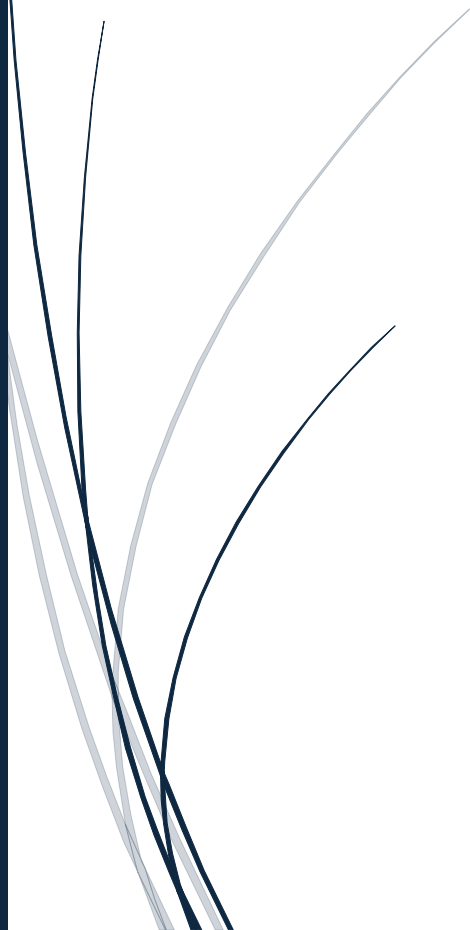




[Date]

Mise en place de l'agent SNMP – Debian – Switch Cisco



Mamadou CAMARA
[NOM DE LA SOCIETE]

Tables de matières :

1. Présentation

2. Installer le serveur SNMP sur l'hôte Debian

3. Configurer le serveur SNMP sur l'hôte Debian :

4. Supervision d'un serveur sur Centreon

4.1 Pour le serveur DNS

4.2 Pour le Switch Cisco

5. Capture des trames

6. Services Supervisés

1. Présentation

SNMP est un service (démon snmpd) qui écoute sur le **port 161 en udp** pour répondre aux requêtes issues d'un gestionnaire SNMP. L'agent comme le gestionnaire, doivent appartenir à une communauté SNMP pour échanger des informations. Par défaut le serveur SNMP définit une communauté nommé public qui autorise seulement des accès en lecture sur l'hôte lui-même (rocommunity). Il est conseillé de ne pas utiliser les noms de communauté par défaut public ou private. Sachez cependant qu'il existe des logiciels de management qui utilisent uniquement ces noms standards.

2. Installer le serveur SNMP sur l'hôte Debian

Commande :

Apt install snmpd

Afin de permettre de convertir les OID SNMP en langage clair, il faut installer **snmp-mibs-downloader** : Ce paquet logiciel ne remplit pas les conditions pour être considéré par Debian comme libre car non conforme aux DFSG (**Debian Free Software Guidelines** : Principes du logiciel libre selon Debian).

Modifiez le fichier **/etc/apt/sources.list** pour accepter des logiciels qui ne se conforment pas aux DFSG (**Debian Free Software Guidelines** : Principes du logiciel libre selon Debian) en ajoutant **contrib non-free** aux lignes suivantes des dépôts.

```
GNU nano 7.2 /etc/apt/sources.list *
deb http://deb.debian.org/debian bookworm main contrib non-free
deb http://deb.debian.org/debian bookworm-updates main contrib non-free
deb http://security.debian.org bookworm-security main contrib non-free
```

Faites une mise à jour de la liste des paquets et lancez l'installation de **snmp-mibs-downloader** :

Apt update && apt upgrade

Apt install snmp-mibs-downloader

Download-mibs

Après exécution de la commande **download-mibs**, les MIBS sont téléchargées dans le répertoire **/usr/share/mibs**.

3. Configurer le serveur SNMP sur l'hôte Debian :

Sauvegarder le fichier **/etc/snmp/snmpd.conf** créé avec l'installation

cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.orig

Modifiez le fichier de configuration **/etc/snmp/snmpd.conf** :

Autorisez le daemon à écouter sur toutes les adresses IP avec le port 161 et pas seulement sur l'adresse 127.0.0.1 et le port 161 en commentant la ligne suivante:

```
# SECTION: Access Control Setup
#
# This section defines who is allowed to talk to your running
# 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
view all included .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 public default -V all
#
# SNMPv3 doesn't use communities, but users with (optionally) an
# authentication and encryption string. This user needs to be created
# with what they can view with rouser/rwuser lines in this file.
#
# createUser username (MD5|SHA|SHA-512|SHA-384|SHA-256|SHA-224) authpassphrase [DES|AES] [privpassphrase]
# e.g.
# createUser authPrivUser SHA-512 myauthphrase AES myprivphrase
#
# This should be put into /var/lib/snmp/snmpd.conf
#
# rouser: a SNMPv3 read-only access username
# arguments: username [noauth|auth|priv [OID | -V VIEW [CONTEXT]]]
rouser authPrivUser authpriv -V systemonly
#
# include a all *.conf files in a directory
includeDir /etc/snmp/snmpd.conf.d
```

Modifiez le fichier de configuration **/etc/default/snmpd** :

Ajouter l'export de toutes les MIBS en complétant la ligne du fichier. On peut être plus sélectif, dans ce cas à la place de ALL lister les MIBS requises séparées par deux points '.'

```
export MIBS=ALL
```

Modifiez le fichier de configuration **/etc/snmp/snmpd.conf** en commentant la ligne mibs :

```
root@debian:~# service snmpd restart
```

```
# mibs
```

Vérifiez que tout ça fonctionne après avoir installé le client snmp :

```
root@debian:~# apt install snmp
root@debian:~# snmpwalk -v 2c -c public localhost system
```

Redemarr

```

root@ns0:~# snmpwalk -v 2c -c public localhost system
SNMPv2-MIB::sysDescr.0 = STRING: Linux ns0 6.5.11-7-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.11-7 (2023-12-05T09:44z) x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (184236) 0:30:42.36
SNMPv2-MIB::sysContact.0 = STRING: Me <me@example.org>
SNMPv2-MIB::sysName.0 = STRING: ns0
SNMPv2-MIB::sysLocation.0 = STRING: Sitting on the Dock of the Bay
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (33) 0:00:00.33
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: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (33) 0:00:00.33
SNMPv2-MIB::sysORUpTime.10 = Timeticks: (33) 0:00:00.33
root@ns0:~#

```

4. Supervision d'un serveur sur Centreon

4.1 Pour le serveur DNS

Dans **Configuration/Hôtes/Hotes**

Surveillance > Statut des ressources ?

type:host status:up

Nouveau filtre

Hôtes

- Hôtes
- Groupes d'hôtes
- Modèles
- Catégories
- Découverte
- résolution dns
- DHCP
- Centreon

G	Durée	Dernière vérification	Information	Essai
	2W 4d	3 min 42 s	OK : Tous les servi...	1/3 (H)
	2w 6d	1m 14s	OK - 172.16.31.254...	1/3 (H)
	3W 5d	3 min 14 s	OK - 172.16.11.10 :...	1/3 (H)
	3W 5d	4 min 10 s	OK - 192.168.31.20...	1/3 (H)
	3W 5d	4m 42s	OK - 192.168.31.20...	1/3 (H)
	3w 6d	2m 14s	OK - 172.16.31.10 :...	1/3 (H)
	1M 2w	2m 42s	OK - 127.0.0.1 : rta ...	1/3 (H)

172.16.31.25/centreon/main.php?p=60101

- On clique sur Ajouter

Configuration > Hosts

Name	Hostgroup	Poller

More actions... [Add](#)

Ensuite, on complète les lignes suivantes :

6 janvier 2025 09:56

Name * ns0

Alias

Address * 172.16.11.10 [Resolve](#)

SNMP Community & Version public 2c

Monitoring server Central

Timezone Europe/Paris

Templates

+ Add a new entry

App-Protocol-DNS-custom

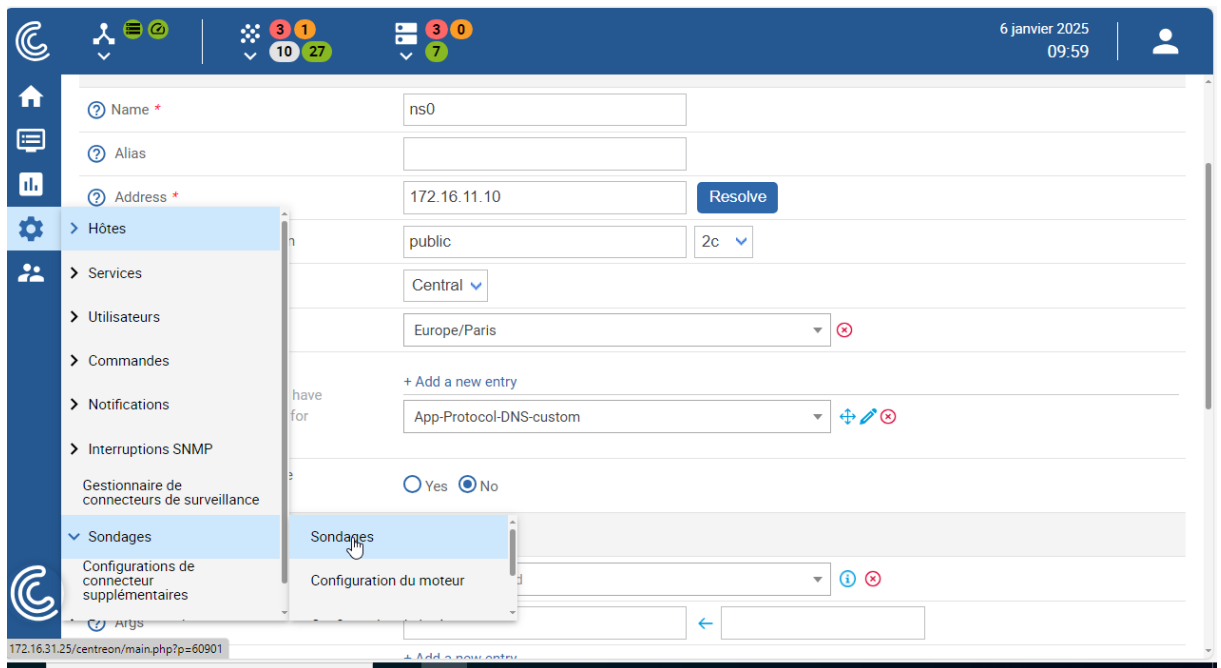
Create Services linked to the Template too ☐ Yes ☒ No

Host check options

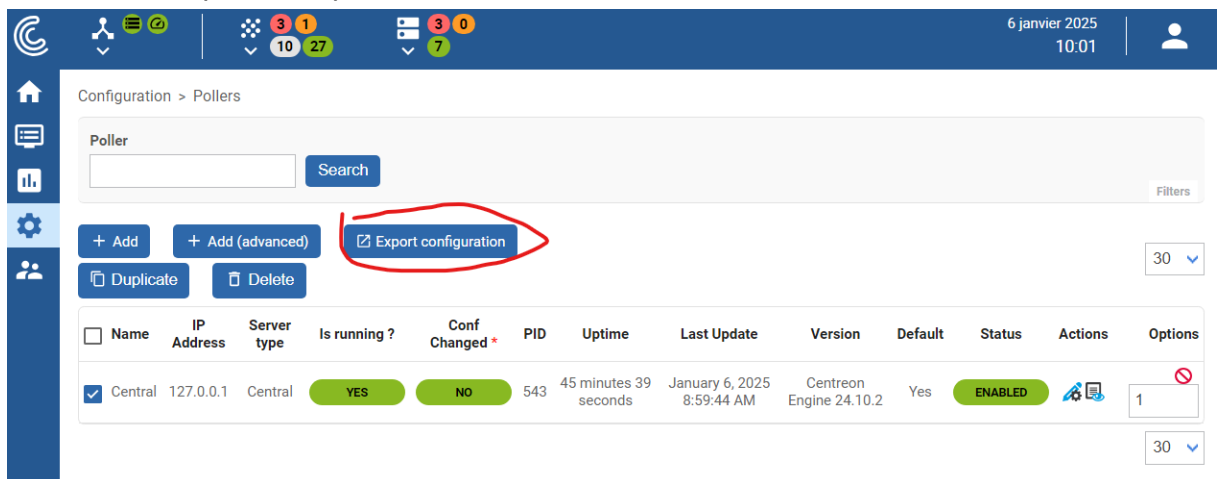
Check Command Check Command

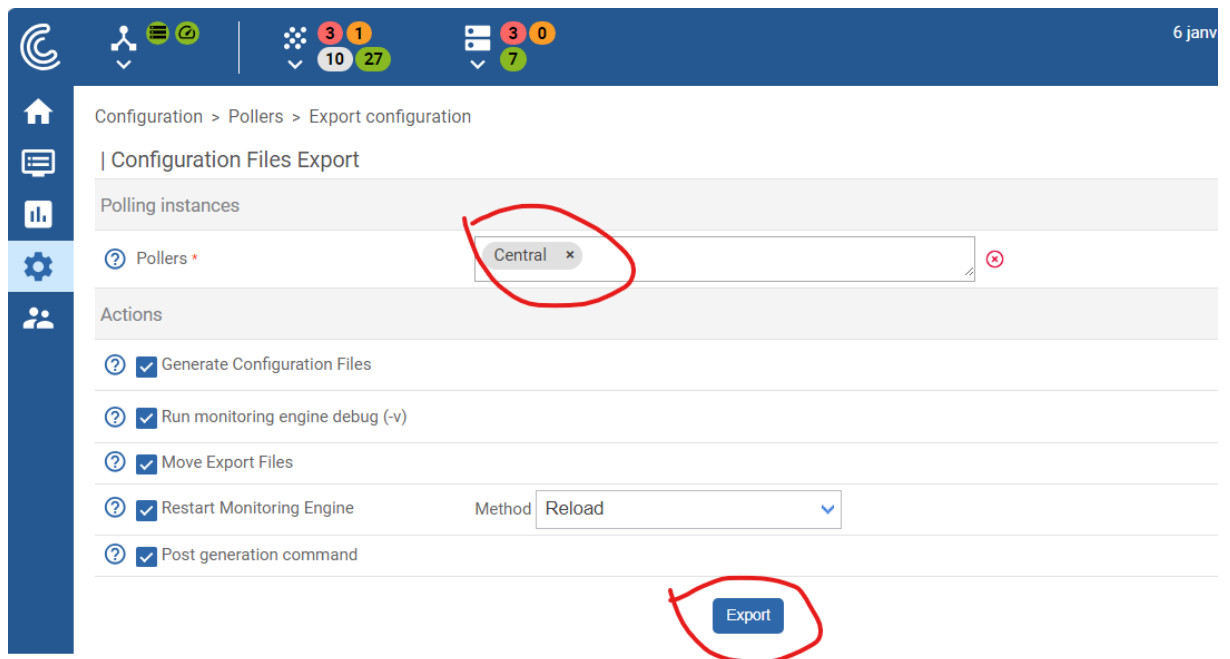
Args

- Ensuite, on exporte la configuration
Pour cela, on va dans **Configuration/Sondages**



Ensuite on clique sur exporter

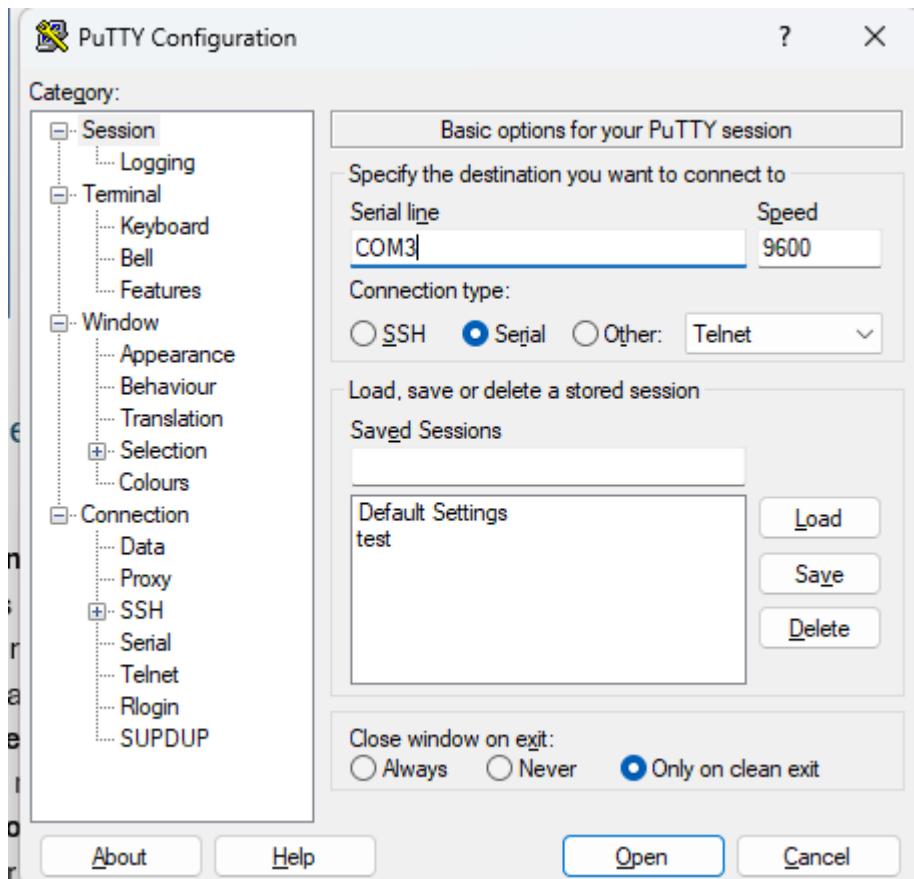




4.2 Pour le Switch Cisco

Connectez-vous à votre switch Cisco

Vous pouvez vous connecter **au terminal** de votre switch Cisco par **Telnet**, **SSH**, ou simplement via le **câble console**. Suivant votre configuration il peut vous être demandé un login et un mot de passe.



Entrez dans le mode « enable »

Pour modifier la configuration d'un **équipement Cisco**, il vous faut être dans le **mode privilégié** « enable ». Pour entrer en mode « enable », il vous suffit de taper la commande *enable*, puis d'entrer le **mot de passe** qui vous sera demandé.

Entrez dans le mode « configuration »

Pour pouvoir configurer votre équipement Cisco, il vous faut être dans le **mode « configuration »**. Entrez simplement la commande :

Configuration terminal

Création d'une adresse virtuelle sur le VLAN serveur

Conf t

Interface vlan 347

Ip address 172.16.31.250 255.255.255.0

No shutdown

Parmi les informations, vous pouvez voir les **communautés activées** avec le **mode d'activation** (RW: Read-Write et RO: Read Only)

Activation de la communauté public et privée :

snmp-server community public RO
snmp-server community private RW

Choisissez la destination et la communauté

Vous devez maintenant définir l'adresse de destination, ainsi que la communauté pour l'envoi des traps SNMP. Afin que SmartReport supervise votre switch Cisco, il vous faut entrer son adresse IP et configurer l'envoi pour la communauté public. Entrez alors cette ligne:

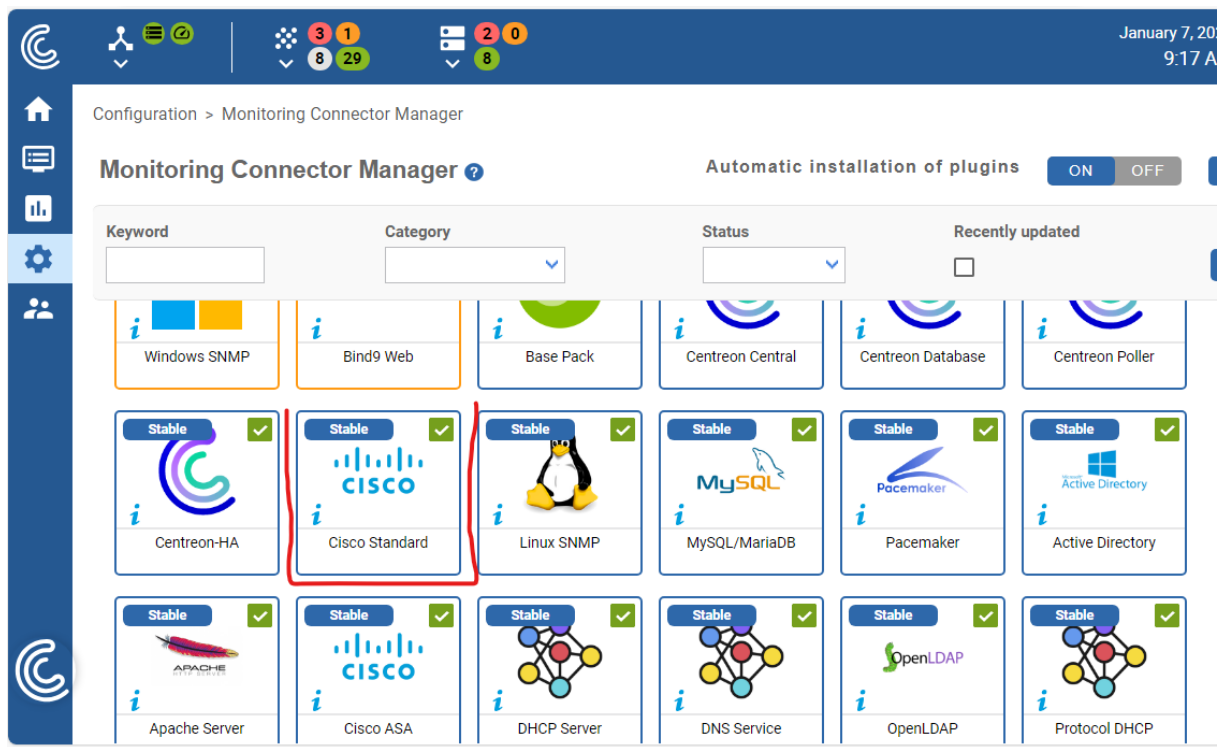
snmp-server host 172.16.31.25 public

NB : 172.16.3.25 est l'adresse du serveur Centreon

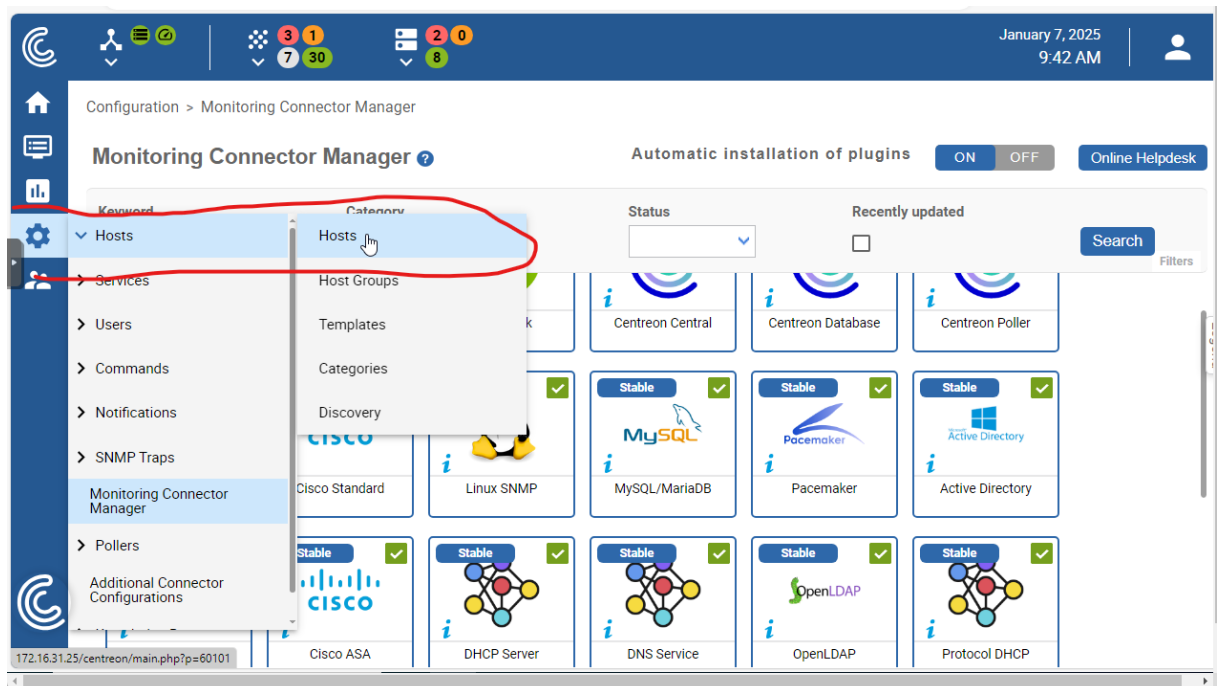
Configuration finale :

```
!  
interface Vlan347  
 ip address 172.16.31.250 255.255.255.0  
!  
interface Vlan348  
 no ip address  
!  
ip classless  
ip http server  
ip http secure-server  
!  
ip sla enable reaction-alerts  
snmp-server community public RO  
snmp-server community private RW  
snmp-server host 172.16.31.25 public  
!  
banner motd ^CAccess autorise pour les etudiants et enseignant du BTS SIO seulem  
ent !^C  
!  
line con 0  
 password 7 130E160B0E1F  
 login  
line vty 0 4  
 login  
line vty 5 15  
 login  
!  
end  
  
Switch-AgenceK#
```

Pour superviser le Switch, on active, sur le serveur Centreon, le plugin Cisco dans **Configuration/Monitoring Connector manager**



Ensuite, dans **Configuration/Hôtes**



On crée un hôte pour le Switch Cisco,

? Name * Switch-cisco
 ? Alias
 ? Address * 172.16.31.250 Resolve
 ? SNMP Community & Version 2c
 ? Monitoring server Central
 ? Timezone Europe/Paris
 Templates
 ? A host or host template can have several templates. See help for more details. + Add a new entry
 Net-Cisco-Standard-SNMP-custom
 ? Create Services linked to the Template too ☐ Yes ☒ No
 Host check options
 ? Check Command Check Command
 ? Args
 + Add a new entry

Ensuite, on exporte la configuration

Configuration > Pollers

Search

Export configuration

Is running ?	Conf Changed *	PID	Uptime	Last Update	Version	Default	Status
YES	NO	458	1 hours 17 minutes	January 7, 2025 8:47:05 AM	Centreon Engine 24.10.2	Yes	ENABLED

groups, hosts and hostgroups are taken in account in order to calculate this status. If you modify a template, it won't tell y

Pollers
 Engine configuration

Ainsi, on peut visualiser les services créés :

Monitoring > Resources Status ?

Search: type:host status:up

Resources Status

Status	Resource	Parent	G
Up	Switch-cisco		
Up	WIN2022		
Up	SNS-Pare-feu		
Up	ns0		
Up	dns0		
Up	dns-resolve		
Up	DHCP		
Up	Centreon		

Switch-cisco

Details Services Timeline Graph Notification

Cpu

OK: 1 CPU(s) average usage is 15.00 % (5s) 6.00 % (1m) 6.00 % (5m) - 33m 7s

Environment

OK: All 2 components are ok [1/1 fans, 1/1 psus]. 31m 31s

Memory

OK: All memories are ok 34m 54s

5. Capture des trames

Capture en cours de Instance Ethernet 0

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

snmp

No.	Time	Source	Destination	Protocol	Length	Info
1449	161.090851	172.16.31.25	172.16.31.19	SNMP	88	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.2
1451	161.094135	172.16.31.19	172.16.31.25	SNMP	705	get-response 1.3.6.1.4.1.77.1.2.3.1.2.7.83.101.114.118.101.117.114 1.3.6.1.4.1.77.1.2.3.1.2.7.83.12...
1452	161.095937	172.16.31.25	172.16.31.19	SNMP	125	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.2.3.4.65.112.112.101.108.32.100.101.32.112.114.111.99.195.169...
1455	161.096576	172.16.31.19	172.16.31.25	SNMP	88	get-response 1.3.6.1.4.1.77.1.2.3.1.2.3.4.83.101.114.118.105.99.101.32.100.101.32.99.97.99.104.101.3...
1456	161.099049	172.16.31.25	172.16.31.19	SNMP	102	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.3.13.84.101.109.112.115.32.87.105.110.100.111.119.115
1458	161.099619	172.16.31.19	172.16.31.25	SNMP	1030	get-response 1.3.6.1.4.1.77.1.2.3.1.3.14.66.97.108.108.111.111.110.83.101.114.118.105.99.101.3.6...
1459	161.101745	172.16.31.25	172.16.31.19	SNMP	131	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.3.40.67.101.110.116.114.101.32.100.101.32.100.105.115.116.114...
1461	161.102250	172.16.31.19	172.16.31.25	SNMP	1347	get-response 1.3.6.1.4.1.77.1.2.3.1.3.40.83.101.114.118.101.117.114.32.71.101.115.116.105.111.110.1...
2817	461.408415	172.16.31.25	172.16.31.19	SNMP	88	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.2
2819	461.415116	172.16.31.19	172.16.31.25	SNMP	685	get-response 1.3.6.1.4.1.77.1.2.3.1.2.7.83.101.114.118.101.117.114 1.3.6.1.4.1.77.1.2.3.1.2.7.83.12...
2820	461.416906	172.16.31.25	172.16.31.19	SNMP	125	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.2.3.4.65.112.112.101.108.32.100.101.32.112.114.111.99.195.169...
2823	461.417620	172.16.31.19	172.16.31.25	SNMP	62	get-response 1.3.6.1.4.1.77.1.2.3.1.2.3.4.83.101.114.118.105.99.101.32.100.101.32.99.97.99.104.101.3...
2824	461.421172	172.16.31.25	172.16.31.19	SNMP	103	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.3.14.66.97.108.108.111.111.110.83.101.114.118.105.99.101...
2826	461.421840	172.16.31.19	172.16.31.25	SNMP	1042	get-response 1.3.6.1.4.1.77.1.2.3.1.3.14.68.105.115.113.117.101.32.118.105.114.116.117.101.108.1.3...
2827	461.424222	172.16.31.25	172.16.31.19	SNMP	135	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.3.40.83.101.114.118.105.99.101.32.66.114.111.107.101.114.32.1...
2829	461.424937	172.16.31.19	172.16.31.25	SNMP	1301	get-response 1.3.6.1.4.1.77.1.2.3.1.3.41.67.111.111.114.100.105.110.97.116.101.117.114.32.100.101.3...
3911	761.643924	172.16.31.25	172.16.31.19	SNMP	88	getBulkRequest 1.3.6.1.4.1.77.1.2.3.1.2

> Frame 1451: 705 bytes on wire (5640 bits), 705 bytes captured (5640 bits) on interface
> Ethernet II, Src: ProxmoxServe_f3:10:40 (bc:24:11:f3:10:40), Dst: ProxmoxServe_18:f2:
> Internet Protocol Version 4, Src: 172.16.31.19, Dst: 172.16.31.25
> User Datagram Protocol, Src Port: 161, Dst Port: 60665
> Simple Network Management Protocol
 version: v2c (1)
 community: public
 data: get-response (2)
 get-response
 request-id: 1062143906
 error-status: noError (0)
 error-index: 0
 variable-bindings: 50 items
 1.3.6.1.4.1.77.1.2.3.1.2.7.83.101.114.118.101.117.114: 4
 Object Name: 1.3.6.1.4.1.77.1.2.3.1.2.7.83.101.114.118.101.117.114 (isc
 Value (Integer32): 4
 1.3.6.1.4.1.77.1.2.3.1.2.7.83.121.115.77.97.105.110: 4
 1.3.6.1.4.1.77.1.2.3.1.2.7.84.104.195.168.109.101.115: 4

0000 bc 24 11 18 f2 7f bc 24 11 f3 10 40 08 00 45 00 ...\$.....\$...@...E-
0010 02 b3 79 fd 00 b9 80 11 00 00 ac 10 1f 13 ac 10 ...y.....
0020 1f 19 01 02 03 01 02 1d 53 65 72 76 69 63 65 20 Service
0030 64 65 20 70 72 6f 66 69 6c 20 75 74 69 6c 69 73 ...de profil utilis
0040 61 74 65 75 72 02 01 04 30 2e 06 29 2b 06 01 04 ...ateur... 0.)....
0050 01 4d 01 02 03 01 02 1d 53 65 72 76 69 63 65 73 ...M..... Services
0060 20 57 65 62 20 41 63 74 69 76 65 20 44 69 72 65 ...Web Act ive Dire
0070 63 74 6f 72 79 02 01 04 30 37 06 32 2b 06 01 04 ...ctory... 07-2...
0080 01 4d 01 02 03 01 02 1d 53 79 73 74 81 43 81 28 ...M..... Syst-C:(
0090 6d 65 20 64 81 62 81 00 81 19 81 43 81 29 76 81 ...me d-b... (C)...
00a0 43 81 29 6e 65 6d 65 6e 74 20 43 4f 4d 2b 02 01 ...C...)nemen t COM+...
00b0 04 30 31 06 2c 2b 06 01 04 01 4d 01 02 03 01 02 ...01,+... M.....
00c0 1e 43 6c 69 65 6e 74 20 64 65 20 73 74 72 61 74 ...Client de strat
00d0 81 43 81 29 67 69 65 20 64 65 20 67 72 6f 75 70 ...C...)gie de group
00e0 65 02 01 04 30 2f 06 2a 2b 06 01 04 01 4d 01 02 ...e...0/* +...M...
00f0 03 01 02 1e 47 65 73 74 69 6f 6e 6e 61 69 72 65 ...Gest ionnaire
0100 20 64 65 20 73 65 73 73 69 6f 6e 20 6c 6f 63 61 ...de sess ion loca
0110 6c 65 02 01 04 30 32 06 2d 2b 06 01 04 01 4d 01 ...le...02+...M...
0120 02 03 01 02 1f 53 65 72 76 69 63 65 20 64 65 20 ...Ser vice de

Frame (705 bytes) Reassembled IPv4 (2151 bytes)

Packets: 17054 Affichés: 56 (0.5%) Profil: Default

6. Services Supervisés

Monitoring > Resources Status

type:host status:up

January 6, 2025 10:46 AM

Status	Resource	Parent	G	Duration	Last check	Information	Tries
Up	WIN2022			2w 4d	4m 35s	OK: All services are ok	1/3 (H)
Up	SNS-Pare-feu			3w 20m	2m 8s	OK - 172.16.31.254: rta 0.32...	1/3 (H)
Up	ns0			3w 6d	4m 7s	OK - 172.16.11.10: rta 0.759...	1/3 (H)
Up	dns0			3w 6d	5m 4s	OK - 192.168.31.20: rta 0.40...	1/3 (H)
Up	dns-resolve			3w 6d	36s	OK - 192.168.31.20: rta 1.23...	1/3 (H)
Up	DHCP			3w 6d	3m 8s	OK - 172.16.31.10: rta 0.099...	1/3 (H)
Up	Centreon			1M 2w	3m 36s	OK - 127.0.0.1: rta 0.049ms, ...	1/3 (H)

The screenshot shows the Nagios XI 'Resources Status' page. The top navigation bar includes the Nagios logo, a list of icons with status counts (3 critical, 1 warning, 10 OK, 27 pending), and the date/time 'January 6, 2025 10:48 AM'. The breadcrumb trail is 'Monitoring > Resources Status'. A search bar contains the query 'type:host state:unhandled status:down'. Below the search bar, there are icons for user, group, refresh, and a list of resources. The main table displays the status of three resources, all of which are 'Down'.

☐	Status	Resource	Parent	G	Duration	Last check	Information	Tries
☐	Down	LDAP			1h 32m	1m 36s	CRITICAL - 172.16.31.20: Ho...	1/3 (H)
☐	Down	Apache2			1h 33m	2m 6s	CRITICAL - 172.16.31.253: H...	1/3 (H)
☐	Down	Switch-cisco			2w 4d	4m 58s	CRITICAL - 172.16.31.250: H...	1/3 (H)

- Supervision physique des serveurs Linux (ping, cpu, mémoire, ...)
- Supervision physique du serveur Windows 2022
- Supervision pare feu SNS
- Supervision Switch Cisco
- Supervision Apache2
- Supervision DNS (résolveur)
- Supervision DHCP
- Supervision BD