



Installation et configuration de Nagios XI

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`

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.

```

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`

```

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

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 !!!

memo + Nagios - x | Nagios - Google D x | Install · Nagios XI x

Non sécurisé | 192.168.23.138/nagiosxi/install.php

Applications Mails Drive Réseau CERTA Plateforme CFA

» | Liste de lecture

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
http://192.168.23.138/nagiosxi/ ?

Timezone
(UTC+01:00) Paris

Language
English (English)

User Interface Theme
Modern

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

License Settings

License Type
Nagios XI

[About](#) | [Legal](#) | Copyright © 2008-2022 [Nagios Enterprises, LLC](#)

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

Id : nagiosadmin

Mdp : Copier le mot de passe

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!tpL09j

[se connecter à nagios xi >](#)

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.

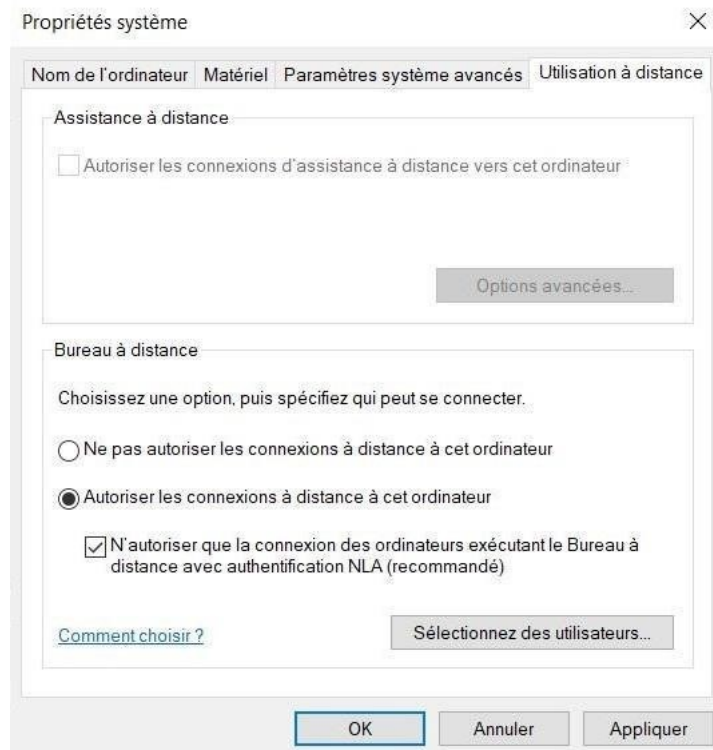
On a quatre méthodes principales de supervision par Nagios : **SNMP**, **NCPA (Nagios CrossPlatform Agent)**, **NRPE** et **Auto-discover**. NRPE ne sera pas couvert ici (on ne l'a pas vu durant ces deux séances).

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" :

BTS 2022-2024



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" :

Sélectionner des fonctionnalités

SERVEUR DE DESTINATION
Hermes.Sitka.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

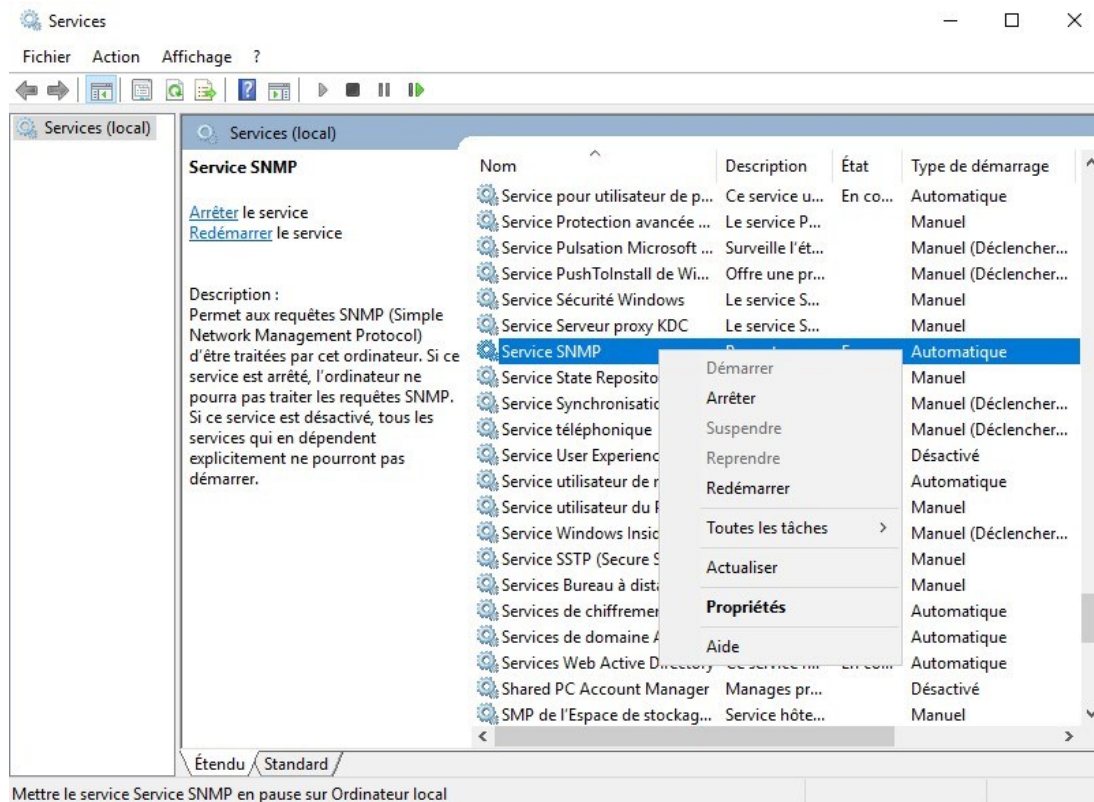
Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités	Description
<input type="checkbox"/> Sauvegarde Windows Server	
<input type="checkbox"/> Serveur de gestion des adresses IP (IPAM)	
<input type="checkbox"/> Serveur SMTP	
<input type="checkbox"/> Serveur WINS	
▸ <input type="checkbox"/> Service d'activation des processus Windows	
<input type="checkbox"/> Service de recherche Windows	
<input type="checkbox"/> Service de réseau local sans fil	
▸ <input type="checkbox"/> Service de transfert intelligent en arrière-plan (BITS)	
<input type="checkbox"/> Service Serveur iSNS	
▸ <input checked="" type="checkbox"/> Service SNMP	Le service SNMP (Simple Network Management Protocol) inclut des agents qui analysent l'activité des périphériques réseau et rapportent les résultats de cette analyse à la console système du réseau.
<input type="checkbox"/> Simple TCP/IP Services	
▸ <input type="checkbox"/> SMB 1.0/CIFS File Sharing Support	
<input type="checkbox"/> Sous-système Windows pour Linux	
<input type="checkbox"/> Stockage étendu	
<input type="checkbox"/> Support Hyper-V pour Host Guardian	
<input type="checkbox"/> Telnet Client	
<input type="checkbox"/> TFTP Client	
<input type="checkbox"/> Virtualisation de réseau	
<input type="checkbox"/> Windows Biometric Framework	

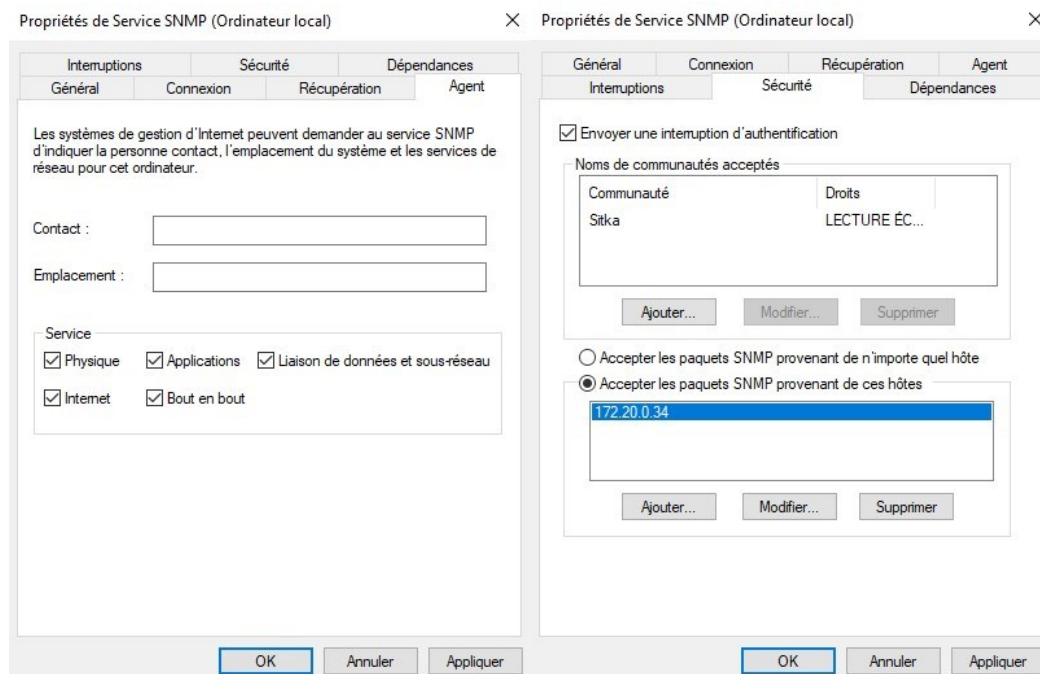
< Précédent Suivant > Installer Annuler

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" :

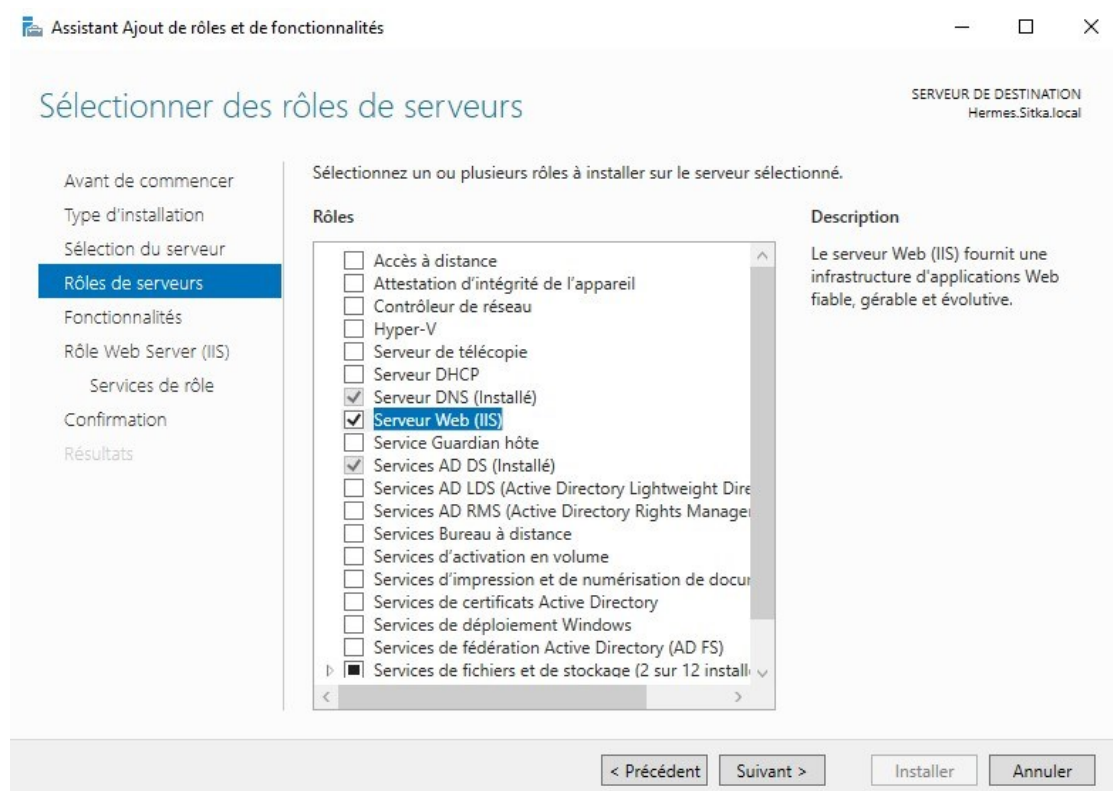


Puis dans l'onglet "Sécurité" on va d'abord ajouter notre communauté "Sitka" à la liste en cliquant sur "Ajouter..." et en définissant ses droits et en la nommant, puis on coche "Accepter les paquets SNMP provenant de ces hôtes" et on retire "localhost" de la liste avant d'y ajouter l'adresse IP de notre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

Installation de l'agent NCPA sur Windows Server 2019 :

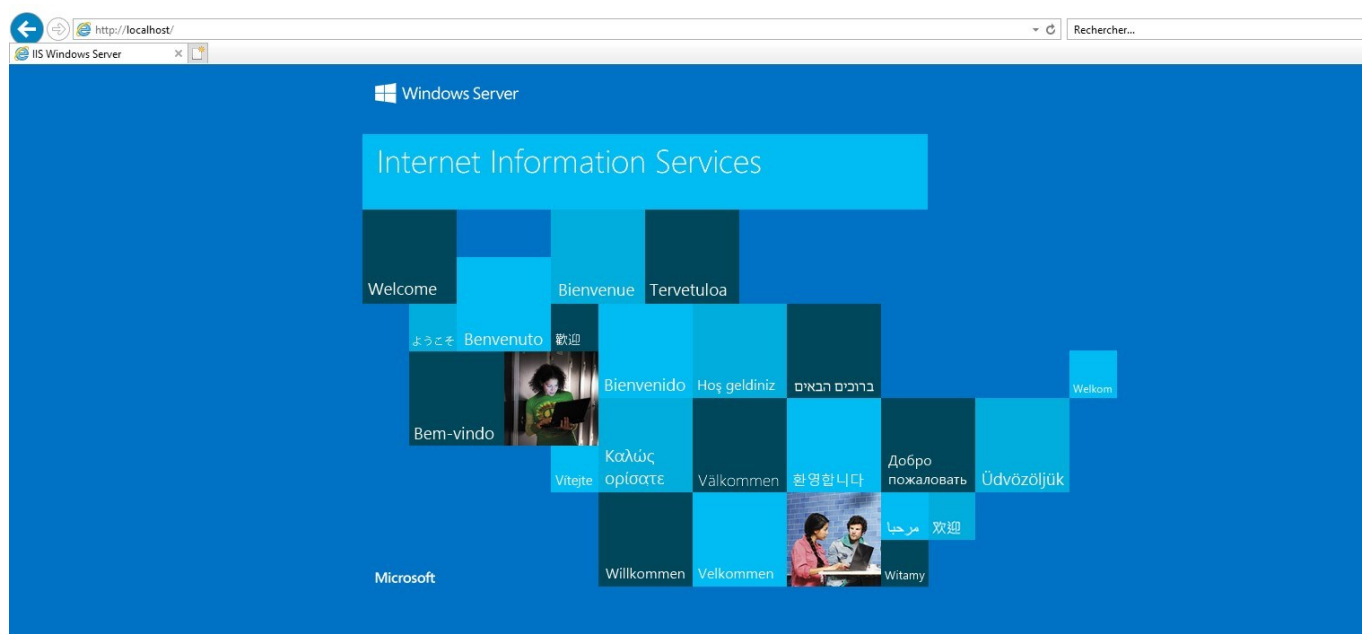
BTS 2022-2024

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" :

N Listener Configuration — □ ×

Nagios Cross-Platform Agent (NCPA)
Windows Version - 2.4.0 **Nagios**[®]

Set configuration for API access, active checks via `check_ncpa.py`, and connection settings for the web GUI. These options are related to the NCPA listener service.

API Configuration

Token

The token used for API access, active checks, and logging into the web GUI.

Listener Configuration

Bind IP

Bind Port

Advanced Listener Configuration

SSL Version

Log Level

Nagios Enterprises, LLC

N NCPA Setup — □ ×

Choose Users
Choose for which users you want to install NCPA. **Nagios**[®]

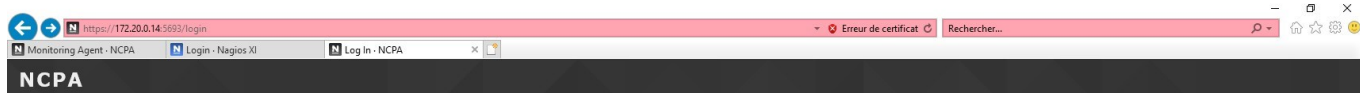
Select whether you want to install NCPA for yourself only or for all users of this computer. Click Next to continue.

Install for anyone using this computer

Install just for me

Nagios Enterprises, LLC

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 :

```
.1.5.4
iso.3.6.1.2.1.88.1.4.3.1.1.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.97.
105.108.117.114.101 = OID: iso.3.6.1.2.1.88.2.0.4
iso.3.6.1.2.1.88.1.4.3.1.1.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.97.
108.108.105.110.103 = OID: iso.3.6.1.2.1.88.2.0.3
iso.3.6.1.2.1.88.1.4.3.1.1.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.105
.114.101.100 = OID: iso.3.6.1.2.1.88.2.0.1
iso.3.6.1.2.1.88.1.4.3.1.1.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.82.105
.115.105.110.103 = OID: iso.3.6.1.2.1.88.2.0.2
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.108.105.110.107.68.111.119.110 = STRING: "_sn
mpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.108.105.110.107.85.112 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.97.
105.108.117.114.101 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.97.
108.108.105.110.103 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.105
.114.101.100 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.2.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.82.105
.115.105.110.103 = STRING: "_snmpd"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.108.105.110.107.68.111.119.110 = STRING: "_li
nkUpDown"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.108.105.110.107.85.112 = STRING: "_linkUpDown
"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.97.
105.108.117.114.101 = STRING: "_triggerFail"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.97.
108.108.105.110.103 = STRING: "_triggerFire"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.70.105
.114.101.100 = STRING: "_triggerFire"
iso.3.6.1.2.1.88.1.4.3.1.3.6.95.115.110.109.112.100.95.109.116.101.84.114.105.103.103.101.114.82.105
.115.105.110.103 = STRING: "_triggerFire"
iso.3.6.1.2.1.92.1.1.1.0 = Gauge32: 1000
iso.3.6.1.2.1.92.1.1.2.0 = Gauge32: 1440
iso.3.6.1.2.1.92.1.2.1.0 = Counter32: 0
iso.3.6.1.2.1.92.1.2.2.0 = Counter32: 0
root@servubuntu:/# _
```

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---]
```

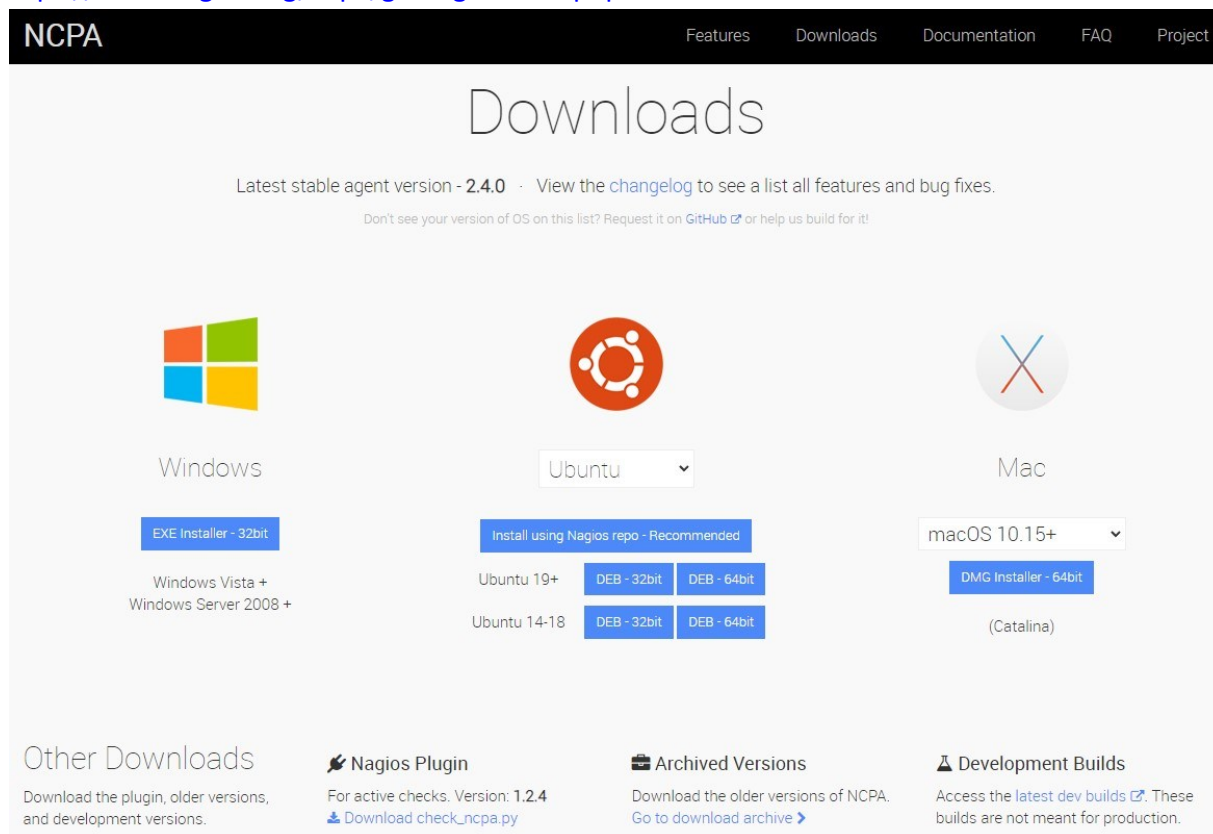
----- Ctrl + x > yes > Entrée

Installation de l'agent NCPA sur le serveur Ubuntu :

BTS 2022-2024

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
```

BTS 2022-2024

→ 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---]
```

BTS 2022-2024

```
# 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 :

BTS 2022-2024

Login

[Forgot your password?](#)

Nagios Products



Nagios XI
Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house applications, services, and systems.

Contact Us

Looking for more information? Have a technical or sales question?

Sales Phone: (651) 204-9102 Email: sales@nagios.com	Web Nagios Website Nagios Exchange	Support Support Forum Knowledgebase
--	---	--

Détection de machines 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 Windows :

The screenshot shows the Nagios XI interface. The top navigation bar includes Home, Views, Dashboards, Reports, Configure, Tools, Help, and Admin. A notification banner 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 main content area is titled "Configuration Wizards - Select a Wizard" and includes a search bar with "snmp" entered. Below the search bar, there are four wizard options: "Linux SNMP" (Monitor a Linux workstation or server using SNMP), "Windows SNMP" (Monitor a Microsoft® Windows workstation or server using SNMP), "SNMP" (Monitor a device, service, or application using SNMP), and "SNMP Trap" (Monitor SNMP Traps). A "Get More Wizards" button is also visible.

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 :

- ▼ **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: Windows SNMP - Step 1

Windows Machine Information

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

Operating System:

SNMP Settings

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

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

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

SNMP Version Settings

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

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 :

- ▼ **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

Windows SNMP Monitoring Wizard

✔️ Configuration applied successfully.

Your configuration changes have been successfully applied and the monitoring engine was restarted.

Configuration Request Successful

Other Options:

- [View status details for 172.20.0.14](#)
- [View the latest configuration snapshots](#)

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 :

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.

Host Status

All hosts

Host Status Summary

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

Last Updated: 2022-02-18 19:20:06

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
16	0	0	1	0
Unhandled		Problems	All	
1		1		17

Last Updated: 2022-02-18 19:20:06

Showing 1-2 of 2 total records

Host	Status	Duration	Attempt	Last Check	Status Information
172.20.0.14	Up	4m 27s	1/5	2022-02-18 19:18:23	OK - 172.20.0.14 rta 0.340ms lost 0%
localhost	Up	29d 7h 48m 27s	1/10	2022-02-18 19:19:13	OK - 127.0.0.1 rta 0.014ms lost 0%

Last Updated: 2022-02-18 19:20:06

Nagios XI 5.8.7 • Check for Updates

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.

Core Config Manager

Hosts

Search

[+ Add New](#) *Displaying 1-4 of 4 results*

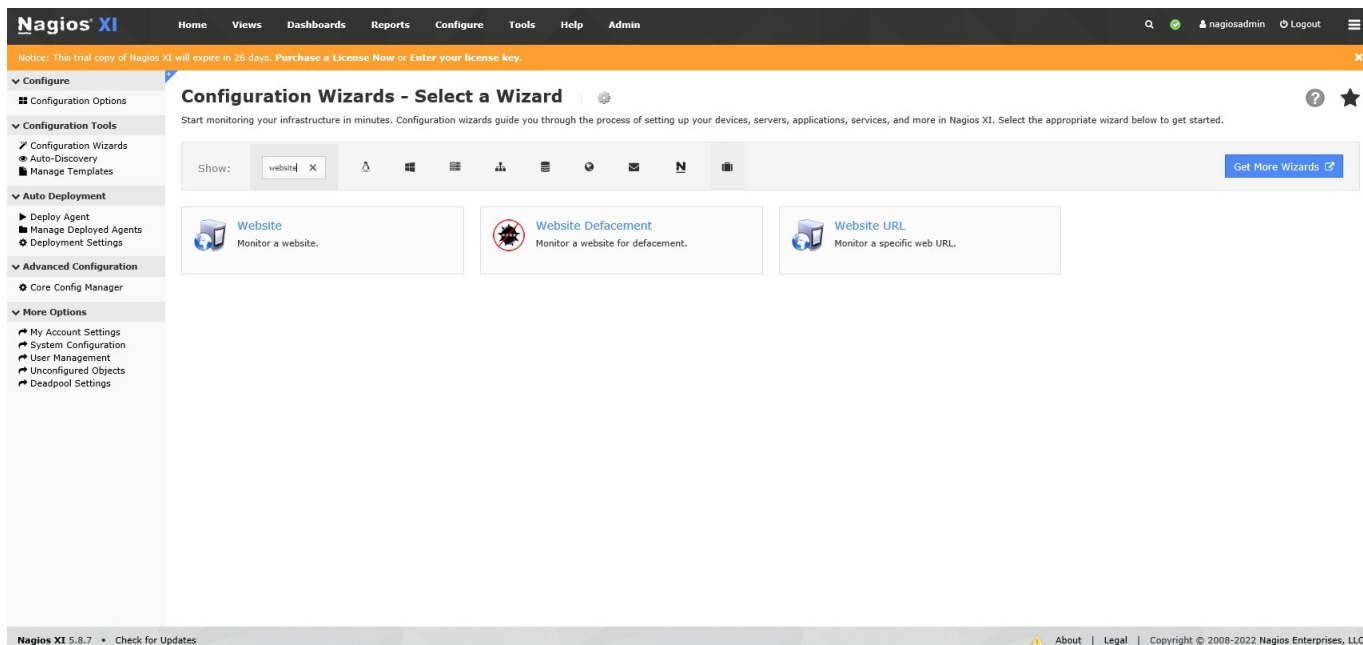
<input type="checkbox"/> Host Name	Alias	I Active	I Status	Actions	I ID
<input type="checkbox"/> 172.20.0.14		Yes	Applied	  	2
<input type="checkbox"/> 172.20.0.52		Yes	Applied	  	3
<input type="checkbox"/> localhost	localhost	Yes	Applied	  	1
<input type="checkbox"/> winner2019		Yes	Applied	  	4

[+ Add New](#) [Apply Configuration](#) Results per page 15

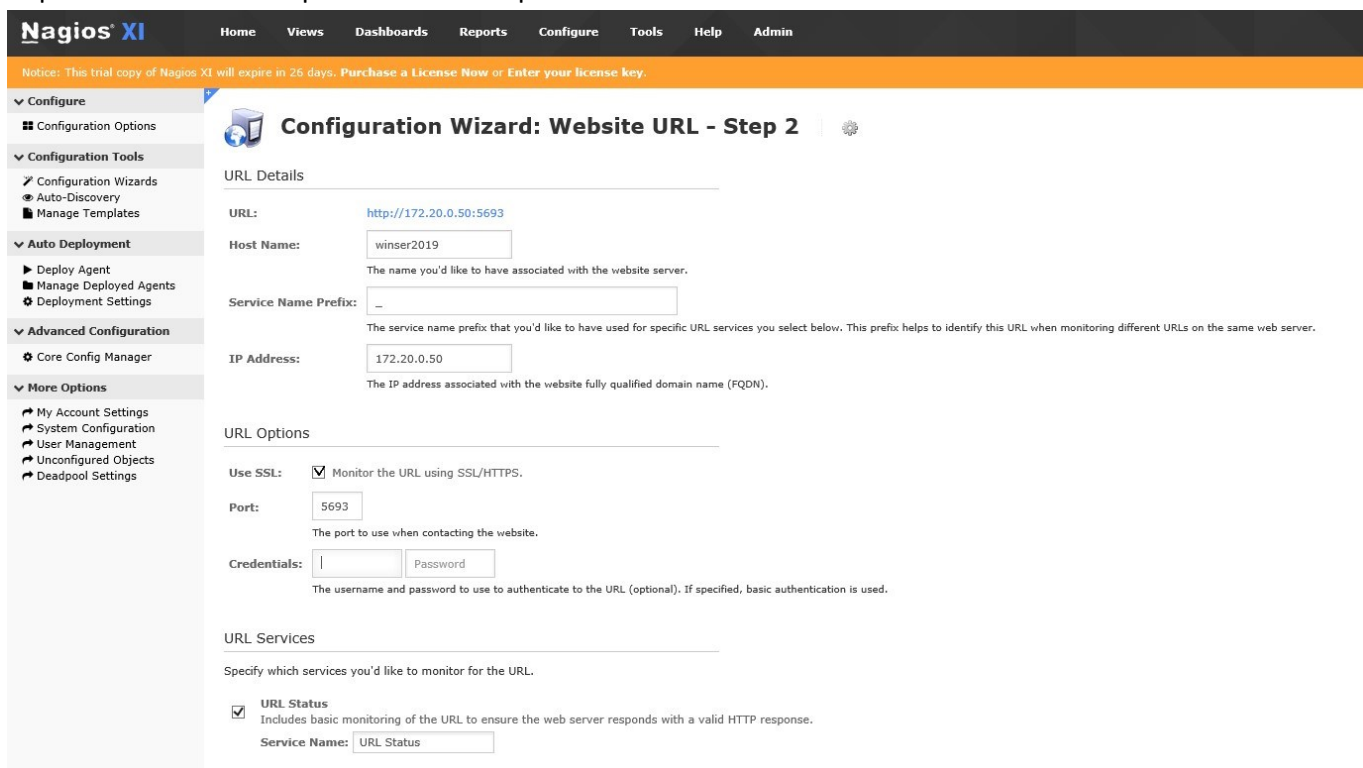
Nagios XI 5.8.7 • Check for Updates

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 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 :

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:	<input type="checkbox"/> New hosts only <input type="checkbox"/> 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" :

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: [masked]

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" :

- ▼ **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".