

Installation de Nagios XI

Nagios®
XI™

Sommaire

Introduction

- 1- Préparation d'une machine Debian pour l'installation de Nagios xi
 - a- Mise à jour de la distribution
 - b- Renommer la machine en Nagios xi c- Configuration des interfaces réseaux
- 2- Installation de Nagios XI
 - a- Installation rapide
 - b- Installation manuelle
 - c- Finalisation de l'installation
- 3- La supervision des clients
 - a- Supervision d'une machine Windows
 - i- Utilisassions du protocole Snmp
 - j- Utilisation de NCPA
 - b- Supervision d'une machine Linux
 - i- Utilisassions du protocole Snmp
 - j- Utilisation de NCPA
 - c- Supervision d'un site internet
 - d- Supervision d'une machine Windows
 - e- Supervision des switch et routeurs Cisco

<https://www.nagios.org/ncpa/#docs>

Introduction

Nagios XI une des solutions de supervision d'infrastructures réseaux parmi les plus utilisées.
Développée afin de combiner flexibilité et adaptabilité, elle permet de gérer des problématiques de supervision complexes de manière simple.

Allant au-delà des fonctionnalités de bases de supervision, Nagios XI est une solution d'alerte et de contrôle elle fournit une vue complète de l'infrastructure informatique, afin d'anticiper et de résoudre des problèmes pouvant affecter celle-ci.

VMs dont on aura besoin :

- Contrôleur de Domaine Windows Server avec le service Dns installé :
- PfSense : qui sert de routeur.
- Notre machine physique

1- Préparation d'une machine Debian pour l'installation de Nagios xi

a- Renommer la machine en Nagios xi

```
root@debian:~# hostnamectl set-hostname nagiosxi
```

b- Mettre une adresse fixe et configurer la résolution Dns

```
root@nagiosxi:~# vim /etc/network/interfaces
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address 172.20.0.34/24
    gateway 172.20.0.250
```

Maintenant on configure la résolution Dns

```
root@nagiosxi:~# vim /etc/resolv.conf |
```

```
domain sitka.local
search sitka.local
nameserver 172.20.0.14
```

On fait le test de résolution Dns

```
root@nagiosxi:~# nslookup www.google.com
Server: 172.20.0.14
Address: 172.20.0.14#53

Non-authoritative answer:
Name: www.google.com
Address: 142.250.178.132
Name: www.google.com
Address: 2a00:1450:4007:805::2004
```

c- Mise à jour de la distribution

```
root@debian:~# apt update && apt upgrade -y
```

1- Installation de Nagios XI

Il existe deux méthodes pour installer Nagios XI, elles effectuent toutes les deux une installation complète.

a- Méthode rapide

Tout d'abord on installe la commande curl car elle n'est pas installée par défaut,

```
root@nagiosxi:~# apt install curl
```

Sure un terminal on tape la commande ci-dessous, pour déclencher l'installation de Nagios

```
root@nagiosxi:~# curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh
```

b- Méthode manuelle

On crée un répertoire tmp

```
root@nagiosxi:~# mkdir tmp
```

On se place dans le répertoire tmp

```
root@nagiosxi:~# cd tmp
```

On télécharge sur le site officiel la dernière version de Nagios avec la commande wget

```
root@nagiosxi:~/tmp# wget http://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
```

On décomprime le fichier téléchargé

```
root@nagiosxi:~/tmp# tar xzfv xi-latest.tar.gz |
```

Une fois notre fichier est décompressé on se place dans le répertoire nagiosxi

```
root@nagiosxi:~/tmp# cd nagiosxi/
```

Puis on lance l'installation en exécutant le fichier fullinstall ; on confirme en choisissant Y pour continuer l'installation

```

root@nagiosxi:~/tmp/nagiosxi# ./fullinstall |
=====
Nagios XI Full Installer
=====

This script will do a complete install of Nagios XI by executing all necessary sub-scripts.

IMPORTANT: This script should only be used on a 'clean' install of CentOS, RHEL, Ubuntu LTS, Debian, or Oracle. Do NOT use this on a system that has been tasked with other purposes or has an existing
install of Nagios Core. To create such a clean install you should have selected only the base package in the OS installer.

Do you want to continue? [Y/n] Y

```

Une fois l'installation finaliser l'installation sur un navigateur avec l'url suivante

terminée le programme nous indique qu'on peut

<http://172.20.0.34/nagiosxi>

```

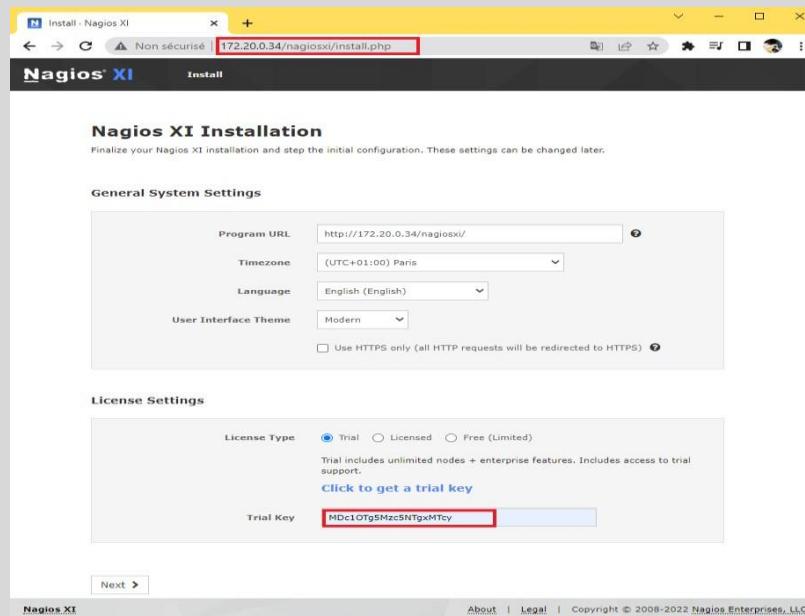
CCM data imported OK.
RESULT=0
Running './F-startdaemons'...
Daemons started OK
RESULT=0
Running './Z-webroot'...
RESULT=0

Nagios XI Installation Complete!
-----
```

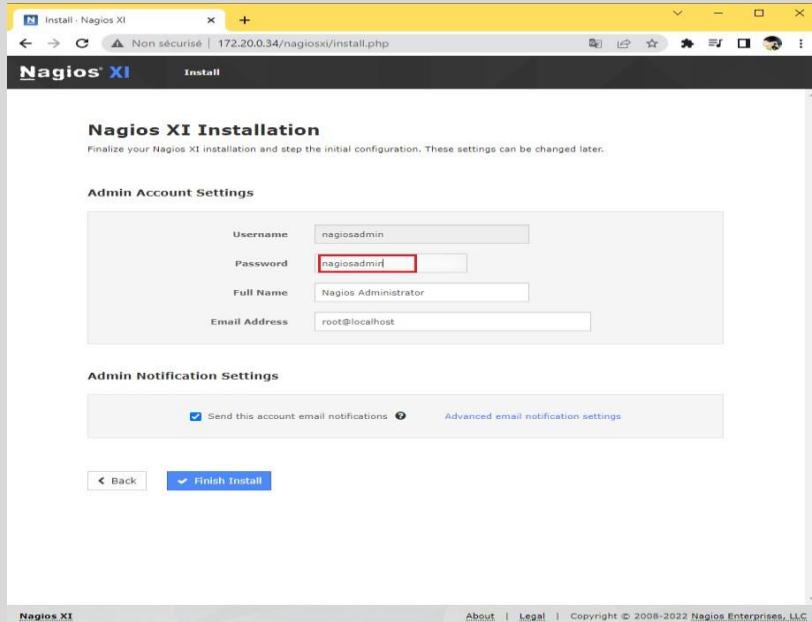
You can access the Nagios XI web interface by visiting:
<http://172.20.0.34/nagiosxi/>

c- Finalisation de l'installation sur un navigateur web

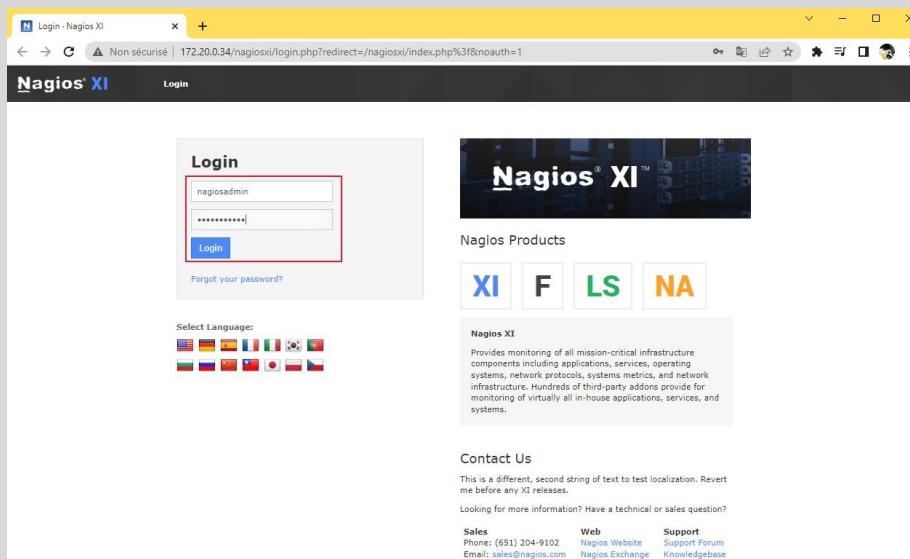
Avant de finaliser l'installation il va falloir s'inscrire sur le site de Nagios afin de recevoir une clé qui nous permettra d'avoir une période de 60 jours afin d'évaluer Nagios



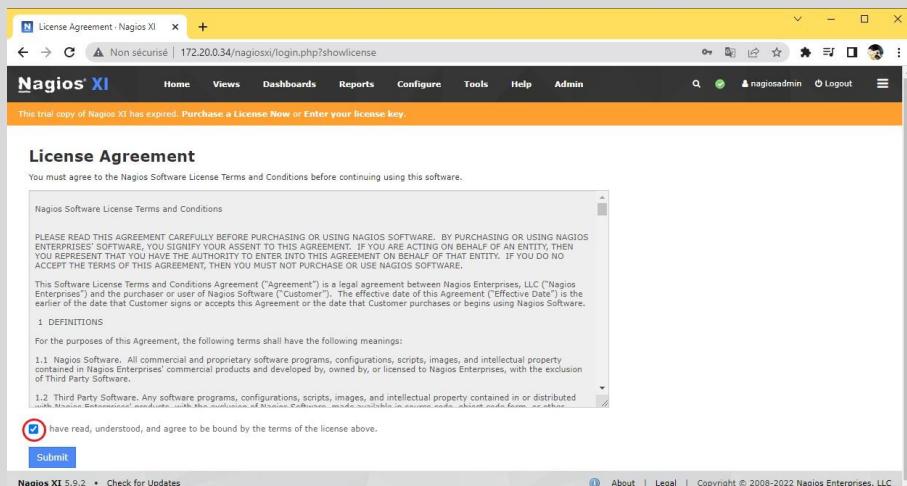
On rentre le login et on change le mot de passe par défaut le mot de passe continue en cliquant sur Finish install



On rentre à nouveau le login et le mot de passe : nagiosadmin pour les deux



On accepte les termes du contrat



On tombe en final sur l'interface web de nagiosxi

2- La supervision des clients

Nagios offre plusieurs moyens afin de remonter les clients pour la supervision: **SNMP, NCPA (Nagios Cross- Platform Agent), NRPE et Auto-discover**

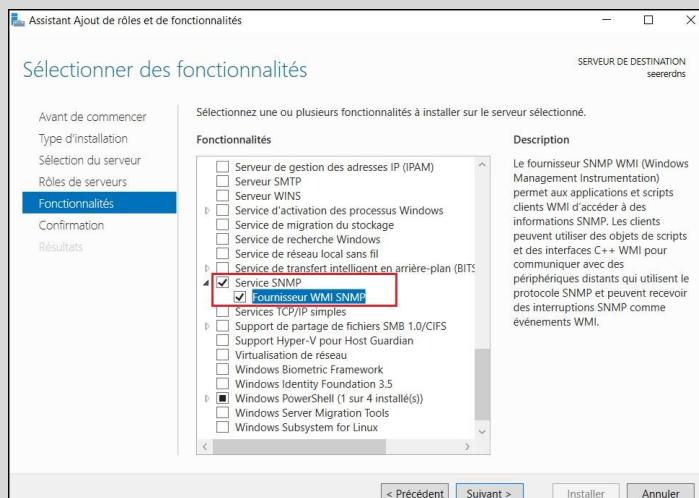
a- Supervision d'une machine Windows

<https://www.nagios.org/ncpa/getting-started.php>

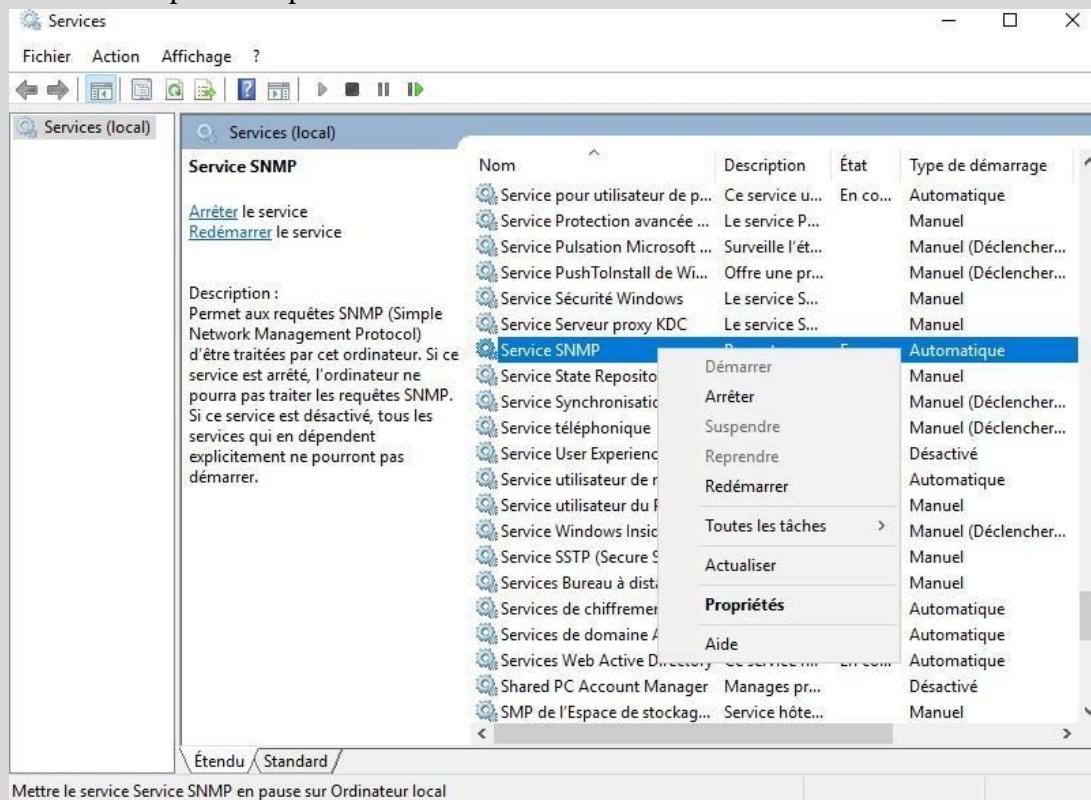
Installation du service/agent SNMP sur Windows Server :

On va dans "Gérer > Ajouter des rôles et fonctionnalités" on coche "Installation basée sur un rôle une fonctionnalité", on sélectionne le serveur local, on ne choisit aucun nouveau rôle mais on va ensuite cocher la fonctionnalité "Service SNMP" puis on clique sur "Ajouter la fonctionnalité" **Service SNMP + Fournisseur WMI SNMP**:

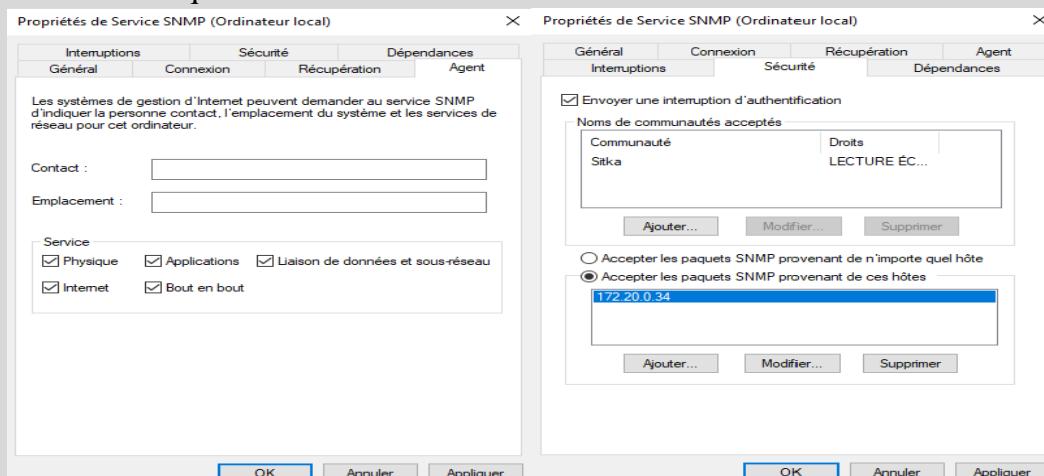
On clique ensuite sur "Installer" à l'écran de confirmation puis sur "Fermer" une fois le service installé.



On va ensuite ouvrir le gestionnaire des services en tapant "services" dans la barre de recherche Windows. Ensuite on va rechercher le service que l'on vient d'installer, faire un clic droit dessus puis "Propriété" :

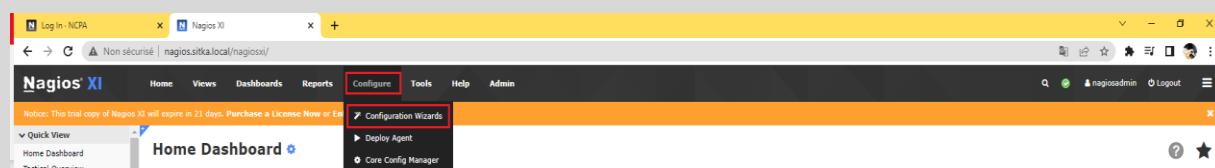


Dans l'onglet "Agent" des propriétés du service SNMP on coche toutes les cases en dessous dans la rubrique "Service" :



Puis dans l'onglet "Sécurité" on va d'abord ajouter notre communauté "Sitka" à la liste en Cliquant sur "Ajouter..." et en définissant ses droits et en la nommant, puis on coche "Accepter les paquets SNMP provenant de ces hôtes" et on retire "localhost" de la liste avant d'y ajouter l'adresse IP de notre serveur Nagios (??) Enfin on n'oublie pas de cliquer sur "Appliquer" puis "OK".

Maintenant on va sur le manager (Nagios XI) on sélectionne configure + configuration wizard



Ensuite on sélectionne Start Monitoring Now

The screenshot shows the Nagios XI configuration interface. On the left, a sidebar lists various configuration options like 'Configure Options', 'Configuration Wizards', and 'Auto Deployment'. The 'Auto Deployment' section is currently selected. In the main content area, there are four cards: 'Start Monitoring Now' (highlighted with a red box), 'Auto-Discovery', 'Advanced Configuration', and 'Manage Account Settings'. Below these cards, a message says 'Manage your monitoring config files using an advanced web interface. Recommended for experienced users.' A link 'Go to Nagios Core Config Manager' is provided.

On peut filtrer en fonction de l'équipement ou du système

The screenshot shows the Nagios XI configuration interface with the 'Show:' dropdown menu open. The menu contains several filter options: 'All', 'Hosts', 'Services', 'Problems', 'Events', 'Logs', 'Config', 'Jobs', and 'Metrics'. The 'All' option is selected. Below the menu, a list of monitoring targets is shown, each with a small icon and a brief description. Two specific items are highlighted with red boxes and numbered arrows: 'Windows Desktop' (arrow 1) and 'Windows SNMP' (arrow 2).

On rentre les paramètres de la machine qu'on veut superviser comme indiquer ci-dessous

Configuration Wizard: Windows SNMP - Step 1

Windows Machine Information

IP Address: 172.20.0.13
The IP address of the Windows machine you'd like to monitor.

Operating System: Windows Server 2019

SNMP Settings

Specify the settings used to monitor the Windows machine via SNMP.

SNMP Version: v2c
The SNMP protocol version used to communicate with the machine.
You may need to use SNMP v1 if your Windows system language is not English.

SNMP Port: 161
The SNMP port to use, the default is port 161.

SNMP Version Settings

SNMP Community: sitka

The SNMP community string required used to query the Windows machine.

< Back Next >

On sélectionne les éléments qu'on veut superviser

Configuration Wizard: Windows SNMP - Step 2

Windows Machine Details

IP Address: 172.20.0.13

Host Name: 172.20.0.13
The name you'd like to have associated with this Windows machine.

Server Metrics

Specify which services you'd like to monitor for the Windows machine.

Ping Monitors the machine with an ICMP "ping". Useful for watching network latency and general uptime.

CPU Monitors the CPU (processor usage) on the machine.
80 % | 90 %

Physical Memory Usage Monitors the physical (real) memory usage on the machine.
80 % | 90 %

Virtual Memory Usage Monitors the virtual memory usage on the machine.
5 % | 10 %

Disk Usage Monitors disk usage on the machine.
The wizard will populate detected drives automatically. To add more drives select a new drive from the dropdown list.

< Back Next >

Configuration Wizard: Windows SNMP - 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 >

The screenshot shows the Nagios XI Service Status page for host 172.20.0.13. It displays two summary tables: 'Host Status Summary' and 'Service Status Summary'. Below these are two detailed tables: 'Service Status' and 'Service Details'.

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0
Unhandled	Problems	All	
0	0	1	

Last Updated: 2023-01-01 16:56:13

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
0	0	0	0	11
Unhandled	Problems	All		
0	0	11		

Last Updated: 2023-01-01 16:56:13

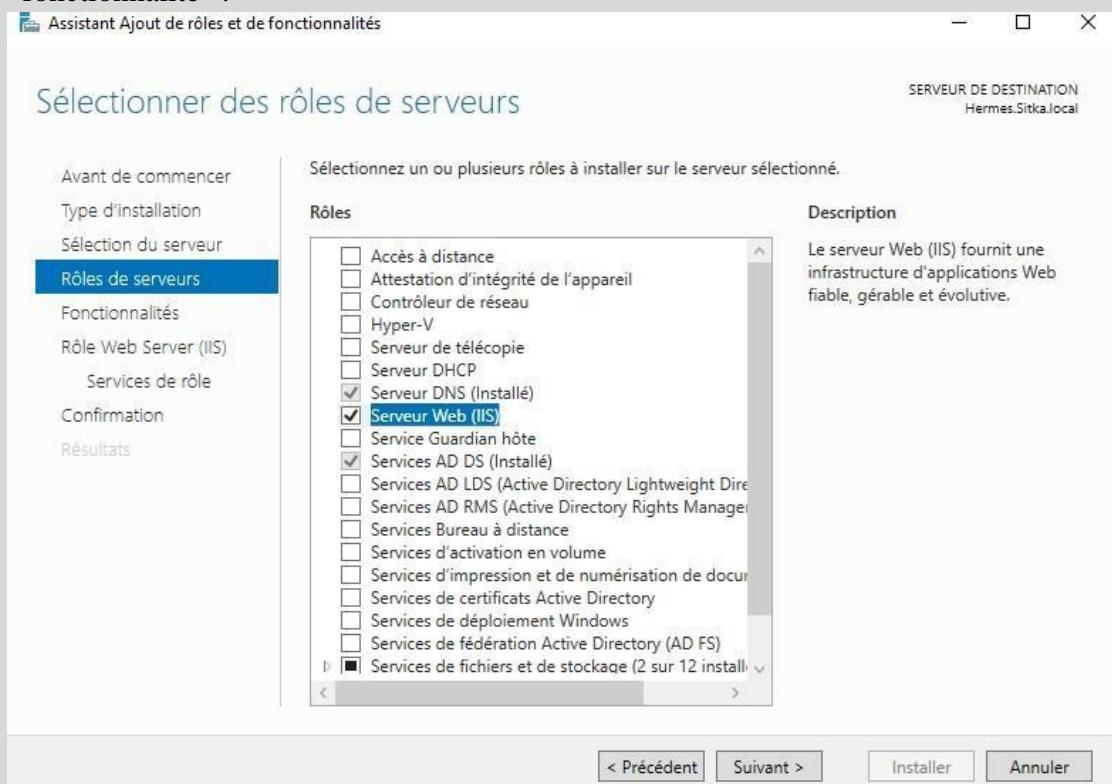
Service Status

Host	Service	Status	Duration	Attempt	Last Check	Status Information
172.20.0.13	CPU Usage	Ok	N/A	1/5	2023-01-01 16:56:14	2 CPU, average load 0.0% < 80% : OK
	Drive C: Disk Usage	Ok	N/A	1/5	2023-01-01 16:56:40	C:\ Label: Serial Number 6ef2d23c: 18%used(10931MB/61110MB) (>80%) : OK
	Physical Memory Usage	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 16:57:06
	Ping	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 16:57:32
	Serveur DHCP	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 16:57:58
	Serveur DNS	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 16:58:24
	Service SNMP	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 16:58:50
	Virtual Memory Usage	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 16:59:16
	dns.exe	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 16:59:42
	dwm.exe	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 17:00:08
	snmp.exe	Pending	N/A	1/5	N/A	Service check is pending... Check is scheduled for 2023-01-01 17:00:34

Last Updated: 2023-01-01 16:56:44

J- Utilisation de NCPA

Pour utiliser l'agent NCPA avec sa version web on va avoir besoin d'un serveur web, on va donc d'abord en installer un sur notre machine : on va dans "Gérer > Ajouter des rôles et fonctionnalités" on coche "Installation basée sur un rôle une fonctionnalité", on sélectionne le serveur local et on coche le rôle "Serveur Web (IIS)" puis on clique sur "Ajouter la fonctionnalité" :



On ne coche aucune fonctionnalité supplémentaire et on laisse aussi les services de rôle par défaut pour enfin cliquer sur "Installer" à l'écran de confirmation puis sur "Fermer" une fois le service installé.

On peut d'ailleurs vérifier l'installation du serveur web en tapant <http://localhost> dans le navigateur web du serveur WS 2022 :



On peut trouver les fichiers de la page d'accueil du serveur web dans le dossier
C:\inetpub\wwwroot

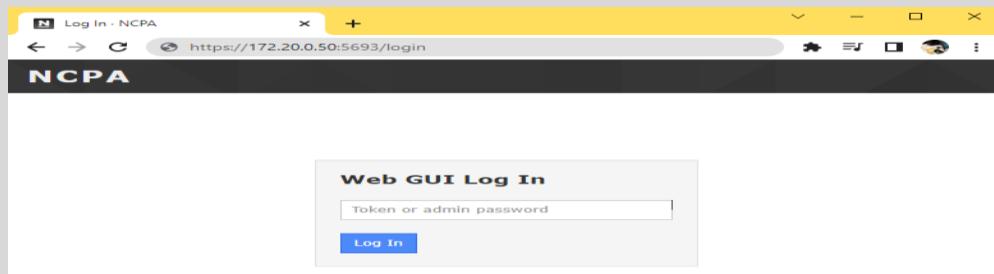
On va maintenant télécharger l'agent NCPA sur notre machine Windows Serveur à superviser à partir de ce lien : <https://www.nagios.org/ncpa/#downloads> (à gauche pour Windows)

On exécute d'abord le fichier téléchargé pour commencer l'installation de l'agent NCPA. On clique sur "I agree" en ce qui concerne la licence puis dans le champ "Token" de la configuration API on entre le nom de notre communauté ici "**Sitka**", dans le champ "Bind IP" on entre l'adresse IP du serveur client et on sélectionne aussi l'installation pour tous les utilisateurs. On laisse tout le reste par défaut et on clique sur "Install" :

On peut accéder à l'URL de NCPA par l'adresse
Charlie Li - BTS SIO SISR

École IRIS

<https://172.20.0.50:5693>



b- Supervision d'une machine Linux

i- Utilisassions du protocole Snmp

Installation du service/agent SNMP sur un serveur Ubuntu :

```
root@ubuntu:~# apt install snmpd snmp -y
```

On efface le contenu du fichier

```
root@ubuntu:~# echo "" > /etc/snmp/snmpd.conf
```

Ajouter les lignes suivantes :

```
root@ubuntu:~# vim /etc/snmp/snmpd.conf
sysLocation      sitka
sysContact       root <root@sitka.local>

#Snmp écoute toutes les adresses IPv4 du serveur
agentaddress    udp:161,udp6:[::1]:161

#nom de la community est sitka, avec l'argument {default} la communauté créée sera accessible par tout le monde,
#pour limiter l'accès à un réseau ou une adresse IP, il faut remplacer default par une notation CIDR
rocommunity      sitka default
```

On redémarre le service Snmpd

```
root@ubuntu:~# service snmpd restart
```

On vérifie le bon fonctionnement du service Snmpd

```
root@ubuntu:~# service snmpd status
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-01-02 09:26:30 UTC; 4min 5s ago
     Main PID: 16852 (snmpd)
        Tasks: 1 (limit: 4534)
       Memory: 3.6M
          CPU: 72ms
        CGroup: /system.slice/snmpd.service
                └─16852 /usr/sbin/snmpd -L0w -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f

janv. 02 09:26:30 ubuntu systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon...
janv. 02 09:26:30 ubuntu systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
```

On peut ensuite vérifier si le service SNMP fonctionne avec la commande ci-dessous

```
root@ubuntu:~# snmpwalk -v1 -c Sitka 172.20.0.51
```

Si le service fonctionne, la commande affichera plein d'OID à l'écran :

```

iso.3.6.1.2.1.1.1.0 = STRING: "Linux ubuntu 5.15.0-56-generic #62-Ubuntu SMP Tue Nov 22 19:54:14 UTC 2022 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (29623) 0:04:56.23
iso.3.6.1.2.1.1.4.0 = STRING: "root <root@sitka.local>"
iso.3.6.1.2.1.1.5.0 = STRING: "ubuntu".
iso.3.6.1.2.1.1.6.0 = STRING: "sitka"
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00

```

Maintenant que SNMP est installé sur notre machine on peut remonter Ubuntu sur Nagios même procédure qu'avec Windows en choisissant les service qu'on veut superviser

The screenshot shows the Nagios XI configuration interface. On the left, a sidebar lists various configuration sections like Configuration Options, Configuration Tools, Auto Deployment, Advanced Configuration, and More Options. The main panel is titled 'Configuration Wizard: Linux SNMP - Step 1'. It has three main sections: 'Linux Machine Information' (IP Address: 172.20.0.51), 'SNMP Settings' (SNMP Version: 2c, SNMP Port: 161), and 'SNMP Version Settings' (SNMP Community: sitka). At the bottom, there are 'Back' and 'Next >' buttons.

j- Utilisation de NCPA ; même principe qu'avec Windows

Installation de l'agent NCPA sur le serveur Ubuntu :

Pour utiliser l'agent NCPA on peut utiliser un serveur web, on installe donc aussi le paquet **apache2**.

```
root@ubuntu:~# apt install apache2 -y
```

Au lieu des paquets **snmpd** et **snmp** ici on effectuera l'installation et la configuration de base selon le guide du site officiel de Nagios <https://www.nagios.org/ncpa/#downloads> (sélectionner notre OS et cliquer sur "Install using Nagios repo" pour procédure) puis <https://www.nagios.org/ncpa/getting-started.php#linux>

Downloads

Latest stable agent version - **2.4.0** · View the [changelog](#) to see a list all features and bug fixes.

Don't see your version of OS on this list? Request it on [GitHub](#) or help us build for it!



Windows

[EXE Installer - 32bit](#)

Windows Vista +
Windows Server 2008 +



Ubuntu

[Install using Nagios repo - Recommended](#)

Ubuntu 19+ DEB - 32bit DEB - 64bit
Ubuntu 14-18 DEB - 32bit DEB - 64bit



Mac

[macOS 10.15+ DMG Installer - 64bit](#)

(Catalina)

Other Downloads

Download the plugin, older versions, and development versions.

Nagios Plugin

For active checks. Version: **1.2.4**
[Download check_ncpa.py](#)

Archived Versions

Download the older versions of NCPA. Go to [download archive](#)

Development Builds

Access the latest dev builds. These builds are not meant for production.

Install From Nagios DEB Repository

Since NCPA 2.1.3, the DEB Ubuntu binaries can also be found in the Nagios repository. We recommend installing the DEB using this method if you'd like to be able to upgrade using apt-get in the future.

Installing the Nagios Repository

Add the following into `/etc/apt/sources.list.d/nagios.list`:

Ubuntu 22.04 LTS 20.04 LTS 18.04 LTS 16.04 LTS
deb https://repo.nagios.com/deb/jammy /

For other versions of Ubuntu [find the repo here](#).

Add the Nagios public GPG key:

wget -qO - https://repo.nagios.com/GPG-KEY-NAGIOS-V2 | apt-key add -

Update your repos:

apt-get update

Installing NCPA

Once the repo has been added to apt, just install NCPA with the apt-get command.

apt-get install ncpa

[Close](#)

Ajoutez deb <https://repo.nagios.com/deb/jammy/> dans /etc/apt/sources.list.d/nagios.list :

```
root💀ubuntu:~# echo "deb https://repo.nagios.com/deb/jammy/" >> /etc/apt/sources.list.d/nagios.list
```

```
root💀ubuntu:~# echo "deb https://repo.nagios.com/deb/jammy/" >> /etc/apt/sources.list.d/nagios.list
```

Ajout de la clé public Nagios GPG

```
root💀ubuntu:~# wget -qO - https://repo.nagios.com/GPG-KEY-NAGIOS-V2 | apt-key add -
```

Mise à jour de notre machine

```
root💀ubuntu:~# apt update
```

Installation du module NCPA

```
root💀ubuntu:~# apt-get install ncpa
```

On ouvre le fichier ncpa.cfg et on modifier la ligne suivante dans partie [api] : community_string = sitka

```
root💀ubuntu:~# vim /usr/local/ncpa/etc/ncpa.cfg
```

```
[api]
```

```
# The token that will be used to log into the basic web GUI (API browser, graphs, top charts, etc)
# and to authenticate requests to the API and requests through check_ncpa.py
```

```
#
```

```
community_string = sitka
```

On redémarre le service et vérifier son status

Charlie Li - BTS SIO SISR

École IRIS

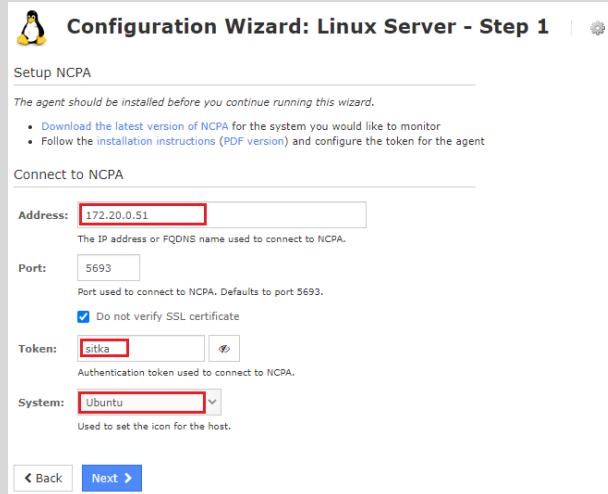
```
root@Ubuntu:~# /etc/init.d/ncpa_listener restart
Stopped NCPA Listener
Started NCPA Listener

root@Ubuntu:~# /etc/init.d/ncpa_listener status
NCPA Listener: Service is running. (pid 18043)
```

On peut remonter maintenant notre machine en allant dans configuration wizard et en choisissant le lien ci-dessous



On rentre ensuite nos paramètres



Méthode plus rapide en téléchargeant le paquet ncpa-2.4.0.u22.amd64.deb

```
root@Ubuntu:~# wget https://assets.nagios.com/downloads/ncpa/ncpa-2.4.0.u22.amd64.deb
```

On installe le paquet téléchargé, après on déclare le community_string avec le nom sitka et on redemarre le service ncpa_listener

```
root@Ubuntu:~# dpkg -i ncpa-2.4.0.u22.amd64.deb
```

Détection de machines en utilisant NCPA :

On peut aussi utiliser NCPA pour superviser nos serveurs, on se rend toujours dans le menu "Configure > Configuration Wizards" puis on tape "website" dans la barre de recherche.

Ensuite on clique sur "Website URL" pour commencer la configuration :

The screenshot shows the Nagios XI interface. On the left, there's a sidebar with various configuration options like Configuration Options, Configuration Tools, Auto Deployment, Advanced Configuration, and More Options. The main area is titled "Configuration Wizards - Select a Wizard". It has a sub-instruction: "Start monitoring your infrastructure in minutes. Configuration wizards guide you through the process of setting up your devices, servers, applications, services, and more in Nagios XI. Select the appropriate wizard below to get started." Below this are three cards: "Website" (Monitor a website), "Website Defacement" (Monitor a website for defacement), and "Website URL" (Monitor a specific web URL). At the bottom right of the main area, there's a link "Get More Wizards".

On entre ensuite d'abord l'adresse URL de notre serveur, puis on configure son nom d'hôte puis on précise les différents paramètres de surveillances :

The screenshot shows the "Configuration Wizard: Website URL - Step 2" page. The URL Details section contains fields for URL (http://172.20.0.50:5693), Host Name (winser2019), Service Name Prefix (empty), and IP Address (172.20.0.50). The URL Options section includes "Use SSL" (checked), Port (5693), and Credentials (empty). The URL Services section has a checked checkbox for "URL Status" (Includes basic monitoring of the URL to ensure the web server responds with a valid HTTP response) and a "Service Name" field set to "URL Status".

Détection de machines en utilisant Autodiscover :

On peut aussi utiliser la méthode d'Autodiscover pour faire remonter les machines à superviser au serveur Nagios : ce dernier va envoyer une requête en Broadcast sur le réseau spécifier pour "découvrir" les machines qui s'y trouve. En fait, les machines sur ce réseau vont chacune répondre à la requête envoyée par le serveur Nagios ce qui permettra à ce dernier de les reconnaître et de les superviser par la suite.

On peut donc utiliser cette méthode en premier avant d'installer les agents de supervision car on pourra en installer automatiquement ensuite par l'intermédiaire du serveur Nagios.

On commence par aller dans le menu "Configure > Configuration Wizards" puis dans l'onglet "Configuration Tools" à gauche on clique sur "Auto-Discovery". On clique ensuite sur "+ New Auto-Discovery Job" :

The screenshot shows the "Auto-Discovery Jobs" page. On the left, a sidebar lists various configuration options under sections like "Configure", "Configuration Tools", "Auto Deployment", "Advanced Configuration", and "More Options". The "Configuration Tools" section is expanded, showing "Configuration Wizards", "Auto-Discovery" (which is selected), and "Manage Templates". The main area displays a table header with columns: Scan Target, Exclusions, Schedule, Last Run, Devices Found, Created By, Status, and Actions. Below the header, a message says "There are no auto-discovery jobs. Add one now." A blue button labeled "+ New Auto-Discovery Job" is visible.

On spécifie ensuite le réseau que l'on veut scanner (sur lequel sont nos machines à superviser) ainsi que quelques paramètres que l'on laissera ici par défaut (ici on peut exclure l'adresse IP du serveur Nagios si on veut). Une fois que l'on a fini, on clique sur "Submit" :

The screenshot shows the "New Auto-Discovery Job" configuration form. The left sidebar is identical to the previous screenshot. The main form has the following fields:

- Scan Target:** 172.20.0.0/24 (with a note: Enter an network address and netmask to define the IP ranges to scan.)
- Exclude IPs:** (with a note: 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 (with a note: Specify the schedule you would like this job to be run.)
- OS Detection:** On (with a note: Attempt to detect the operating system of each host. Note: OS detection may cause the scan to take longer to complete and may not be 100% accurate.)
- Scan Delay:** (with a note: Adjust delay between probes to a given host. If set, this option causes Nmap to wait at least the given amount of time between each probe it sends to a given host. This is particularly useful in the case of rate limiting, milliseconds.)
- System DNS:** Off (with a note: Use system DNS.)
- Custom Ports:** (with a note: Specify Custom ports. Ex: 22; 1-65535; U:53,111,137,T:21-25,80,139,8080,S:9)

At the bottom are two buttons: "Submit" (highlighted in blue) and "Cancel".

Le serveur Nagios va ensuite débuter l'Auto-Discovery Job que l'on vient de configurer. Une fois terminé (Status : Finished) on va cliquer sur l'icône en forme de feuille (View job results) sur la même ligne à droite :

The screenshot shows the Nagios configuration interface under the 'Auto-Discovery' section. A message box at the top right says 'Auto-discovery job added.' Below it is a table with one row. The columns are: Scan Target (172.20.0.0/24), Exclusions (-), Schedule (Once), Last Run (2022-02-19 12:50:37), Devices Found (2 New / 4 Total), Created By (nagiosadmin), Status (Finished), and Actions (with icons for edit, refresh, and delete). An orange arrow points to the 'Actions' column.

À partir d'ici on va pouvoir sélectionner sur quelles machines on veut installer les agents de supervision NCPA et le serveur Nagios les installera automatiquement. On coche donc les machines que l'on veut superviser* puis on clique sur "Deploy Agents to Selected Hosts" :

The screenshot shows the 'Scan Results' page. It includes a 'Scan Summary' table with details like Scan Date (2022-02-19 13:10:19), Scan Address (172.20.0.0/24), and Total Hosts Found (4). It also has 'Processing Options' for CSV export and monitoring configuration. Below is a table of 'Discovered Items' with columns: Address, Host Name, Type, Device/Operating System [Accuracy], MAC Vendor, Agent Deployed, and Status. The table lists four hosts: 172.20.0.14 (Windows Server, Old), 172.20.0.34 (Linux Server, New), 172.20.0.52 (Linux Server, Old), and 172.20.0.250 (Unknown, New). A checkbox next to 172.20.0.52 is checked. At the bottom is a blue button labeled 'Deploy Agents to Selected Hosts'.

*Les nouvelles machines (Status : New) devraient être directement affichées mais si pour une raison ou pour une autre, elles ne s'affichent pas toutes : cliquez sur "Show all" au milieu à gauche sur la ligne "Total Hosts Found:"

Ensuite on précise l'adresse IP des machines à superviser (rempli automatiquement d'après ce que l'on a coché), leur système d'exploitation ainsi que les paramètres d'identifications et l'agent que l'on veut installer (par défaut NCPA) puis on clique sur "Deploy" :

Deploy Agent

Deploy an agent to a system or a list of systems. Select monitoring type, credentials, and checks to run on the system. [View past auto deploy jobs.](#)

IP Addresses (or Hostnames)

172.20.0.52

List one host per line. A single list of comma separated values is also valid.

Operating System

Linux

Credentials

Auth Type

Password

Username

root

If not using root user, the user should have access to become root using sudo.

Password

Deployment Settings

Agent Software

NCPA

Deploy >

Le résultat de l'installation s'affiche ensuite.

À partir de la page des résultats du scan du serveur Nagios (Scan Results), on peut aussi configurer la supervision des nouvelles machines détectées comme ce que l'on a vu précédemment avec SNMP et NCPA en cliquant sur "New hosts" (ou autre) au milieu sur la ligne "Configure Basic Monitoring:".

On sélectionne le bon "Job" (celui que l'on vient de configurer) et on laisse les paramètres par défaut :

Configuration Wizard: Auto-Discovery - Step 1

Auto-Discovery Job

Job:

Scan of 172.20.0.0/24 @ 2022-02-19 12:50:37 - Found 2 New / 4 Total Hosts

Select the auto-discovery job you wish to use for choosing new hosts and services to monitor.
If you wish, you can also launch a new discovery job.

Show:

All Hosts

Choose whether you'd like to see results from all hosts that were found during the scan, or only new hosts that aren't currently being monitored.

Default Services:

Common

Select the types of services that you would like to be selected for monitoring by default. You can override individual services on the next page.

Host Addresses:

IP Addresses

Select the type of addresses that you would prefer to use for newly configured hosts.

< Back

Next >

On coche ensuite les machines que dont on souhaite configurer la supervision par le serveur Nagios et on clique sur "Next" :

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			
					Service Name	Service	Port	Protocol
172.20.0.14	Windows Server	Microsoft Windows Server 2012	Old	172.20.0.14	<input type="checkbox"/> TCP Port 53 - domain	domain	53	TCP
					<input type="checkbox"/> TCP Port 88 - kerberos	kerberos	88	TCP
					<input type="checkbox"/> TCP Port 135 - epmap	epmap	135	TCP
					<input checked="" type="checkbox"/> NetBIOS	netbios-ssn	139	TCP
					<input checked="" type="checkbox"/> LDAP	ldap	389	TCP
					<input type="checkbox"/> TCP Port 445 - microsoft-ds	microsoft-ds	445	TCP
					<input checked="" type="checkbox"/> RDP	ms-wbt-server	3389	TCP
172.20.0.34	Linux Server	Linux 2.6.32	New	172.20.0.34	<input checked="" type="checkbox"/> SSH	ssh	22	TCP
					<input checked="" type="checkbox"/> HTTP	http	80	TCP
					<input checked="" type="checkbox"/> LDAP	ldap	389	TCP
					<input checked="" type="checkbox"/> HTTPS	https	443	TCP
172.20.0.52	Linux Server	Linux 2.6.32	Old	172.20.0.52	<input checked="" type="checkbox"/> SSH	ssh	22	TCP
172.20.0.250	Unknown		New	172.20.0.250	<input type="checkbox"/> TCP Port 53 - domain	domain	53	TCP
					<input checked="" type="checkbox"/> HTTP	http	80	TCP

[◀ Back](#) [Next ▶](#)

Comme pour NCPA ou SNMP on spécifie les derniers paramètres de supervisions et on clique sur "Finish".