Nagios

Emetteur(s) : Saviard Matthieu

Destinataire(s) : Jury BTS SIO

Date : 18/02/2024

Objet : Mise en place d'un serveur NAGIOS au sein de mon infrastructure

Nagios est un système de surveillance open source utilisé pour superviser en temps réel la disponibilité, les performances et l'état des éléments d'un environnement informatique, tels que les réseaux, les systèmes et les applications.

Il utilise des plugins pour effectuer des vérifications spécifiques et envoie des alertes en cas de détection d'anomalies, permettant aux administrateurs de réagir rapidement. Nagios offre une interface web facile d'utilisation, prend en charge la personnalisation des plugins, la planification des tâches et peut être étendu grâce à une communauté active.

Nagios XI est une version améliorée avec des fonctionnalités avancées.

1. Prérequis

Pour réaliser notre serveur Nagios, voici donc nos prérequis →

NAGIOS			
RAM	OS	HARD DRIVE	NECESSITE
2GB	Debian 12	30GB	Routeur
			DNS

Voici la configuration reseau :

CARTE RESEAUX	
ENS33	192.168.110.10
ENS160	NAT

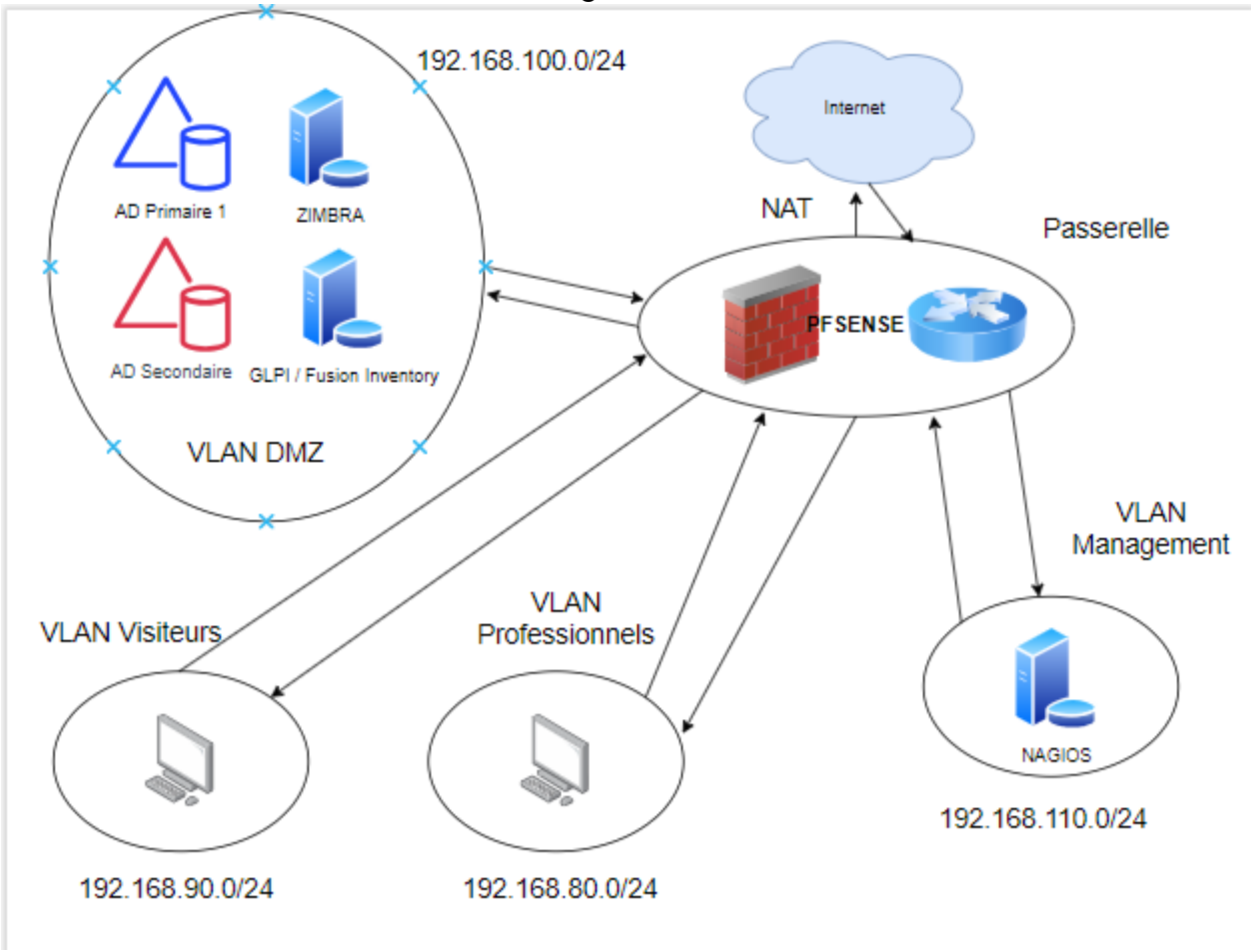
La carte NAT sera retirée après l'installation du service Nagios

Nagios est utilisé principalement via son interface web. Quand les utilisateurs sont connectés, ils peuvent accéder au tableau de bord principal, qui montre les statuts des équipements réseau, des services et des applications en surveillant. L'interface permet de visualiser rapidement l'état opérationnel de chaque élément, que ce soit en termes de

disponibilité, de performances ou d'éventuelles erreurs, grâce à des codes couleur faciles à comprendre.

Les sections dédiées aux "hôtes" et aux "services" offrent des détails spécifiques, des graphiques de performance et un historique des événements. Cette interface offre également des fonctionnalités de configuration, de filtrage, de recherche et de gestion des notifications, ce qui rend la surveillance, la personnalisation et la réaction rapide aux incidents plus simples. Par conséquent, l'interface web de Nagios

Voici le schéma de notre infrastructure globale →



2. Préparation de la machine et installation de nagios

a. Configuration de la machine

On commence par mettre à jour la machine

```
root@nagios:~# root@nagios:~# apt update && upgrade
```

Ensuite on met à jour le fichier resolv.conf avec notre DNS et domaine

```
  GNU nano 5.4
domain localdomain
search localdomain
nameserver 192.168.32.2
```

On installe les outils DNS et la commande WGET ainsi que curl

```
root@nagios:~# apt install {wget,dnsutils,curl} -y
```

b. Installation de Nagios

On va commencer par installer Nagios sur notre machine →

curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh

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

Une fois installé, on va aller sur notre dashboard depuis une AD primaire via edge grâce à notre IP Nagios →

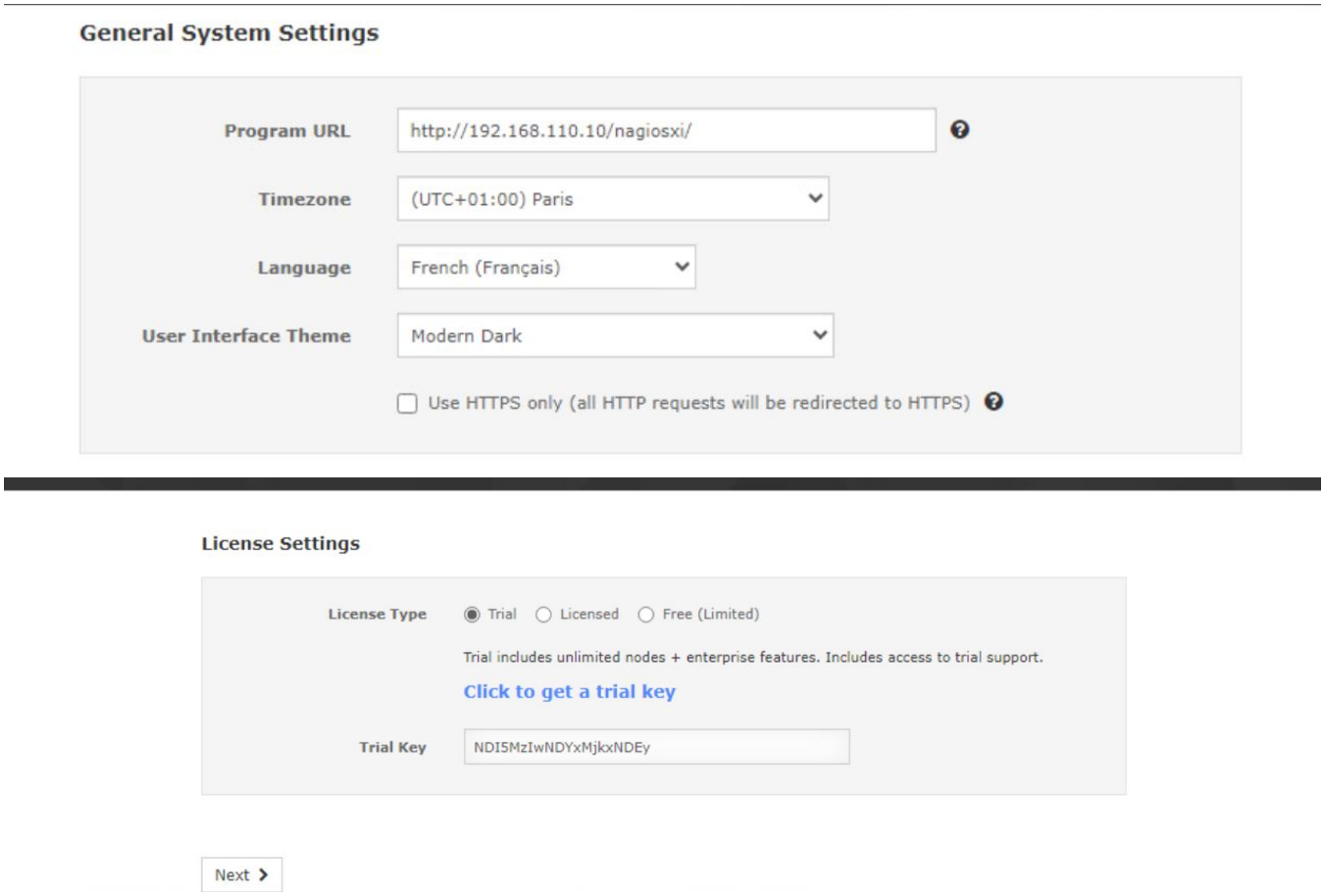
```
Nagios XI Installation Complete!
--------------------------------

You can access the Nagios XI web interface by visiting:
    http://192.168.32.154/nagiosxi/

root@nagios:~#
```

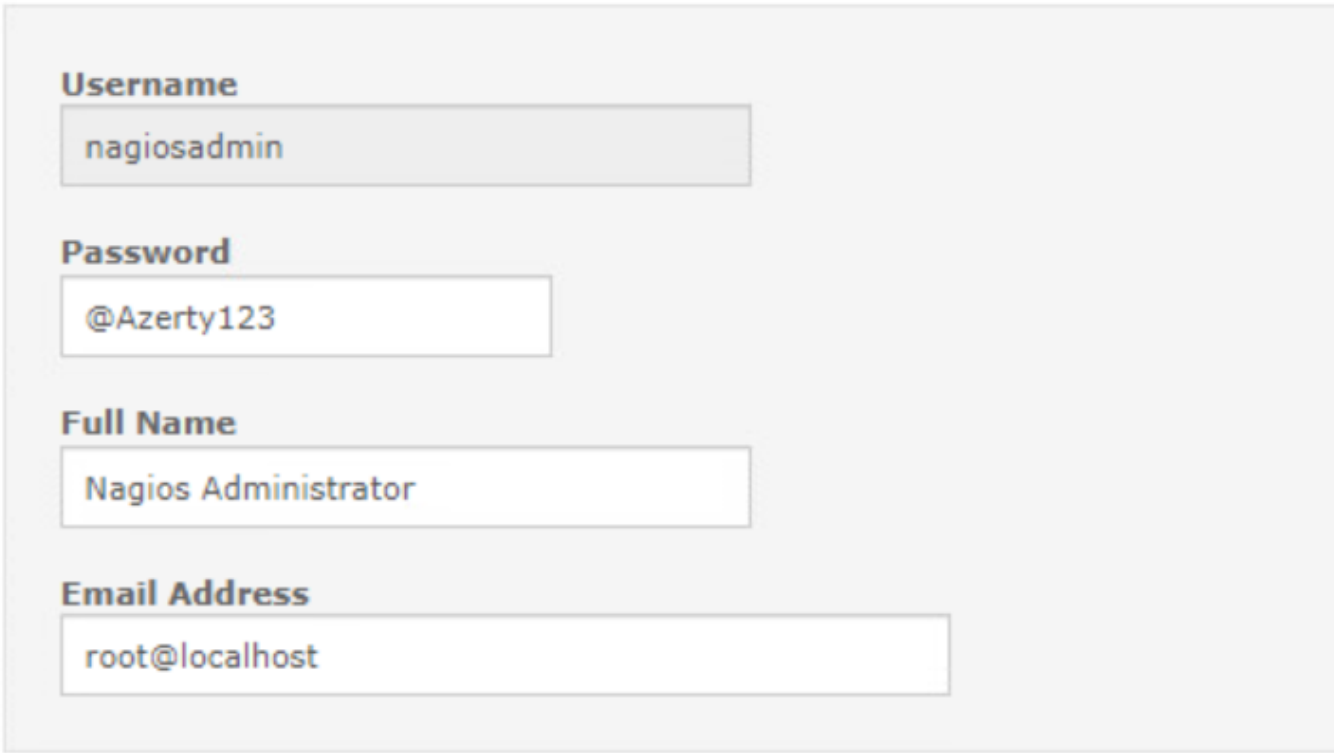
On va donc aller sur http://192.168.110.10 et retirer la carte NAT qu'on avait utilisé pour l'installation

On arrive sur une page qui va nous demander de configurer nagios et de rentrer une clé pour un trial

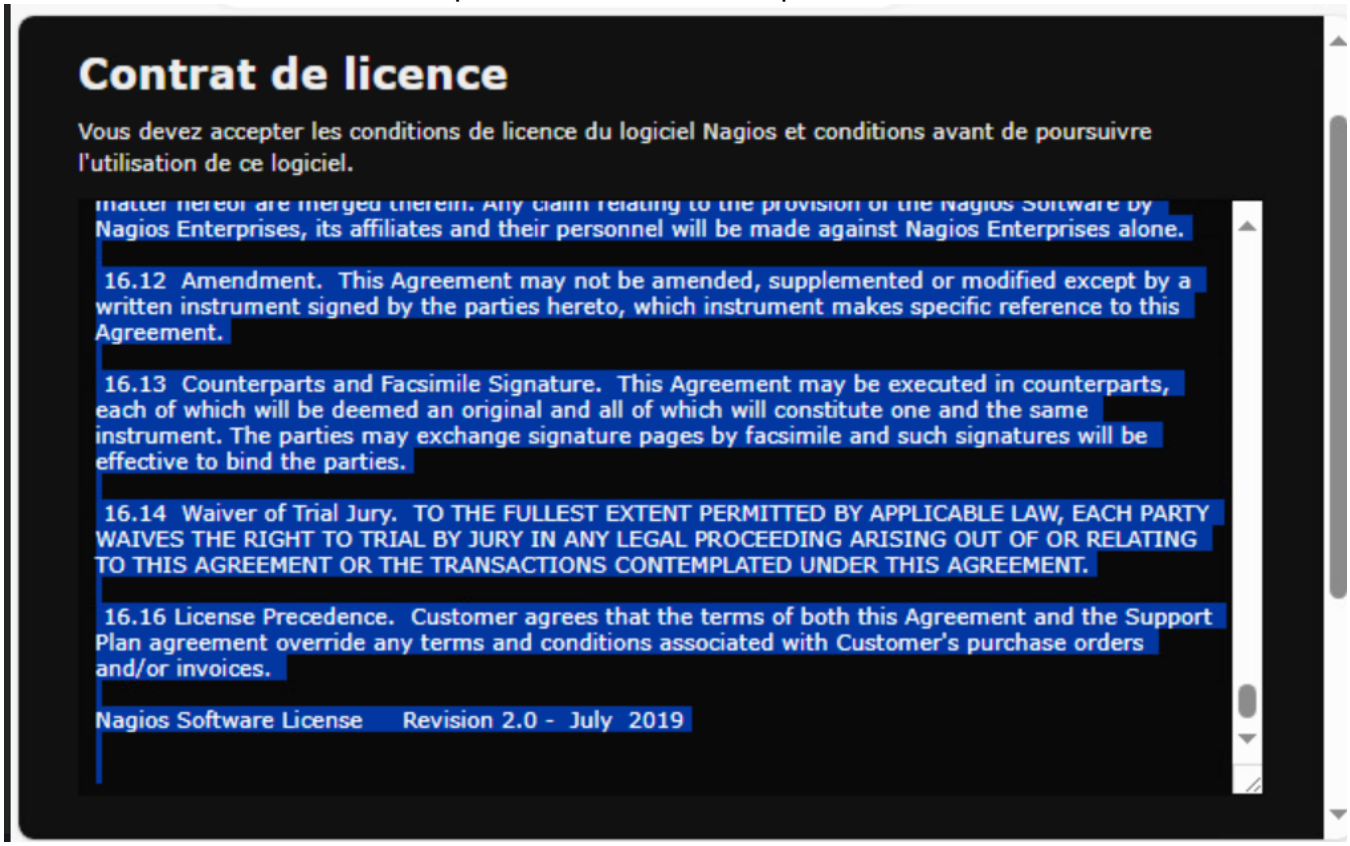


On change le mot de passe →

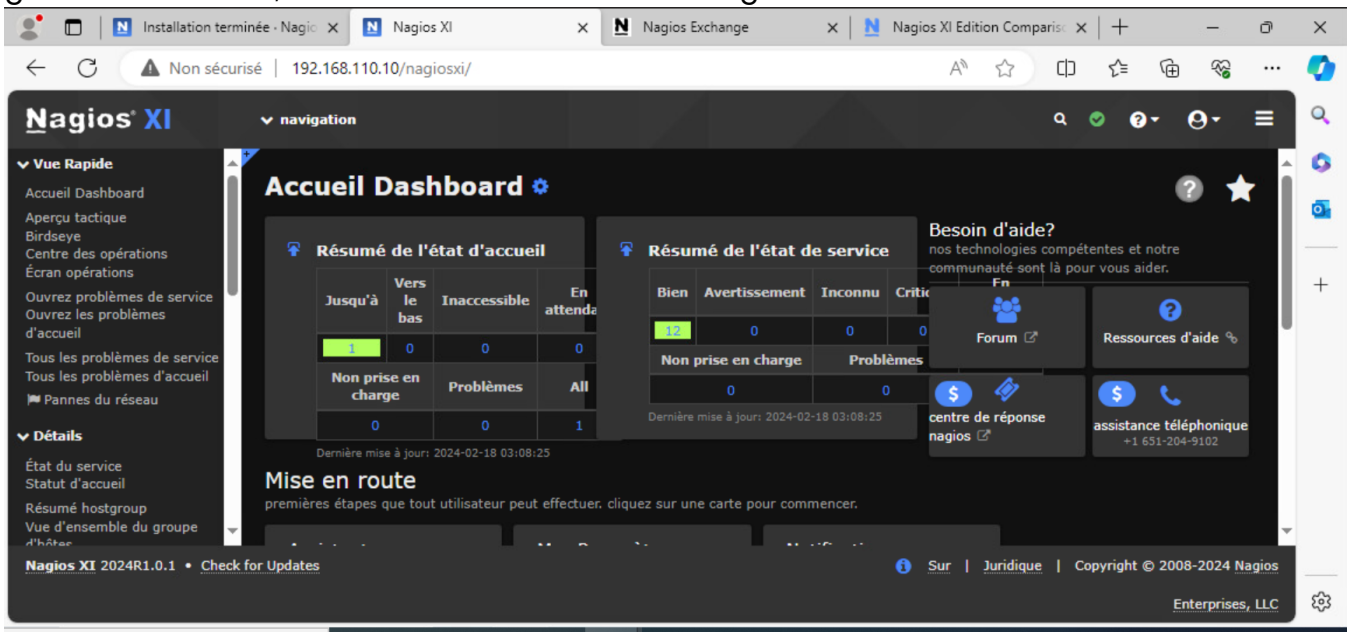
- ID : nagiosadmin
- MDP : @Azerty123



Ensuite, il se connecter et accepter le contrat → Pour pouvoir accéder au dashboard



On arrive sur le dashboard. Le dashboard sera le lieu ou nous pourrons faire la supervision de nos serveurs. En effet, dans le cadre de notre infrastructure, Nagios sera utilisé pour gérer nos serveurs, et évaluer si ils sont en surcharge ect.



On y trouve des fonctionnalités telles que :

Des fonctionnalités telles que :

- **Vue d'ensemble** : Statut global et graphiques récapitulatifs.
- **Hôtes et Services** : Liste et détails des hôtes et services surveillés.
- **Cartes** : Représentation visuelle de la topologie du réseau.
- **Événements** : Journal des événements, alertes et notifications.
- **Rapports** : Rapports prédéfinis et personnalisables.
- **Configuration** : Gestion des hôtes, services, politiques de notification.
- **Planification** : Horaires de vérification des hôtes et services.
- **Administration** : Gestion des utilisateurs, configuration système.
- **Tableau de bord personnel** : Personnalisation pour des besoins spécifiques.

3. Installation d'un agent Windows

Notre machine Nagios est finalement prête, nous allons donc pouvoir ensuite installer sur notre serveur AD primaire. En effet, on peut découper les agents nagios en deux parties :

- Les machines Windows
- Les machines Linux

Ici, nous allons commencer par installer sur notre serveur AD Windows

C'est lui qui va remonter les infos vers notre serveur Nagios →

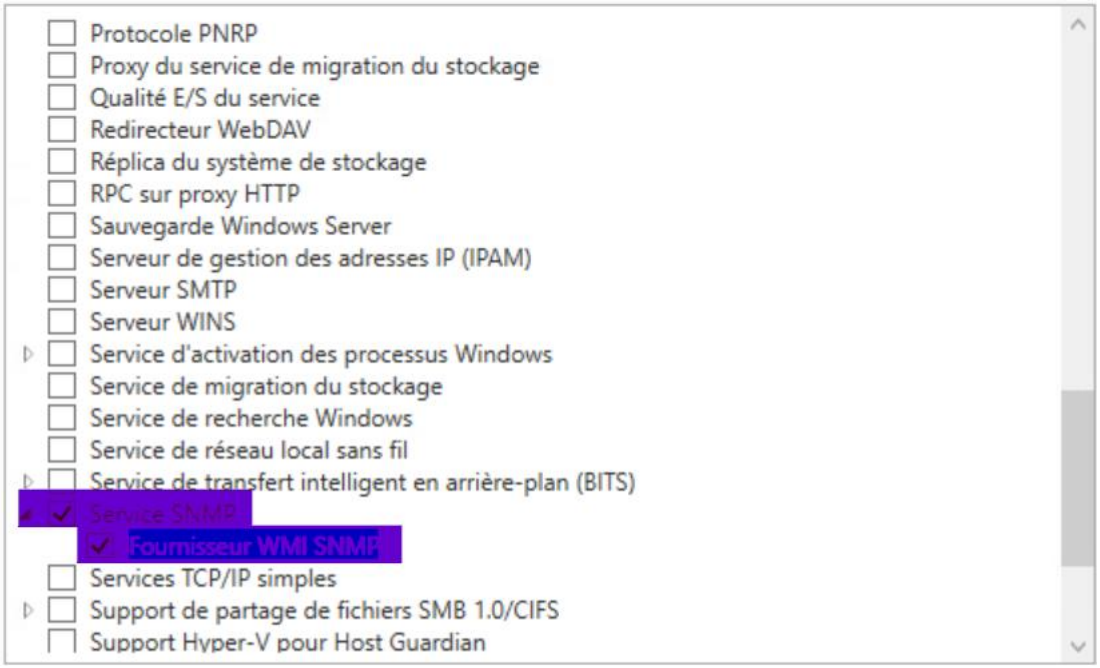
Un agent Nagios est un logiciel léger installé sur les systèmes à surveiller. Son rôle principal est de **collecter** des informations locales sur la santé et les performances du système, puis de les **transmettre** au serveur Nagios central pour une analyse approfondie. Voici un résumé de son utilité et de son fonctionnement :

➔ Ici on va installer un agent de type **NCPA** (Nagios Cross- Platform Agent)

Un agent NCPA :

Allons donc commencer en allant sur notre machine primaire →

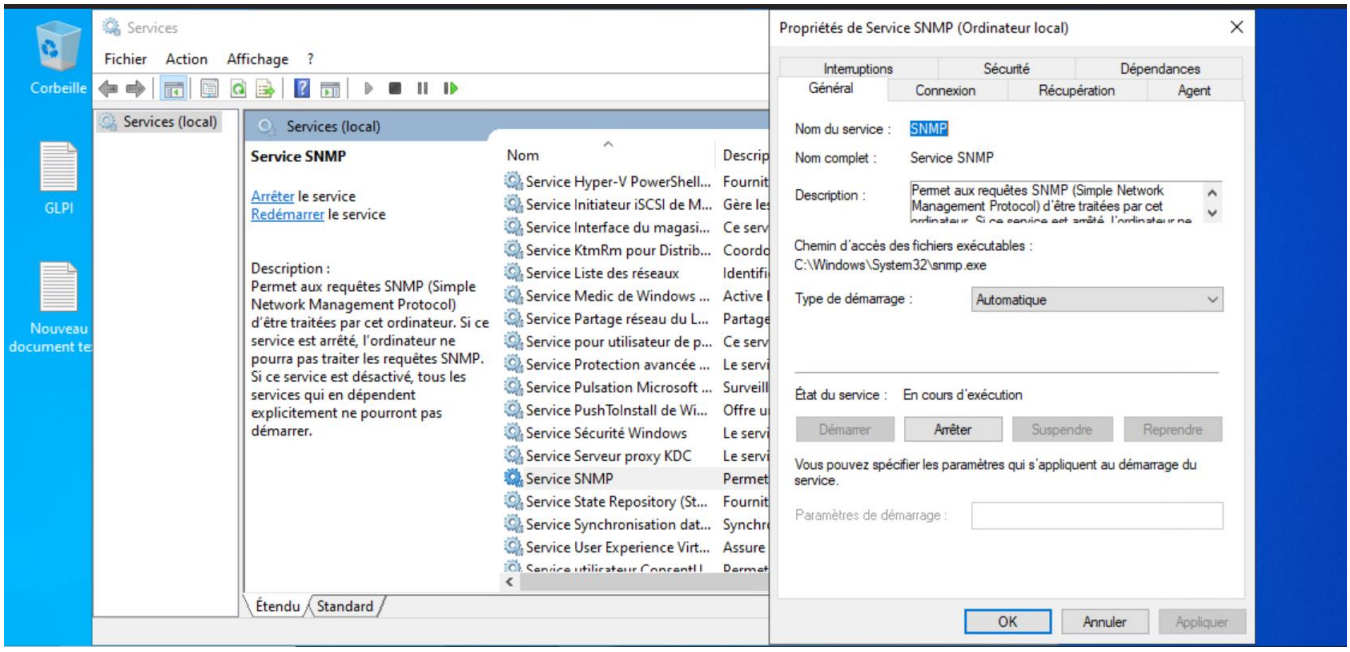
On va donc aller dans Gérer → « Ajouter des rôles et fonctionnalités » → « Installation basée sur un rôle une fonctionnalité » → Serveurs SNMP



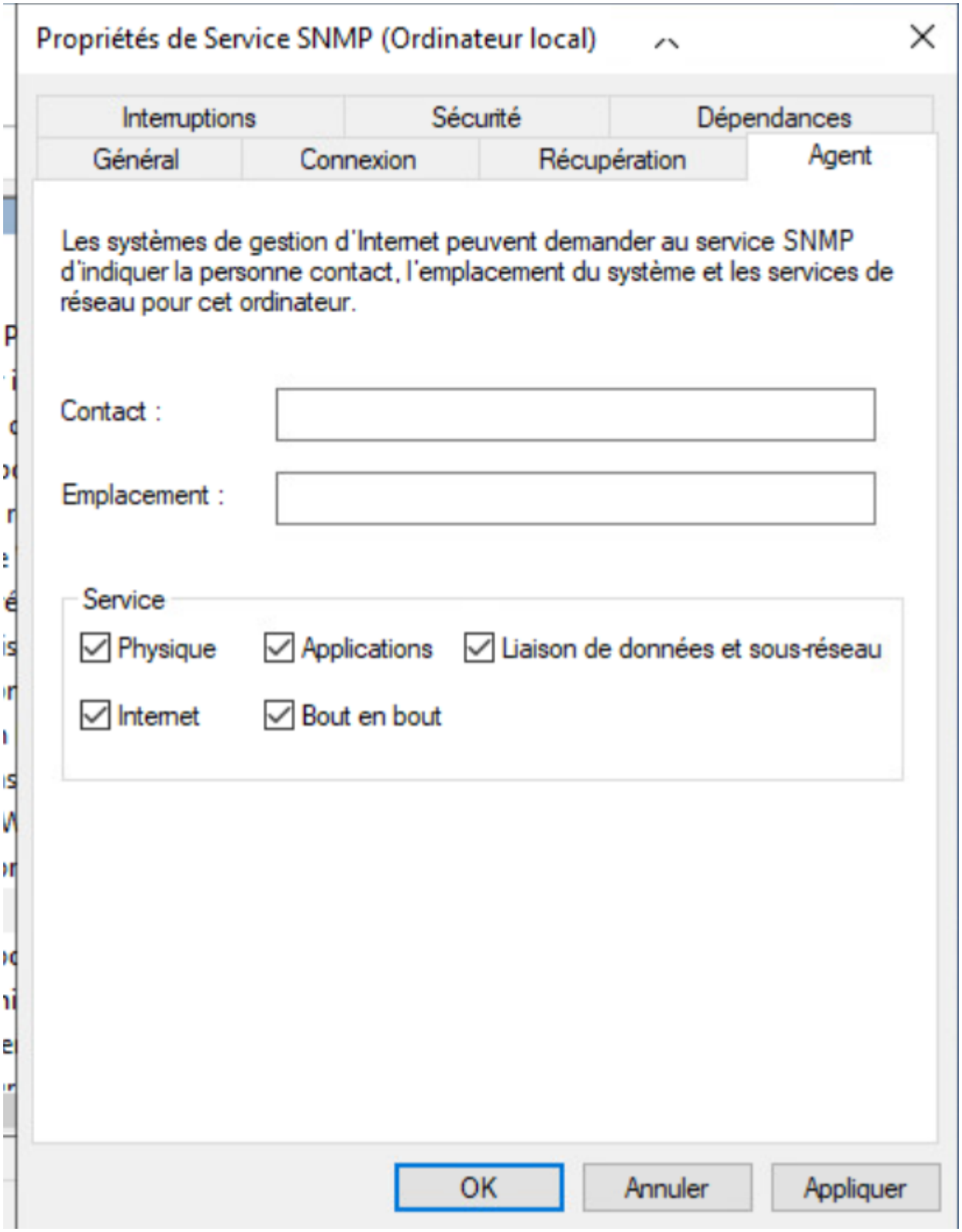
On va faire suivant → Puis installer ce service

En fait, quand on installe des Outils et fonctionnalités, c'est comme si on installait des services va cette icône →

On va donc aller sur notre service installé, sur notre machine. Taper « Services » dans la barre de recherche Windows et chercher → « Service SNMP »

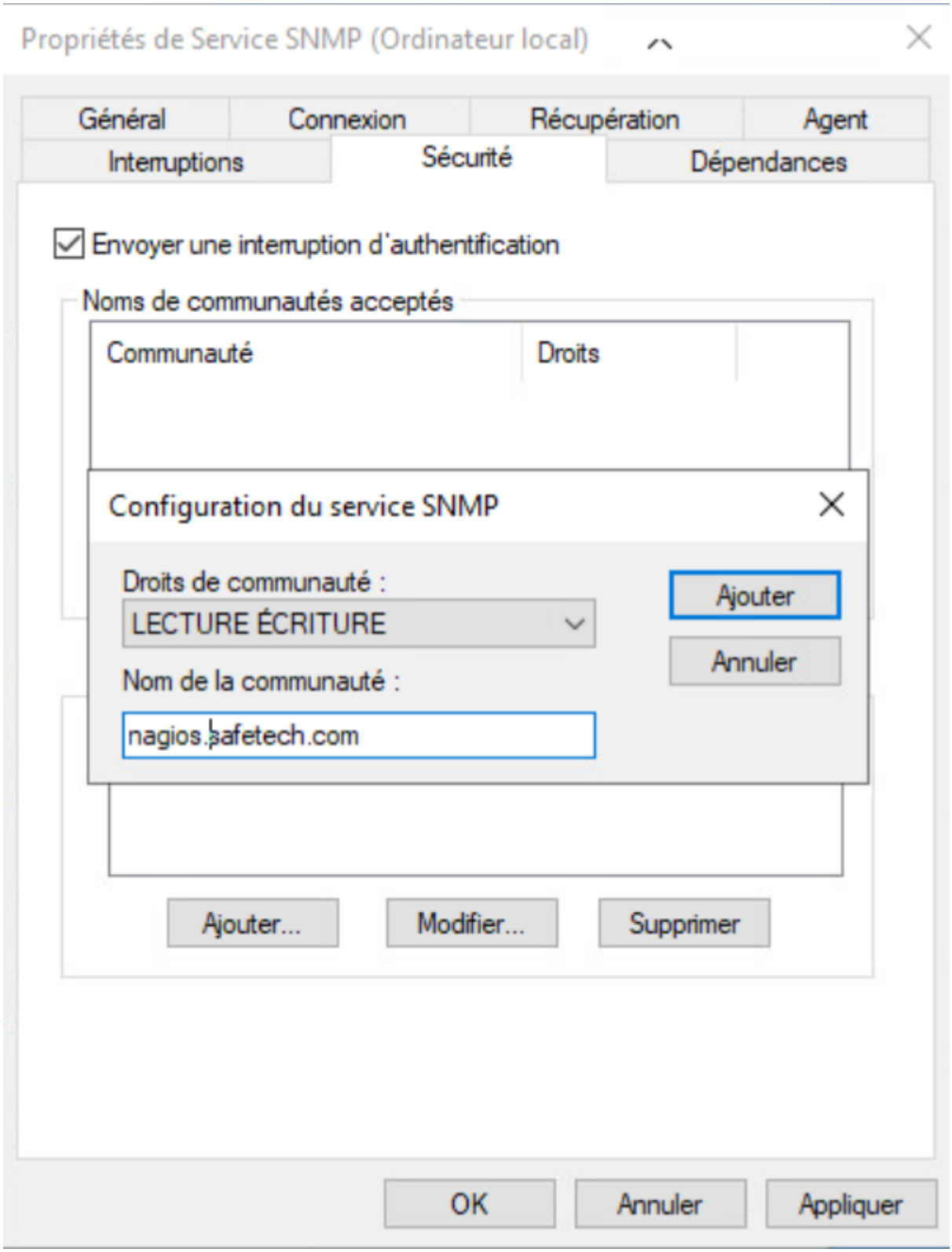


On va donc dans Propriétés → On va **cocher toutes les cases dans la rubrique Agent** →



Puis ensuite nous allons aller dans → « Sécurité »

- Dans l'onglet "Sécurité", commencez par ajouter votre communauté SNMP, dans cet exemple nommée "safetech.com", à la liste. Suivez ces étapes :
- Cliquez sur "Ajouter...".
- Définissez les droits et le nom de la communauté, par exemple, "safetech.com".

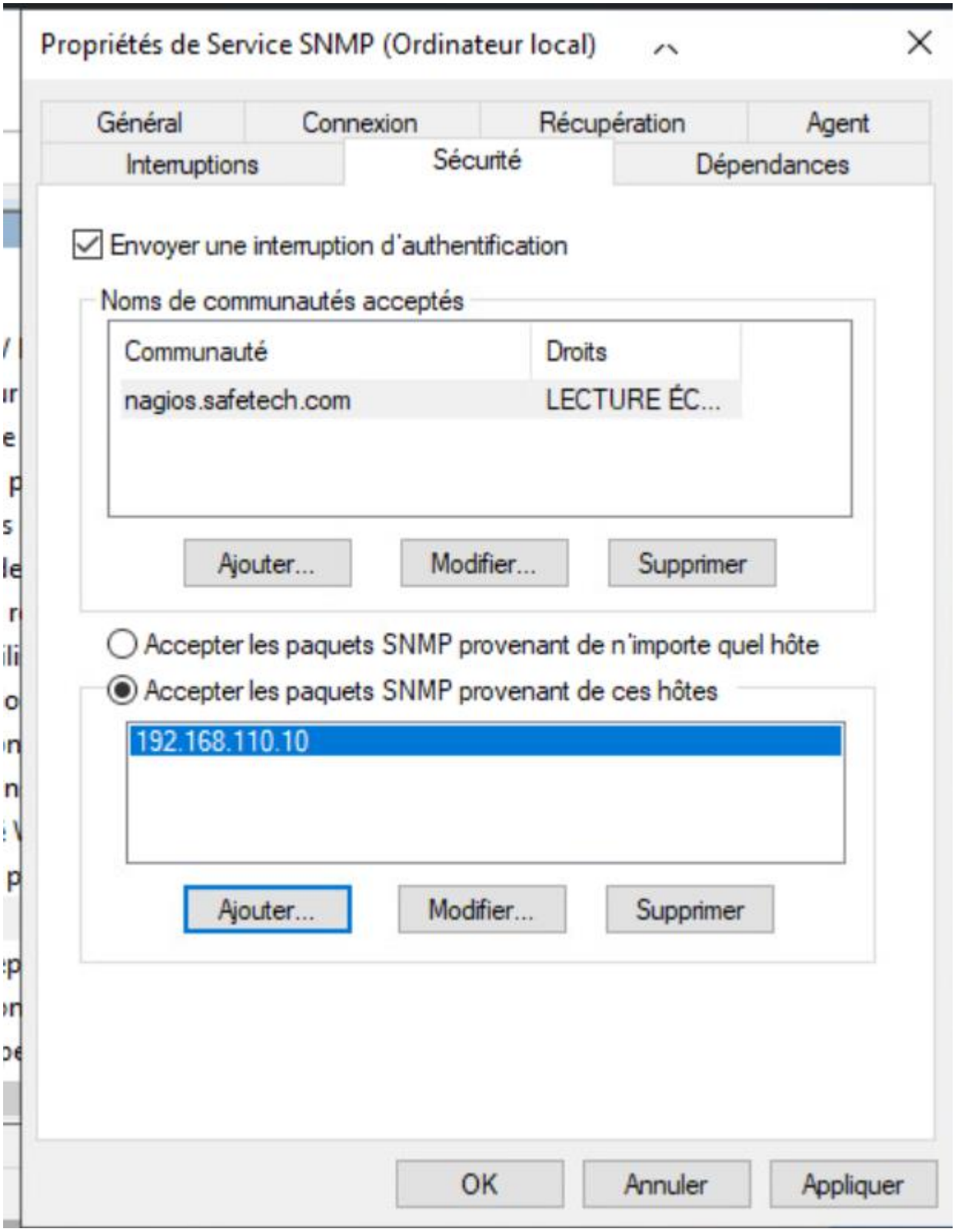


➔ Cochez l'option "Accepter les paquets SNMP provenant de ces hôtes".

Ensuite, ajustez la liste d'hôtes autorisés comme suit :

1) Retirer"localhost" de la liste si présente.

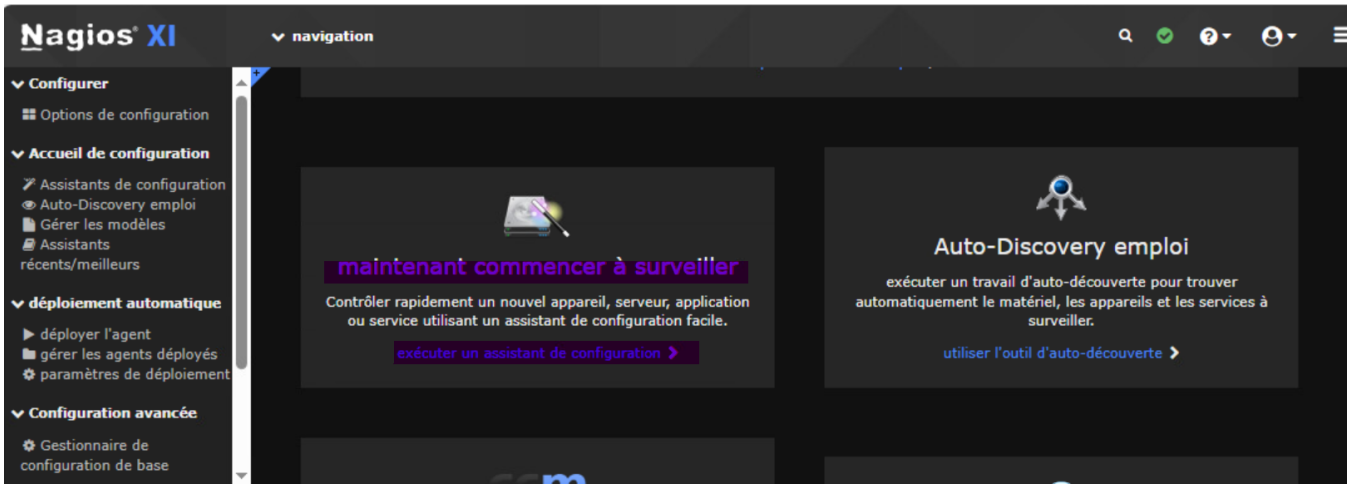
Ajoutez l'adresse IP du serveur Nagios dans les serveurs autorisés



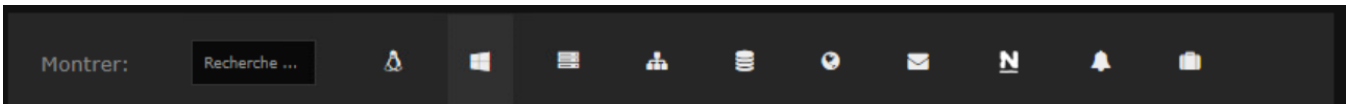
Ensuite on enregistre → Puis on retourne sur notre dashboard Nagios

Sur le dashboard aller dans configure → configuration wizard

On va cliquer sur cette icône et ensuite commencer à configurer notre premier agent →

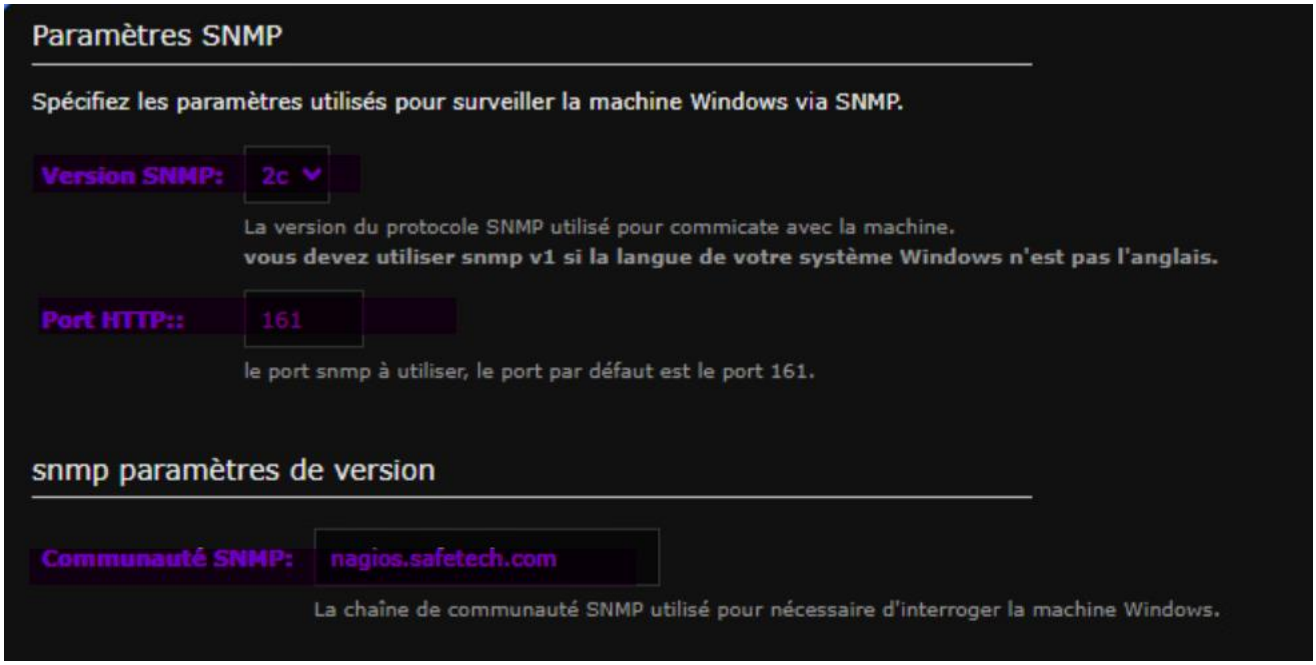


➔ On choisit Windows



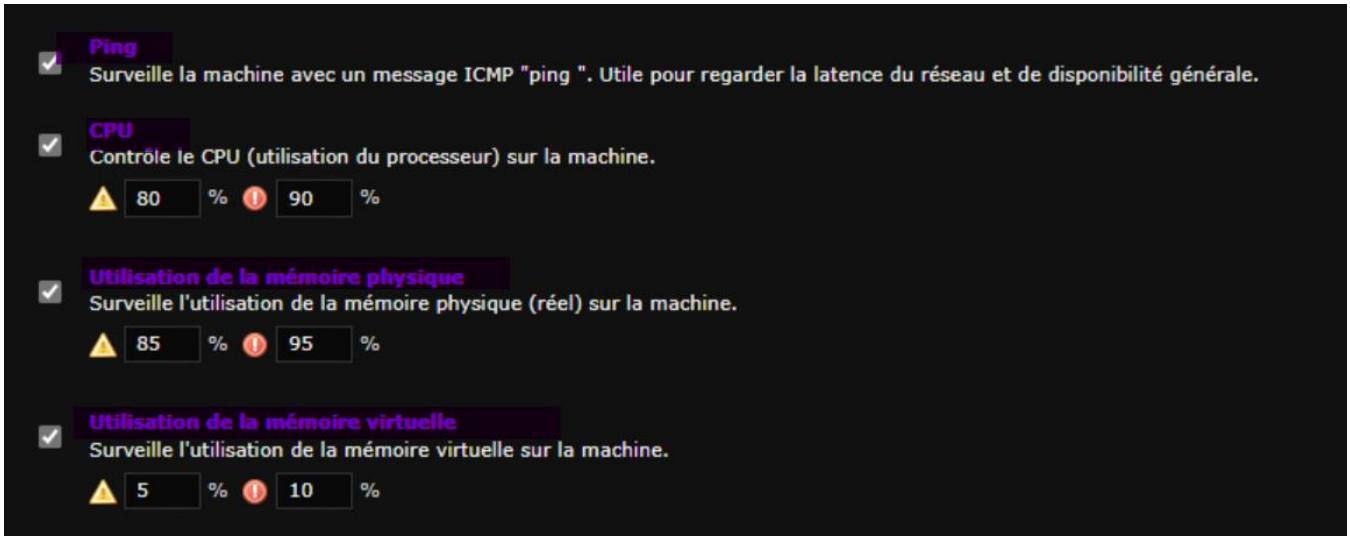
Et on cherche ensuite tout en bas « Windows SNMP »

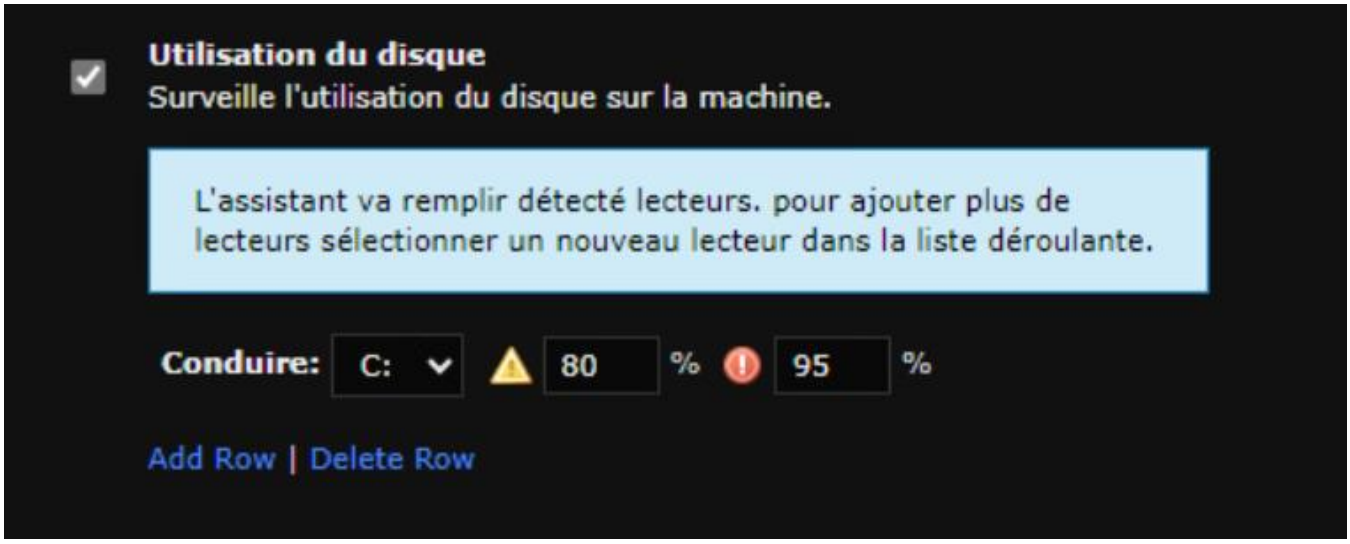
➔ On va donc ensuite rentrer les paramètres de notre machine AD primaire qu'on veut superviser



Faire « Next » et ensuite on va choisir les éléments lesquels ont veut superviser →

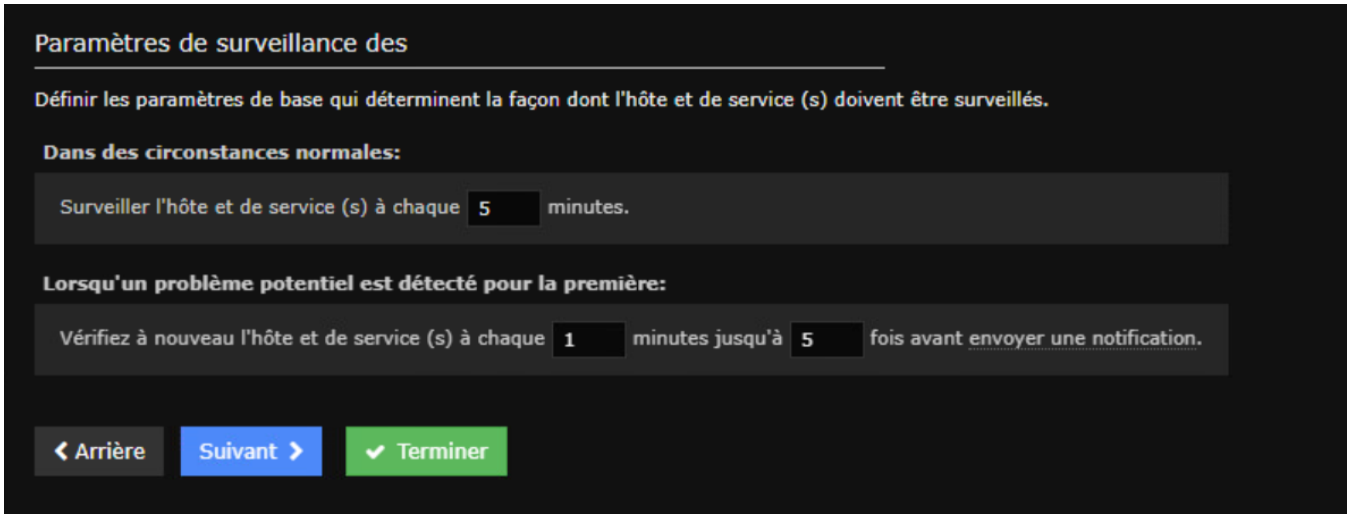
Voici la liste des éléments que nous pouvons surveiller →





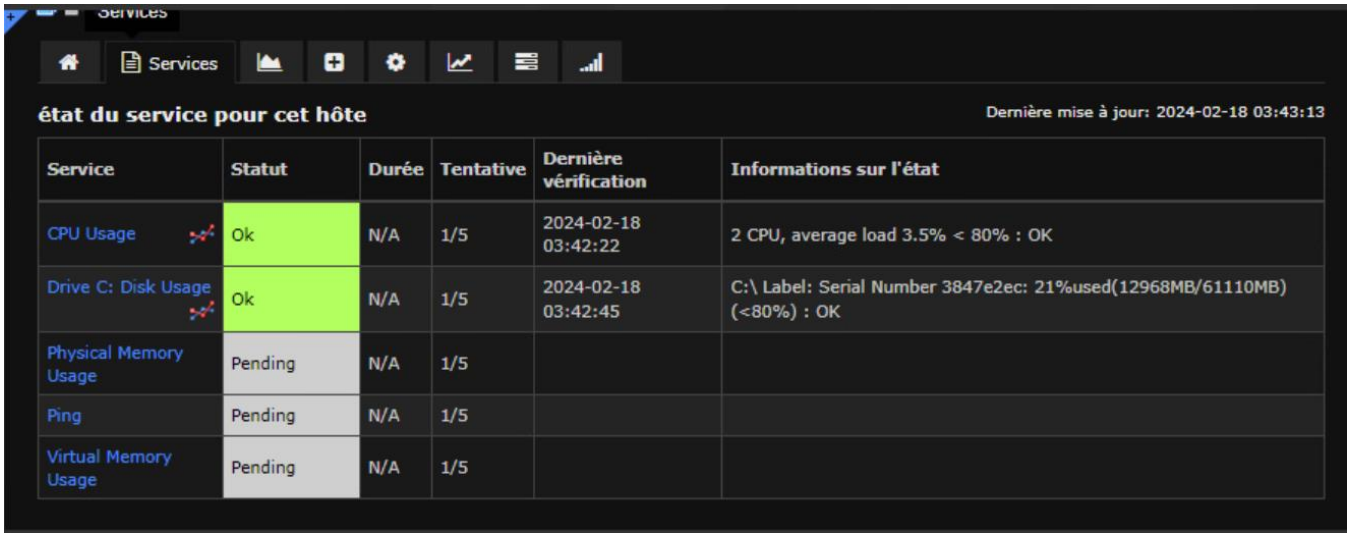
➔ On fait suivant

On laisse la configuration de base, avec l'agent qui enverra son statut toutes les 5 minutes



On fait « terminé »

On peut ensuite voir sur nos dashboards nos infos remonter →



On va faire la même sur notre autre serveur Windows AD Secondaire →

Au final, pour note infrastructure nous obtenons les machines suivantes →

4. Installation d'un agent Linux

On va donc installer un agent GLPI sur une de nos machines Linux → Nous allons tout d'abord commencer par notre serveur Ubuntu Zimbra qui est une application critique pour notre infrastructure →

Comme pour Windows, nous allons devoir installer le service SNMP →

```
root@zimbra:~# apt install snmpd -y_
```

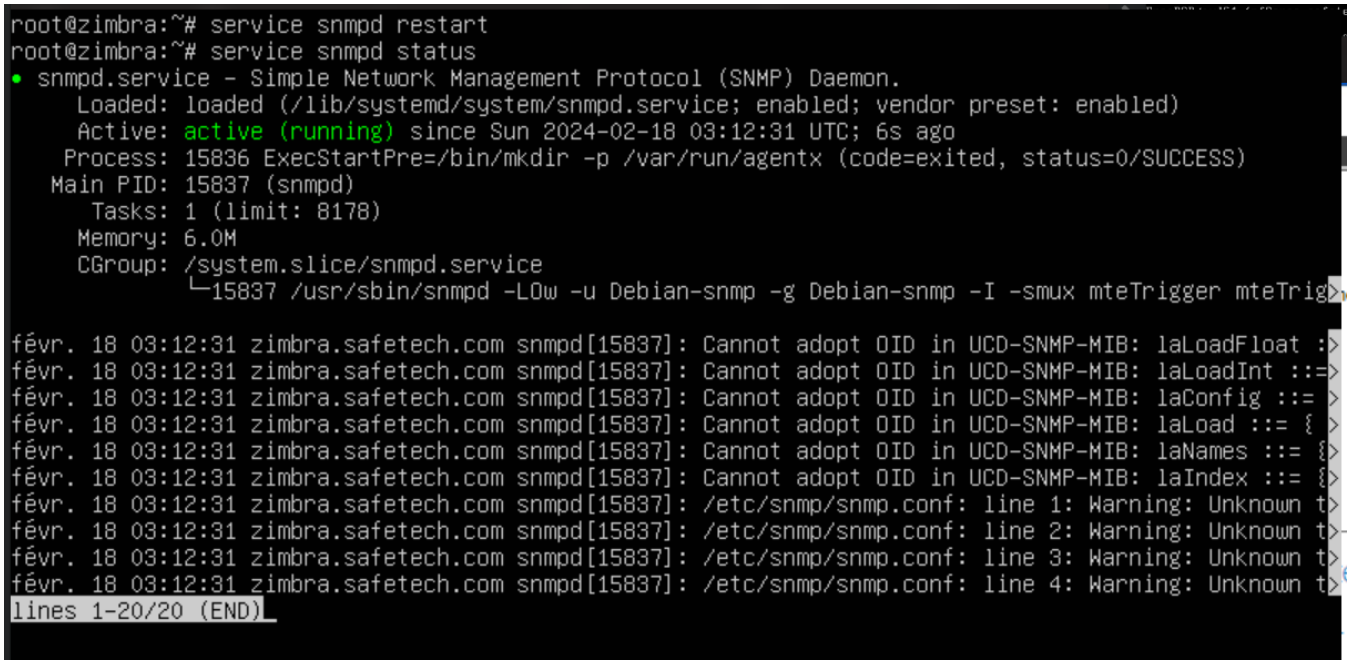
On va supprimer le contenu du fichier de configuration →

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

Et on va ensuite le remplir de cette façon →

```
  GNU nano 4.8
sysLocation nagios.safetech.com
sysContact root<root@safetech.com>
agentaddress udp:161,udp:[::1]:161
rocommunity nagios.sitka.local default
```

Puis on restart le service →



➔ On vérifie que ca marche bien avec la commande suivante :

5. Installation et configuration de NCAP