TP Supervision

Sommaire

I. Introduction *2*

II. Installation et premiers pas (SNMP) *2*

1. Installation et configuration 2
2. Test de l'utilitaire tkmib 7

III. Supervision *8*

IV. Centreon *9*

1. Installation 9
2. Présentation de l'interface 13
3. Mise en place Centreon Windows 15
4. Mise en place de Centreon Linux 28
5. Mise en place de Centreon sur Switch Cisco 33
6. Mise en place de Centreon sur Imprimante 38
7. Création d'un dashboard 40
8. Création d'un utilisateur et modification du mot de passe admin 45

I. Introduction

SNMP (Simple Network Management Protocol) permet à l'administrateur réseau à distance d'obtenir des informations et de modifier divers équipements. C'est un protocole conçu pour unifier et simplifier la gestion des équipements et logiciels, mais il n'est pas simple ! A réserver pour les grands réseaux.

SNMP v3 : 1999

Chaque équipement ou logiciel interrogeable dispose d'un serveur (agent) qui écoute sur le port UDP 161. Tous les paramètres disponibles sont stockés dans une MIB (Management Information Base) -> Registre Windows.

Exemple MIB-II : objet sys contact

Chaine contenant le nom de l'administrateur

Les OID (Object Identifiers) sont des paires unique clé-valeur

Le protocole permet 4 types de messages :

- Get pour récupérer un objet précis
- Get next pour l'objet suivant
- Set pour modifier

II. Installation et premiers pas (SNMP)

1. Installation et configuration

sudo apt update

sudo apt upgrade

sudo apt install snmp snmpd snmp-mibs-downloader

sudo service snmpd start

sudo service snmpd enable

Test : snmpwalk -v 2c -c public localhost

⇨ On voit défiler toute la MIB du localhost.

On peut restreindre sur une partie :

snmpwalk -v 2c -c public localhost system

Sur quel système tourne la machine ?

La machine tourne sur Debian 13 :

```
root@debian:/home/rdubois# snmpwalk -v 2c -c public localhost system
SNMPv2-MIB::sysDescr.0 = STRING: Linux debian 6.12.57+deb13-arm64 #1 SMP Debian 6.12.57-1 (2025-11-05) aarch64
```

Quel est le fichier de configuration ?

Le fichier de configuration principal de l'agent est dans ce répertoire :

/etc/snmp/snmpd.conf

Pour récupérer un objet précis :

snmpget -v 2c -c public localhost sysContact.0

```
root@debian:/home/rdubois# snmpget -v 2c -c public localhost sysContact.0
SNMPv2-MIB::sysContact.0 = STRING: Me <me@example.org>
root@debian:/home/rdubois#
```

Test avec l'argument -On :

```
root@debian:/home/rdubois# snmpget -v 2c -c public localhost -On sysContact.0
.1.3.6.1.2.1.1.4.0 = STRING: Me <me@example.org>
root@debian:/home/rdubois#
```

Le résultat obtenu avec l'argument -On correspond à l'OID (Object Identifier) affiché sous sa forme numérique brute.

Comment faire pour récupérer l'uptime de la machine ?

La commande pour récupérer l'uptime est la suivante :

snmpget -v 2c -c public localhost sysUpTimeInstance

```
root@debian:/home/rdubois# snmpget -v 2c -c public localhost sysUpTimeInstance
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (59088) 0:09:50.88
root@debian:/home/rdubois# snmpget -v 2c -c public localhost sysUpTimeInstance
```

La mémoire ?

La commande pour récupérer la mémoire (RAM) totale du système est la suivante :

snmpget -v 2c -c public localhost UCD-SNMP-MIB::memTotalReal.0

```
root@Ubuntu:/home/vboxuser# snmpget -v 2c -c public 192.168.88.5 UCD-SNMP-MIB::memTotalReal.0
UCD-SNMP-MIB::memTotalReal.0 = INTEGER: 8129292 kB
```

Création d'une communauté pour limiter l'accès :

```
rocommunity communaute1 192.168.88.0/24 -V systemonly
```

Ici, nous autorisons l'accès aux machines dans le réseau « 192.168.88.0/24 ».

- Sauvegarder le fichier de conf :

sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.bak

```
root@debian:/home/rdubois# cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.bak
root@debian:/home/rdubois#
```

- Éditer et rajouter la ligne :

rocommunity communaute1 192.168.X.0/24

rdubois@debian: ~

```
 GNU nano 8.4                                  /etc/snmp/snmpd.conf
#   snmp agent.

# Views
#   arguments viewname included [oid]

#  system + hrSystem groups only
view   systemonly  included   .1.3.6.1.2.1.1
view   systemonly  included   .1.3.6.1.2.1.25.1


# rocommunity: a SNMPv1/SNMPv2c read-only access community name
#   arguments:  community [default|hostname|network/bits] [oid | -V view]

# Read-only access to everyone to the systemonly view
rocommunity  public default -V systemonly
rocommunity6 public default -V systemonly
rocommunity communaute1 192.168.X.0/24
```

- Redémarrer le serveur et tester :

systemctl restart snmpd

```
[sudo] password for vboxuser:
root@Ubuntu:/home/vboxuser# systemctl restart snmpd
Warning: The unit file, source configuration file or drop-ins of snmpd.service changed on disk. Run 'systemctl daemon-reload' to reload units.
root@Ubuntu:/home/vboxuser#
```

snmpget -v 2c -c communaute1 localhost sysDescr.0

```
root@Ubuntu:/home/vboxuser# snmpget -v 2c -c communaute1 192.168.88.5 sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Linux Ubuntu 6.17.0-14-generic #14~24.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Jan 15 15:52:10 UTC 2 x86_64
root@Ubuntu:/home/vboxuser#
```

Notre communauté a bien été créer et est fonctionnel !

Sécuriser une communauté avec :

- Stopper le service (systemctl stop snmpd)
- Créer un utilisateur pour SNMPv3 en lecture seule :

sudo net-snmp-create-v3-user -ro -a SHA -A "authentication123" -x AES -X "encryption123" snmpadmin

```
root@debian:/home/rdubois# sudo net-snmp-create-v3-user -ro -a SHA -A "authentication123" -x AES -X "encryption123" snmpadmin
adding the following line to /var/lib/snmp/snmpd.conf:
   createUser snmpadmin SHA "authentication123" AES "encryption123"
adding the following line to /etc/snmp/snmpd.conf:
   rouser snmpadmin
root@debian:/home/rdubois#
```

L'utilisateur est-il créé dans le fichier de conf ?

L'utilisateur est créé dans le fichier suivant (/var/lib/snmp/snmpd.conf) :

```
createUser snmpadmin SHA "authentication123" AES "encryption123"
```

```
^G Aide  ^O Écrire  ^F Chercher  ^K Couper  ^T Exécu
```

- Vérifier la connexion

snmpwalk -v3 -a SHA -A authentication123 -x AES -X encryption123 -l authPriv -u snmpadmin localhost head

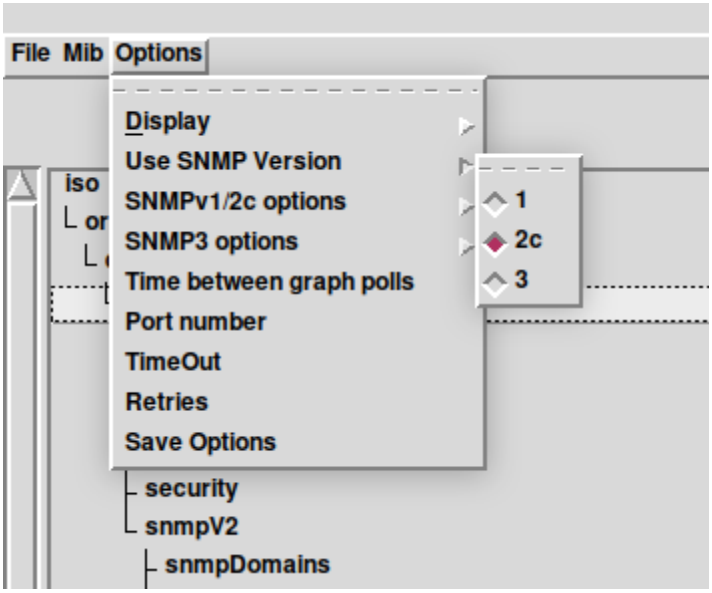
```
root@debian:/home/rdubois# snmpwalk -v3 -a SHA -A authentication123 -x AES -X encryption123 -l authPriv -u snmpadmin localhost system
SNMPv2-MIB::sysDescr.0 = STRING: Linux debian 6.12.57+deb13-arm64 #1 SMP Debian 6.12.57-1 (2025-11-05) aarch64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (3442) 0:00:34.42
SNMPv2-MIB::sysContact.0 = STRING: Me <me@example.org>
SNMPv2-MIB::sysName.0 = STRING: debian
SNMPv2-MIB::sysLocation.0 = STRING: Sitting on the Dock of the Bay
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.9 = STRING: The MIB modules for managing SNMP Notification, plus filtering.
SNMPv2-MIB::sysORDescr.10 = STRING: The MIB module for logging SNMP Notifications.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORUpTime.10 = Timeticks: (0) 0:00:00.00
root@debian:/home/rdubois#
```

Consulter le fichier de conf : Ce n'est pas simple !

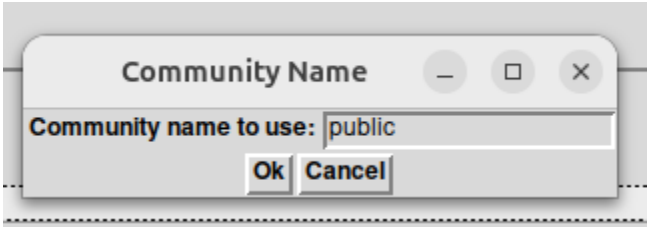
2. Test de l'utilitaire tkmib

Tkmib nous permet d'effectuer diverses tâches tel que les snmpget ou les snmpwalk directement depuis une interface graphique. Pour cela, il suffit d'installer cet utilitaire, de définir notre version de snmp, notre communauté, notre OID ainsi que l'IP de notre serveur pour obtenir les informations que l'on souhaite

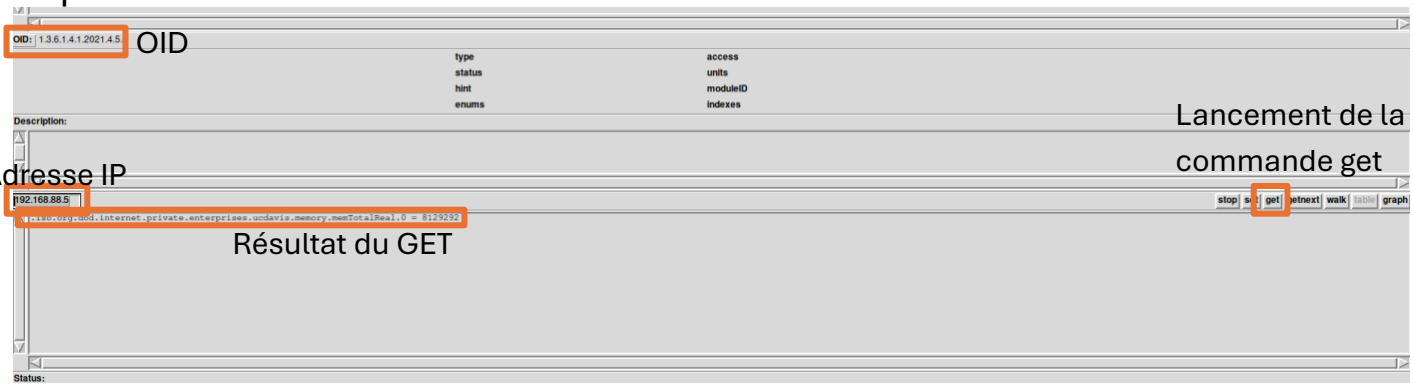
Définition de la version sur « 2c » :



Définition du nom de notre communauté (communaute1) :



Tentative de snmpget avec **tkmib** :



III. Supervision

L'informatique est au cœur de l'entreprise, comme le système nerveux chez l'être humain… Elle doit fonctionner en permanence, donc les problèmes soient anticipés et réduits au minimum.

Disponibilité	90%	99%	99,9%	99,99%	99,999%
Indisponibilité par an	>36j	>3j	>8h	>52min	>5min

Pour garantir la disponibilité, il faut une supervision.

Plusieurs méthodes :

- Analyser les fichiers de logs
- Récupérer les résultats de scripts
- SNMP

Plusieurs modules :

- Supervision réseau
- Supervision système (technique et applicative)
- Lancement de commandes
- Envoi d'alertes
- Visualisation : cartographie, tableau de bord
- Comptes-rendus, rapports d'activité

- Métrologie (Évaluation des performances)

Sur le marché :

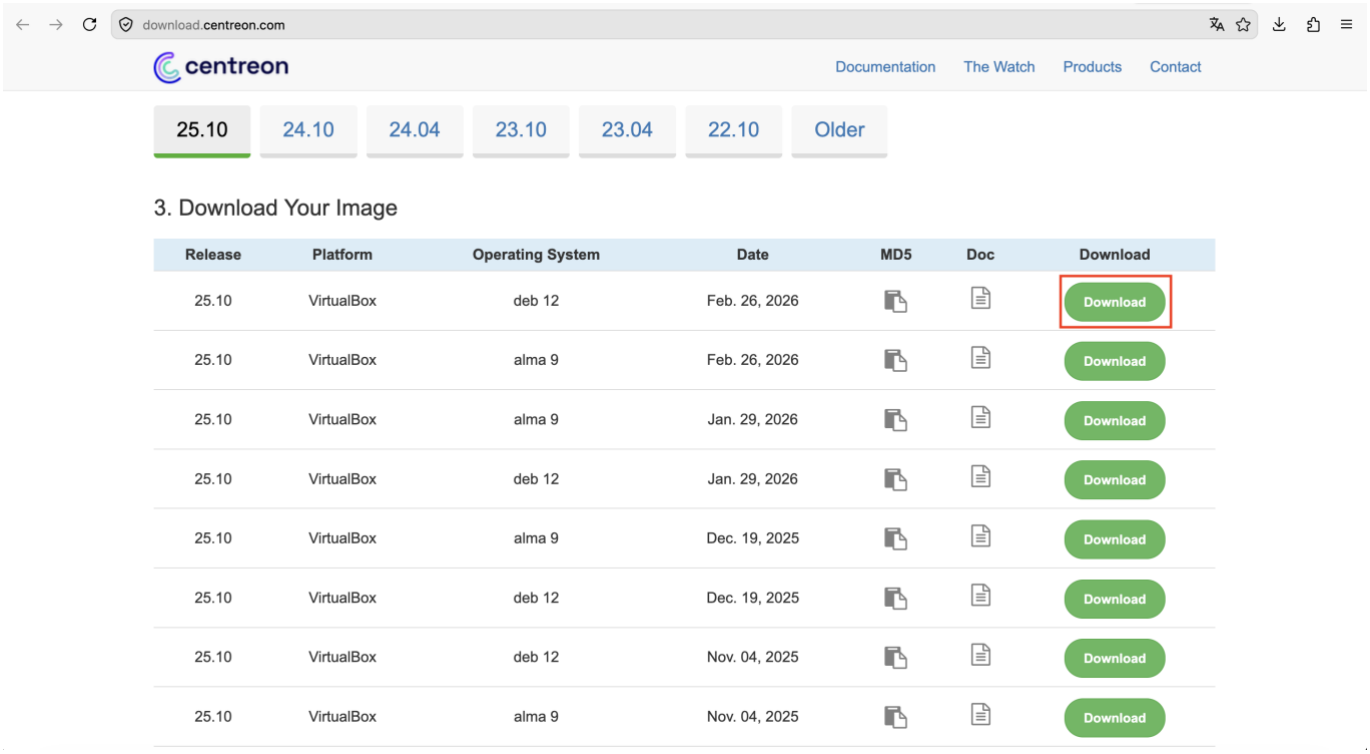
- Offres commerciales : OpenView (HP), Pateol (BMC), Tivoli (IBM)
- Offres libres : Nagios, Zabbix, Cacti, OpenNMS, **Centreon**, CheckMK

IV. Centreon

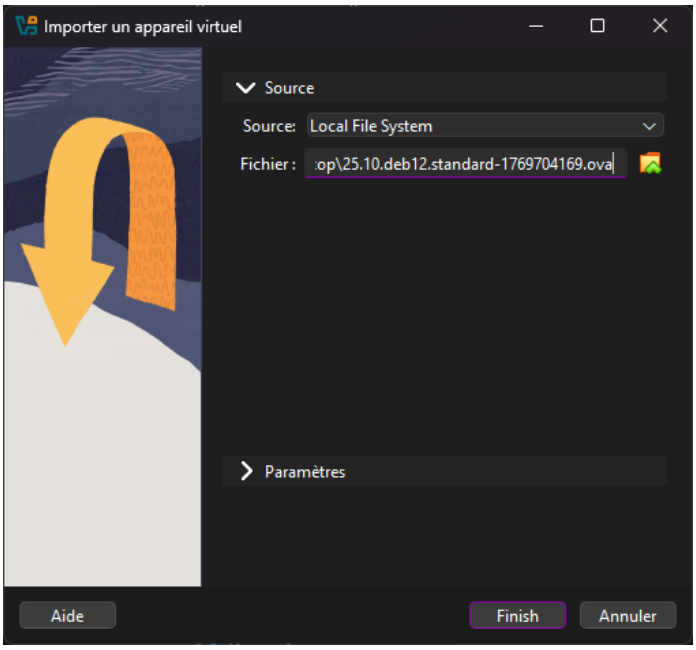
1. Installation

Fork de Nagios. GPL

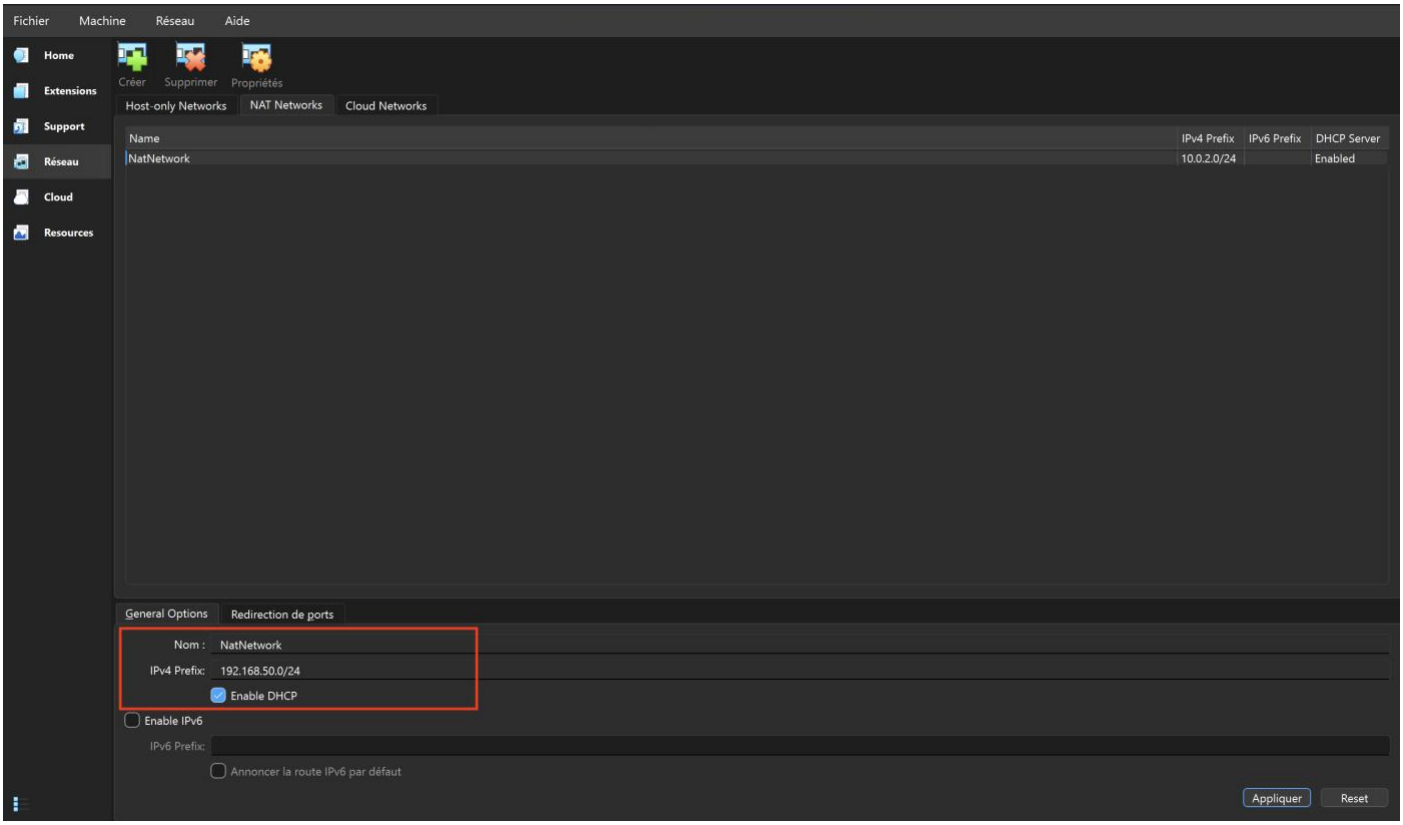
Télécharger directement la VM VirtualBox (https://download.centreon.com)



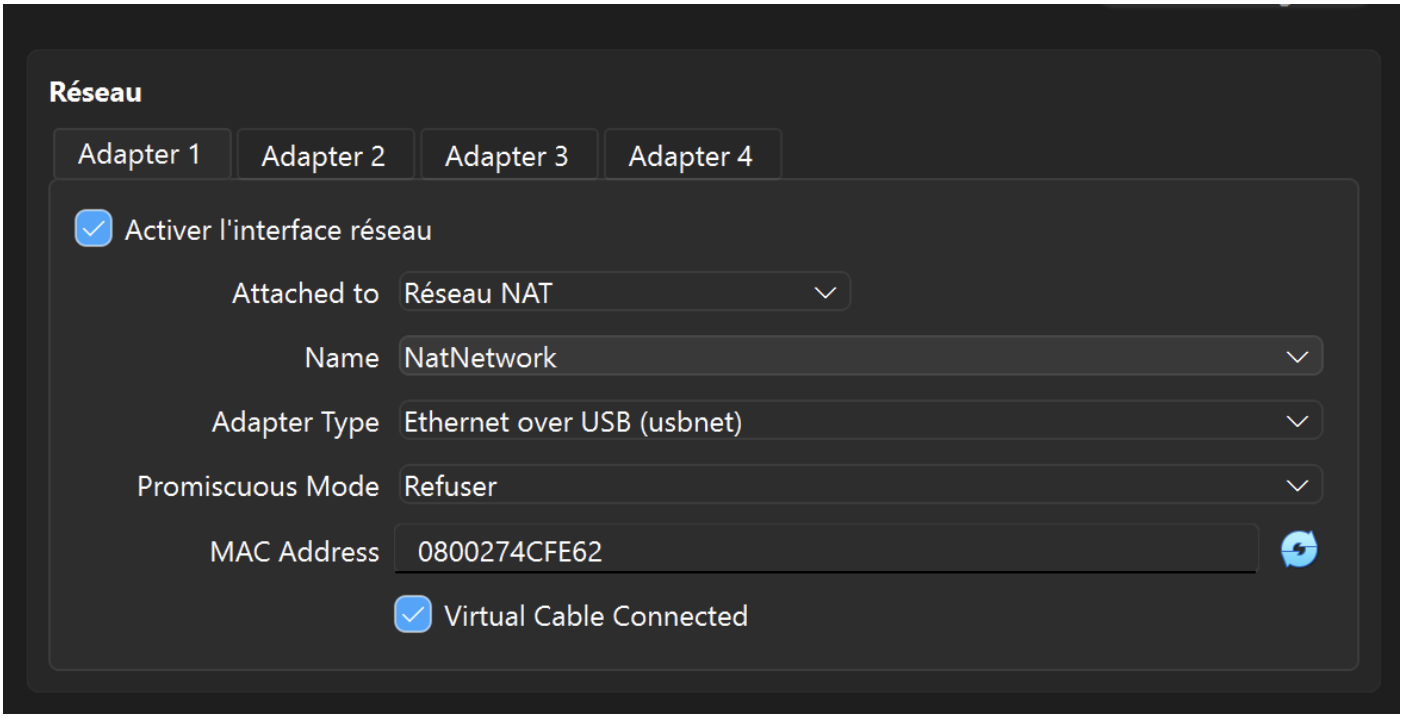
Une fois le fichier téléchargé, on obtient un fichier .ova pouvant être importé dans VirtualBox :



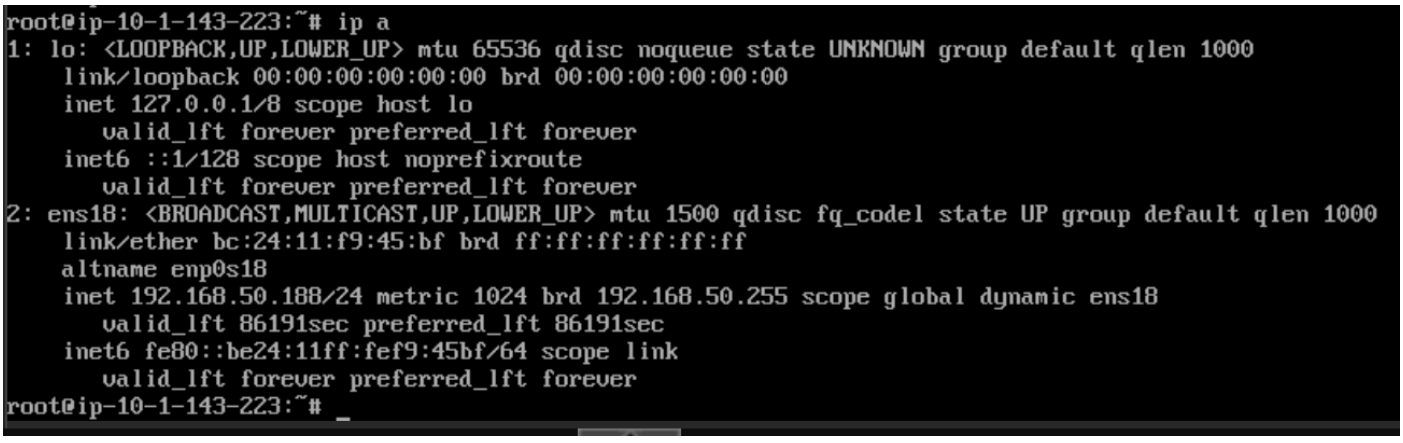
Une fois la VM importée, nous pouvons l'importer dans un réseau NAT (avec réseau DHCP de VirtualBox, comme ça, nous n'aurons pas besoin de définir une IP en dur dans le serveur) :



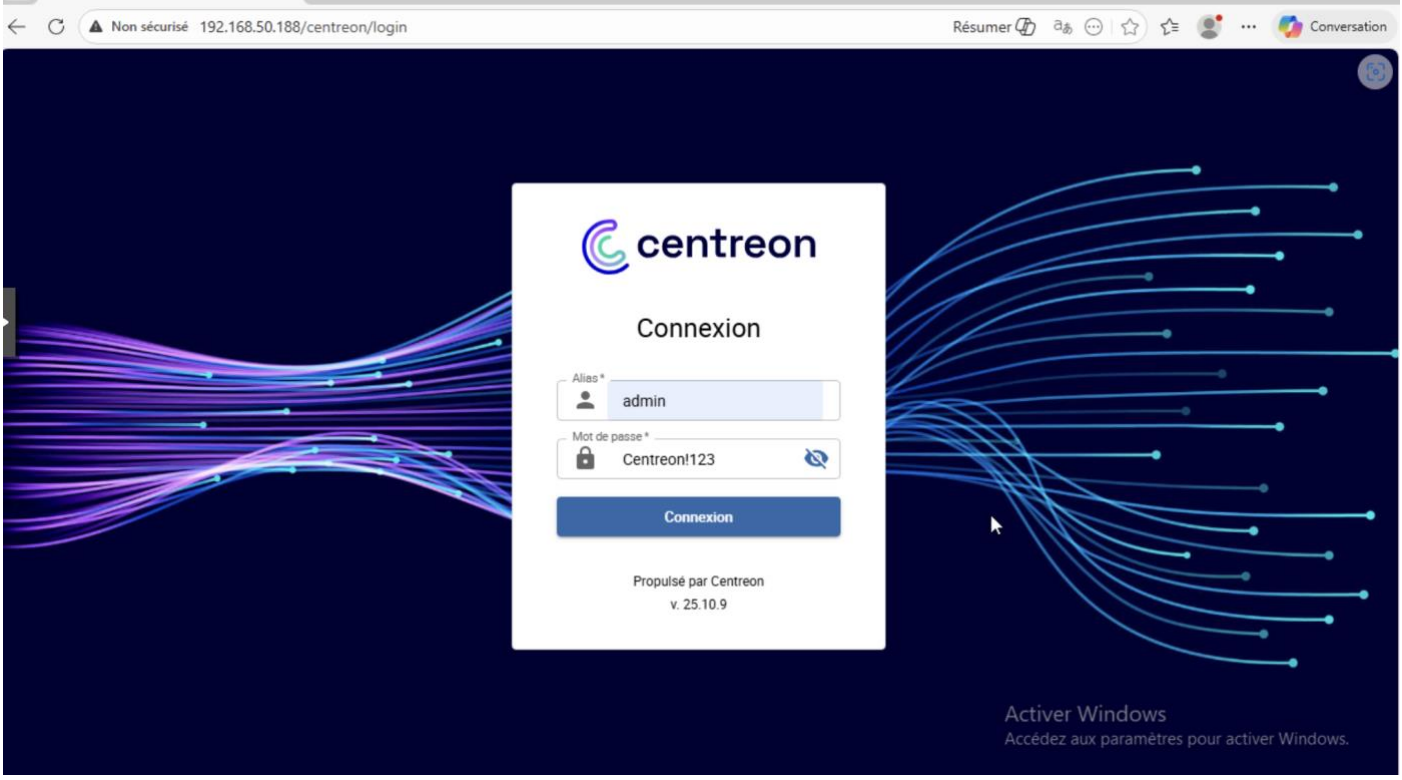
Cette carte réseau devra être associée à notre VM Centreon :



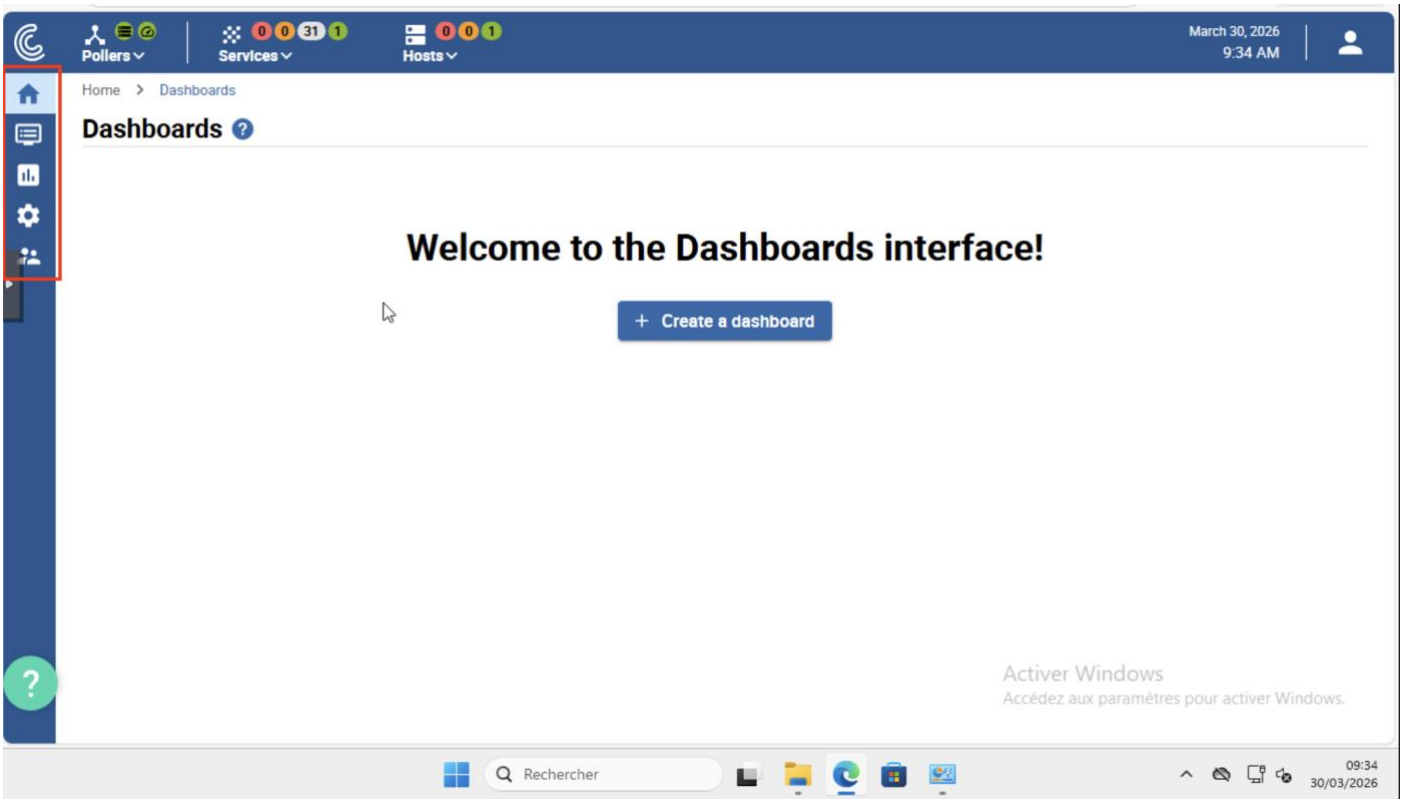
Une fois notre VM importée et connectée au réseau, nous pouvons nous y connecter avec les login par défaut (root / centreon), et nous pouvons faire un « ip a » pour y obtenir son adresse IP :



Nous allons maintenant grâce à son adresse IP nous connecter à l'interface web de Centreon. Les login par défaut sont les suivants (admin / Centreon!123) :



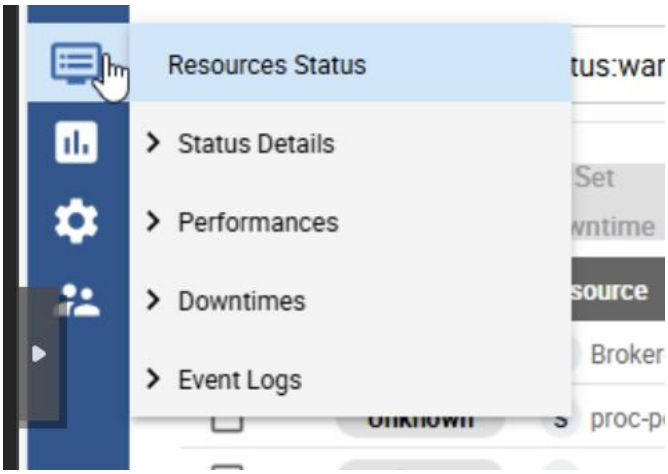
Une fois connecté, nous arrivons sur l'interface de Centreon !



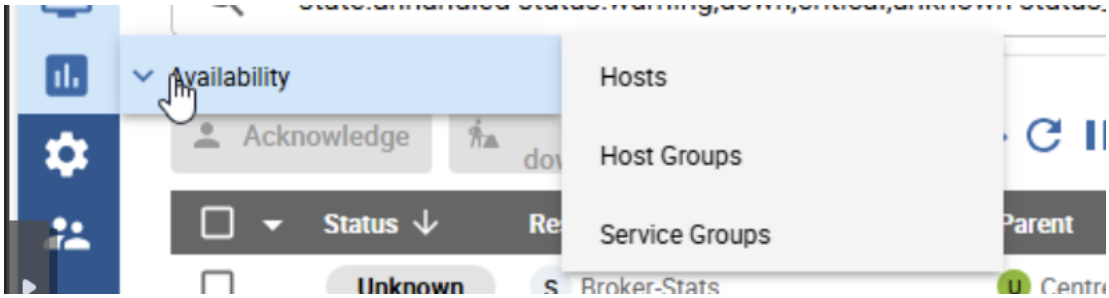
2. Présentation de l'interface

En arrivant, nous arrivons sur le dashboard. Cet endroit est entièrement personnalisable avec les données que l'on souhaite afin qu'on puisse par exemple directement voir si nos machines sont en ligne ou non.

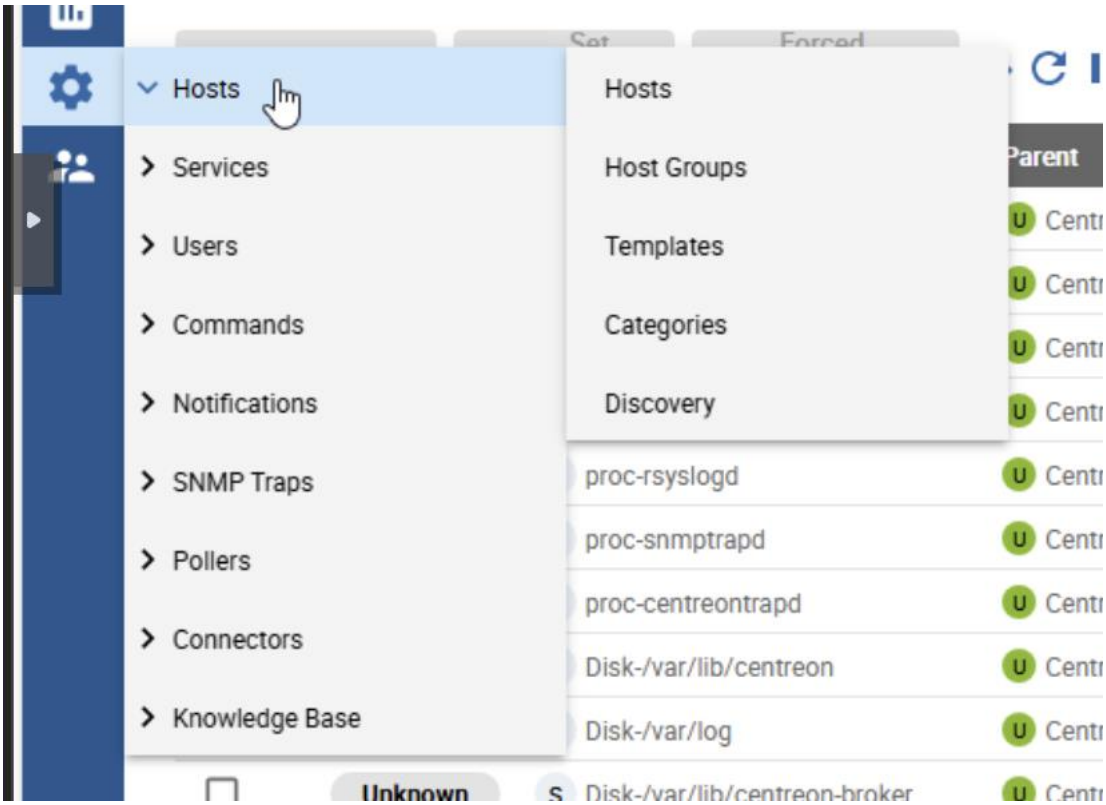
Le deuxième menu est dédié à la vérification des statuts, des downtime, des évènements sur nos hosts et services Centreon :



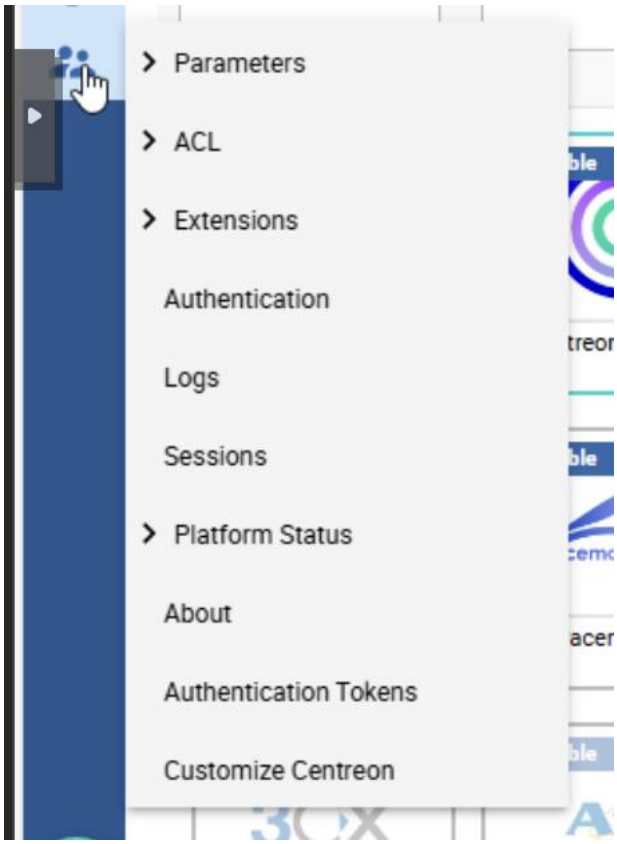
Le 3ème onglet lui est dédié à la vérification de la disponibilité des équipements (services et hosts) :



Le 4ème menu tandis lui permet de gérer les différents hosts, services, users, connecteurs et pollers (serveurs Centreon) et bien plus encore. Ce menu nous sera important par la suite pour ajouter un hôte Windows, Linux, un Switch ou bien même, une imprimante :

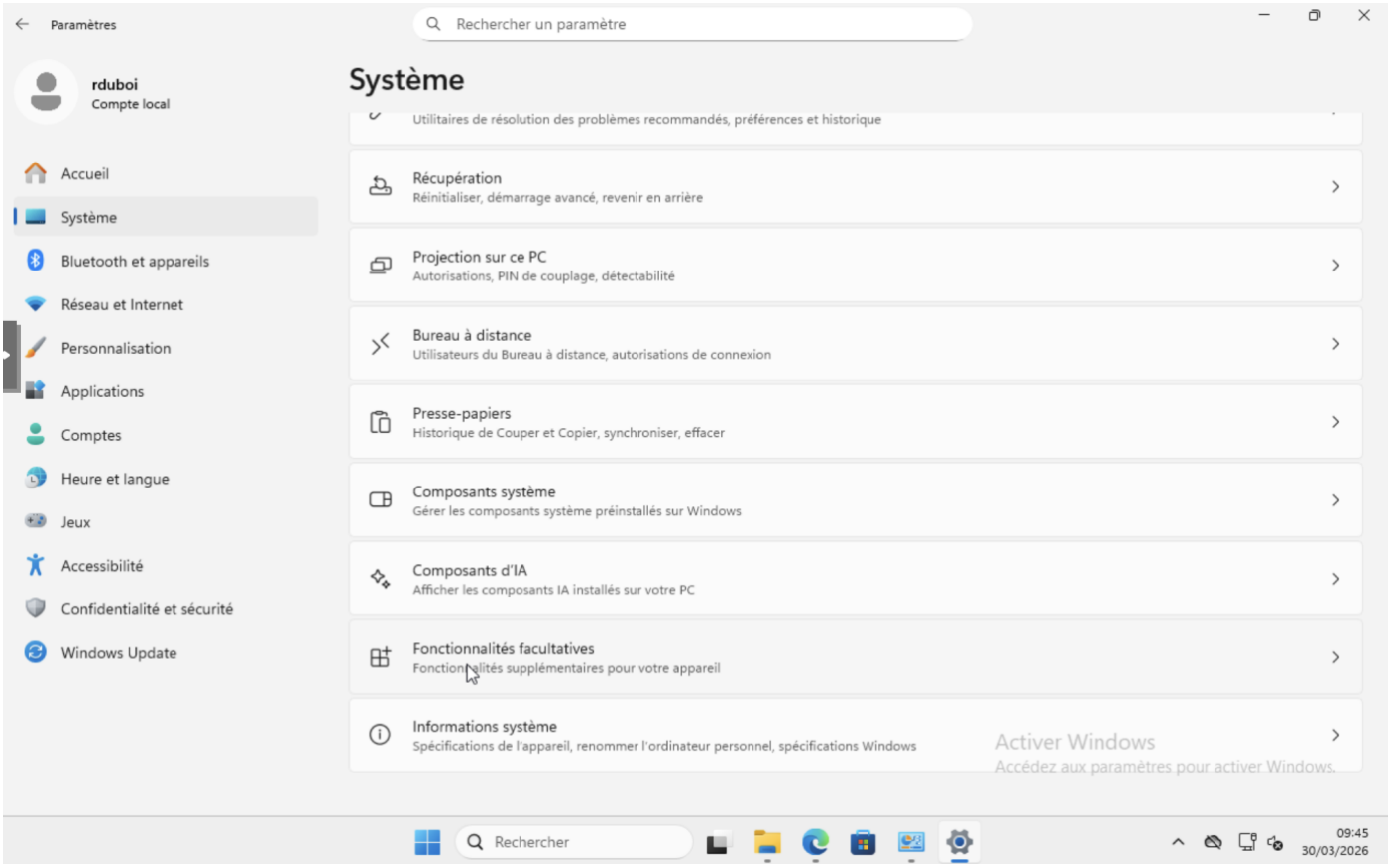


Le 5ème (et dernier menu) lui concerne plus les paramètres liées à l'interface web (utilisateurs, authentification, logs…) :



3. Mise en place Centreon Windows

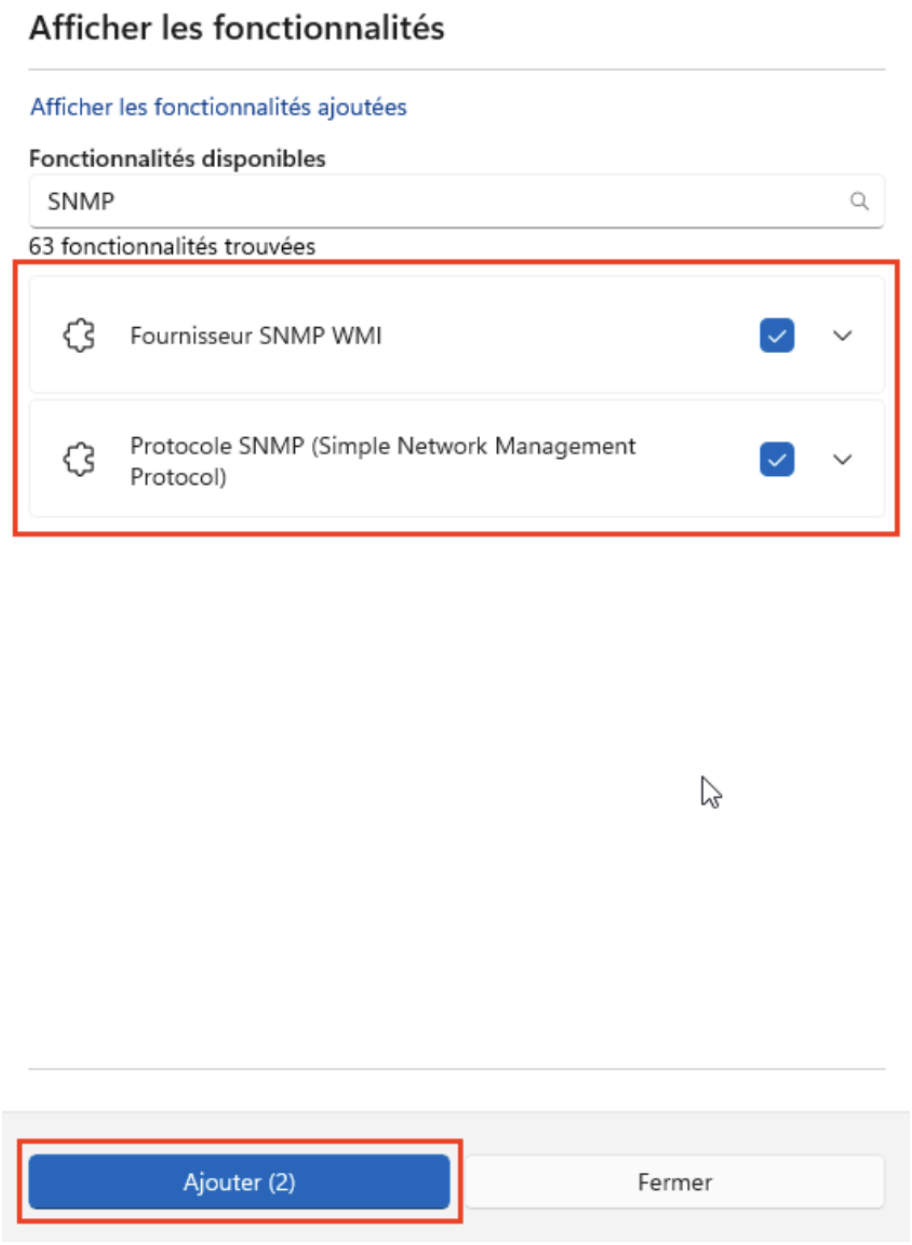
Pour commencer, nous devons premièrement ajouter la fonctionnalité « SNMP » à notre client Windows. Pour cela, nous allons nous rendre dans les paramètres, puis dans « Système » et enfin « Fonctionnalités facultatives » :



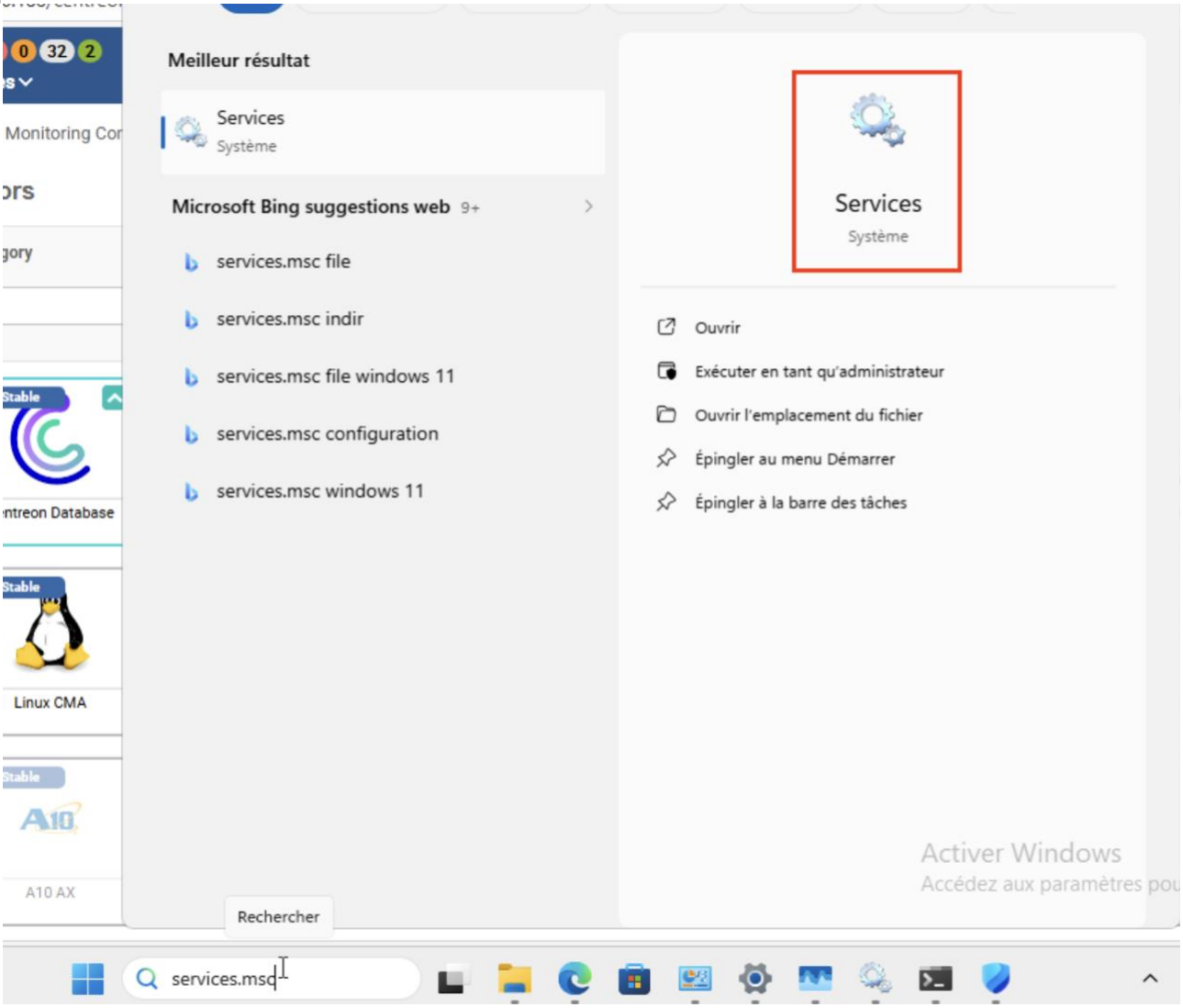




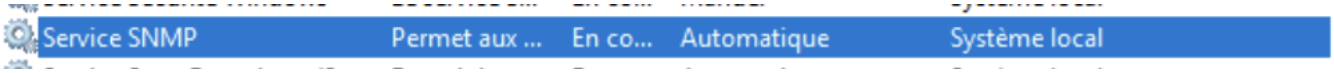
Une fois dans le menu des fonctionnalités facultatives, nous allons chercher « SNMP » et installer les deux fonctionnalités correspondant à cette dernière :



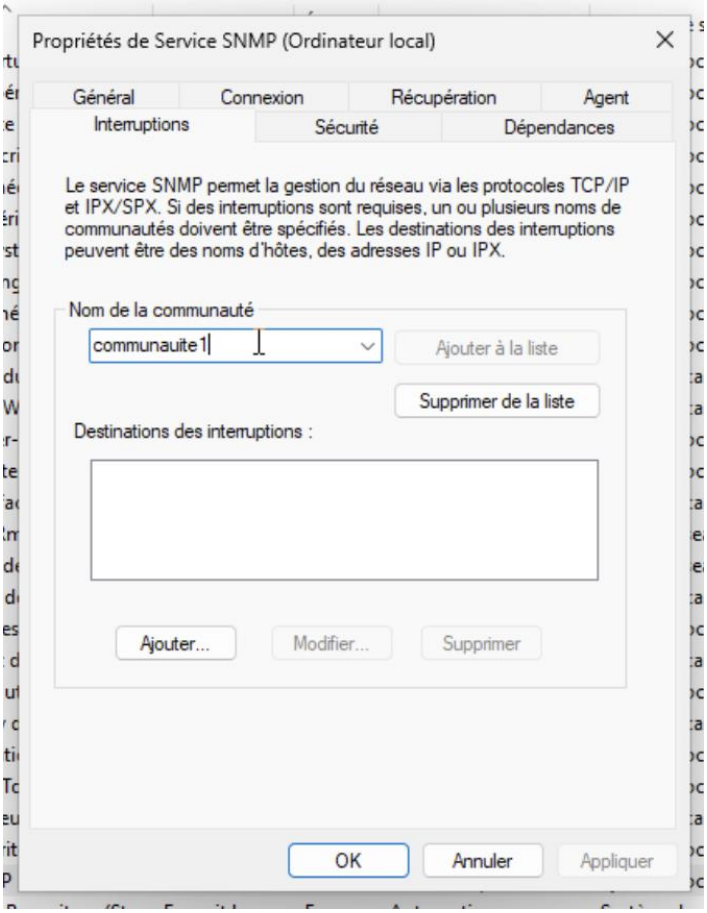
Maintenant, nous allons pouvoir configurer notre service SNMP, pour cela, dans Windows, nous allons ouvrir « services.msc » depuis la barre de recherche :



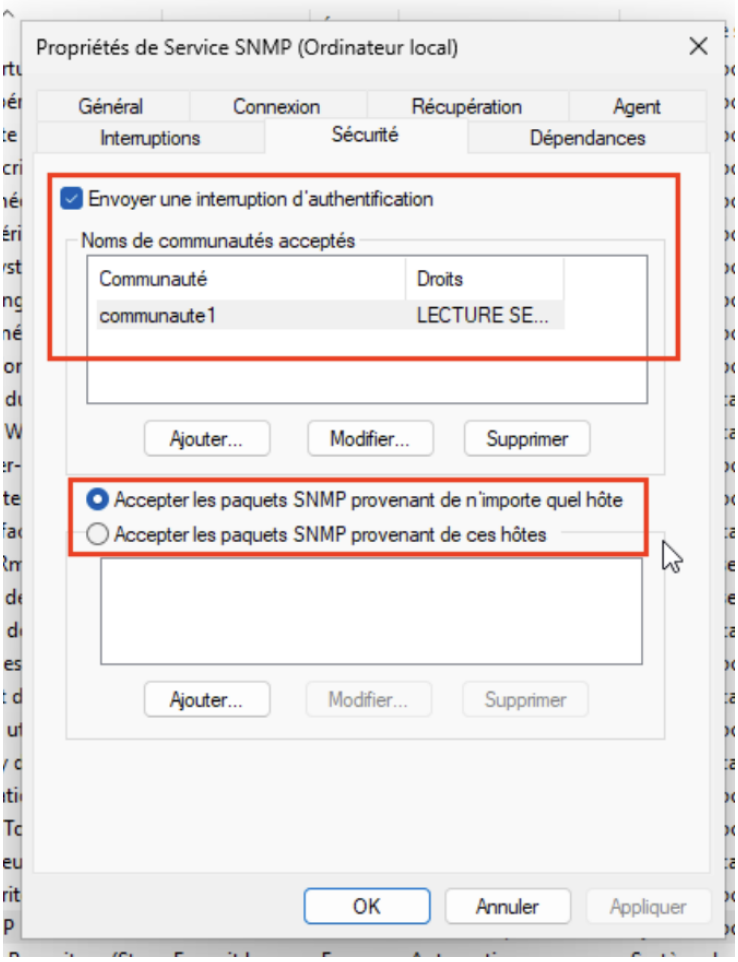
Puis dans les services, nous allons chercher « Service SNMP » puis nous allons l'ouvrir :



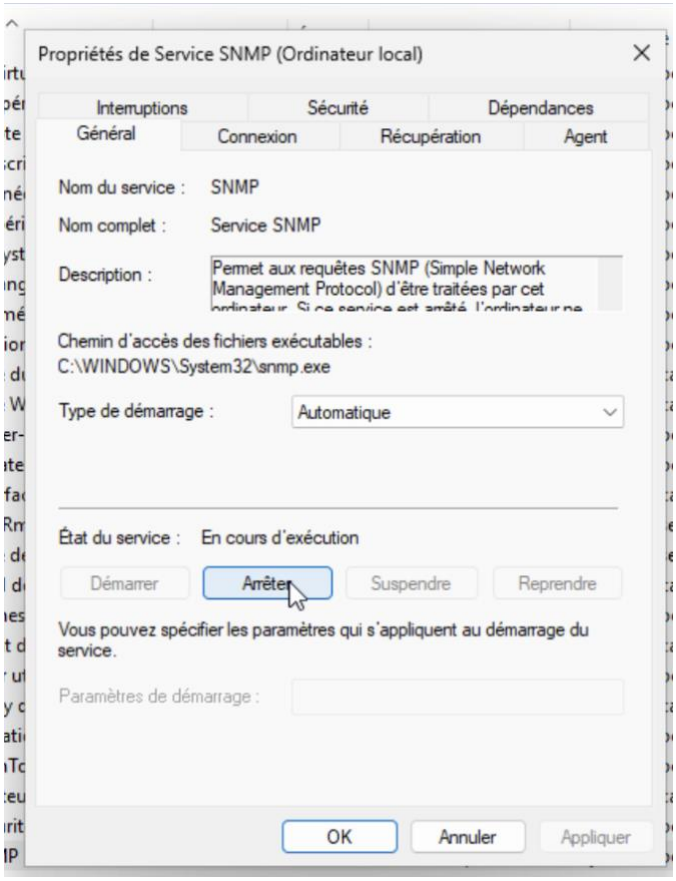
Une fois dans le menu de configuration de SNMP, nous allons nous rendre dans l'onglet « Interruptions », et nous allons créer notre communauté nommée « communaute1 » :



Une fois ajouté à la liste, nous allons nous rendre dans l'onglet « Sécurité ». Dans cet onglet, nous allons définir communaute1 en lecture seul, en autorisant les requêtes SNMP de n'importe quel hôte (dans notre cas de test, accepter tous les hôtes pour du SNMP reste une option, mais en production, il vaut mieux définir un hôte précis, ou encore mieux d'utiliser le SNMP v3) :



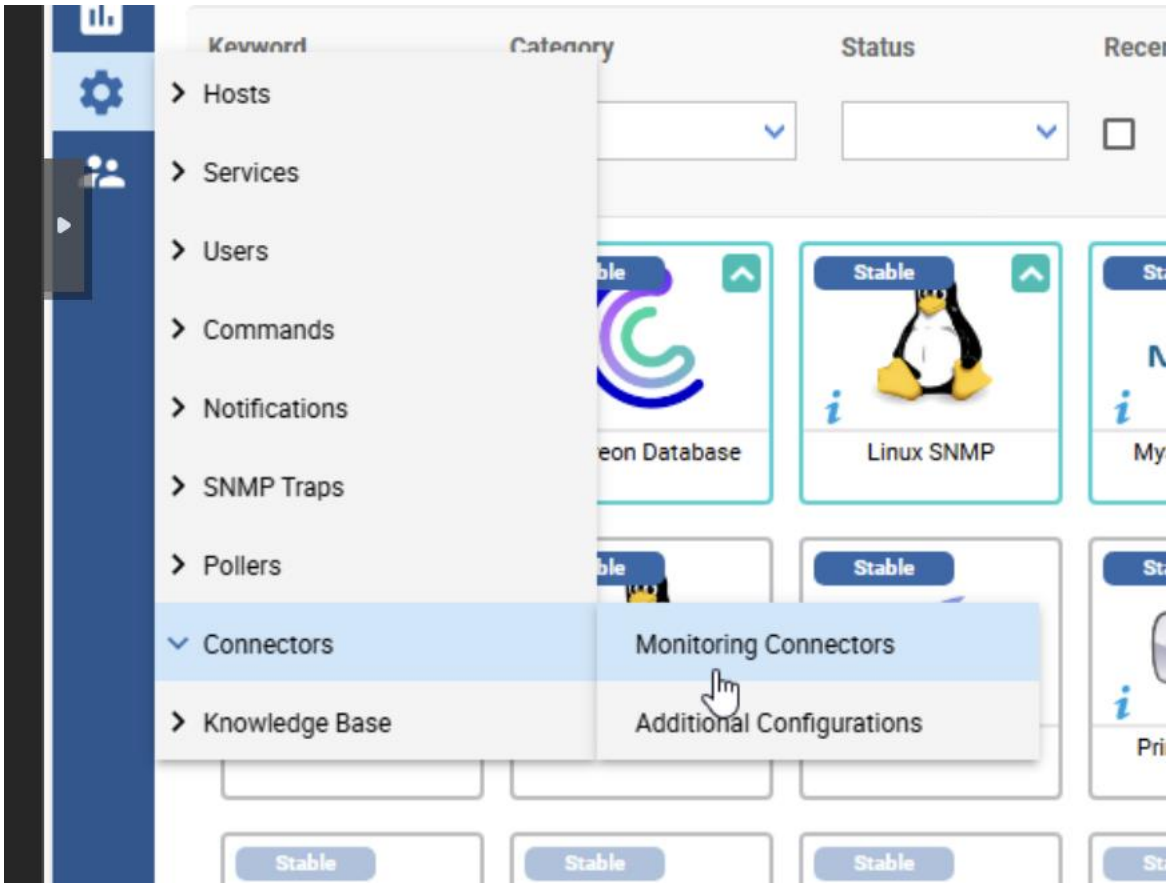
Une fois ceci fait, nous allons appliquer, arrêter puis relancer le service afin d'être sûr que les changements soient appliquées :



Avant d'ajouter notre hôte dans Centreon, nous allons devoir installer les plugins « Windows SNMP » pour faire en sorte que Centreon puisse envoyer des commandes SNMP à un hôte Windows. Pour cela, nous allons installer le paquet « centreon-plugin-operatingsystems-windows-snmp ».

```
42 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ip-10-1-143-223:~# sudo apt install centreon-plugin-operatingsystems-windows-snmp_
```

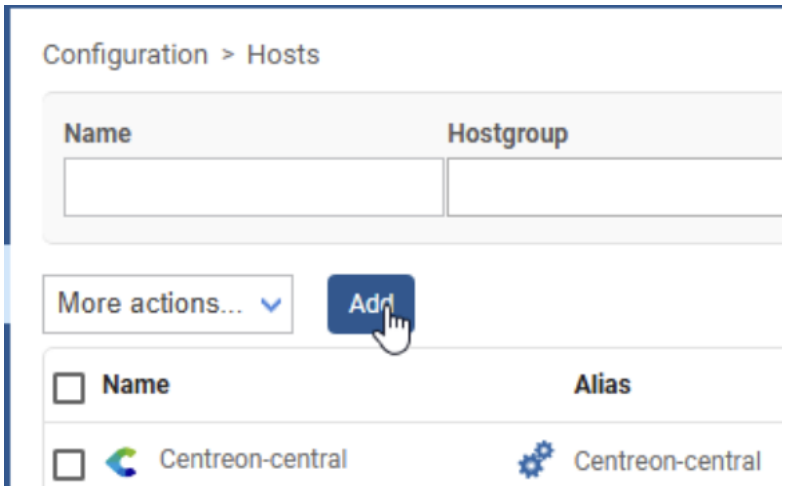
Une fois ce dernier installé, nous allons nous rendre dans Centreon, puis dans « connectors » puis dans « monitoring connectors » :



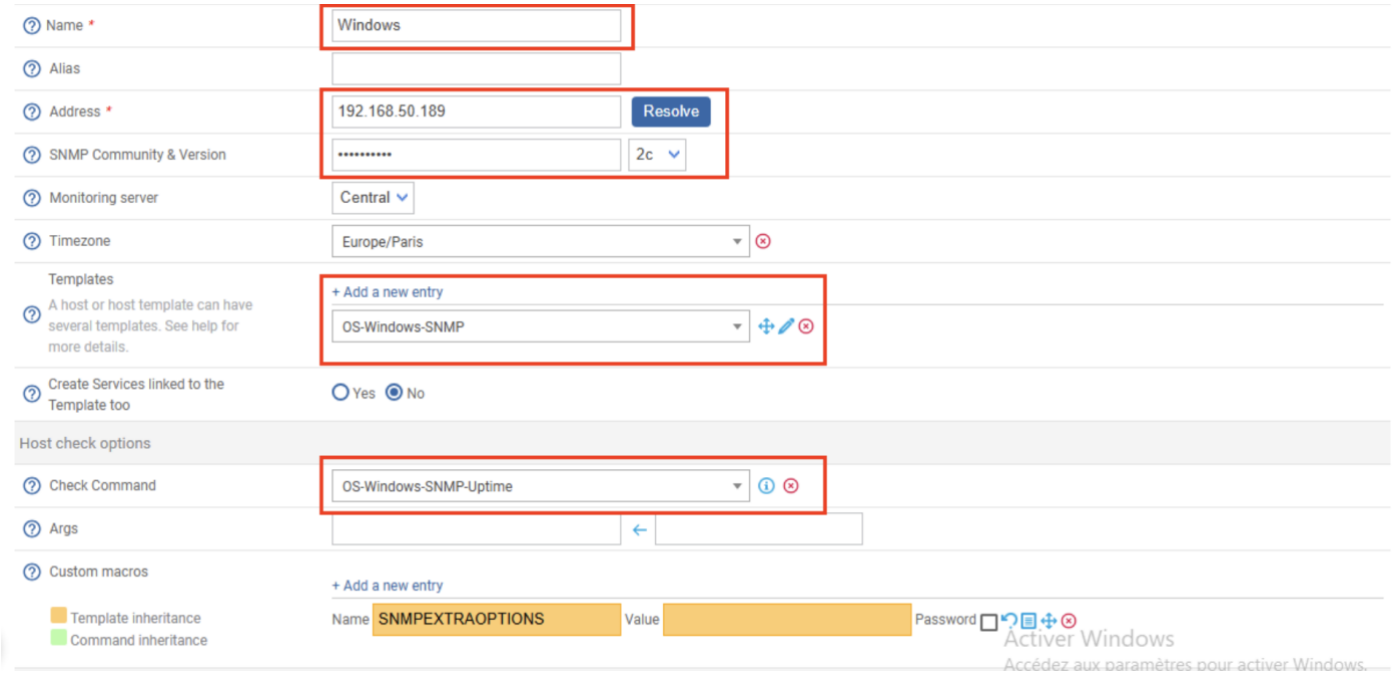
Dans cet interface, nous allons installer le connecteur « Windows SNMP »



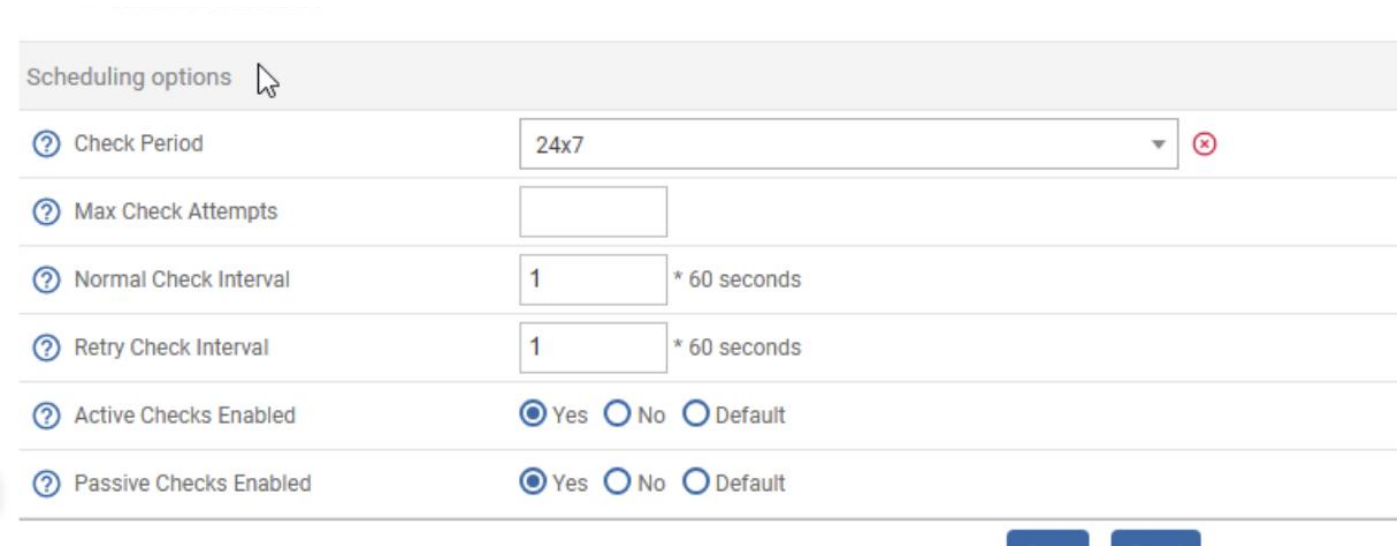
Une fois installé, nous allons pouvoir ajouter notre host à Centreon, pour cela, nous allons nous rendre dans le 4ème onglet puis « hosts ». Ici, nous allons cliquer sur « Add » :



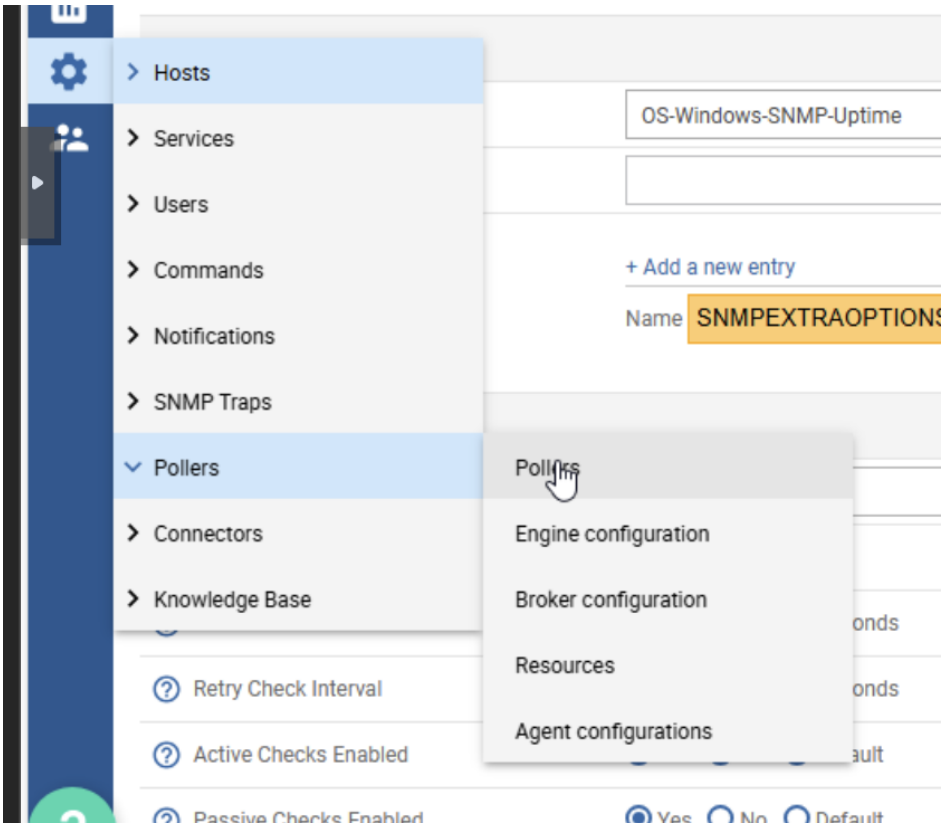
Dans un premier temps, nous allons définir un nom, une adresse IP, la communauté (avec la version sur 2c), un Template (dans notre cas OS-Windows-SNMP) puis une commande pour check (en l'occurrence, nous allons check l'uptime de notre machine Windows). Nous allons aussi mettre « Yes » pour créer les services liées à ce Template (en l'occurrence, il n'y a que le ping associé à ce service, pas de requête SNMP) :



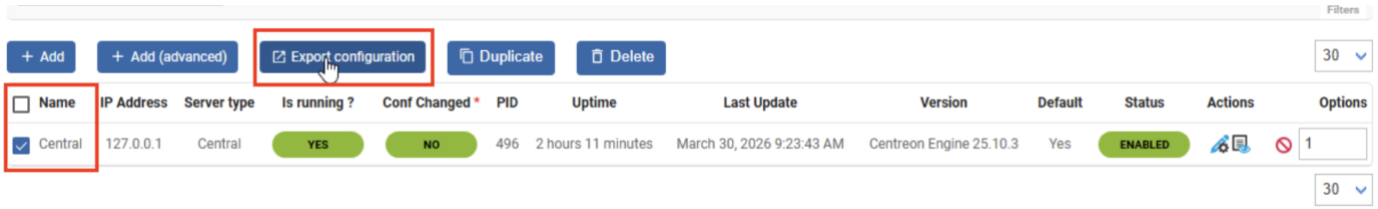
Dans un second temps, nous allons définir tous les combien de temps Centreon doit check notre machine Windows (dans le cadre de notre test, nous allons définir toute les minutes) :



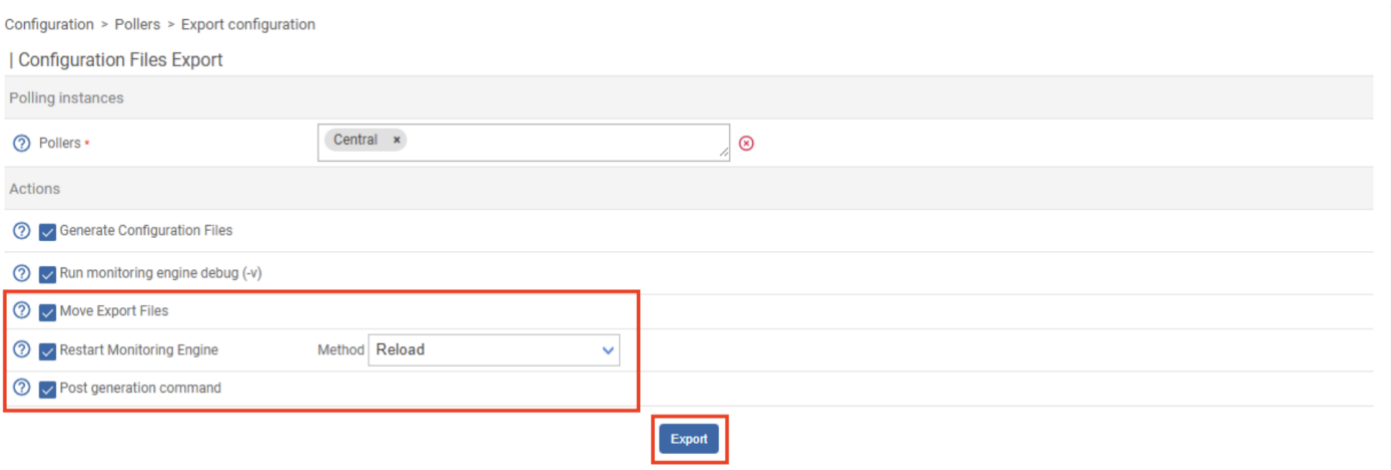
Une fois cela fait, nous pouvons sauvegarder les changements. Maintenant, nous devons les appliquer à notre serveur Centreon, pour cela, nous allons nous rendre dans le 4ème menu puis « pollers » :



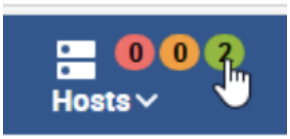
Ici, nous allons devoir sauvegarder notre configuration, pour cela nous allons cliquer sur notre serveur, puis « Export configuration » :



Avant de cliquer sur export, nous allons cocher toute les cases puis nous pouvons lancer l'exportation :

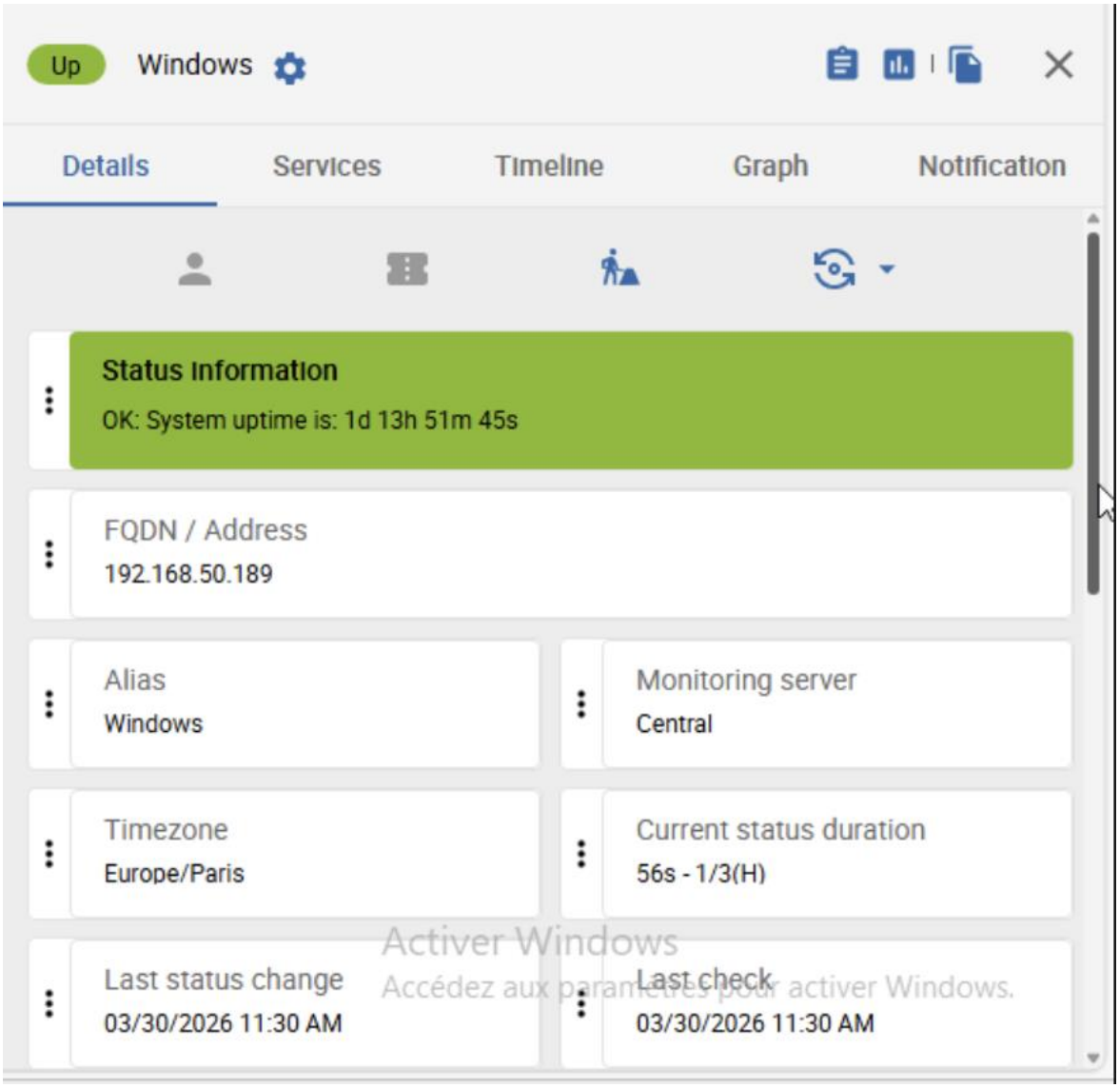


Une fois ceci fait, il suffit d'attendre quelques minutes afin d'observer la barre supérieure afficher « 2 hôtes en ligne » :



Si l'on clique dessus, on observe que notre machine Windows est up et que la requête SNMP nous répond bien l'uptime de cette dernière :

Status	Resource	Parent	G	Duration	Last check	Information	Tries
Up	Windows			23s	25s	OK: System uptime is: 1d 13h 51m 45s	1/3 (H)
Up	Centreon-central			3w 6d	1m 55s	OK - localhost: rta 0.078ms, lost 0%	1/3 (H)



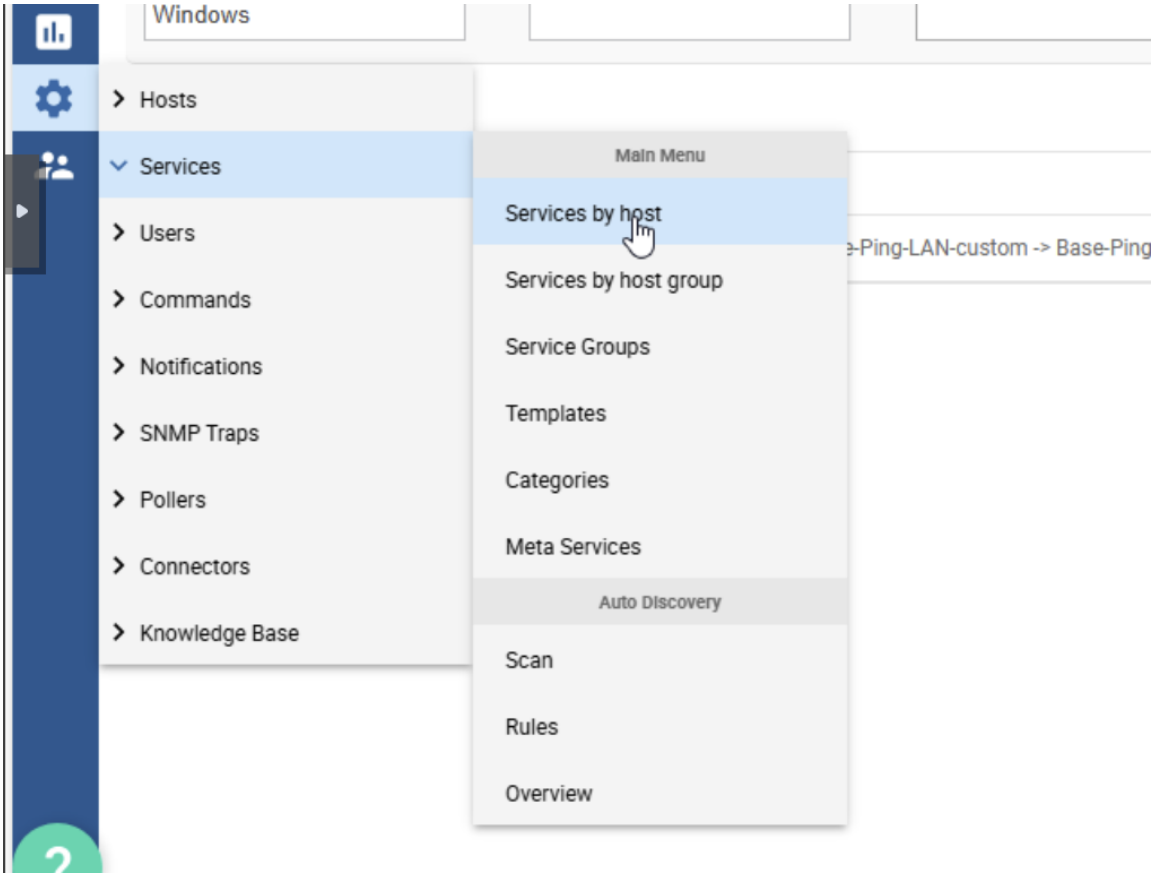
Si l'on observe toujours la barre supérieur, on observe aussi qu'un nouveau « Service » est apparu en vert :

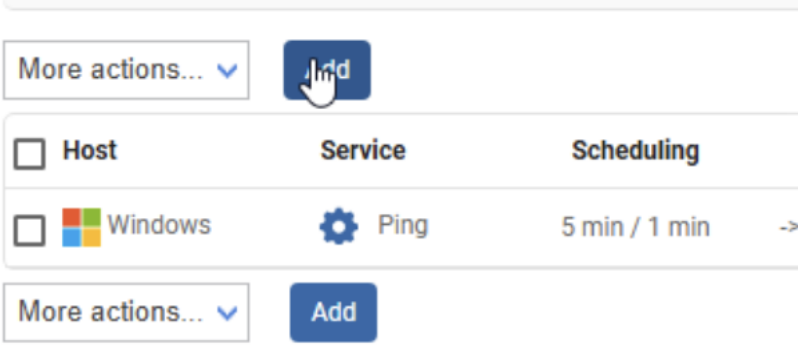


Si l'on clique dessus pour voir ce qu'il y a, nous pouvons voir que la création de notre host a entrainé la création d'un service « ping » vers notre hôte Windows. Ce dernier se charge d'effectuer régulièrement des ping pour vérifier si l'hôte est en ligne :

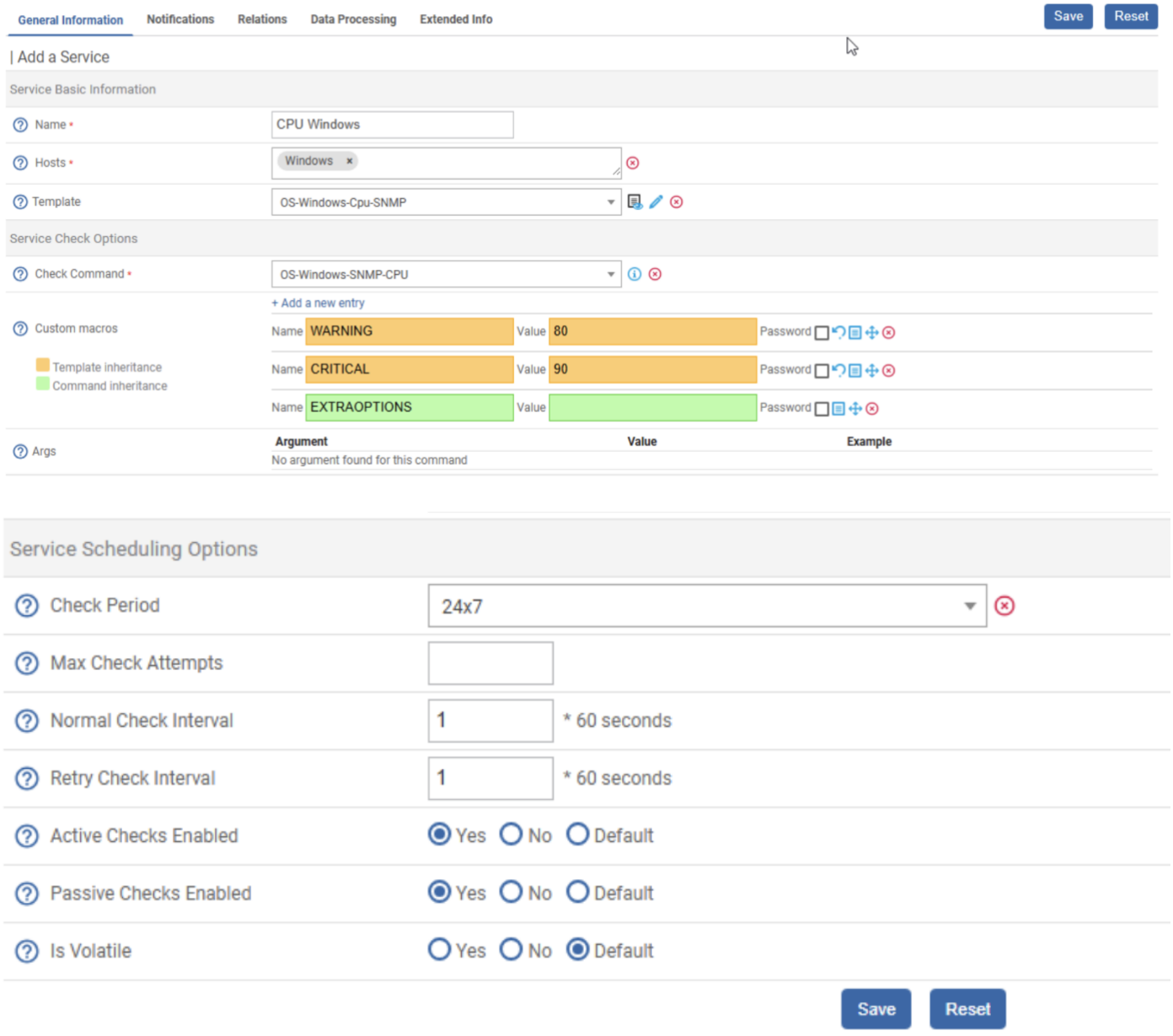
Status	Resource	Parent	G	Duration	Last check	Information	Tries
OK	S Ping	U Windows		38m 40s	32s	OK - 192.168.50.189: rta 0.809ms, lost 0%	1/3 (H)
OK	S Ping	U Centreon-central		2h 18m	2m 43s	OK - localhost: rta 0.018ms, lost 0%	1/3 (H)

A noter qu'il est possible de créer ces propre services pour tout et n'importe quoi dans le 4ème onglet, « Services » puis « Services by host » :

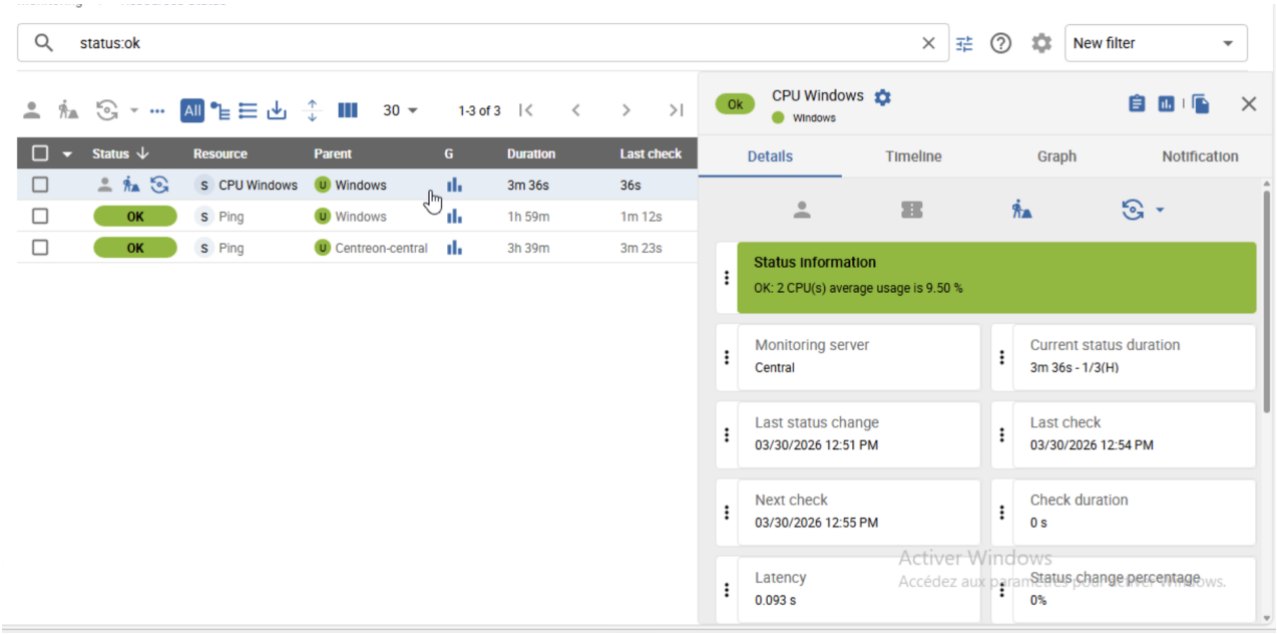




Exemple de création de service pour vérifier l'usage du CPU :



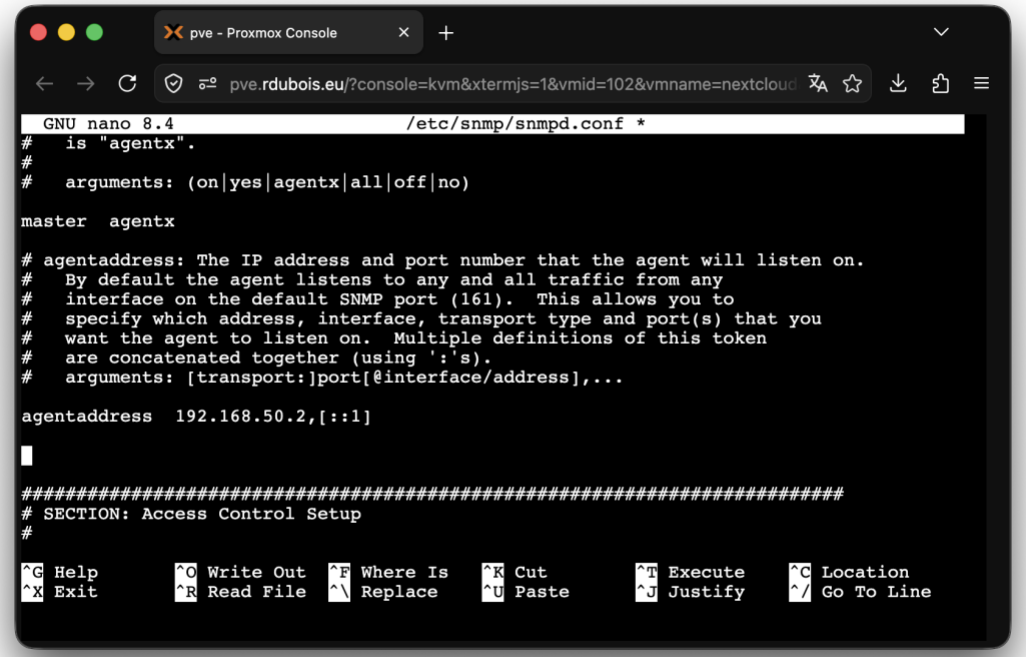
Une fois ceci fait, nous pouvons exporter la configuration, attendre quelques secondes / minutes, et vérifier si dans les services, nous avons bien un nouveau service « Windows CPU » ayant été créer (nous pouvons maintenant y observer le % d'utilisation de notre CPU avec le nombre de cœur que notre machine possède) :



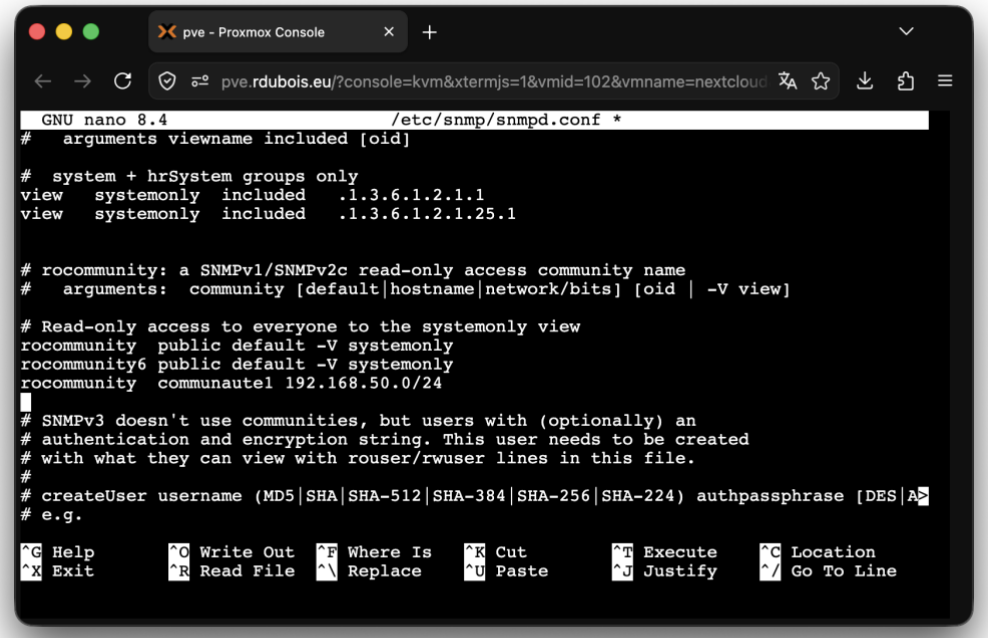
4. Mise en place de Centreon Linux

Cette fois ci, nous allons faire la même chose que précédemment mais avec un hôte Linux. Étant donné que nous avons déjà configuré le SNMP précédemment sur une VM, nous sommes en mesure de pouvoir mettre notre machine directement dans Centreon. Cependant, quelques modifications sont à prévoir.

Premièrement, dans le fichier de configuration (/etc/snmp/snmpd.conf), nous allons devoir, à la ligne « agentAddress », remplacer l'adresse « 127.0.0.1 » par l'adresse IP du serveur Debian :



Ensuite, si ce n'est pas déjà fait, nous allons devoir créer une communauté « communaute1 » (avec comme autorisation, seulement les appareils dans le réseau 192.168.50.0/24) :



Une fois ceci fait, nous pouvons redémarrer le service (systemctl restart snmpd).

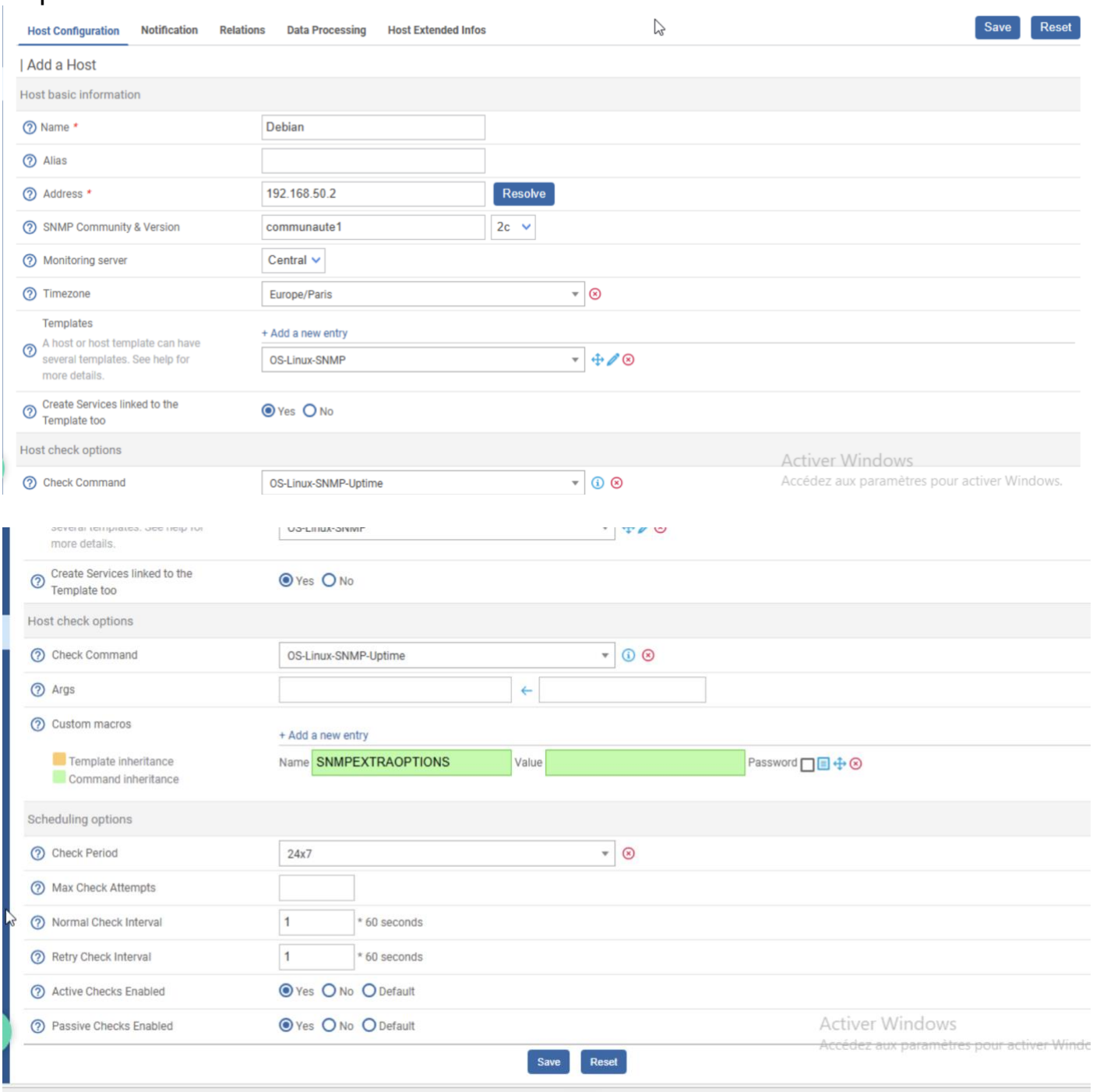
Avant d'ajouter notre host, nous allons faire comme précédemment, installer le plugin Linux SNMP. Pour cela, nous allons ouvrir notre VM Centreon en interface de commande pour exécuter la commande suivante (sudo apt install centreon-plugin-operatingsystems-linux-snmp) :

```
root@ip-10-1-143-223:~# sudo apt install centreon-plugin-operatingsystems-linux-snmp_
```

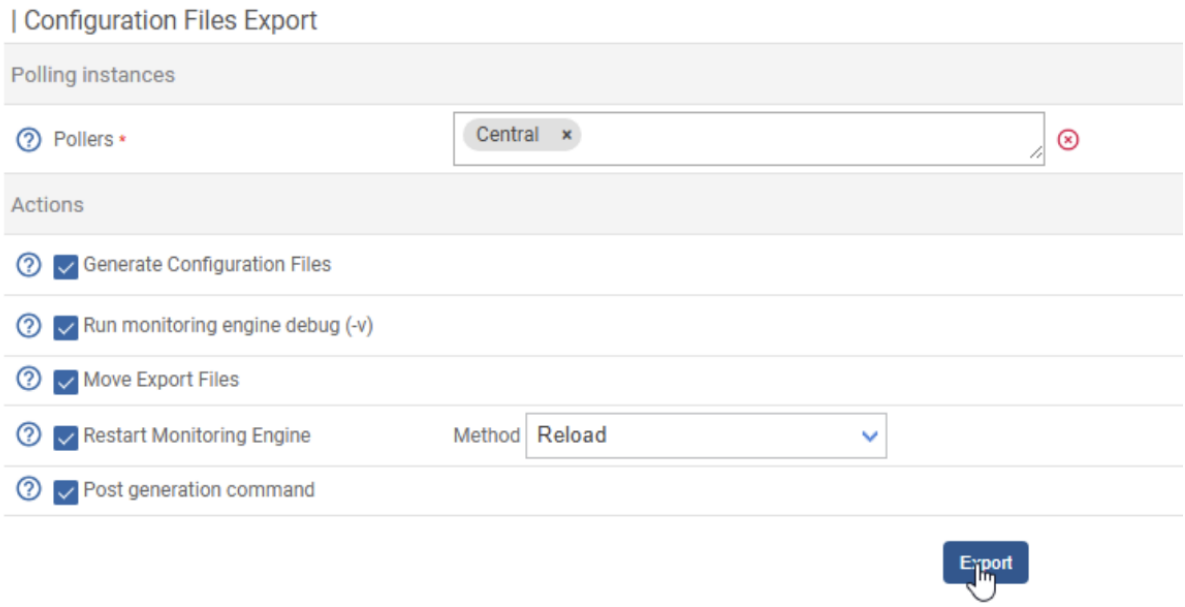
Une fois la commande effectuée, nous allons revenir sur l'interface web pour vérifier si le connecteur est bien présent (par défaut, il doit être déjà actif) :



Maintenant, nous pouvons ajouter dans « hosts » notre serveur Debian (de la même manière que nous avons fait avec Windows, mais cette fois ci, nous allons bien sélectionner le Template Linux SNMP avec un check uptime pour Linux) :

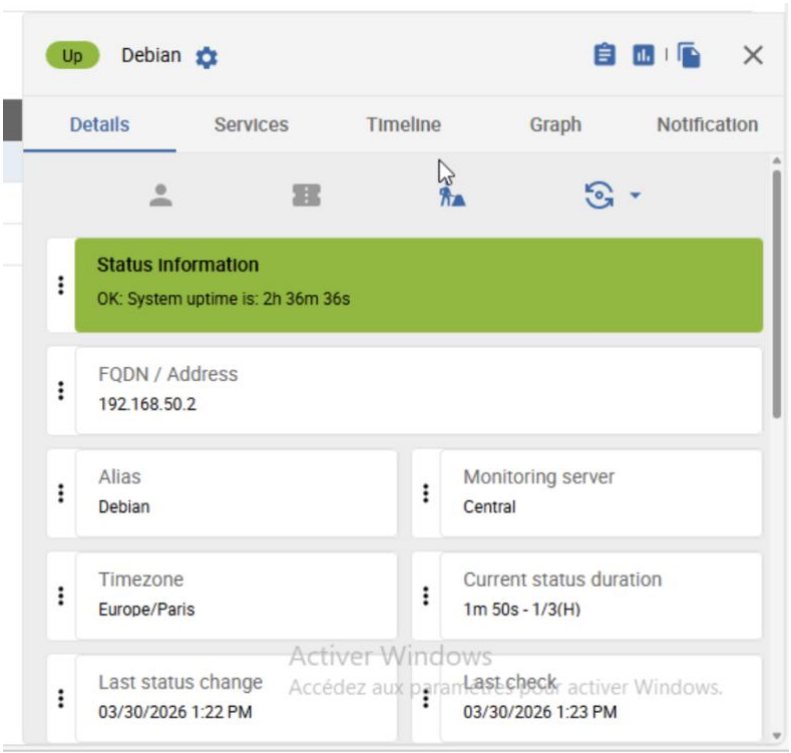


Une fois ceci fait, on n’oublie pas d’exporter la configuration de notre serveur :

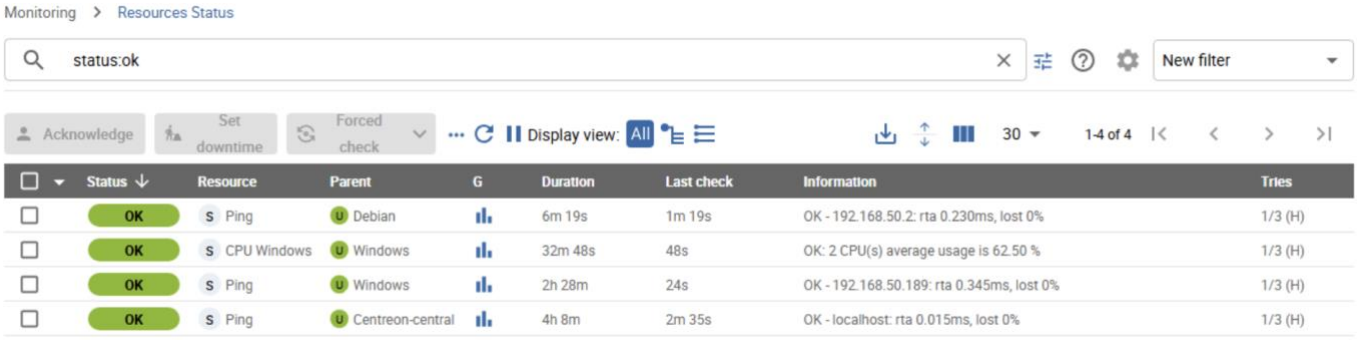


Maintenant, nous pouvons attendre quelques secondes / minutes, et vérifier si un nouvel host est bien apparu :





Si l'on vérifie les services, on remarque qu'un service ping a bien été créer pour Debian :



5. Mise en place de Centreon sur Switch Cisco

Maintenant, nous allons mettre en place le SNMP sur un Switch Cisco physique qui sera sur un réseau que nous allons créer sur ce dernier. Pour cela, on va brancher le Switch sur la deuxième carte réseau de notre machine, et nous allons définir une IP à notre Switch sur la Vlan 1 :

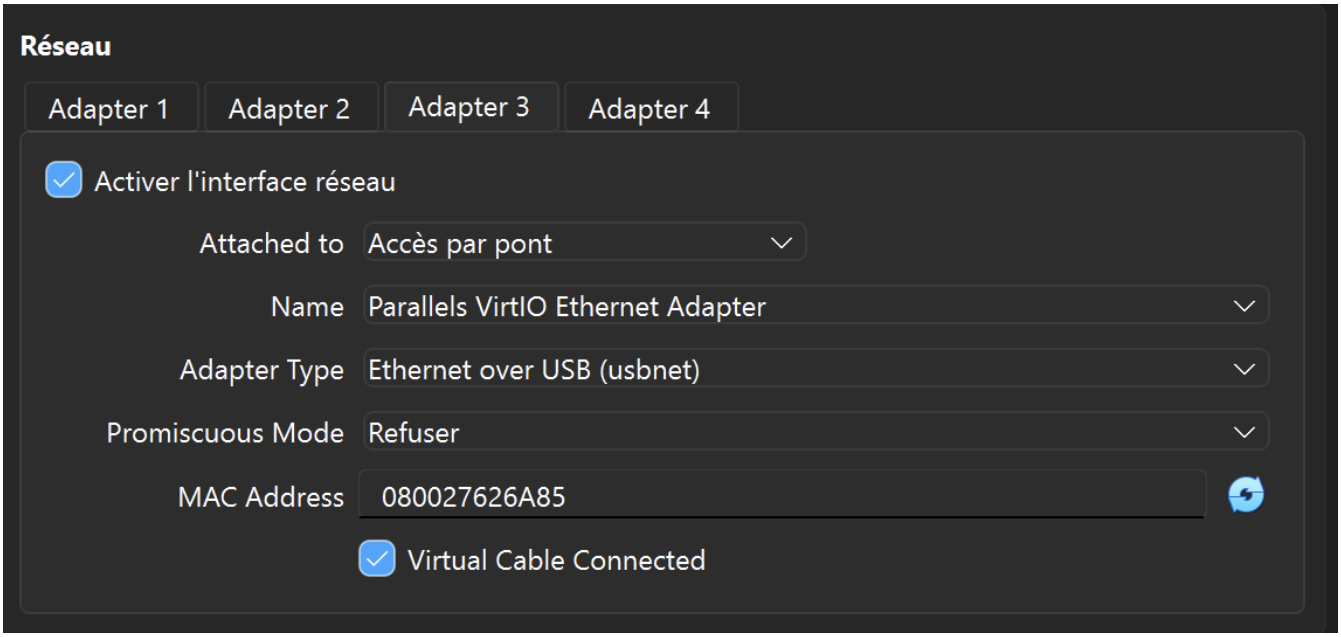
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface Vla
Switch(config)#interface Vlan 1
Switch(config)#interface Vlan 1
Switch(config-if)#ip add
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-3-UPDOWN: Interface Vlan1, changed state to down

Switch(config-if)#
```

Ensuite, nous allons activer le SNMP sur notre Switch avec la communauté « communaute1 » (en lecture seule ou RO) :

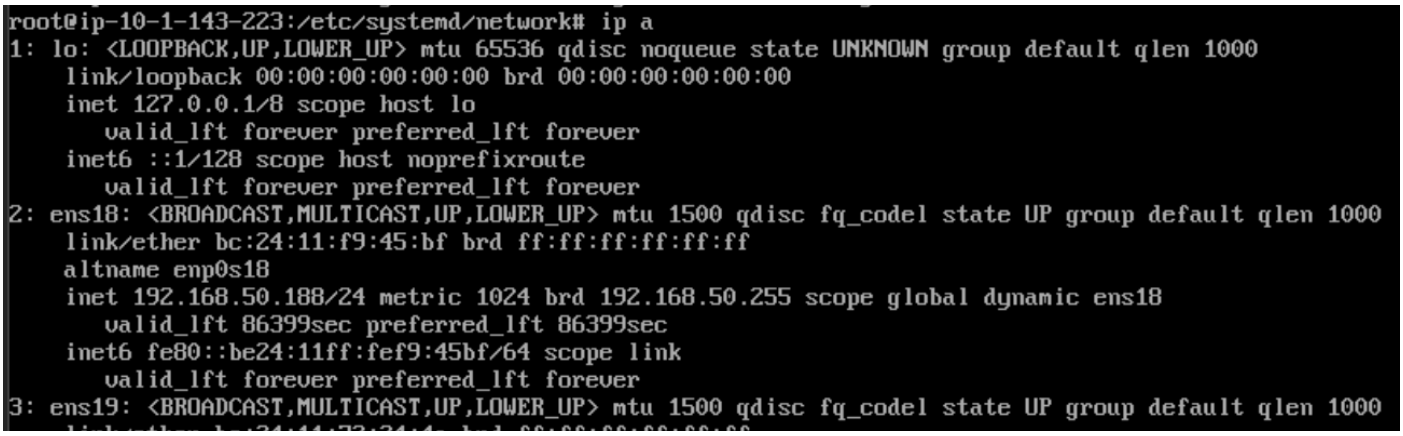
```
Switch(config)#snmp-server community communaute1 RO
```

Une fois ceci fait, nous pouvons configurer le réseau sur notre PC.

Sur notre VM, nous allons ajouter une nouvelle interface réseau (Adaptateur 3) en accès par pont à cette carte réseau physique connecté à notre Switch Cisco :

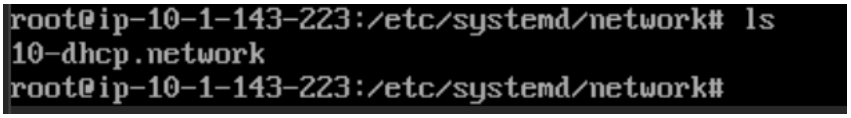


Maintenant, nous allons devoir modifier l'IP de la deuxième carte réseau sur la VM Centreon, pour cela, nous allons tout d'abord faire un « ip a » pour récupérer le nom de nos 2 cartes réseaux :

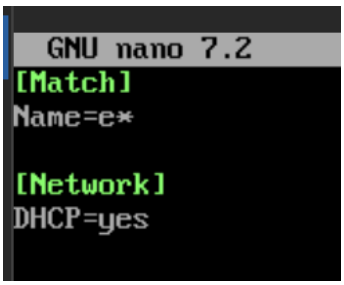


On remarque la carte ens18 étant sur le réseau ou nous avons mis en place nos machines Linux et Windows, et une nouvelle carte « ens19 » correspondant à la carte que nous venons de créer.

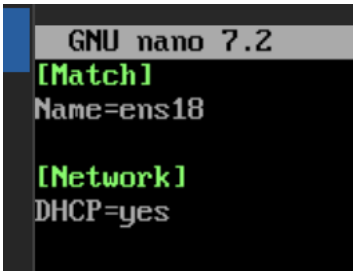
Pour modifier son adresse IP, nous allons premièrement nous rendre dans le dossier (/etc/systemd/network) :



Par défaut, nous avons un fichier « 10-dhcp.network » correspondant à la configuration par défaut (DHCP uniquement) :



Ici, on remarque que le DHCP est actif pour toute les cartes commençant par « e ». Nous allons changer ceci en ens18 pour que le client DHCP ne soit actif que sur cette carte réseau :



Nous allons maintenant créer un nouveau fichier « 9-net.network » avec une IP fixe pour notre interface ens19 :

```
root@ip-10-1-143-223:/etc/systemd/network# ls
10-dhcp.network  9-net.network
root@ip-10-1-143-223:/etc/systemd/network# _
```

```
  GNU nano 7.2
[Match]
Name=ens19

[Network]
Address=192.168.1.2/24
```

(On prend la .2 étant donné que la .1 est prise par le Switch)

Une fois ceci fait, nous pouvons redémarrer le service systemd-networkd (systemctl restart systemd-networkd). Maintenant, nous pouvons vérifier les adresses IP de nos interfaces, voir si elles correspondent bien à nos changements :

```
root@ip-10-1-143-223:/etc/systemd/network# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:f9:45:bf brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.50.188/24 metric 1024 brd 192.168.50.255 scope global dynamic ens18
       valid_lft 85921sec preferred_lft 85921sec
    inet6 fe80::be24:11ff:fef9:45bf/64 scope link
       valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:72:24:4a brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.1.2/24 brd 192.168.1.255 scope global ens19
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe72:244a/64 scope link
       valid_lft forever preferred_lft forever
root@ip-10-1-143-223:/etc/systemd/network#
```

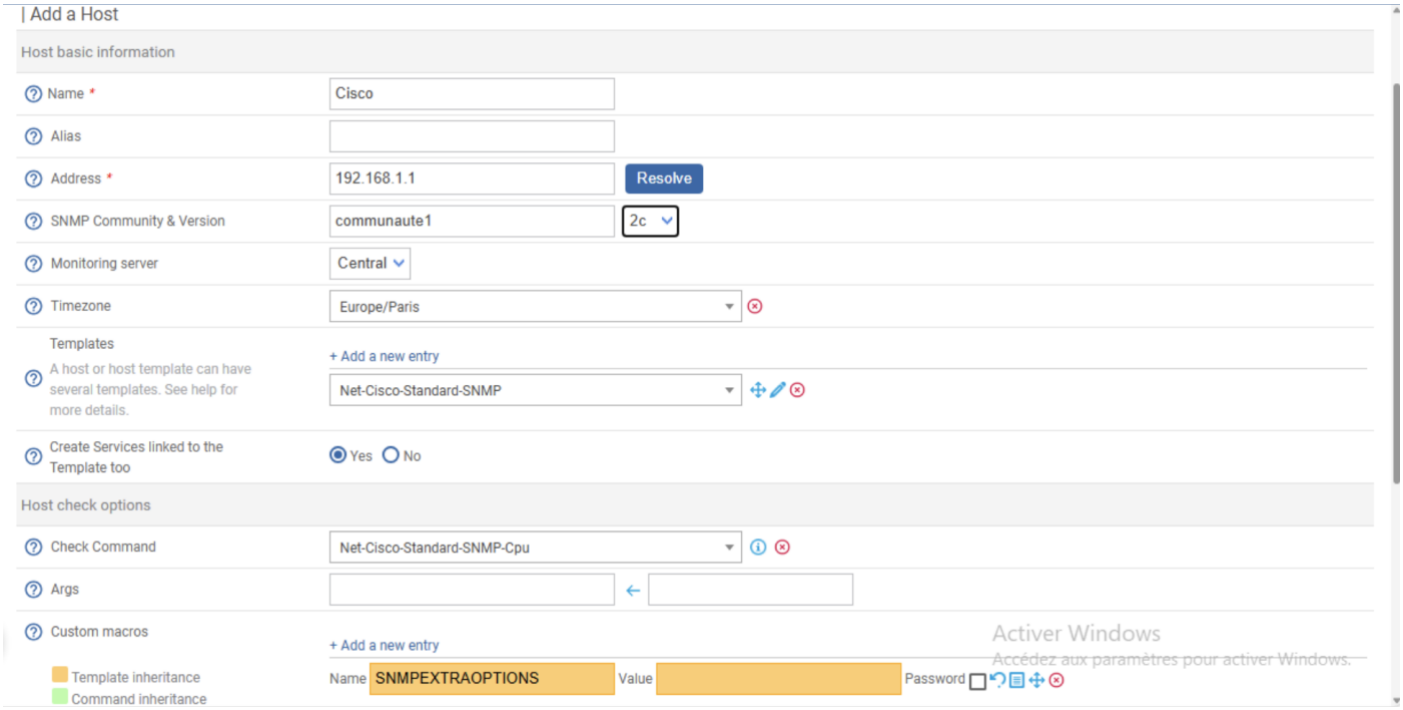
Une fois que tout est bon, nous pouvons installer le plugin : « centreon-plugin-network-cisco-standard-snmp ». Pour que notre Switch fonctionne sur Centreon :

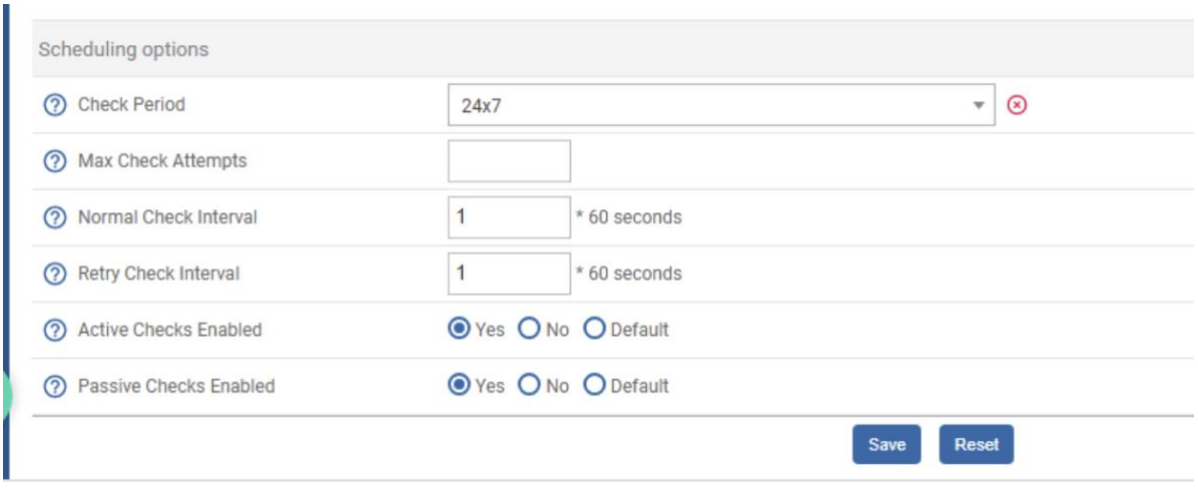
```
root@ip-10-1-143-223:/etc/systemd/network# sudo apt install centreon-plugin-network-cisco-standard-snmp_
```

Pareil dans les connecteurs, nous allons installer le connecteur « Cisco SNMP » :

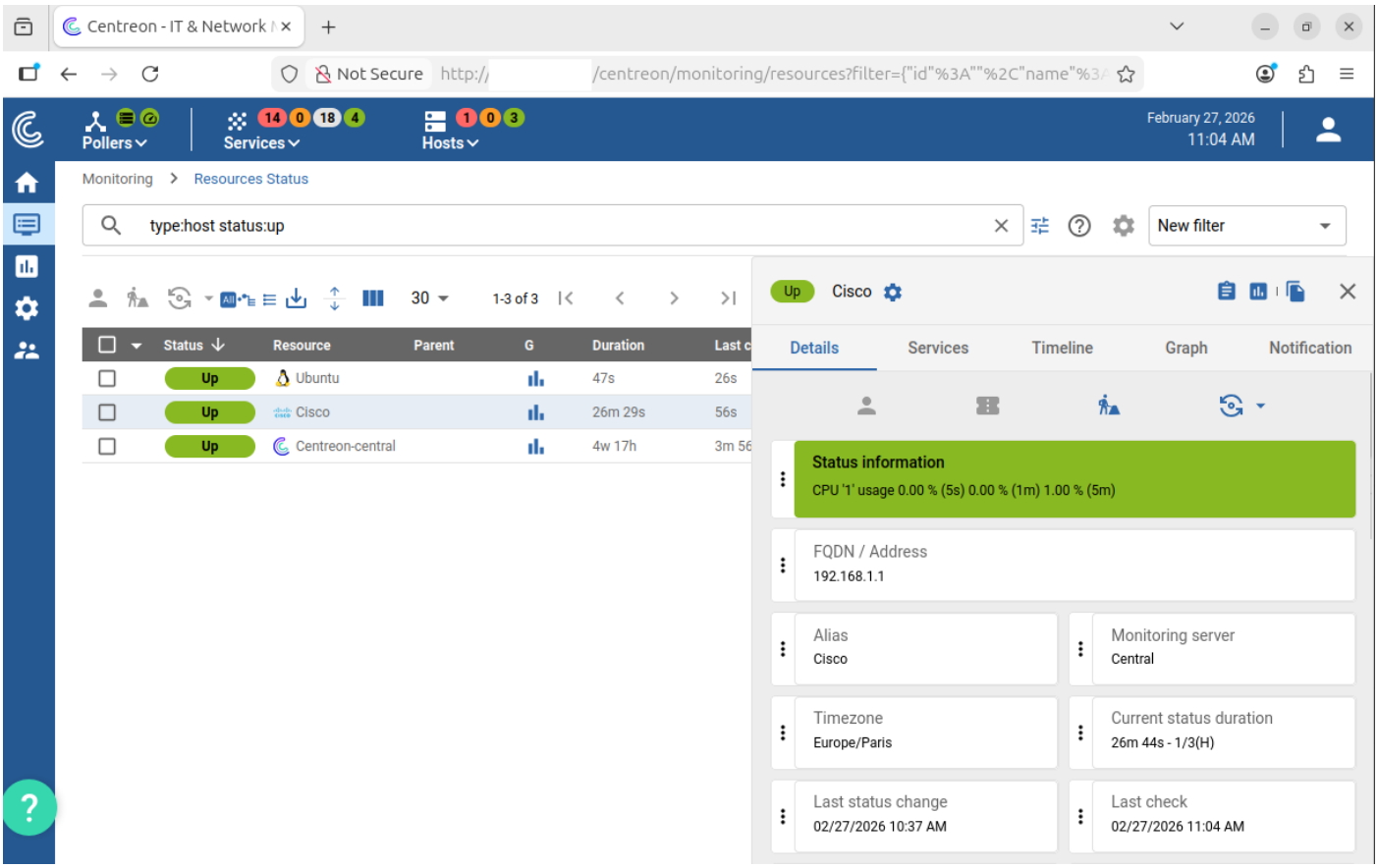


Une fois tout cela réalisé, comme précédemment, nous allons créer notre host. Cette fois ci, nous allons vérifier le CPU de notre Switch :





Une fois exporté, et avoir attendu quelques minutes, on a bien notre Switch Cisco qui remonte sur Centreon avec l'utilisation de son CPU :



6. Mise en place de Centreon sur Imprimante

Pour le test de l'imprimante, nous allons créer une interface réseau que nous laisserons cette fois ci en DHCP sur le réseau de la salle 407 :

```
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:72:24:4a brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.0.195/24 metric 1024 brd 192.168.0.255 scope global dynamic ens19
       valid_lft 82963sec preferred_lft 82963sec
    inet6 fe80::be24:11ff:fe72:244a/64 scope link
       valid_lft forever preferred_lft forever
root@ip-10-1-143-223:/etc/systemd/network#
```

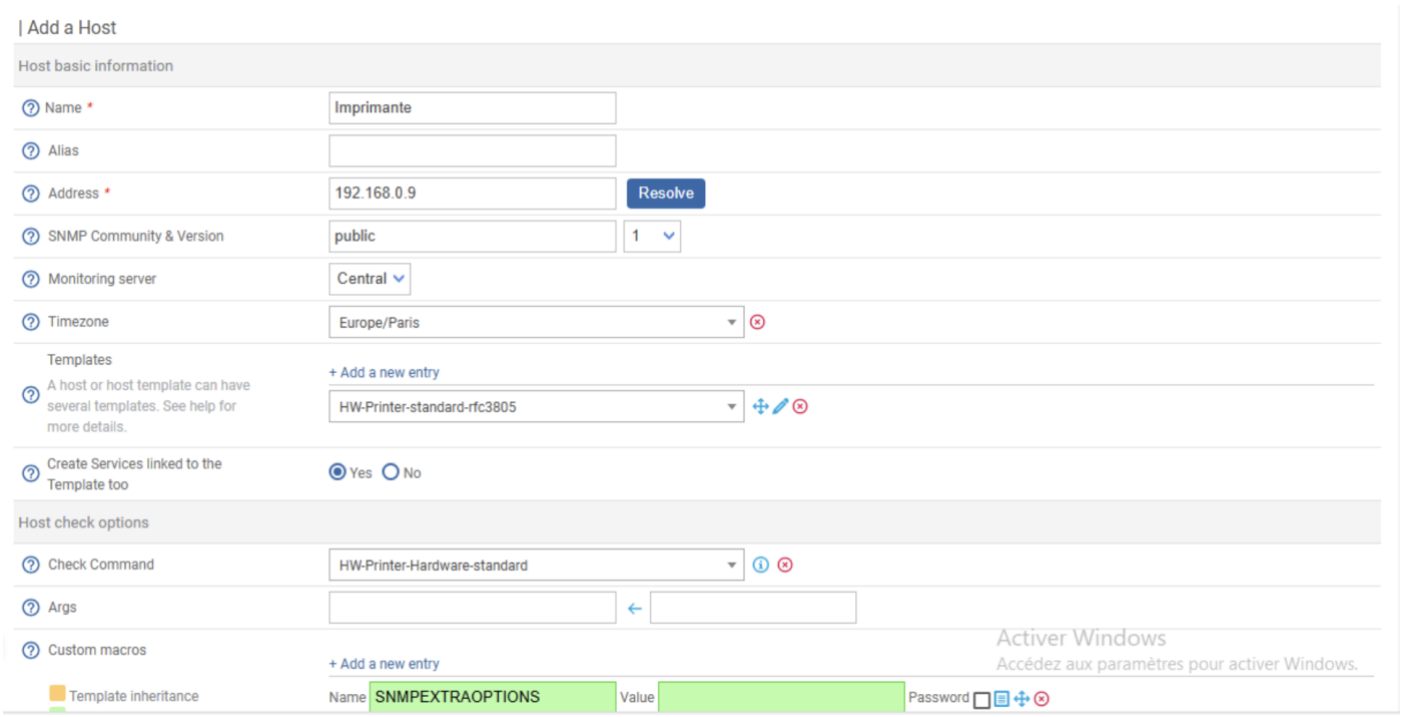
Comme pour les précédents tests, nous allons installer le plugin pour les imprimantes :

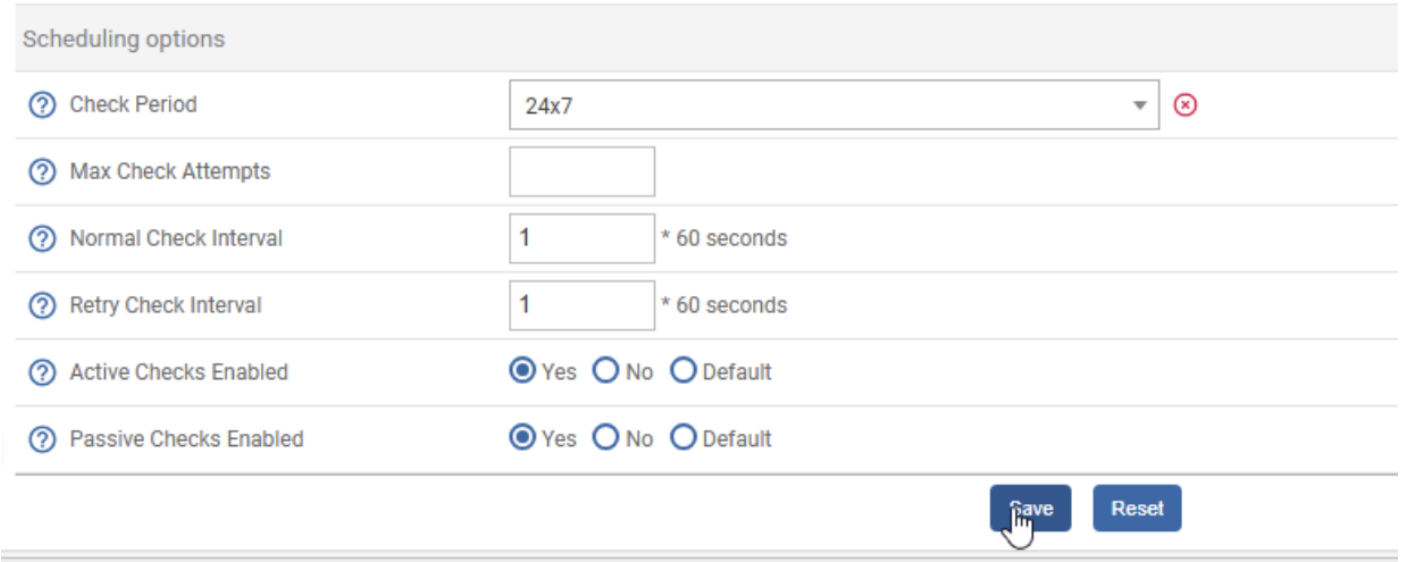
```
root@ip-10-1-143-223:/etc/systemd/network# sudo apt install centreon-plugin-hardware-printers-generic-snmp
```

Puis dans les connecteurs, nous allons ajouter le « Printer standard » :

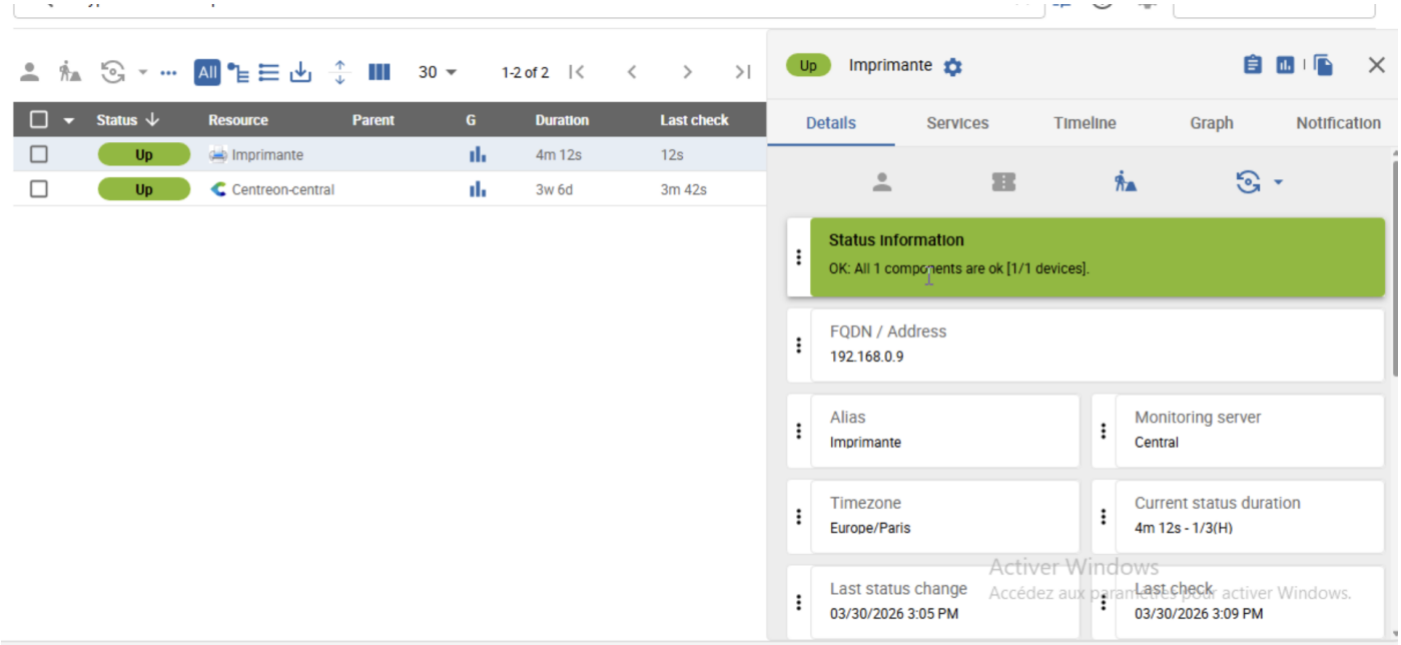


Et enfin, nous allons créer un nouvel host (attention, cette imprimante ne fonctionne qu'en version 1 de SNMP) Dans notre cas, nous allons check le hardware de notre imprimante (s'il est fonctionnel ou non) :





Et enfin, comme précédemment, nous allons sauvegarder notre configuration, patienter quelques secondes, et voir l'imprimante remonter dans nos « hosts » en ligne :

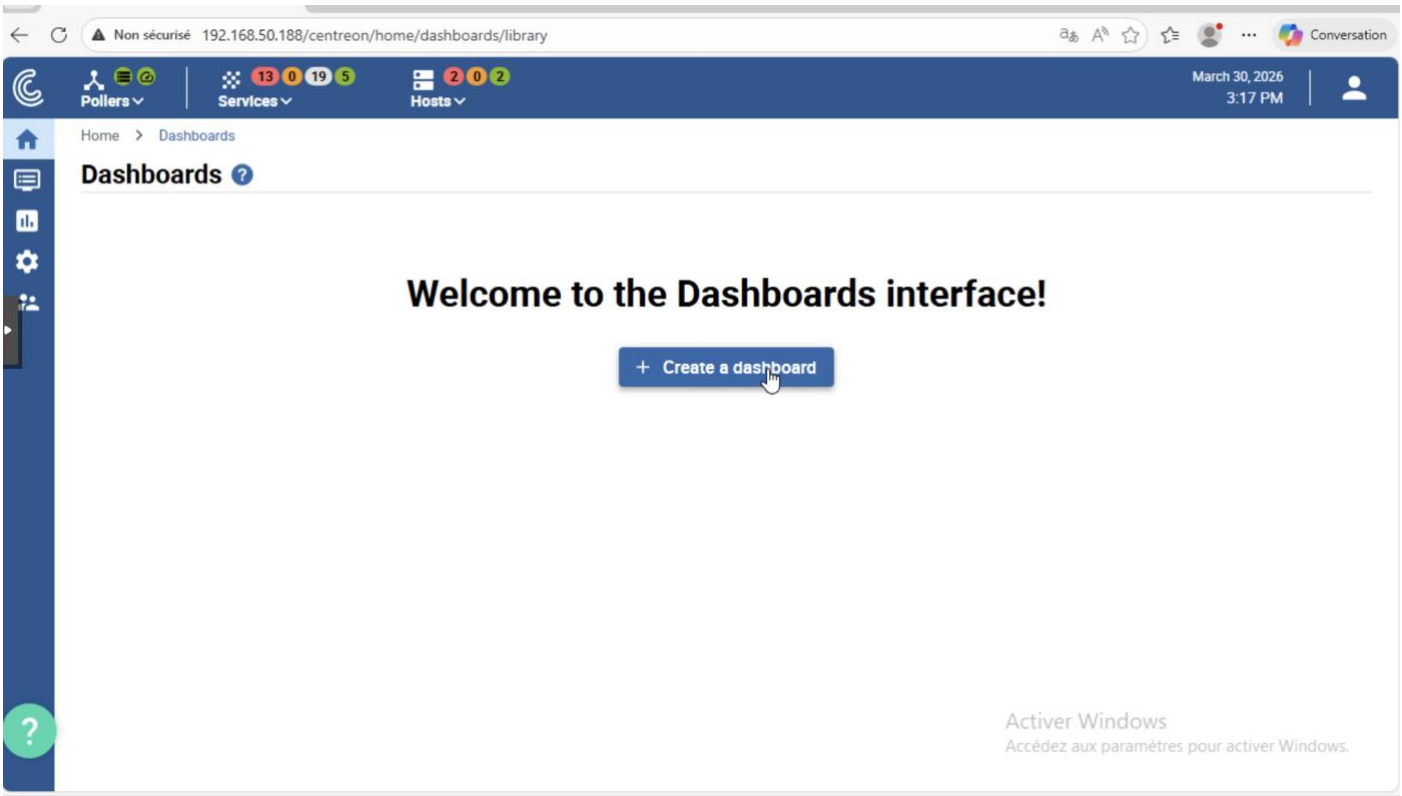


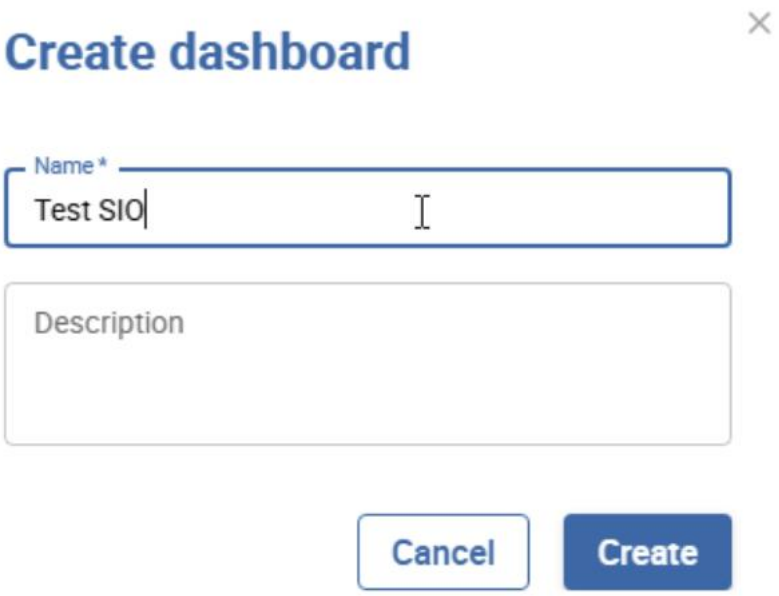
7. Création d'un dashboard

Dans cette partie, nous allons voir comment et pourquoi créer un dashboard dans Centreon.

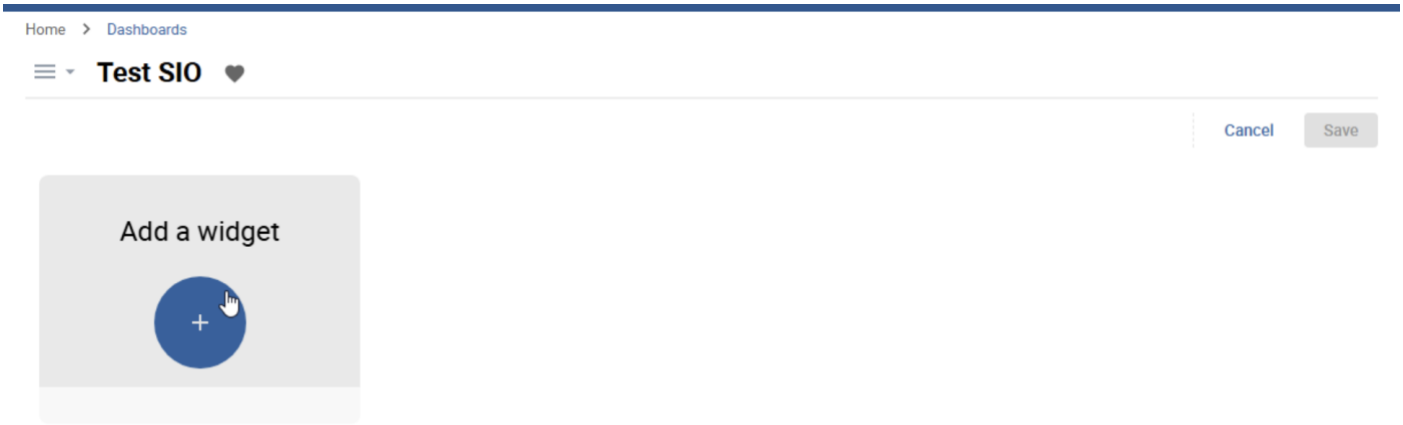
Un dashboard dans Centreon permet de centraliser et de visualiser en temps réel l'état de l'infrastructure informatique, facilitant ainsi la prise de décision et la réactivité en cas d'incident. Il offre une vue synthétique et personnalisable des différents équipements et services surveillés, ce qui permet de repérer rapidement les anomalies ou les performances dégradées. Grâce à cet outil, les équipes peuvent optimiser la gestion des ressources, améliorer la disponibilité des systèmes et garantir une meilleure qualité de service auprès des utilisateurs.

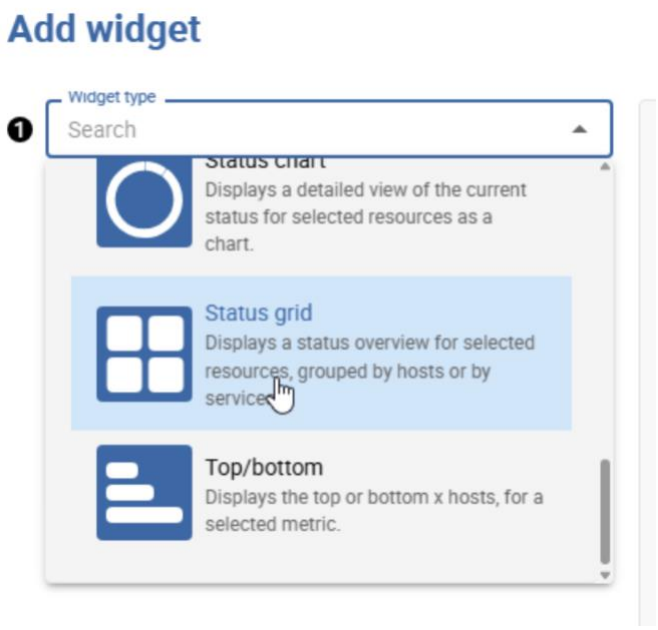
Pour cela, rendons-nous dans le premier onglet de Centreon intitulé « dashboard », puis créons en un nouveau :



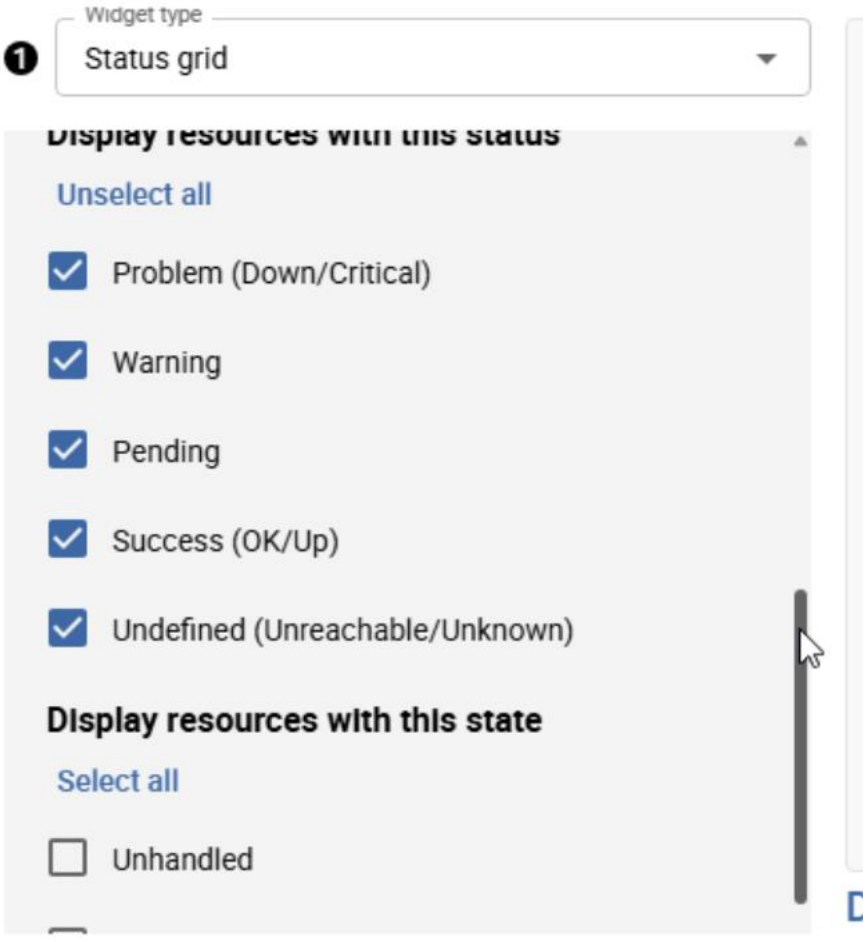


Dans ce dashboard, nous pouvons créer divers widgets, pour notre test, nous allons ajouter une grille de statuts (permettant de voir en un coup d'œil si nos appareils sont en ligne ou non) :





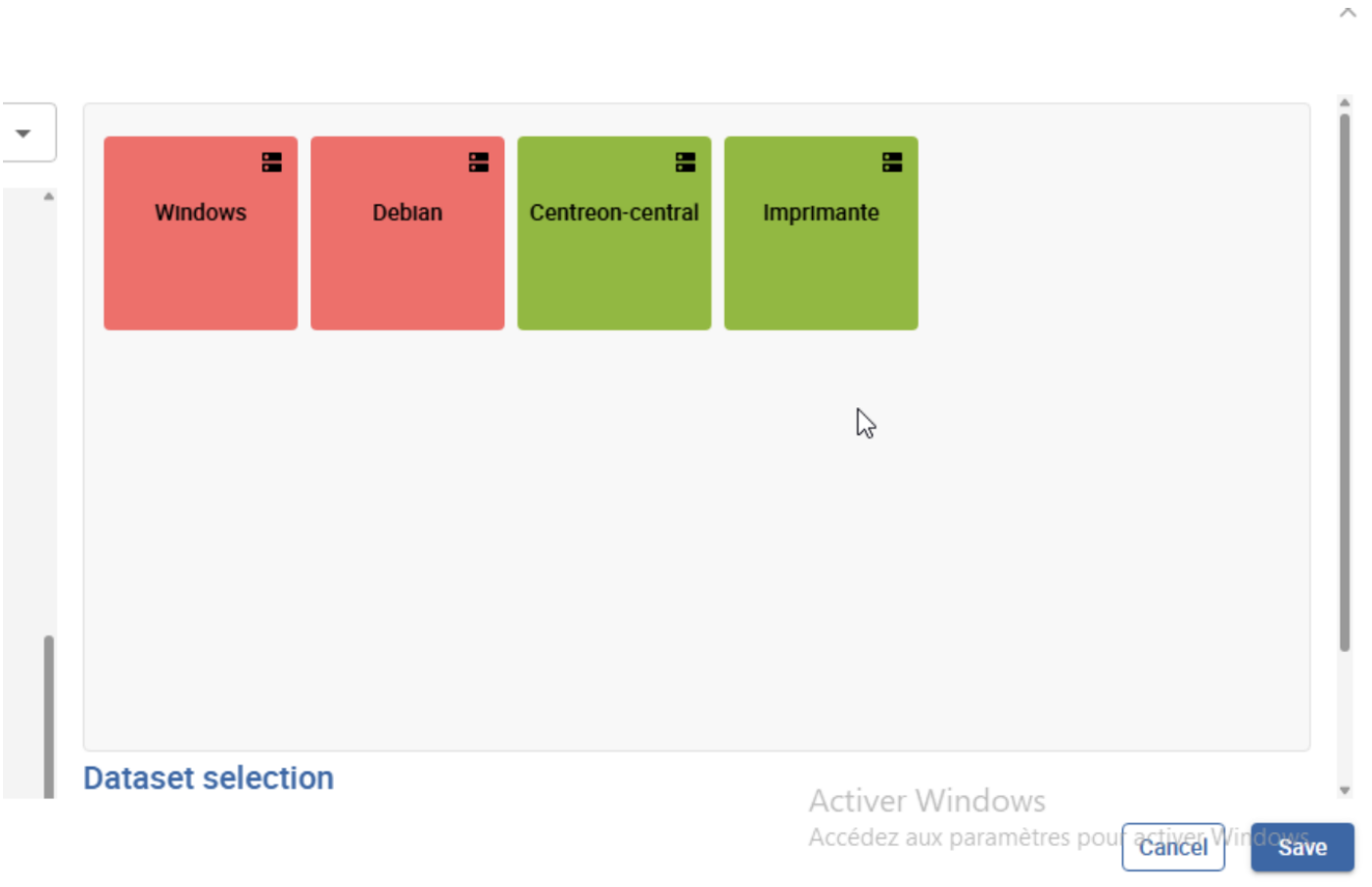
Ici, nous allons tout cocher :



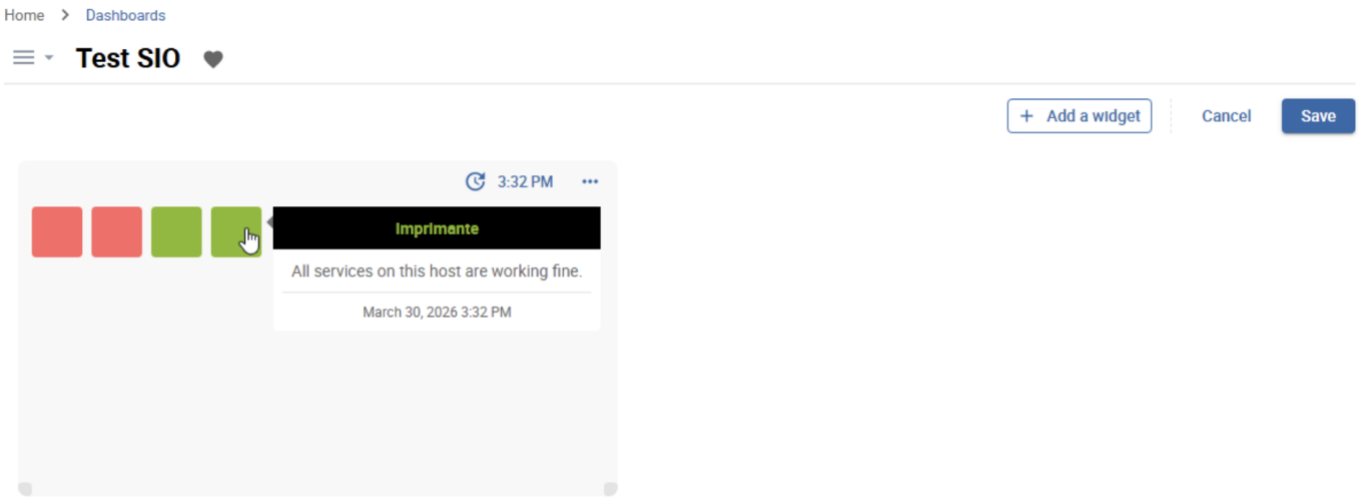
Et un peu en bas, dans « display ressources with this state », nous allons décocher tout :



Une fois ceci fait, tous nos hôtes devraient s'afficher sur notre widget :



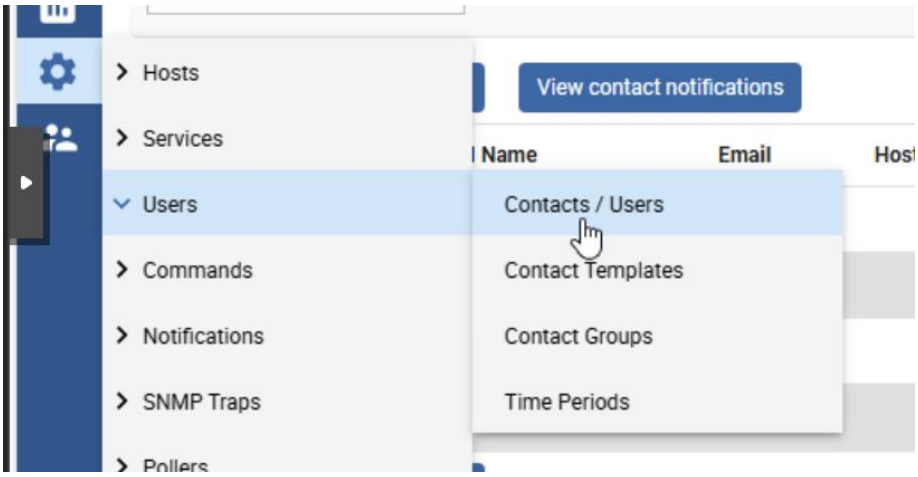
Nous pouvons sauvegarder ce que nous venons de faire (contrairement aux hosts, pas besoin de recharger la configuration ou de redémarrer quoi que ce soit !) :



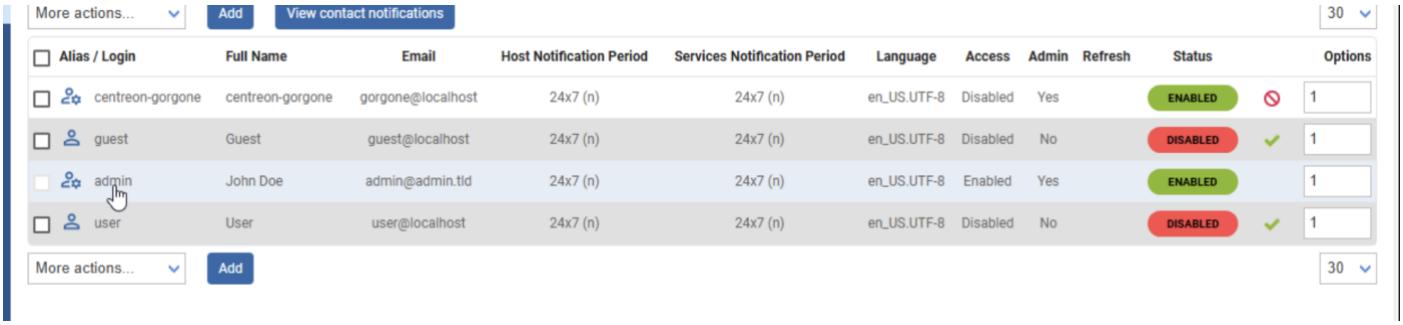
A présent, le statuts de nos hosts sont visibles d'un simple glissement de souris ! Pas besoin d'aller dans les paramètres ou dans un sous menu pour chercher notre information. Il existe bien sur d'autres façon d'afficher nos informations. Ceci est aussi applicable aux services.

8. Création d'un utilisateur et modification du mot de passe admin

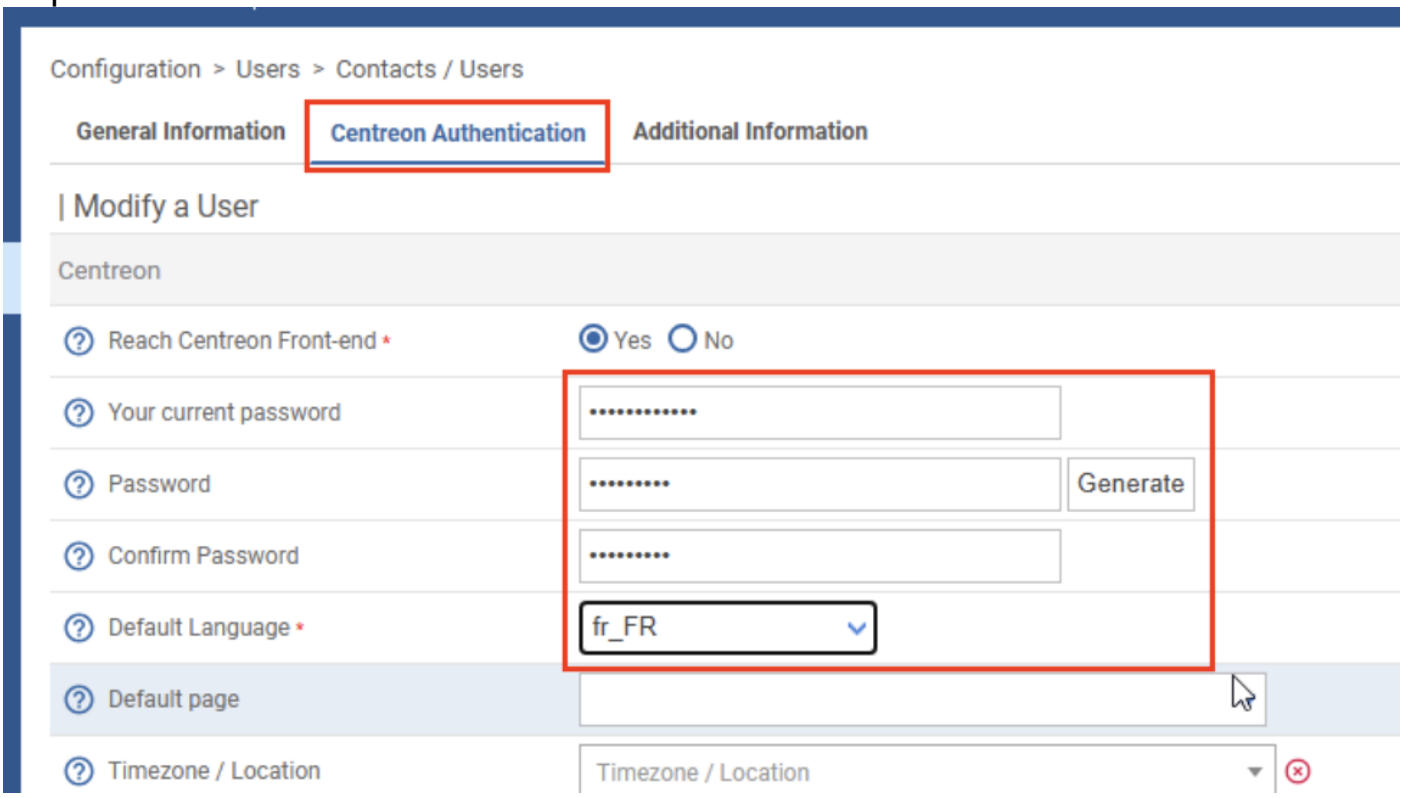
Maintenant, pour sécuriser l'accès à notre supervision, nous allons dans un premier temps modifier le mot de passe admin par défaut, puis ensuite, créer un nouvel utilisateur. Pour cela, nous allons nous rendre dans le 4ème onglet (configuration), dans « Users » puis dans « Contacts / Users » :



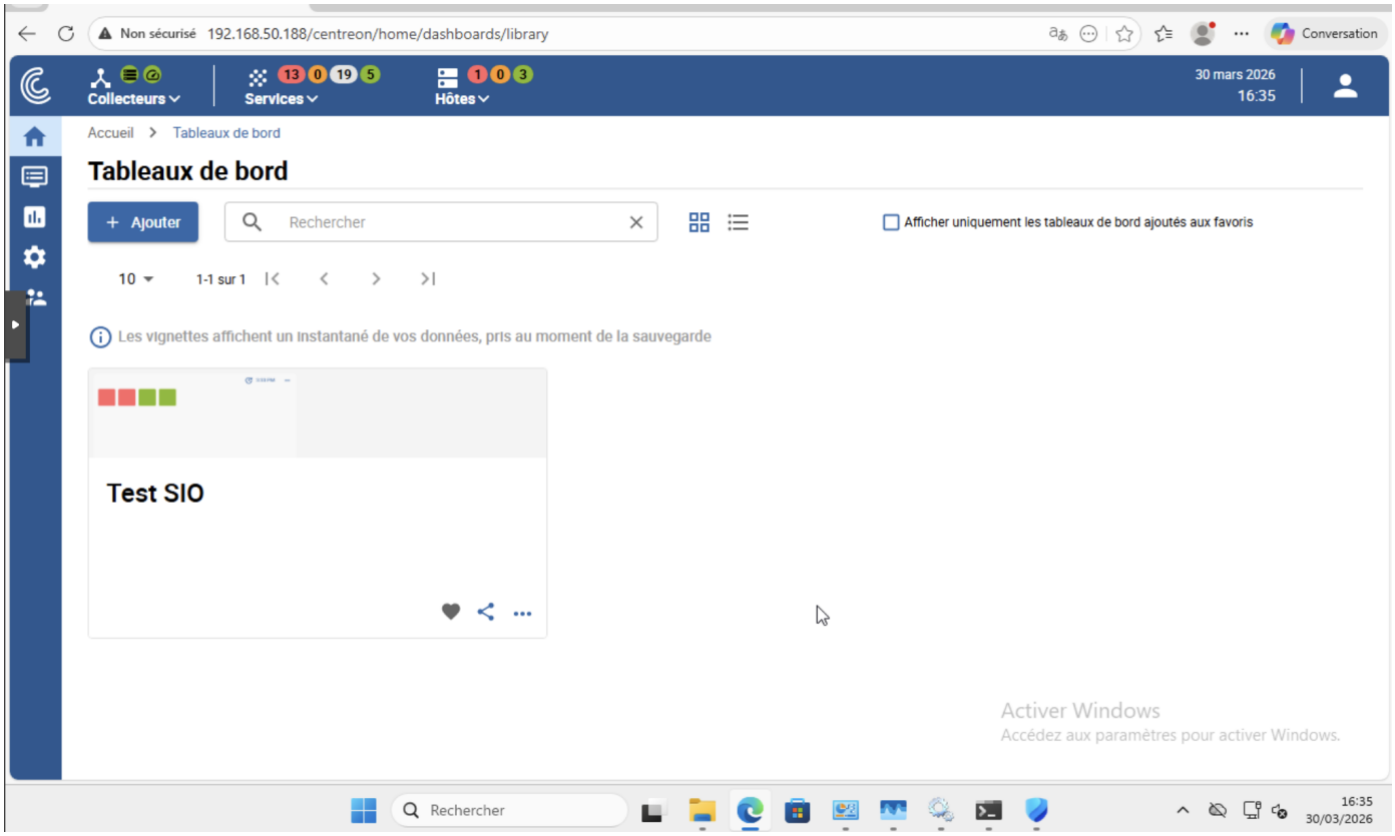
Ici, nous allons cliquer sur notre utilisateur « admin » :



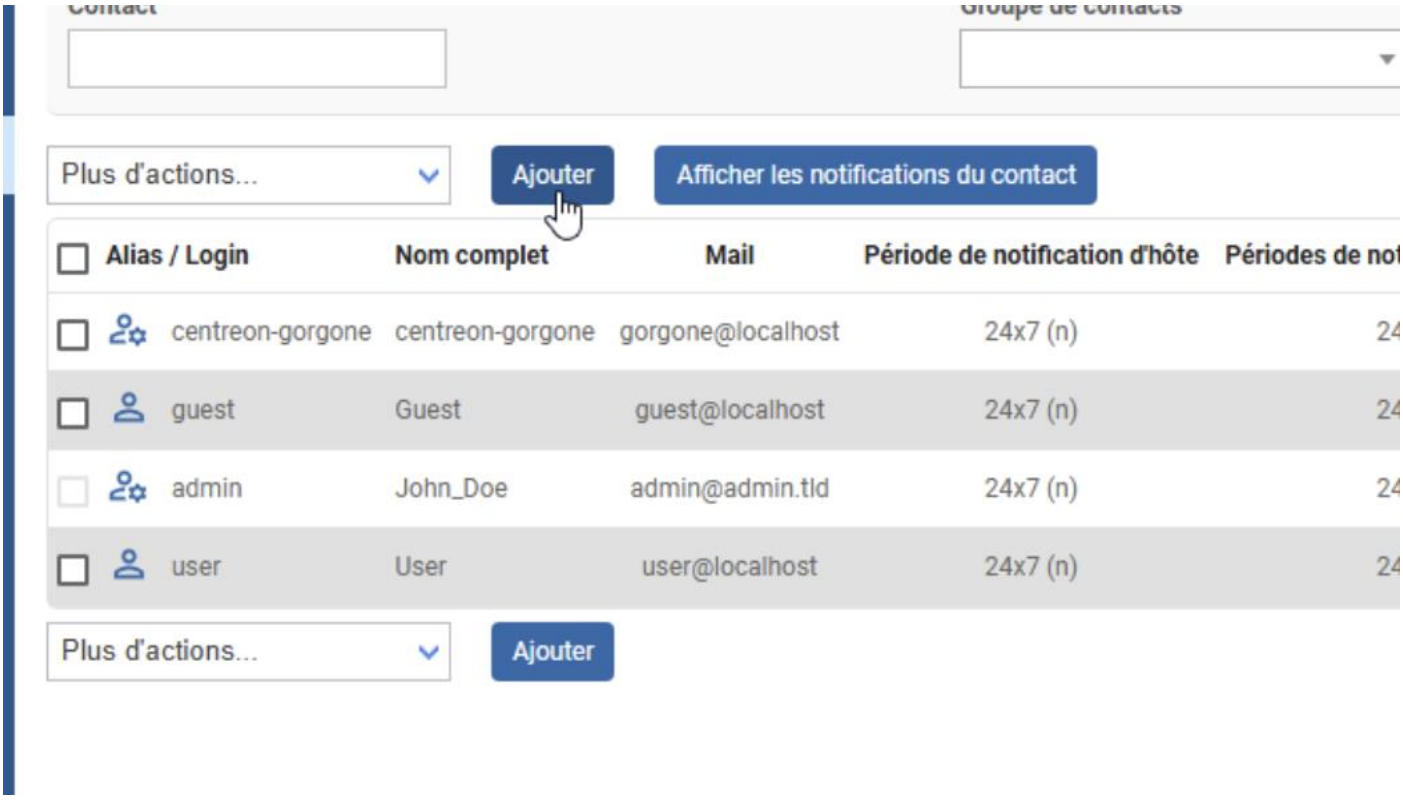
Nous allons nous rendre dans « Centreon Authentication » et changer notre mot de passe avec un nouveau mieux sécurisé (nous allons aussi en profiter pour passer la langue en français)

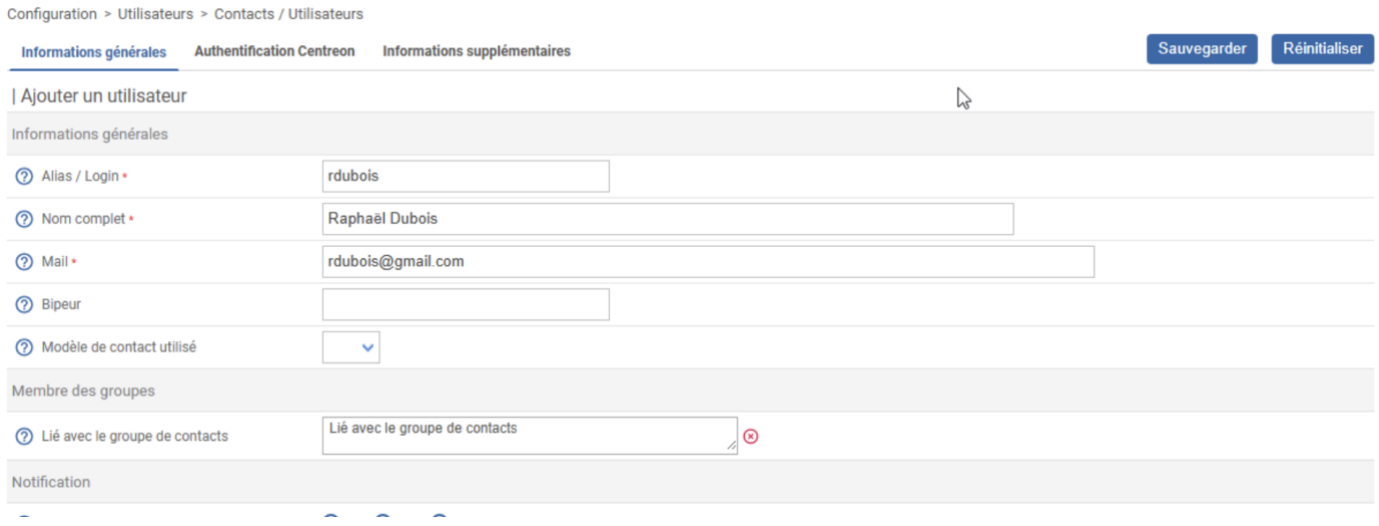


Une fois ceci fait, nous pouvons nous déconnecter, nous reconnecter avec le nouveau mot de passe et vérifier si l'interface est bien en français (ce qui est le cas !) :

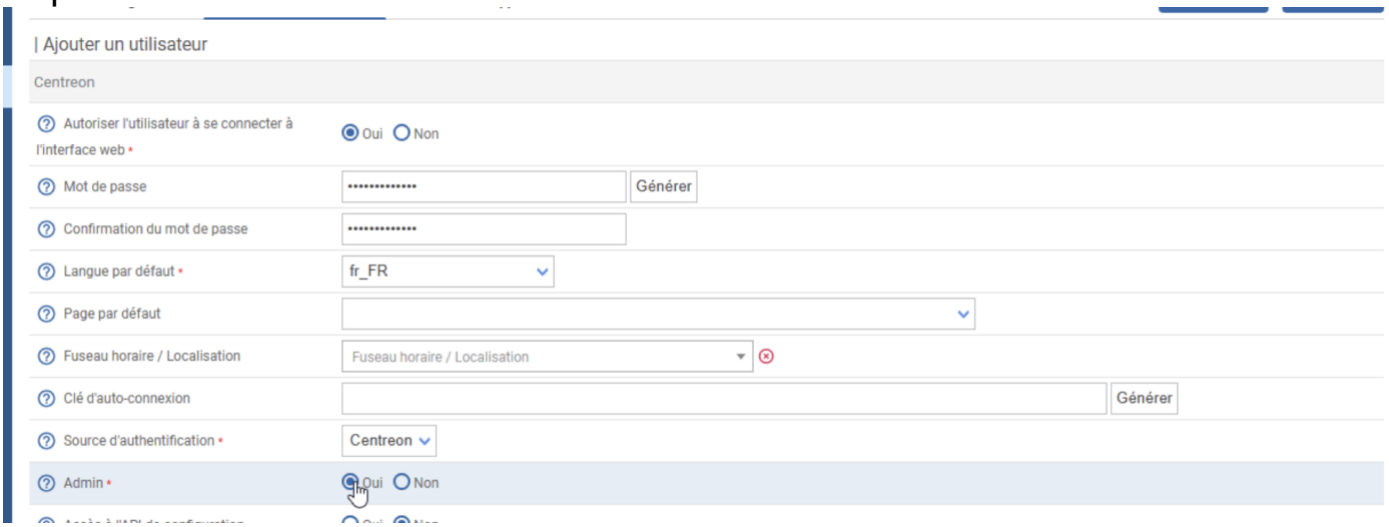


Maintenant, nous allons revenir dans le menu des utilisateurs pour cette fois ci en créer un nouveau :

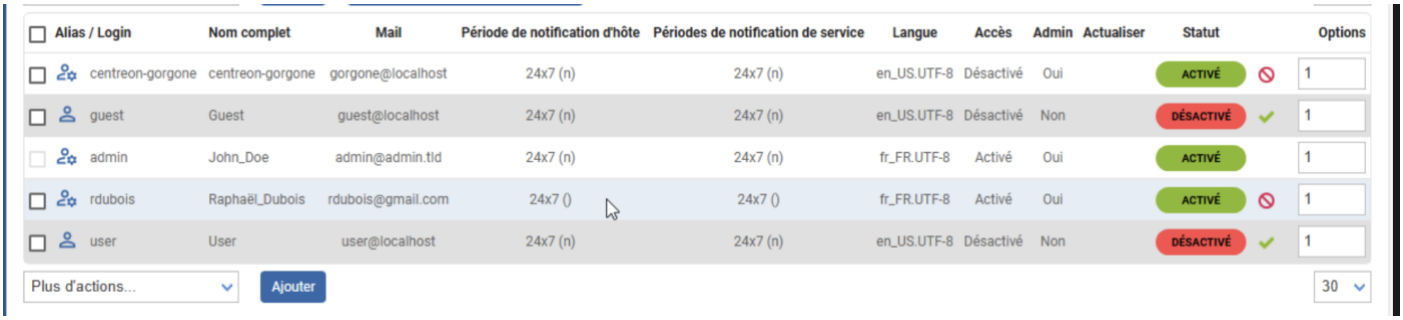




Nous pouvons définir en un clic si on souhaite que notre utilisateur possède les droits d'administrateur ou non :



Une fois les cases obligatoires remplies (avec une *), nous pouvons sauvegarder notre utilisateur et observer qu'il a bien été créer :



Maintenant, nous pouvons tenter de se connecter à cet utilisateur et observer que tout fonctionne !

