

Labo 3 Nagios

Joel Schär, Yann Lederrey, Yohann Meyer

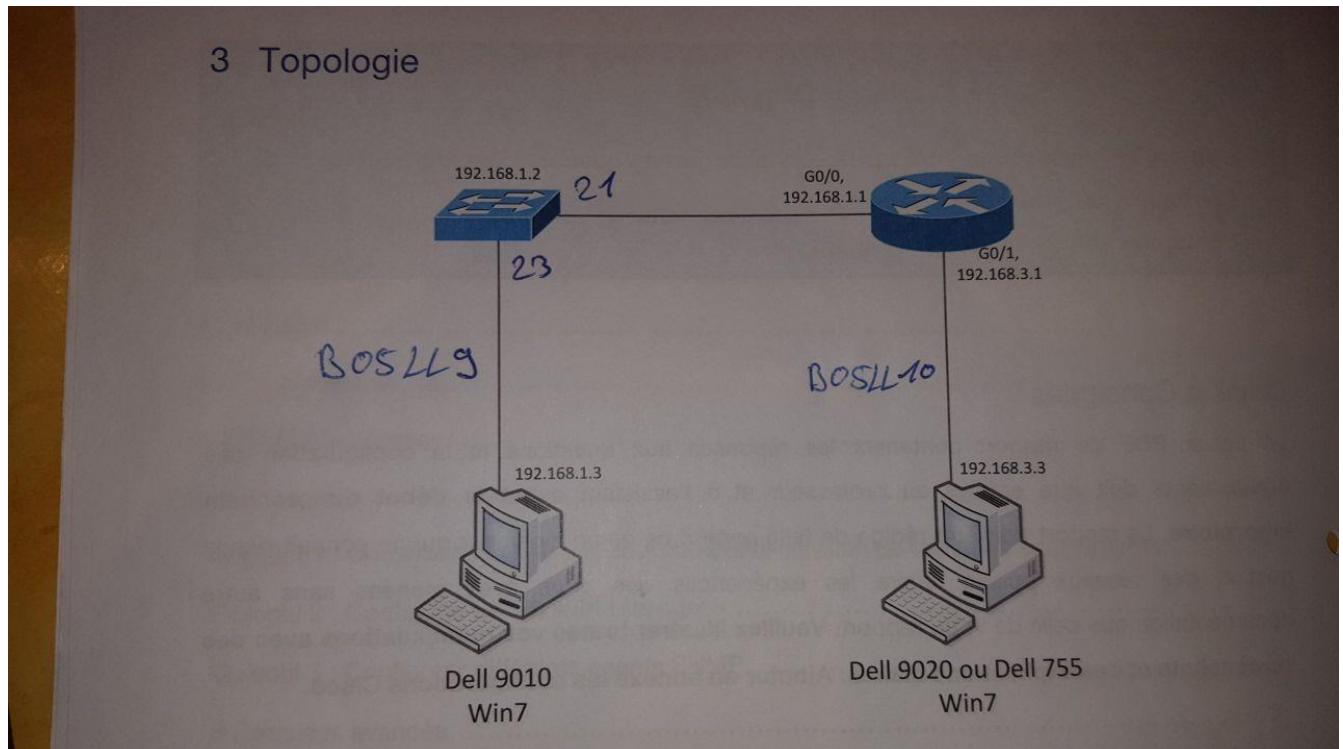
Objectif 1

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
> interface 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.

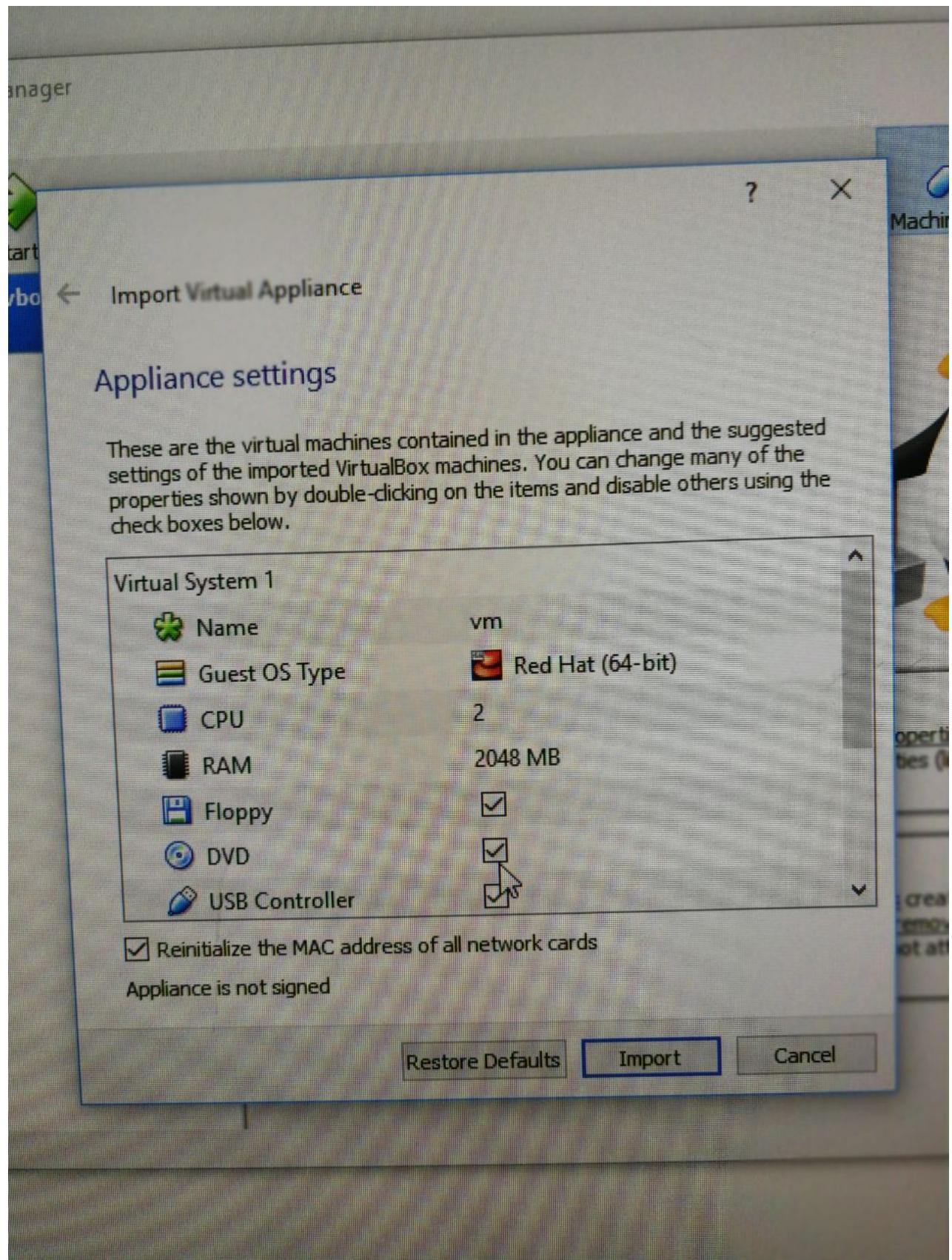
```
> enable
> configure terminal
> interface vlan1
> ip address 192.168.1.2 255.255.255.0
> no shutdown
> exit
> ip default-gateway 192.168.1.1
> exit
> exit
```

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

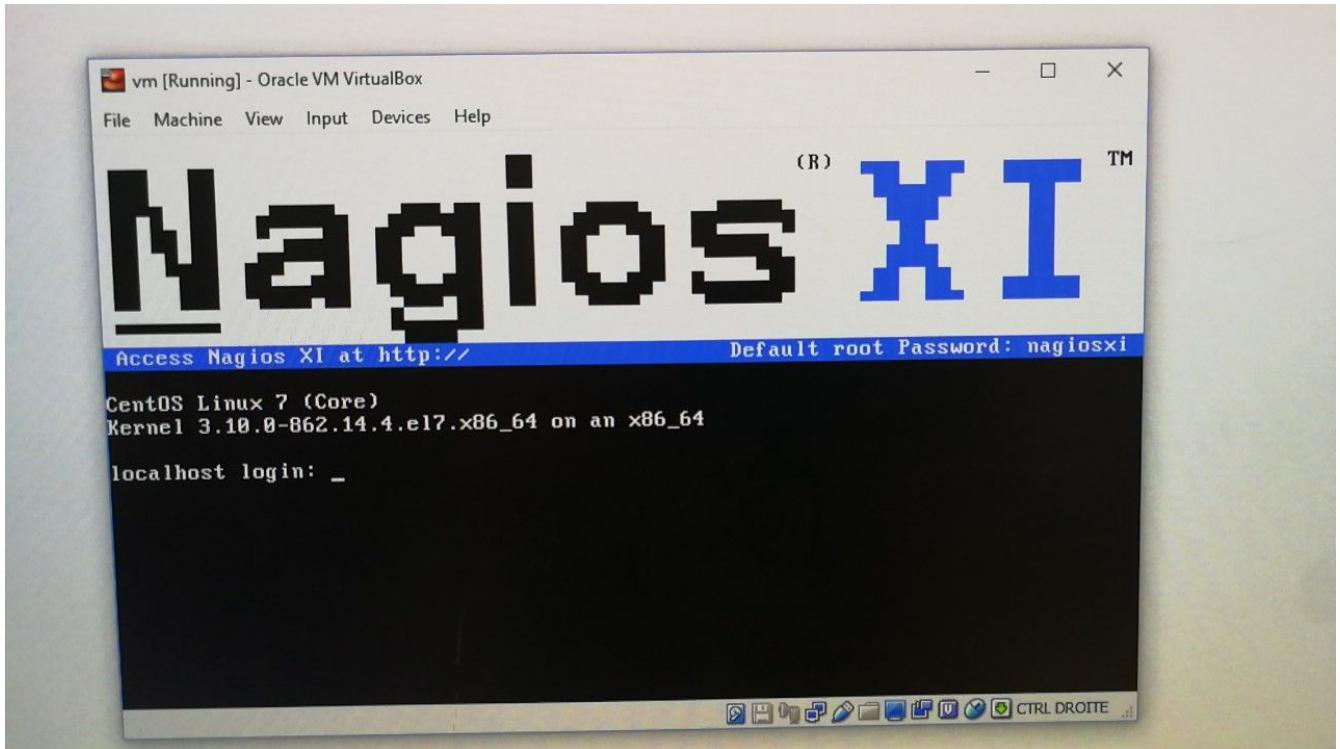
Objectif 2

Tutoriel:

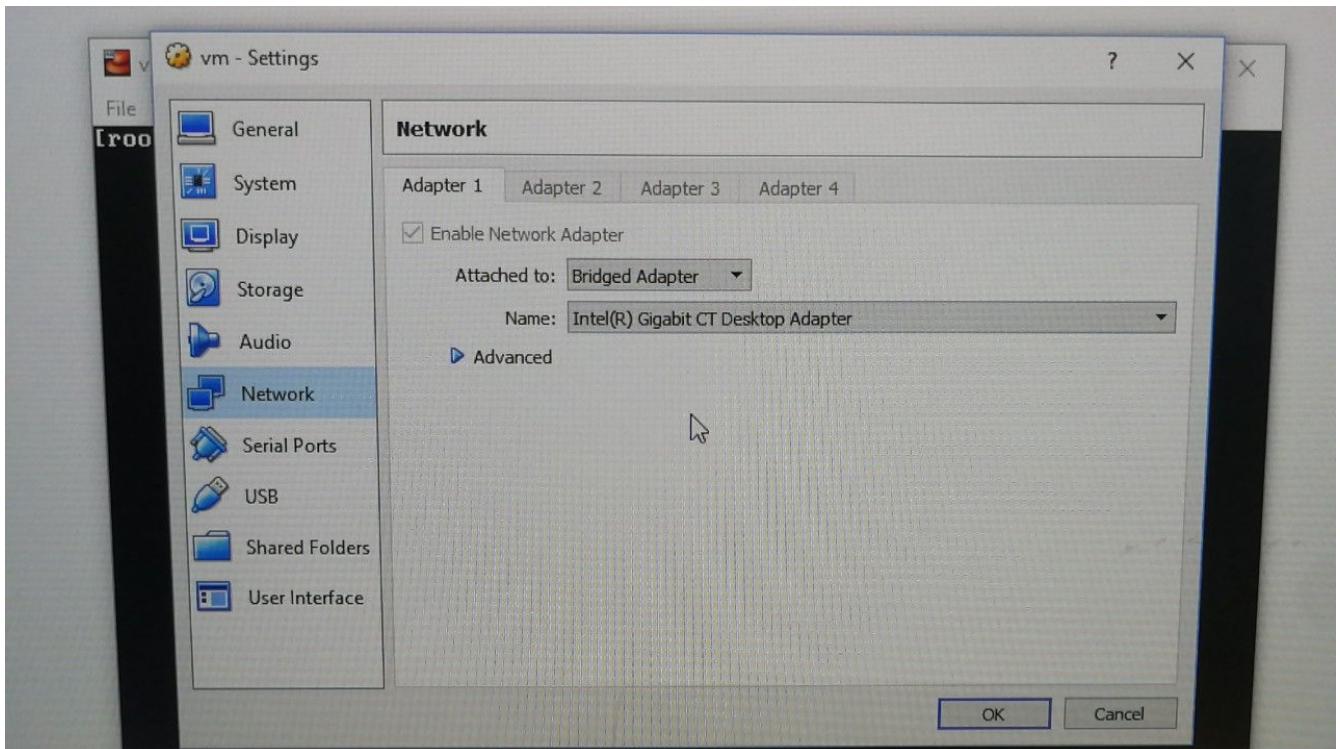
1. Télécharger la machine virtuel sur <https://www.nagios.com/downloads/nagios-xi/vmware>
2. double cliquez sur le fichier ova.
3. virtual box ouvre une page de settings, copiez les configurations suivantes.



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 `:wq` pour sauver vos changements.

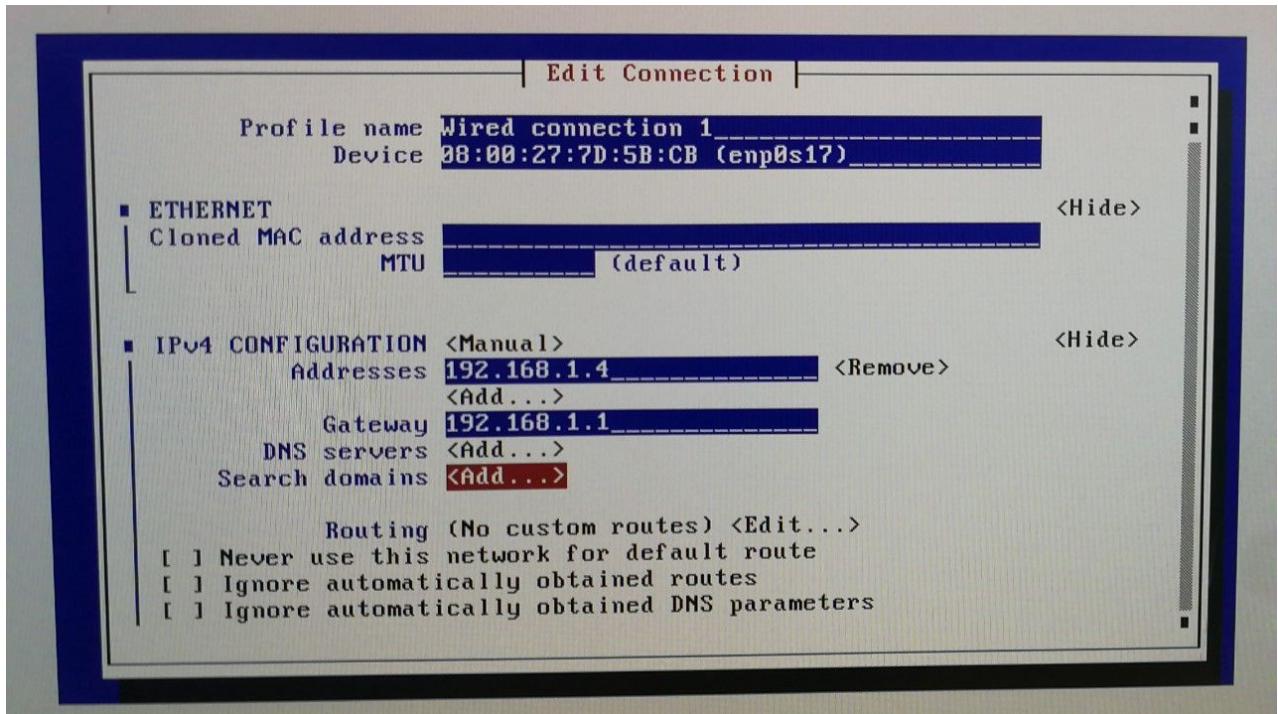
1. si le fichier n'existe pas, faites `localectl set-keymap ch-fr`

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.

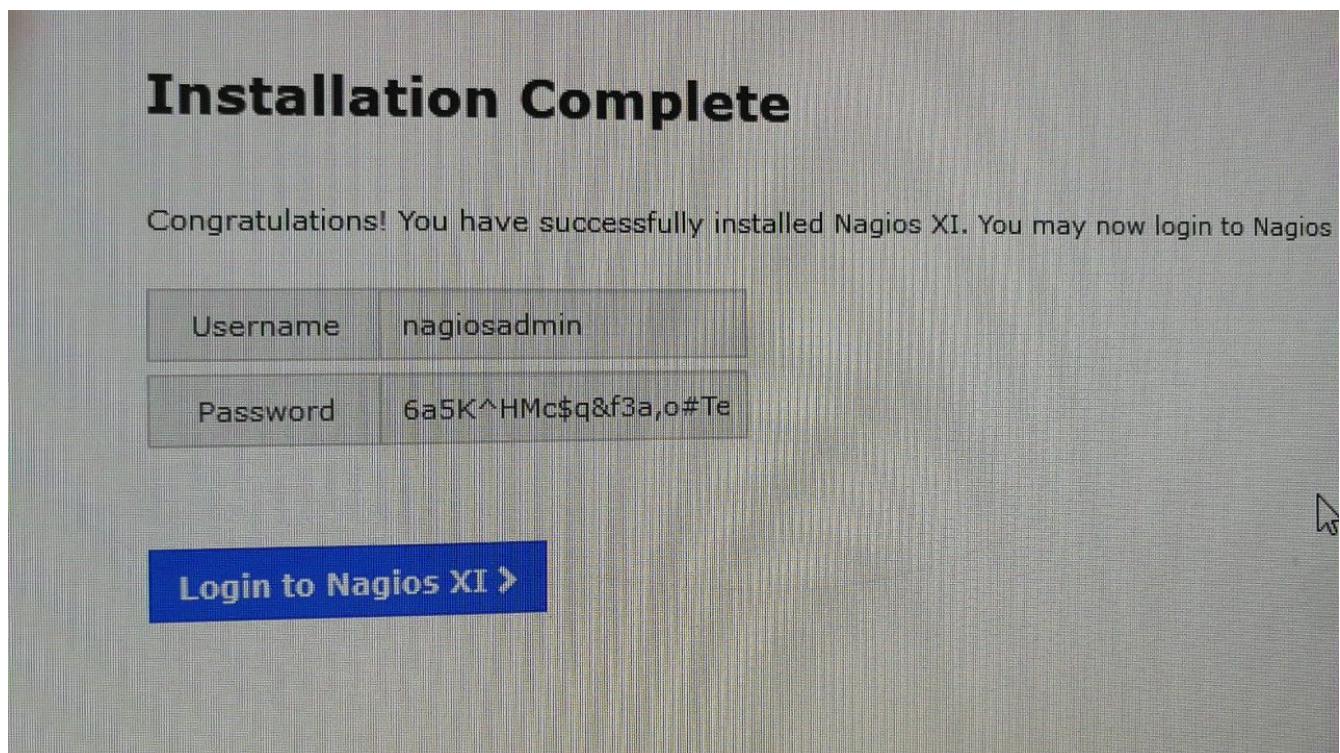
nmtui

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

The screenshot shows the 'Configuration Wizard: Network Switch / Router - Step 1' interface. At the top, there is a red error message box containing the text 'Must give either community or username.' Below this, the 'Router/Switch Information' section contains fields for 'IP Address' (192.168.1.1) and 'Port' (161). A note below the port field specifies it is 'The port of the network device'. There are three tabs at the bottom of this section: 'SNMPv1' (selected), 'SNMPv2c', and 'SNMPv3'. The 'SNMP Community' field is set to 'public'. A note below it says 'The SNMP community string required used to query the network device'. In the 'Monitoring Options' section, 'Monitor Using' is set to 'Port's Number'. A note below it says 'Select the port naming scheme that should be used.' The 'Scan Interfaces' checkbox is checked. In the 'Default Values' section, there are two pairs of input fields: 'Input Rate' (50%) and 'Output Rate' (80%). Below these is a 'Default Port Speed' field set to '100000000 bytes/second'. At the bottom of the page are 'Back' and 'Next >' buttons.

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 '10000000' '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 ▶](#)

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 minutes.

When a potential problem is first detected

Re-check the host and service(s) every minutes up to times before sending a notification.

◀ Back

Next ➤

✓ Finish

7. On fait la même manipe pour le switch

Configuration Wizard: Network Switch / Router - Step 1

Router/Switch Information

IP Address:

The IP address of the network device you'd like to monitor

Port:

The port of the network device

SNMPv1 SNMPv2c SNMPv3

SNMP Community:

The SNMP community string required used to query the network device

Monitoring Options

Monitor Using:

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 and bandwidth usage.

Default Values

⚠ Input Rate: % ⚠ Input Rate: %

⚠ Output Rate: % ⚠ Output Rate: %

Default Port Speed: bytes/second

[◀ Back](#) [Next ▶](#)

Configuration Wizard: Network Switch / Router - Step 3

Switch Details

Switch/Router Address:

Host Name:

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 minutes.

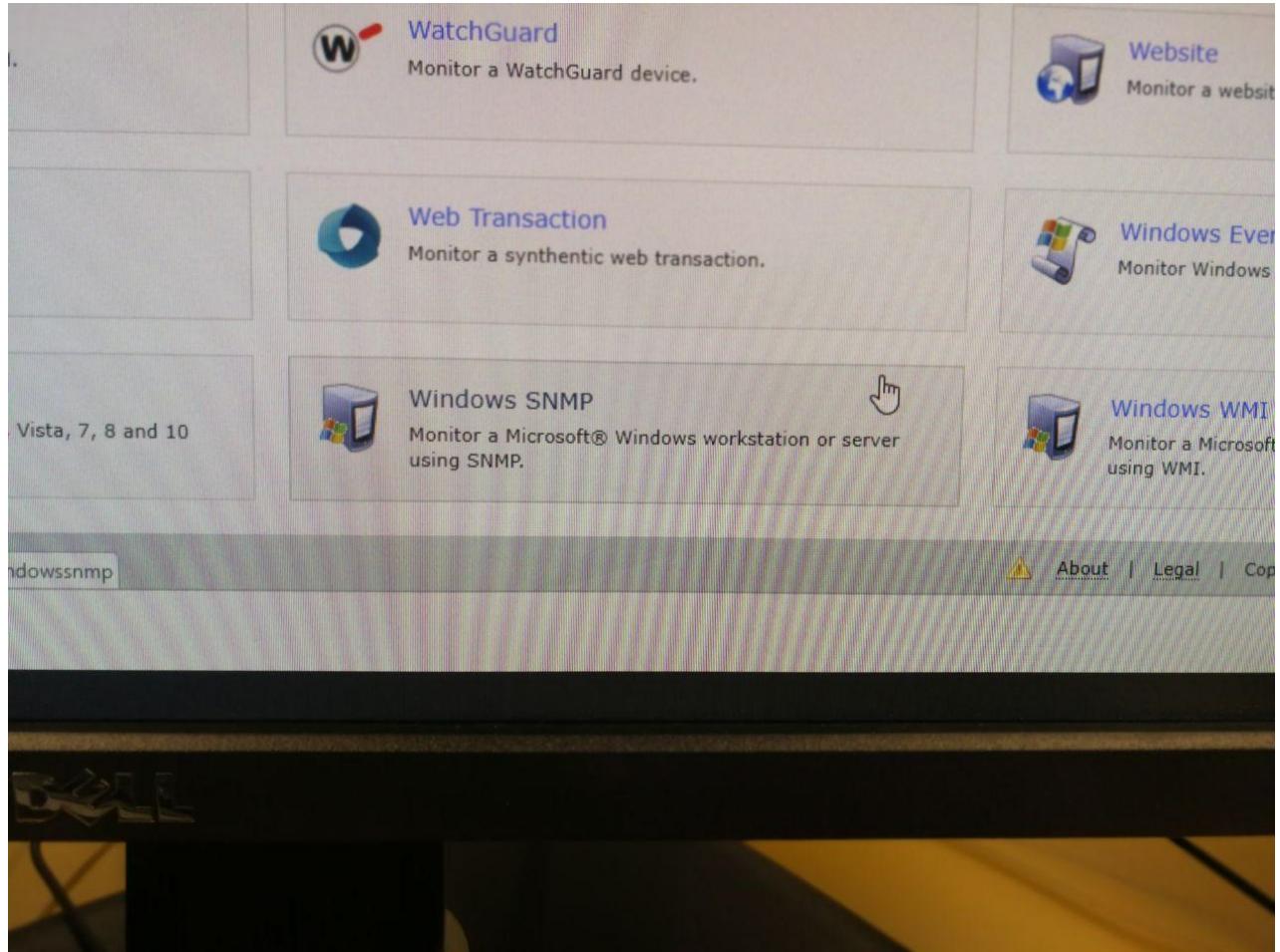
When a potential problem is first detected

Re-check the host and service(s) every minutes up to 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 X

Showing 1-4 of 4 total records

Host	Status	Duration	Attempt	Last Check
192.168.1.2	 Up	6m 39s	1/5	2018-12-11 11:06:21
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

Page 1 of 1 15 Per Page Go

Filters: Host=Up Service=Ok X

Showing 1-15 of 15 total records

Host	Service	Status	Duration	Attempt	Last C
192.168.1.2	Ping	Ok	10m 0s	1/5	2018-12-
192.168.3.3	Ping	Ok	N/A	1/5	2018-12-
gateway	Ping	Ok	11m 54s	1/5	2018-12-1
localhost	Current Load	Ok	28d 2h 37m 9s	1/4	2018-12-1
	Current Users	Ok	28d 2h 36m 44s	1/4	2018-12-1
	HTTP	Ok	28d 2h 36m 19s	1/4	2018-12-1
	PING	Ok	28d 2h 35m 54s	1/4	2018-12-11
	Root Partition	Ok	28d 2h 35m 29s	1/4	2018-12-11
	Service Status - crond	Ok	4h 51m 5s	1/4	2018-12-11
	Service Status - httpd	Ok	4h 50m 40s	1/4	2018-12-11
	Service Status - mysqld	Ok	4h 50m 15s	1/4	2018-12-11
	Service Status - ndo2db	Ok	4h 49m 50s	1/4	2018-12-11
	SSH	Ok	4h 51m 30s	1/4	2018-12-11
Swap Usage	Ok	4h 49m 23s	1/4	2018-12-11	
Total Processes	Ok	4h 49m 8s	1/4	2018-12-11	

Last Updated: 2018-12-11 11:12:22

Page 1 of 1 15 Per Page

Check for Updates

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.

Your Nagios XI license will expire in 60 days. 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

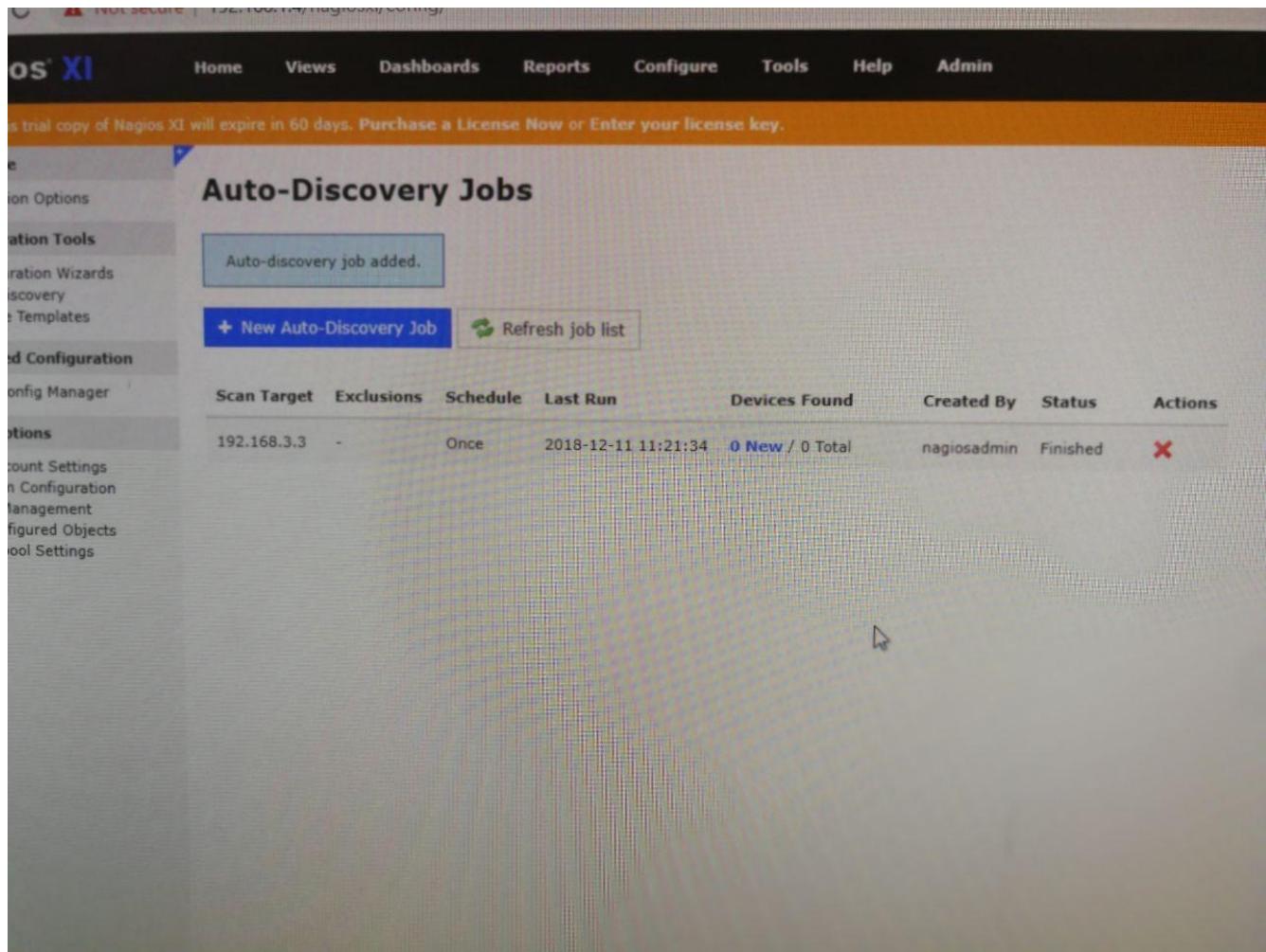
This trial copy of Nagios XI will expire in 60 days. Purchase a License Now or Enter your license key.

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	X



X will expire on 2014-08-15. Please [Renew](#) or [Enter your license key](#).

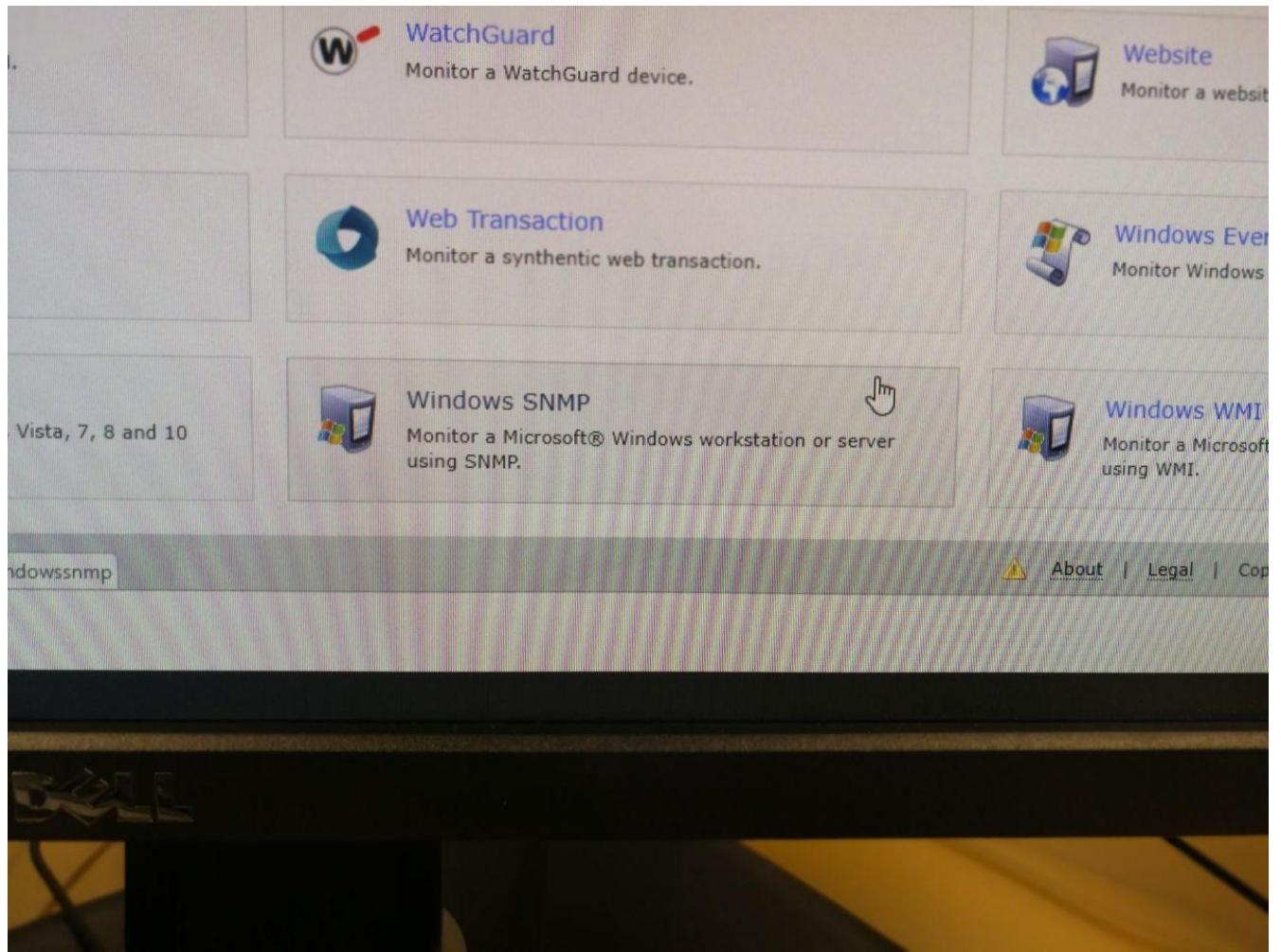
Configuration Wizard: Auto-Discovery - Step 2

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
						<input type="checkbox"/> Service Name
<input checked="" type="checkbox"/>	192.168.3.1	Router	Cisco 836, 890, 1751, 1841, 2800, or 2900 router (IOS 12.4 - 15.1)	New	192.168.3.1	<input checked="" type="checkbox"/> Telnet
<input checked="" type="checkbox"/>	192.168.3.3	Unknown		New	192.168.3.3	No services were detected on this host.

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 moniterer les services suivant.

Showing 1 to 21 of 21 results

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

[+ Add New](#) [Apply Configuration](#) With checked ▾ Go 1 2 >

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:	<input type="text"/>
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: <input type="button" value="One Time"/>
Specify the schedule you would like this job to be run.	
<input type="button" value="Show Advanced Options +"/>	
<input type="button" value="Submit"/> <input type="button" value="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.

<input type="checkbox"/>	Address	Type	OS	Status	Host Name	Services			
						<input type="checkbox"/>	Service Name	Service	Port
<input checked="" type="checkbox"/>	10.192.74.1	Unknown	Cisco 1131AG WAP (IOS 12.3)	New	10.192.74.1		No services were detected on this host.		
<input checked="" type="checkbox"/>	10.192.74.13	Unknown		New	pc15bb05.teleinfo.einet.ad.eivd.ch		No services were detected on this host.		
<input checked="" type="checkbox"/>	10.192.74.55	Unknown		New	pc02ab05.teleinfo.einet.ad.eivd.ch		No services were detected on this host.		
<input checked="" type="checkbox"/>	10.192.74.69	Unknown		New	pc13bb05.teleinfo.einet.ad.eivd.ch		No services were detected on this host.		
<input checked="" type="checkbox"/>	10.192.74.89	Unknown		New	pc02bb05.teleinfo.einet.ad.eivd.ch		No services were detected on this host.		
<input checked="" type="checkbox"/>	10.192.74.103	Unknown		New	dhcp-10-192-74-103.teleinfo.einet		No services were detected on this host.		
<input checked="" type="checkbox"/>	10.192.74.165	Unknown		New	10.192.74.165		No services were detected on this host.		
<input checked="" type="checkbox"/>	10.192.74.180	Unknown		New	iict-my138-codecheck-asd.teleinfo		No services were detected on this host.		

	SSH		Ok	5h 39m 52s	1/4
	Current Load		Ok	28d 3h 25m 31s	1/4
	Current Users		Ok	28d 3h 25m 6s	1/4
	Total Processes		Ok	5h 37m 30s	1/4
10.192.74.1	Ping		Ok	6m 0s	1/5
10.192.74.165	Ping		Ok	N/A	1/5
iict-mv138-codecheck-asd.teleinfo.einet.ad.eivd.ch	Ping		Ok	N/A	1/5
pc15bb05.teleinfo.einet.ad.eivd.ch	Ping		Ok	N/A	1/5
pc15bb05.teleinfo.einet.ad.eivd.ch	Ping		Ok	5m 46s	1/5
192.168.1.2	Ping		Critical	18m 39s	5/5
192.168.3.1	Telnet		Critical	16m 0s	5/5
192.168.3.3	CPU Usage		Critical	30m 36s	5/5
	Drive C: Disk Usage		Critical	29m 15s	5/5
	Memory Usage		Critical	28m 12s	5/5
	Ping		Critical	18m 18s	5/5
	Uptime		Critical	27m 7s	5/5
gateway	Ping		Critical	6d 21h 56m 43s	5/5
dhcp-f9-192-74-103.teleinfo.einet.ad.eivd.ch	Ping		Critical	51s	1/5
pc02ab05.teleinfo.einet.ad.eivd.ch	Ping		Critical	5m 33s	1/5
pc02bb05.teleinfo.einet.ad.eivd.ch	Ping		Critical	5m 28s	1/5

Last Updated: 2018-12-18 09:42:00

Page 1 of 1 250 Per Page

<http://es/components/xicore/status.php?show=hostdetail&host=iict-mv138-codecheck-asd.teleinfo.einet.ad.eivd.ch>

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