'd like to monitor.
Address
Type
OS
Status
Host Name
Services
Service Name
Service
Port
Protocol
10.192.74.1 Unknown Cisco 1131AG WAP (IOS 12.3) New 10.192.74.1
No services were detected on this host.
10.192.74.13 Unknown New pc15bb05.teleinfo.einet.ad.eivd.ch
No services were detected on this host.
10.192.74.55 Unknown New pc02ab05.teleinfo.einet.ad.eivd.ch
No services were detected on this host.
10.192.74.69 Unknown New pc13bb05.teleinfo.einet.ad.eivd.ch
No services were detected on this host.
10.192.74.89 Unknown New pc02bb05.teleinfo.einet.ad.eivd.ch
No services were detected on this host.
10.192.74.103 Unknown New dhcp-10-192-74-103.teleinfo.einet
No services were detected on this host.
10.192.74.165 Unknown New 10.192.74.165
No services were detected on this host.
10.192.74.180 Unknown New iict-mv138-codecheck-asd.teleinfo
No services were detected on this host.



Vu que les services sont bloqués sur le réseau de l'école, nous ne pouvons pas identifier les services tournant sur les machines détectées. Nous pouvons tout de même supposer le rôle des serveurs :

- DHCP
- code check
- téléinfo

Objectif 5

- La supervision réseau (SMTP, POP3, HTTP, NNTP, PING)
- La supervision de ressources systèmes (charge processeur, état de disques, nombre d'utilisateurs connectés, process)
- La supervision d'applications.
- La notification par différents moyens de communications (SMS, mail, wap)
- L' exécution de commandes manuelles ou automatiques
- La représentation des états de ressources supervisées, par coloration.
- La cartographie du système d'information supervisé
- Le reporting