DOCUMENTATION
PROJET AP

STORMSHIELD

VALENTIN, THEO

BTS SIO 2024-2025

SOMMAIRE

Plan d’adressage

ID VLAN	Adresses de sous-réseaux	Adresses IP de votre firewall Stormshield
330	**DMZ :** 172.16.7.0/24	**dmz :** 172.16.7.254
331	**SERVEURS :** 172.16.27.0/24	**dmz :** 172.16.27.254
332	**LAN 1 :** 192.168.7.0/24	**in/lan1 :** 192.168.7.254
333	**LAN 2 :** 192.168.27.0/24	**lan2 :** 192.168.27.254
302	**WAN :** 192.168.229.0/26	**out :** 192.168.229.24

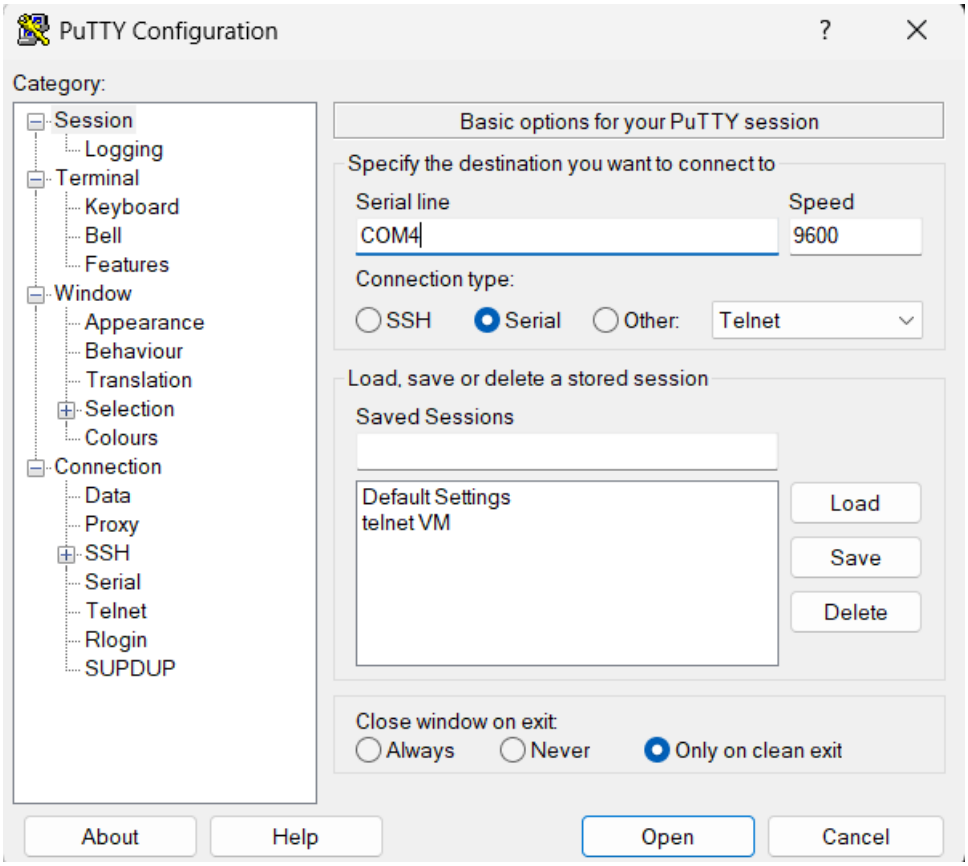
Mission 1

Contexte

La configuration suivante a été réalisée sur le **Switch Cisco Catalyst 2960**, dans le cadre du projet d'interconnexion de l'agence **galway.cub.fr** au sein de l'infrastructure CUB. Cette configuration permet l’accès sécurisé au switch, la gestion des VLANs, ainsi que la mise en place d’un lien **trunk** pour le transport de plusieurs VLANs.

Accès initial au commutateur

Lancer **PuTTY** et établir une connexion **série (console)** via le port COM correspondant.



Configuration de base

Sécuriser l'accès à la console :

```
Switch# conf t
Switch(config)# line console 0
Switch(config-line)#  password galway
Switch(config-line)# login
Switch(config-line)# exit
```

Sécuriser l'accès au mode privilégié (enable) :

```
Switch> en
Switch# conf t
Switch(config)# enable password galway
Switch(config)# exit
```

Il y a désormais deux niveaux de sécurité :

- **Accès à la console (mot de passe galway).**
- **Accès au mode privilégié (enable password galway).**

Renforcer la sécurité avec un mot de passe secret chiffré

Remplacer le mot de passe non chiffré par un mot de passe secret :

```
Switch# conf t
Switch(config)# enable secret galway@
Switch(config)# exit
```

Activer le chiffrement des mots de passe (console, VTY, etc.) :

```
Switch# conf t
Switch(config)# service password-encryption
Switch(config)# exit
```

Sauvegarde de la configuration

Enregistrer la configuration active dans la NVRAM :

```
copy running-config startup-config
```

Création des VLAN

```
Switch> enable
Switch# conf t
Switch(config)# vlan 302
Switch(config-vlan)# name WAN
Switch(config)# vlan 331
Switch(config-vlan)# name Serveurs
Switch(config)# vlan 332
Switch(config-vlan)# name Utilisateurs1
Switch(config)# vlan 333
Switch(config-vlan)# name Utilisateurs2
Switch(config)# vlan 330
Switch(config-vlan)# name DMZ
Switch(config-vlan)# exit
```

Affectation des VLAN aux ports

```
Switch(config)#  interface range gigabitEthernet 0/2
Switch(config-if)#  switchport mode access
Switch(config-if)# switchport access vlan 302

Switch(config)#  interface range gigabitEthernet 0/3-4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 331

Switch(config)#  interface range gigabitEthernet 0/5-6
Switch(config-if)#  switchport mode access
Switch(config-if)#  switchport access vlan 332

Switch(config)#  interface range gigabitEthernet 0/7-8
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 333

interface range gigabitEthernet 0/9-10
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 330
Switch(config-if)# exit
```

Configuration du trunk sur le port G1/0/1:

```
Switch(config)# interface gigabitEthernet G1/0/1
Switch(config-if)#  switchport trunk encapsulation dot1q
Switch(config-if)#  switchport mode trunk
Switch(config-if)# name Serveurs
Switch(config-if)# exit
```

Voici la configuration final sur le switch :

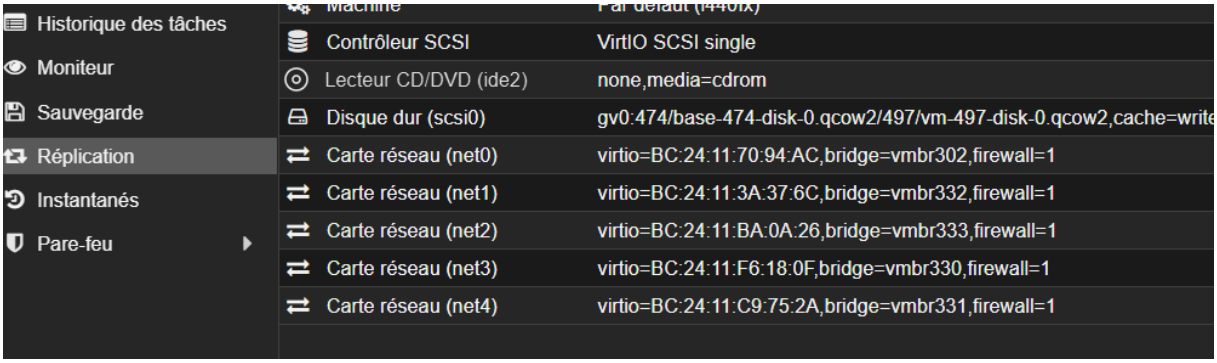
```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/12, Gi1/0/13, Gi1/0/14
                                                Gi1/0/15, Gi1/0/16, Gi1/0/17
                                                Gi1/0/18, Gi1/0/19, Gi1/0/20
                                                Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                Gi1/0/24, Gi1/0/25, Gi1/0/26
                                                Gi1/0/27, Gi1/0/28
302  wan                              active    Gi1/0/2
330  DMZ                              active    Gi1/0/9, Gi1/0/10
331  serveurs                         active    Gi1/0/3, Gi1/0/4
332  Utilisateurs1                    active    Gi1/0/5, Gi1/0/6
333  Utilisateurs2                    active    Gi1/0/7, Gi1/0/8
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

SNS GALWAY

Stormshield

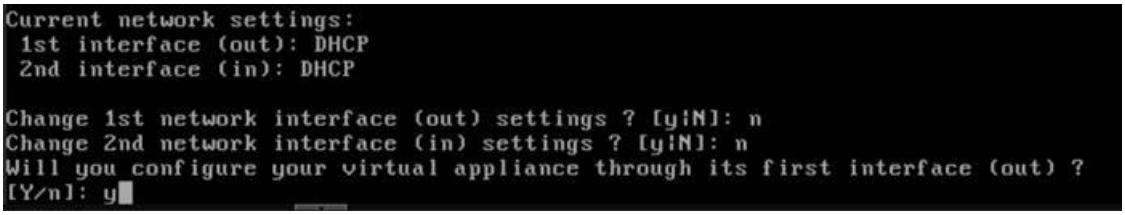
Configuration du clone de « Modele-SNS-4.3 » :

Il faut ajouter les cartes réseaux pour les différents réseaux de galway l'interface du SNS doit être dans le VLAN 302 qui est celui de CUB WAN

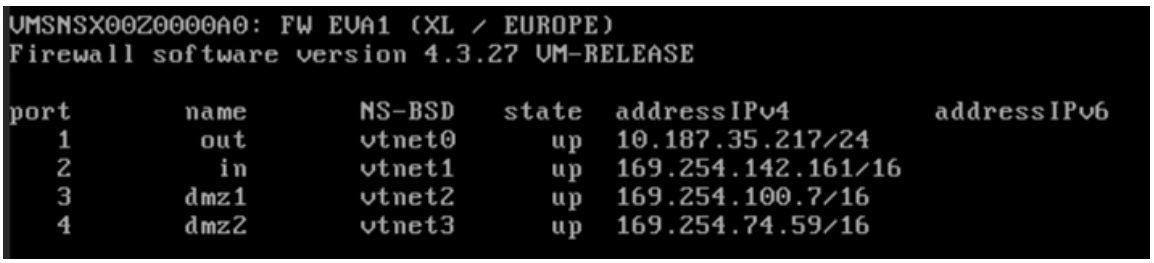


Répondre non pour changer les interfaces réseau out/in :

Répondre oui pour la configuration virtuel :



Connexion avec l'adresse Out 10.187.35.217 au site Stormshield qu'il faudra changer par la suite :

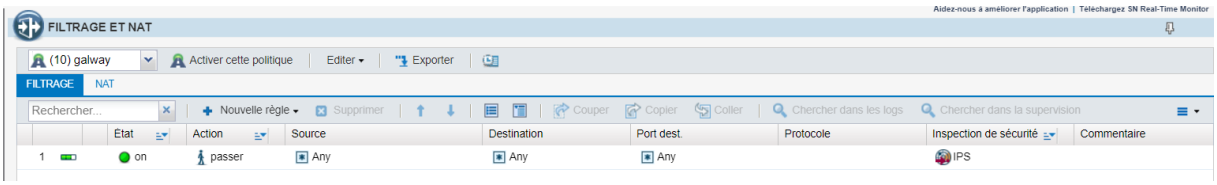


Configuration du pare feu virtuel

Une fois sur l'interface web nous devons ajouter comme passerelle le pare feu prof en 192.168.229.1

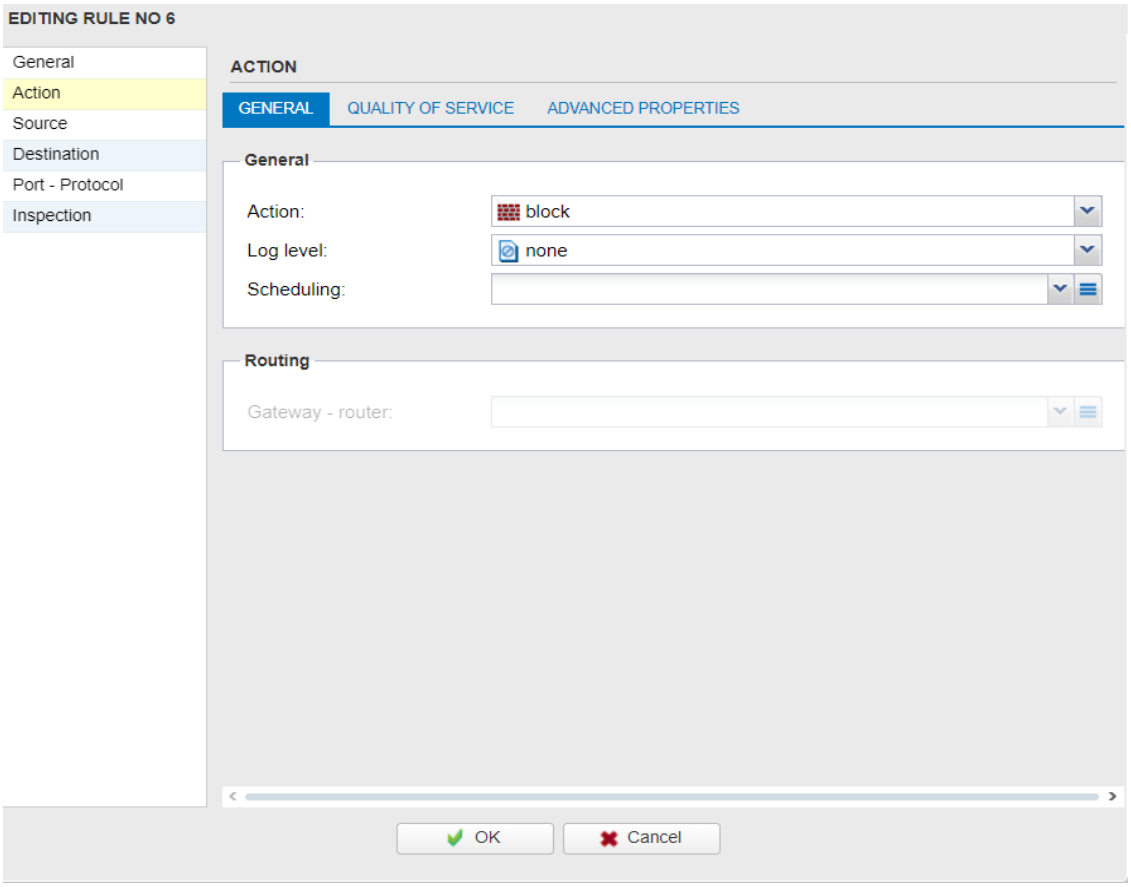
On donne accès au pare-feu via internet en donnant un IP fixe au WAN en 192.168.229.60

On met le pare-feu en pass all pour avoir accès au pare-feu librement au début nous mettrons en place nos règles après :

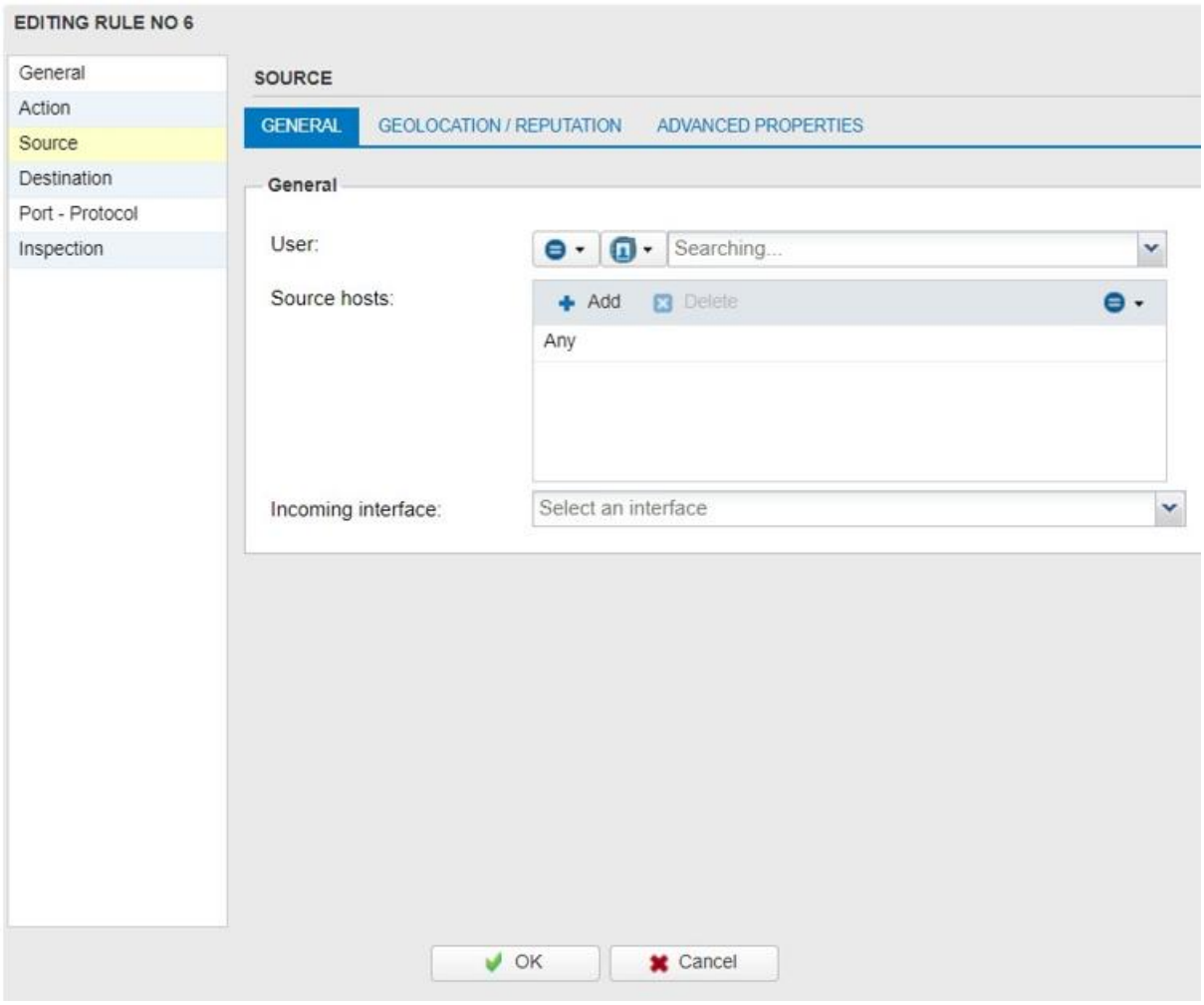


Dans la partie Security Policy - Filtrage et Nat nous créons différentes règles de sécurité de la manière suivante:

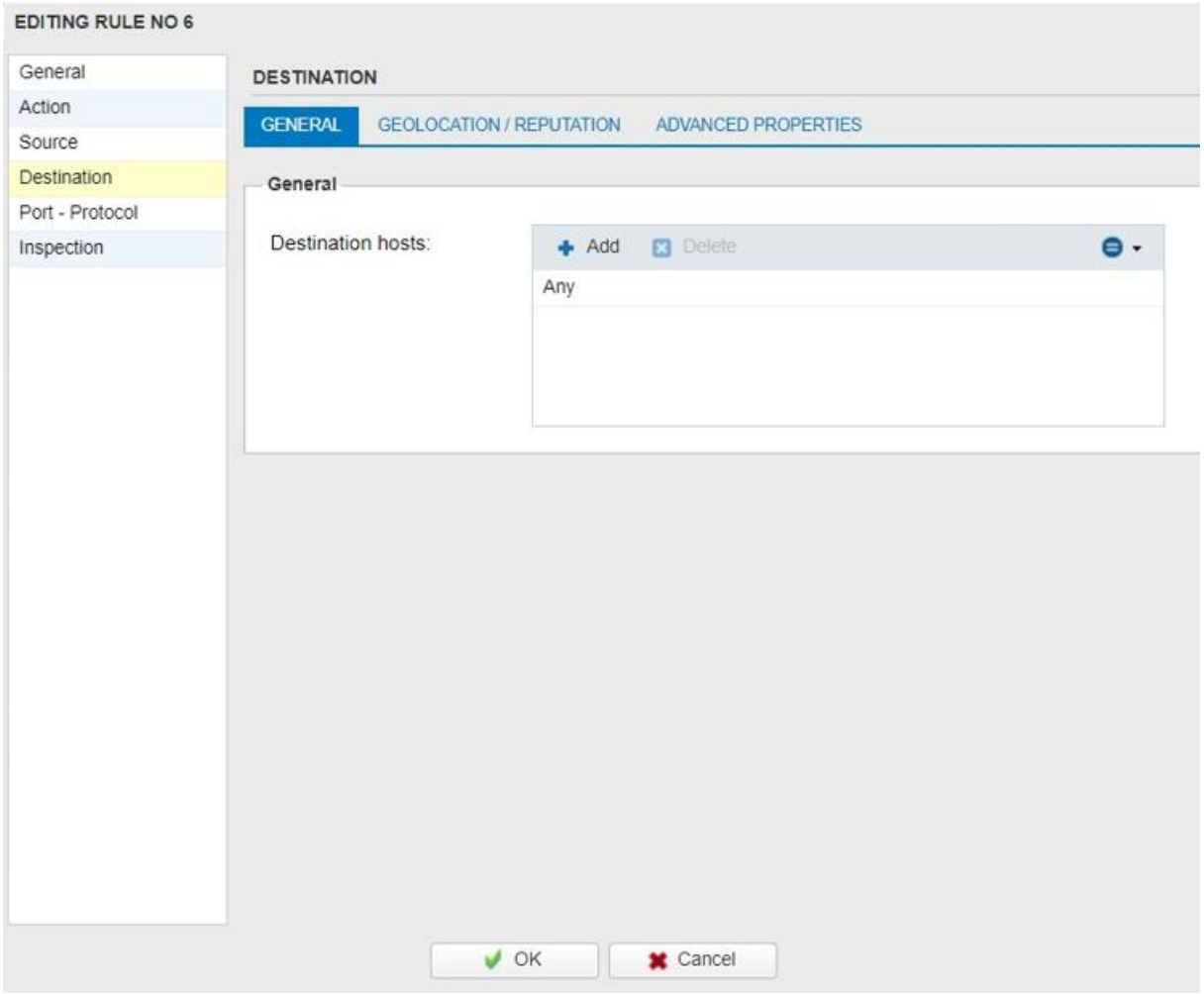
Création d'une nouvelle règle simple puis choisir son action



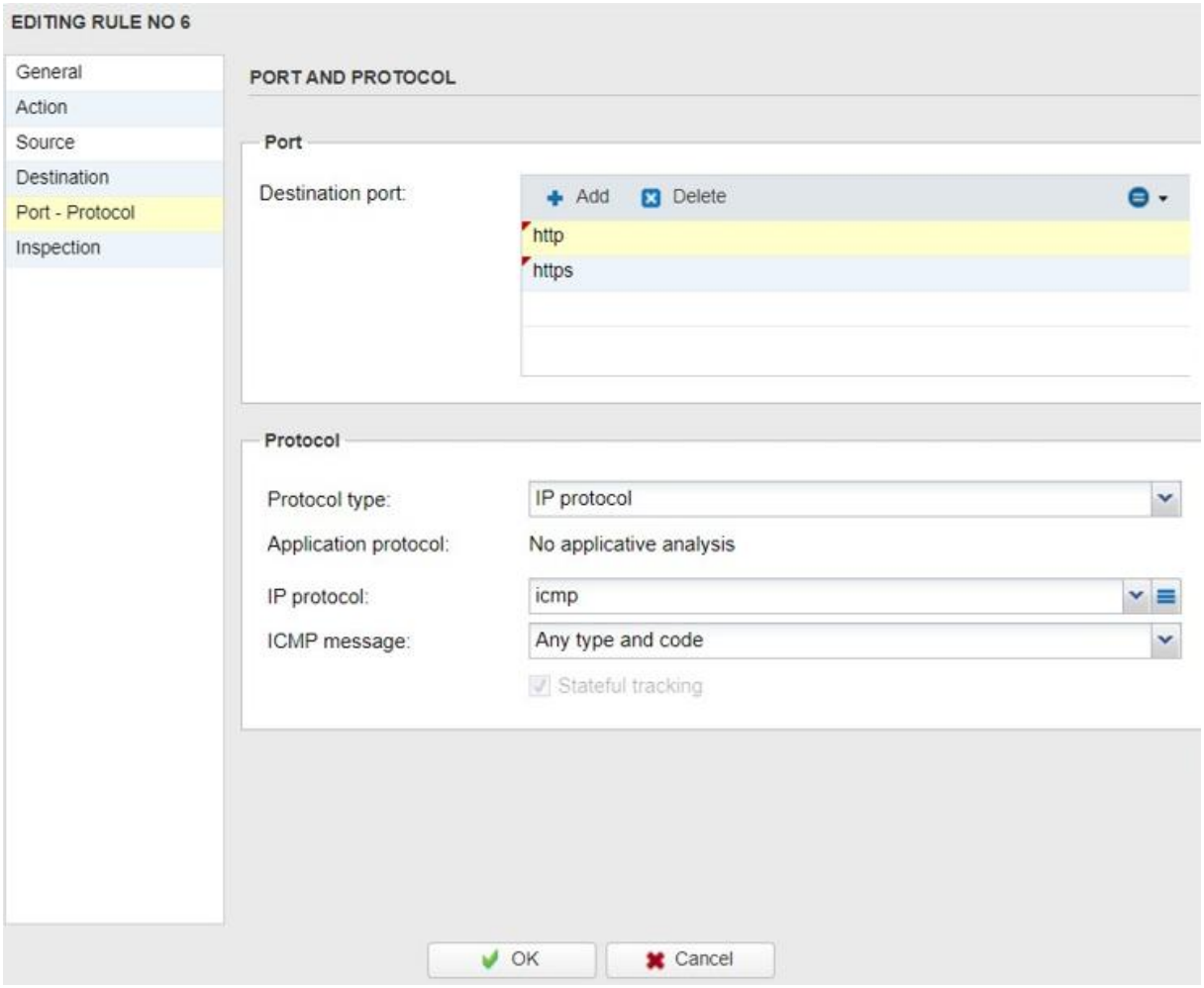
Ensuite choisir sa source :



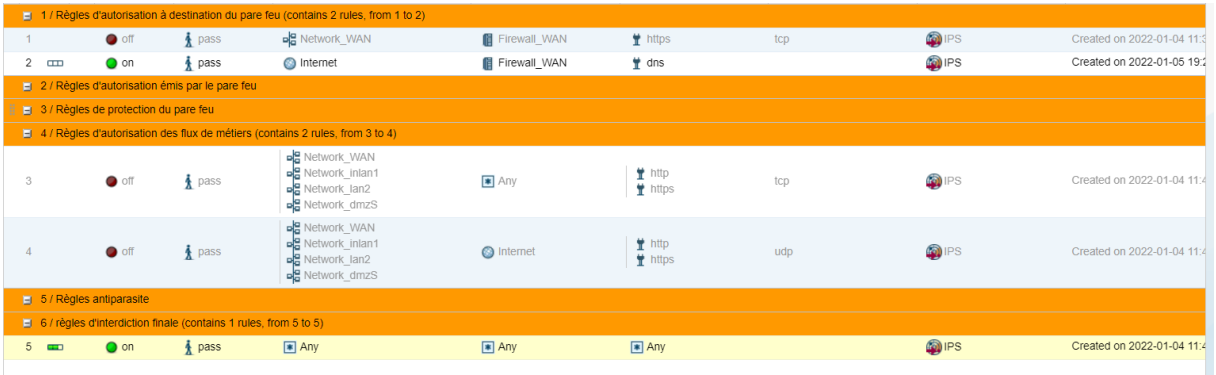
Choisir sa destination :



Choisir son port par exemple ici http/https et son protocole ici ICMP :



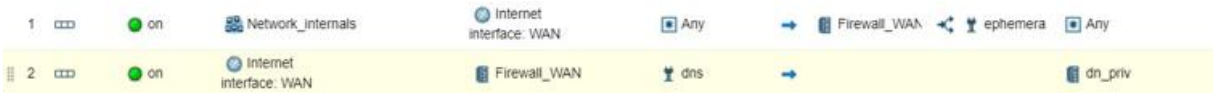
Une fois nos règles crée on les organise selon leurs utilisations :



1. **Permet au réseau WAN à destination du pare feu d'utiliser le port https sur le protocole TCP (inactif)**
2. **Permet à internet d'accéder à la destination du pare feu vers le port du DNS (actif)**
3. **Autorise l'accès pour le réseau WAN, le LAN 1, 2 et la DMZ serveur à n'importe quelle destination via le port http et https par le protocole TCP (inactif)**

4. **Autorise l’accès pour le réseau WAN, le LAN 1, 2 et la DMZ serveur internet via le port http et https par le protocole UDP (inactif)**
5. **Autorise tout (actif)**

Pour le filtrage Nat on crée deux règles :



1. **Les IP provenant d'un réseau interne destiné à Internet, passant par l'interface WAN par n’importe quelle protocol est autorisé à sortir vers l'interface WAN avec un mécanisme appelé "ephemeral ports". Cela signifie que les ports éphémères (temporairement utilisés pour des connexions sortantes) sont utilisés, et NAT est appliqué pour traduire les adresses internes.**
2. **Elle permet aux requêtes DNS externes (venant d’Internet) d’être redirigées vers notre adresse DNS privé (dn_priv),**

Service DHCP

Qu’est-ce que le service DHCP :

DHCP utilise le protocole **DHCP** (Dynamic Host Configuration Protocol) permettant la **configuration TCP/IP dynamique** (automatique) des hôtes d'un réseau local en fournissant au minimum les informations suivantes pour une communication sur le **réseau local et sur Internet** :

-Une **adresse IP**,

-Le **masque de sous-réseau**,

-La **passerelle par défaut**,

-Les **serveurs de noms DNS primaire et secondaire**.

Ce service DHCP apporte une solution pour :

-Fournir sur le réseau une configuration aux ordinateurs quand ils sont **actifs** ,

-Centraliser la gestion des informations de configuration TCP/IP et permettre de répercuter facilement toutes modifications de ces informations;

-Faciliter les tâches d'administration répétitives et fastidieuses tout en **évitant les erreurs** de configuration.

Contexte

- **Il faut configurer le service DHCP sur le VLAN Serveurs 172.16.27.0/24 Adresse du serveur : 172.16.27.1**

Configuration du service DHCP

Configuration de base sur Proxmox

Mise à jour de la machine.

```
apt update && apt upgrade
```

Installation du service.

```
apt install isc-dhcp-server
```

Configuration du service.

```
nano /etc/dhcp/dhcpd.conf
```

Modifié les lignes ci-dessous pour ajouter les DNS résolveur et le domaine galway.cub.fr

```
  GNU nano 7.2                                  /etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
option domain-name "galway.cub.fr";
option domain-name-servers 172.16.27.10;
option domain-name-servers 172.16.27.15;

default-lease-time 600;
max-lease-time 7200;
```

On déclare le serveur.

```
  GNU nano 7.2                                    /etc/dhcp/dhcpd.conf
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
#ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

#subnet 10.152.187.0 netmask 255.255.255.0 {
#}
```

Authoritative ;

Cette ligne indique que ce serveur DHCP est l'autorité principale pour la distribution des adresses IP sur le réseau local.

Log-facility local7 ;

Cette directive indique où les journaux du serveur DHCP seront envoyés.

local7 est une "facility" utilisée par syslog, qui permet de diriger les logs vers un fichier spécifique dans /var/log.

On ajoute la plage d'adresse que le serveur va distribuer :

```
  GNU nano 7.2                                    /etc/dhcp/dhcpd.conf

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
subnet 192.168.7.0 netmask 255.255.255.0 {
        range 192.168.7.1 192.168.7.100;
        option domain-name-servers 172.16.27.15;
        option domain-name-servers 172.16.27.10
        option domain-name "galway.cub.fr";
        option routers 192.168.7.254;
option broadcast-address 192.168.7.255;
}

# Hosts which require special configuration options can be listed in
```

- **Adresse du LAN 1 en .7.0 + le masque**
- **La plage d'adresse distribué de .1 à .100**
- **Dns résolveur 1**
- **DNS résolveur 2**
- **Nom de domaine CUB**
- **Passerelle**
- **Adresse broadcast**

On ajoute également les DNS résolveur dans le fichier resolv.conf :

```
  GNU nano 7.2                                    /etc/resolv.conf
# --- BEGIN PVE ---
search galway.cub.fr
nameserver 172.16.27.15
nameserver 172.16.27.10
# --- END PVE ---
```

Service agent relais

Qu'est-ce qu'un agent relais DHCP

Dans un réseau divisé en plusieurs sous-réseaux, un **agent relais DHCP** (ou **DHCP relay agent**) permet de relayer les requêtes DHCP des clients vers un serveur DHCP situé dans un autre sous-réseau.

En effet, les requêtes DHCP sont envoyées en **broadcast**, et ces messages ne traversent pas les routeurs. L'agent relais résout ce problème en **réacheminant les requêtes DHCP** des clients vers le serveur DHCP central, généralement via **des requêtes unicast**.

Fonctionnement :

- Le client DHCP envoie une requête (broadcast) pour obtenir une adresse IP.
- L'agent relais, généralement configuré sur un routeur ou un serveur intermédiaire, intercepte cette requête.
- Il la transmet au serveur DHCP distant, en y ajoutant l'**adresse IP de l'interface par laquelle la requête a été reçue** (option 82 ou 54 selon le protocole).
- Le serveur DHCP attribue une adresse IP en fonction du sous-réseau d'origine et renvoie la réponse via l'agent relais, qui la retransmet au client.

Contexte

- **Le serveur qui héberge le service DHCP est appelée DHCP ;**
- **Le réseau IP sur lequel se trouve le serveur DHCP est 172.16.27.0/24 ;**
- **L'adresse IP du serveur DHCP est 172.16.27.1/24 ;**
- **Le serveur qui va héberger le service Agent relais DHCP est appelé AgentRelais et est situé dans le VLAN Utilisateurs**

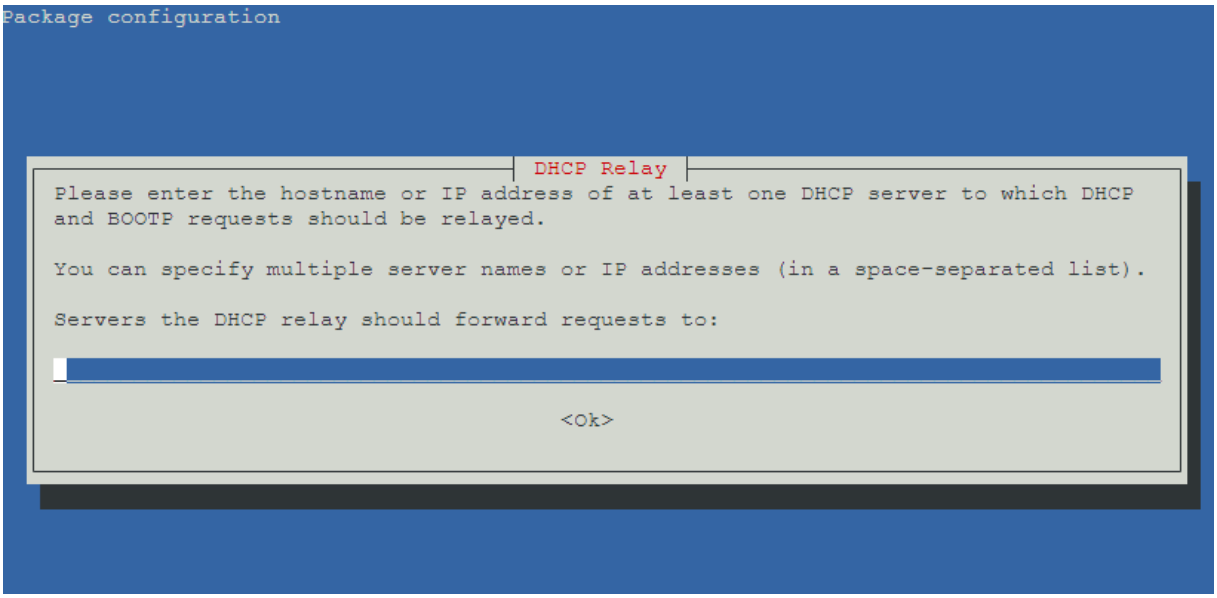
Configuration du service agent relais

En premier lieu, il faut installer les paquets du service :

AgentRelais:~# apt-get install isc-dhcp-relay --fix-missing

```
root@AgentRelais:~# apt-get install isc-dhcp-relay --fix-missing
Reading package lists... Done
Building dependency tree... Done
The following NEW packages will be installed:
  isc-dhcp-relay
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 1089 kB of archives.
After this operation, 2943 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 isc-dhcp-relay amd64 4.4.3-P1-2 [108
 kB]
0% [1 isc-dhcp-relay 0 B/1089 kB 0%]
```

L'assistante d'installation va nous demander l'IP de notre serveur DHCP :

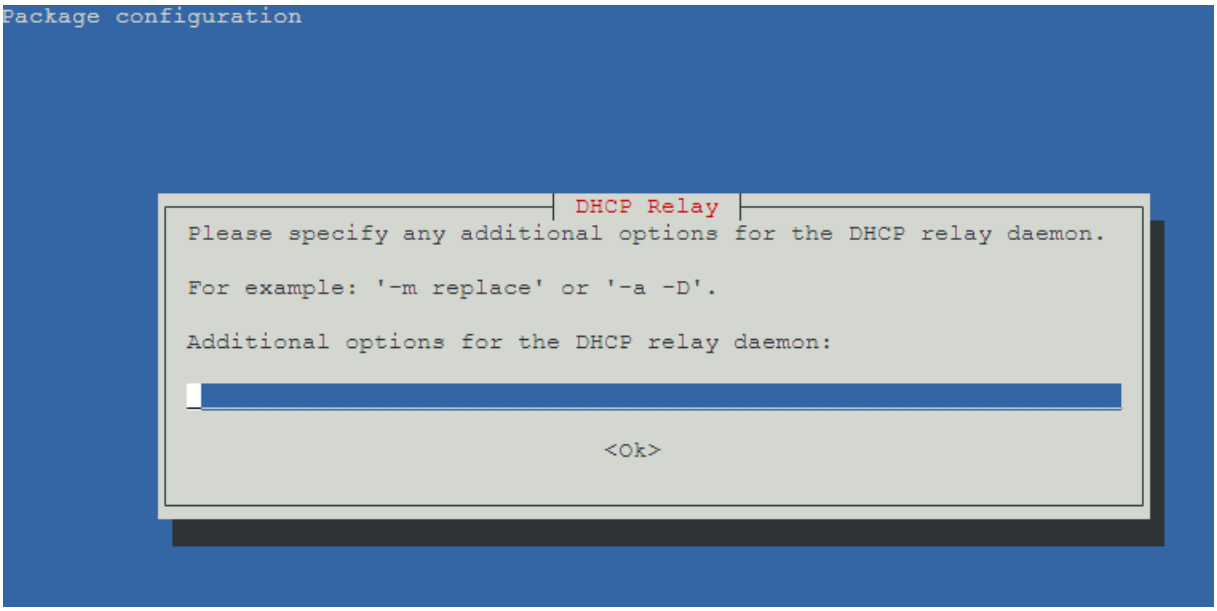


Nous allons rentrer l'ip de notre serveur DHCP :

- **172.16.27.1**

Ensuite, l'assistante d'installation nous demandera sur quelle interface réseau l'agent relais DHCP va écouter, il ne faut pas renseigner cette partie.

Pour l'étape suivante, on nous demandera de préciser des options, il ne faudra rien mettre :



Affichage de la configuration

On peut visualiser le fichier de configuration du relais DHCP dans /etc/default/isc-dhcp-relay :

```
  GNU nano 7.2                                /etc/default/isc-dhcp-relay
# Defaults for isc-dhcp-relay initscript
# sourced by /etc/init.d/isc-dhcp-relay
# installed at /etc/default/isc-dhcp-relay by the maintainer scripts

#
# This is a POSIX shell fragment
#

# What servers should the DHCP relay forward requests to?
SERVERS="172.16.27.1"

# On what interfaces should the DHCP relay (dhrelay) serve DHCP requests?
INTERFACES=""
```

On redémarrera le service agent relais avec la commande :

AgentRelais:~# systemctl start isc-dhcp-relay

Modification de la configuration du service

Il va falloir définir le subnet dans le fichier dhcpd.conf du serveur DHCP :

```
# A slightly different configuration for an internal subnet.
subnet 192.168.9.0 netmask 255.255.255.0 {
  range 192.168.9.10 192.168.9.250;
  option domain-name-servers 8.8.8.8;
  option domain-name "ingolstadt.cub.fr";
  option routers 192.168.9.254;
  option broadcast-address 192.168.9.255;
  default-lease-time 600;
  max-lease-time 7200;
}

subnet 172.16.29.0 netmask 255.255.255.0 {
   range 172.16.29.10 172.16.29.250;
   option routers 172.16.29.254;
   option broadcast-address 172.16.29.255;
}
```

On pourra ensuite le redémarrer avec la commande :

AgentRelais:~#systemctl restart isc-dhcp-server

Configuration de règle du pare-feu SMS

Pour que l'agent Relais puisse contacter le serveur DHCP, on définit la règle suivant :

N°		Source	Destination	Port D	Protocole	Action
		192.168.7.252	172.16.27.1	bootps		Passer

- **192.168.7.252 : est notre serveur relais (Source)**
- **172.16.27.1 : est notre serveur DHCP (Destination**
- **Bootps (67) : est le port utilisé**
- **Passer : on autorise l'agent relais à communiquer avec le serveur DHCP**

DNS RÉSOLVEUR

Qu'est-ce que le serveur DNS récursif Unbound

Le logiciel Unbound permet de mettre en place un serveur DNS récursif sur un système Debian. Ce serveur se limite à effectuer des requêtes DNS récursives, sans héberger de zones DNS.

Dans le cadre du contexte CUB, le domaine cub.fr est un domaine fictif. Le résolveur ne doit donc pas suivre son comportement habituel, qui consiste à interroger les serveurs racine d'Internet lorsqu'il doit résoudre un nom de domaine.

Au lieu de cela, la configuration doit spécifier que toute requête concernant le domaine cub.fr doit être redirigée vers le serveur DNS situé dans la DMZ du siège, qui fait autorité pour ce domaine.

- **Pour cela, nous utiliserons une stub-zone, et non une forward-zone, afin d'indiquer explicitement l'adresse du serveur faisant autorité pour cub.fr.**
- **Pour la résolution des autres noms de domaine sur Internet, nous utiliserons une forward-zone pour rediriger les requêtes vers un serveur DNS récursif public, comme 8.8.8.8, 1.1.1.1 ou 9.9.9.9.**
-

Contexte

- **galway.cub.fr : sous-domaine de l'agence (autoritaire sur 172.16.7.20)**
- **cub.fr : domaine principal (siège, DNS en 192.168.229.1)**
- **Résolveur Unbound : 172.16.27.15 (ne gère aucune zone, uniquement récursif)**

Installation de Unbound

Mise à jour de la machine.

```
apt update && apt upgrade
```

Installation de unbound.

```
apt install unbound dnsutils
```

Création d'un répertoire pour les log.

```
mkdir /var/log/unbound
```

Crée un fichier de journalisation.

```
touch /var/log/unbound/unbound.log
```

Changer le propriétaire du fichier et de fichier de journaux.

```
chown -R unbound:unbound /var/log/unbound
```

Redémarrer unbound.

```
# systemctl restart unbound
```

Configuration de unbound.

```
nano /etc/unbound/unbound.conf
```

On ajoute l'IP du serveur a son interface d'écoute puis on ajoute les accès aux différents réseaux.

```
  GNU nano 7.2                                  /etc/unbound/unbound.conf
# The following line includes additional configuration files from the
# /etc/unbound/unbound.conf.d directory.
include-toplevel: "/etc/unbound/unbound.conf.d/*.conf"
server:

interface: 172.16.27.15
interface: 127.0.0.1

access-control: 192.168.27.0/24 allow
access-control: 192.168.7.0/24 allow
access-control: 172.16.7.0/24 allow
access-control: 172.16.27.0/24 allow
access-control: 127.0.0.0/8 allow
access-control: 0.0.0.0/0 refuse

hide-version: yes
hide-identity: yes

do-ip4: yes
```

On ajoute le chemin de log crée .

```
logfile: /var/log/unbound/unbound.log
verbosity: 2
```

On crée une récursivité pour le domaine cub.fr en utilisant le pare feu prof.

```
private-domain: cub.fr.
domain-insecure: cub.fr
# interroger le serveur DNS du siege
stub-zone:
name: "cub.fr."
stub-addr: 192.168.229.1
```

On crée une récursivité sur internet en utilisant le DNS Google.

```
forward-zone:
name: "."
forward-addr: 8.8.8.8
forward-addr: 8.8.4.4
```

On crée une récursivité pour le domaine galway.cub.fr en utilisant le DNS autoritaire.

```
stub-zone:
name: "galway.cub.fr."
stub-addr: 172.16.7.20
```

Aller dans le fichier /etc/resolv.conf et ajoutez y votre DNS.

```
nano /etc/resolv.conf
```

```
search galway.cub.fr
nameserver 172.16.27.15
```

Tester si votre DNS résolveur obtient des réponse par google.fr.

```
# dig google.fr
```

Vous devez voir Query(question) à 1 et Answer(réponse) à 1 également

En bas de votre commande vous pouvez retrouver le server utilisé pour faire cette résolution.

```
root@dns0:~# dig google.fr

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> google.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57595
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;google.fr.                     IN      A

;; ANSWER SECTION:
google.fr.              300     IN      A       142.251.37.227

;; Query time: 72 msec
;; SERVER: 172.16.27.15#53(172.16.27.15) (UDP)
;; WHEN: Tue Apr 01 07:05:11 UTC 2025
;; MSG SIZE  rcvd: 54
```

DNS AUTORITAIRE

Qu'est-ce que le service DNS

Le service **BIND9** (Berkeley Internet Name Domain version 9) est l'un des serveurs DNS les plus utilisés pour héberger et gérer des **zones DNS** dans un réseau. Il permet de répondre aux requêtes DNS des clients en fournissant les correspondances entre noms de domaine et adresses IP.

Contrairement à un résolveur DNS récursif comme **Unbound**, **BIND9** est généralement utilisé pour jouer le rôle de **serveur faisant autorité** pour un ou plusieurs domaines.

Contexte

Mettre en place un serveur DNS (BIND9) sur une machine Debian, afin d'assurer la résolution de noms locaux dans le réseau de l'agence galway.cub.fr.

Configuration

Mise à jour de la machine

```
apt update && sudo apt upgrade
```

Installation du service DNS(bind9)

```
apt -y install bind9 dnsutils
```

```
nano /etc/bind/named.conf.options
```

Modification du fichier /etc/bind/named.conf.options pour :

- **Indiquer l'interface d'écoute du serveur (127.0.0.1 et 172.16.7.20) et le port en 53 :**

```
 GNU nano 7.2                                    named.conf.options
options {
        directory "/var/cache/bind";
        listen-on port 53 { 127.0.0.1; 172.16.7.20; };
```

On ajoute également les différents réseaux

```
        dnssec-validation auto;
        version none;
        listen-on-v6 { any; };
        allow-query {
                172.16.7.0/24;
                172.16.27.0/24;
                192.168.7.0/24;
                192.168.27.0/24;
                192.168.229.0/24;
        };
};
```

Création du fichier de zone maitre

nano /etc/bind/db.galway.cub.fr

```
  GNU nano 7.2                                          db.galway.cub.fr
$TTL 1D
galway.cub.fr.    IN      SOA     ns0.galway.cub.fr. root.galway.cub.fr. (
        2006031201      ; serial
        1D              ; refresh
        1H              ; retry
        1W              ; expire
        3H)             ; Negative Cache TTL

galway.cub.fr.   IN       NS     ns0.galway.cub.fr.
@       IN      A       192.168.229.60
ns0     IN      A       192.168.229.60
www     IN      A       192.168.229.60
dhcp    IN      A       192.168.229.60
```

Création du fichier de zone inverse

```
  GNU nano 7.2                                          db.172.16.7.rev
$TTL 3D
@        IN SOA ns0.galway.cub.fr. root.galway.cub.fr. (
        2006031201      ; serial
        28800           ; refresh
        14400           ; retry
        3600000         ; expire
        86400 )         ; minimum

    NS  ns0.galway.cub.fr.
444 PTR ns0.galway.cub.fr.
445 PTR dhcp.galway.cub.fr.
```

Déclaration des zones

Modifier le fichier/etc/bind/named.conf.local

On y ajoute la zone directe et la zone inverse

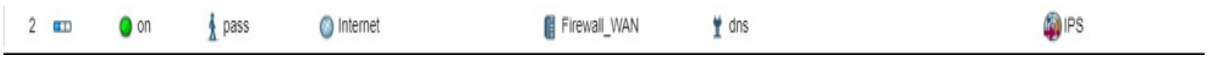
```
  GNU nano 7.2                                  named.conf.local
zone "galway.cub.fr" {
    type master;
    file "/etc/bind/db.galway.cub.fr";
};

zone " 7.16.172.in-addr.arpa" {
        type master;
        file "/etc/bind/db.172.16.7.rev";
};
```

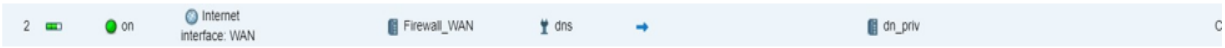
Configuration du NAT et pare-feu

Comme vous l'avez vu au début dans le fichier db.galway.cub.fr nous avons renseigné le pare feu il nous faut donc crée quelque règles d'accès et de sécurité.

Dans le filtrage NAT on permet depuis internet vers le pare feu (réseau WAN) d'accéder au DNS



Dans le filtrage NAT on permet depuis internet vers le pare feu (réseau WAN) d'accéder au DNS en 172.16.7.20



NAT on permet depuis internet vers le pare feu d'accéder au dns mais cette fois ci l'objet crée DNS est à l'addresse publique 192.168.229.24 (qui correspond au port du WAN il permet de faire le lien entre les deux réseau car le DNS est dans le réseau privée.

Teste réaliser sur le wifi CUBWAN :

```
C:\Users\theoh>nslookup www.galway.cub.fr 192.168.229.24
Serveur :   UnKnown
Address:  192.168.229.24

Nom :    www.galway.cub.fr
Address:  192.169.229.24
```

Faire une vérification de la syntaxe

```
named-checkconf -z
```

En cas de nom erreur redémarrer le service via la commande :

```
systemctl restart bind9
```

En cas d’erreur vous pouvez utiliser la commande :

```
named -g
```

SSH

Connexion/Client

Génération de clé publique/privé

```
ssh-keygen -t ed25519
```

Autorisation règles de pare feu sur le port 8022 ssh

Connexion au client DHCP de Proxmox depuis un compte crée

mdp = azerty

```
ssh -p 8022 theo@192.168.229.60
```

Création d'un dossier .ssh dans le client

```
mkdir .ssh
```

Ajout de la clé publique depuis windows sur le clientdebian (ce placer dans le bon dossier)

```
scp -P 8022 id_ed25519.pub theo@192.168.229.60:/home/theo/.ssh
```

Ouvrir le fichier dans le clientdebian puis copier et le coller dans le dossier .ssh

```
cat id_ed25519.pub
```

Cela permet de ne plus avoir besoin de donner le mdp mais juste la pass phrase
pass phrase = azerty

HAPROXY

SERVEUR APACHE

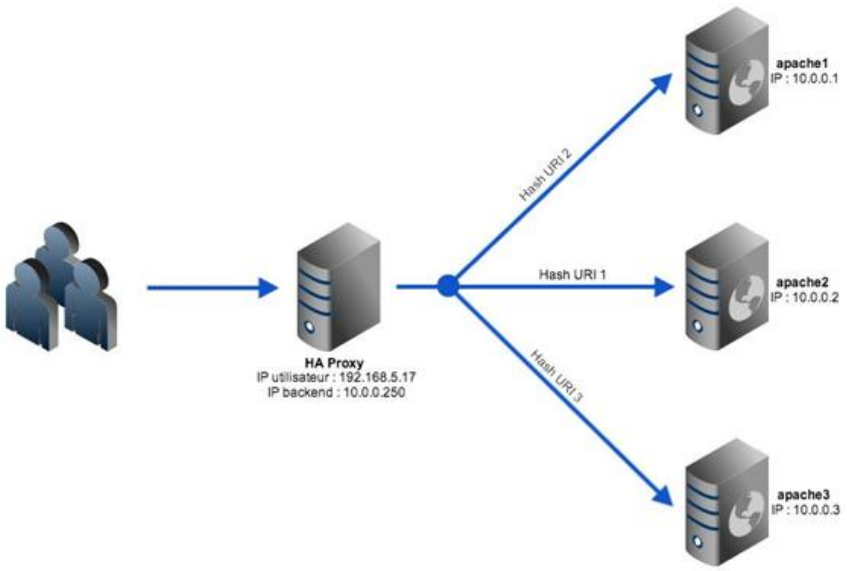
Nous allons utiliser 4 Machine pour faire ce projet toute dans le vlan 330 de l'agence galway qui est le vlan DMZ en 172.16.7.0 :

- Serveur web de Valentin sous apache en **172.16.7.40**
- Serveur web de Theo sous apache en **172.16.7.35**
- Machine Windows pour faire le client en **172.16.7.41**
- Serveur Haproxy en **172.16.7.5**

Nous voulons utiliser Haproxy pour permettre une répartition des charges entre les deux serveur web de Valentin et de Theo

Haproxy est un logiciel gratuit et open source qui fournit un équilibreur de charge haute disponibilité et un proxy inverse pour les applications TCP et HTTP qui répartissent les requêtes sur plusieurs serveurs.

Cela est utile pour les applications à gros trafic qui peuvent notamment avoir des pics d'utilisateurs.



Création de deux serveurs apache

Nous allons faire la configuration du serveur de Theo l'autre doit être identique en ne changeant que quelques détails comme le nom.

Mise à jour de votre Machine.

```
Apt update && apt upgrade
```

Installation de apache2.

```
Apt install apache2
```

Création du dossier ou seront stockés les fichiers web de notre serveur.

```
Mkdir -p /var/www/theo-web
```

On s'assure qu'apache puisse y accéder.

```
chown -R www-data:www-data /var/www/theo-web
chmod -R 755 /var/www/theo-web
```

Création d'une page index.html et ajouter son contenu voulu à l'intérieur.

```
nano /var/www/theo-web/index.html
```

Configuration du VirtualHost Apache

Création d'un fichier de conf.

```
nano /etc/apache2/sites-available/theo-web.conf
```

On y ajoute notre virtualhost :

```
<VirtualHost *:80>
    ServerName theo-web
    DocumentRoot /var/www/theo-web

    <Directory /var/www/theo-web>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/theo-web-error.log
    CustomLog ${APACHE_LOG_DIR}/theo-web-access.log combined
</VirtualHost>
```

On active notre site.

```
a2ensite theo-web.conf
```

On désactive le site par défaut.

```
sudo a2dissite 000-default.conf
```

On recharge Apache.

```
sudo systemctl reload apache2
```

Test Windows.

Dans le poste client Windows vous devez ajouter dans le fichier Hosts les serveurs.

Ouvrez le fichier avec le bloc note et ajoutez le serveur .

C:\Windows\System32\drivers\etc\hosts

```
#config perso
172.16.7.40 valentin-web
172.16.7.35 theo-web
```

Teste sur votre navigateur de votre client Windows la requête.

http://theo-web

Configuration du serveur Haproxy

Mise à jour de votre Machine.

Apt update && apt upgrade

Installation de Haproxy.

Apt install haproxy -y

Pour voir la version installé.

haproxy -v

```
root@Haproxy:~# haproxy -v
HAProxy version 2.6.12-1+deb12u1 2023/12/16 - https://haproxy.org/
Status: long-term supported branch - will stop receiving fixes around Q2 2027.
Known bugs: http://www.haproxy.org/bugs/bugs-2.6.12.html
Running on: Linux 6.5.11-7-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.11-7 (2023-12-05T09:44Z) x86_64
```

Modification du fichier de configuration.

```
Nano /etc/haproxy/haproxy.cfg
```

Ajout d'un frontend et d'un backend en configuration perso à la fin de la conf .

On ajoute nos deux serveurs apache crée.

```
#Configuration personnalise
#Tout le trafic destination du port 80 de HAProxy sera redirige vers les serveurs web.
#frontend
frontend http_front
    bind *:80
    mode http
    default_backend web_servers

#backend
backend web_servers
    mode http
    balance roundrobin
    server valentin-web 172.16.7.40:80 check
    server theo-web 172.16.7.35:80 check
```

Tester le fichier de configuration pour vérifier les erreurs.

```
haproxy -c -f /etc/haproxy/haproxy.cfg
```

Redémarre Haproxy.

```
Systemctl restart haproxy
```

Active haproxy au démarrage.

```
Systemctl enable haproxy
```

Une fois cela fait vous devez l'ajouter à votre fichier hosts de la machine Windows.

Rajoute la ligne suivante en dessous des serveurs apache fait précédemment :

```
172.16.7.5 haproxy-web
```

Teste sur votre navigateur de votre client Windows la requête.

http://haproxy-web

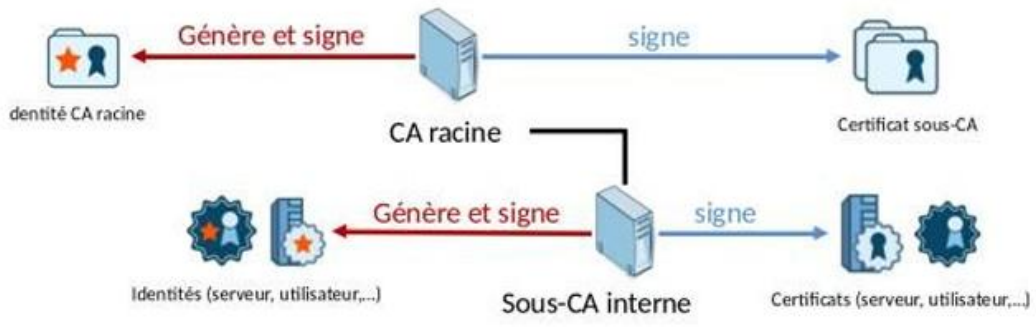
Si tout fonctionne bien à chaque rafraichissement il devrait switch entre le serveur de Valentin et celui de Theo.

Infrastructure à Clés Publiques (PKI) – Identité

Contexte

L'objectif de ce projet est la mise en œuvre d'une infrastructure à clé publique (PKI) via un pare-feu Stormshield SNS. Les actions comprennent :

- Création d'une autorité de certification racine (CA).
- Génération de certificats utilisateurs signés.
- Authentification sur un serveur Debian distant.
- Authentification via l'interface d'administration Stormshield.



Stormshield SNS permet de gérer une PKI interne avec les fonctionnalités suivantes :

- **Autorité de certification racine (CA) : Le pare-feu agit comme autorité racine auto-signée.**

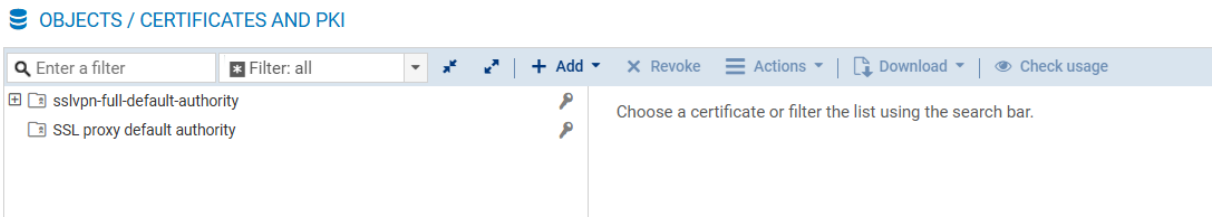
- **Sous-autorité de certification : Il peut aussi agir comme sous-autorité d'une CA parente.**

Services:

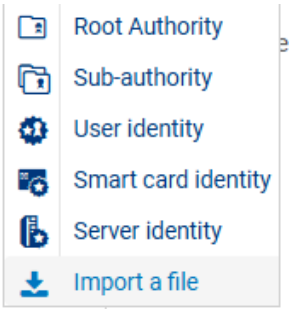
- **Création et signature de certificats.**
- **Révocation et gestion de listes CRL.**
- **Déploiement pour VPN SSL, proxy, et authentification.**

Création de l’autorité de certification (CA)

Accédez à : Configuration > Objets > Certificats et PKI

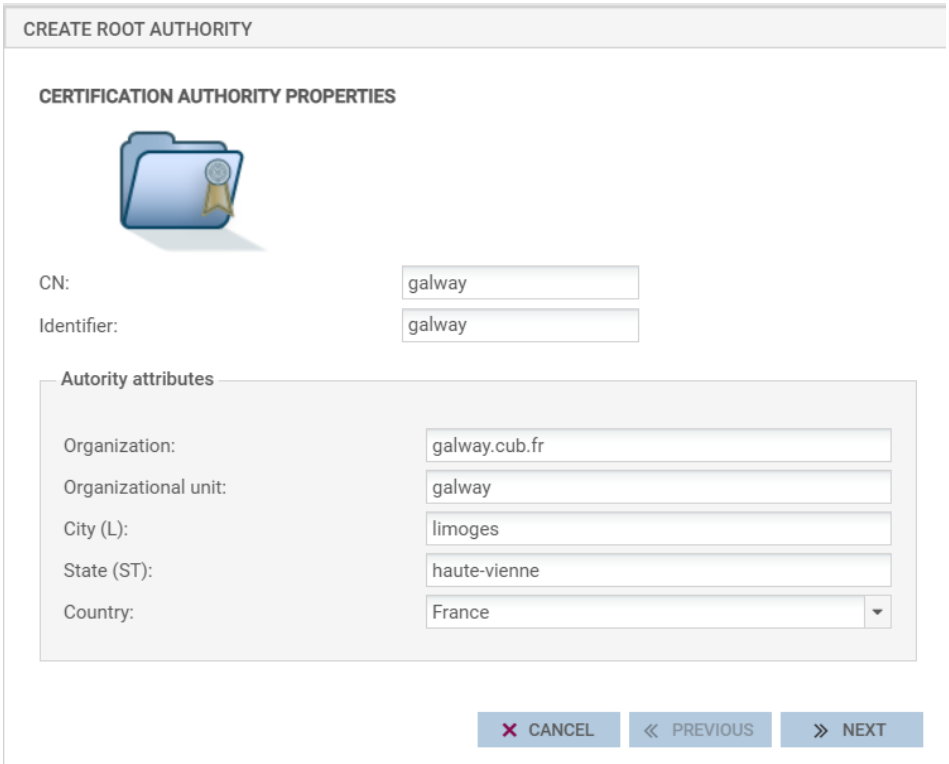


Cliquez sur **Ajouter** → **Autorité racine**

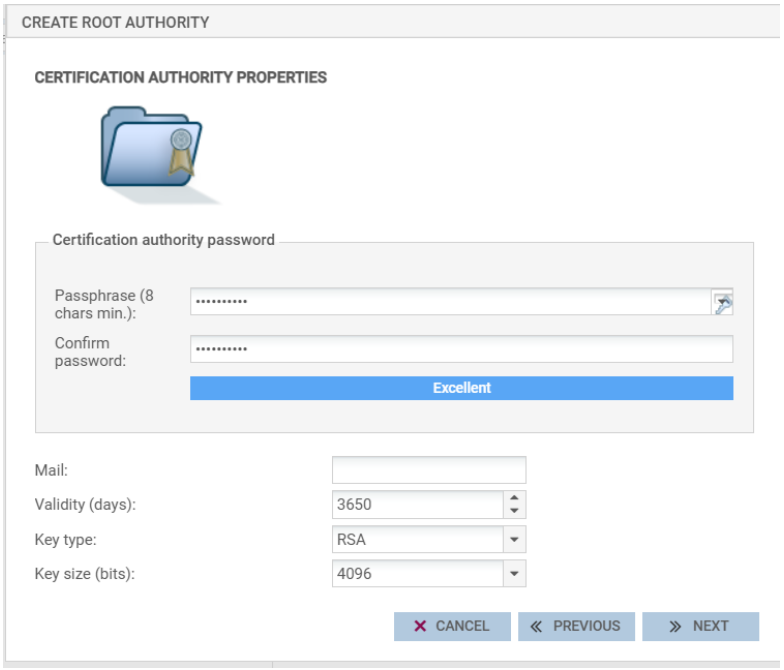


Remplissez les champs :

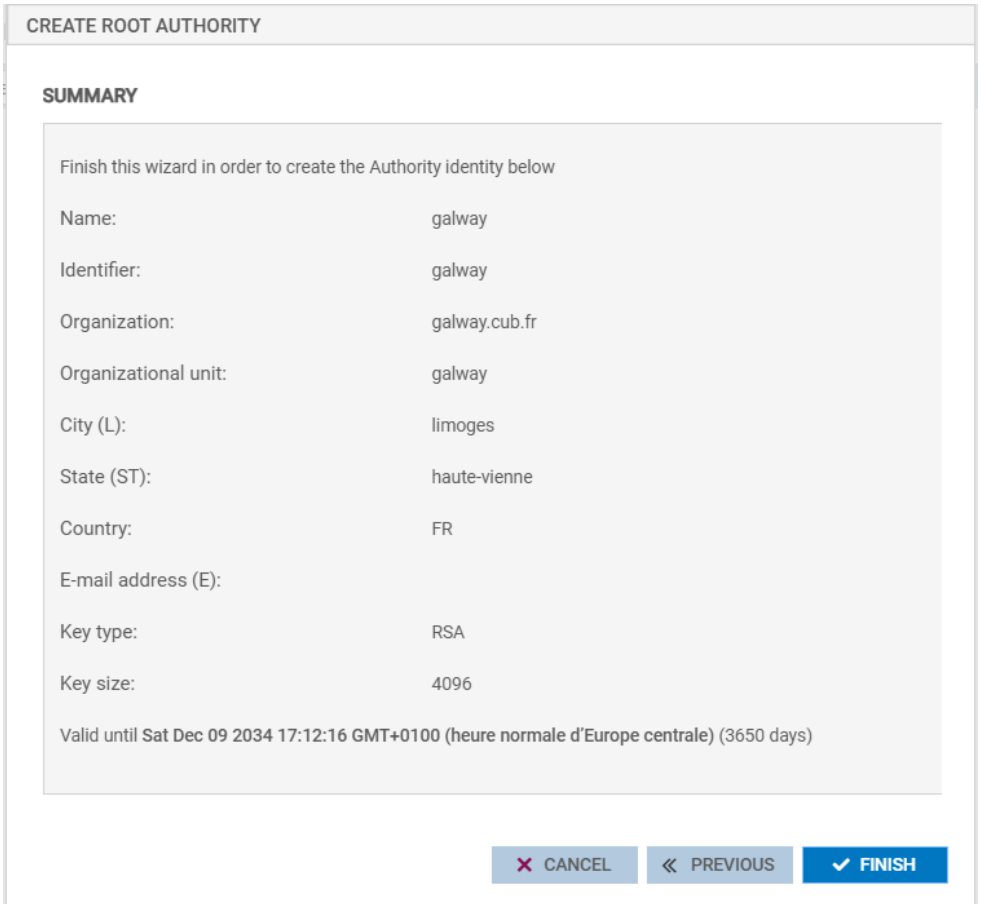
- **CN** : Nom unique ()
- **Identifiant** (optionnel)
- **Organisation (O)**, **Unité (OU)**, **Ville (L)**, **Département (ST)**, **Pays (C)**



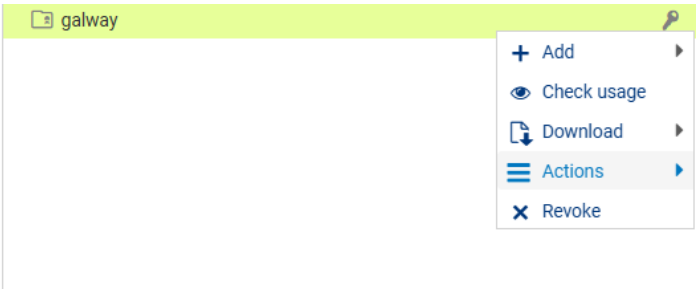
Cliquer sur **suivant** :



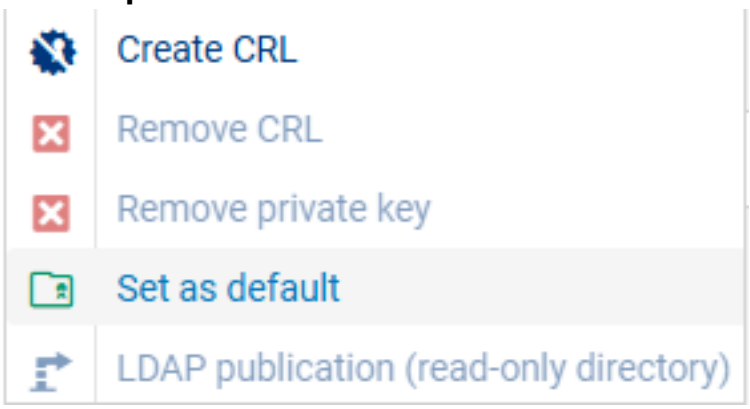
Le ca est créé .



L’autorité racine est désormais visible dans l’arborescence du pare-feu.



Définir par défaut l’autorité de certification :

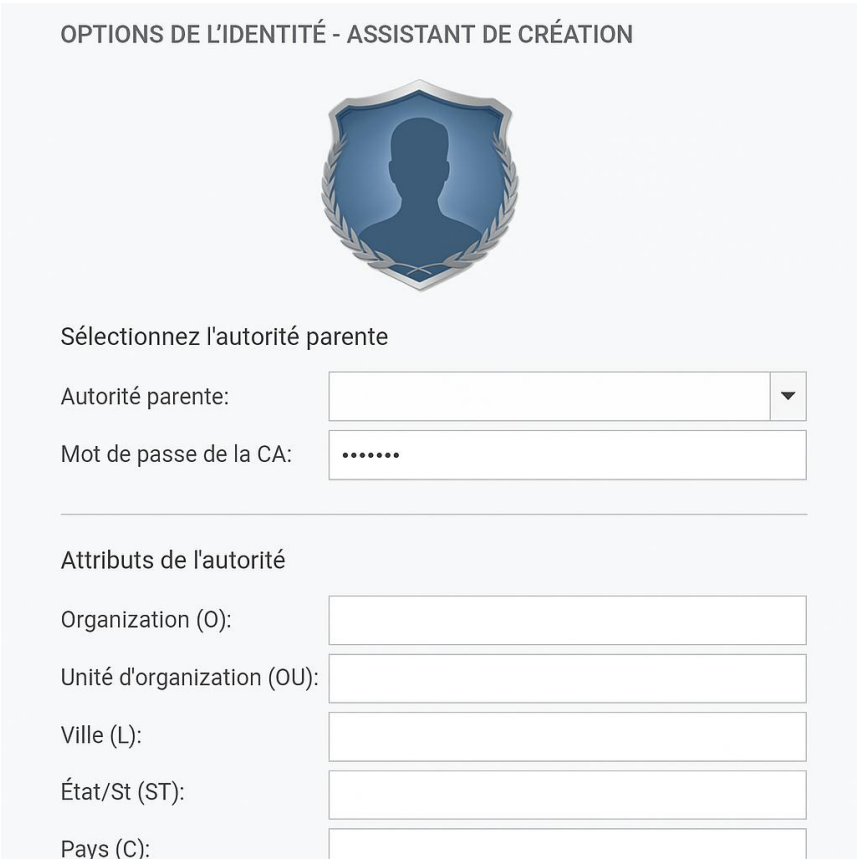


Création de l’identité utilisateur

Allez dans Configuration > Objets > Certificats et PKI
Cliquez sur **Ajouter** → **Identité utilisateur**
Renseignez :

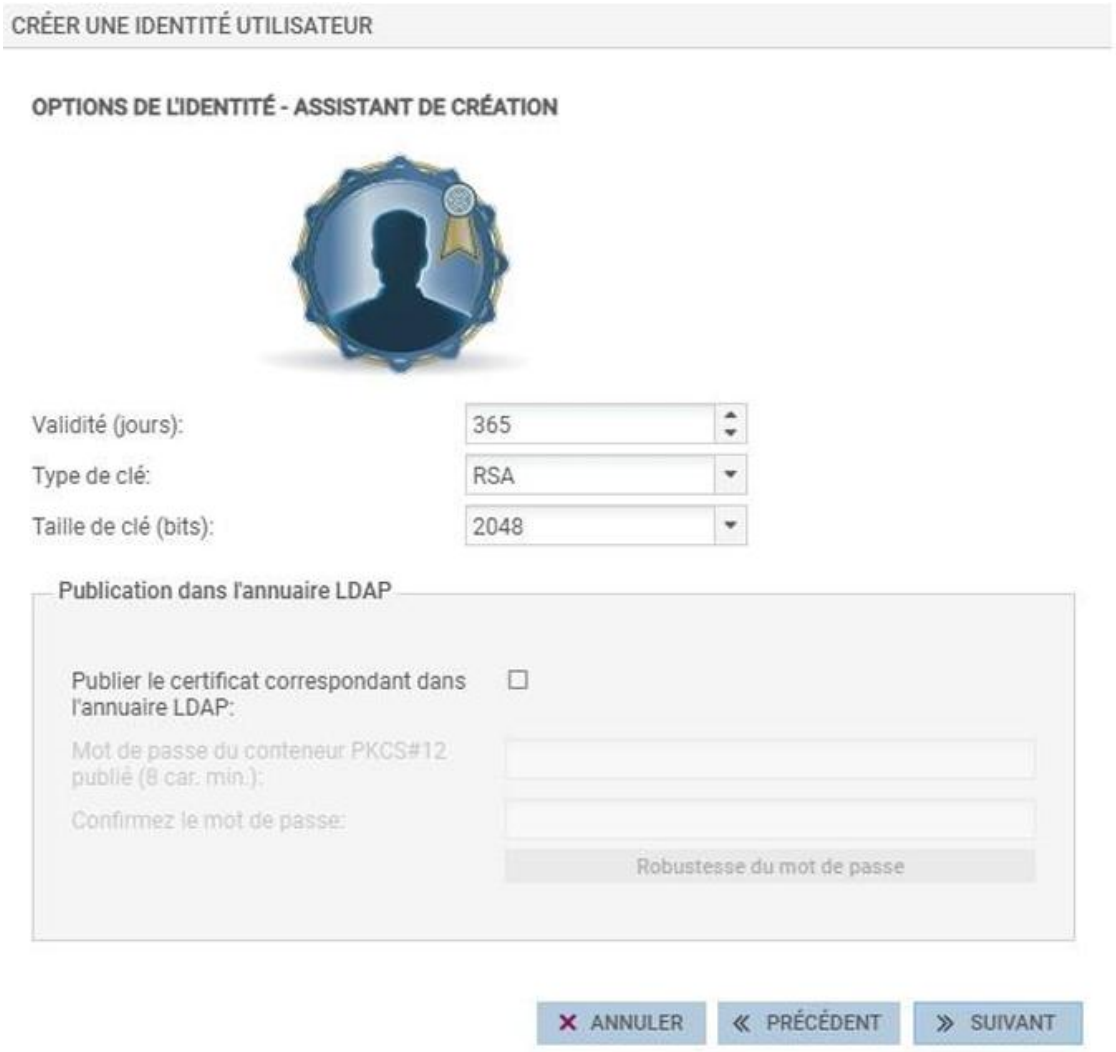
- **CN** : Nom de l’utilisateur (obligatoire)
- **Identifiant** (optionnel)
- **Adresse e-mail** (obligatoire)

Sélectionnez l'**autorité parente** pour signer le certificat.
Entrez le mot de passe de l'autorité.

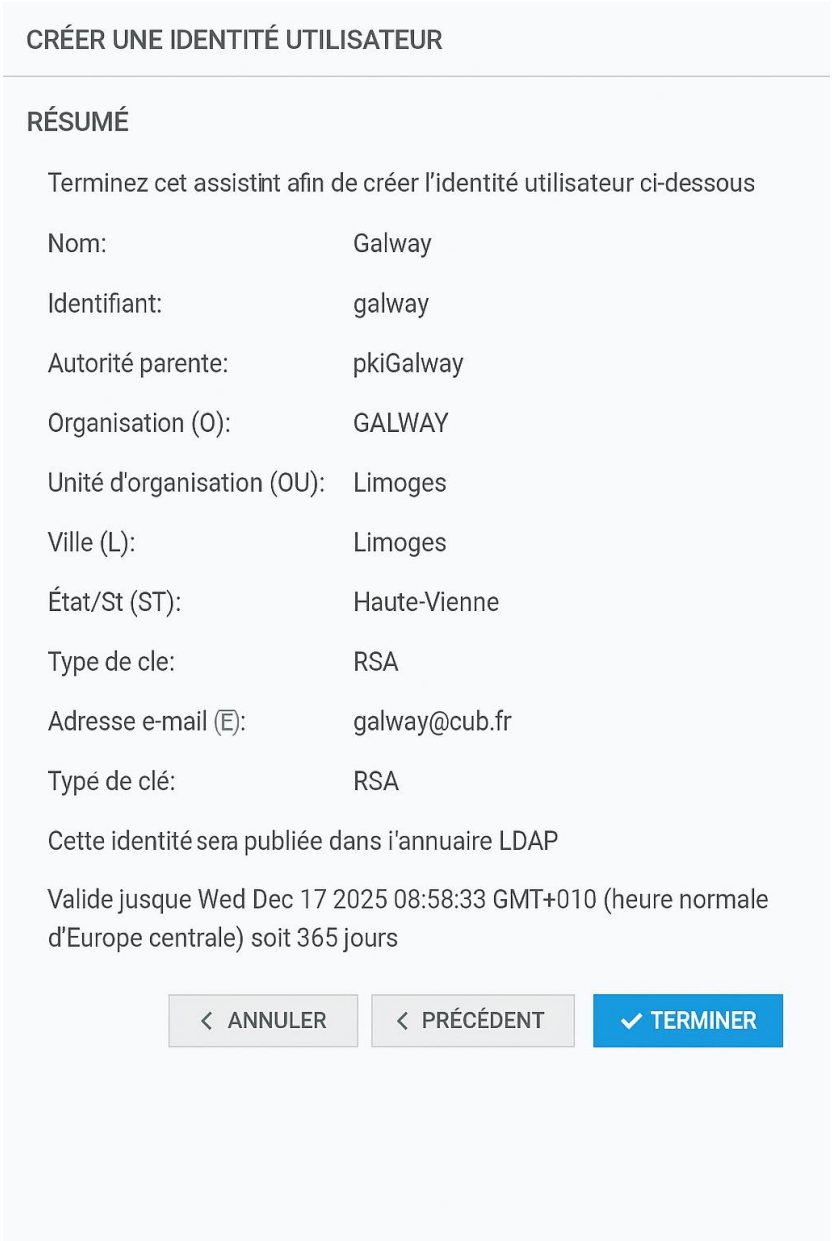


Activez l'option : **Publier dans l'annuaire LDAP**

Définissez un mot de passe pour protéger le fichier .p12



Cliquez sur **Terminer**.



L'identité est automatiquement ajoutée à l'arborescence des autorités, identités et certificats définis sur le firewall, sous son autorité parente.

Service Centreon

Qu’est-ce que Centreon ?

Centreon est une solution open source de **supervision réseau** qui permet de :

🖥️ **Surveiller l’état des serveurs, applications et équipements réseau**

📈 **Visualiser en temps réel les performances de votre infrastructure**

🔔 **Recevoir des alertes** en cas de défaillance d’un service ou d’un matériel

📡 **Centraliser les informations de supervision** sur une seule interface web

CONTEXTE

Mise en place du service Centreon pour réaliser la supervision des différents services.

Configuration serveur

Mettre à jour le système.

```
apt update && apt upgrade
```

Installer les dépendances :

```
apt update && apt install lsb-release ca-certificates apt-transport-https software-properties-common wget gnupg2 curl
```

Ajouter le dépôt Sury APT pour PHP 8.2 :

```
echo "deb https://packages.sury.org/php/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/sury-php.list
```

Importer la clé du dépôt :

```
wget -O- https://packages.sury.org/php/apt.gpg | gpg --dearmor | tee /etc/apt/trusted.gpg.d/php.gpg  > /dev/null 2>&1
```

Dépôt de base de données.

```
curl -LsS https://r.mariadb.com/downloads/mariadb_repo_setup | sudo bash -s -- --os-type=debian --os-version=12 --mariadb-server-version="mariadb-10.11"apt update
```

Installez le dépôt Centreon.

```
echo "deb https://packages.centreon.com/apt-standard-24.10-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon.list

echo "deb https://packages.centreon.com/apt-plugins-stable/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/centreon-plugins.list
```

Importer la clé du dépôt Centreon.

```
wget -O- https://apt-key.centreon.com | gpg --dearmor | tee
/etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1
```

Étape 2 : Installation

Installer ce serveur avec une base de données locale au serveur, ou une base de données distante sur un serveur dédié.

```
apt update
apt install -y centreon-mariadb centreon
systemctl daemon-reload
systemctl restart mariadb
```

Étape 3 : Configuration

Changer le nom d'hôte (optionnel) avec :

```
hostnamectl set-hostname nouveau-nom
```

Démarrage des services au démarrage du système

Pour que les services démarrent automatiquement au démarrage du système, exécutez les commandes suivantes sur le serveur central :

```
systemctl enable php8.2-fpm apache2 centreon cbd centengine
gorgoned centreontrapd snmpd snmptrapd
```

Exécutez ensuite la commande suivante (sur le serveur central si vous utilisez une base de données locale, ou sur votre serveur de base de données distant) :

```
systemctl enable mariadb
systemctl restart mariadb
```

Sécuriser la base de données.

```
mariadb-secure-installation
```

Répondez oui à toutes les questions, sauf à "Disallow root login remotely ?".

```
Disallow root login remotely? [Y/n]
```

Il est obligatoire de définir un mot de passe pour l'utilisateur root de la base de données. Ce mot de passe vous sera demandé pendant l'installation web.

```
root@centreon:~# mariadb-secure-installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
```

Étape 4 : Installation web

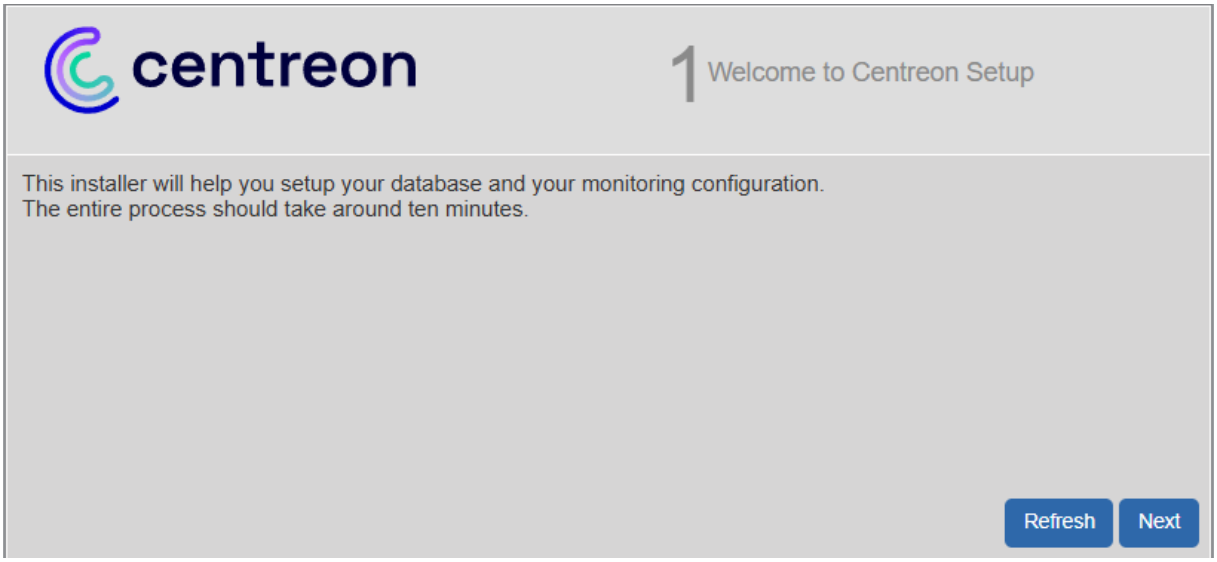
Démarrez le serveur Apache avec la commande suivante :

```
systemctl start apache2
```

Accéder à l'interface via le navigateur : http://[IP]/centreon

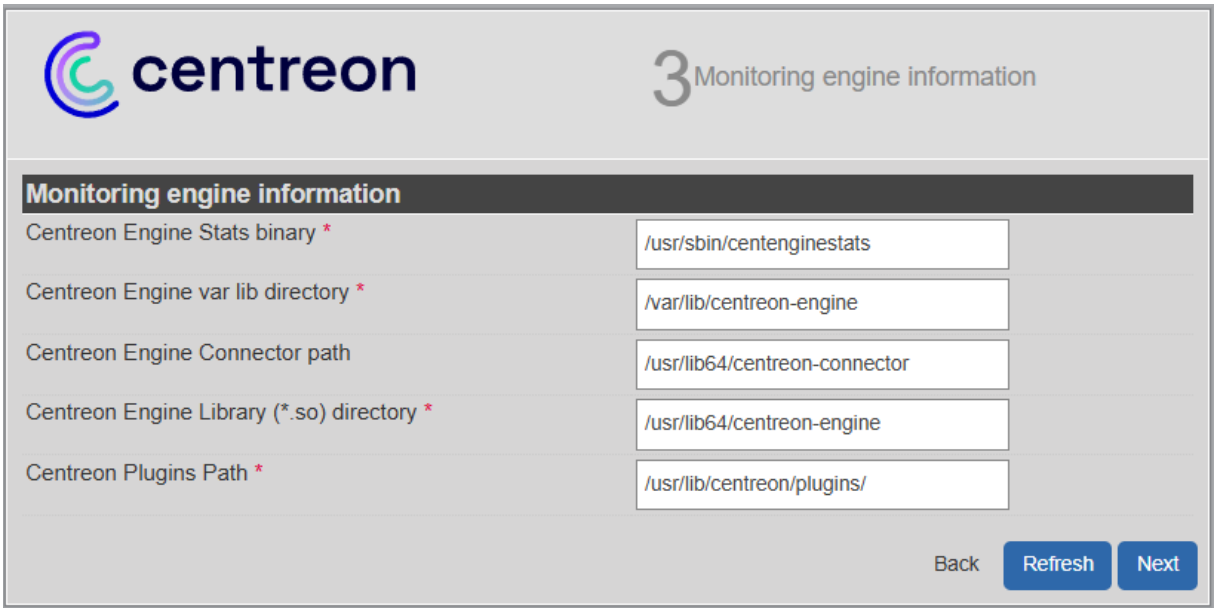
Vous devez voir cette page :

Taper sur Next.

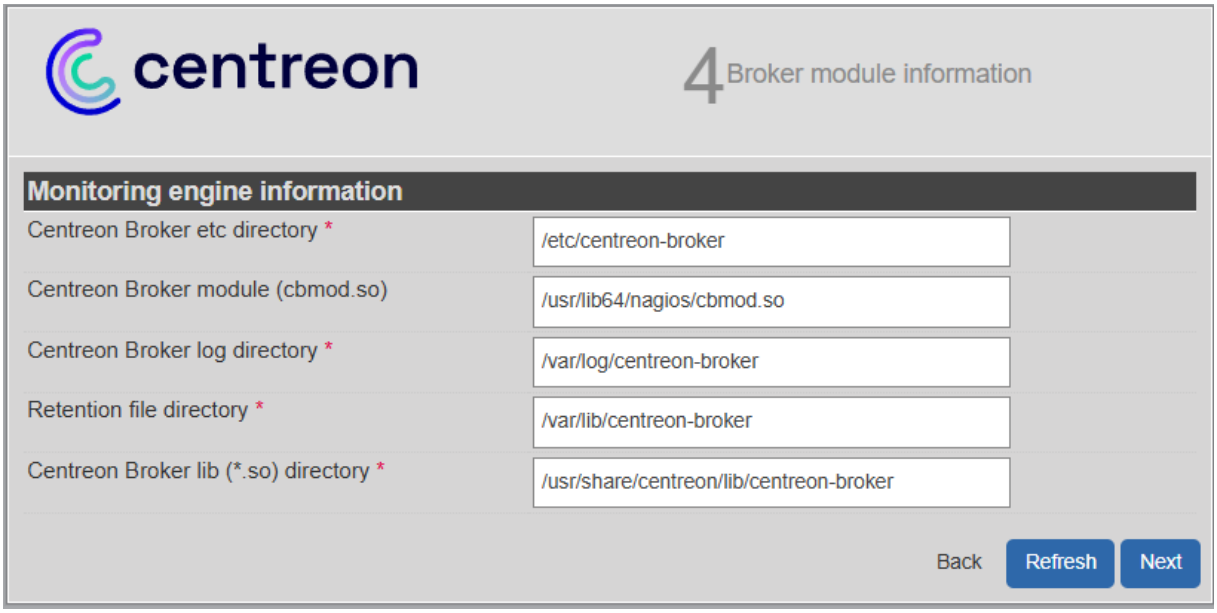


Taper sur Next.

Taper sur Next.



Taper sur Next.



Renseigner les informations pour le compte admin (log :admin mot de passe...)

Entrez les information de la base de données

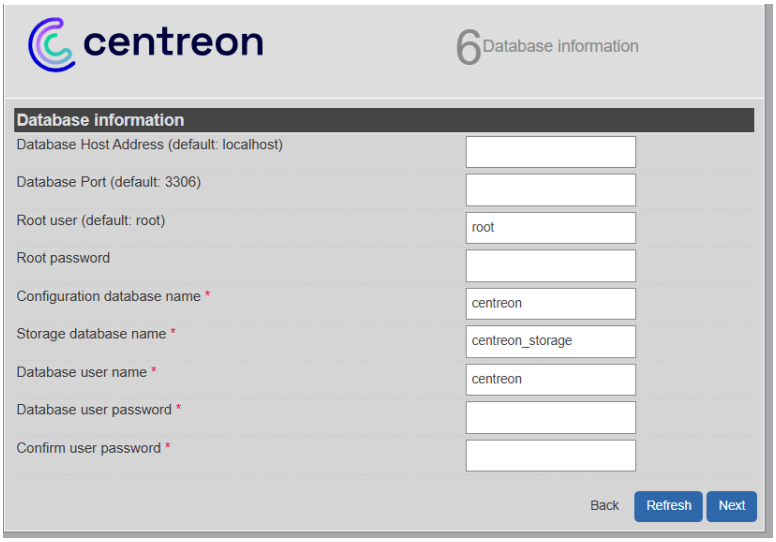
Log :root

Mot de passe :

Database(base de données)

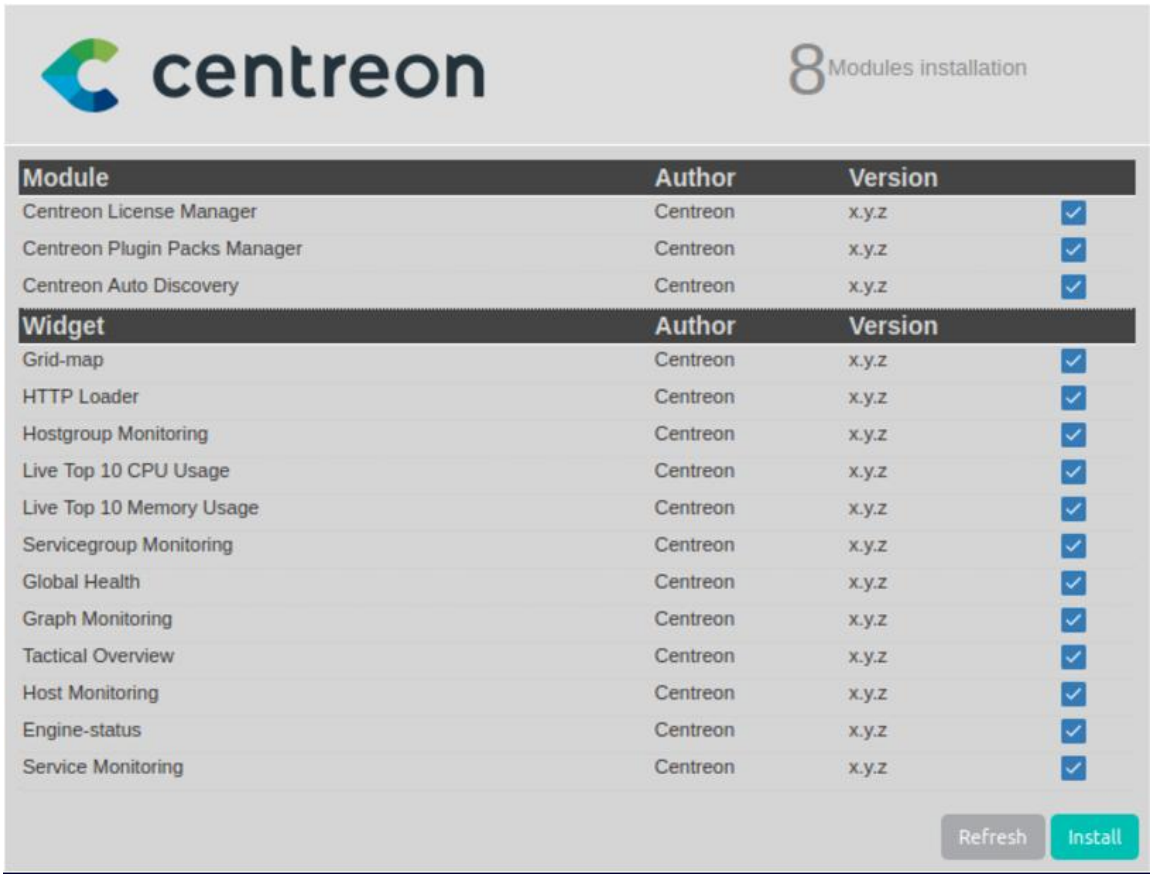
Name :centreon

Password :centreon

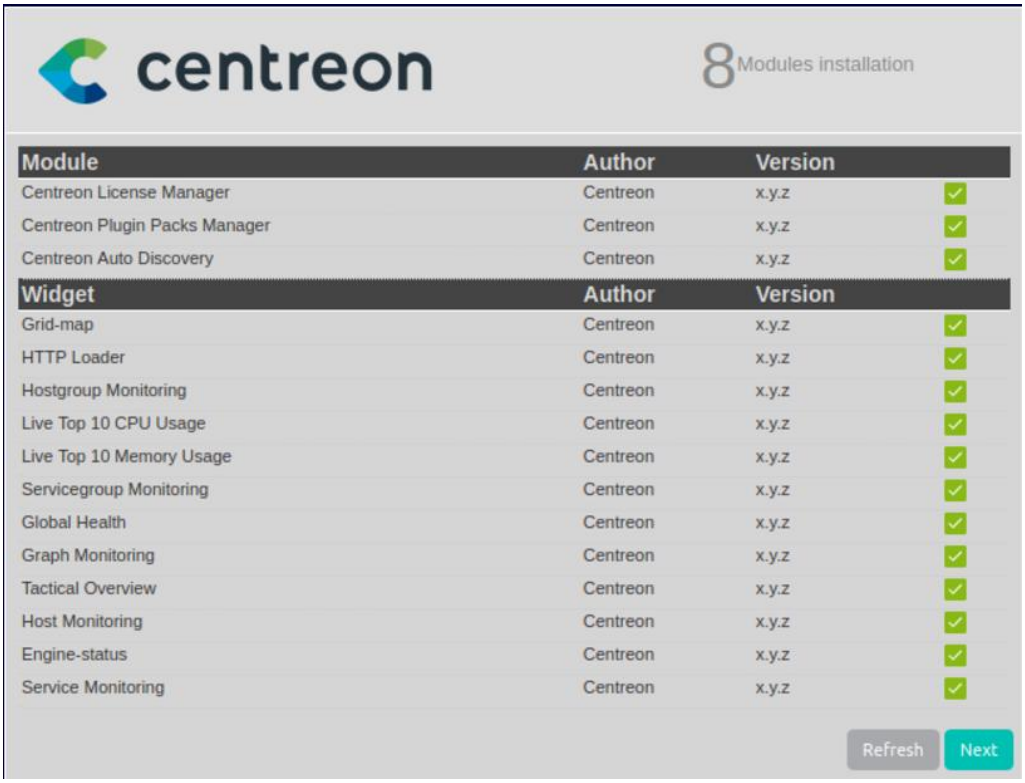


Taper sur Next.

Cliquer sur installer.



Cliquer sur Next.



Cliquer sur Finish.

Vous pouvez maintenant vous connecter en utilisant le compte admin.

Installation Agent SNMPD SUR DEBIAN

Installer le service SNMPD.

```
root@debian:~# apt install snmpd
```

Modifier le fichier /etc/apt/sources.list

```
root@debian:~# nano /etc/apt/sources.list
```

Pour accepter les 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.

```
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
```

Mettre à jour la liste des paquets et lancez l'installation de snmp-mibs-downloader :

```
root@debian:~# apt update && apt upgrade
root@debian:~# apt install snmp-mibs-downloader
root@debian:~# download-mibs
```

Download-mibs, les MIBS sont téléchargées dans le répertoire /usr/share/mibs.

Configurer le serveur SNMP sur l'hôte Debian :

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

```
root@debian:~# cp /etc/snmp/snmpd.conf
```

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

```
root@debian:~# nano /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:

```
#agentAddress udp:127.0.0.1:161
```

Et en décommentant la ligne suivante :

```
#agentAddress udp:161,udp6:[::1]:161
```

Modifier dans ce fichier les conditions d'accès à la MIB :

L'accès en lecture est défini par la directive rocommunity.
Par défaut, cet accès est restreint à une seule vue systemonly via l'option -V.
Crée votre propre view.

```
#view centreon included .1.3.6.1
#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]
rocommunity public default -V all
# Read-only access to everyone to the systemonly view
#rocommunity  public default -V systemonly
#rocommunity6 public default -V systemonly
```

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

```
root@debian:~# nano /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 ':'

```
# This file controls the behaviour of /etc/init.d/snmpd
# but not of the corresponding systemd service file.
# If needed, create an override file in
# /etc/systemd/system/snmpd.service.d/local.conf
# see man 5 systemd.unit and man 5 systemd.service

# Don't load any MIBs by default.
# You might comment this lines once you have the MIBs downloaded.
export MIBS=ALL

# snmpd options (use syslog priority warning, close stdin/out/err).
#SNMPDOPTS='-LSwd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I -smux,mt
```

Modifiez le fichier de configuration /etc/snmp/snmpd :

```
root@debian:~# nano /etc/snmp/snmp.conf
```

Et commentant la ligne mibs (nano /etc/snmp/snmp.conf):

```
# As the snmp packages come without MIB files due to license reasons, loading
# of MIBs is disabled by default. If you added the MIBs you can reenable
# loading them by commenting out the following line.
#mibs :
```

Redémarrer le service snmpd :

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

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

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

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

```
root@debian:~# nano /etc/snmp/snmpd.conf
```

Restreindre les accès en créant une communauté gsb et précisez par exemple comme adresse IP du gestionnaire 172.17.0.1. Si vous voulez autoriser n'importe quel gestionnaire SNMP sur le réseau, indiquez l'adresse du réseau c'est-à-dire 172.17.0.0/24.

```
# Views
#   arguments viewname included [oid]
 rocommunity gsb 172.17.0.1
```

Démarrez/redémarrez les processus de collecte :

```
root@debian:~# systemctl restart cbd centengine
```

Redémarrez le gestionnaire de tâches.

```
root@debian:~# systemctl restart gorgoned
```

Démarrez les services de supervision passive

```
root@debian:~# systemctl start snmptrapd centreontrapd
```

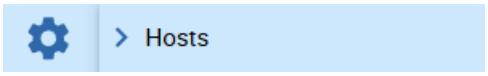
Si vous voulez superviser ce serveur, démarrer le démon SNMP.

```
root@debian:~# systemctl start snmpd
```

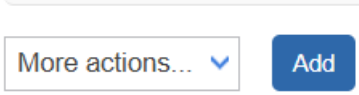
Partie serveur Centreon

Ajout d'un hôte :

Aller dans Hosts.



Cliquer sur Add.



Ajouter les informations ci-dessous :

Donne-lui un nom.

Alias ne mettait rien.

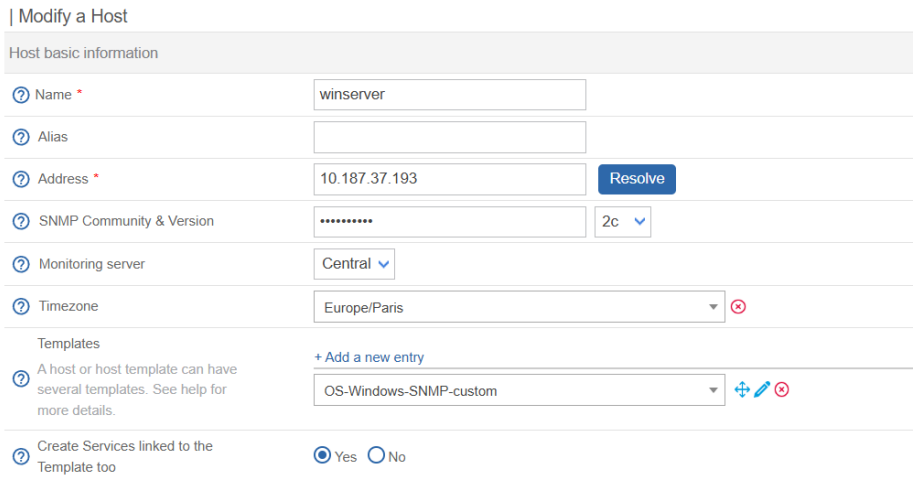
Mettre le nom de votre communauté et la version.

Monitoring server laissé central.

Timezone, mettez votre lieu géographique.

Template server windows-SNMP-custom

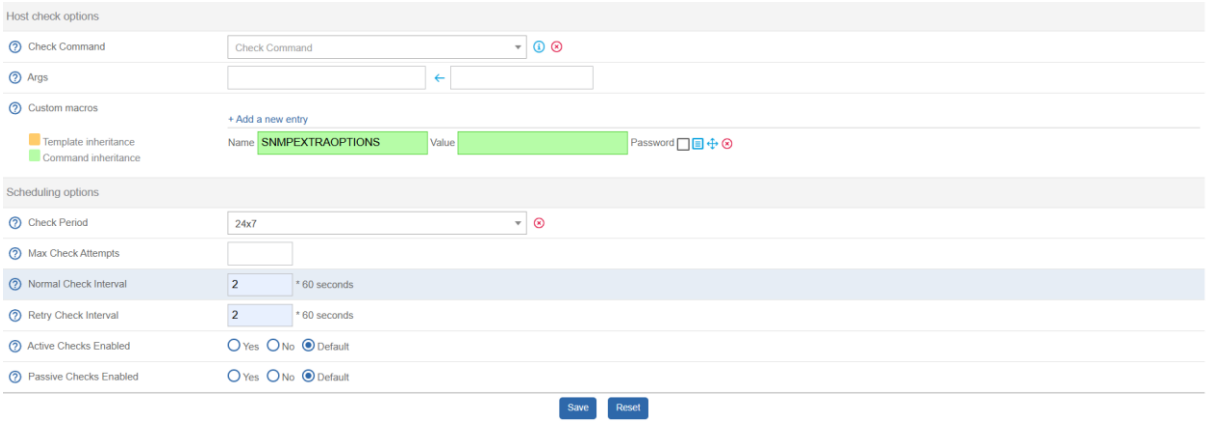
Cliquer sur yes.



Check period mettre 24x7.

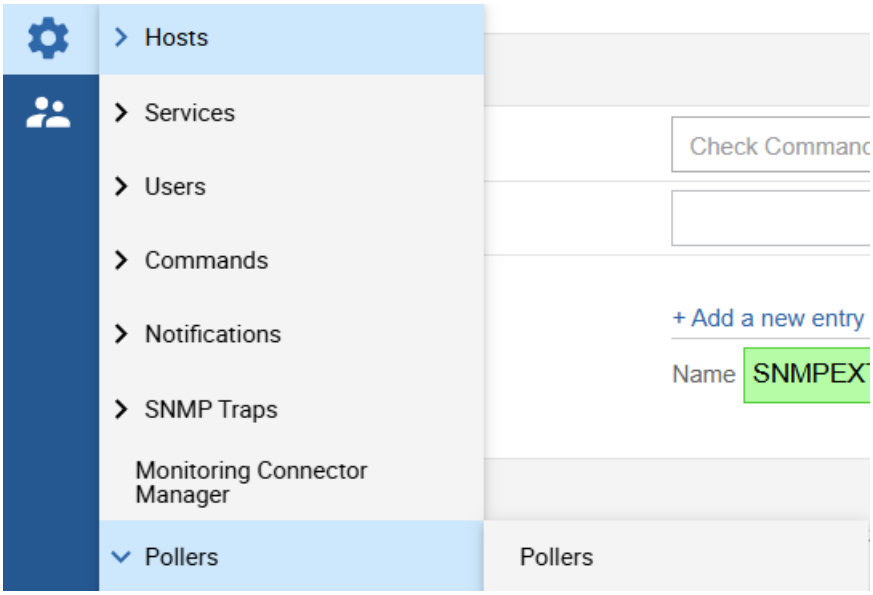
Pour les intervalles mettre la valeur que vous voulez, c'est en seconde.

Puis cliquer sur Save.



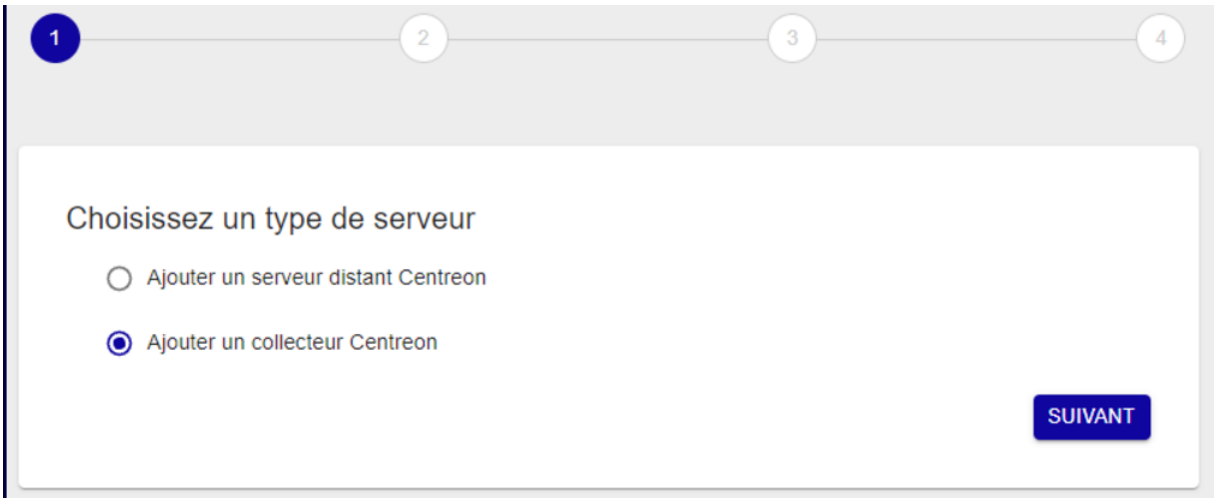
Exporter la configuration :

Aller dans pollers.

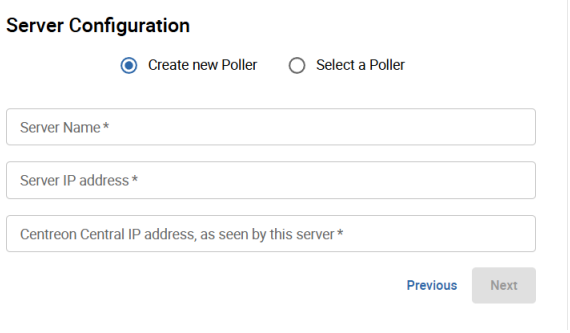


Nous allons créer le serveur central.

Choisir le type de server et cliquer sur suivant.

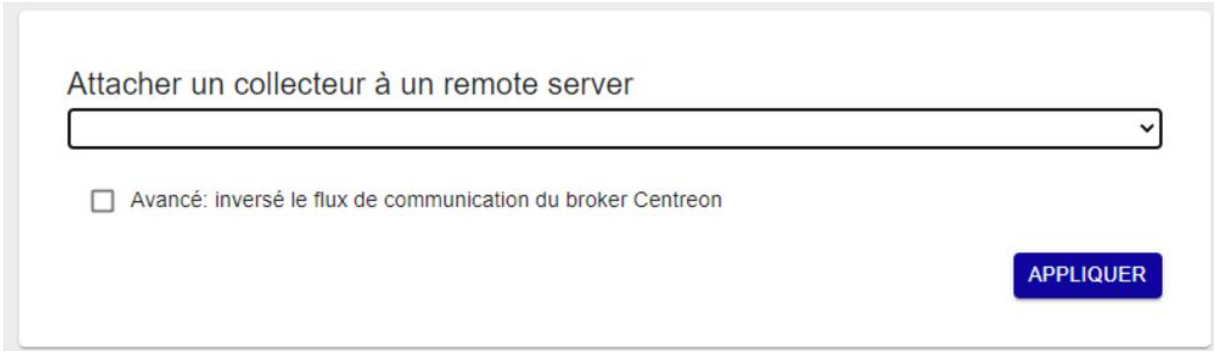


Choisir un nom pour votre serveur, renseigner l'adresse IP du serveur et celle de la centrale de Centreon puis cliquer sur Next.



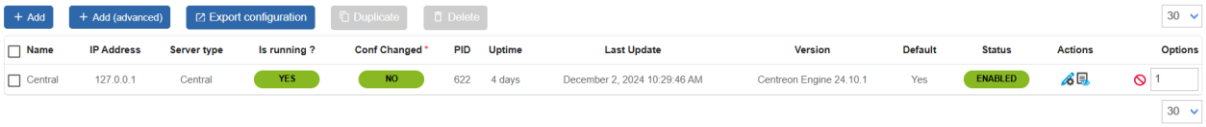
Si vous souhaitez lier ce collecteur au serveur Central, cliquez sur Appliquer :

Mais si vous souhaitez lier ce collecteur à un serveur distant, sélectionnez celui-ci dans la liste et cliquez sur Appliquer.

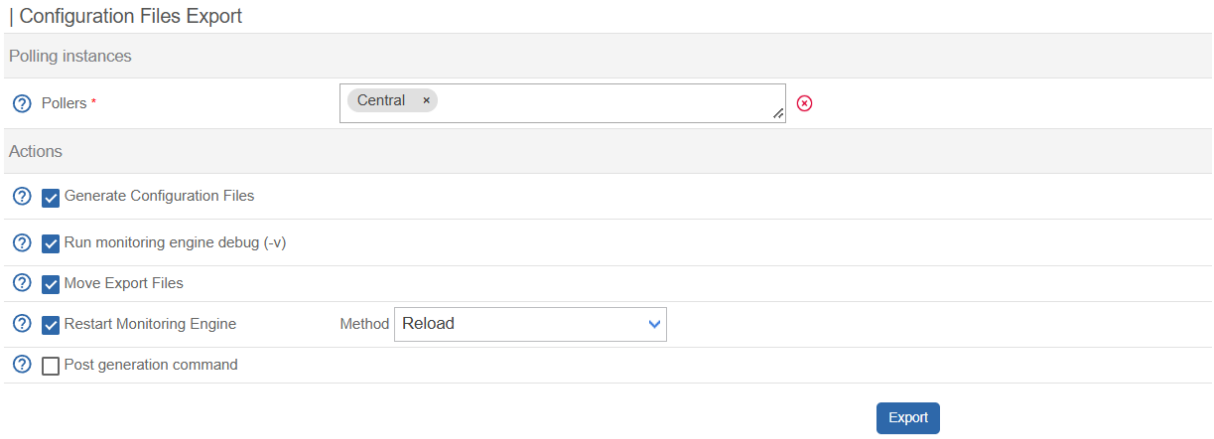


Patientez quelques secondes, l'assistant va configurer votre nouveau serveur.

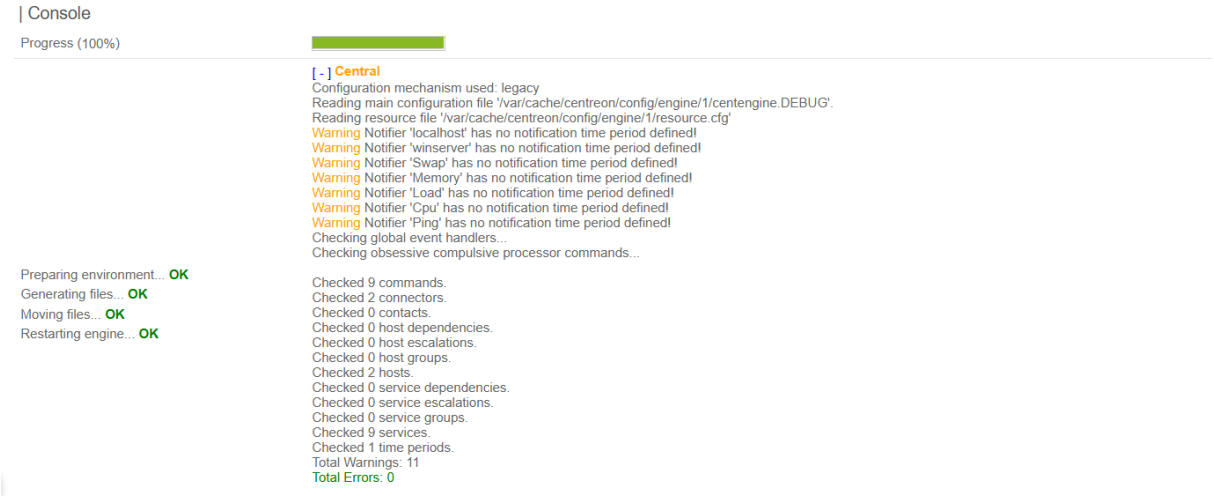
Voici notre Serveur. Cliquer sur export configuration.



Cocher les quatre premières cases puis cliquer sur export.

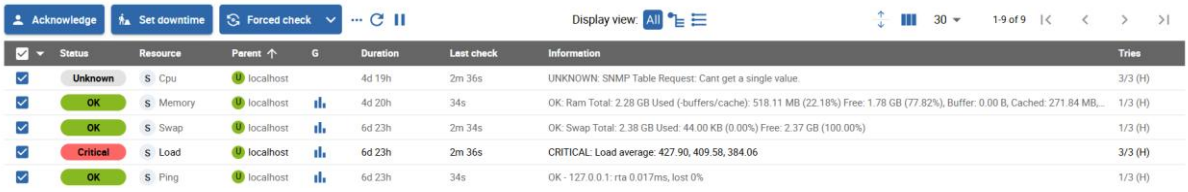


Une fois l'exportation terminée.



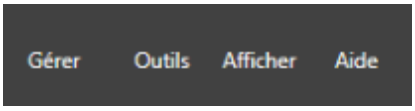
On peut voir les services qui apparaissent.

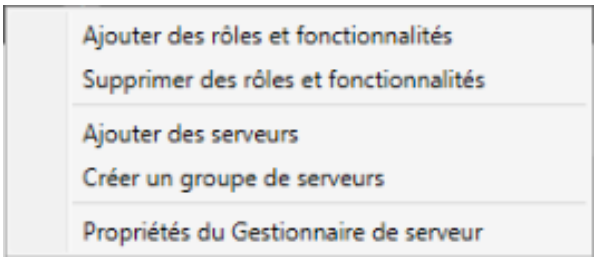
Si le service n'apparaît pas, cliquez sur Services. Puis cocher les cases et cliquer sur forced check.



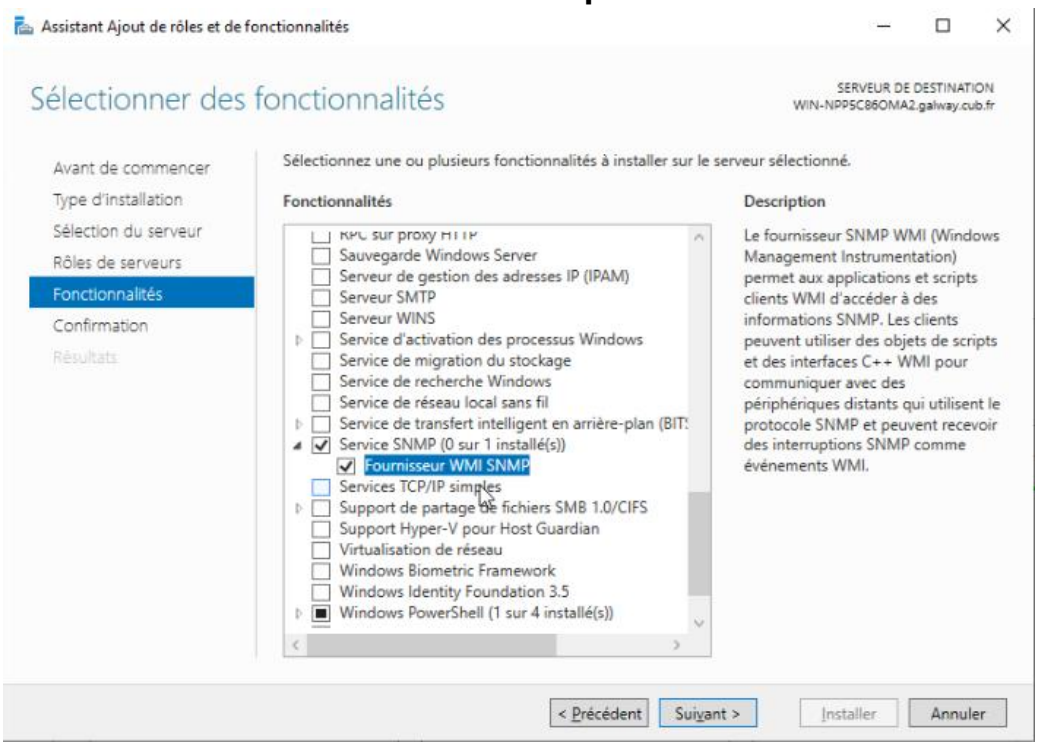
Installation Agent SNMPD SUR WINDOWS

Ouvrir le Gestionnaire de serveur > Gérer > Ajouter des rôles.

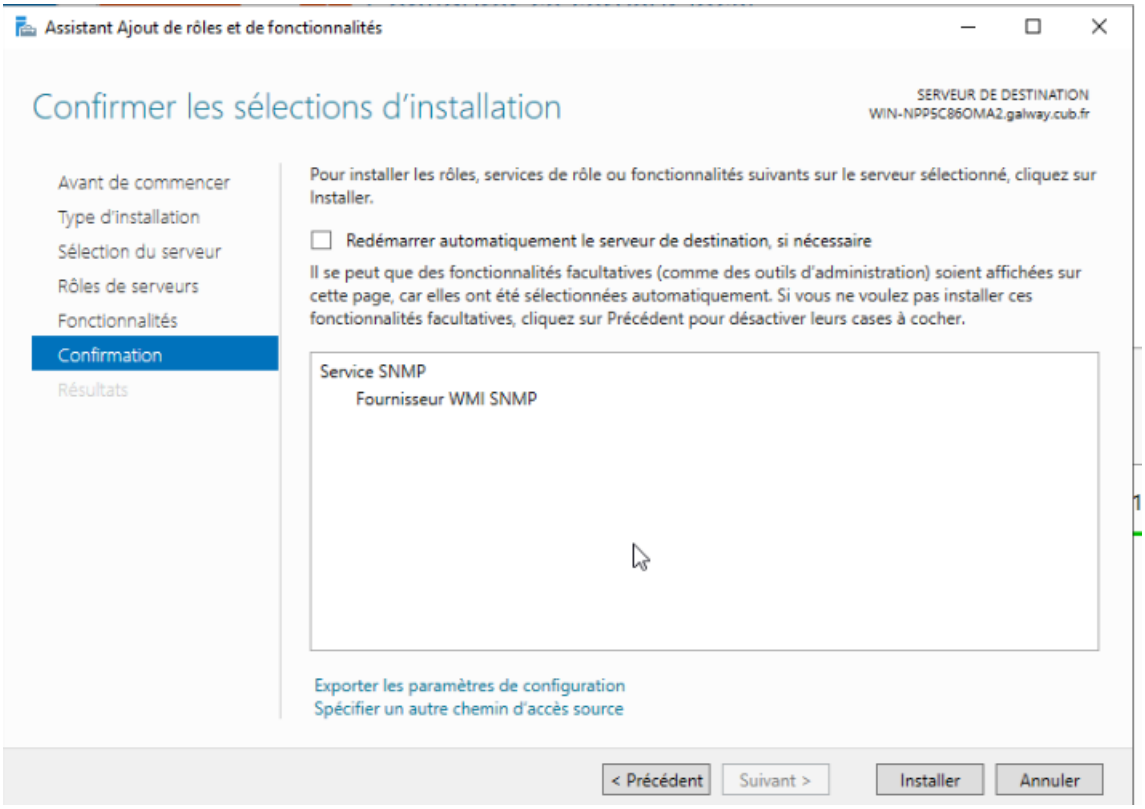




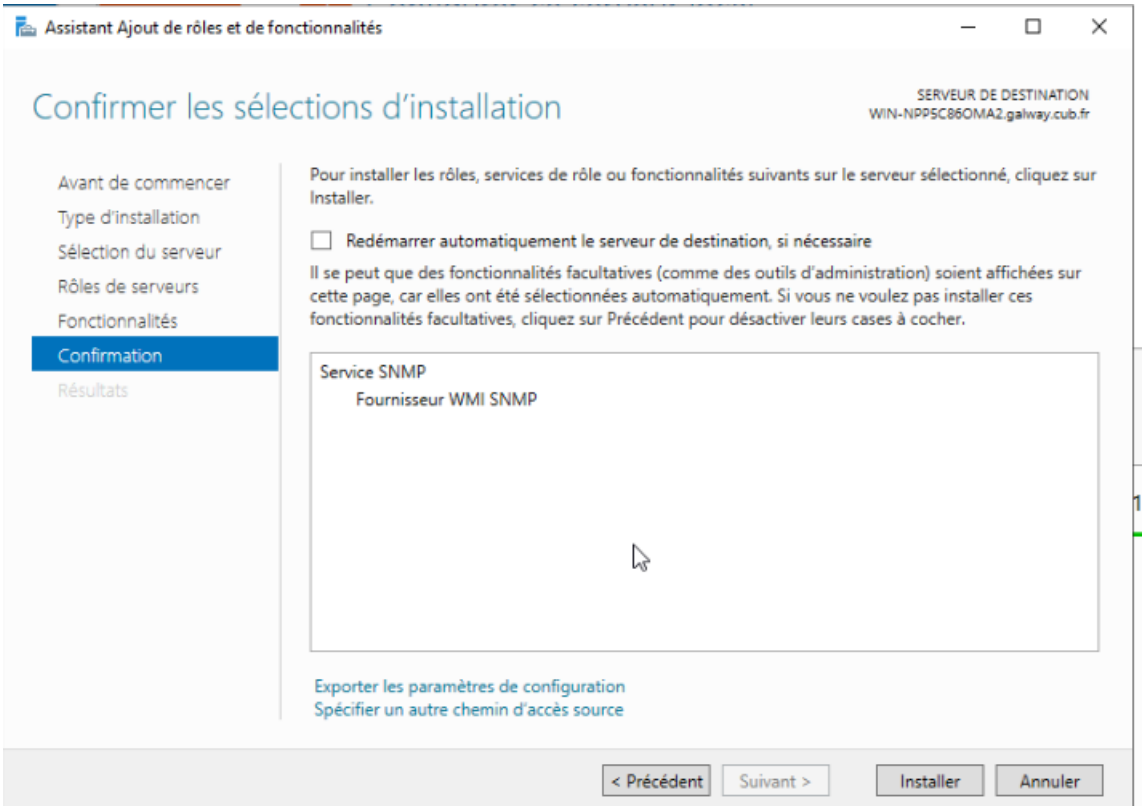
Passez les 4 premières étapes sans effectuer de modifications, jusqu'à arriver à l'étape Fonctionnalités. Ici, vous devez cocher Service SNMP et fournisseur WMI SNMP. Puis cliquer sur suivant.



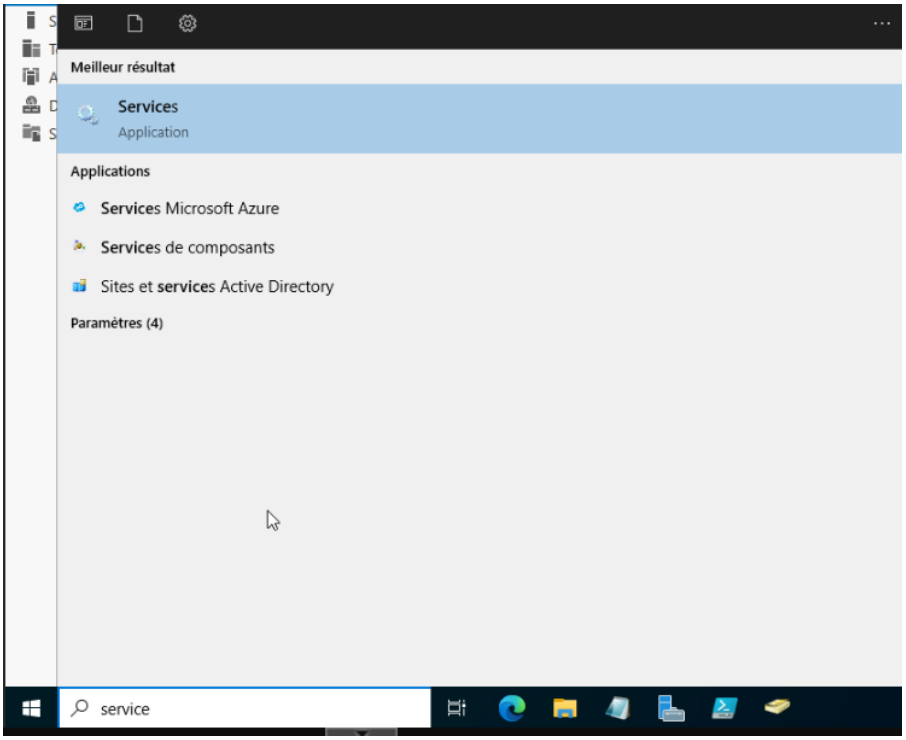
Cliquer sur Installer.



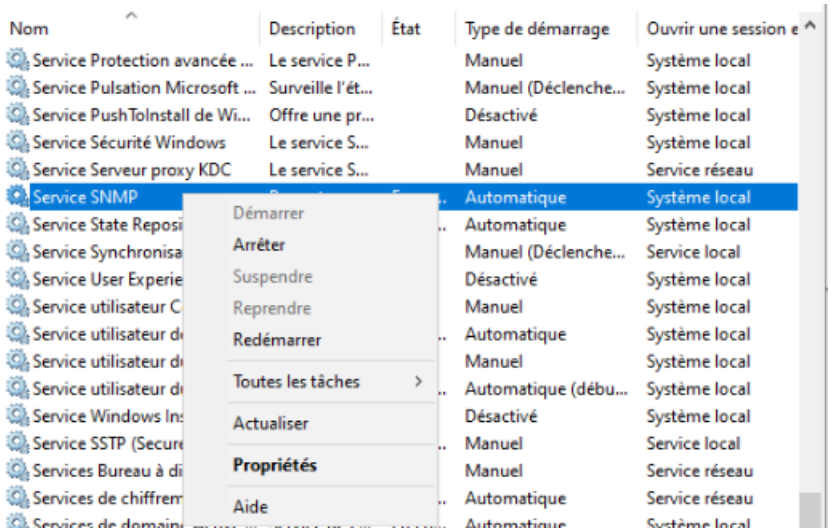
Une fois installé, cliquer sur fermer.



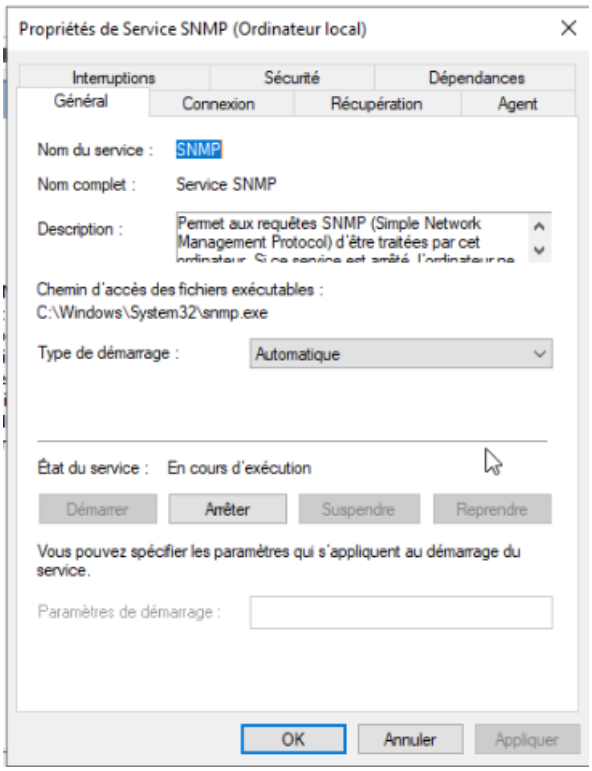
Aller dans la barre des tâches, cliquer sur rechercher et taper service.



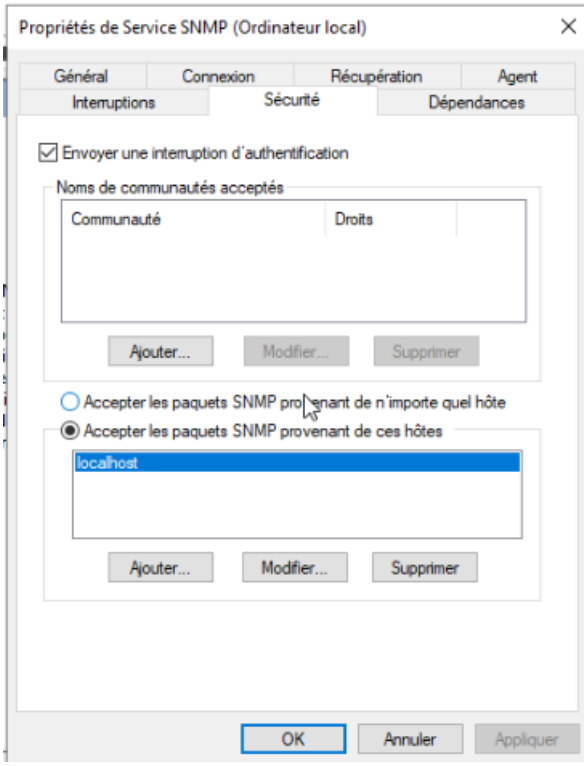
Chercher le service SNMP et faites un clic droit puis cliquez sur propriétés.



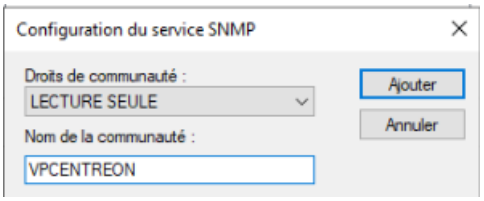
Aller dans sécurité.



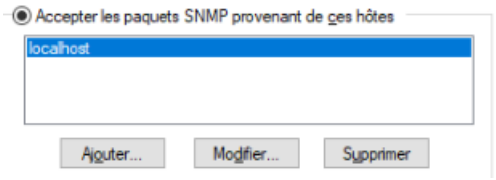
Cliquer sur ajouter nom de communauté.



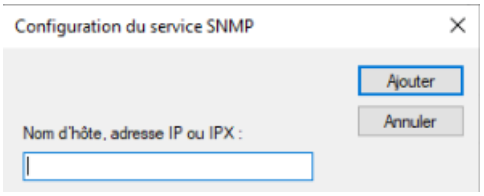
Ajouter un nom de communauté et cliquer sur ajouter.



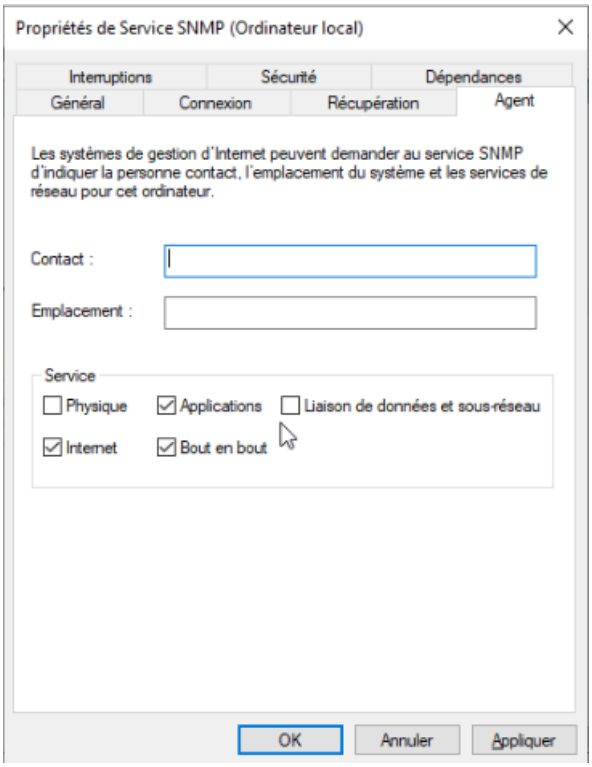
Laisser accepter les paquets SNMP. Et ensuite cliquer encore sur ajouter.



Ajouter l'adresse IP de votre serveur Centreon et cliquer sur ajouter.



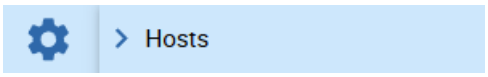
Ensuite, cliquer sur l'onglet Agent.



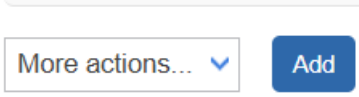
Cet onglet sert à indiquer des informations à votre serveur pour les intégrer dans l'agent SNMP. *Contact* va permettre d'indiquer les infos sur la personne qui administre ce serveur (un nom, un prénom, ou une adresse e-mail), alors que le champ *Emplacement* sert à indiquer où se trouve ce serveur. Une fois cela fait cliquer sur Ok.

Sur la partie serveur Centreon

Aller dans Hosts.



Puis cliquer sur Add.



Ajouter les informations ci-dessous :

Donne-lui un nom.

Alias ne mettait rien.

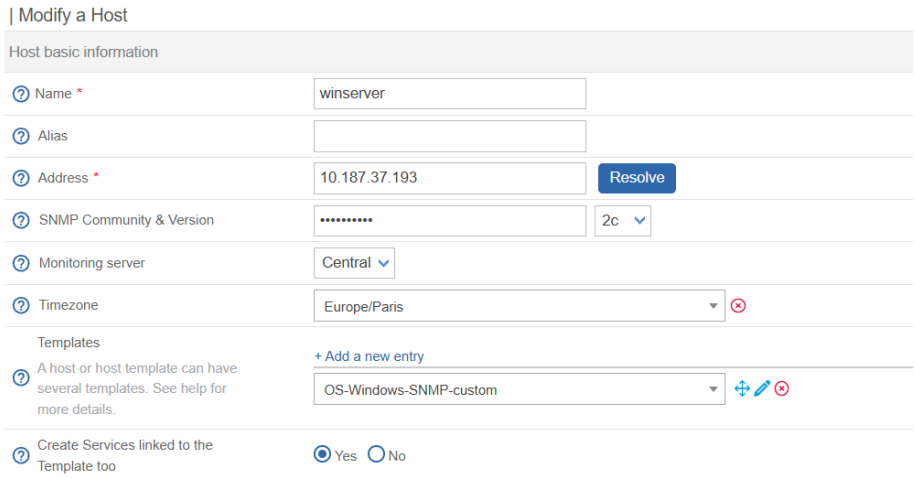
Mettre le nom de votre communauté et la version.

Monitoring server laissé central.

Timezone, mettez votre lieu géographique.

Template server windows-SNMP-custom

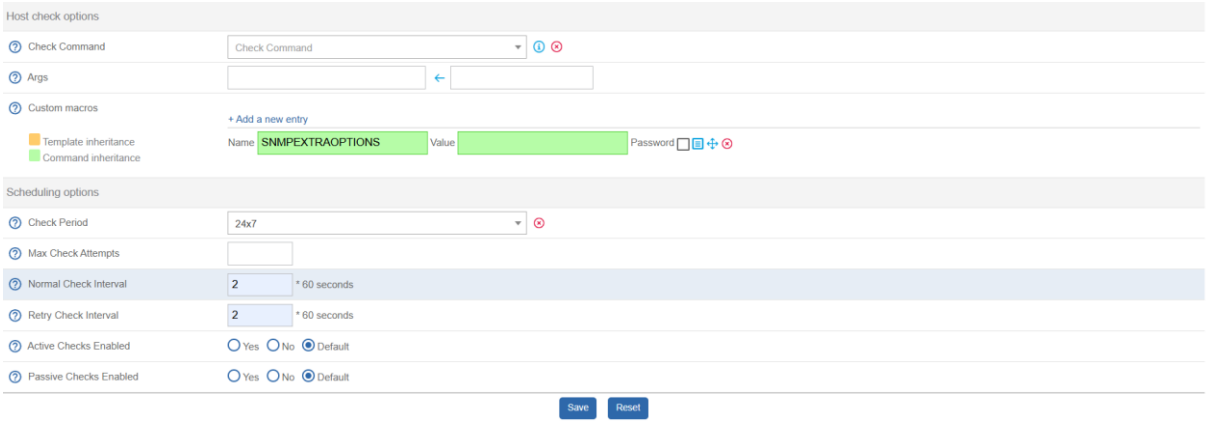
Cliquer sur yes.



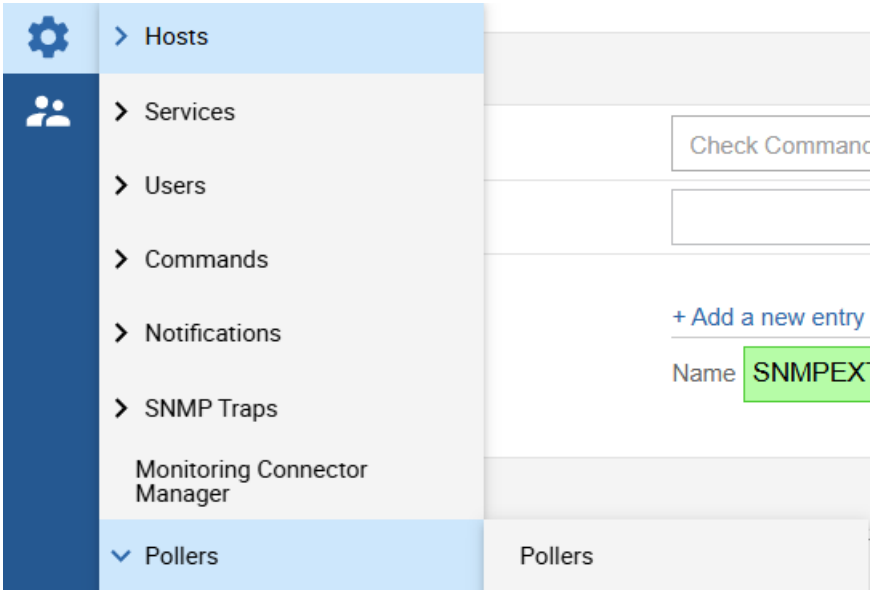
Check period mettre 24x7.

Pour les intervalles mettre la valeur que vous voulez, c'est en seconde.

Puis cliquer sur Save.

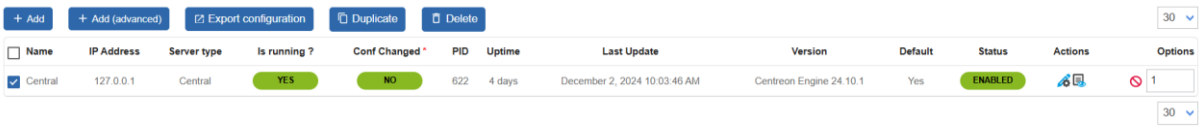


Aller dans pollers.

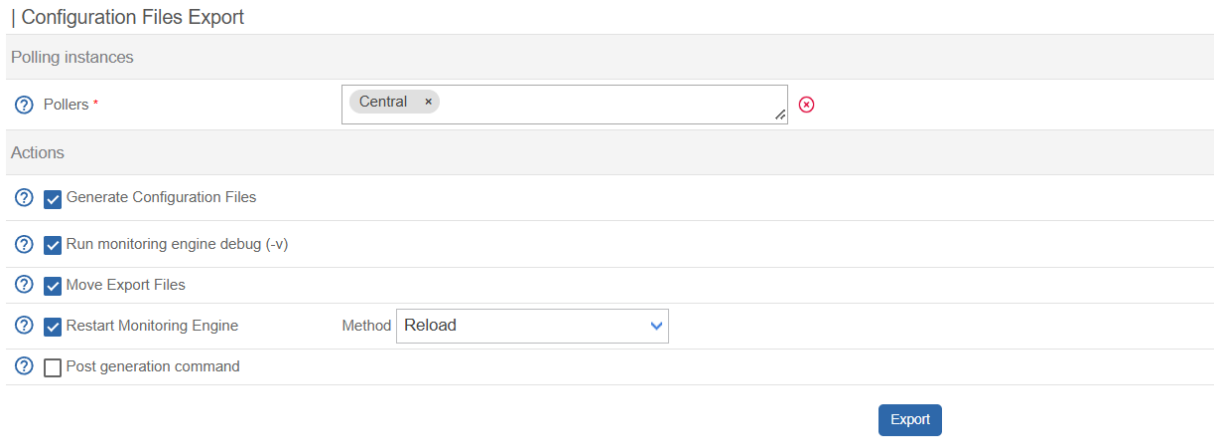


Nous allons utiliser le serveur central qu'on a créé.

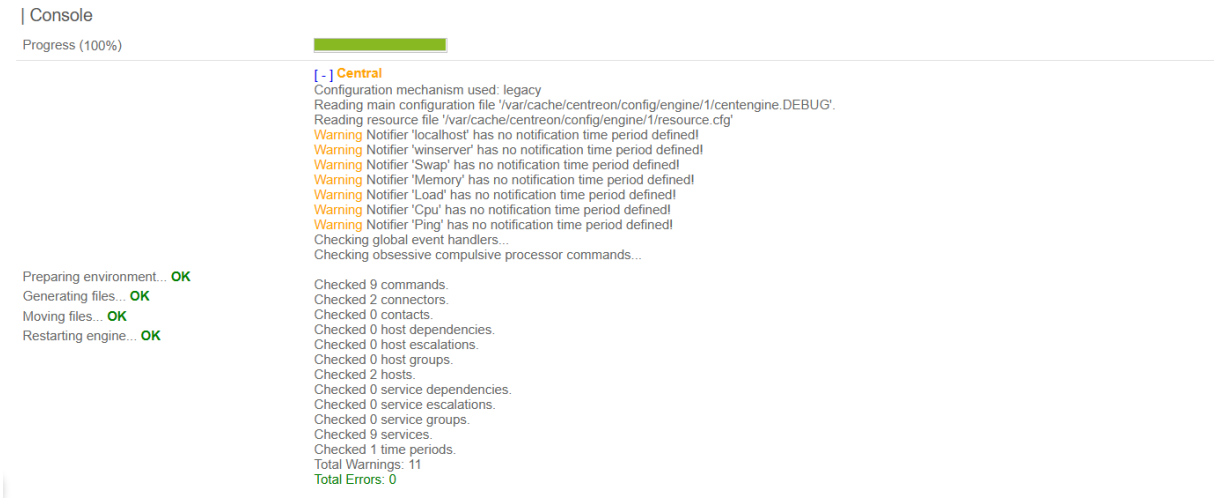
Cliquer sur le petit carré, puis export configuration.



Cocher les quatre premières cases puis cliquer sur export.

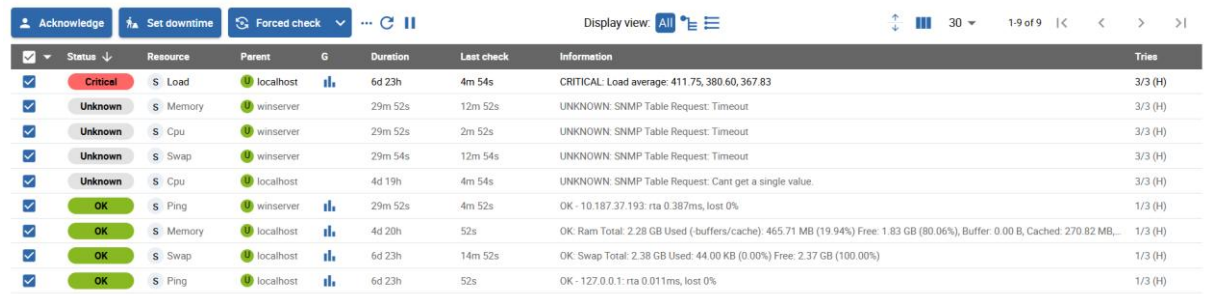


Une fois l'exportation terminée.



On peut voir les services qui apparaissent.

Si le service n'apparaît pas, cliquez sur Services. Puis cocher les cases et cliquer sur forced check.

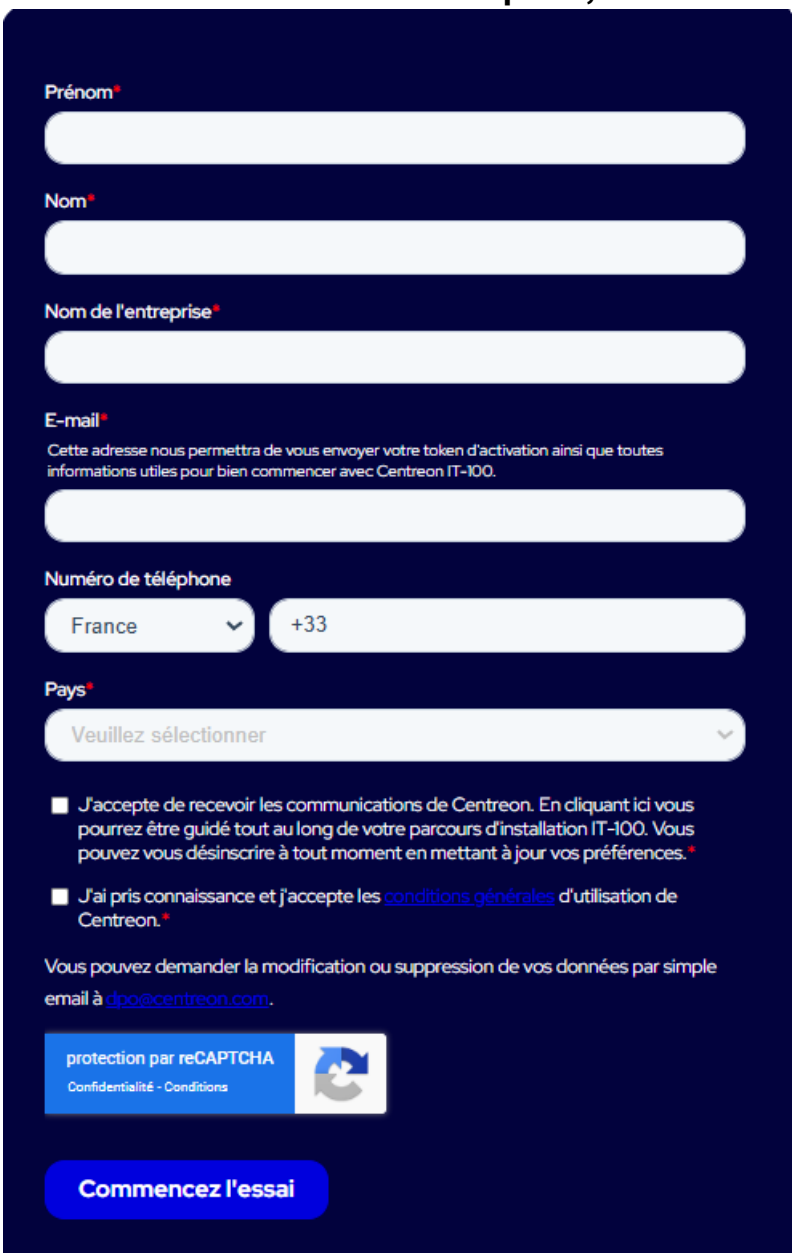


Ajout Centreon IT Edition

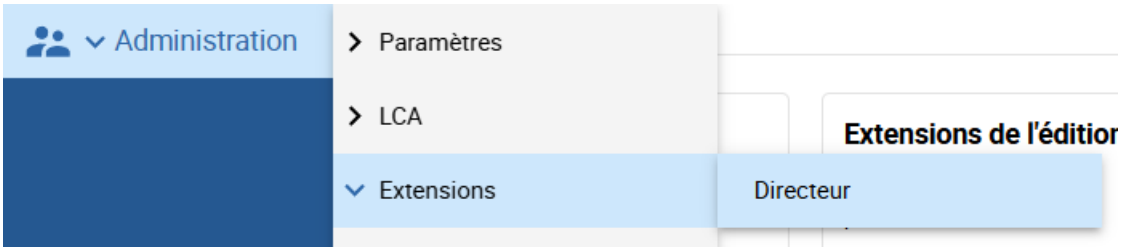
Cliquer sur le lien ci-dessous

https://www.centreon.com/fr/essai-gratuit/

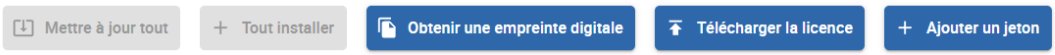
Une fois les informations remplies, le code vous a été envoyé par mail.



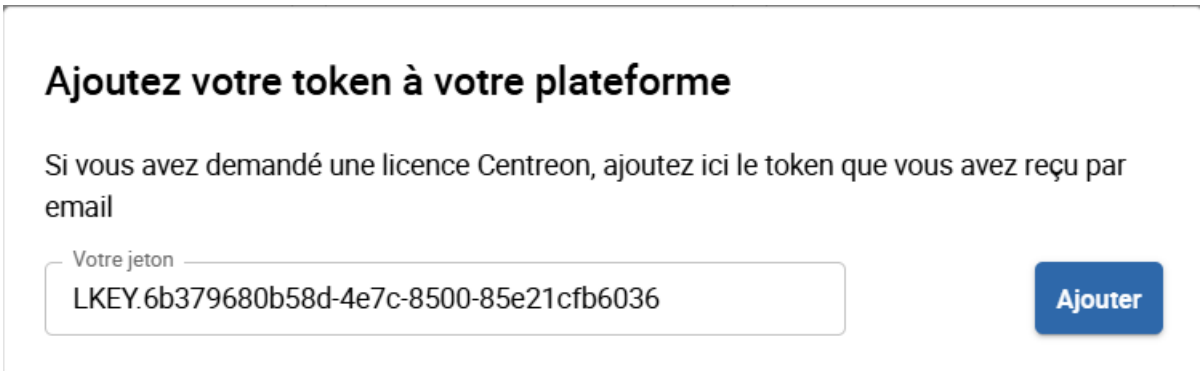
Retourner sur votre serveur Centreon et aller dans administration.



Cliquer sur ajouter un jeton .



Entrez le code, puis cliquez sur ajouter.



Si votre licence a été ajoutée, vous verrez ce message.