PARIS PANTHÉON-ASSAS UNIVERSITÉ

Installation et configuration de Nagios XI

BTS 2022-2024

Contexte : SITKA est une entreprise de services informatiques spécialisée dans la fourniture de solutions technologiques innovantes pour répondre aux besoins variés de ses clients. Fondée en 1990 SITKA a su établir sa réputation en tant que partenaire fiable et efficace dans le domaine de la technologie de l'information.

À Propos de SITKA

- **Nom de l'Entreprise : SITKA**
- **Type de Société : Société Anonyme (SA)**
- **Nombre d'Employés : 1560**
- **Le chiffre d'affaires annuel de SITKA s'élève à 19 600 000€**

Procédure :

SERVICE NAGIOS XI

Pour commencer on a besoin plusieurs machines Virtual :

- Debian
- Windows 10 pro
- Windows server 2019 ou 2022

apt update && apt upgrade → Pour la mise à jour Debian.

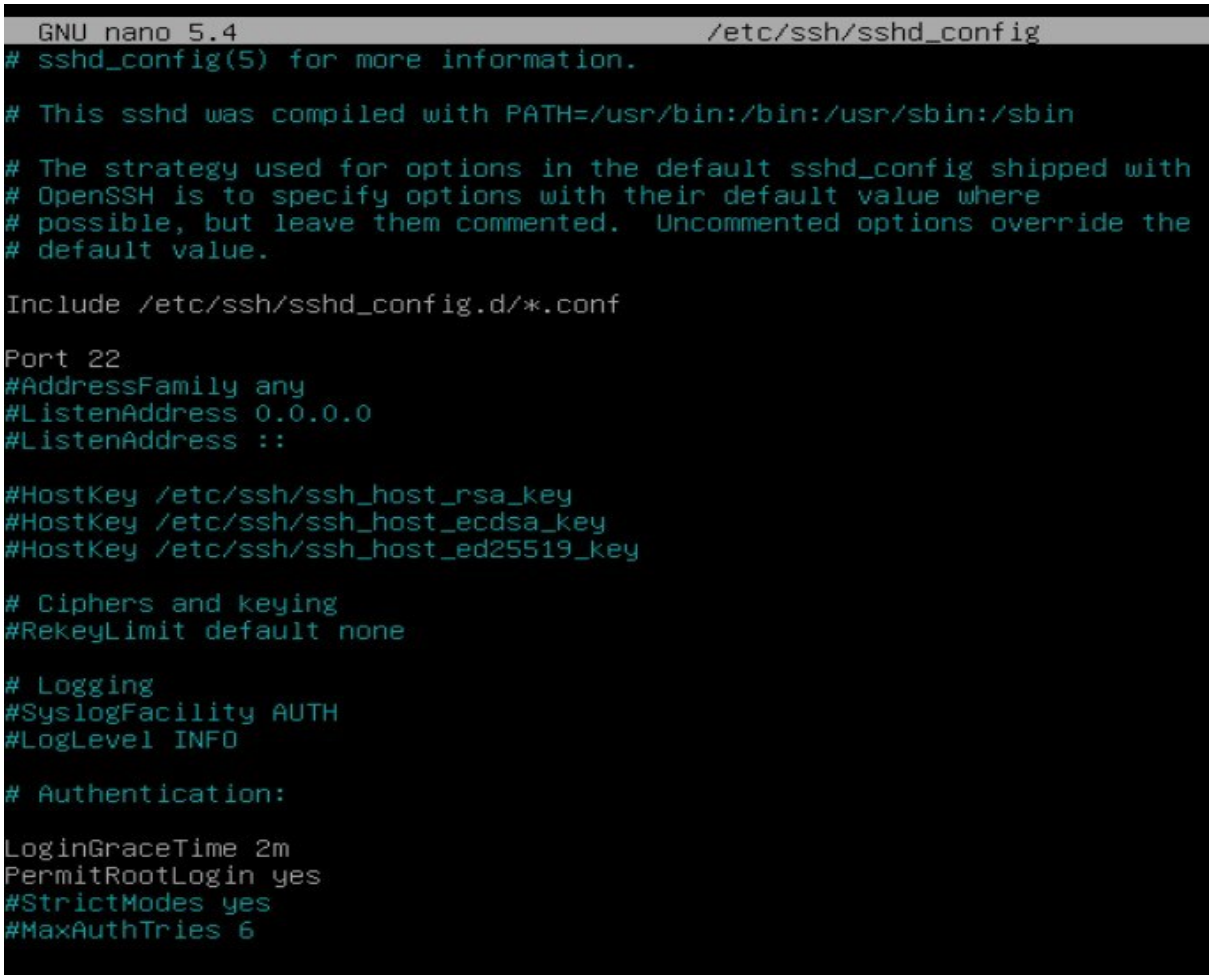
Verification bash ET local
ls –al

Étape 1 : Installer SSH sur toutes Debian.apt **apt**

install openssh-server –y

Etape 2 : Connexion ssh modifié le fichier etc de configuration.

Nano /etc/ssh/sshd_config



CTRL + X
OUI et Entrée

service sshd restart
service ssh restart

Etape 3 : Pour une bannière on installe le paquet : apt install figlet

Ajout de la couleur : apt install lolcat
Polices: apt install figlet
: gem install lolcat

En suite vous faites ip ad sur la VM pour récupérer son ip.

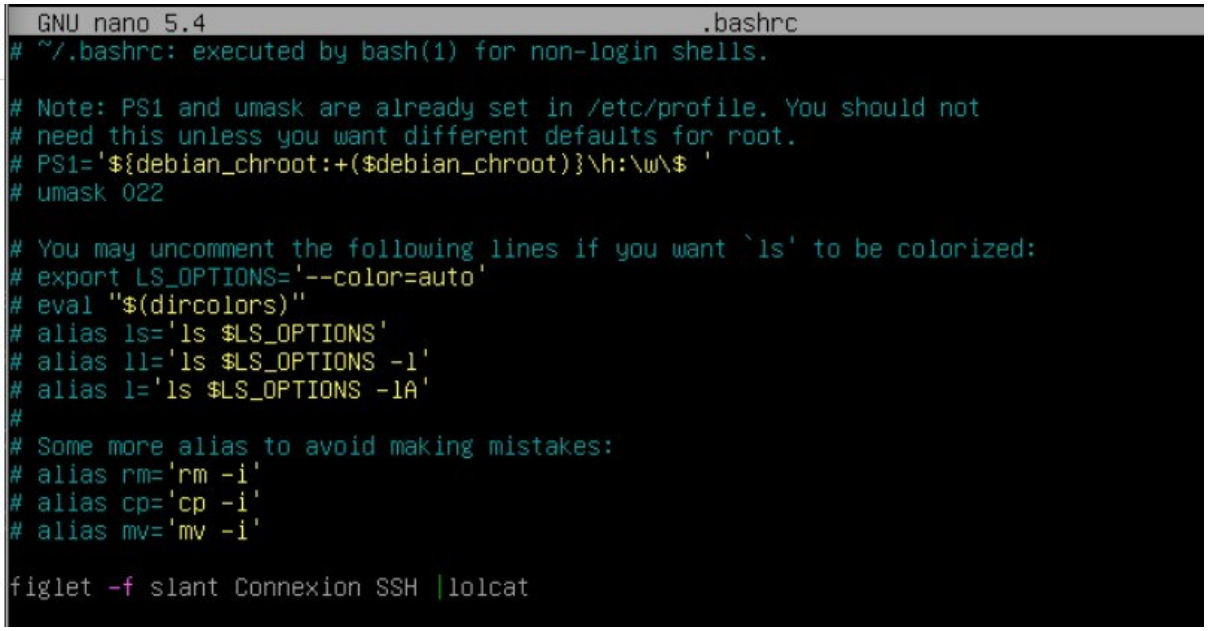
Et puis vous connectez sur un terminal sur la machine physique.

```
PS C:\Users\Tooba> ssh root@192.168.253.142
root@192.168.253.142's password:
Linux debian 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Feb  5 22:55:40 2022 from 192.168.253.1
```

Etapes 4 : On rentre dans le bash

Fichier à modifier .bashrc nano
.bashrc

Ajouter en dernière ligne : figlet -f slant Connexion SSH |lolcat



CTRL + X
OUI et Entrée
Exit

Etapes 5 : on rentre les restes cmd dessus l'un après l'autre.

cd /tmp
wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
tar xzf xi-latest.tar.gz cd nagiosxi
./fullinstall

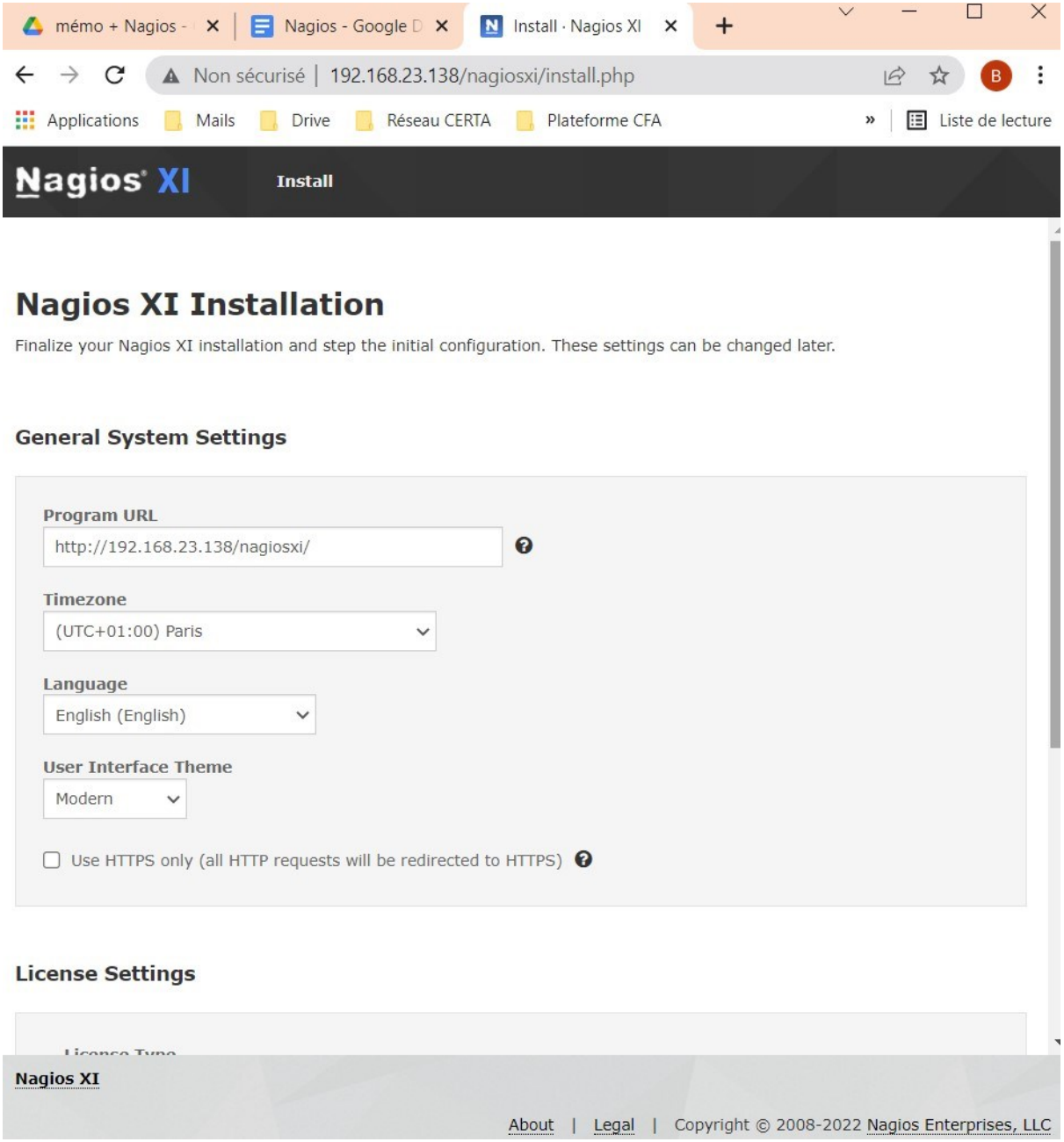
Etape 6: Finalize Installation

Once the installation has completed you should see a message like the following:
Nagios XI Installation Complete!

You can access the Nagios XI web interface by visiting:

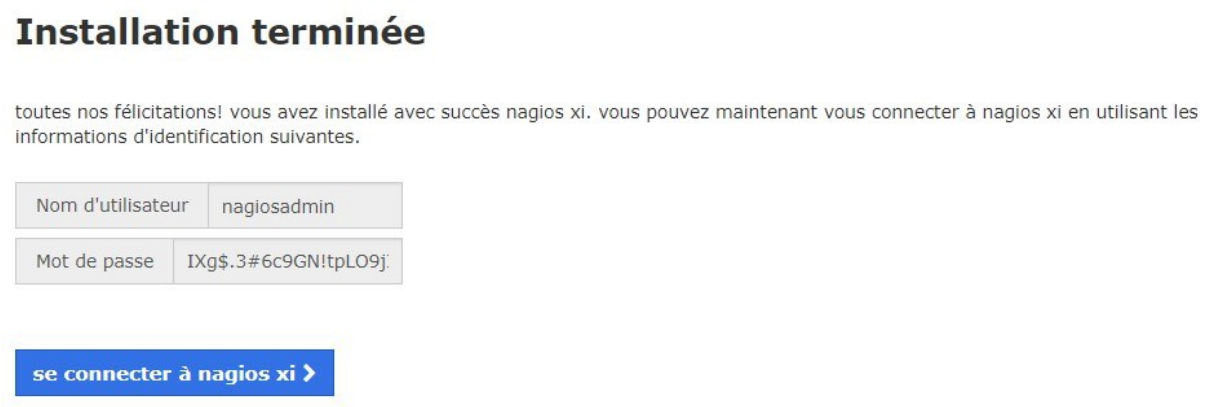
Se connecter avec l'adresse IP sur le serveur Nagios http://<server_address>/nagiosxi/
+ adresse IP de la machine→ par exemple : (http://192.168.229.148/nagiosxi/)

Le test fera sur une page web !!!



Dans la fenêtre plus basse on ne change rien sauf mettre : Free
Sauvegarder

Id : nagiosadmin
Mdp : Copier le mot de passe



La supervision des clients

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

TP Nagios du 14-15 février 2022 :

VMs dont on a toujours besoin :
- Contrôleur de Domaine Windows Server : on se servira de son navigateur web pour accéder à l'interface web du serveur Nagios (et celle du serveur pfSense aussi si besoin).
- Serveur pfSense : qui sert de routeur et d'intermédiaire à l'accès Internet.
- Service DNS.

On prépare 4 nouvelles machines : serveur Nagios ☮ 172.20.0.34/24 (qu'on avait déjà installé sur une VM Debian clean) serveur Windows Serv 2019 ☮ 172.20.0.50/24 serveur Ubuntu* ☮ 172.20.0.51/24 serveur Debian* ☮ 172.20.0.52/24
*donc sans interface graphique

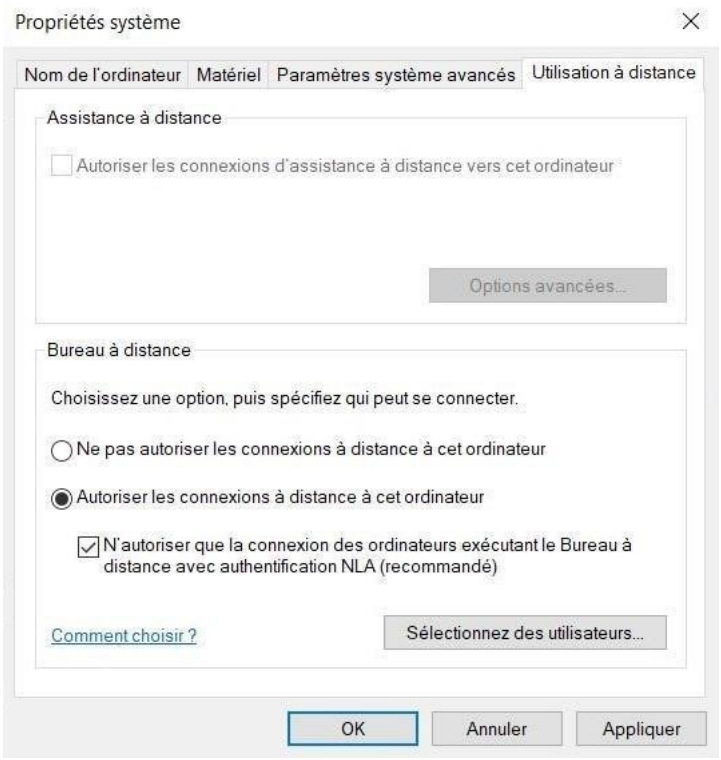
Les machines Windows Server, Debian et Ubuntu seront ici des machines test supervisées par le serveur Nagios. Il faudra donc installer un agent de supervision sur ces 3 serveurs (ce seront les machines client) et ensuite les faire remonter dans le serveur Nagios.

On a quatre méthodes principales de supervision par Nagios : **SNMP**, **NCPA (Nagios CrossPlatform Agent)**, **NRPE** et **Auto-discover**. NRPE ne sera pas couvert ici (on ne l'a pas vu durant ces deux séances).

Note : désactiver Snort s'il est installé sur pfSense pour éviter qu'il interfère et bloque les connexions des nouvelles machines ci-dessus.

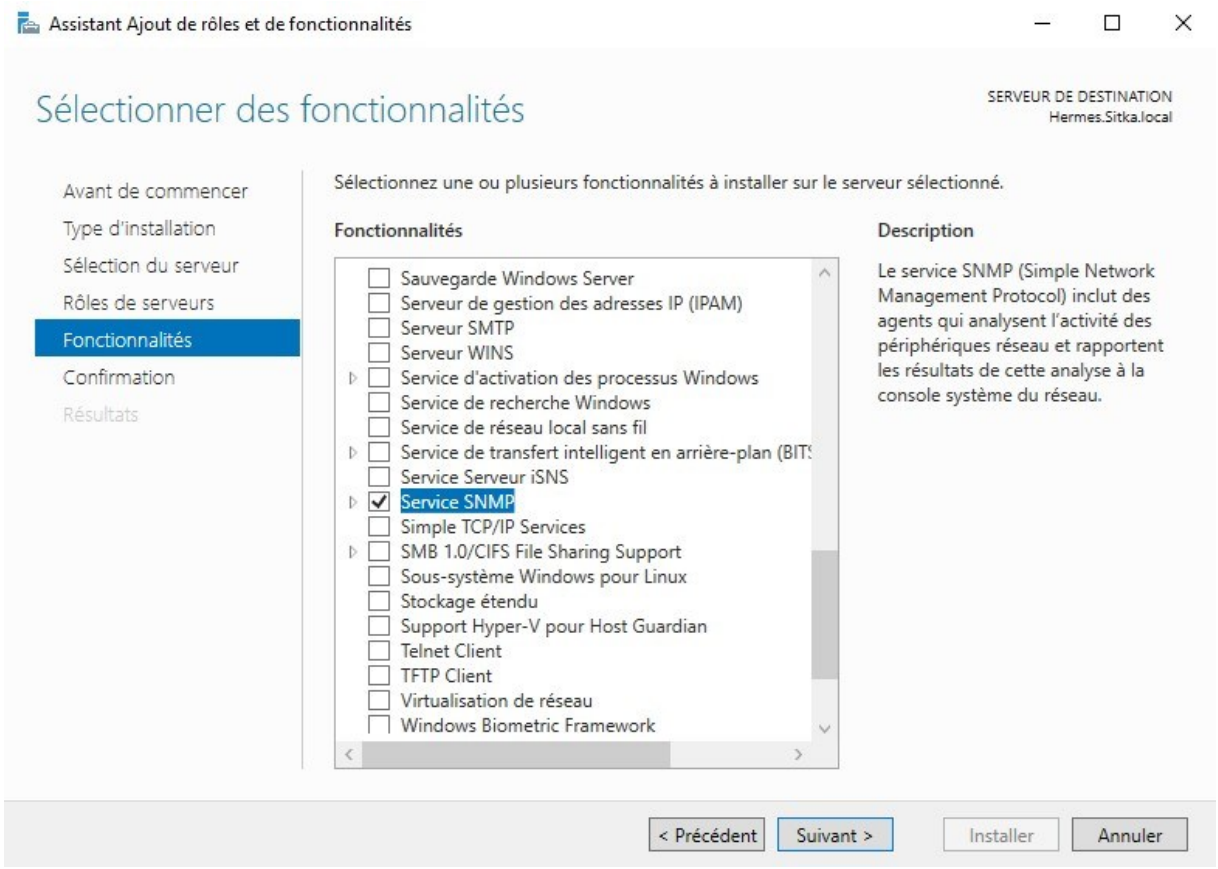
Machine Windows Server 2019 :

Dans le Gestionnaire de Serveur > serveur local et cliquer sur "Bureau à distance" puis cocher "Autoriser les connexions à distance à cet ordinateur" :



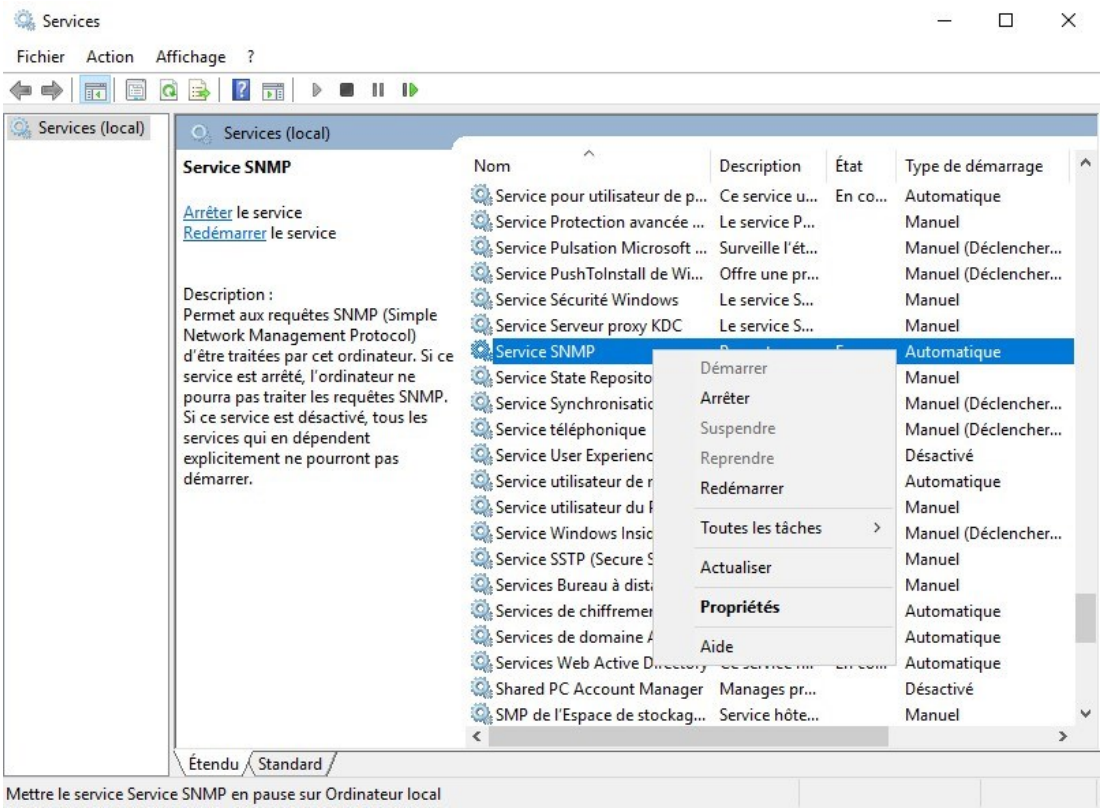
Installation du service/agent SNMP sur Windows Server 2019 :

On va dans "Gérer > Ajouter des rôles et fonctionnalités" puis comme d'habitude 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" :

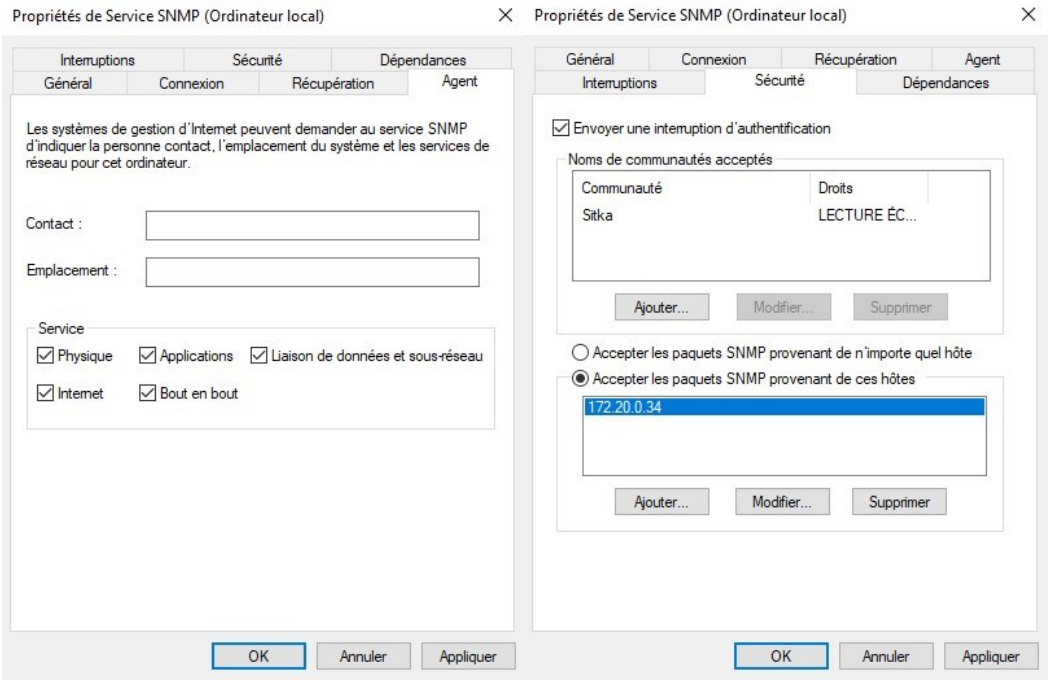


On clique ensuite sur "Installer" à l'écran de confirmation puis sur "Fermer" une fois le service installé.

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" :



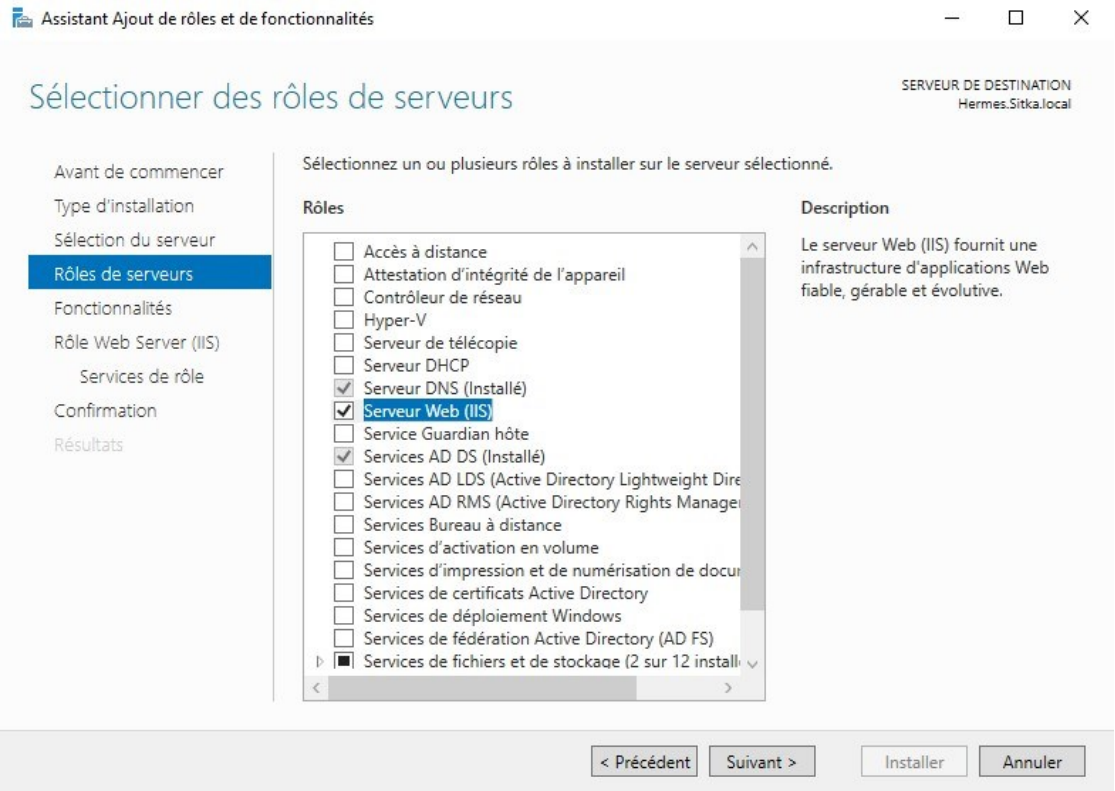
Dans l'onglet "Agent" des propriétés du service SNMP on coche toutes les cases en dessous dans la rubrique "Service" :



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".

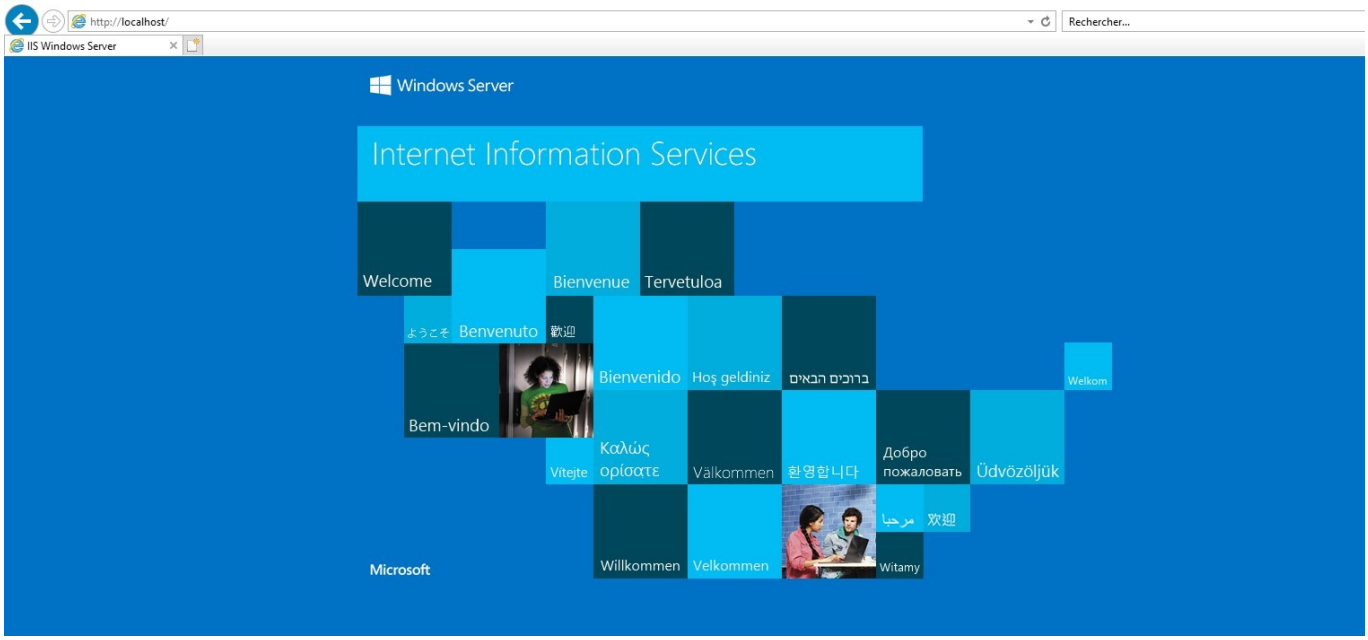
Installation de l'agent NCPA sur Windows Server 2019 :

Pour utiliser l'agent NCPA on va avoir besoin d'un serveur web (pas très bien compris pourquoi mais bon), 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" :



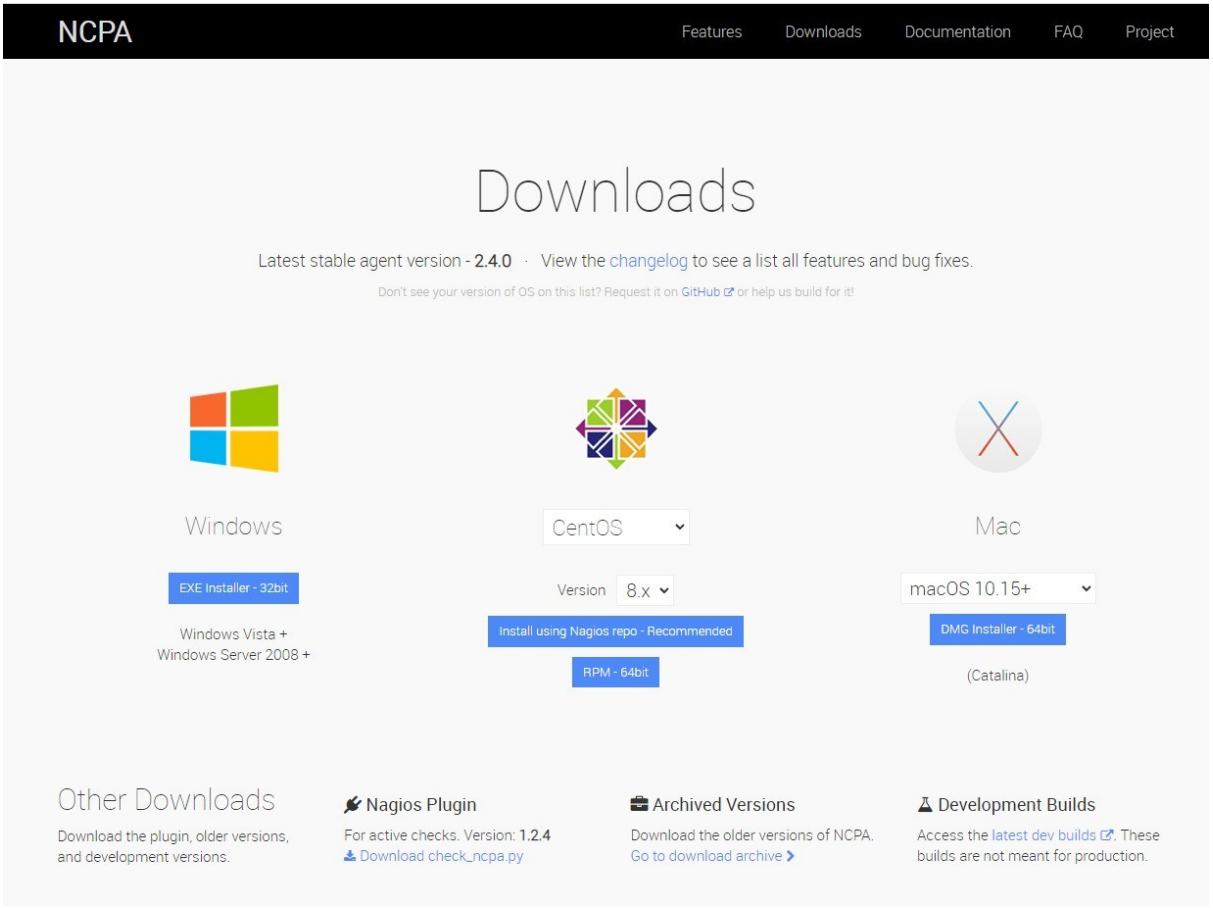
On ne coche aucune fonctionnalité supplémentaire et on laisse aussi les services de rôle par défaut pour enfin cliquer sur "Installer" à l'écran de confirmation puis sur "Fermer" une fois le service installé.

On peut d'ailleurs vérifier l'installation du serveur web en tapant http://localhost dans le navigateur web du serveur WS 2019 :

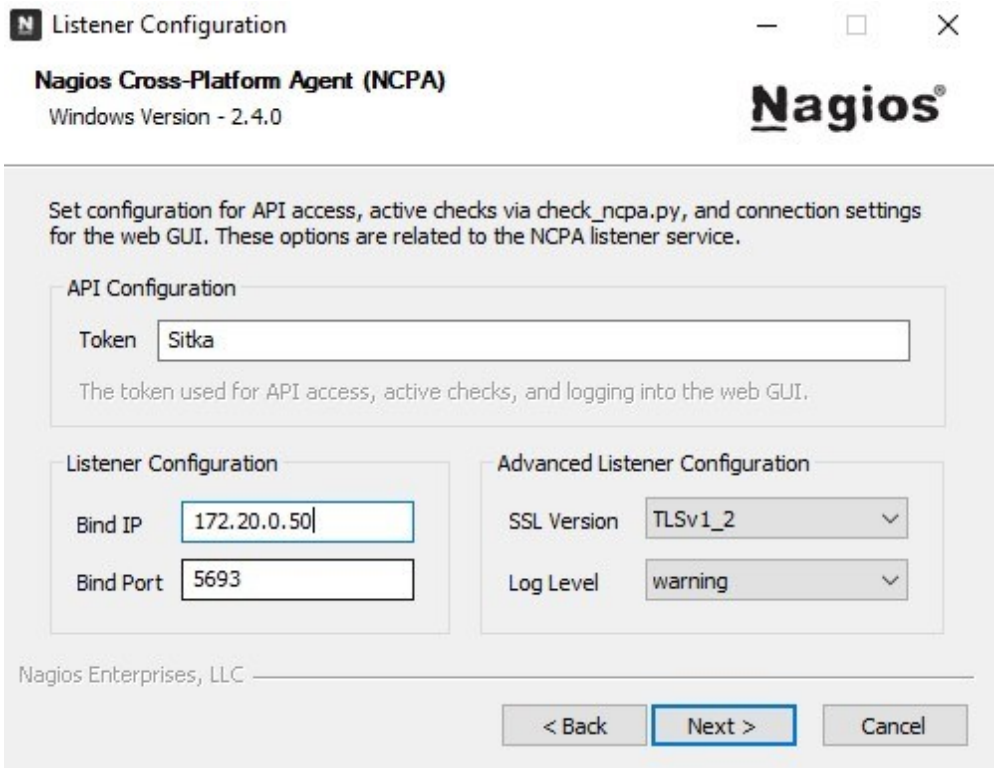


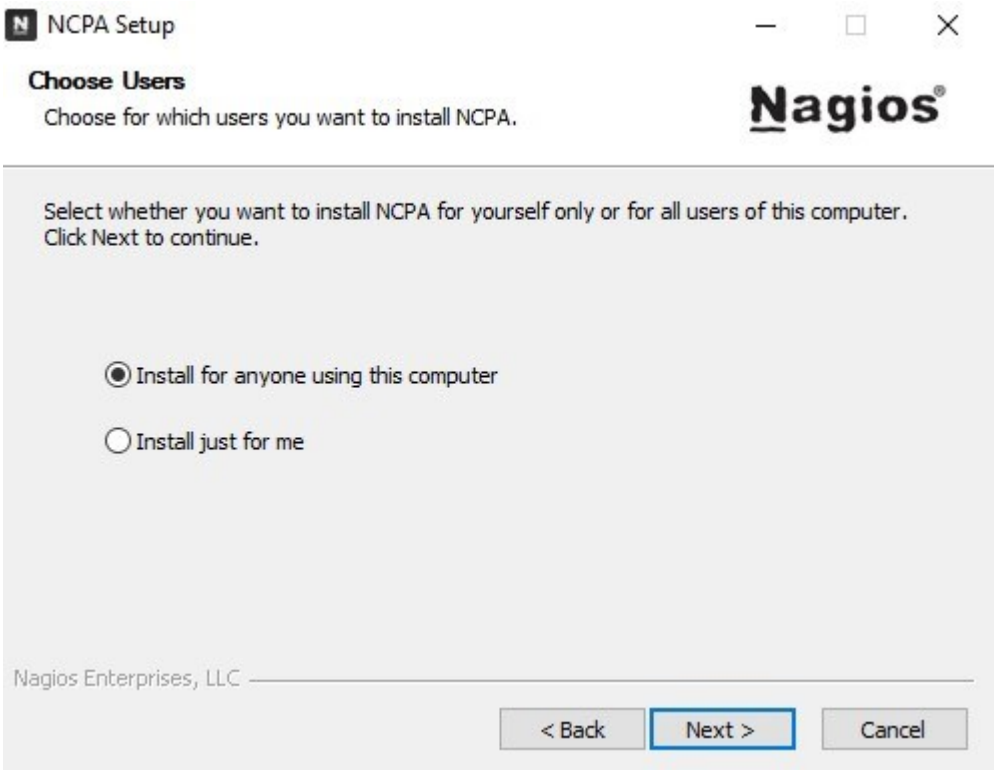
On peut trouver les fichiers de la page d'accueil du serveur web dans le dossier **C:\inetpub\wwwroot**

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)

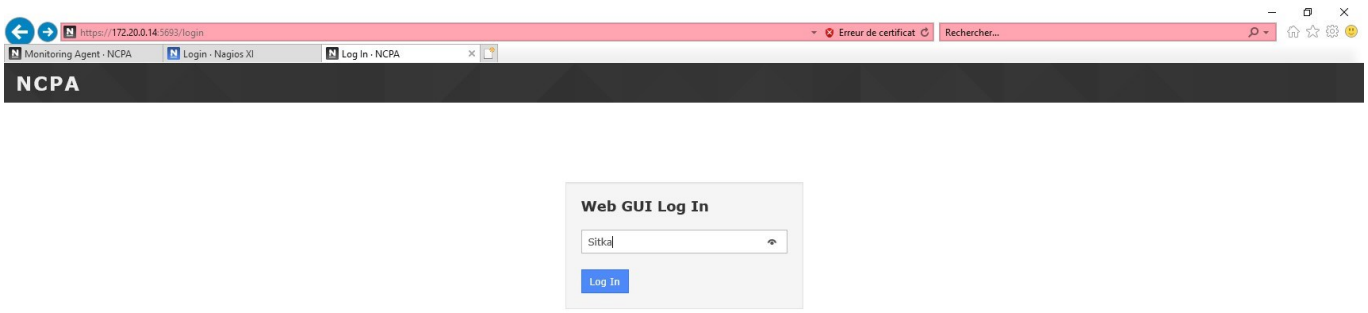


On exécute d'abord le fichier télécharger pour commencer l'installation de l'agent NCPA. On clique sur "I agree" en ce qui concerne la licence puis dans le champs "Token" de la configuration API on entre le nom de notre communauté ici "Sitka", dans le champ "Bind IP" on entre l'adresse IP du serveur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





Là aussi on peut vérifier l'installation de l'agent NCPA en tapant https://172.20.0.50:5693/ (adresse IP entrée à l'installation avec port par défaut) dans le navigateur web du serveur WS 2019 :



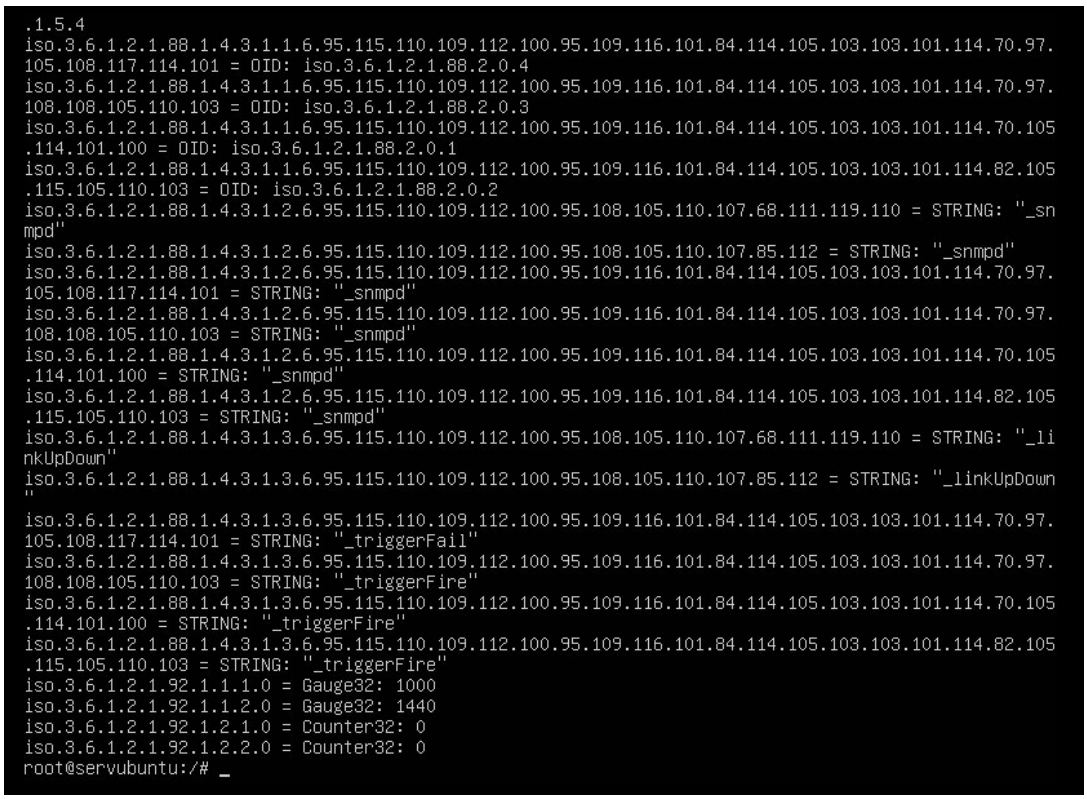
Serveur Ubuntu :

Sur Ubuntu, par défaut il n'existe pas le fichier **/etc/network/interfaces** pour modifier l'adresse IP de la machine (comme sur Debian)*. On va installer donc d'abord installer le paquet **ifupdown** permettant de réinitialiser les interfaces réseaux mais surtout qui créera aussi le fichier **/etc/network/interfaces** où l'on pourra modifier l'adresse IP de la machine.
*à la place il faut modifier le fichier **/etc/netplan/00-installer-config.yaml**

Installation du service/agent SNMP (et autres) sur le serveur Ubuntu :

apt install -y ifupdown
apt purge -y netplan.io
apt -y autoremove
rm -rf netplan/ [---on retire manuellement les deux dossiers lié à netplan---]
rm -rf /etc/cloud/cloud.cfg.d
ip addr
nano /etc/network/interfaces
→ Modifier les dernières lignes pour avoir :
auto lo iface lo inet loopback # Carte réseau
auto ens33 [---si votre interface réseau se nomme ens37 ou autres, remplacer ens33 par en37---] iface ens33 inet static address 172.20.0.51/24 gateway 172.20.0.250
---------- Ctrl + o > Entrée puis Ctrl + x OU Ctrl + x > yes > Entrée
ifdown ens33
ifup --force ens33
apt update
apt -y upgrade [---si besoin---]
apt -y autoremove
apt install -y snmpd snmp
echo '' > /etc/snmp/snmpd.conf [---on efface le contenu du fichier---]

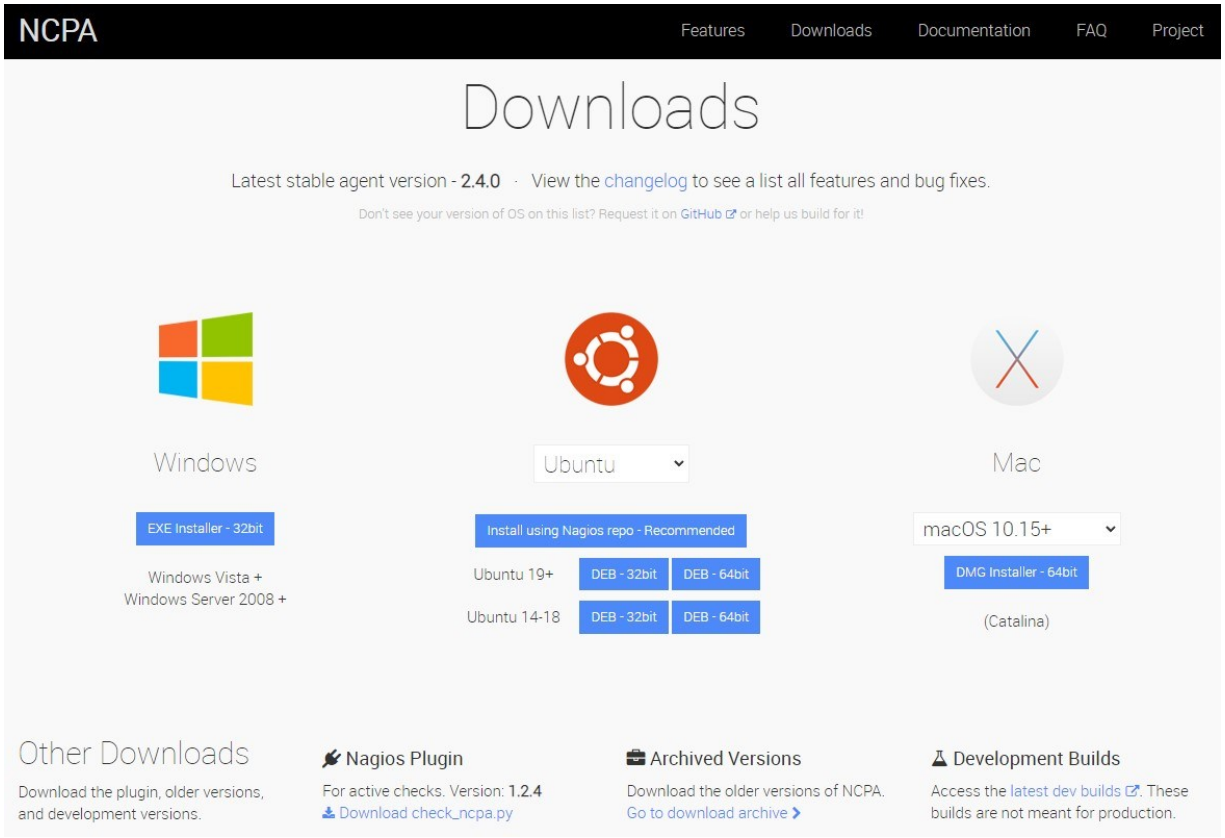
nano /etc/snmp/snmpd.conf → Ajouter les lignes suivantes :
rocommunity Sitka # Droits communauté (ro = read only)
syslocation Sitka syscontact root <root@sitka.local> # Ou autre adresse mail
---------- Ctrl + x > yes > Entrée
#reboot
On peut ensuite vérifier si le service SNMP fonctionne avec :
snmpwalk -v1 -c Sitka 172.20.0.51
Si le service fonctionne, la commande affichera plein d'IUOID à l'écran :



Activation manuelle de la résolution DNS :
Ne pas oublier d'activer la résolution DNS (sur Linux). Pour cela on va supprimer le fichier par défaut **/etc/resolv.conf** - qui est en fait un raccourci/symlink - car sinon celui-ci sera réinitialisé à chaque redémarrage de la machine. On modifiera ensuite notre nouveau fichier pour y mettre l'adresse IP de notre serveur DNS :
cp /etc/resolv.conf /etc/resolv.conf.old
rm /etc/resolv.conf
touch /etc/resolv.conf [---nouveau fichier de même nom mais qui n'est pas un raccourci--]
nano /etc/resolv.conf
→ Ajouter les lignes suivantes :
nameserver 172.20.0.14 [---OU nameserver 172.20.0.250 ? pas trop sûr, j'ai pas eu le temps de tout noter---]
---------- Ctrl + x > yes > Entrée

Installation de l'agent NCPA sur le serveur Ubuntu :

Pour utiliser l'agent NCPA on va avoir besoin d'un serveur web (pas très bien compris pourquoi mais bon), on installe donc aussi le paquet **apache2**.
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



apt install -y apache2
[---pas mal de truc à faire pour les configurations du serveur web Apache mais on l'avait fait avant les séances du 14-15 février et il y avait pas mal de trucs que j'ai pas eu le temps de noter---]
touch /etc/apt/sources.list.d/nagios.list
echo 'deb https://repo.nagios.com/deb/focal /' >> /etc/apt/sources.list.d/nagios.list
OU
nano /etc/apt/sources.list.d/nagios.list →
Ajouter la ligne suivante :
deb https://repo.nagios.com/deb/focal / [---attention aux espaces---]
---------- Ctrl + x > yes > Entrée
wget -qO - https://repo.nagios.com/GPG-KEY-NAGIOS-V2 | apt-key add -
apt update
apt -y upgrade [---si besoin---]
apt -y autoremove
apt install -y ncpa
nano /usr/local/ncpa/etc/ncpa.cfg

→ Modifier la ligne suivante dans partie [api] : community_string
= Sitka
---------- Ctrl + x > yes > Entrée
/etc/init.d/ncpa_listener restart

Serveur Debian :

Comme précédemment on configurera d'abord l'adresse IP de l'interface réseau dans le fichier **/etc/network/interfaces**. Les commandes d'installation et configuration de SNMP sur Debian seront identiques que sur Ubuntu et très similaires pour l'installation et configuration de NCPA.

Activation manuelle de la résolution DNS :

Ne pas oublier d'activer la résolution DNS sur nos machines Linux ! Pour cela on va supprimer le fichier par défaut **/etc/resolv.conf** (qui est en fait un raccourci/symlink) car sinon ce dernier sera réinitialisé au redémarrage de la machine. On modifiera ensuite notre nouveau fichier pour y mettre l'adresse IP de notre serveur DNS :

cp /etc/resolv.conf /etc/resolv.conf.old
rm /etc/resolv.conf
touch /etc/resolv.conf [---nouveau fichier de même nom mais qui n'est pas un raccourci--]
nano /etc/resolv.conf →
Ajouter les lignes suivantes :
nameserver 172.20.0.14 [---OU nameserver 172.20.0.250 ? pas trop sûr, j'ai pas eu le temps de tout noter---]
---------- Ctrl + x > yes > Entrée

Installation du service/agent SNMP (et autres) sur le serveur Debian :

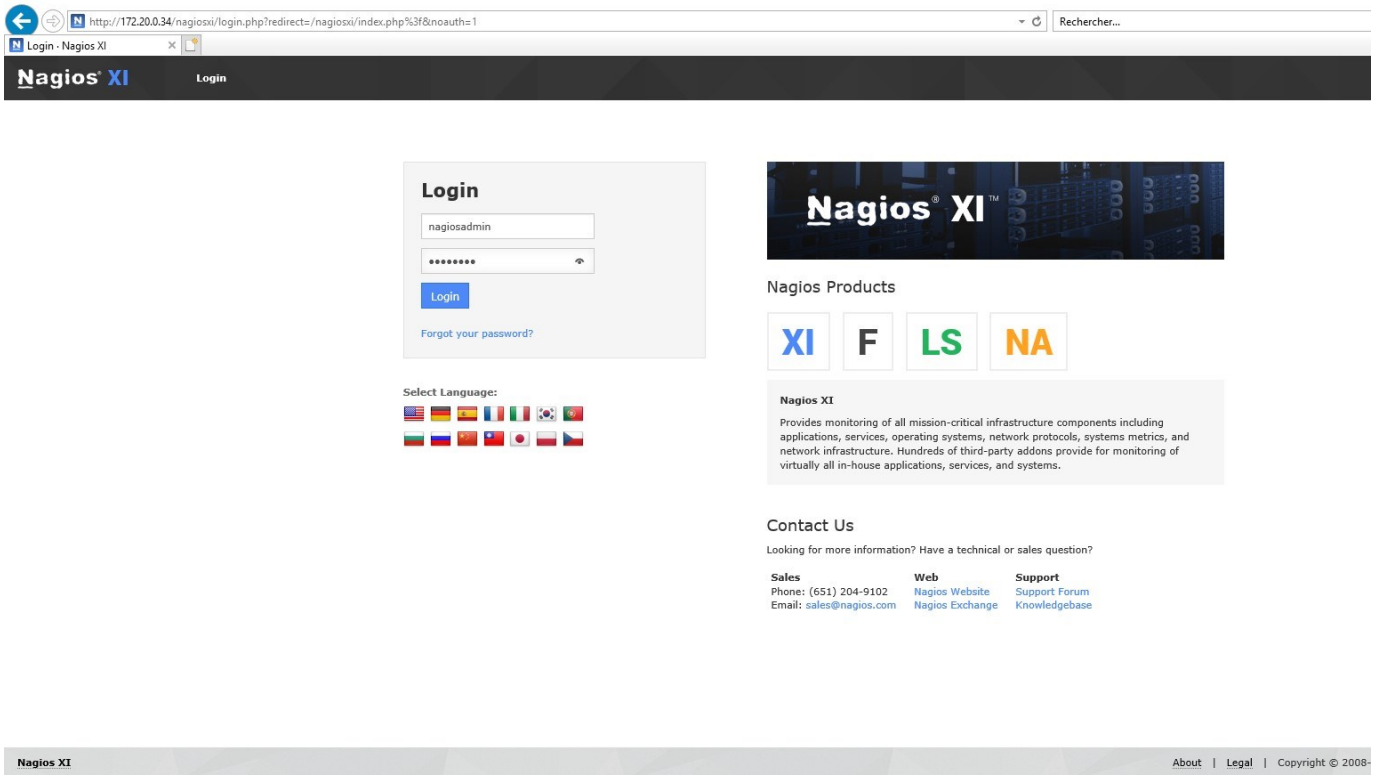
ip addr
nano /etc/network/interfaces
→ Modifier les dernières lignes pour avoir :
auto lo iface lo inet
loopback
the primary network interface
allow-hotplug ens33 iface
ens33 inet static address
172.20.0.52/24 gateway
172.20.0.250
---------- Ctrl + x > yes > Entrée
ifdown ens33
ifup --force ens33
apt update
apt -y upgrade [---si besoin---]
apt -y autoremove
apt install -y snmpd snmp
echo '' > /etc/snmp/snmpd.conf [---on efface le contenu du fichier---]

nano /etc/snmp/snmpd.conf → Ajouter les lignes suivantes :
rocommunity Sitka # Droits communauté (ro = read only)
syslocation Sitka syscontact root <root@sitka.local> # Ou autre adresse mail
---------- Ctrl + x > yes > Entrée
#reboot
On peut ensuite vérifier si le service SNMP fonctionne avec :
snmpwalk -v1 -c Sitka 172.20.0.52
Si le service fonctionne, la commande affichera plein d'IUOID à l'écran.

Installation de l'agent NCPA sur le serveur Debian :
Pour utiliser l'agent NCPA on va avoir besoin d'un serveur web (pas très bien compris pourquoi mais bon), on installe donc aussi le paquet **apache2**.
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

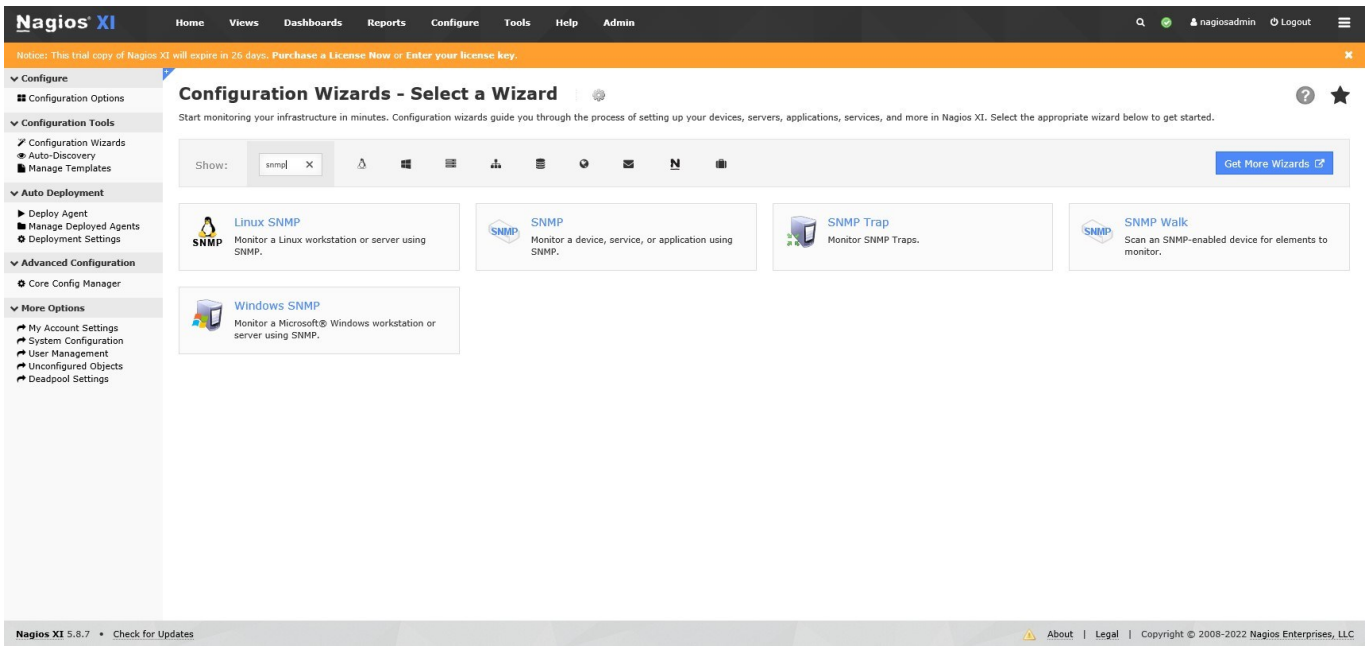
apt install -y apache2
[---pas mal de truc à faire pour les configurations du serveur web Apache mais on l'avait fait avant les séances du 14-15 février et il y avait pas mal de trucs que j'ai pas eu le temps de noter---]
touch /etc/apt/sources.list.d/nagios.list
nano /etc/apt/sources.list.d/nagios.list →
Ajouter la ligne suivante :
deb https://repo.nagios.com/deb/buster / [---attention aux espaces---] ----------
---------- Ctrl + x > yes > Entrée
apt install -y gnupg2
wget -qO - https://repo.nagios.com/GPG-KEY-NAGIOS-V2 | apt-key add -
apt install -y apt-transport-https
apt update
apt -y upgrade [---si besoin---]
apt -y autoremove
apt install -y ncpa
nano /usr/local/ncpa/etc/ncpa.cfg
→ Modifier la ligne suivante dans partie [api] : community_string = Sitka
---------- Ctrl + x > yes > Entrée
/etc/init.d/ncpa_listener restart

Détection des machines supervisées par serveur Nagios :
Sur le Contrôleur de Domaine Windows Server, on va accéder à l'interface web de Nagios dans un navigateur web en tapant l'adresse IP du serveur Nagios dans la barre d'URL http://172.20.0.34/nagiosxi puis s'identifie en entrant l'identifiant administrateur et son mot de passe :

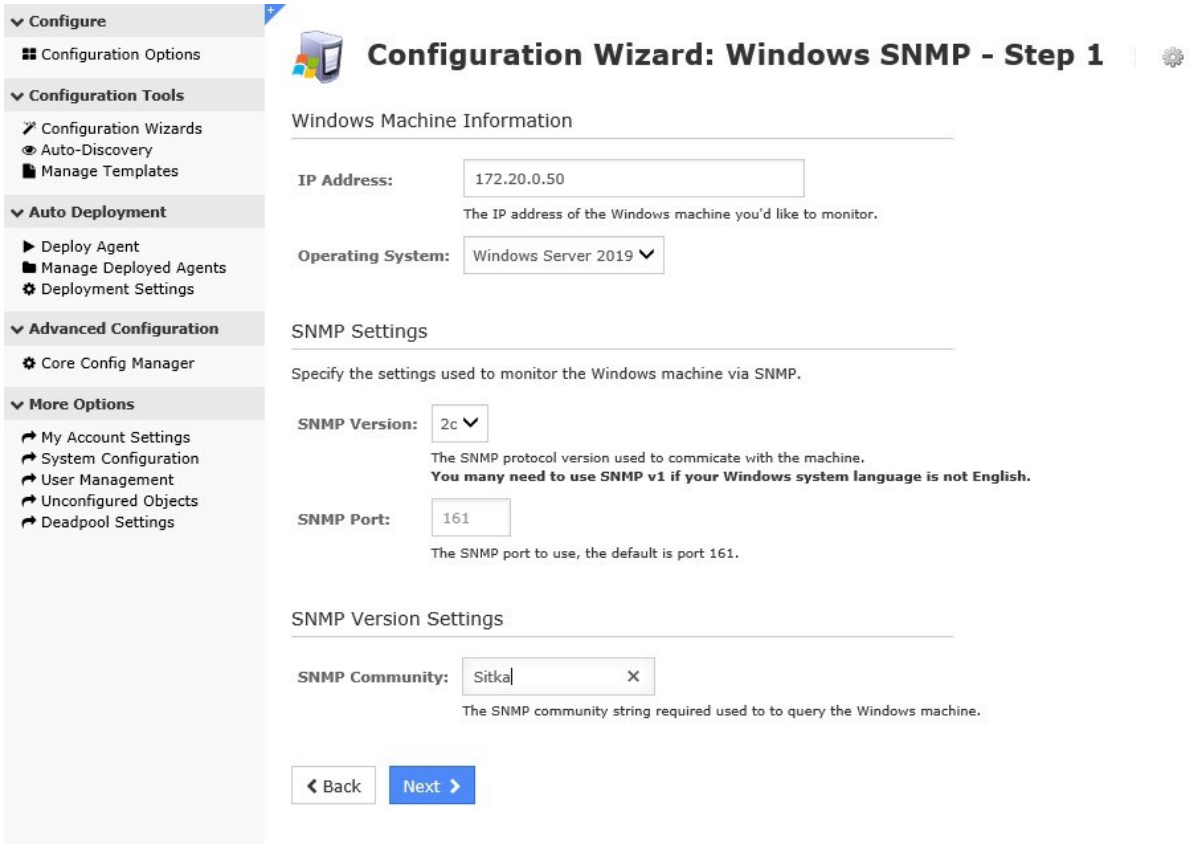


Détection de machines en utilisant SNMP :

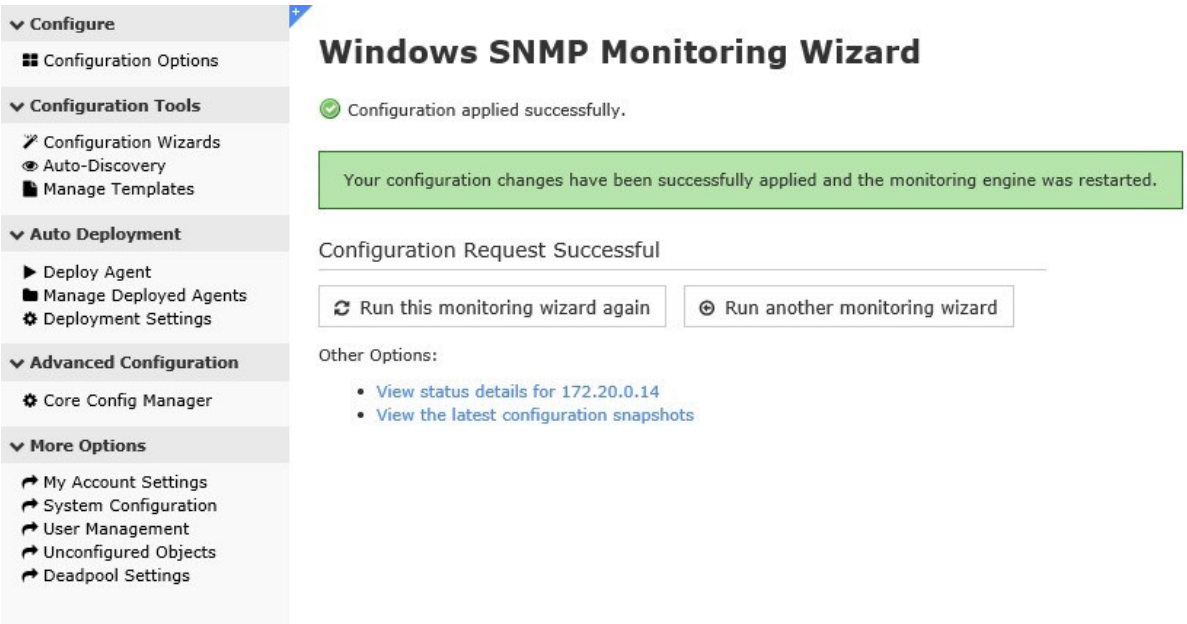
On va ensuite dans le menu "Configure > Configuration Wizards" puis on tape "snmp" dans la barre de recherche. Ensuite on clique sur "Linux SNMP" s'il s'agit d'une machine Linux sur laquelle on a installé le service SNMP ou "Windows SNMP" s'il s'agit d'une machine d'une machine Windows :



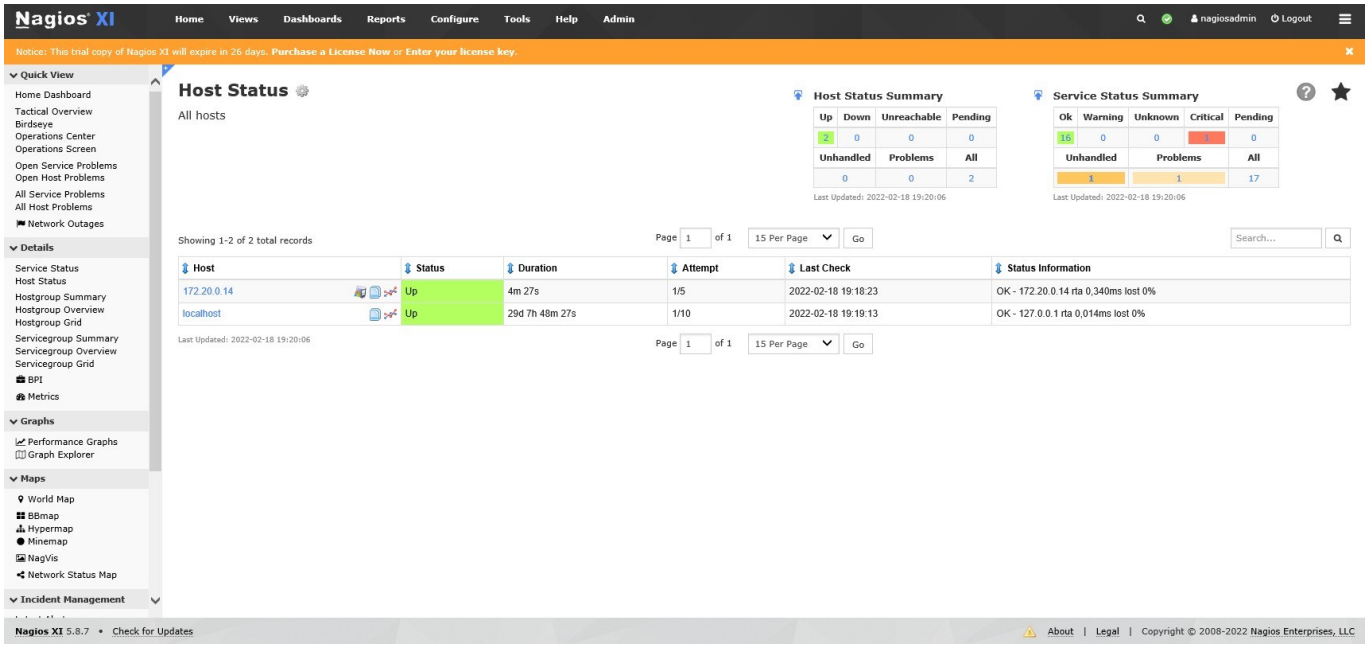
Dans le Wizard on précise ensuite l'adresse IP de la machine à superviser (donc à relier au serveur Nagios), son système d'exploitation (si demandé) ainsi que le nom de la communauté/token :

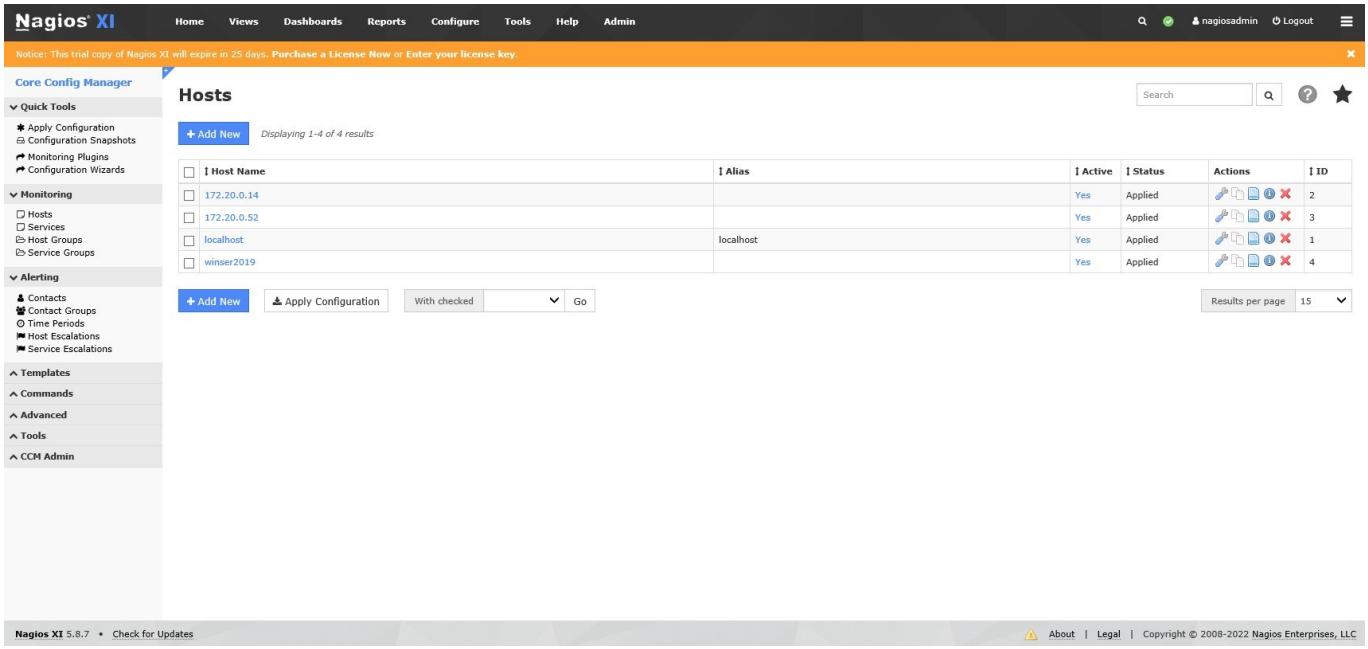


On peut aussi préciser les paramètres de supervisions mais ici on laissera tous par défaut avant de cliquer sur "Finish". Normalement un message de configuration réussie doit alors s'afficher :



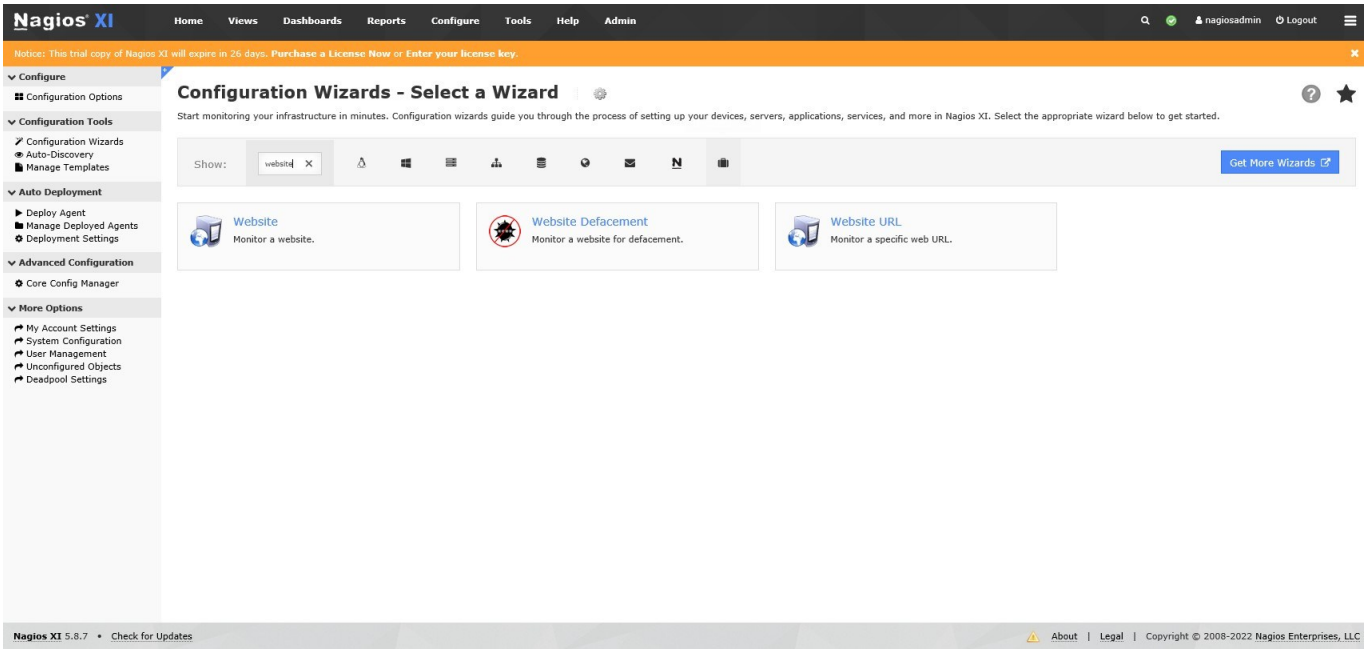
On peut aussi ensuite aller dans "Home" puis dans l'onglet "Details > Host Status" à gauche pour voir les machines maintenant supervisées par le serveur Nagios (en temps réel). On peut aussi aller dans "Configure > Core Config Manager" puis dans l'onglet "Monitoring > Hosts" à gauche pour cela :



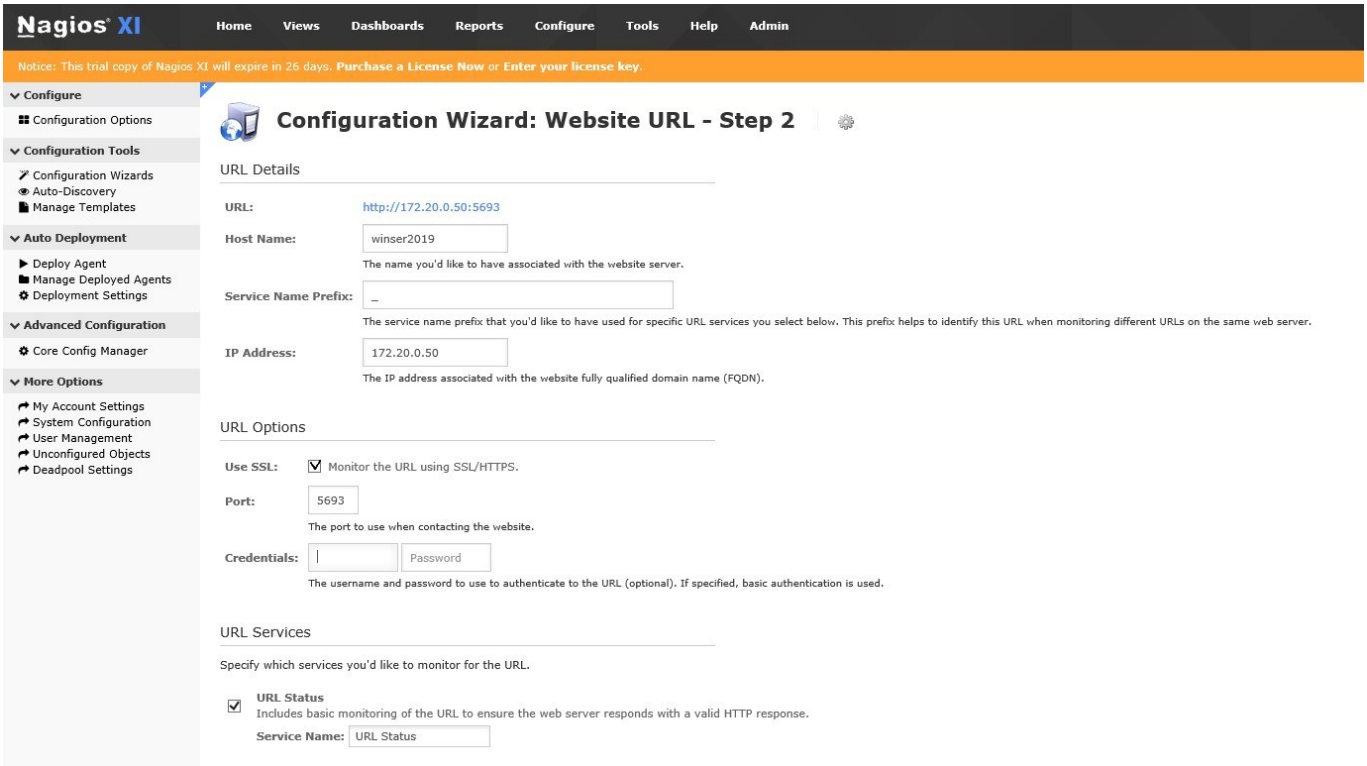


Détection de machines en utilisant NCPA :

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 :



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 supervisions :

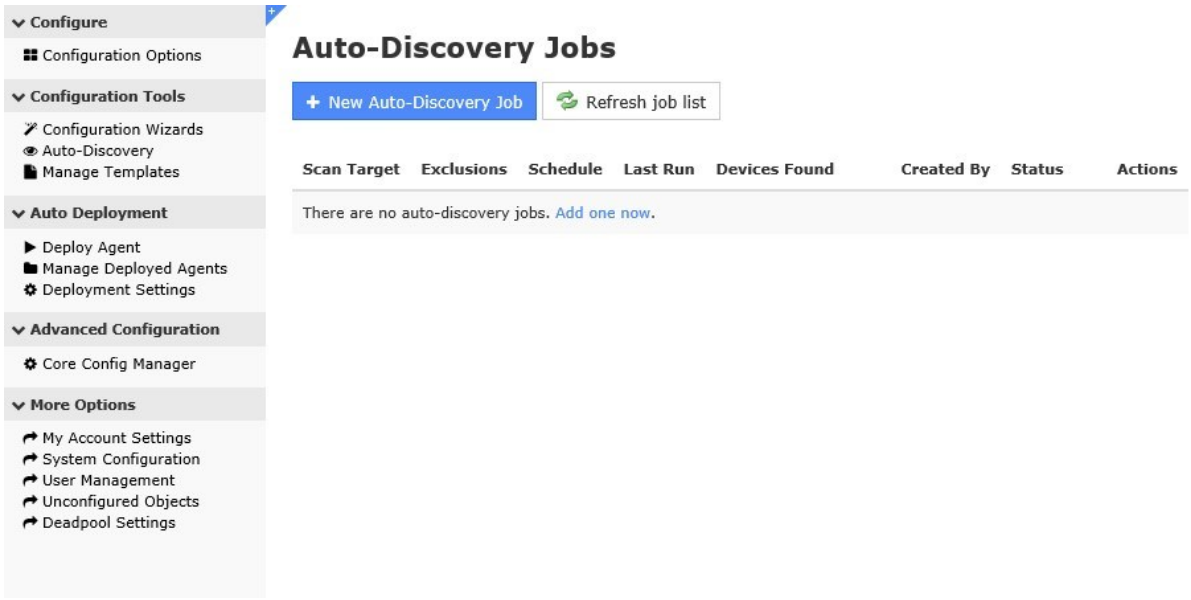


Détection de machines en utilisant Autodiscover :

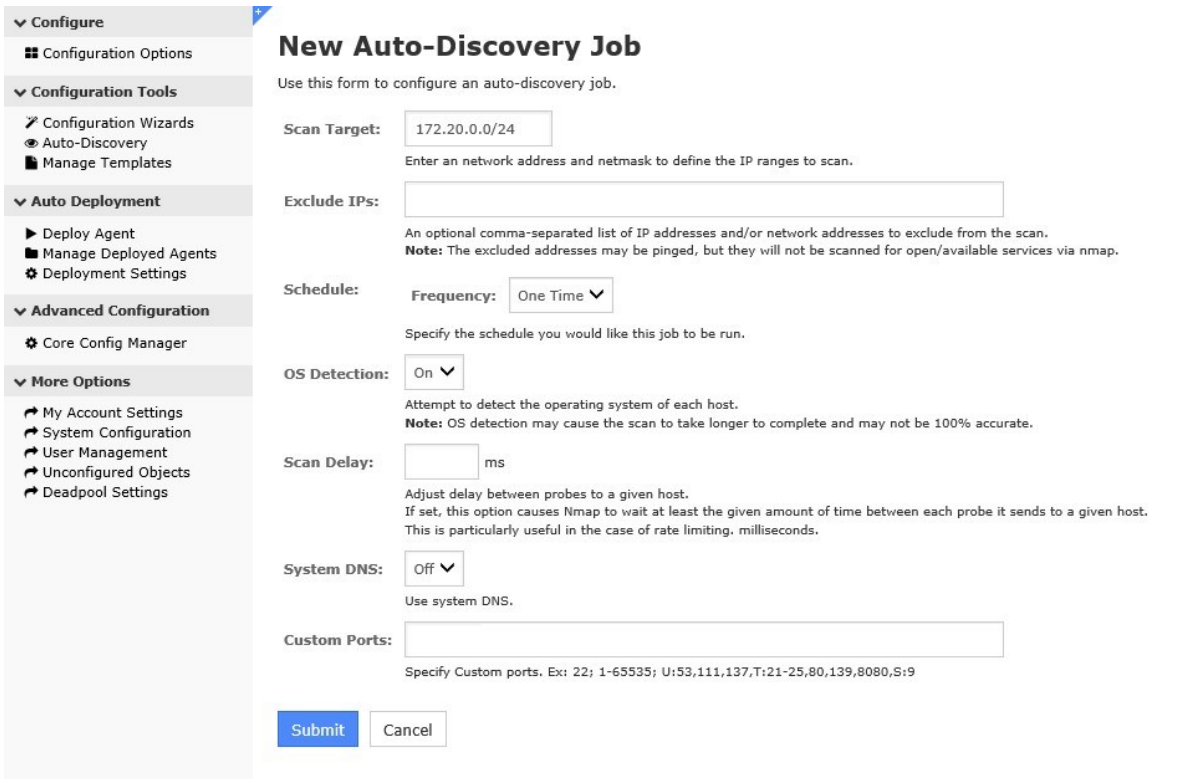
On peut aussi utiliser la méthode d'Autodiscover pour faire remonter les machines à superviser au serveur Nagios : ce dernier va envoyer une requête en Broadcast sur le réseau spécifier pour "découvrir" les machines qui s'y trouve. En fait, les machines sur ce réseau vont chacune répondre à la requête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

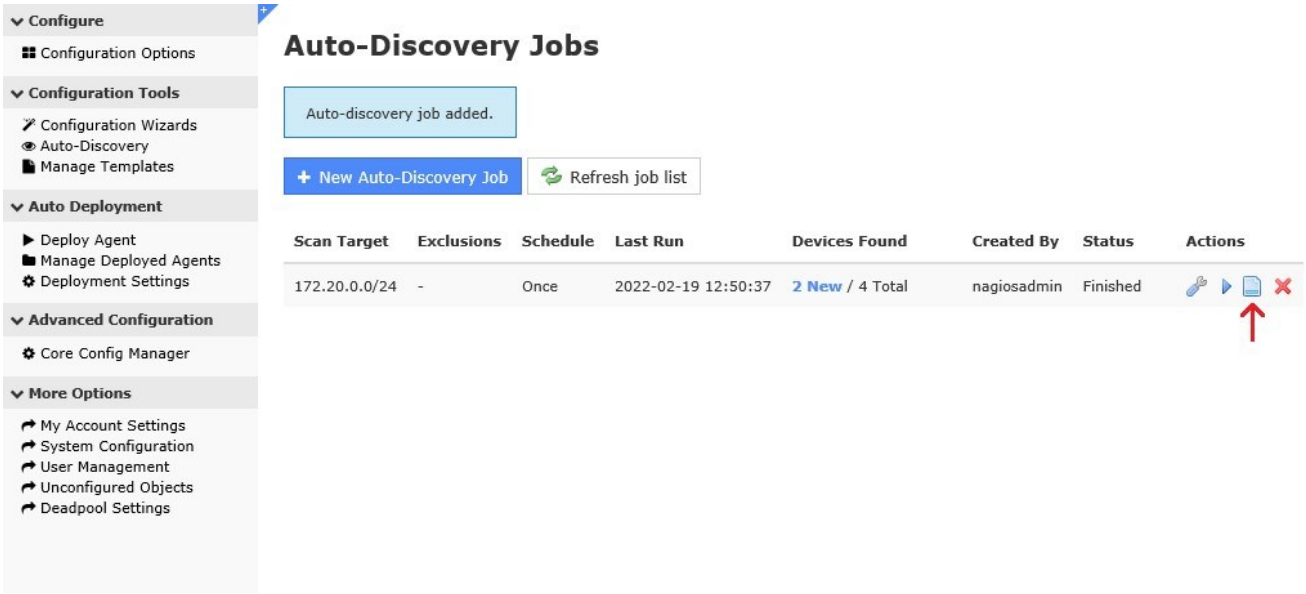
On commence par aller dans le menu "Configure > Configuration Wizards" puis dans l'onglet "Configuration Tools" à gauche on clique sur "Auto-Discovery". On clique ensuite sur "+ New Auto-Discovery Job" :



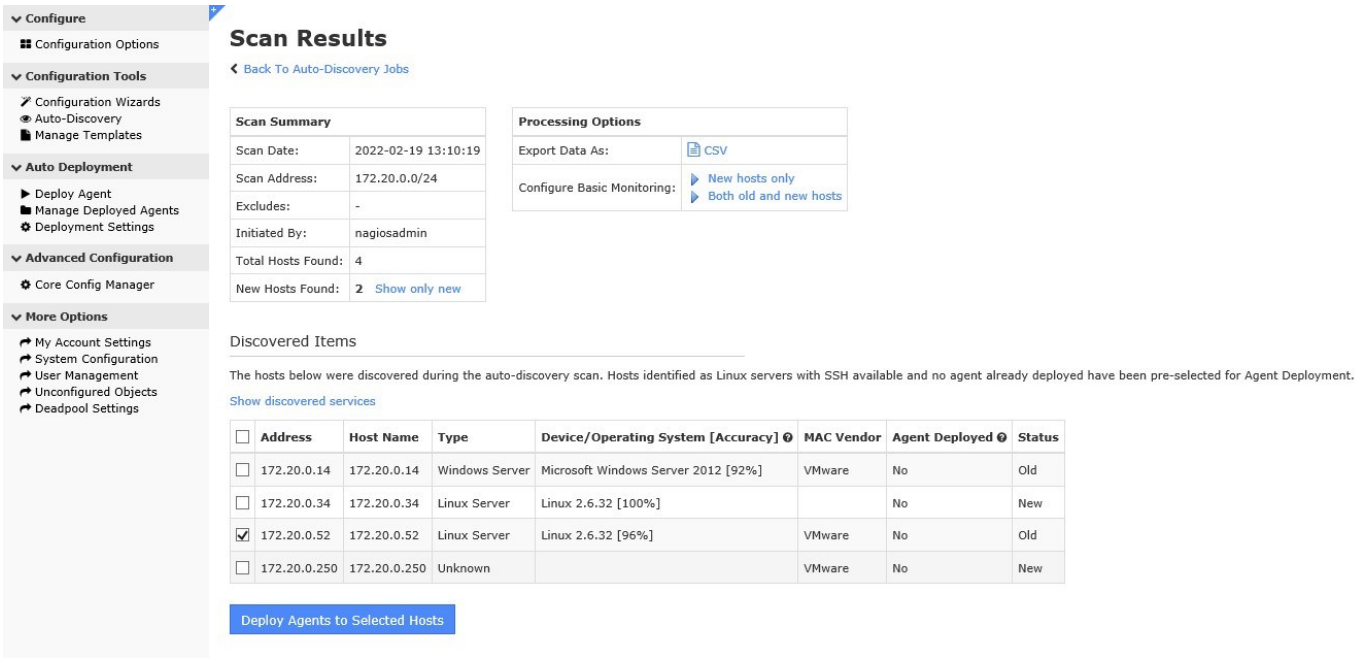
On spécifie ensuite le réseau que l'on veut scanner (sur lequel sont nos machines à superviser) ainsi que quelques paramètres que l'on laissera ici par défaut (ici on peut exclure l'adresse IP du serveur Nagios si on veut). Une fois que l'on a fini, on clique sur "Submit" :



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 :

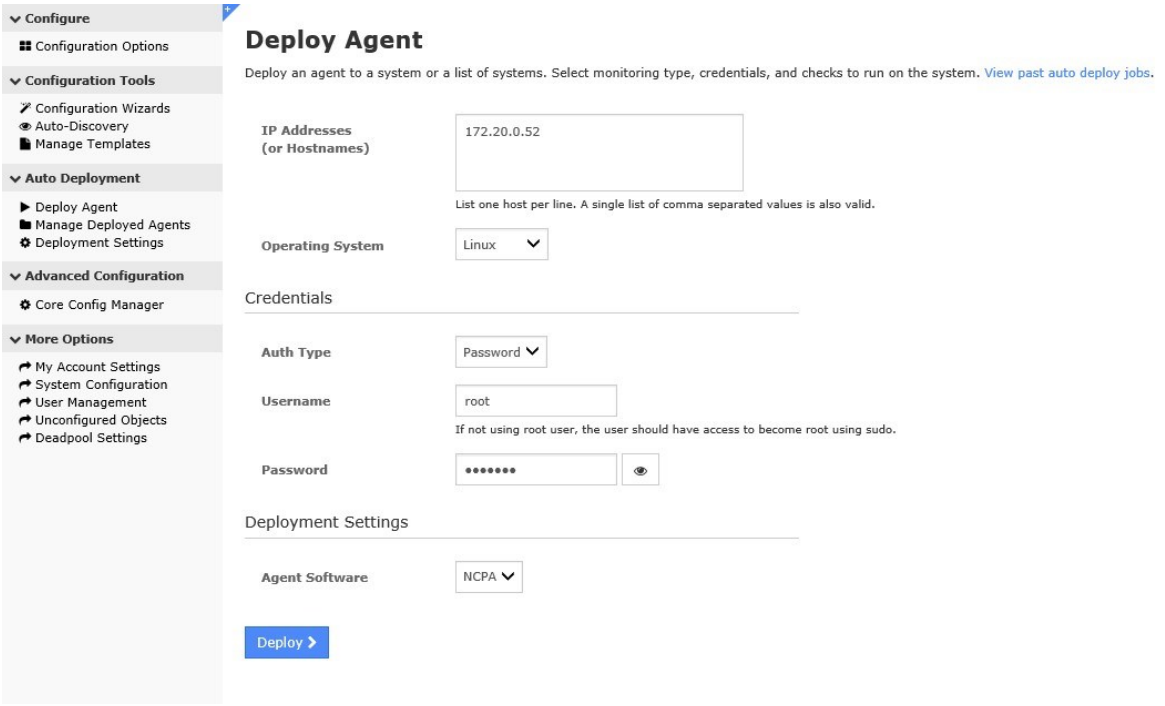


À partir d'ici on va pouvoir sélectionner sur quelles machines on veut installer les agents de supervision NCPA et le serveur Nagios les installera automatiquement. On coche donc les machines que l'on veut superviser* puis on clique sur "Deploy Agents to Selected Hosts" :



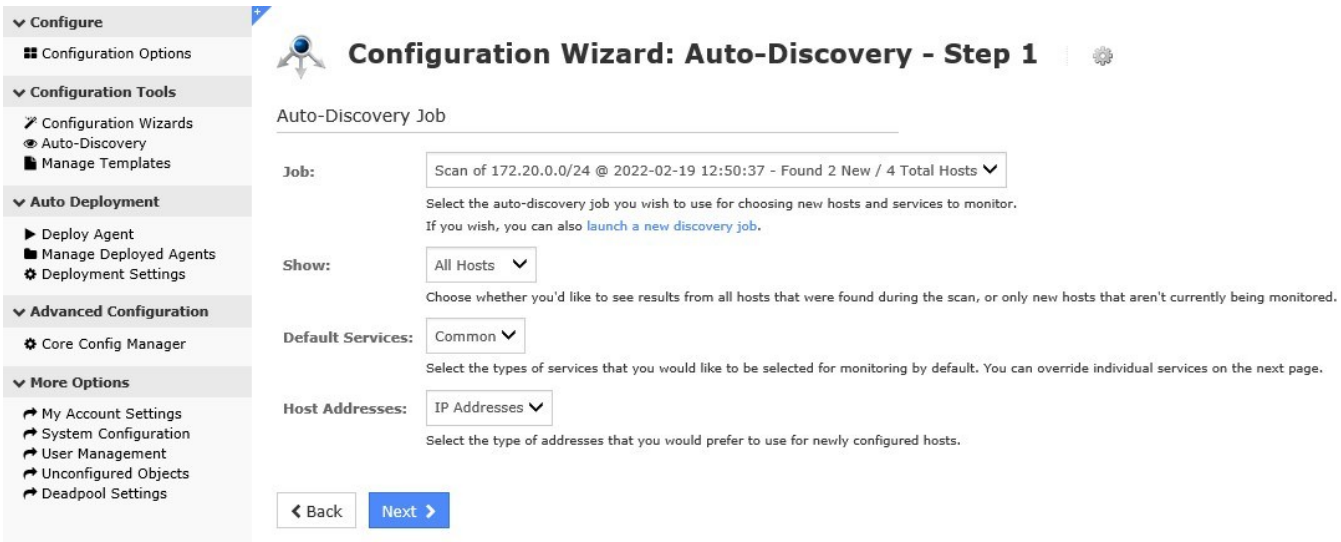
*Les nouvelles machines (Status : New) devraient être directement affichées mais si pour une raison ou pour une autre, elles ne s'affichent pas toutes : cliquez sur "Show all" au milieu à gauche sur la ligne "Total Hosts Found:"

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 paramêtres d'identifications et l'agent que l'on veut installer (par défaut NCPA) puis on clique sur "Deploy" :

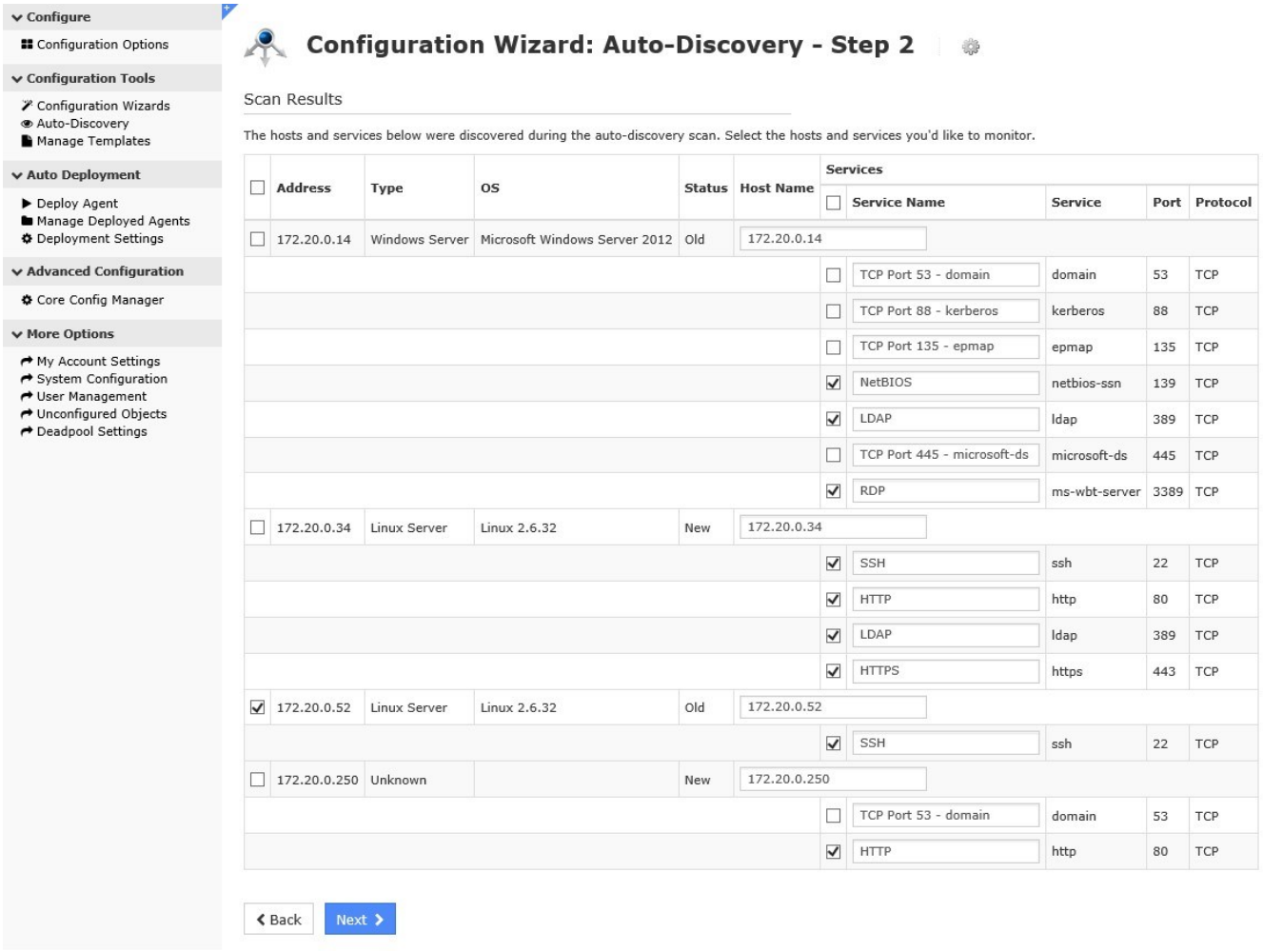


Le résultat de l'installation s'affiche ensuite.

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 :



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



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