

Projet sur la supervision

Présentation :

E4 : Épreuve pratique officielle du BTS SIO, spécialité SISR.

SERVICE NAGIOS XI

Introduction : À l'heure où les entreprises sont toutes dépendantes de leur système informatique, le moindre dysfonctionnement ou perte de données peut entraîner des conséquences graves sur leur chiffre d'affaires. C'est la raison pour laquelle la supervision informatique est un aujourd'hui un enjeu essentiel : pour tout savoir sur le sujet, découvrez vite notre petit guide de la supervision informatique !

Qu'est-ce que la supervision informatique ?

La supervision informatique désigne l'utilisation de techniques et d'outils permettant de surveiller un système informatique, afin de garantir son bon fonctionnement. Elle contrôle les opérations et les processus en permanence. L'objectif est de prévenir les défaillances, d'éviter les interruptions de service, et de détecter les failles de sécurité pour limiter les risques de cyberattaques. Les outils de supervision assurent la surveillance de tous les éléments du système informatique : serveurs et postes de travail, espaces de stockage et bases de données, applications et protections antivirus, sites web et sauvegardes, ils sont personnalisables en fonction des besoins du système. Un excellent moyen d'éprouver sa cybersécurité. Lorsqu'un problème est détecté, le système de surveillance émet des alertes sur la disponibilité des services ; les dysfonctionnements peuvent ensuite être résolus à distance ou sur site de manière centralisée.

Contexte :

La société HOLO 3D est une entreprise de fabrication de livre ayant un bâtiment dans différentes villes entre autres Bordeaux, Poitiers et Paris.

Elle connaît depuis peu de fortes réussites étant la seule société à proposer des livres 3D.

Pour se développer à l'international, il décide de racheter Intrade London.

En ce qui concerne l'infrastructure on compte :

LAURENT GRACE SOUMBOU COMPTE RENDU

À Paris : 100 utilisateurs, 110 postes de travail et 10 serveurs

À Poitiers : 15 utilisateurs 70 stations de travail (workstations) et 11 serveurs

À Bordeaux : 80 utilisateurs 90 stations de travail (workstations) et 11 serveurs

À Londres : 15 utilisateurs 15 stations et 4 serveurs

En 2019 une faille a fait découvrir des dysfonctionnements

Architecture réseau de l'entreprise :

Service active directory

Windows client 10,11

Une DMZ

Router/switch

Un portail captif répondant

Le wifi pour l'accès à internet

Un serveur web

Un firewall

Un VPN

Serveur DHCP

Service DNS

Hyperviseur (Serveur de virtualisation),

Service de messagerie,

En 2019 une faille a fait découvrir des dysfonctionnements

Le besoin :

Holo 3D a besoin de mettre en place un système de supervision sur son architecture réseau afin d'avoir une vue globale et d'avoir un taux de disponibilité de service élevé dans son entreprise.

Objectif :

Mise en place de **Nagios XI** afin de superviser le réseau de l'entreprise Holo 3D

Pour commencer on a besoin de plusieurs machines Virtual :

- Debian
- Windows 10 pro
- Windows server 2016 ou 2022

Réseau de l'entreprise : 192.168.1.0/24

- Debian 192.168.1.114
- Windows 10 pro 192.168.1.176
- Windows server 2016 ou 2022 192.168.1.174

Préparation de la mise place

Commandes indispensables pour débuter :

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

Vérification `bash` ET `local`
`ls -al`

Étape 1 : Installer SSH sur toutes Debian. Apt

`apt install openssh-server -y`

Étape 2 : Connexion ssh modifié le fichier `etc` de configuration.

`Nano /etc/ssh/sshd_config`

```
GNU nano 5.4 /etc/ssh/sshd_config
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
```

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.

```
C:\Users\soumb> ssh root@192.168.1.1141
ssh: Could not resolve hostname 192.168.1.1141: H\364te inconnu.

C:\Users\soumb> ssh root@192.168.1.114
The authenticity of host '192.168.1.114 (192.168.1.114)' can't be
ED25519 key fingerprint is SHA256:0kUm/sc8TQzgwcSCA87BjbWSvrH3jD9Q
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])
Host key verification failed.

C:\Users\soumb> ssh root@192.168.1.114
The authenticity of host '192.168.1.114 (192.168.1.114)' can't be
ED25519 key fingerprint is SHA256:0kUm/sc8TQzgwcSCA87BjbWSvrH3jD9Q
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])
Warning: Permanently added '192.168.1.114' (ED25519) to the list of
root@192.168.1.114's passwords:
Linux debian 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12)

The programs included with the Debian GNU/Linux system are free so
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: Thu May 18 17:58:35 2023 from 192.168.1.114
```

Etapes 4 : On rentre dans le bash

Fichier à modifier. `bashrc`


`nano .bashrc`

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

```
GNU nano 5.4 .bashrc *
# ~/.bashrc: executed by bash(1) for non-login shells.

# Note: PS1 and umask are already set in /etc/profile. You should not
# need this unless you want different defaults for root.
# PS1='${debian_chroot:+($debian_chroot)}\h:\w\$ '
# umask 022

# You may uncomment the following lines if you want 'ls' to be colorized
# export LS_OPTIONS='--color=auto'
# eval "$(dircolors)"
# alias ls='ls $LS_OPTIONS'
# alias ll='ls $LS_OPTIONS -l'
# alias l='ls $LS_OPTIONS -lA'
#
# Some more alias to avoid making mistakes:
# alias rm='rm -i'
# alias cp='cp -i'
# alias mv='mv -i'
figlet -f slant Connexion SSH | lolcat
```



CTRL + X

OUI et Entrée

Exit

Etapas 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

```
Checked 1 hosts
Checked 0 service dependencies
Checked 0 host dependencies
Checked 8 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight c
> Return Code: 0
-----

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://192.168.1.114/nagiosxi/
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 18 17:58:35 2023 from 192.168.1.114
root@debian:~# .bashrc
bash: .bashrc : commande introuvable
root@debian:~# nano .bashrc
root@debian:~# cd/tmp
bash: cd/tmp: Aucun fichier ou dossier de ce type
root@debian:~# cd /tmp
root@debian:/tmp# wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
--2023-05-18 18:10:18-- https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz
Résolution de assets.nagios.com (assets.nagios.com)... 2600:3c00::f03c:92ff:fe77:45ce, 45.79.49.120
Connexion à assets.nagios.com (assets.nagios.com)|2600:3c00::f03c:92ff:fe77:45ce|:443... connecté.
Requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 80735576 (77M) [application/x-gzip]
Sauvegarde en : « xi-latest.tar.gz »

xi-latest.tar.gz          9%[==>] 7,09M 1,22MB/s
```

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://192.168.1.114/nagiosxi/>)

Le test fera sur une web

The screenshot displays the Nagios XI web interface. The top navigation bar includes links for Home, Views, Dashboards, Reports, Configure, Tools, Help, and Admin. A user is logged in as 'nagiosadmin'. A notice at the top states: 'Notice: This trial copy of Nagios XI will expire in 26 days. Purchase a License Now or Enter your license key.' The left sidebar contains a menu with categories: Configure, Configuration Tools, Auto Deployment, Advanced Configuration, and More Options. The main content area is titled 'Configuration Wizards - Select a Wizard' and includes a search bar with 'snmp' entered. Below the search bar, there are five wizard options: Linux SNMP, SNMP, SNMP Trap, SNMP Walk, and Windows SNMP. Each option has a brief description of what it monitors. The footer shows 'Nagios XI 5.8.7' and a 'Check for Updates' link, along with 'About', 'Legal', and 'Copyright © 2008-2022 Nagios Enterprises, LLC'.

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

Id : nagiosadmin

Mdp : %^S#Qbnp.,g3#rA&A,vM (mot de passe par défaut attribuer par NagiosXi)

Install - Nagios XI

192.168.1.114/nagiosxi/install.php

Nagios XI

Install

Nagios XI Installation

Finalize your Nagios XI installation and step the initial configuration. These settings can be changed later.

General System Settings

Program URL:

Timezone:

Language:

User Interface Theme:

☐ Use HTTPS only (all HTTP requests will be redirected to HTTPS)

License Settings

License Type: ☒ Trial ☐ Licensed ☐ Free (Limited)

Trial includes unlimited nodes + enterprise features. Includes access to trial support.

[Click to get a trial key](#)

Nagios XI About Legal Copyright © 2008-2023 Nagios Enterprises, LLC

Finalize your Nagios XI installation and step the initial configuration. These settings can be change

Admin Account Settings

Username:

Password:

Full Name:

Email Address:

LAURENT GRACE SOUMBOU COMPTE RENDU

Installation terminée

toutes nos félicitations! vous avez installé avec succès nagios xi. vous pouvez maintenant vous connecter à nagios xi en utilisant les informations d'identification suivantes.

Nom d'utilisateur	nagiosadmin
Mot de passe	IXg\$.3#6c9GN!tpLO9j.

[se connecter à nagios xi >](#)

Interface WEB DE NAGIOSXI

Nagios XI Home Views Dashboards Reports Configure Tools Help Admin

Quick View

- Home Dashboard
- Tactical Overview
- Birdseye
- Operations Center
- Operations Screen
- Open Service Problems
- Open Host Problems
- All Service Problems
- All Host Problems
- Network Outages

Details

- Service Status
- Host Status
- Hostgroup Summary
- Hostgroup Overview
- Hostgroup Grid
- Servicegroup Summary
- Servicegroup Overview
- Servicegroup Grid
- BPI
- Metrics

Graphs

- Performance Graphs
- Graph Explorer

Maps

- World Map
- BBmap

Home Dashboard

Getting Started Guide

Common Tasks:

- [Change your account settings](#)
Change your account password and general preferences.
- [Change your notifications settings](#)
Change how and when you receive alert notifications.
- [Configure your monitoring setup](#)
Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- [Learn about XI](#)
Learn more about XI and its capabilities.
- [Signup for XI news](#)
Stay informed on the latest updates and happenings for XI.

Host Status Summary

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

Last Updated: 2023-05-18 18:42:35

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
11	1	0	0	0
Unhandled		Problems	All	
1		1	12	

Last Updated: 2023-05-18 18:42:35

Administrative Tasks

II/ La supervision des clients

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

TP Nagios du 14-15 février 2023 :


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

- Service DNS.

On prépare 4 nouvelles machines :

Serveur Nagios  192.168.1.114/24 (qu'on avait déjà installé sur une VM Debian

~~en~~) serveur Windows Serv 2016  192.168.1.174/24

Serveur Ubuntu*  192.168.1.176/24

serveur Debian*  192.168.1.178/24

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.

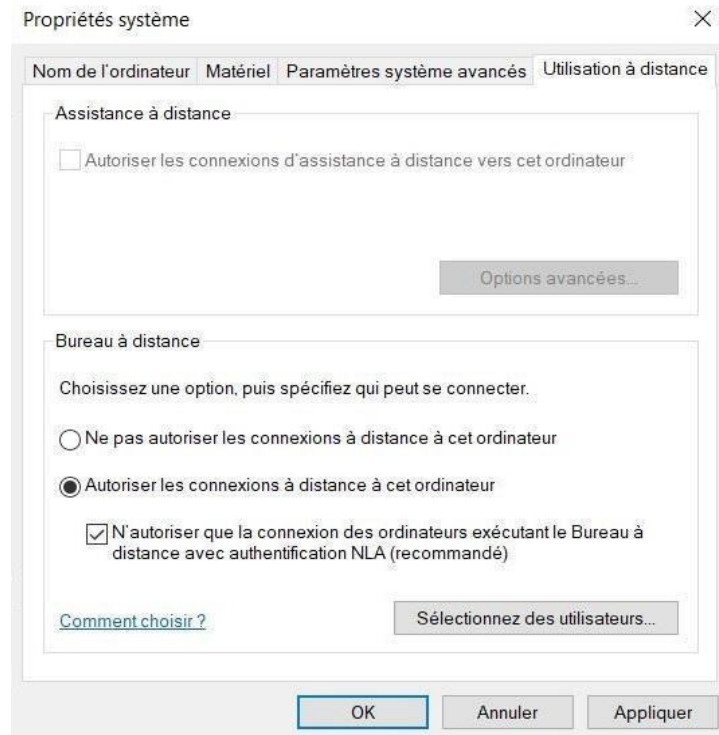
On a quatre méthodes principales de supervision par Nagios : **SNMP**, **NCPA (Nagios Cross-Platform Agent)**, **NRPE** et **Auto-discover**

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

Machine Windows Server 2016

LAURENT GRACE SOUMBOU COMPTE RENDU

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

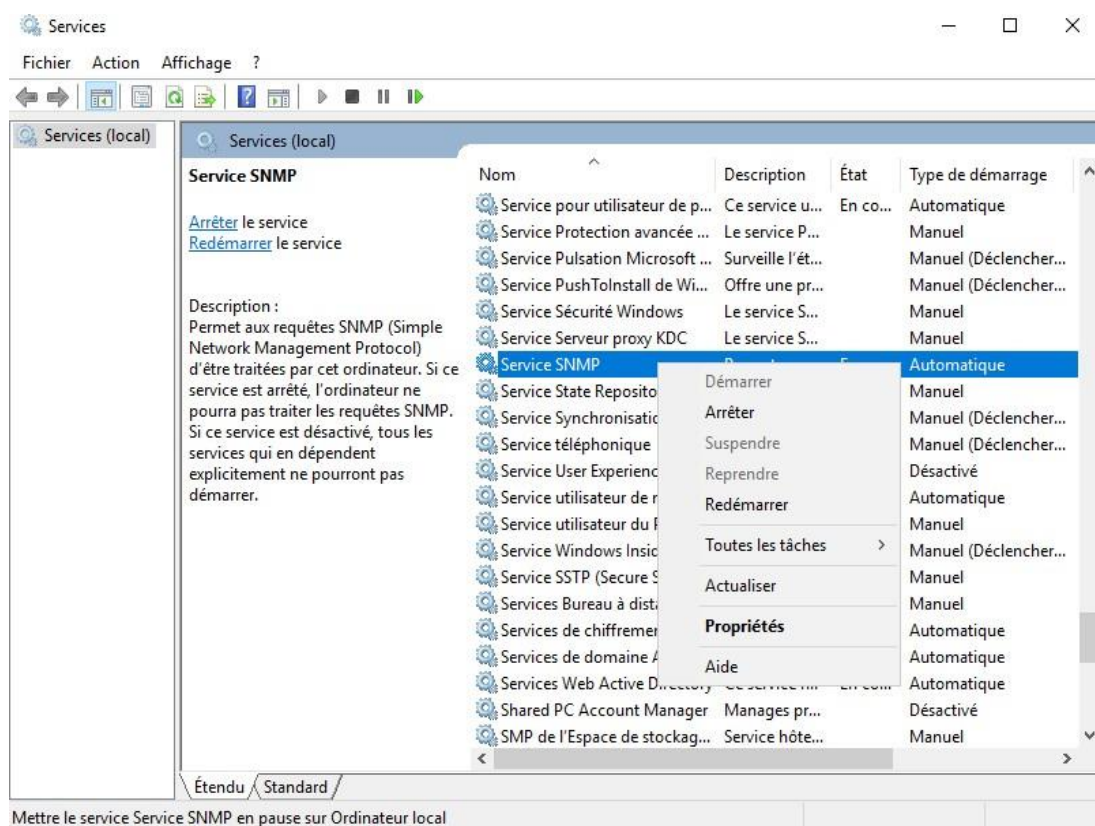


Installation du service/agent SNMP sur Windows Server 2016 :

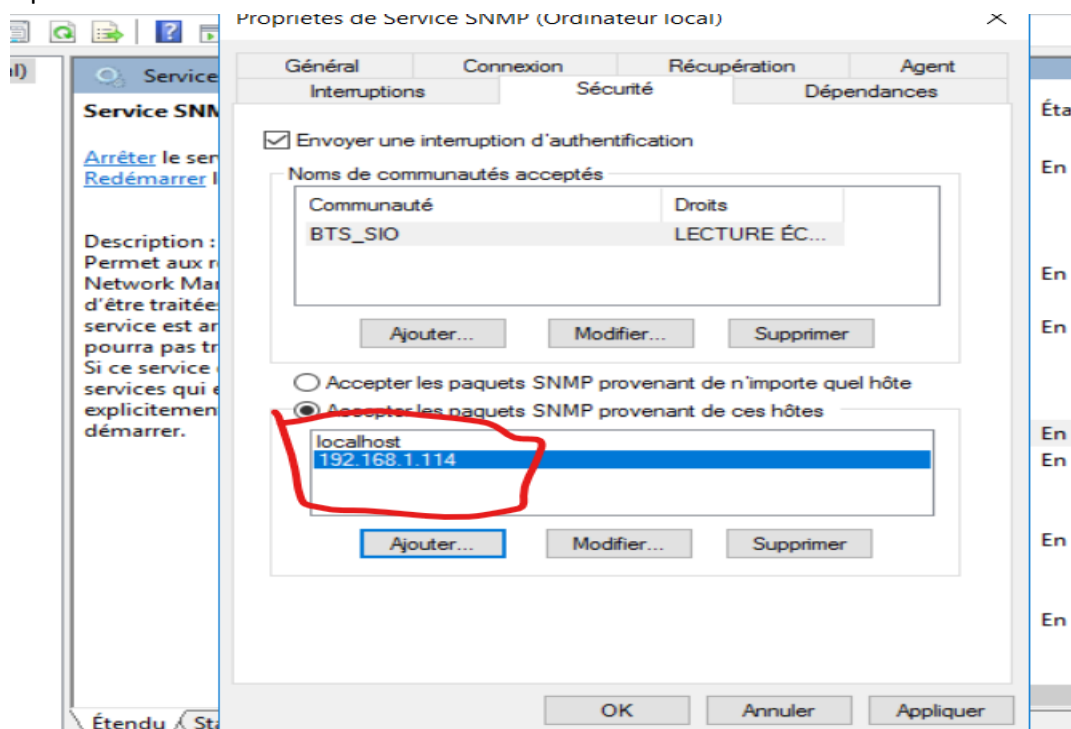
On va dans "Gérer > Ajouter des rôles et fonctionnalités" puis comme d'habitude on coche "Installation basée sur un rôle une fonctionnalité", on sélectionne le serveur local, on ne choisit aucun nouveau rôle mais on va ensuite cocher la fonctionnalité "Service SNMP" puis on clique sur "Ajouter la fonctionnalité"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

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" :



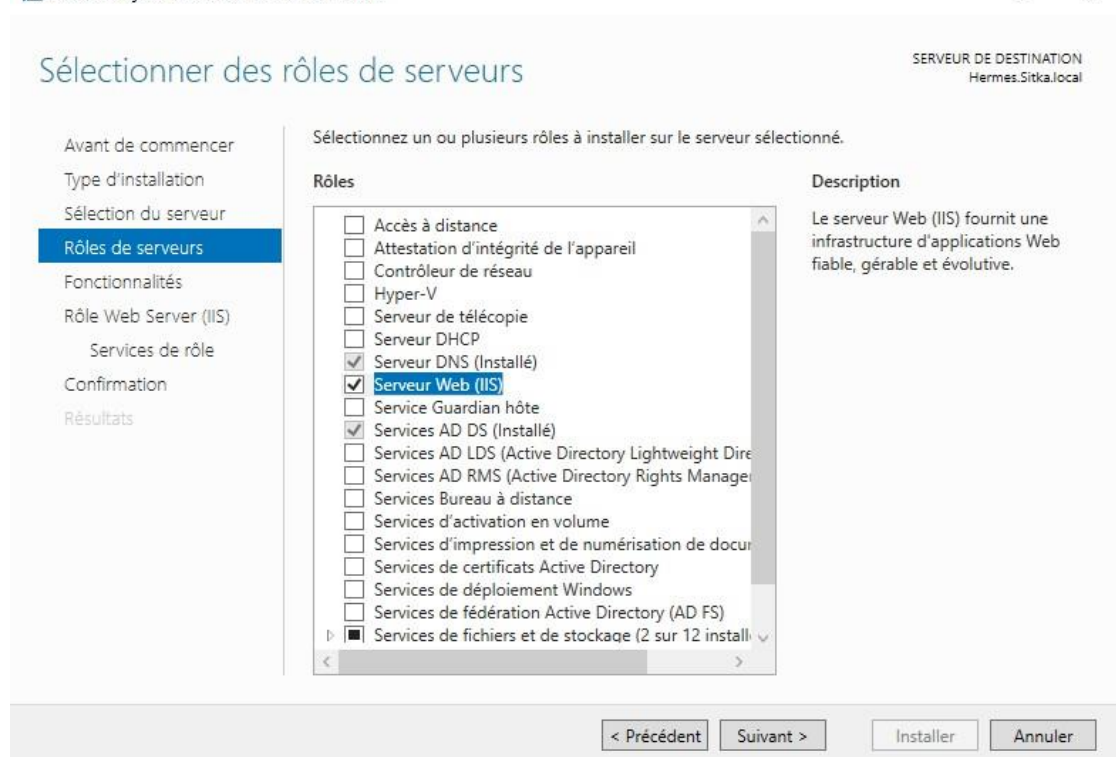
Dans l'onglet "Agent" des propriétés du service SNMP on coche toutes les cases en dessous dans la rubrique "Service" :



Puis dans l'onglet "Sécurité" on va d'abord ajouter notre communauté "BTS_SIO" 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".

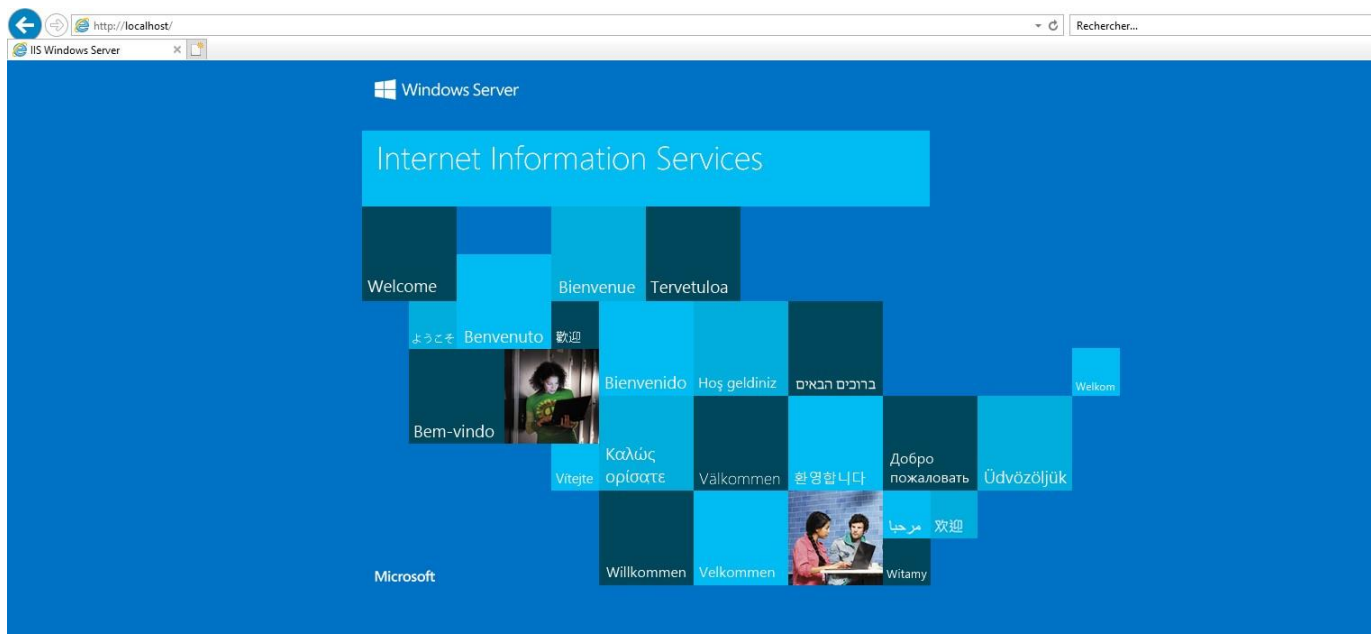
Installation de l'agent NCPA sur Windows Server 2016 :

Pour utiliser l'agent NCPA 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 2016 :

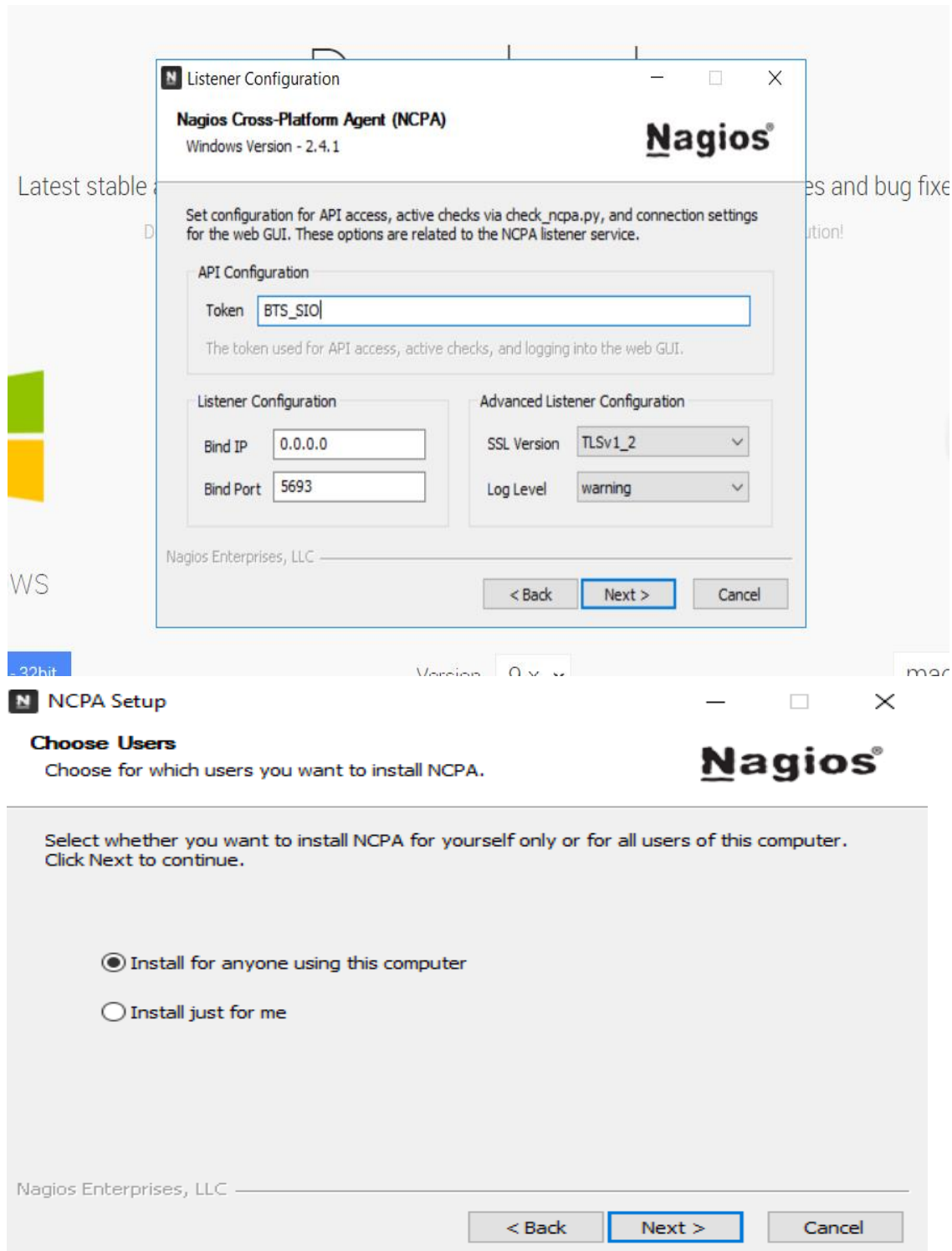


On peut trouver les fichiers de la d'accueil du serveur web dans le dossier **C:\inetpub\wwwroot**

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)

The screenshot shows the 'NCPA' Downloads page. The header includes links for Features, Downloads, Documentation, FAQ, and Project. The main heading is 'Downloads'. Below it, a message states: '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!'. The page is divided into three main sections for different operating systems: Windows, CentOS, and Mac. The Windows section features the Windows logo, a dropdown for 'CentOS' (which is currently selected), a 'Version' dropdown set to '8.x', and buttons for 'EXE Installer - 32bit' and 'RPM - 64bit'. The CentOS section has a button for 'Install using Nagios repo - Recommended'. The Mac section features the Apple logo, a dropdown for 'macOS 10.15+', and a button for 'DMG Installer - 64bit'. Below these sections, there are four links: 'Other Downloads' (for plugin, older versions, and development versions), 'Nagios Plugin' (for active checks, version 1.2.4, with a link to 'Download check_ncpa.py'), 'Archived Versions' (for older versions of NCPA, with a link to 'Go to download archive'), and 'Development Builds' (for latest dev builds, with a note that these are not meant for production).

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 "BTS_SIO", 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://192.168.1.174:5693/> (adresse IP entrée à l'installation avec port par défaut) dans le navigateur web du serveur WS 2016 :



Web GUI Log In

Nagios XI Domicile Affichage Tableaux Rapports Configurer Outils Aide Admin

Effectuez une mise à niveau vers une version sous licence de Nagios XI et bénéficiez d'une assistance et d'avantages de mise à niveau.

Configurer

- Configuration Options
- Outils de configuration**
 - Assistants de configuration
 - Découverte automatique
 - Gérer les modèles
- Déploiement automatique**
 - Déployer l'agent
 - Gérer les agents déployés
 - Paramètres de déploiement
- Configuration avancée**
 - Gestionnaire de configuration de base
- Plus d'options**
 - Paramètres de mon compte
 - Configuration du système
 - Gestion des utilisateurs
 - Objets non configurés
 - Paramètres de Deadpool

Windows Machine Information

IP Address: 192.168.1.174
The IP address of the Windows machine you'd like to monitor.

Operating System: Windows Server 2016

SNMP Settings

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

SNMP Version: 2c
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: BTS_SIO
The SNMP community string required used to query the Windows machine.

MONTE DE WINDOWS SERVER SUR NAGIOS :

Nagios XI Home Views Dashboards Reports Configure Tools Help Admin

Quick View

- Home Dashboard
- Tactical Overview
- Birdseye
- Operations Center
- Operations Screen
- Open Service Problems
- Open Host Problems
- All Service Problems
- All Host Problems
- Network Outages

Host Status

All hosts

Host Status Summary

Up	Down	Unreachable	Pending
2	0	0	0
Unhandled	Problems	All	
0	0	2	

Last Updated: 2023-05-18 21:08:33

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
15	0	0	3	0
Unhandled	Problems	All		
3	3	18		

Last Updated: 2023-05-18 21:08:33

Showing 1-2 of 2 total records

Page 1 of 1 15 Per Page Go

Host	Status	Duration	Attempt	Last Check	Status Information
BTS_SIO	Up	16m 18s	1/5	2023-05-18 21:05:14	OK - 192.168.1.174 rta 0,638ms lost 0%
localhost	Up	2h 43m 15s	1/10	2023-05-18 21:07:18	OK - 127.0.0.1 rta 0,019ms lost 0%

Last Updated: 2023-05-18 21:08:33

Page 1 of 1 15 Per Page Go

Details

- Service Status
- Host Status
- Hostgroup Summary
- Hostgroup Overview
- Hostgroup Grid
- Servicegroup Summary
- Servicegroup Overview
- Servicegroup Grid
- BPI
- Metrics

Graphs

- Performance Graphs

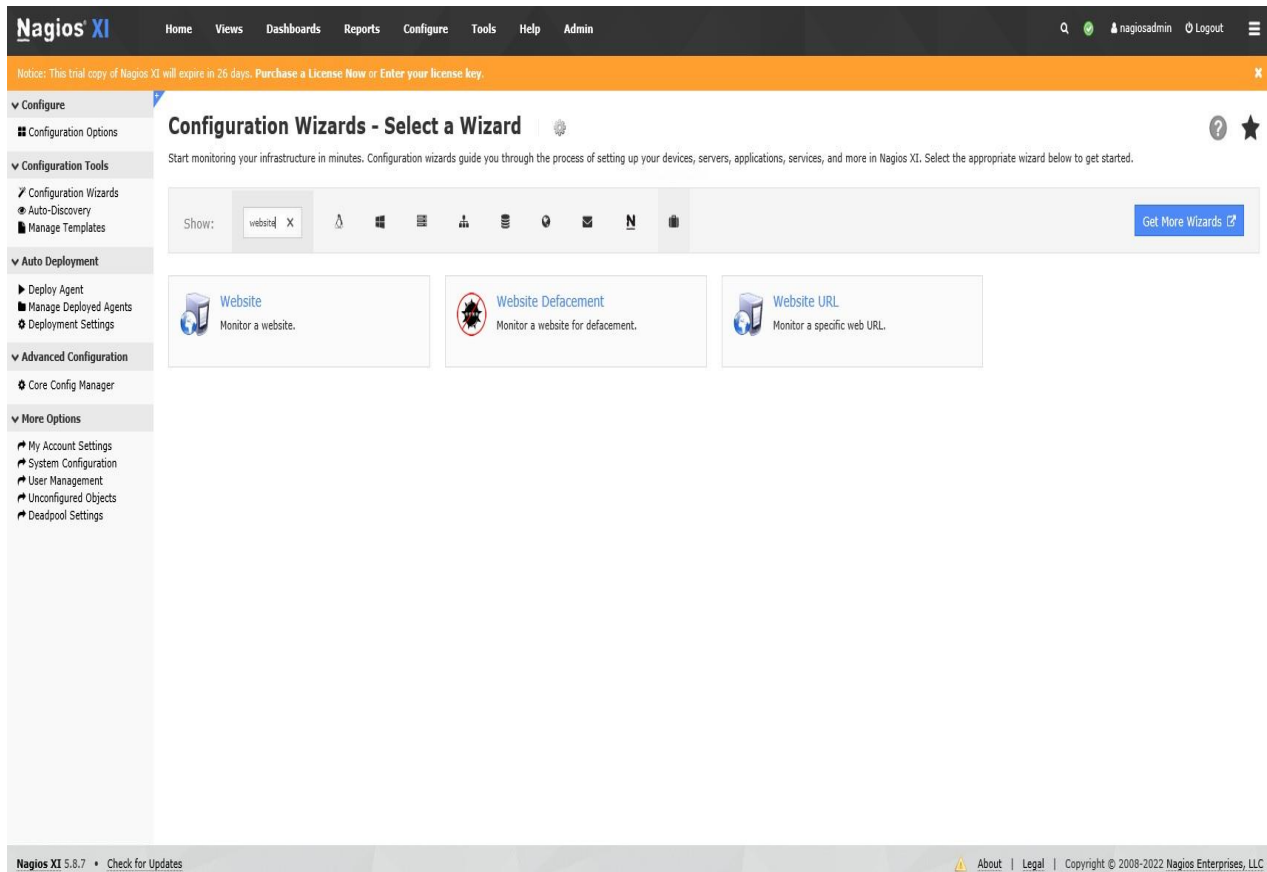
Dans le Wizard on précise ensuite l'adresse IP de la machine à superviser (donc à relier au serveur Nagios), son système d'exploitation (si demandé) ainsi que le nom de la communauté/token :

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 :

Nagios XI Home Views Dashboards Reports Configure Tools Help Admin

Notice: This trial copy of Nagios XI will expire in 26 days. [Purchase a License Now](#) or [Enter your license key](#).

Configuration Wizard: Website URL - Step 2

URL Details

URL:

Host Name:
The name you'd like to have associated with the website server.

Service Name Prefix:
The service name prefix that you'd like to have used for specific URL services you select below. This prefix helps to identify this URL when monitoring different URLs on the same web server.

IP Address:
The IP address associated with the website fully qualified domain name (FQDN).

URL Options

Use SSL: ☒ Monitor the URL using SSL/HTTPS.

Port:
The port to use when contacting the website.

Credentials:
The username and password to use to authenticate to the URL (optional). If specified, basic authentication is used.

URL Services

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

☒ **URL Status**
Includes basic monitoring of the URL to ensure the web server responds with a valid HTTP response.

Service Name:

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" :

Auto-Discovery Jobs

[+ New Auto-Discovery Job](#) [Refresh job list](#)

Scan Target	Exclusions	Schedule	Last Run	Devices Found	Created By	Status	Actions
There are no auto-discovery jobs. Add one now.							

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" :

New Auto-Discovery Job

Use this form to configure an auto-discovery job.

Scan Target:
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:

Specify the schedule you would like this job to be run.

OS Detection:
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: ms
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:
Use system DNS.

Custom Ports:
Specify Custom ports. Ex: 22; 1-65535; U:53,111,137,T:21-25,80,139,8080,S:9

[Submit](#) [Cancel](#)





Le serveur Nagios va ensuite débiter 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 :

LAURENT GRACE SOUMBOU COMPTE RENDU

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
172.20.0.0/24	-	Once	2022-02-19 12:50:37	2 New / 4 Total	nagiosadmin	Finished	   

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" :


Scan Results

[Back To Auto-Discovery Jobs](#)

Scan Summary

Scan Date:	2022-02-19 13:10:19
Scan Address:	172.20.0.0/24
Excludes:	-
Initiated By:	nagiosadmin
Total Hosts Found:	4
New Hosts Found:	2 Show only new

Processing Options

Export Data As:	 CSV
Configure Basic Monitoring:	New hosts only Both old and new hosts

Discovered Items

The hosts below were discovered during the auto-discovery scan. Hosts identified as Linux servers with SSH available and no agent already deployed have been pre-selected for Agent Deployment.

[Show discovered services](#)

<input type="checkbox"/>	Address	Host Name	Type	Device/Operating System [Accuracy]	MAC Vendor	Agent Deployed	Status
<input type="checkbox"/>	172.20.0.14	172.20.0.14	Windows Server	Microsoft Windows Server 2012 [92%]	VMware	No	Old
<input type="checkbox"/>	172.20.0.34	172.20.0.34	Linux Server	Linux 2.6.32 [100%]		No	New
<input checked="" type="checkbox"/>	172.20.0.52	172.20.0.52	Linux Server	Linux 2.6.32 [96%]	VMware	No	Old
<input type="checkbox"/>	172.20.0.250	172.20.0.250	Unknown		VMware	No	New

[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:"

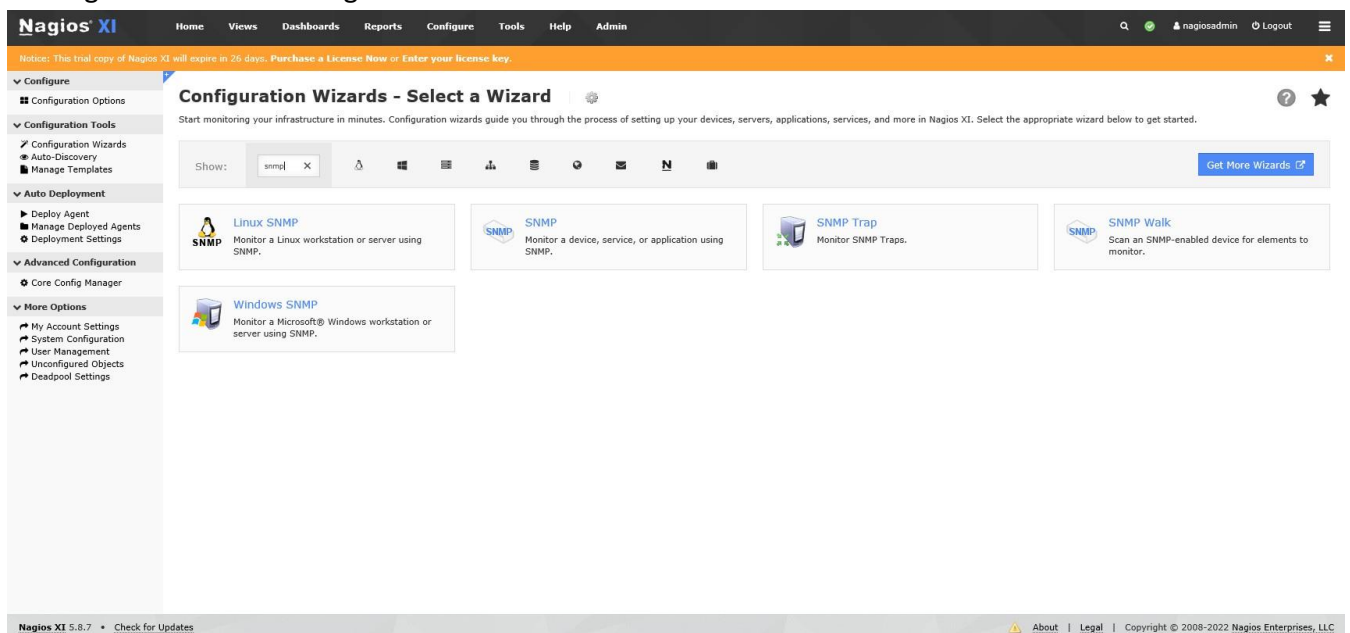
Ensuite on précise l'adresse IP des machines à superviser (rempli automatiquement d'après ce que l'on a coché), leur système d'exploitation ainsi que les paramètres d'identifications et L'agent que l'on veut installer (par défaut NCPA) puis on clique sur "Deploy" :

LAURENT GRACE SOUMBOU COMPTE RENDU

The screenshot shows the 'Deploy Agent' configuration page in Nagios XI. On the left is a sidebar menu with categories: Configure, Configuration Tools, Auto Deployment, Advanced Configuration, and More Options. The 'Deploy Agent' option under 'Auto Deployment' is selected. The main content area is titled 'Deploy Agent' and includes a description: '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.' The form contains several sections: 'IP Addresses (or Hostnames)' with a text input containing '172.20.0.52' and a note 'List one host per line. A single list of comma separated values is also valid.'; 'Operating System' with a dropdown menu set to 'Linux'; 'Credentials' section with 'Auth Type' set to 'Password', 'Username' set to 'root', and a note 'If not using root user, the user should have access to become root using sudo.'; and 'Deployment Settings' with 'Agent Software' set to 'NCPA'. A blue 'Deploy >' button is at the bottom.

Le résultat de l'installation s'affiche ensuite.

À partir de là 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 :"



Nagios® XI

HomeViewsDashboardsReportsConfigureToolsHelpAdmin

Notice! This trial copy of Nagios XI will expire in 26 days. Purchase a License Now or Enter your license key.

- Configuration
 - Configuration Options
- Configuration Tools
 - Configuration Wizards
 - Auto-Discovery
 - Manage Templates
- Auto Deployment
 - Deploy Agent
 - Manage Deployed Agents
 - Deployment Settings
- Advanced Configuration
 - Core Config Manager
- More Options
 - My Account Settings
 - System Configuration
 - User Management
 - Unconfigured Objects
 - Deadpool Settings

Configuration Wizards - Select a Wizard

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.

Show: snmp X
 [Get More Wizards](#)

Linux SNMP
 Monitor a Linux workstation or server using SNMP.

SNMP
 Monitor a device, service, or application using SNMP.

SNMP Trap
 Monitor SNMP Traps.

SNMP Walk
 Scan an SNMP-enabled device for elements to monitor.

Windows SNMP
 Monitor a Microsoft® Windows workstation or server using SNMP.

Nagios XI 5.8.7 • Check for Updates

About | Legal | Copyright © 2008-2022 Nagios Enterprises, LLC

🔍 🌱 👤 nagiosadmin 🔒 Logout

✕ Notice: This trial copy of Nagios XI will expire in 26 days. [Purchase a License Now](#) or [Enter your license key.](#)

- [▼ Configuration](#)
 - Configuration Options
- [▼ Configuration Tools](#)
 - Configuration Wizards
 - Auto-Discovery
 - Manage Templates
- [▼ Auto Deployment](#)
 - ▶ Deploy Agent
 - Manage Deployed Agents
 - Deployment Settings
- [▼ Advanced Configuration](#)
 - Core Config Manager
- [▼ More Options](#)
 - ➡ My Account Settings
 - ➡ System Configuration
 - ➡ User Management
 - ➡ Unconfigured Objects
 - ➡ Deadpool Settings

Configuration Wizards - Select a Wizard ⚙️

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.

Show:
 ✕
 [Get More Wizards ➦](#)

Linux SNMP
Monitor a Linux workstation or server using SNMP.

SNMP Trap
Monitor SNMP Traps.

SNMP Walk
Scan an SNMP-enabled device for elements to monitor.

Windows SNMP
Monitor a Microsoft® Windows workstation or server using SNMP.

Nagios XI 5.8.7 • [Check for Updates](#)
⚠️ About | Legal | Copyright © 2008-2022 Nagios Enterprises, LLC

Nagios XI
Home Views Dashboards Reports Configure Tools Help Admin

Notice: This trial copy of Nagios XI will expire in 25 days. [Purchase a License Now](#) or [Enter your license key.](#)

- ▼ **Configure**
 - Configuration Options
- ▼ **Configuration Tools**
 - Configuration Wizards
 - Auto-Discovery
 - Manage Templates
- ▼ **Auto Deployment**
 - ▶ Deploy Agent
 - Manage Deployed Agents
 - Deployment Settings
- ▼ **Advanced Configuration**
 - Core Config Manager
- ▼ **More Options**
 - My Account Settings
 - System Configuration
 - User Management
 - Unconfigured Objects
 - Deadpool Settings

Configuration Wizards - Select a Wizard ? ★

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.

Show: snmp X

[Get More Wizards](#)

Linux SNMP

Monitor a Linux workstation or server using SNMP.

Windows SNMP

Monitor a Microsoft® Windows workstation or server using SNMP.

SNMP Trap

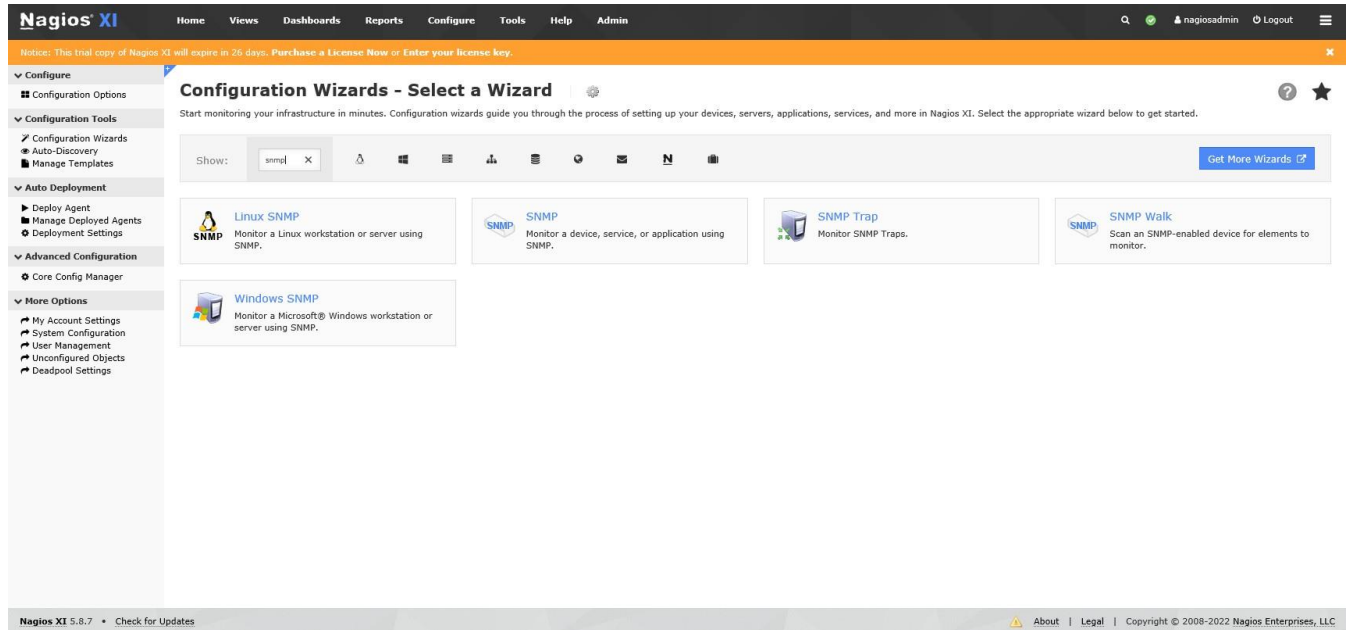
Monitor SNMP Traps.

SNMP Walk

Scan an SNMP-enabled device for elements to monitor.

Nagios XI 5.8.7 • [Check for Updates](#)
About | Legal | Copyright © 2008-2022 Nagios Enterprises, LLC

LAURENT GRACE SOUMBOU COMPTE RENDU



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" :

LAURENT GRACE SOUMBOU COMPTE RENDU

Configure

Configuration Options

Configuration Tools

Configuration Wizards

Auto-Discovery

Manage Templates

Auto Deployment

Deploy Agent

Manage Deployed Agents

Deployment Settings

Advanced Configuration

Core Config Manager

More Options

My Account Settings

System Configuration

User Management

Unconfigured Objects

Deadpool Settings

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.

<input type="checkbox"/>	Address	Type	OS	Status	Host Name	Services			
						<input type="checkbox"/> Service Name	Service	Port	Protocol
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input checked="" type="checkbox"/>	172.20.0.52	Linux Server	Linux 2.6.32	Old	172.20.0.52	<input checked="" type="checkbox"/> SSH	ssh	22	TCP
<input type="checkbox"/>	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".

Conclusion :