Documentation technique

Schéma logique du réseau CUB ET Plan d'adressage

schema_reseau-marrakech.drawio.drawio.xml

Agence Marrakech

Agence	ID VLAN	Adresses de sous-réseaux	Adresses IP de votre firewall Stormshield
Marrakech	342	**DMZ :** 172.16.13.0/24	**dmz :** 172.16.13.254
343	**SERVEURS :** 172.16.33.0/24	**dmz :** 172.16.33.254	
344	**LAN :** 192.168.13.0/24	**in/lan :** 192.168.13.254	
302	**WAN :** 192.168.229.0/24	**out :** 192.168.229.42	

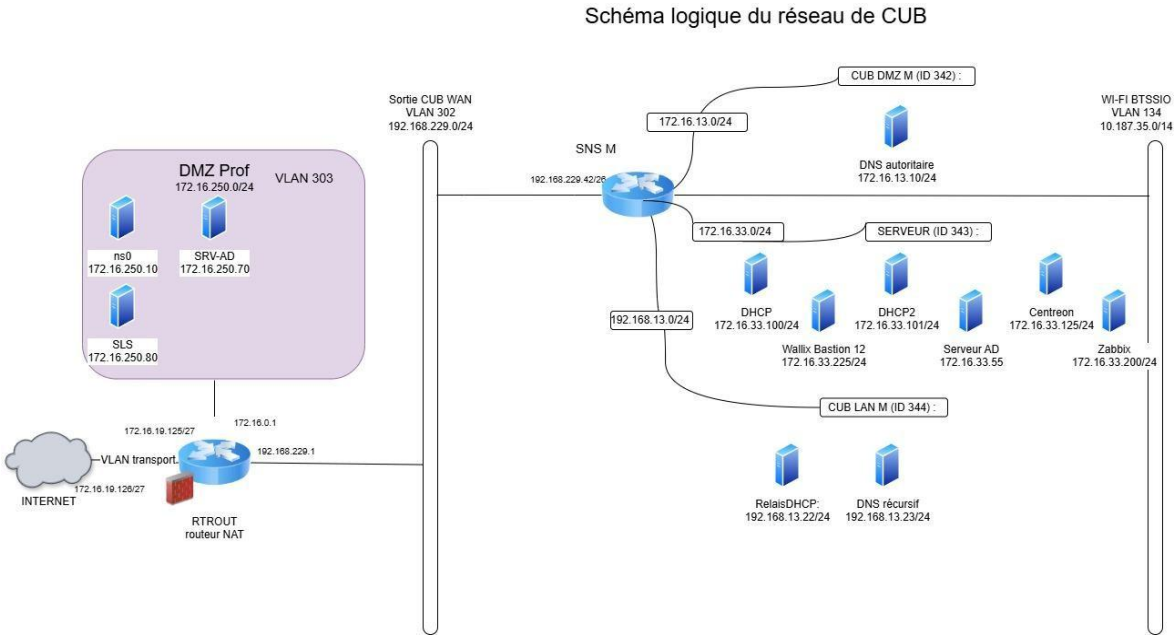
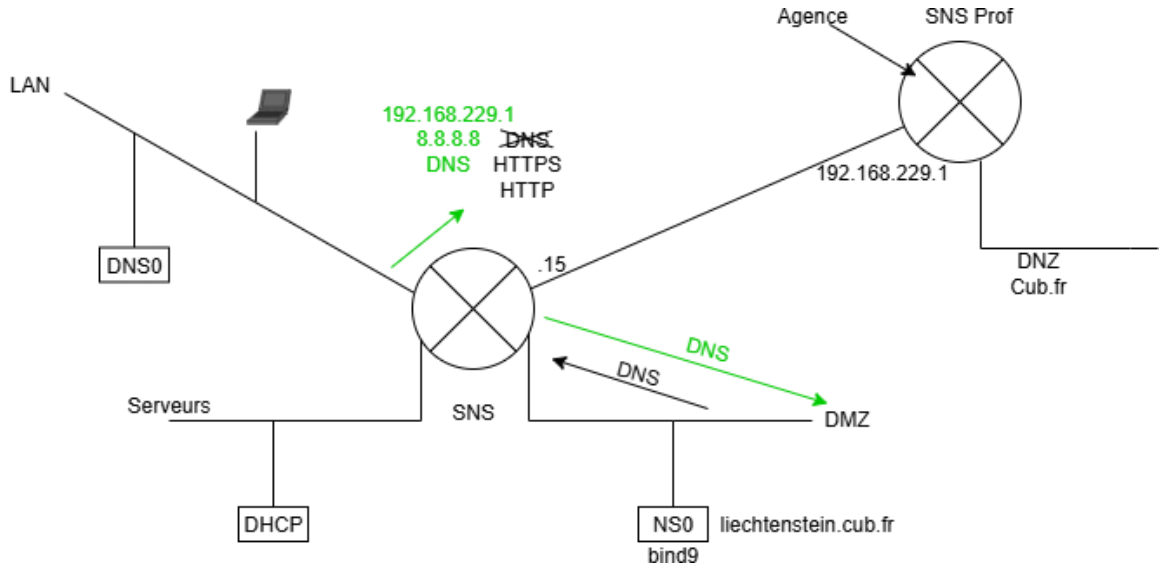


Schéma réseau DNS :



projets :

- I -Configuration des ports d'un Switch L3
- II -Configuration du service DHCP et de l'Agent relais DHCP avec Linux Debian
- III -Configuration du pare-feu Stormshield
- IV -Configuration du service DNS (ns0)
- V -Configuration du service DNS récursif(Dns0)
- VI -Configurer un domaine Microsoft Active Directory
- VII -Configuration du service DHCP en Failover/Load-balancing
- VIII - Configurer le service DNS pour adapter ses réponses aux clients internes et externes au réseau
- IX - Mise en place d'une solution de supervision Centreon avec activation de licence IT-100
- X - Supervisation du service Apache2 et PHP
- XI - Déploiement Wallix Bastion
- XII - Mise en place d'une solution de supervision Zabbix et Ajouts des agents Zabbix
- XIII - Activité réplication de bases de données

Retour :

- Retour à la page d'accueil de l'équipe

Création des VLANs:

Depuis la console de configuration du switch :

configure terminal
vlan 342
 name DMZ
vlan 343

```
 name SERVEURS
vlan 344
 name LAN
vlan 302
name WAN
exit
```

vlan 342 correspondant au réseau DMZ (172.16.13.0/24)

- **vlan 343** pour le réseau SERVEURS (172.16.33.0/24)
- **vlan 344** pour le réseau LAN (192.168.13.0/24)

- **vlan 302** pour le réseau WAN (192.168.229.0/24)
- Les VLANs sont donc ainsi créer dans la base de données du switch.

Affectation des ports aux VLANs:

Il faut maintenant indiquer quels ports physiques appartiennent à quel VLAN.

Ports vers les équipements internes (mode Access)

```
interface GigabitEthernet0/2
 description DMZ
 switchport mode access
 switchport access vlan 342
 no shutdown


interface GigabitEthernet0/3
 description Serv
 switchport mode access
 switchport access vlan 343


interface GigabitEthernet0/4
 description LAN
 switchport mode access
 switchport access vlan 344
```

Port vers le pare-feu Stormshield (mode Trunk)

Ce port transporte tous les VLANs vers le pare-feu.

```
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 342,343,344,302
 no shutdown
```

Vérification:

show vlan brief : liste des VLANs et des ports assignés.

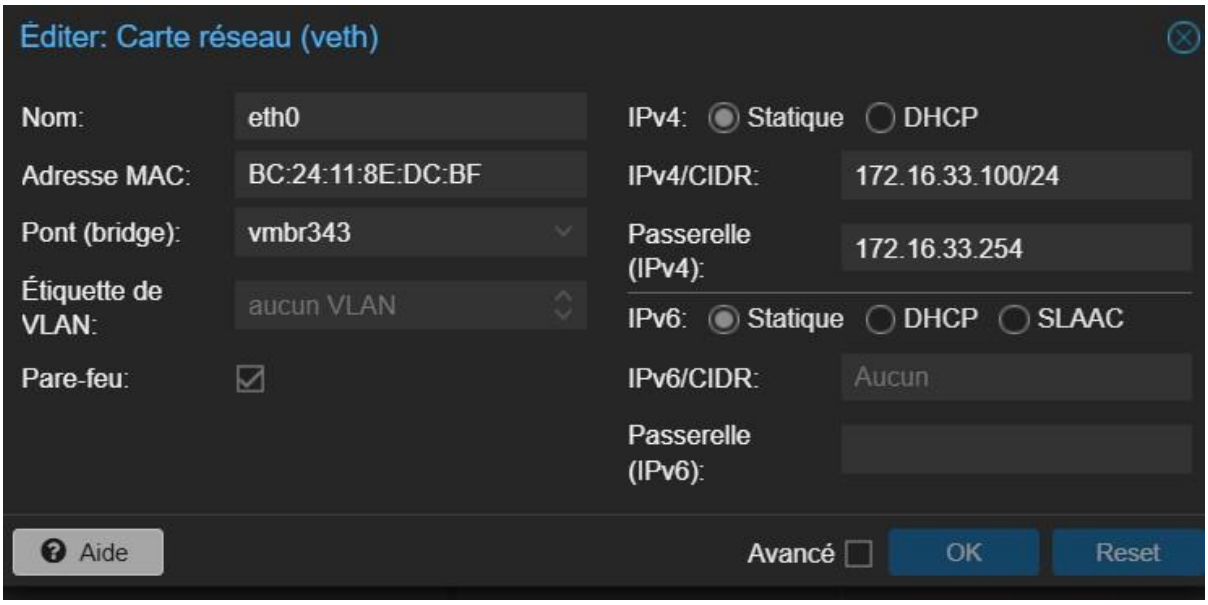
- show interfaces trunk : confirme que le port trunk transporte bien les VLANs 342, 343, 344, 302.

Retour :

Retour à la Documentation Technique

Configuration du service DHCP

Dans un premier temps on crée le conteneur LXC sur Proxmox: *(le bridge doit point vers notre vlan 343)*



Mettre à jour le système:

```
sudo apt update
sudo apt upgrade -y
```

Installer le serveur DHCP:

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

1- **Configurer le fichier dhcpd.conf**

* Éditer /etc/dhcp/dhcpd.conf :

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

```
# option definitions common to all supported networks...
option domain-name "marrakech.cub.fr";
option domain-name-servers 192.168.13.23;

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

2- **Place maintenant à la configuration de l'interface réseau:**

On édite le fichier suivant pour ajouter “INTERFACESv4=“eth0” ”
sudo nano /etc/default/isc-dhcp-server

```
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1"
INTERFACESv4="eth0"
INTERFACESv6=""
```

3- **Vérification de la configuration**

sudo dhcpd -t

Si tout est correct, aucun message d’erreur ne s’affiche.

4- **On Démarre et active le service**

sudo systemctl restart isc-dhcp-server
sudo systemctl enable isc-dhcp-server

5- **Vérification que le serveur fonctionne**

sudo systemctl status isc-dhcp-server

6- TEST avec un CLIENT

```
root@Client:~# 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: eth0@if3954: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:2e:97:a4 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.13.3/24 brd 192.168.13.255 scope global dynamic eth0
       valid_lft 467sec preferred_lft 467sec
    inet6 fe80::be24:11ff:fe2e:97a4/64 scope link
       valid_lft forever preferred_lft forever
```

On crée un conteneur client afin de vérifier le bon fonctionnement du DHCP. Comme le montre l’image, le DHCP attribue correctement une adresse IP au conteneur.

Configuration de l'Agent-Relais DHCP

L’agent relais DHCP intercepte les requêtes et réponses BOOTP/DHCP.

Requête client : il reçoit la requête sur le réseau local et la transfère aux serveurs DHCP configurés.

- **Réponse serveur :** il renvoie la réponse soit en **broadcast** sur le segment d’origine, soit en **unicast** directement au client, selon le type de message.

Installer le paquet dhcprelay :

apt-get install isc-dhcp-relay --fix-missing

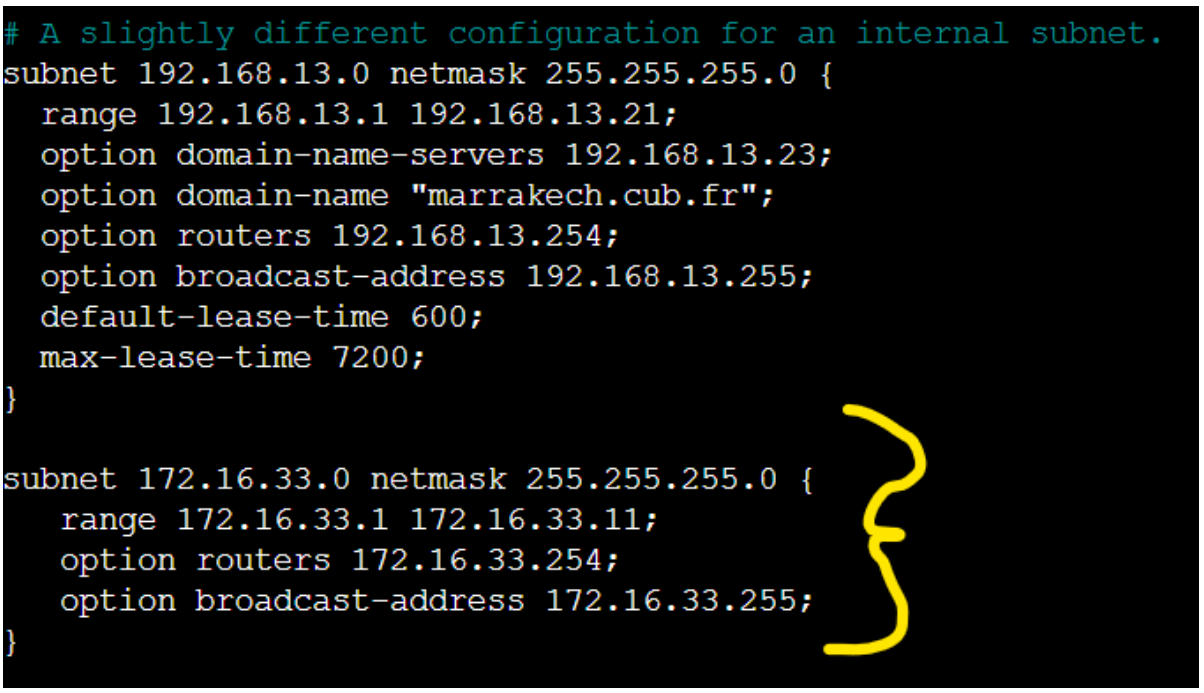
Ouvrir et ajouter l'adresse du serveur dans le fichier de configuration de l’agent relais DHCP dans /etc/default/isc-dhcp-relay.

```
  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="172.16.33.100"

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

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
```

Puis redémarrer le service agent relais DHCP sur le serveur relaisDHCP :

systemctl start isc-dhcp-relay

Puis définir un nouveau subnet dans le fichier dhcpd.conf du serveur DHCP, on rajoutant les lignes suivantes:



Et enfin redémarrer le service sur le serveur DHCP :

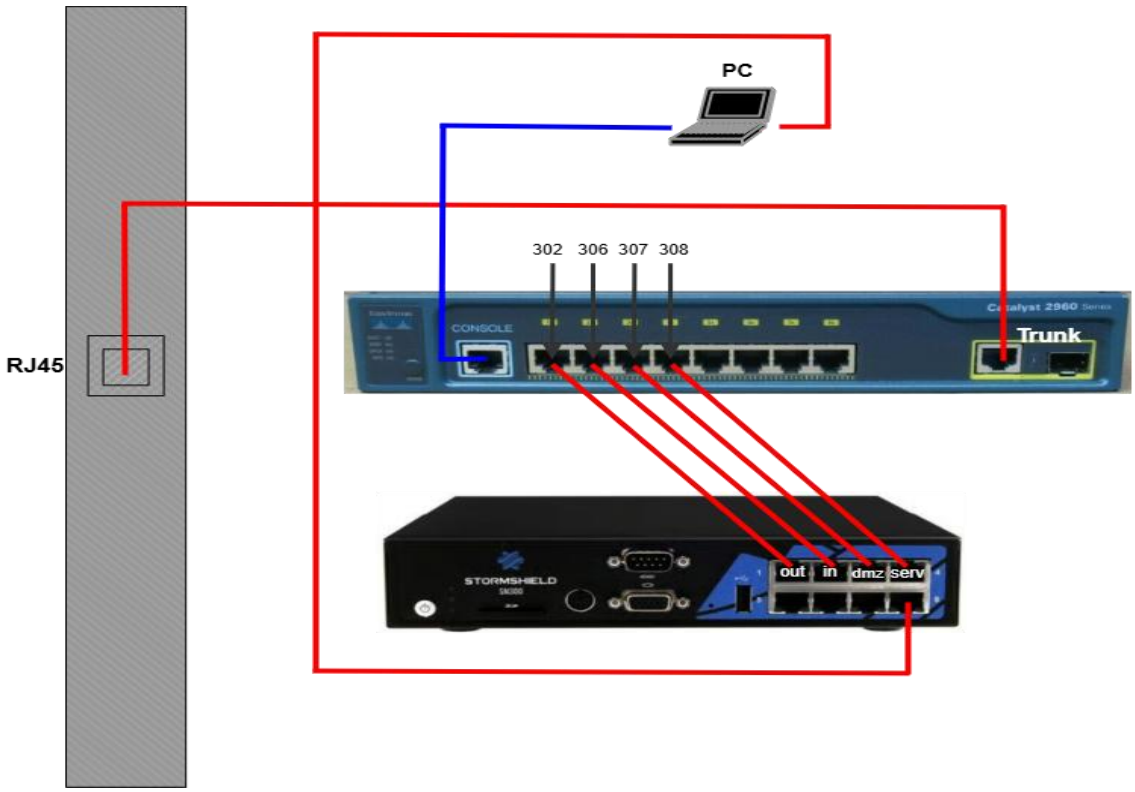
systemctl restart isc-dhcp-server

Retour :

Retour à la Documentation Technique

Configuration du pare-feu virtuel Stormshield

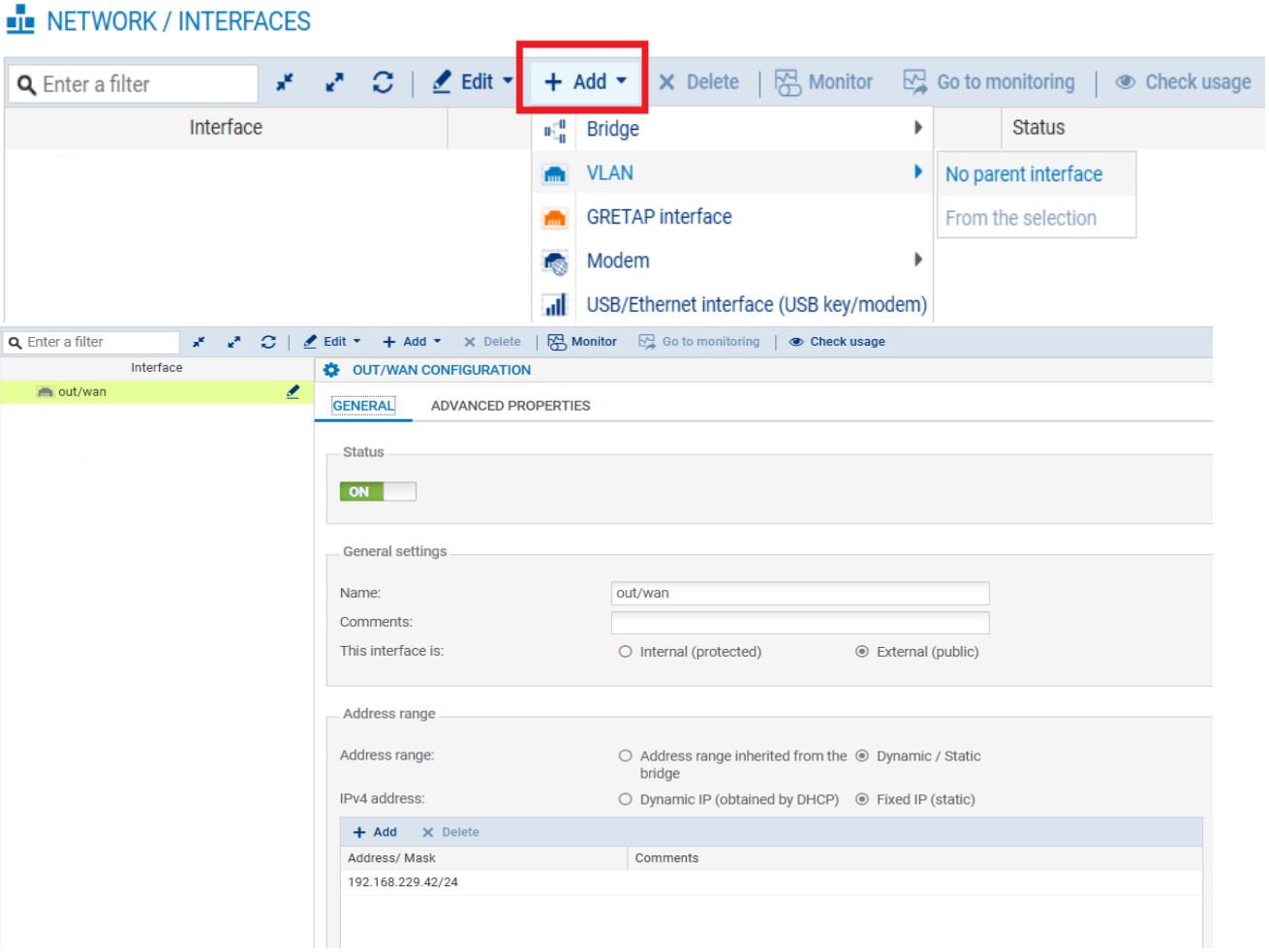
Schéma montage pare-feu Stormshield physique :



Adressage IP des serveurs du contexte de l'équipe :

Création/configuration des serveurs :

- Exemple, vlan out/wan :



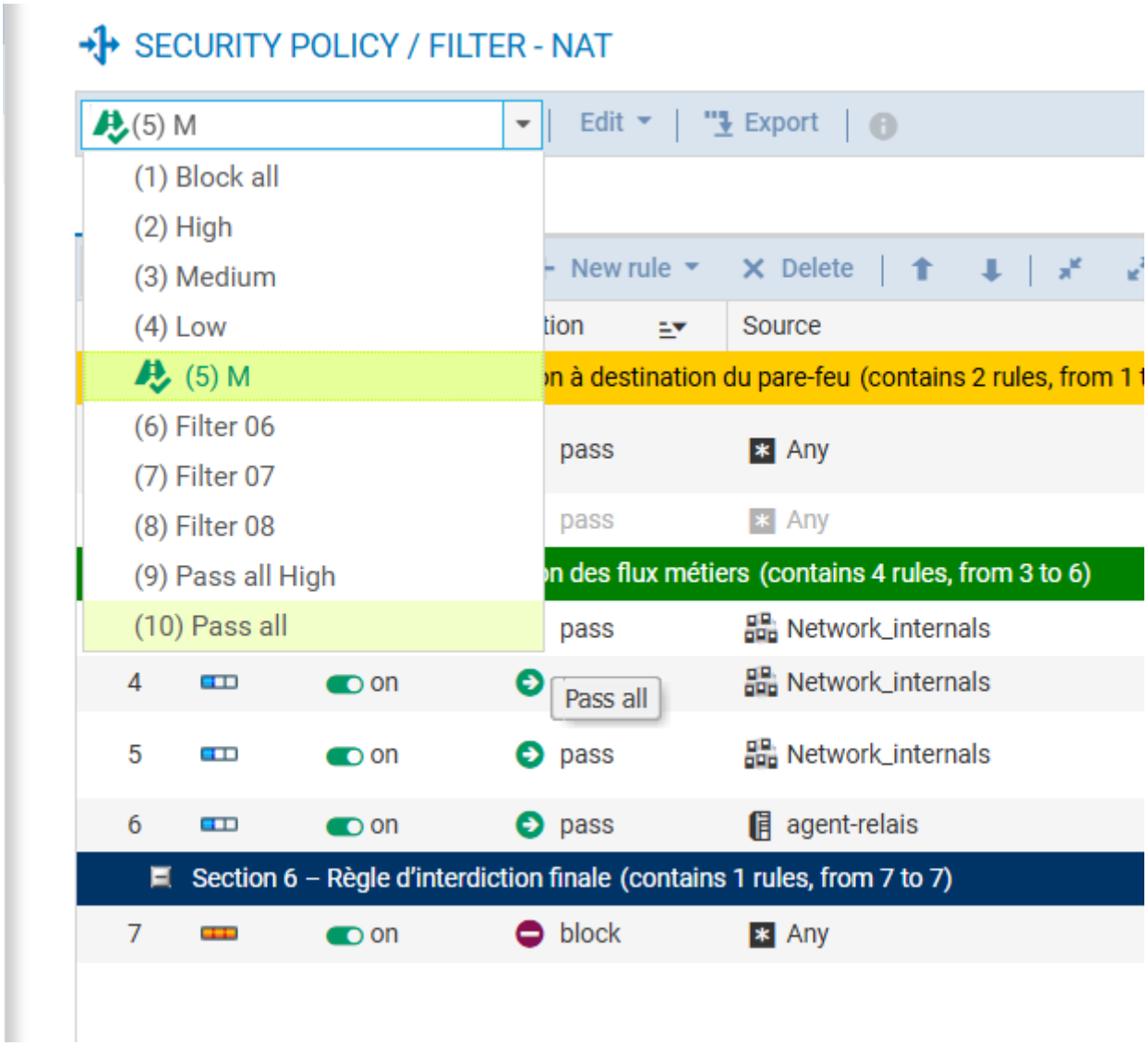
- **Résultat final :**

Interface	Port	Type	Status	IPv4 address
out/wan	1	Ethernet, 10 Gbit/s		192.168.229.42/24
in/lan	2	Ethernet, 10 Gbit/s		192.168.13.254/24
dmz1	3	Ethernet, 10 Gbit/s		172.16.13.254/24
server	4	Ethernet, 10 Gbit/s		172.16.33.254/24
admin	5	Ethernet, 10 Gbit/s		10.187.35.105/24 (DHCP)

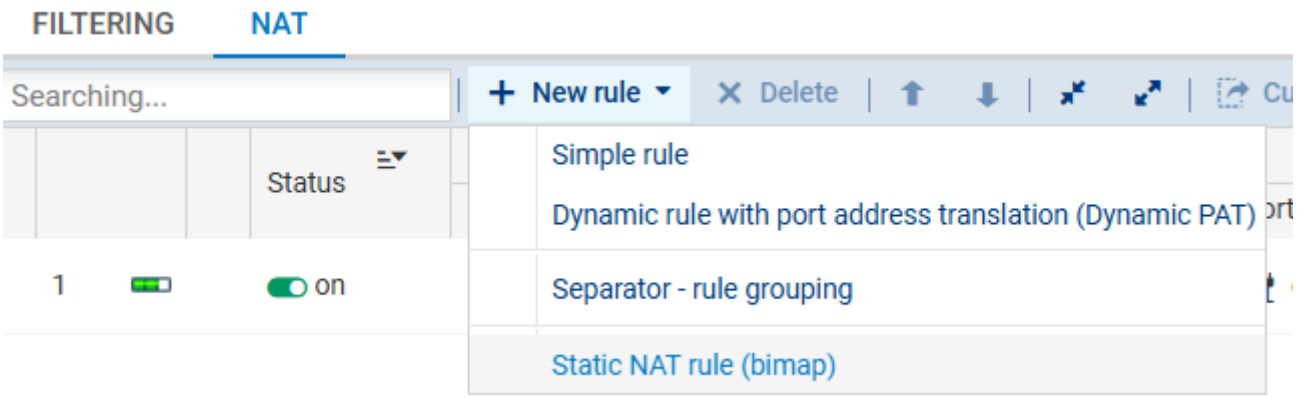
Configuration des règles du Pare feu Stormshield :

1) Traduction des adresses

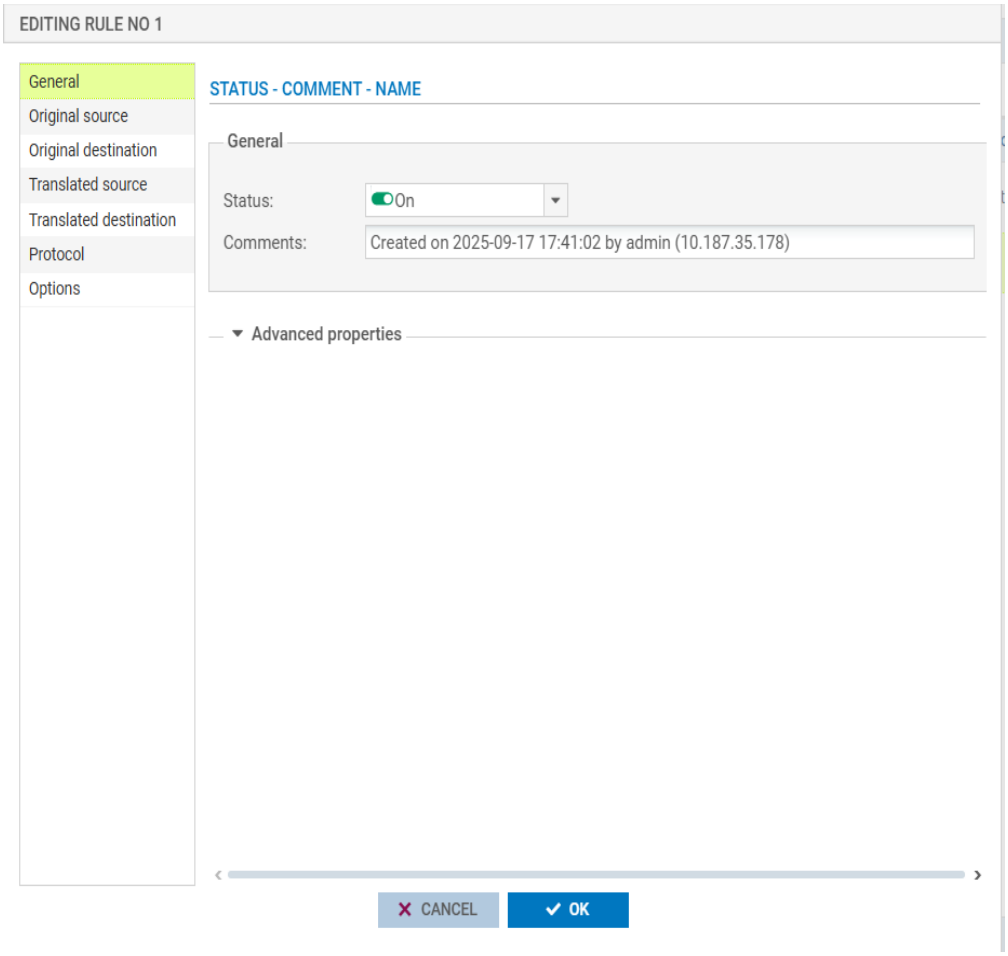
1. Dans l'onglet Routage il faut renseigner la passerelle :
   * Le pare-feu est configuré en mode « **pass all** » c'est-à-dire qu'il laisse passer tout le trafic :



1. Dans l'onglet **NAT** on ajoute une nouvelle règle :

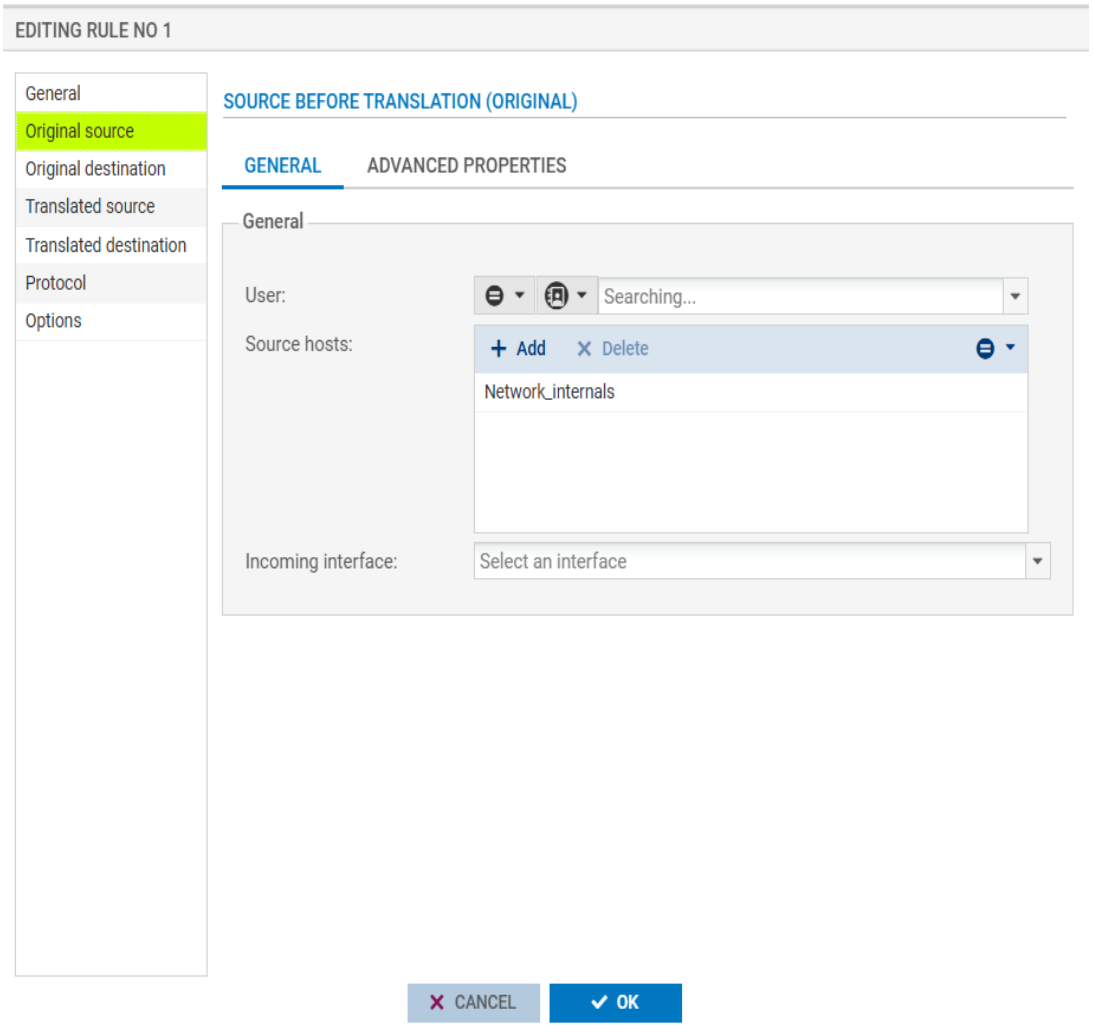


- 2.1 Pour modifier cette règle il suffit de **double-cliquer** sur un espace vide. On commence par activer la règle en la mettant sur **ON**. :

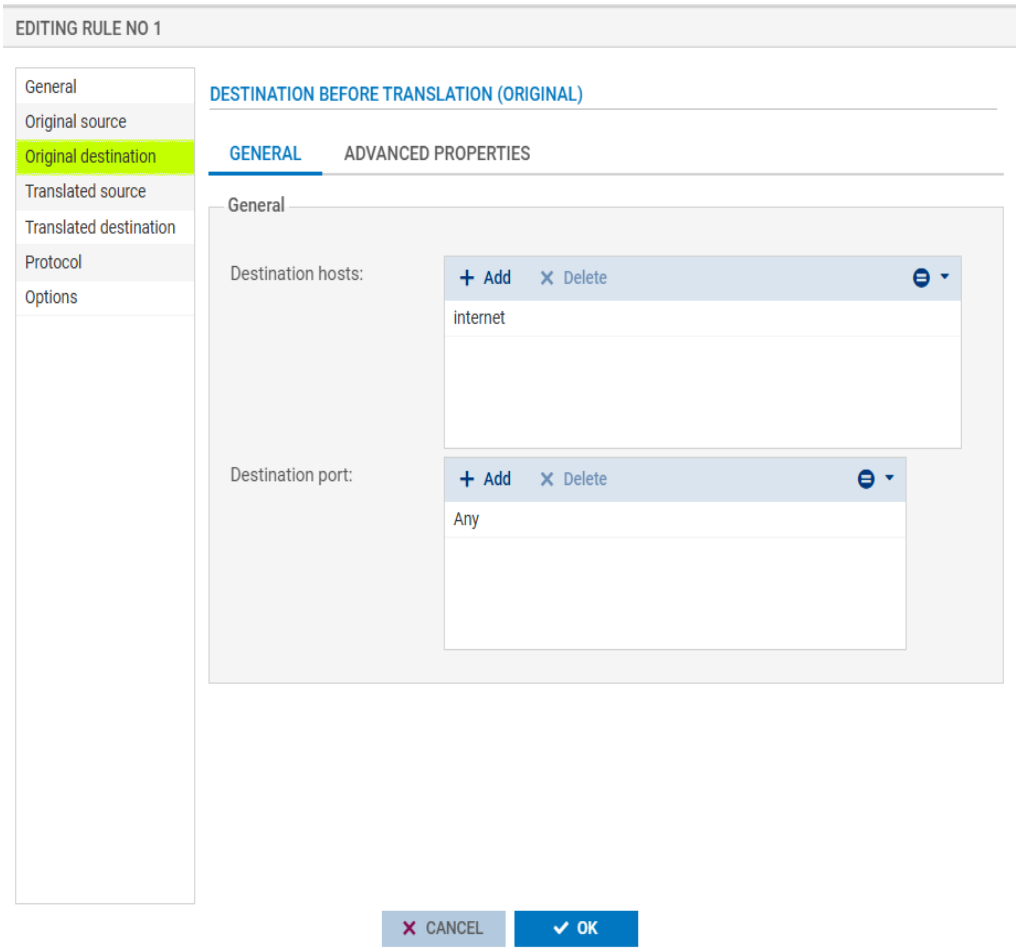


- 2.2 Dans le menu déroulant des hôtes source on choisit **Network_internals** :

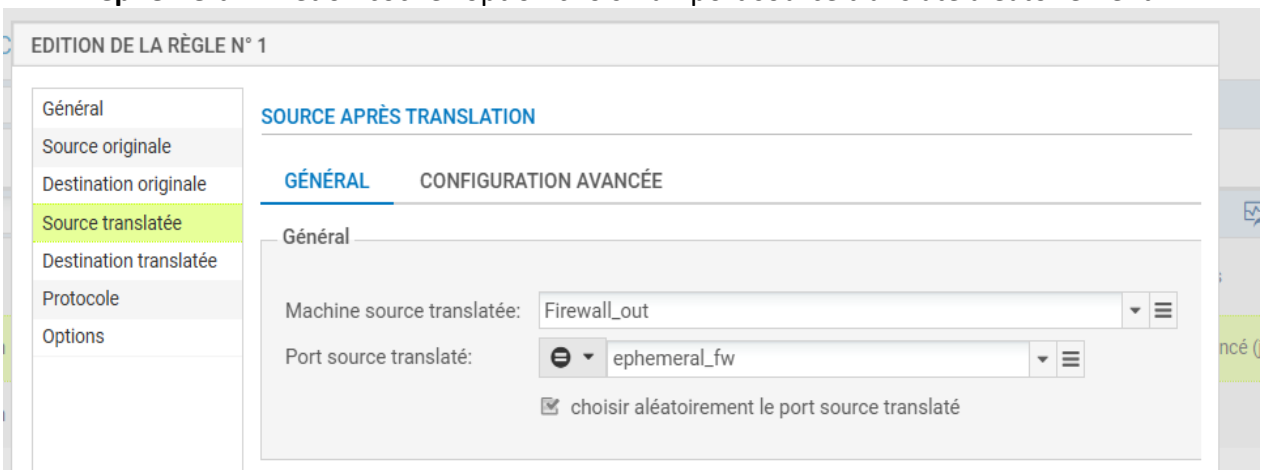
Cela fait en sorte que la règle s'applique uniquement au trafic provenant du réseau interne.



- 2.3 On remplace any par **Internet** sur le **port destination hôtes** :

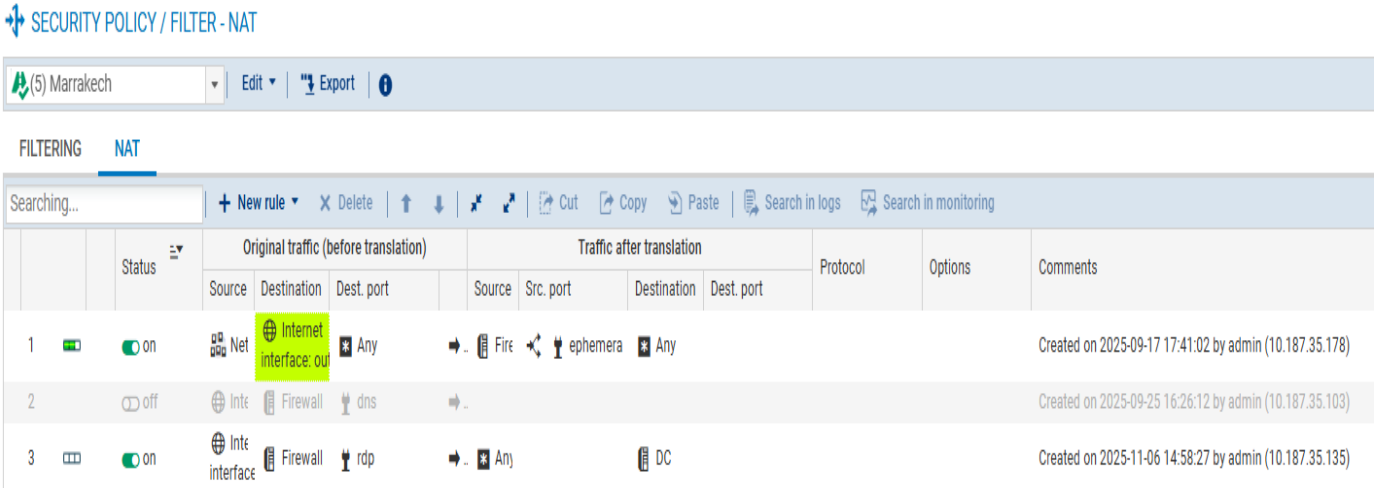


- 2.4 Dans source translaté, on choisit **Firewall_out**. Pour le champ port source translaté on sélectionne **ephemeral-fw** et on coche l'option choisir un port source translaté aléatoirement :



Enfin - Cliquer sur OK pour enregistrer la règle, dans État passer à On et activez la politique !

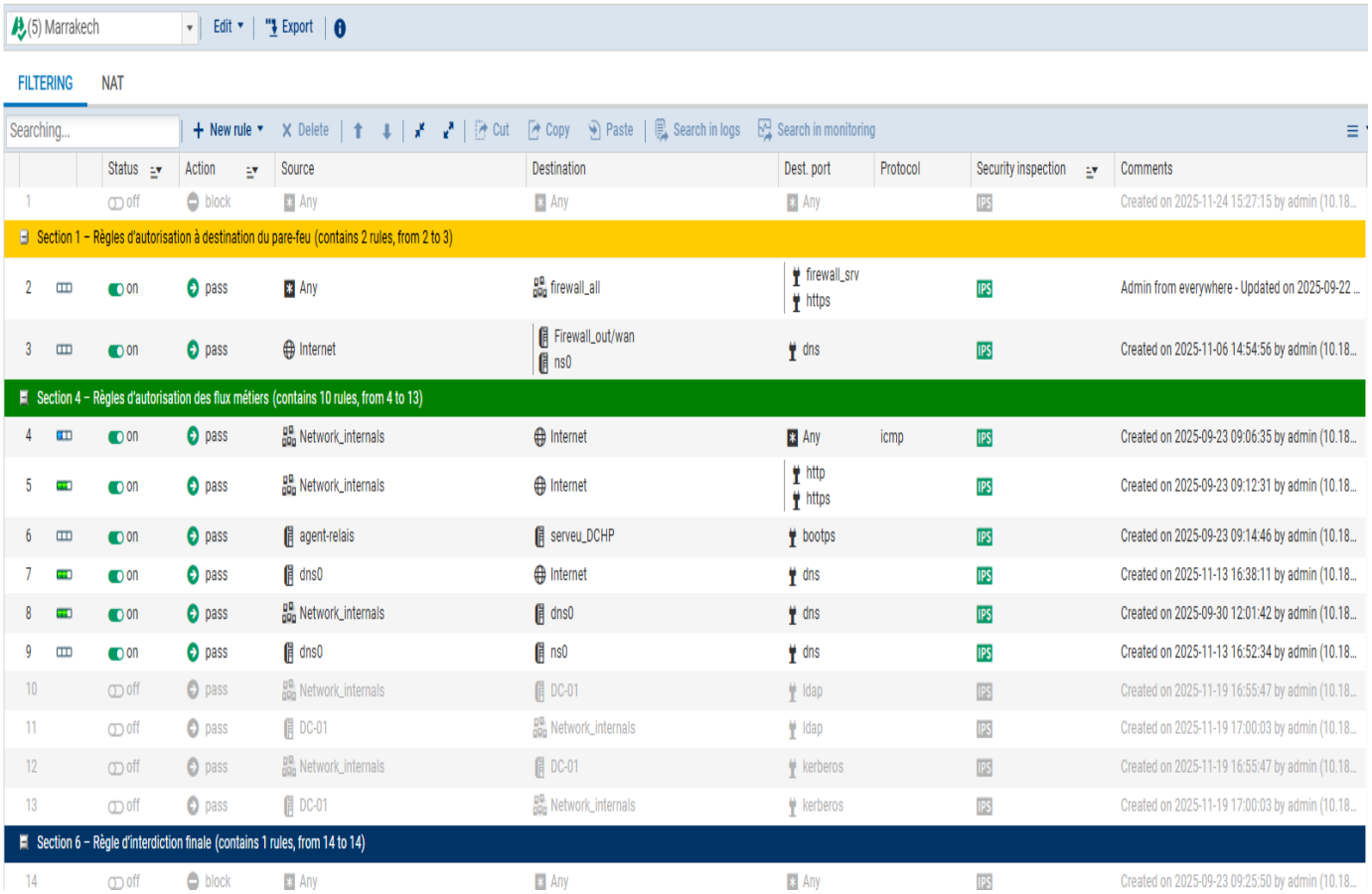
- **Règles NAT actuels :**



Règles de filtrage et NAT

Présentation

contexte des règles de filtrage :



Règles de filtrage

Présentation

Les règles de filtrage du pare-feu sont organisées en différentes sections :

Section 1 : Règles d'autorisation à destination du pare-feu

- Section 4 : Règles d'autorisation des flux métiers

- Section 6 : Règle d’interdiction finale

Chaque règle est décrite uniquement par son objectif fonctionnel dans le réseau.

Section 1 – Règles d’autorisation à destination du pare-feu

Règle 2 – Objectif :
Permettre l’accès d’administration au pare-feu depuis n’importe quelle source afin d’assurer la gestion à distance (accès HTTPS d’administration).

Règle 3 – Objectif :
Autoriser les requêtes DNS provenant d’Internet vers le pare-feu lorsqu’il assure un rôle de serveur DNS public.

Règle 4 – Objectif :
Permettre l’accès d’administration interne au pare-feu depuis le réseau d’administration pour la maintenance technique.

Section 4 – Règles d’autorisation des flux métiers

Règle 5 – Objectif :
Permettre les tests de connectivité (ICMP/ping) du réseau interne vers Internet pour vérifier l’état du réseau.

Règle 6 – Objectif :
Autoriser la navigation web (HTTP/HTTPS) des utilisateurs internes vers Internet.

Règle 7 – Objectif :
Permettre au relais DHCP interne de dialoguer avec le serveur DHCP pour l’attribution des adresses IP.

Règle 8 – Objectif :
Autoriser le serveur DNS interne à résoudre des noms de domaine externes via Internet.

Règle 9 – Objectif :
Permettre aux postes internes d’interroger le serveur DNS interne pour leurs résolutions de noms.

Règle 10 – Objectif :
Assurer les échanges DNS internes entre les serveurs d’infrastructure (synchronisation, redondance).

Règle 11 – Objectif :
Autoriser les échanges LDAP entre le contrôleur de domaine et le réseau interne pour les fonctions d’annuaire.

Règle 12 – Objectif :
Permettre les communications LDAP nécessaires à l’authentification Active Directory.

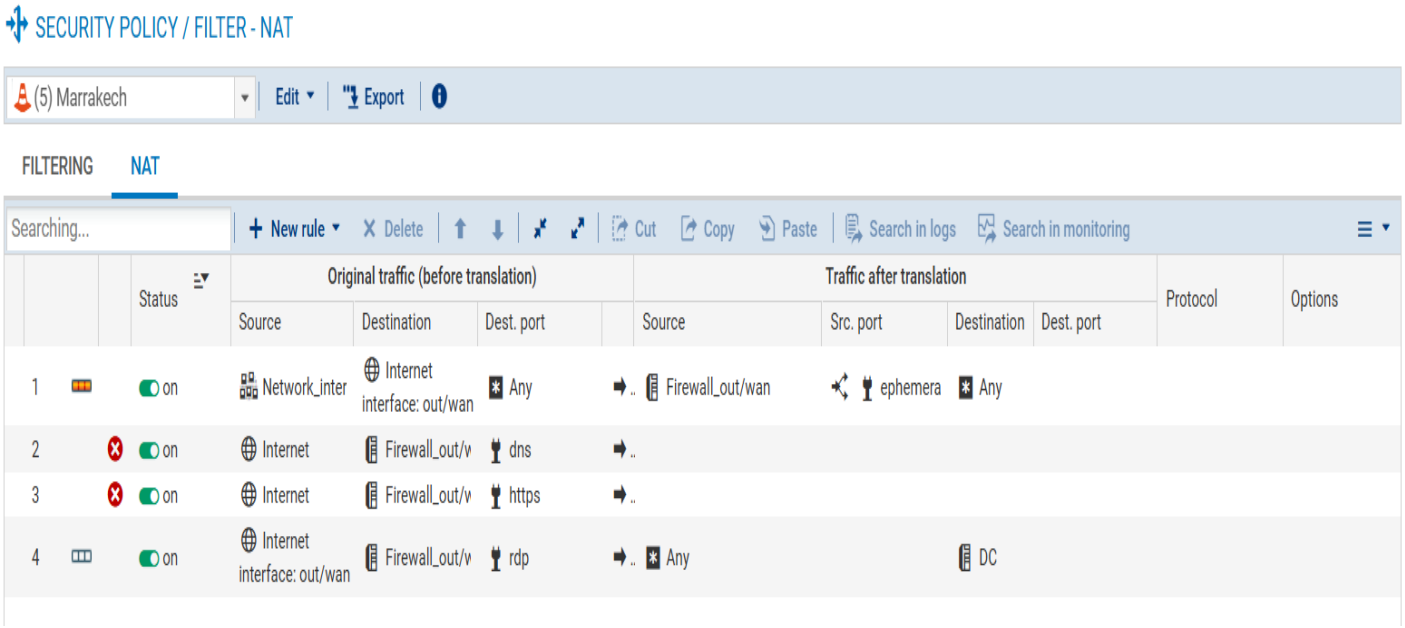
Règle 13 – Objectif :
Autoriser les échanges Kerberos pour l’authentification AD.

Règle 14 – Objectif :
Permettre au contrôleur de domaine de recevoir les flux Kerberos provenant du réseau interne.

Section 6 – Règle d’interdiction finale

Règle 15 – Objectif :
Bloquer tout trafic non autorisé par les règles précédentes afin d’appliquer une politique restrictive (tout ce qui n’est pas explicitement autorisé est interdit).

Règles de NAT



Règle 1 – Objectif :
Assurer la sortie Internet du réseau interne via l'interface WAN du pare-feu (NAT source / masquerading).

Règle 2 – Objectif :
Permettre aux clients Internet d'interroger le service DNS exposé par le pare-feu (redirection du port DNS vers le pare-feu).

Règle 3 – Objectif :
Permettre l'accès externe au portail d'administration du pare-feu via HTTPS depuis Internet (redirection HTTPS vers le pare-feu).

Règle 4 – Objectif :
Rediriger les connexions RDP provenant d'Internet vers le serveur interne (DC), afin de permettre une prise en main distante contrôlée.

Gestion des certificats sur pare-feu Stormshield (PKI)

Présentation

Le pare-feu Stormshield SNS intègre une infrastructure à clés publiques (PKI) permettant la gestion des certificats numériques.
Cette PKI assure l'authentification sécurisée des utilisateurs, serveurs et équipements via des certificats X.509.

Elle permet notamment :

la création d'autorités de certification (CA),
- la génération d'identités utilisateur et serveur,
- la gestion des révocations,
- la sécurisation des accès (VPN, interface d'administration, services TLS).

Accès au module PKI :

CONFIGURATION > OBJETS > Certificats et PKI

Types d'autorités de certification

CA interne

Le pare-feu agit comme autorité de certification locale. Il peut :

créer et signer des certificats,
- gérer les listes de révocation (CRL),
- jouer le rôle de CA racine ou de sous-autorité,
- servir de base de confiance pour VPN SSL/IPSec et authentification.

Le certificat de la CA est auto-signé et contrôle toute la chaîne de confiance interne.

CA externe

Le pare-feu peut importer :

des certificats signés par une autorité tierce,
- des fichiers PKCS#12 (.p12),
- des certificats d'équipements ou serveurs.

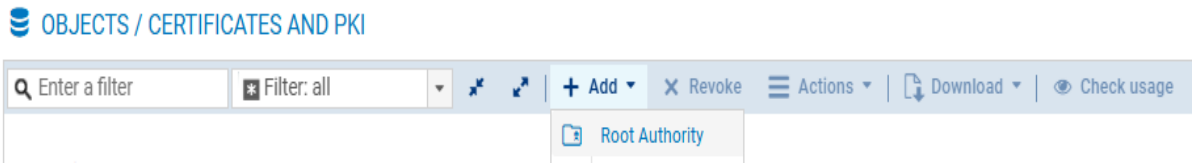
Ces certificats sont utilisés pour :

VPN IPSec / SSL
- HTTPS sécurisé
- authentification des équipements

Création d'une autorité de certification

Procédure :

Menu : CONFIGURATION > OBJETS > Certificats et PKI
2. Cliquer sur **Ajouter > Autorité racine**



Informations à renseigner :

CN : nom de l'autorité (ex : CA_Stormshield)
- Organisation (O)
- Unité d'organisation (OU)
- Ville / Pays

Paramètres :

Mot de passe de protection
- Durée de validité conseillée : 365 jours
- Taille de clé : 2048 bits recommandée

L'autorité devient alors la racine de confiance pour la génération des certificats.

Conclusion

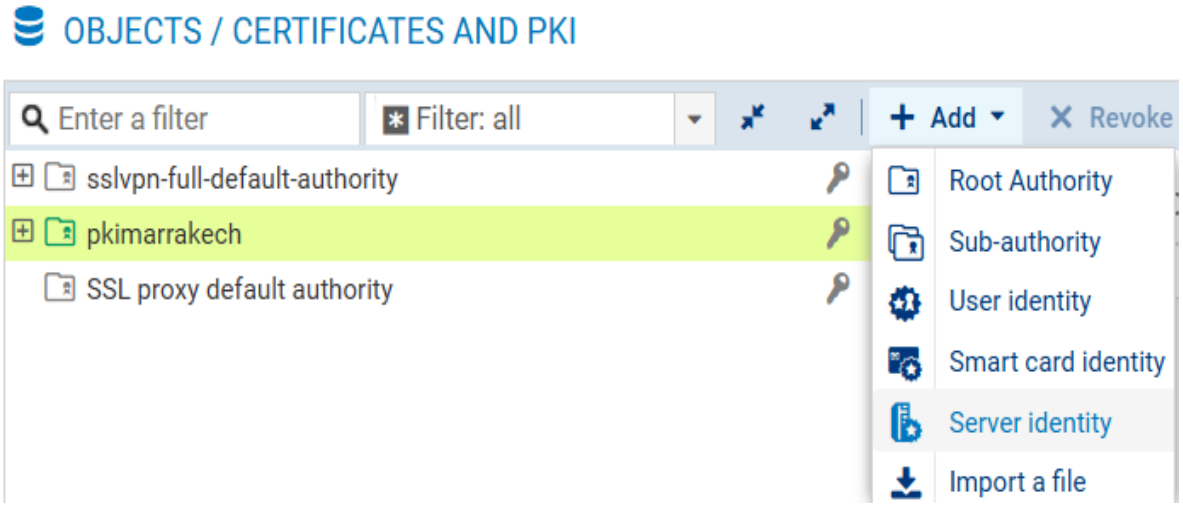
La mise en place d'une PKI sur le pare-feu Stormshield permet de renforcer la sécurité du réseau en garantissant :

l'identité des utilisateurs et équipements,
- l'intégrité des communications,
- une authentification fiable et centralisée.

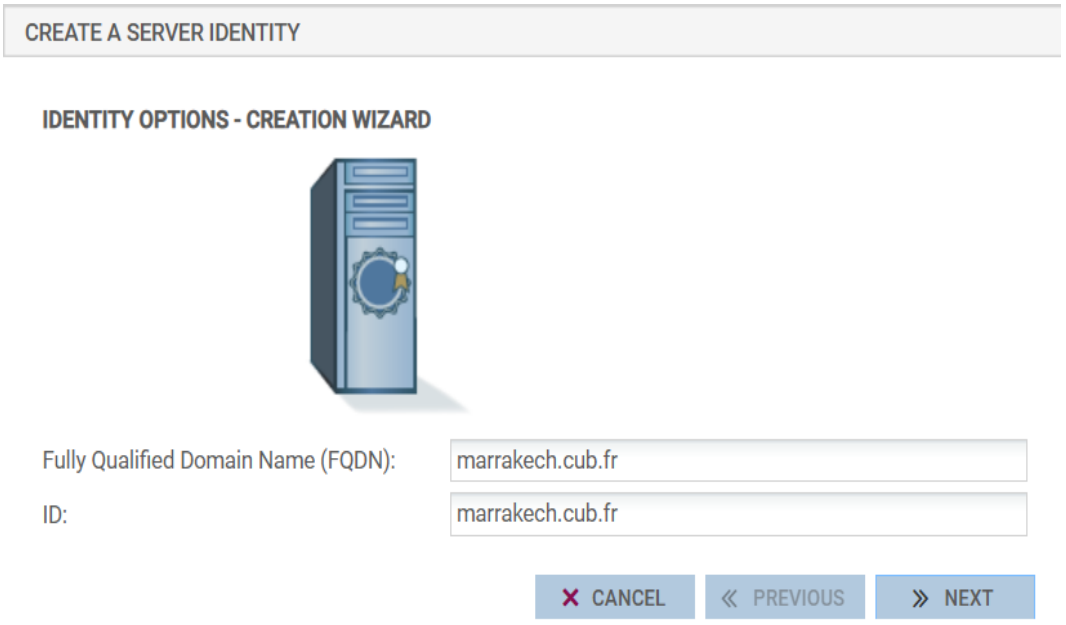
Création d'une identité serveur puis utilisateur

Identité serveur :

Dans **Objects > Certificates and PKI**, on clique **Add → Server identity** :

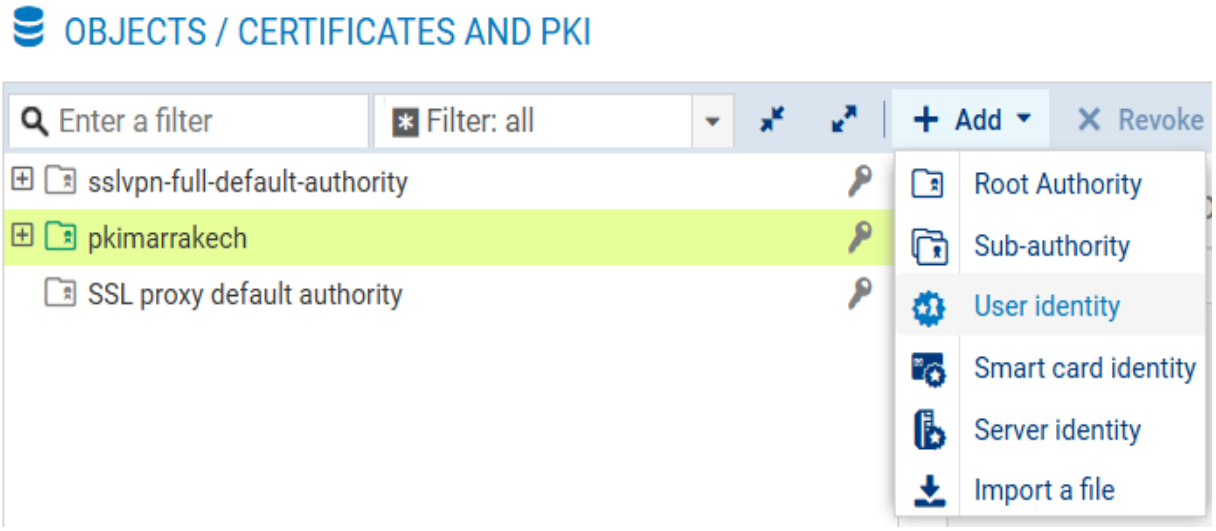


.

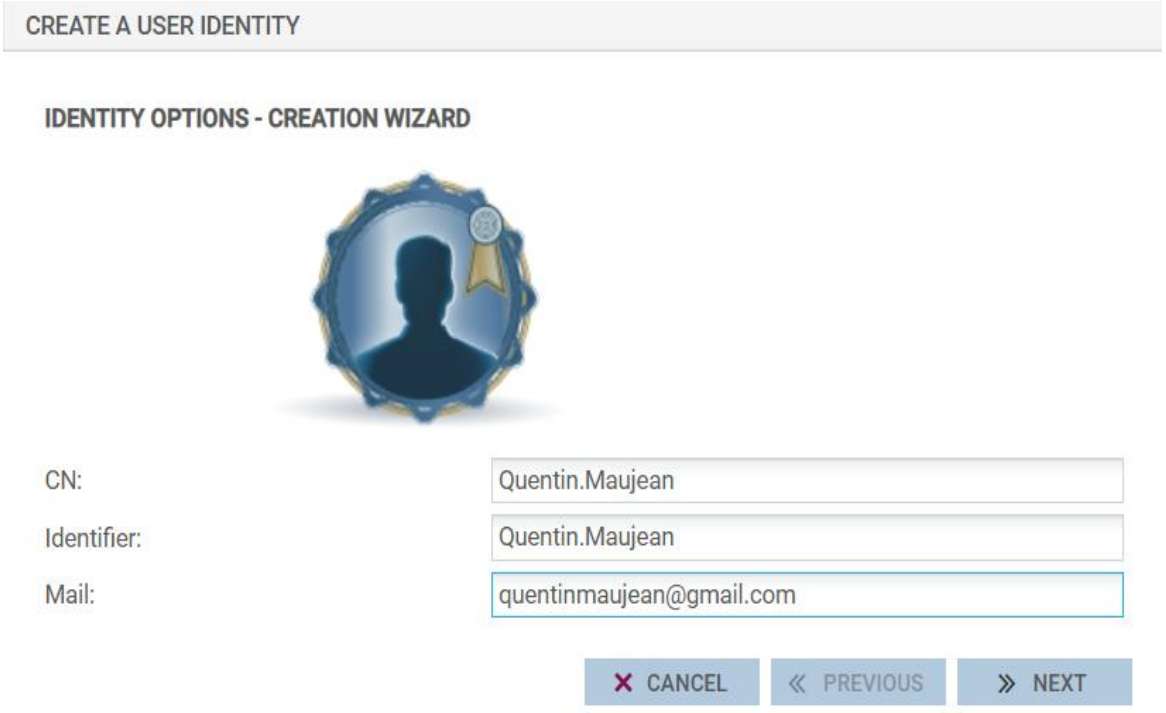


Identité utilisateur :

Dans **Objects > Certificates and PKI**, on clique **Add → User identity** :



On renseigne les informations :



Choix de l'autorité de certification (CA) :

CREATE A USER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD

Select the parent Autority

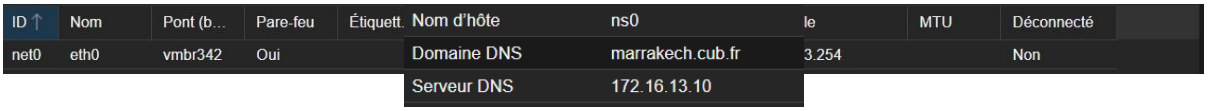
Parent CA:	pkimarrakech
CA passphrase:	••••••••••••••••••••

Autority attributes

Organization:	CUB
Organizational unit:	BTS SIO
City (L):	Limoges
State (ST):	Haute-vienne
Country:	France

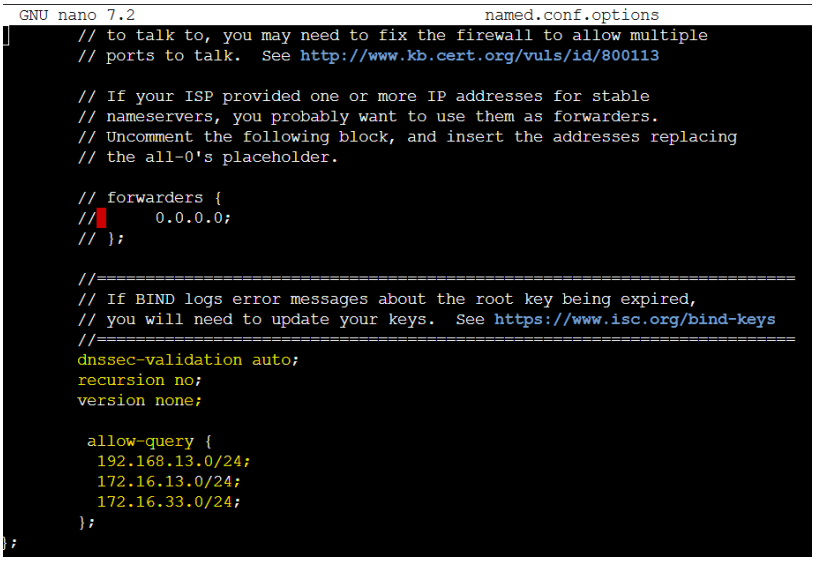
CANCEL PREVIOUS NEXT

Mettre en place le service DNS pour les postes du réseau des utilisateurs.



On désactive la récursivité et on indique l'interface d'écoute du serveur

- Sécuriser le serveur DNS : Par défaut, il n'accepte que les requêtes provenant du sous-réseau local (192.168.x.0/24) afin de réduire les risques d'attaque. Pour autoriser d'autres réseaux, ajoutez leurs adresses dans l'option allow-query du fichier /etc/bind/named.conf.options.



Dans la console , exécutez les commandes suivantes pour installer Bind9 et ses utilitaires :

```
# apt update
# apt install bind9 bind9utils
```

On crée ensuite une zone dns sous named.conf.local :

```
# nano /etc/bind/named.conf.local
```

On ajoute la configuration ci dessous dans la zone exemple :

```
 GNU nano 7.2                        /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "marrakech.cub.fr" {
    type master;
    file "/etc/bind/db.marrakech.cub.fr";
};
```

Ensuite il faut créer le fichier de zone qui contiendra les fichiers du DNS:

cp /etc/bind/db.local /etc/bind/db.marrakech.cub.fr

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

Et on remplace le contenu de tel sorte :

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

marrakech.cub.fr. IN      NS      ns0.marrakech.cub.fr.
@               IN      A       192.168.13.23
ns0             IN      A       172.16.13.10
dhcp            IN      A       172.16.33.100
```

@ correspond à l'adresse du DNS récursif.

- nso pour le DNS autoritaire.
- et enfin l'adresse du DHCP

On redémarre le service pour qu'il face effet :

systemctl restart bind9

systemctl enable bind9

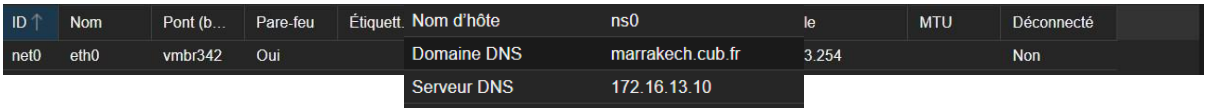
TEST :

```
root@ns0:/etc/bind# hostname
ns0
root@ns0:/etc/bind# host ns0
ns0.marrakech.cub.fr has address 172.16.13.10
```

Retour :

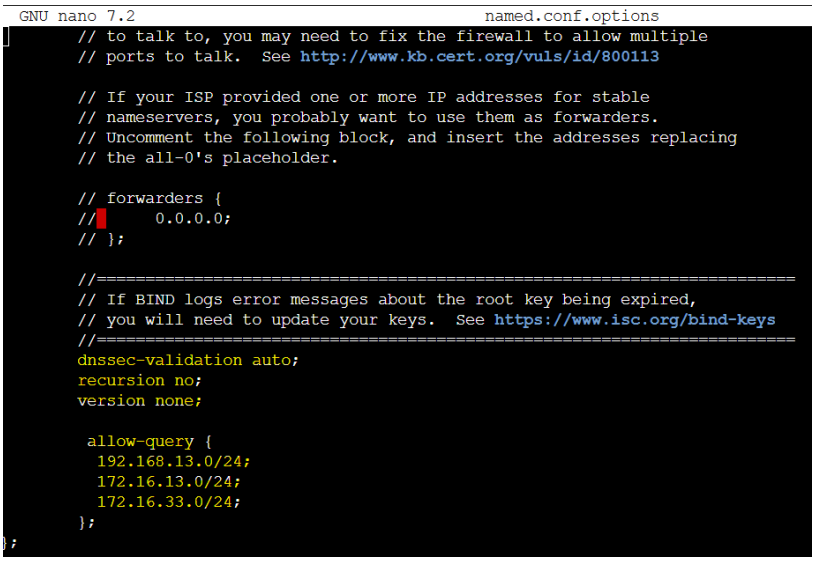
Retour à la Documentation Technique

Mettre en place le service DNS pour les postes du réseau des utilisateurs.



On désactive la récursivité et on indique l'interface d'écoute du serveur

- Sécuriser le serveur DNS : Par défaut, il n'accepte que les requêtes provenant du sous-réseau local (192.168.x.0/24) afin de réduire les risques d'attaque. Pour autoriser d'autres réseaux, ajoutez leurs adresses dans l'option allow-query du fichier /etc/bind/named.conf.options.



Dans la console , exécutez les commandes suivantes pour installer Bind9 et ses utilitaires :

```
# apt update
# apt install bind9 bind9utils
```

On crée ensuite une zone dns sous named.conf.local :

nano /etc/bind/named.conf.local

On ajoute la configuration ci dessous dans la zone exemple :

```
  GNU nano 7.2                        /etc/bind/named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "marrakech.cub.fr" {
    type master;
    file "/etc/bind/db.marrakech.cub.fr";
};
```

Ensuite il faut créer le fichier de zone qui contiendra les fichiers du DNS:

cp /etc/bind/db.local /etc/bind/db.marrakech.cub.fr

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

Et on remplace le contenu de tel sorte :

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

marrakech.cub.fr. IN      NS      ns0.marrakech.cub.fr.
@               IN      A       192.168.13.23
ns0             IN      A       172.16.13.10
dhcp            IN      A       172.16.33.100
```

@ correspond à l'adresse du DNS récursif.

- nso pour le DNS autoritaire.
- et enfin l'adresse du DHCP

On redémarre le service pour qu'il face effet :

systemctl restart bind9
systemctl enable bind9

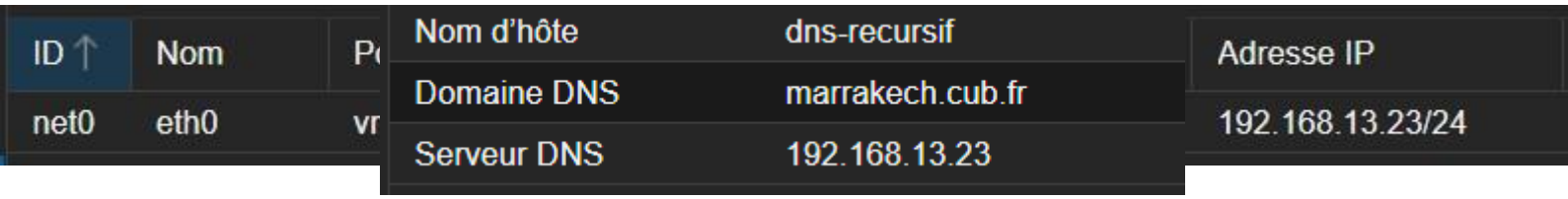
TEST :

```
root@ns0:/etc/bind# hostname
ns0
root@ns0:/etc/bind# host ns0
ns0.marrakech.cub.fr has address 172.16.13.10
```

Retour :

Retour à la Documentation Technique

Configuration le service DNS récursif les ordinateurs du réseau utilisateurs:



Le paquet logiciel Unbound permet de configurer un serveur récursif avec Debian. Ce logiciel ne fera que des requêtes DNS de type récursif sans héberger de zone DNS.

Mettre à jour la VM:
apt update && sudo apt upgrade

Installation du paquet logiciel Unbound:
apt install unbound dnsutils

Configuration du fichier de conf etc/unbound/unbound.conf:
On a créer 2 zones stub pointant vers leurs serveurs DNS internes (pour cub.fr et marrakech.cub.fr), On a aussi une zone foward par défaut vers les DNS publics de Google permet la résolution des domaines Internet.

```
GNU nano                                                    nbound.conf
# /etc/unbo
include-top

server:
interface:
interface:

access-cont
access-cont
access-cont
access-cont
access-cont

hide-versio
hide-identi

do-ip4: yes

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

private-domain: cub.fr
# La ligne suivante    ajouter car le domaine est local et il ne passe p
domain-insecure: cub.fr
```

```
# interroger le serveur DNS de CUB
stub-zone:
name: "cub.fr."
stub-addr: 192.168.229.1

# interroger le serveur DNS du siege
stub-zone:
name: "marrakech.cub.fr."
stub-addr: 172.16.13.10

# r  cursivite pour les domaines sur Internet
forward-zone:
name: "."
forward-addr: 8.8.8.8
forward-addr: 8.8.4.4
```

Lancement du service

1) On crée un répertoire dédié aux logs d'Unbound.

mkdir /var/log/unbound

2) On crée le fichier vide qui recevra les logs.

touch /var/log/unbound/unbound.log

3) On change le propriétaire du dossier et du fichier pour l'utilisateur unbound

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

4) On redémarre le service pour qu'il prenne en compte la configuration de logging

systemctl restart unbound

TEST de la résolution de nom fonctionne.

Premièrement, On vide le cache DNS à l'aide de la commande suivante:

unbound-control flush_zone .

et enfin on test avec un dig le nom de domaine cub.fr

dig www.cub.fr

```
root@dns0:/root# dig www.cub.fr

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> www.cub.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20141
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.cub.fr.             40916   IN      A       192.168.229.1

;; Query time: 0 msec
;; SERVER: 192.168.13.10#53(192.168.13.10) (UDP)
;; WHEN: Tue Sep 30 06:58:17 UTC 2025
;; MSG SIZE  rcvd: 55
```

Retour :

Retour à la Documentation Technique

Création d'une VM Windows avec Proxmox

Premièrement on crée la VM Windows server 2025 sur Proxmox.

1. Configuration du disque et de la mémoire

Type de disque virtuel : privilégier RAW ou QCOW2.

- **Cache du disque virtuel :** utiliser le cache VirtIO.
- **Pilote de la carte réseau :** utiliser VirtIO.
- **Gestion de la mémoire :** activer le ballooning pour adapter dynamiquement la RAM

2. QEMU Guest Agent

Lors de la création de la VM, cocher **QEMU Agent** et l'option Advanced.

3. Pilotes VirtIO

Pilote réseau : VirtIO.

- **Cache du disque :** Write back.
- **Format du disque :** QCOW2

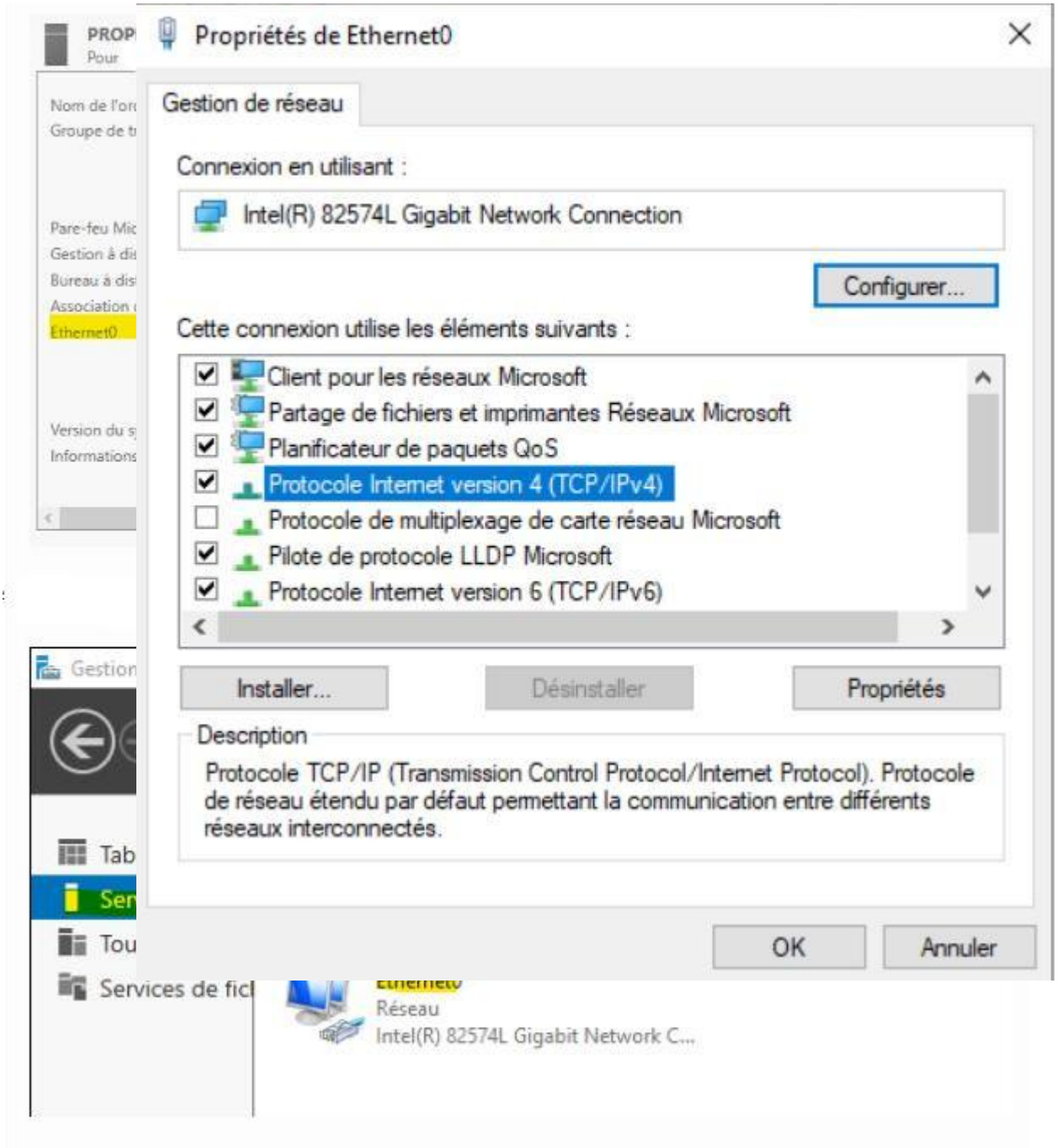
Et enfin le Bridge doit pointer vers notre VLAN serveur (vlan 343), Model = Virtl0 (paravirtulized)

Configurer un domaine Microsoft Active Directory

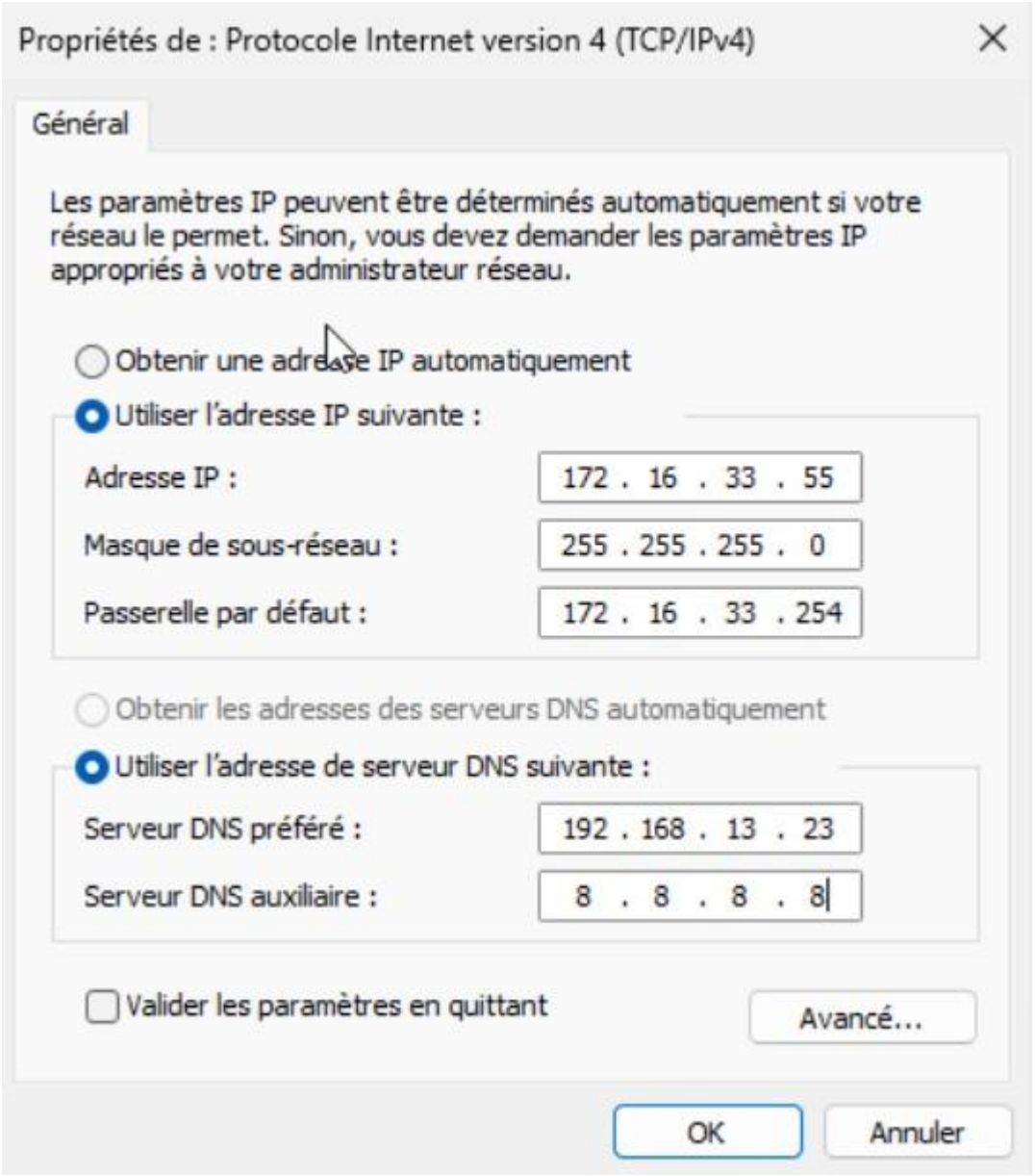
Après l'installation du système d'exploitation Windows Server 2025 avec une interface graphique.

CONFIGURERATION D'UNE INTERFACE RESEAU !!!

Dans l'onglet **« Serveur local »** puis vers la section **« Ethernet0 »** ouvrir les propriétés du Protocole internet



On saisit les informations suivantes : l'adresse IP 172.16.33.50, qui doit être située en dehors du subnet du VLAN serveur, le masque de sous-réseau 255.255.255.0, la passerelle par défaut 172.16.33.254, le serveur DNS préféré 192.168.13.23 (notre DNS récursif) et le serveur DNS auxiliaire 8.8.8.8.



TEST: Vérification de la connectivité de notre machine en faisant un test de « ping » dans une invite de commande.

Mettre à jour le système!!

Installation du rôle AD DS sur Windows Serveur 2022

Dans l'onglet « Ajouter des rôles et des fonctionnalités », on choisit une **installation basée sur un rôle ou une fonctionnalité**.

- Après avoir sélectionné le serveur cible, on coche le rôle « Services de domaine Active directory » et on confirme l'ajout des fonctionnalités nécessaires.

Assistant Ajout de rôles et de fonctionnalités

Sélectionner des rôles de serveurs

Le serveur de destination fait état d'un redémarrage en attente. Il est recommandé de le redémarrer a

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

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- [ ] Serveur de télécopie
- [ ] Serveur DHCP
- [x] Serveur DNS (Installé)
- [ ] Serveur Web (IIS)
- [ ] Service Guardian hôte
- [ ] Services AD LDS (Active Directory Lightweight Dire
- [ ] Services AD RMS (Active Directory Rights Manage
- [ ] Services Bureau à distance
- [ ] Services d'activation en volume
- [ ] Services d'impression et de numérisation de docu
- [ ] Services de certificats Active Directory
- [ ] Services de déploiement Windows
- [x] Services de domaine Active Directory (Installé)
- [ ] Services de fédération Active Directory (AD FS)
- [■] Services de fichiers et de stockage (2 sur 12 install
- [ ] Services de stratégie et d'accès réseau
- [ ] Services WSUS (Windows Server Update Services)

Desc

L'acc
conn
Direc
le pr
Direc
expé
perm
Le se
(RAS)
classi
conn
ou n
Web
certa
HTTP
résea
d'app
résea
fourn

< Précédent | Suivant >

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

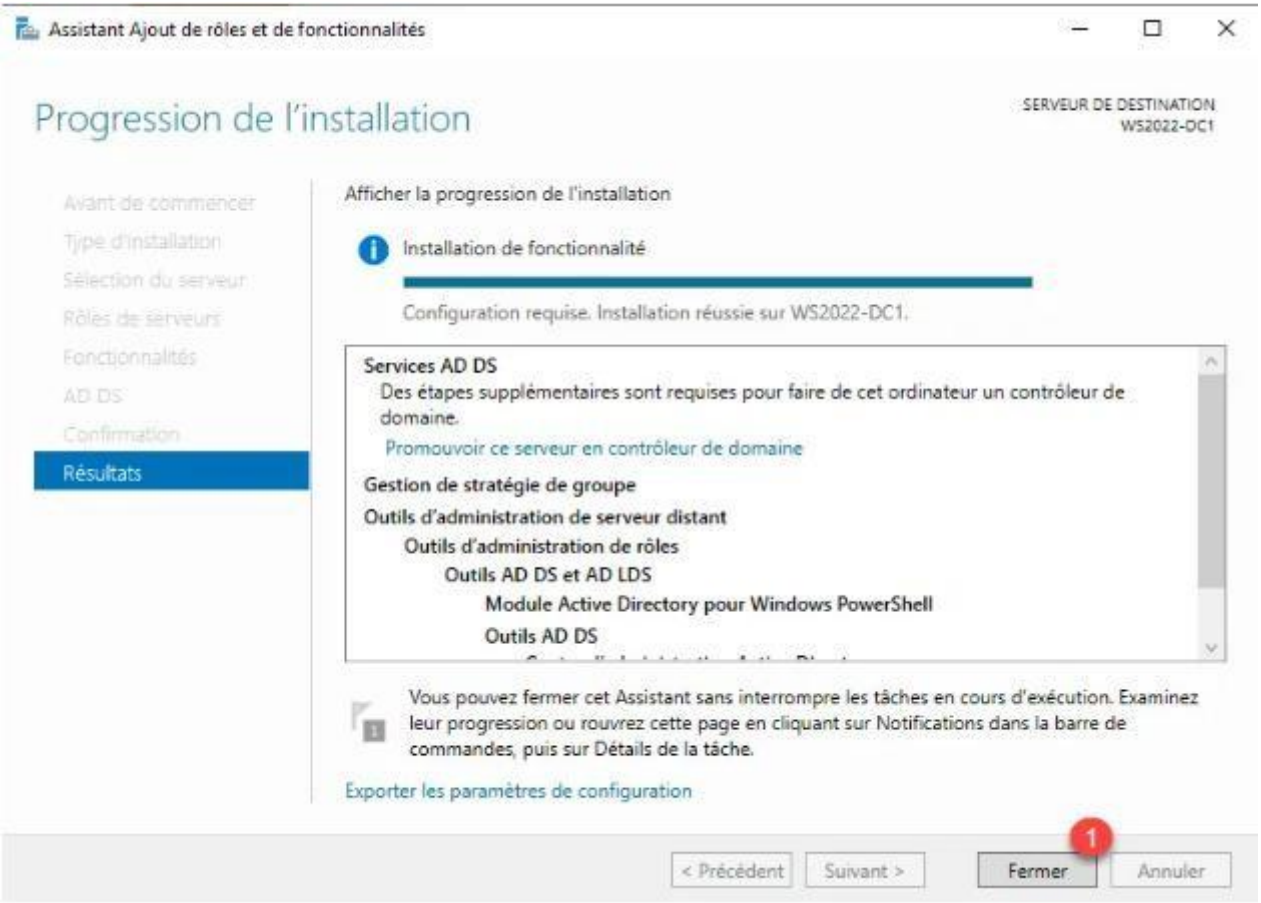
- Avant de commencer
- Type d'installation
- Sélection du serveur
- Rôles de serveurs
- Fonctionnalités

Sélectionnez le serveur ou le disque dur virtuel sur lequel ins

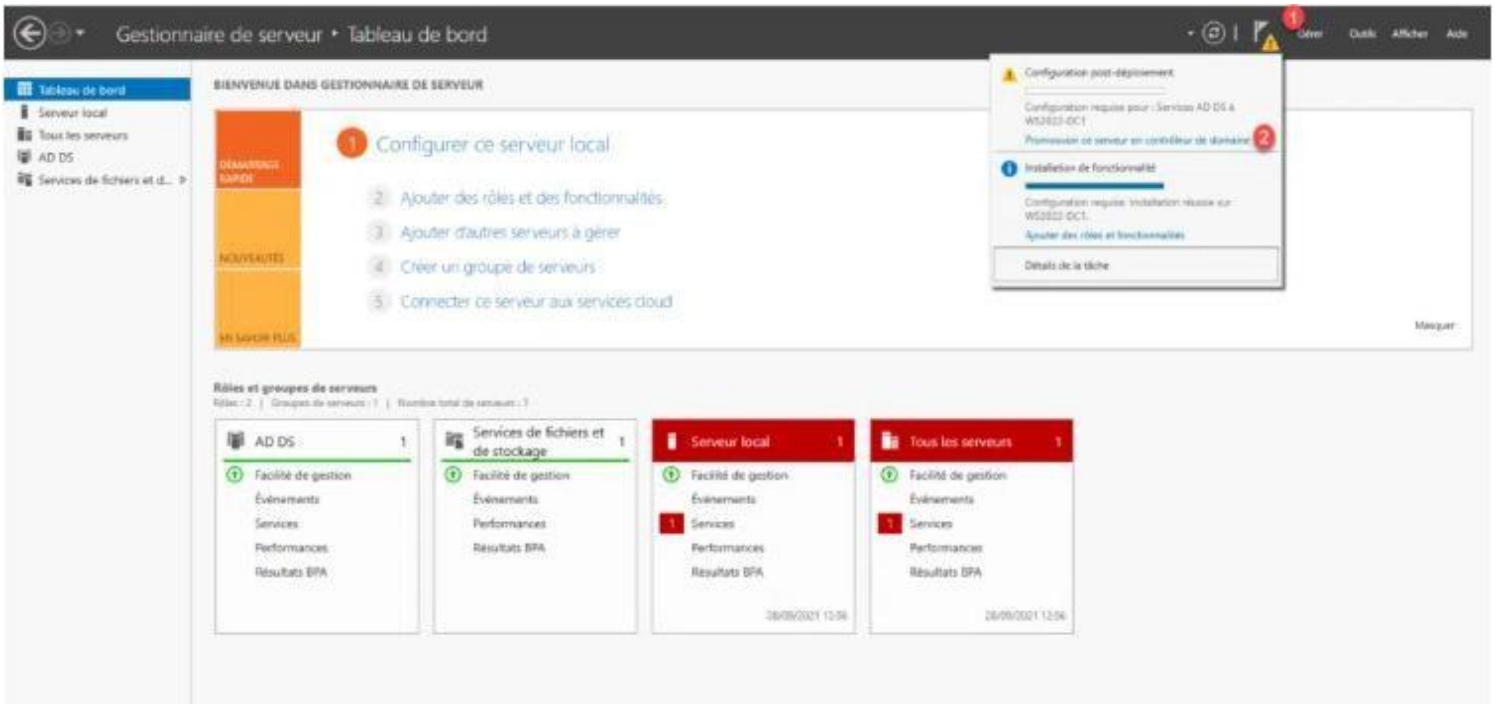
(•) Sélectionner un serveur du pool de serveurs
( ) Sélectionner un disque dur virtuel

Pool de serveurs

On passe les étapes de configuration en validant avec Suivant, puis on lance l'installation en cliquant sur Installer.



Après redémarrage du système, on clique sur l'icône de notification puis sur Promouvoir ce serveur en contrôleur de domaine 2 pour lancer l'assistant.



Quand l’assistant s’ouvre :

Sélectionne « Ajouter une nouvelle forêt »
- Indique le nom du domaine racine: marrakech.cub.fr
- Clique sur Suivant.
- Le nom NetBIOS est proposé automatiquement: MARRAKECH
- Vérification du récapitulatif des paramètres.
- ➜ On clique sur Installer pour lancer la configuration.

Le serveur va redémarré automatiquement et basculer vers le compte:

MARRAKECH\Administrateur

Retour :

Retour à la Documentation Technique

Haute disponibilité du service DHCP : Configuration du service DHCP en Failover/Load-balancing

Premièrement, on clone directement notre conteneur **DHCP** et de le renommer **DHCP2** pour mettre en place **la haute disponibilité du service**:

Assurer la **continuité du service** en cas de panne du serveur primaire (FAILOVER).
- Répartir la charge des **baux DHCP** entre les deux serveurs (LOAD-BALANCING).

I. Architecture

Serveur primaire DHCP (DHCP) : 172.16.33.100

Serveur secondaire DHCP (DHCP2) : 172.16.33.101

Ports Failover : 647 pour les deux serveurs

Les deux serveurs échangent les informations de baux et restent synchronisés pour éviter les conflits d’adressage IP.

II. Configuration du Serveur Primaire (DHCP).

On doit déclarer le **failover** dans le fichier de conf **/etc/dhcp/dhcpd.conf:**

```
# Declaration du FAILOVER DHCP pour le serveur primaire#
failover peer "cub" {
        primary;                        # D  clare ce serveur comme primaire
        address 172.16.33.100;          # Adresse du serveur primaire
        port 647;                       # Port d'  coute du serveur primaire
        peer address 172.16.33.101; # Adresse du serveur secondaire.
        peer port 647;                  # Port d'  coute du serveur secondai
        max-response-delay 60;          # Temps de non r  ponse en secondes.
        max-unacked-updates 10;
        mclt 3;                     # Temps de renouvellement du service
                                        # en cas d'incertitude.
        split 128;                      # R  partition des plages d'adresses
        load balance max seconds 3;
}
```

Le failover peer “cub” {…} permet de mettre en place la haute disponibilité avec le serveur secondaire. On indique l'adresse du primaire et celle du serveur secondaire, ainsi que les ports de communication.

- Primary : Ce serveur est le primaire.
- Split 128 : Découpe la plage IP pour le Load-Balancing.

```
# Les lignes suivantes servent    l'initialisation des deux serveurs DHC
#failover peer "cub" state {
#    my state partner-down;
#}

ddns-update-style none;
option domain-name "cub.fr";
option domain-name-servers 172.16.0.10;
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
```

On définit les paramètre généraux du serveur DHCP (nom de domaine, le serveur dns,…)

```
# A slightly different configuration for an internal subnet.
subnet 192.168.13.0 netmask 255.255.255.0 {
pool {
        failover peer "cub";
  range 192.168.13.1 192.168.13.21;
     }
  option domain-name-servers 192.168.13.23;
  option domain-name "marrakech.cub.fr";
  option routers 192.168.13.254;
  option broadcast-address 192.168.13.255;
  default-lease-time 600;
  max-lease-time 7200;
}

subnet 172.16.33.0 netmask 255.255.255.0 {
   range 172.16.33.1 172.16.33.11;
   option routers 172.16.33.254;
   option broadcast-address 172.16.33.255;
}
```

III. Configuration du Serveur Secondaire (DHCP2).

Pour le serveur secondaire, il est également nécessaire de déclarer le **failover** dans le fichier de configuration **/etc/dhcp/dhcpd.conf:**

```
# Declaration du FAILOVER DHCP pour le serveur secondaire#
failover peer "cub" {
        secondary;              # D  clare ce serveur comme secondaire
        address 172.16.33.101;
        port 647;
        peer address 172.16.33.100;
        peer port 647;
        max-response-delay 60;
        max-unacked-updates 10;
        load balance max seconds 3;
}
```

Le failover peer “cub” { secondary; … }: On définit que le serveur est secondaire et qu'il communique avec le serveur primaire pour qu'il puisse prendre le relais en cas de panne.

- Le split doit être définie que sur le serveur primaire, car c’est lui qui décide de la répartition des baux.

```
# A slightly different configuration for an internal subnet.      DHCP
subnet 192.168.13.0 netmask 255.255.255.0 {
pool {
        failover peer "cub";
  range 192.168.13.1 192.168.13.21;
     }
  option domain-name-servers 192.168.13.23;
  option domain-name "marrakech.cub.fr";
  option routers 192.168.13.254;
  option broadcast-address 192.168.13.255;
  default-lease-time 600;
  max-lease-time 7200;
}

subnet 172.16.33.0 netmask 255.255.255.0 {
   range 172.16.33.1 172.16.33.11;
   option routers 172.16.33.254;
   option broadcast-address 172.16.33.255;
}
```

IV. Initialisation du Failover.

1. On désactive le lancement automatique du service DHCP sur les deux serveurs:

update-rc.d isc-dhcp-server remove
reboot

Ensuite, on vérifie que le port 647 n'est pas actif sur les 2 serveurs:

ss -nlut

1. On décommente la section state sur le serveur primaire pour initialiser le failover:

failover peer "cub" state {
  my state partner-down;
}

1. On démarre le service DHCP primaire uniquement:

systemctl start isc-dhcp-server

Le fichier /var/lib/dhcp/dhcpd.leases contient les informations suivantes :

The format of this file is documented in the dhcpd.leases(5) manual page.
This lease file was written by isc-dhcp-4.4.3-P1

authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

failover peer "cub" state {

```
  my state normal at 2 2025/10/14 07:24:07;
  partner state normal at 2 2025/10/14 07:24:48;
  mclt 3;
}
lease 172.16.33.1 {
  starts 1 2025/09/29 12:44:09;
  ends 1 2025/09/29 13:44:09;
  tstp 1 2025/09/29 13:44:09;
  cltt 1 2025/09/29 12:44:09;
  binding state free;
  hardware ethernet 6e:22:8c:0f:8b:eb;
}
lease 172.16.33.2 {
  starts 4 2025/10/09 14:35:15;
  ends 4 2025/10/09 14:36:04;
  tstp 4 2025/10/09 14:36:04;
  cltt 4 2025/10/09 14:35:15;
  binding state free;
  hardware ethernet bc:24:11:4c:7c:64;
  uid "\001RAS \274$\021L|d\000\000\000\000\000\000";
}
lease 192.168.13.2 {
  starts 4 2025/09/18 12:27:17;
  ends 4 2025/09/18 12:37:17;
  tstp 4 2025/09/18 12:37:17;
  tsfp 4 2025/09/18 12:37:17;
  atsfp 4 2025/09/18 12:37:17;
  cltt 4 2025/09/18 12:27:17;
  binding state free;
  hardware ethernet bc:24:11:62:19:1b;
  uid "\001\274$\021b\031\033";
  set vendor-class-identifier = "d-i";
} …
```

1. On démarre ensuite le serveur secondaire:

```
systemctl start isc-dhcp-server
```

1. On arrête le serveur primaire, On recommente la section state et enfin on redémarre le serveur primaire.
2. On répéte l'opération pour le serveur secondaire.

V. Configuration du DHCP relay

Pour transmettre les requêtes DHCP sur le réseau, il faut configurer l’agent relais dans le fichier /etc/default/isc-dhcp-relay en ajoutant l’adresse du serveur secondaire afin que les clients puissent recevoir des adresses IP même si le serveur primaire est indisponible.

```
  GNU nano 7.2                                  /etc/default/isc-dhcp-rela
# 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="172.16.33.100 172.16.33.101"

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

# Additional options that are passed to the DHCP relay daemon?
OPTIONS=""
```

L'agent relais envoie les requêtes DHCP vers les deux serveurs pour garantir la haute disponibilité.

sudo systemctl restart isc-dhcp-relay

V. TEST sur un client

Pour effectuer le test, il est nécessaire d'arrêter le service DHCP sur le serveur primaire :

systemctl stop isc-dhcp-server

On exécute d'abord ifdown eth0 pour libérer l'adresse IP (Elle désactive l'interface réseau eth0):

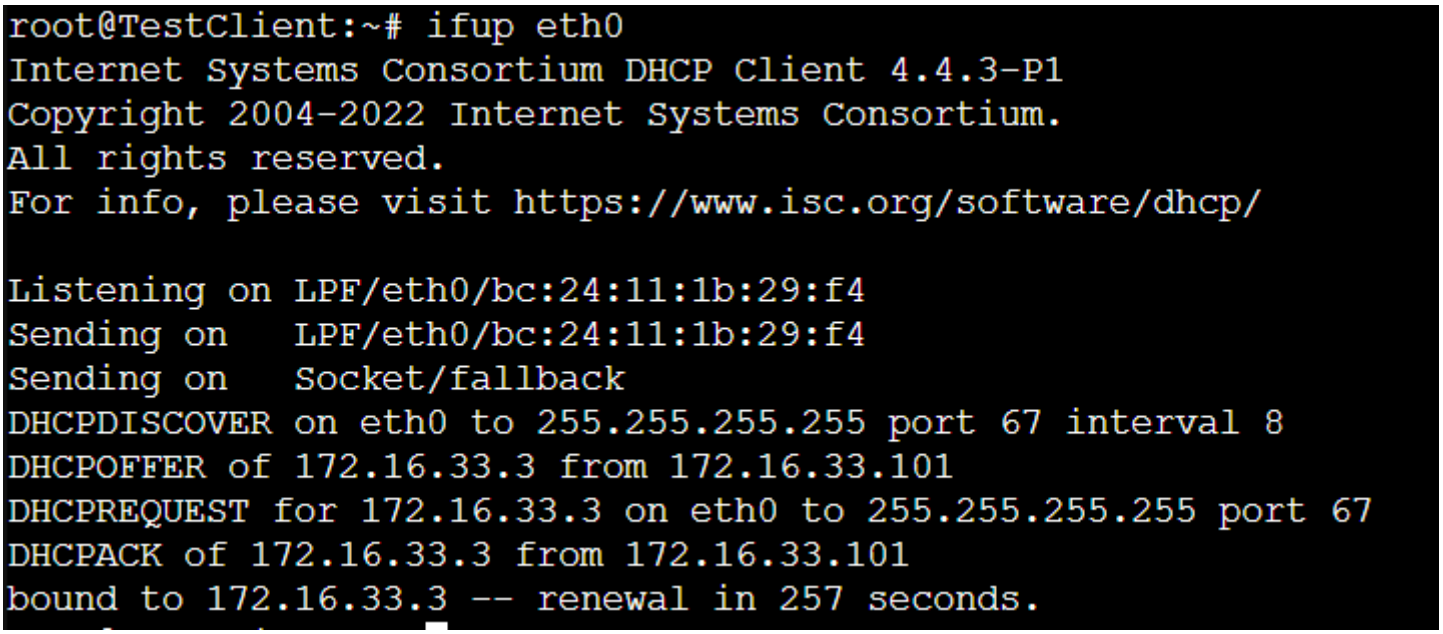
```
root@TestClient:~# ifdown eth0
Killed old client process
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/bc:24:11:1b:29:f4
Sending on   LPF/eth0/bc:24:11:1b:29:f4
Sending on   Socket/fallback
DHCPRELEASE of 172.16.33.3 on eth0 to 172.16.33.101 port 67
```

puis un ifup eth0 :

Elle réactive l'interface et relance le processus DHCP.

- Le client envoie une demande DHCP (DHCPDISCOVER) pour obtenir une adresse IP.

- Le serveur secondaire 172.16.33.101 répond avec une offre (DHCPOFFER).
- Le client accepte cette offre (DHCPREQUEST).
- Le serveur valide et confirme l'attribution (DHCPACK).



Retour :

Retour à la Documentation Technique

Installation du serveur Centreon

Après avoir créé le conteneur LXC relié à notre VLAN serveur 343, nous l'avons mis à jour à l'aide de la commande

apt update && apt upgrade.

1. installation des dépendance requise

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

2. Installation du dépôt Centreon avant l'installation du serveur 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

On importe ensuite la clé du dépôt:
wget -O- https://apt-key.centreon.com | gpg --dearmor | tee /etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1
apt update

3. Installation du serveur Centreon.

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

4. Configuration du serveur.

On a la possibilité de changer le nom de notre serveur:
hostnamectl set-hostname new-server-name

Pour que les services démarrent automatiquement au démarrage du système, il faut exécuter les commandes suivantes:
systemctl enable php8.2-fpm apache2 centreon cbd centengine gorgoned centreontrapd snmpd snmptrapd

On redémarre ensuite mariadb:
systemctl enable mariadb
systemctl restart mariadb

5. Sécurisation de la base de donnée.

mariadb-secure-installation

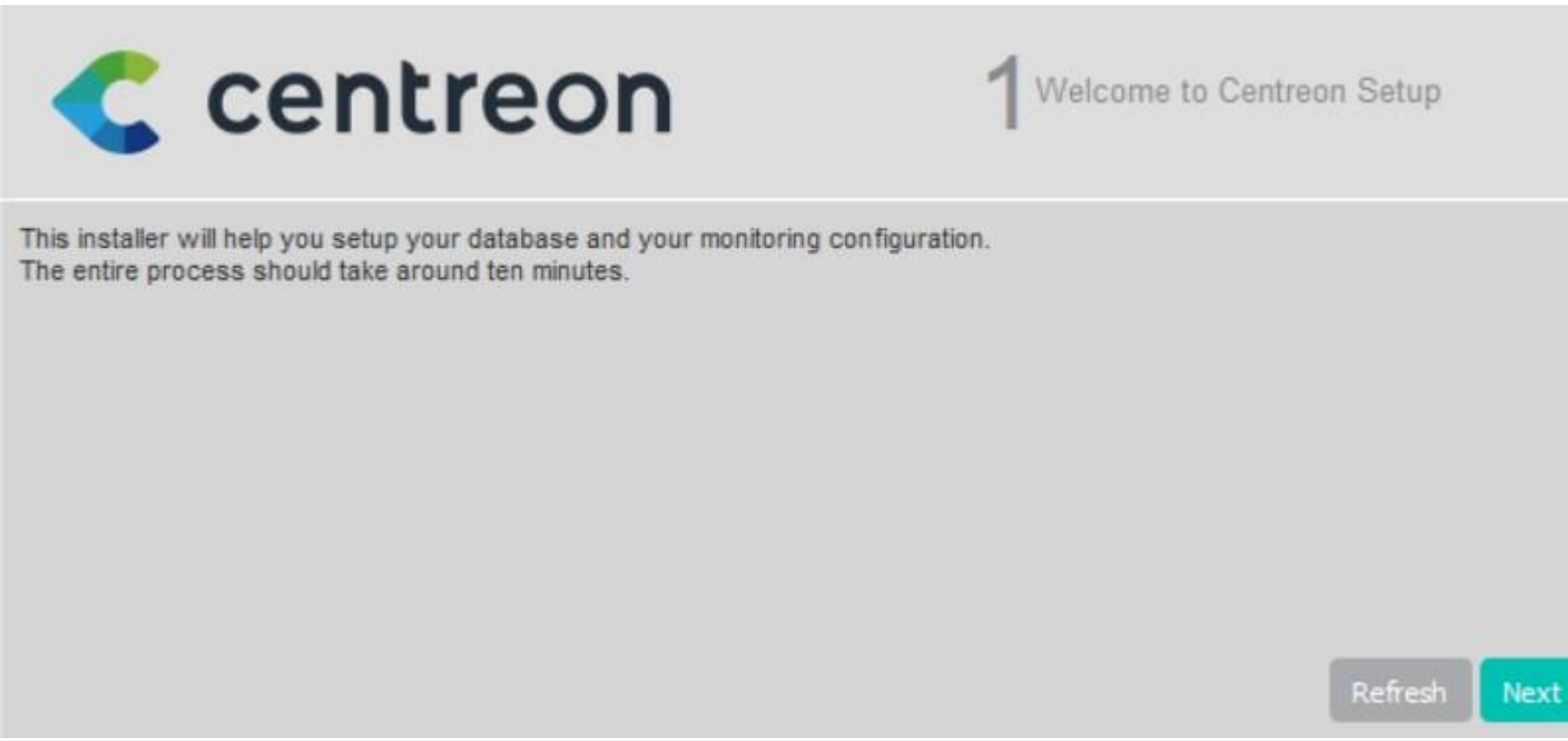
On répond oui à toutes les questions, sauf à “Disallow root login remotely ?”

6. Installation WEB

On redémarre le service apache:
systemctl start apache2

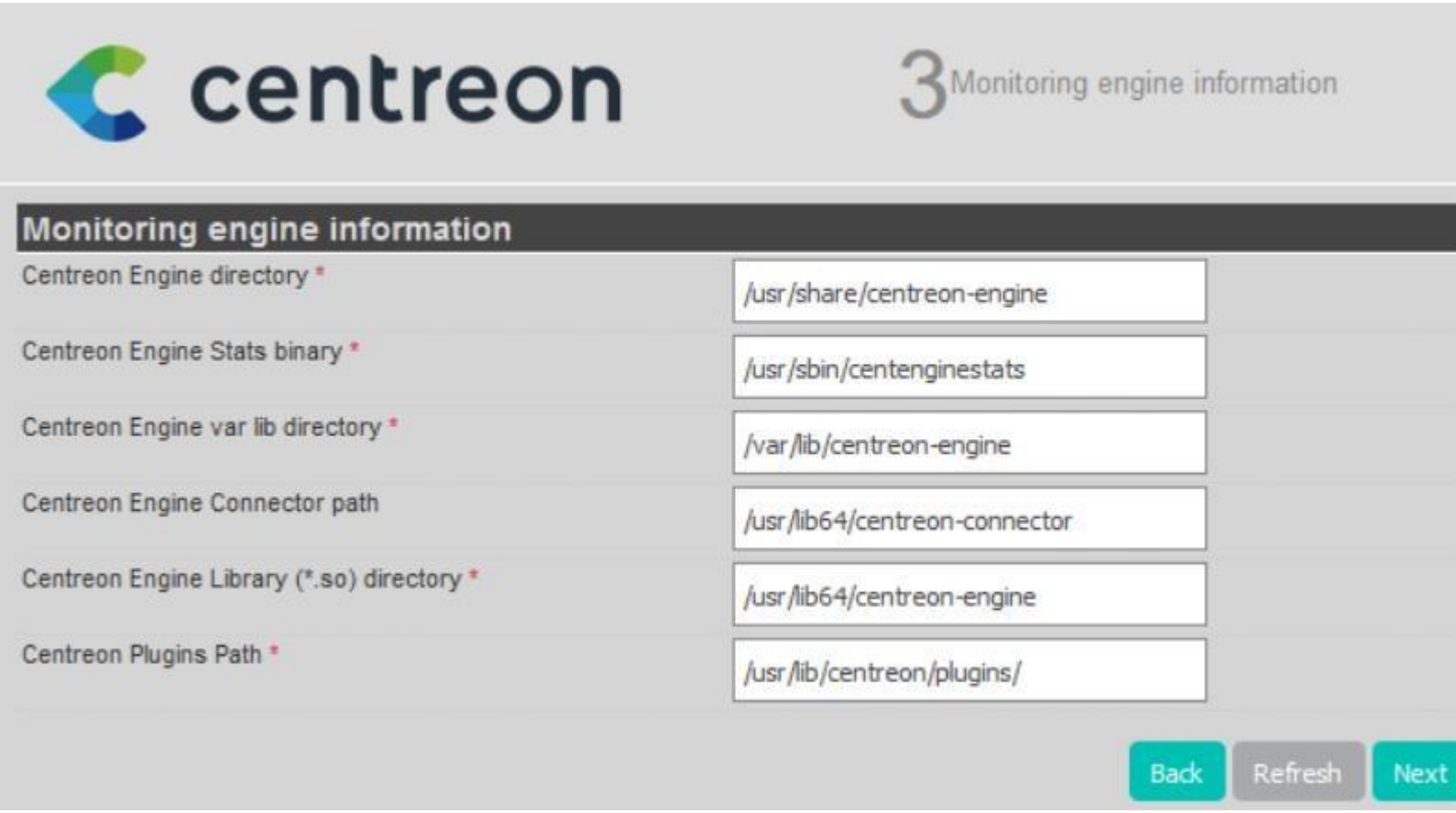
On peut maintenant ce connecté à l'interface web via http:IP/centreon.

L'assistant de configuration de Centreon s'affiche:



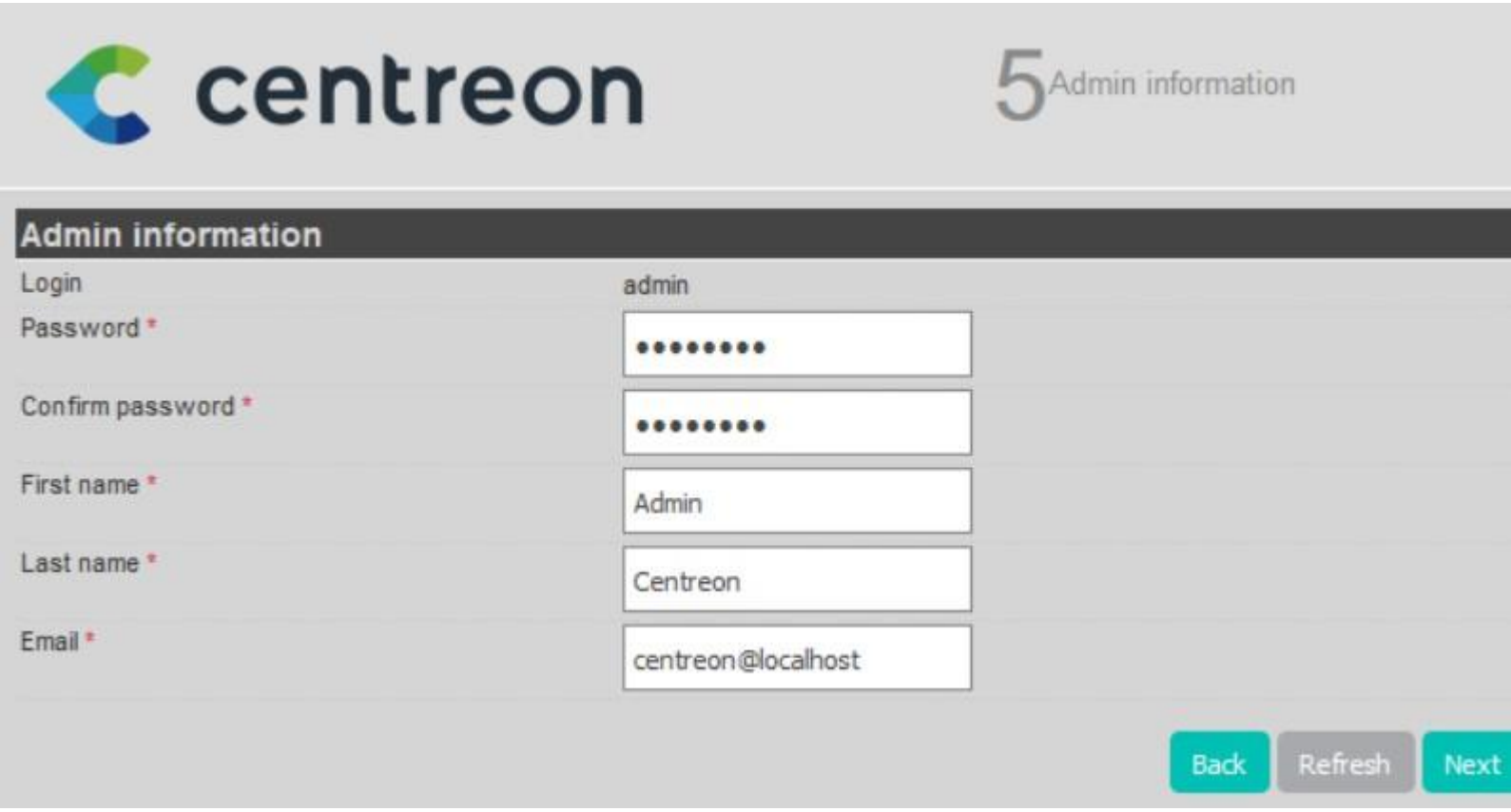
Les modules et les prérequis nécessaires sont vérifiés. Ils doivent tous être satisfaits. On doit ensuite cliquer sur Refresh.

Monitoring engine information (on laisse par défaut)

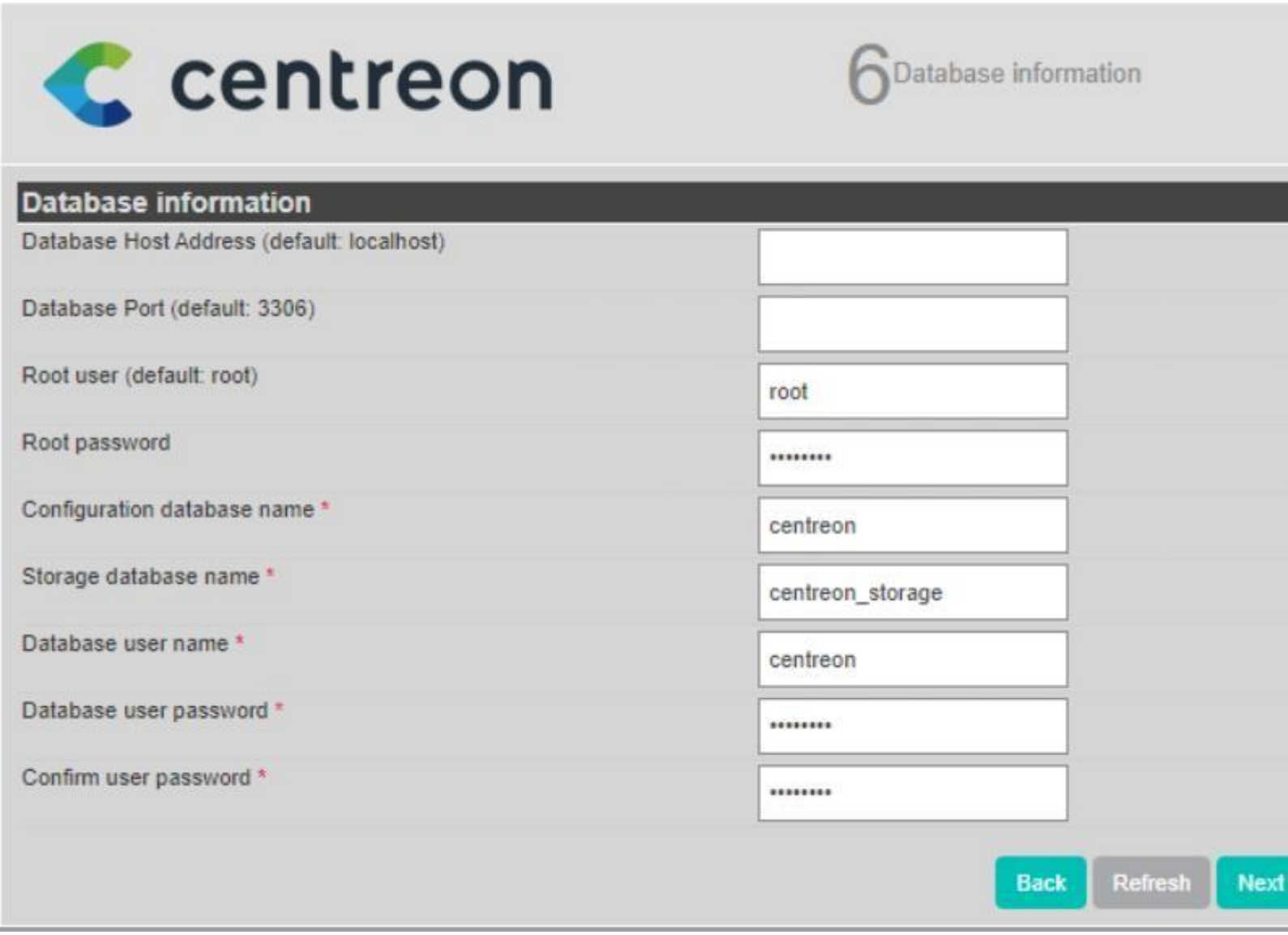


Broker module information (par défaut)

- On définis ensuite le mot de passe admin

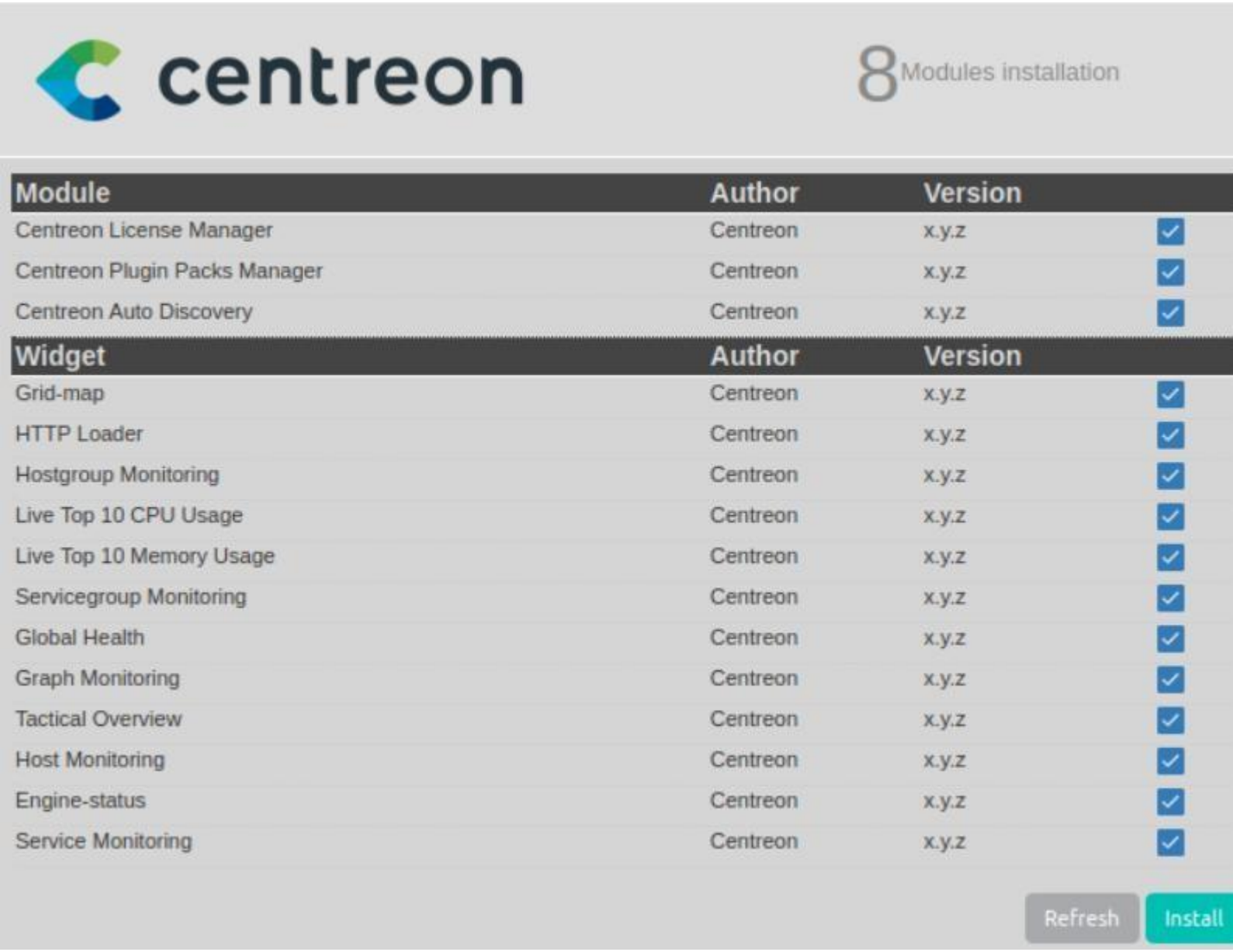


Et enfin on renseigne uniquement le mdp root et de la database



L'assistant de configuration crée les fichiers de configuration et les bases de données.

On doit Sélectionnez les modules et widgets disponibles à l'installation, puis on clique sur Install.



Installation finished

On peut maintenant ce connecter avec le compte admin

7. Initialisation de la supervision

Depuis l'interface web, accédez à Configuration > Collecteurs, sélectionnez le collecteur Central puis exportez la configuration en cochant l'option Déplacer les fichiers générés. Puis sur le serveur centreon, on redémarre les services nécessaire:

On redémarre les processus de collecte :
systemctl restart cbd centengine

On redémarre le gestionnaire de tâches :
systemctl restart gorgoned

On démarre les services de supervision passive :

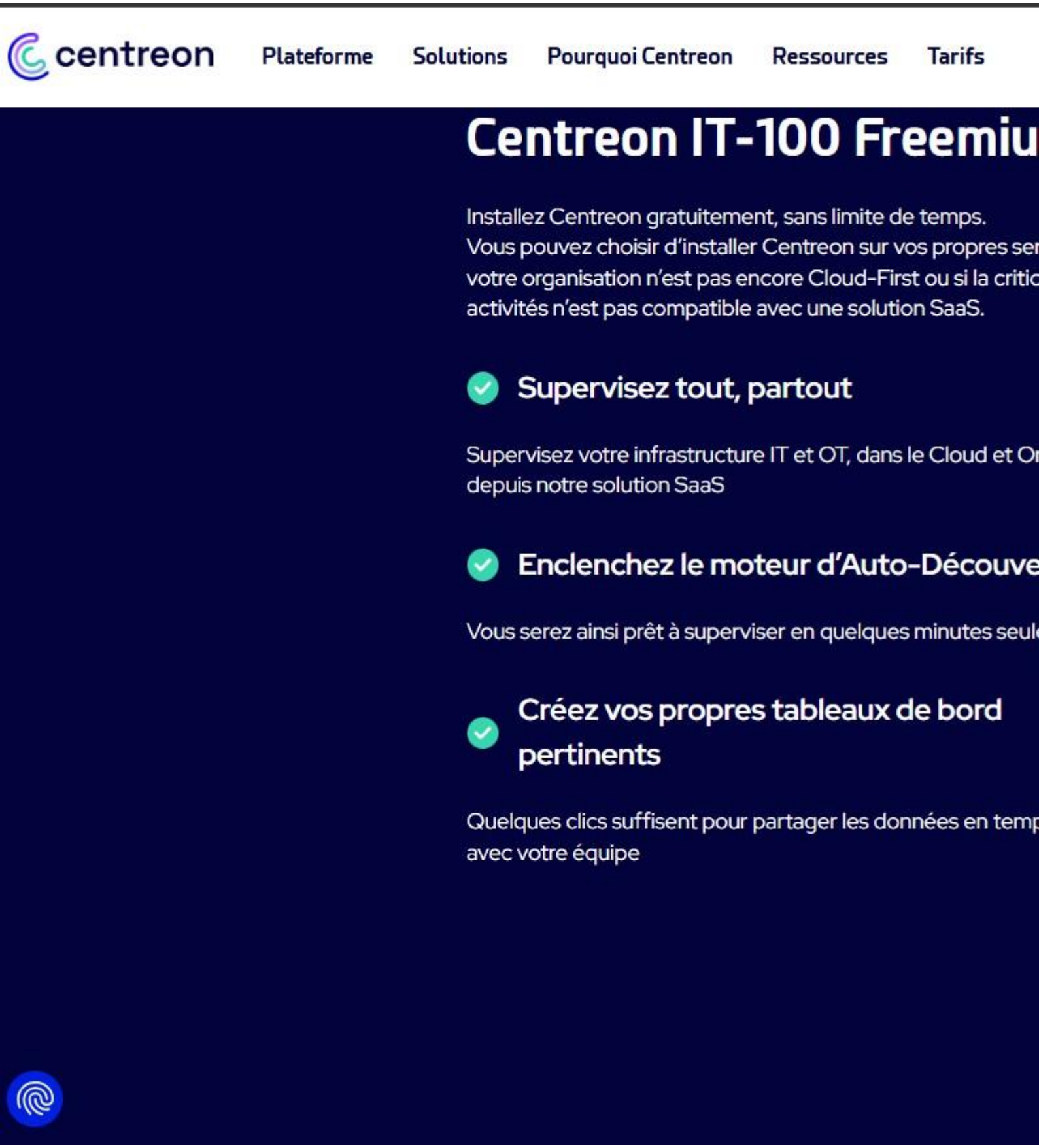
systemctl start snmptrapd centreontrapd

On démarre le démon SNMP :

systemctl start snmpd

8. Ajout de la licence IT-100.

Pour obtenir la version gratuite de Centreon IT-100, il faut se rendre sur le site officiel et remplir le formulaire requis. La clé de licence sera ensuite envoyée par e-mail.



Sur le compte admin de l'interface web, dans le menu Administration > Extensions > Manager et on clique sur le bouton Add Token. On saisie notre jeton puis Ajouter:

Supervision d'un serveur sous Linux

1- Installation de l'agent snmpd:

apt install snmpd

2- Installation des MIBs snmp:

Les MIBs permettent de convertir les OID en langage clair.

- Le paquet snmp-mibs-downloader n'est pas inclus par défaut.

Il faut éditer le fichier /etc/apt/sources.list :

deb http://archive.debian.org/debian/ buster main contrib non-free
deb http://archive.debian.org/debian/ buster-updates main contrib non-free
deb http://archive.debian.org/debian-security/ buster/updates main contrib non-free

3- Mise à jour le système et installation de snmp-mibs-downloader:

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

Les MIBs seront ensuite téléchargées dans le répertoire :

/usr/share/mibs

4- Sauvegarde de la configuration initiale:

Avant toute modification, sauvegardez le fichier de configuration d'origine:
root@debian:~# cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.orig

5- Modifier le fichier /etc/snmp/snmpd.conf:

Pour permettre l'accès depuis d'autres hôtes, il faut commenter la ligne suivante :
#agentAddress udp:127.0.0.1:161

Et il faut décommenter:

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

L'accès en lecture est défini par la directive rocommunity. Par défaut, seule la vue systemonly est autorisée :

view systemonly included .1.3.6.1.2.1.1
view systemonly included .1.3.6.1.2.1.25.1
rocommunity public default -V systemonly

Pour autoriser la lecture sur l'ensemble des objets SNMP, on doit le remplacer par :

view all included .1
rocommunity public default -V all

```
  GNU nano 7.2                                  /etc/snmp/snmpd.conf

#agentaddress  127.0.0.1,[::1]

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

###############################################################################
# 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  public  default  -V all
```

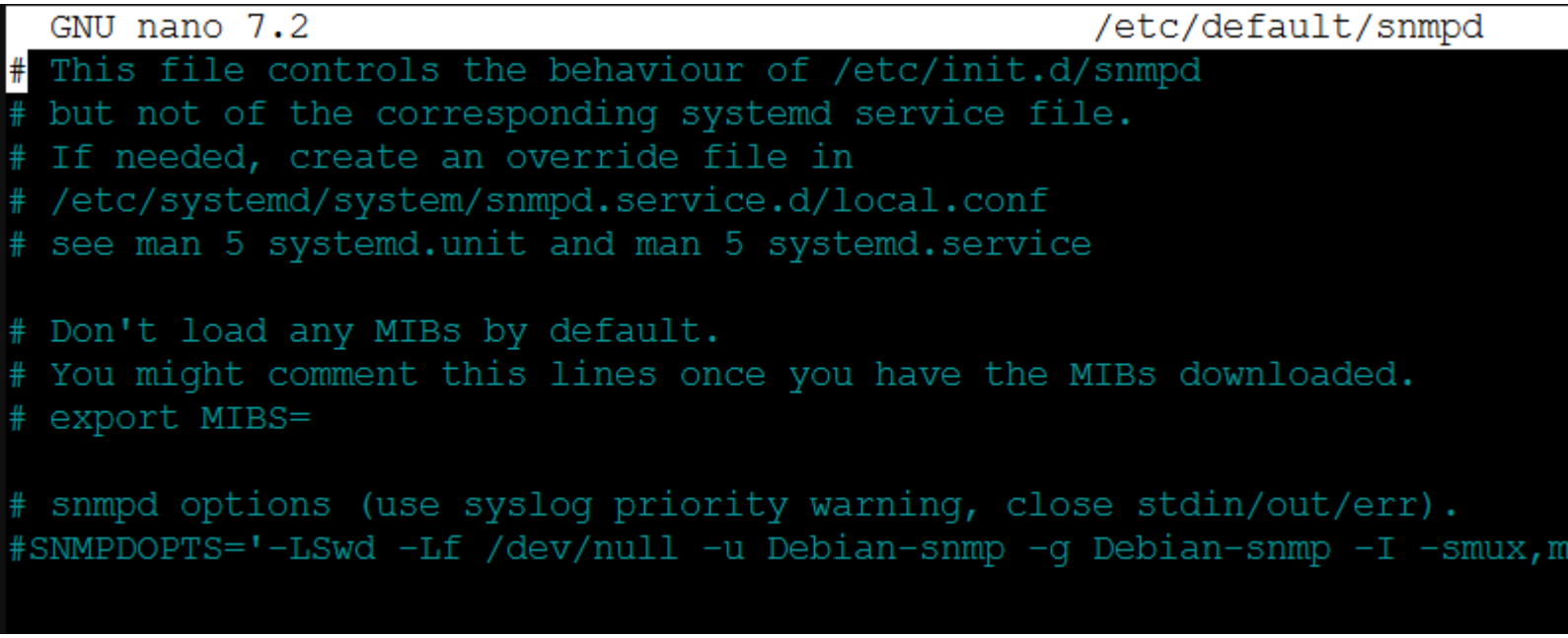
6- Modifier /etc/default/snmpd

On ajoute l'exportation de toutes les MIBs:

export MIBS=ALL

```
  GNU nano 7.2                                  /etc/default/snmpd
# 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
```

Il faut modifier le fichier de configuration /etc/snmp/snmp.conf en commentant la ligne mibs sur le serveur centreon:



7- Redémarrage du service SNMP

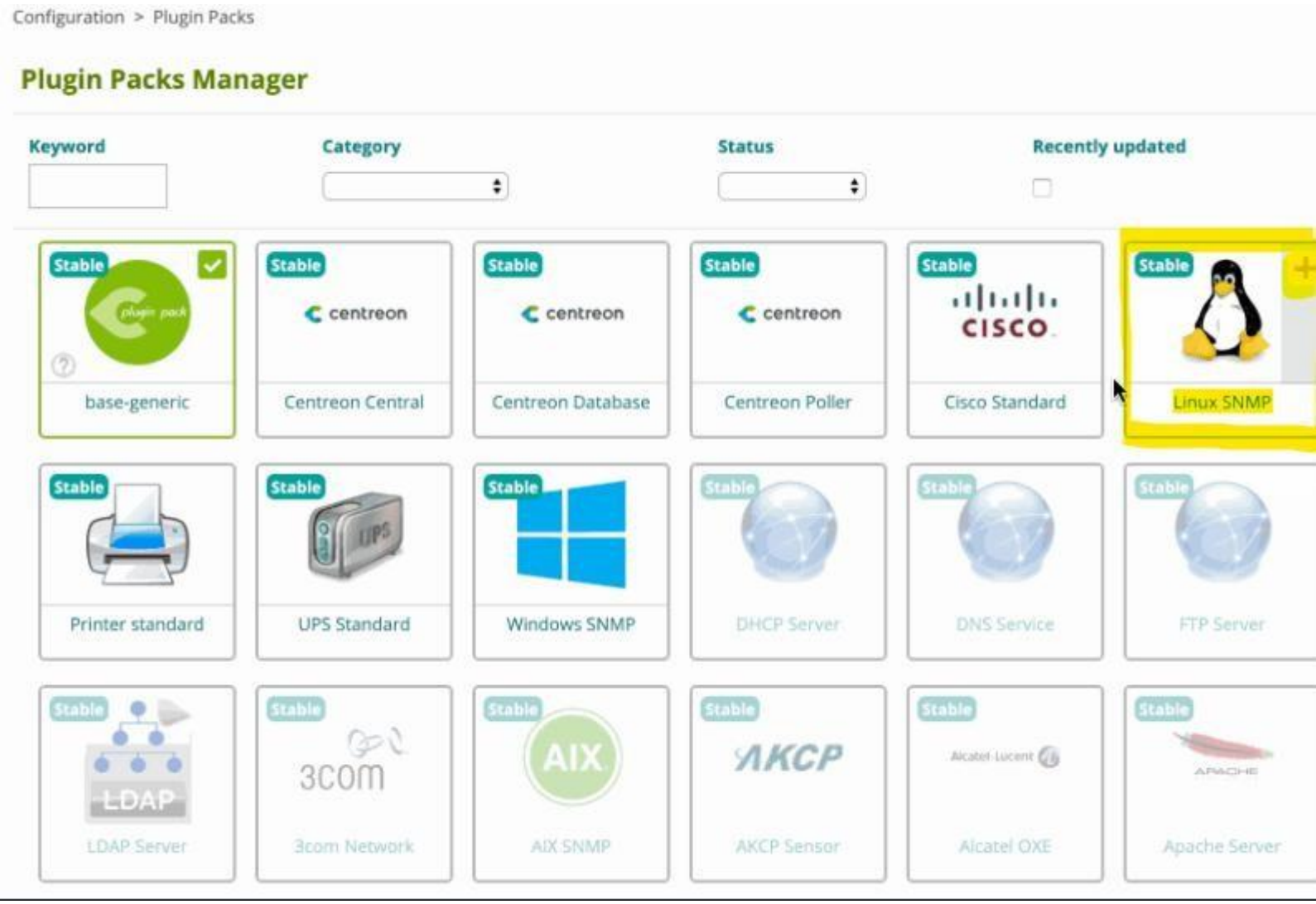
root@debian:~#service snmpd restart

8- Vérification du bon fonctionnement du service après l'installation du client SNMP. :

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

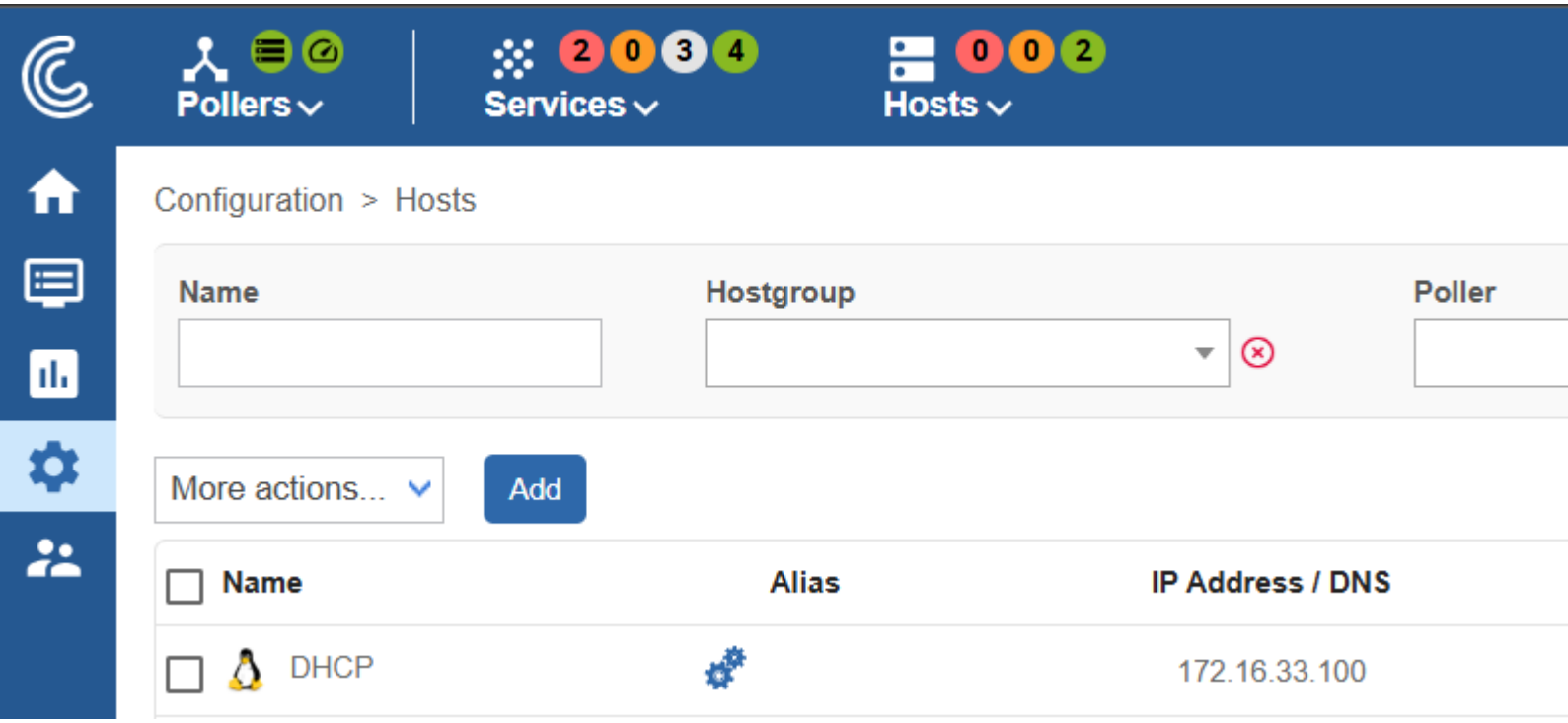
9- Configurer l'hôte et déployer la configuration

Depuis l'interface du serveur Centreon, ouvrez le menu Configuration > Connecteurs > Connecteurs de supervision, puis procédez à l'installation du connecteur de supervision Linux SNMP.

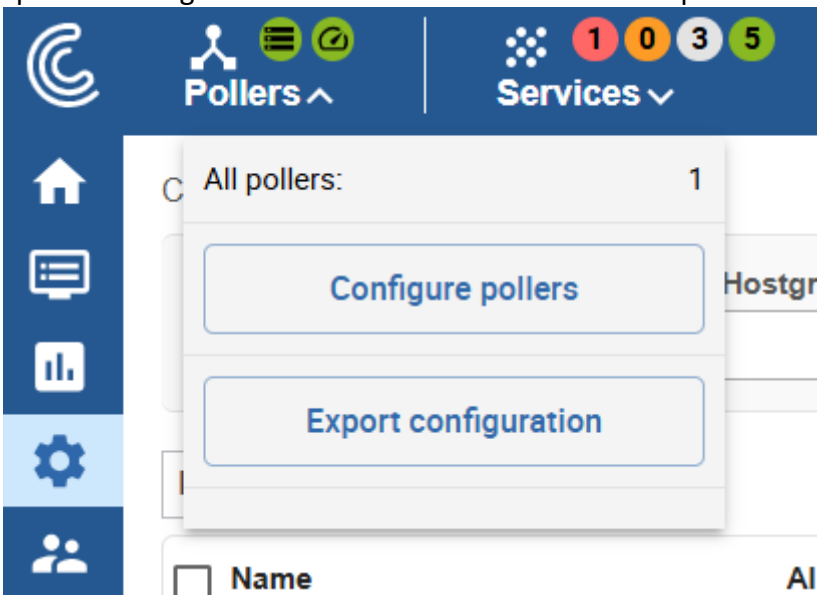


Dans Centreon, configurez un nouvel hôte en accédant à Configuration → Hôtes → Hôtes, puis en sélectionnant Ajouter.

- On doit saisir les informations nécessaire:



Après cette étape, accéder au menu Configuration > Pollers, puis exporter la configuration afin d'appliquer les changements effectués sur le serveur de supervision.



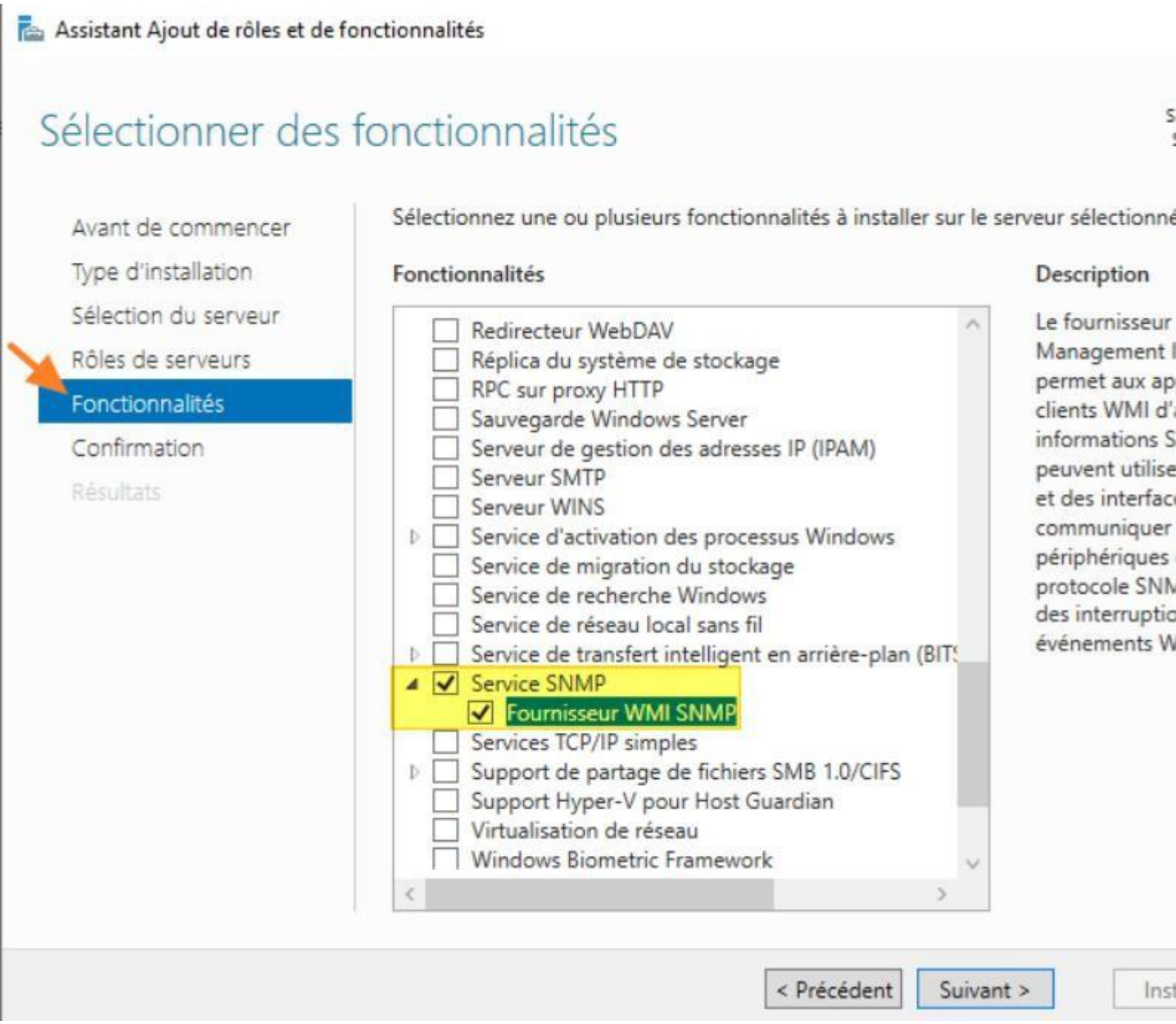
Ensuite dans Configuration > Services > Services par hôte. Un ensemble d'indicateurs a été créé automatiquement.

- Accéder au menu Surveillance > Statut des ressources, puis sélectionner Toutes dans le filtre Statut des ressources.
- Dans un premier temps, les ressources apparaissent avec le statut En attente, indiquant qu'aucun contrôle n'a encore été exécuté par le moteur de supervision.

Il faut que tous les services soit en état “Ok”!

installation et configuration du service SNMP sous Windows Server

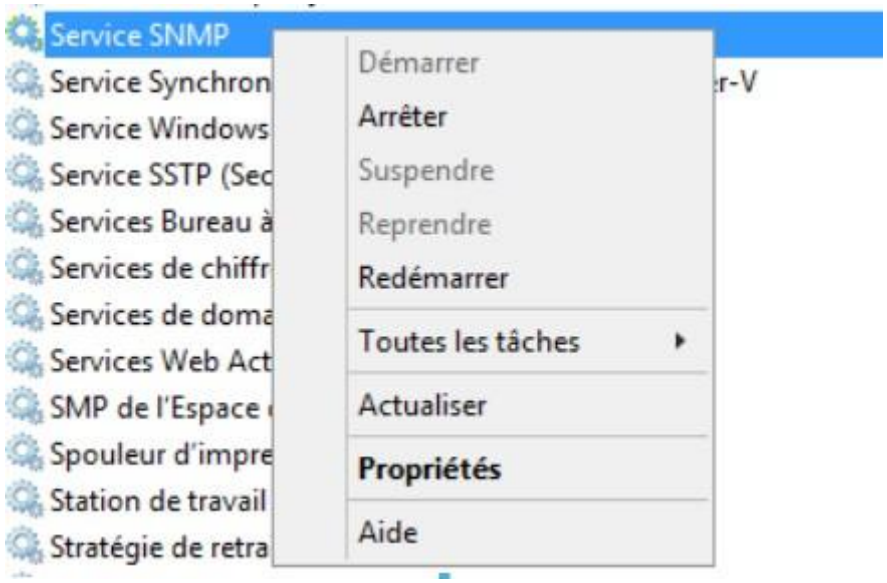
Dans le Gestionnaire de serveur, cliquez sur “Gérer” puis “Ajouter des rôles et fonctionnalités” à l’étape Fonctionnalités, il faut cocher Service SNMP.



1- Il faut accéder au service SNMP

Ouvrez la console Services (services.msc).

- Recherchez le service Service SNMP.
  - Clic droit → Propriétés

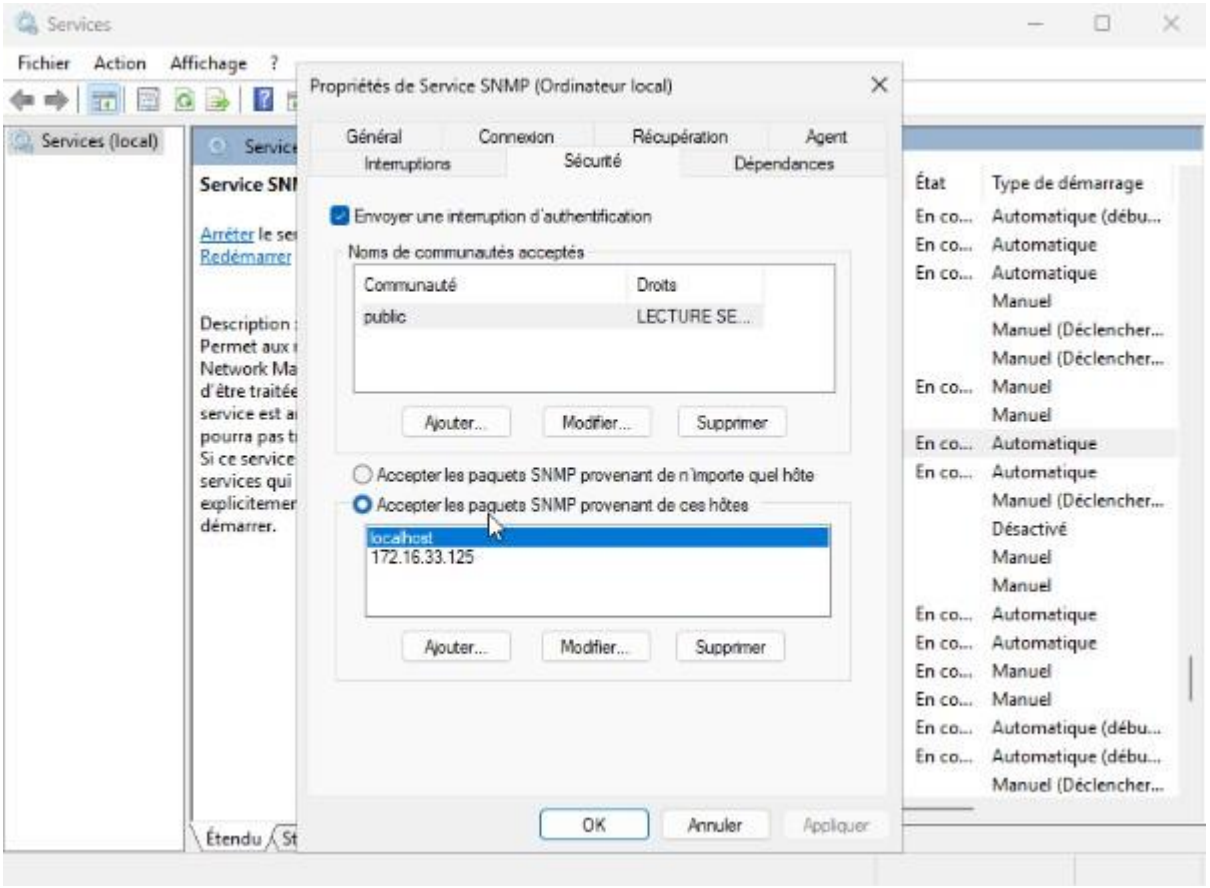


2- Dans l'onglet “Sécurité”:

Cliquez sur Ajouter pour créer une nouvelle communauté.

- Cocher l'option “Accepter les paquets SNMP provenant de ces hôtes” et ajoutez à la liste votre serveur de supervision.

3-

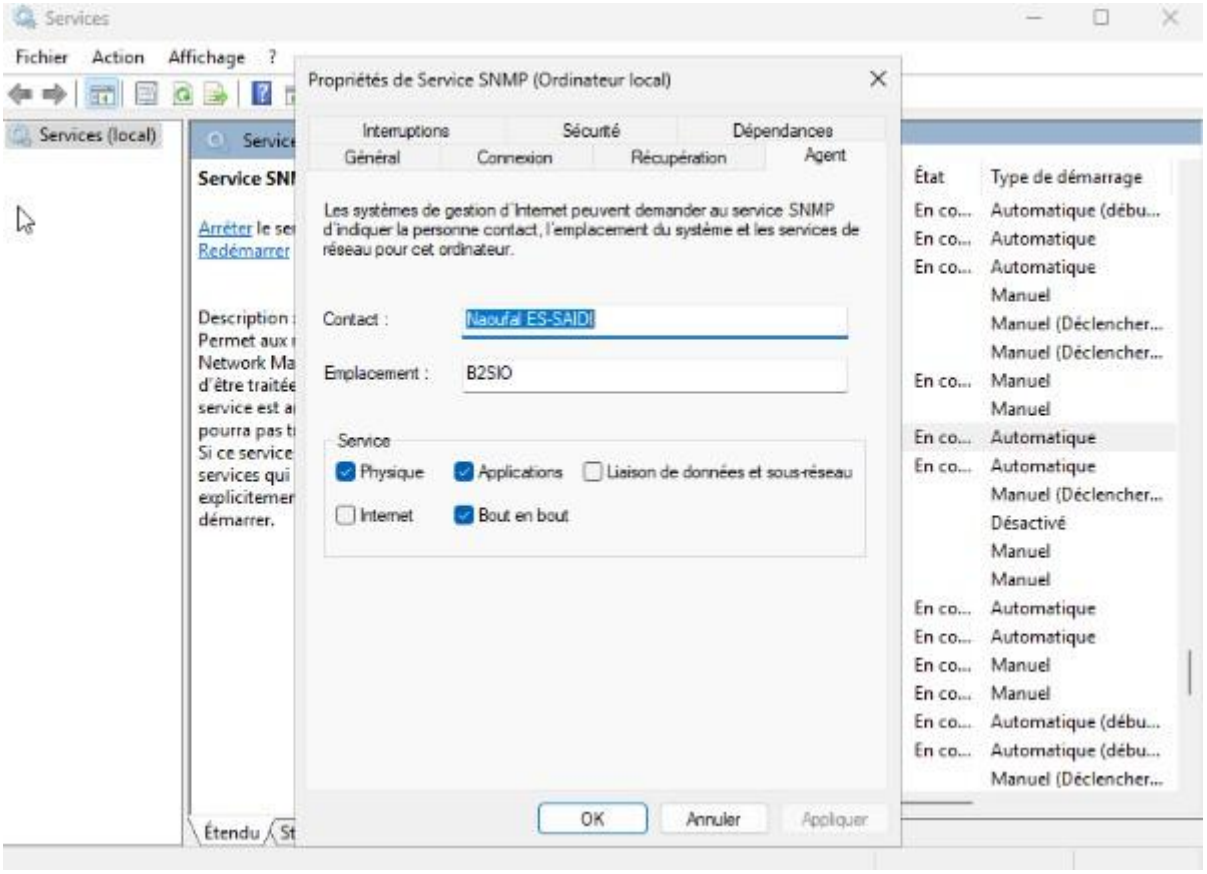


Onglet “Agent”

Permet de renseigner les informations sur le serveur pour l’agent SNMP

Dans Options “Service”

On Indique quelles données le serveur peut gérer : Physique : périphériques matériels (disques, etc.) Applications : applications transmettant des données via TCP/IP Bout en bout : connectivité TCP/IP



Retour :

Retour à la Documentation Technique

Supervision Apache 2 avec mod_status et Centreon 3.0

1 - Activation de mod_status dans Apache et ajout de la directive dans le VHOST :

On active les modules à l'aide des commandes :

a2enmode status

et

a2enmod info

On ajoute les **adresses IP** autorisées à accéder à l'URL **/server-status**, en configurant la directive Location comme suit :

nano /etc/apache2/mods-enabled/status.conf

```
<Location /server-status>
   SetHandler server-status
   Order deny,allow
   Deny from all
   Allow from 127.0.0.1 ::1 172.16.33.125
</Location>
```

centreon récupère donc les informations de **mod_status**

On redemarre ensuite le service **Apache** :

service apache2 restart

Pour vérifier le fonctionnement de **mod_status** on consulte la page http://localhost/server-status :

lynx http://localhost/server-status

On teste ensuite le lien depuis Centreon :

lynx http://IP-serveur-Apache/server-status

↓

lynx http://172.16.33.150/server-status

Supervision de PHP

1 - création d'un utilisateur MySql pour la Supervision

Une fois en root MySql on utilise la commande de création :

CREATE USER 'centreon'@'%' IDENTIFIED BY 'MotDePasseFort';

2 - Attribution des droits

Ce processus permet de lui donner les droits sur la base de données Centreon.

On utilise cette commande :

GRANT SELECT, SHOW DATABASES, PROCESS ON *.* TO 'centreon'@'%';
GRANT SELECT ON centreon.* TO 'centreon'@'%';

On applique ensuite ses privilèges grâce a cette commande :

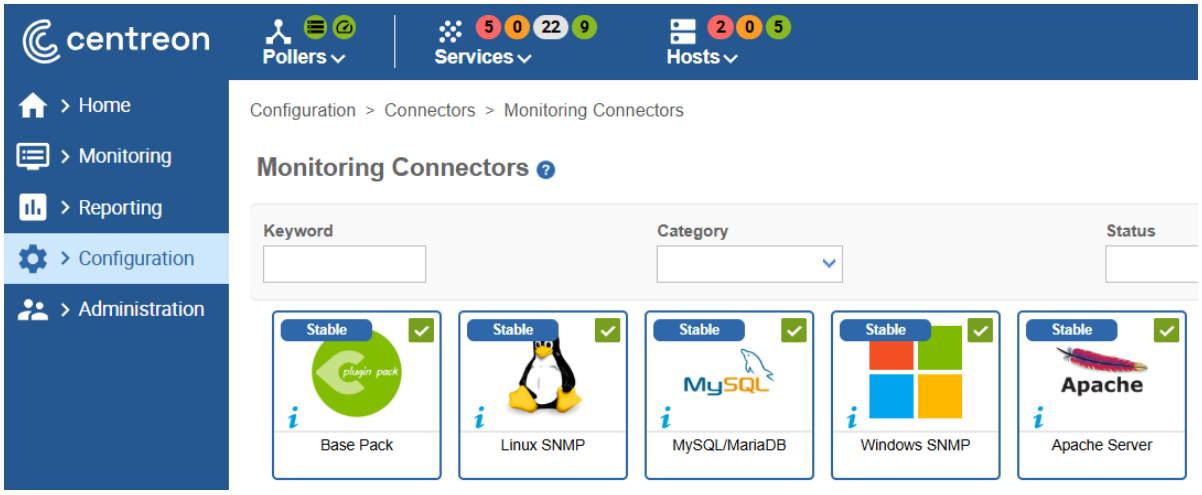
FLUSH PRIVILEGES;

3 - Intégration dans l'interface Centreon

1. Accéder à : Configuration → Plugin Packs → Gestionnaire

2. Rechercher : MySQL / MariaDB

3. Installer le pack correspondant à votre environnement.



On passe ensuite a l'installation sur le Poller :

Centreon :

yum install centreon-plugin-database-mysql

Debian :

apt install centreon-plugin-Applications-Databases-Mysql

On ajoute ensuite l'hôte Mysql dans Centreon :

1. Aller dans : Configuration → Hôtes → Ajouter

2. Renseigner :

Nom de l'hôte : PHP

Adresse IP / FQDN : 172.16.33.151

Modèle : App-DB-MySQL-custom (ou similaire selon le pack)

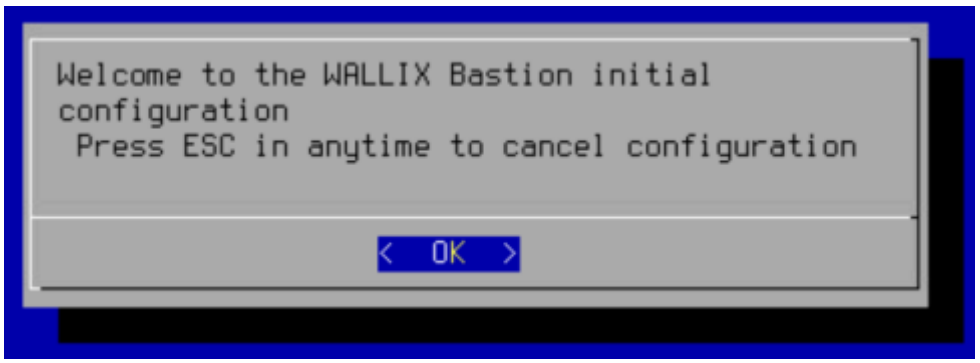
3. Sauvegarder.

Retour :

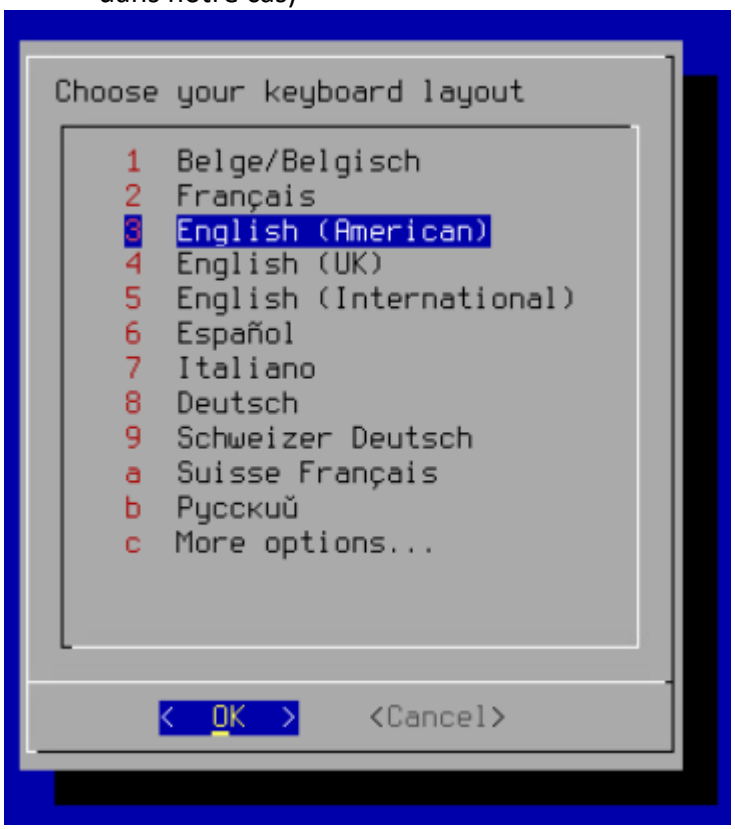
Retour à la Documentation Technique

Déploiement de Wallix Bastion :

Au démarrage, un message de bienvenue pour la configuration initiale du bastion WALLIX s'affiche. On clique sur OK pour continuer.



Sélectionnez la langue et l'emplacement de la disposition de clavier souhaitée. (Français dans notre cas)



.

Déploiement de Access Manager :

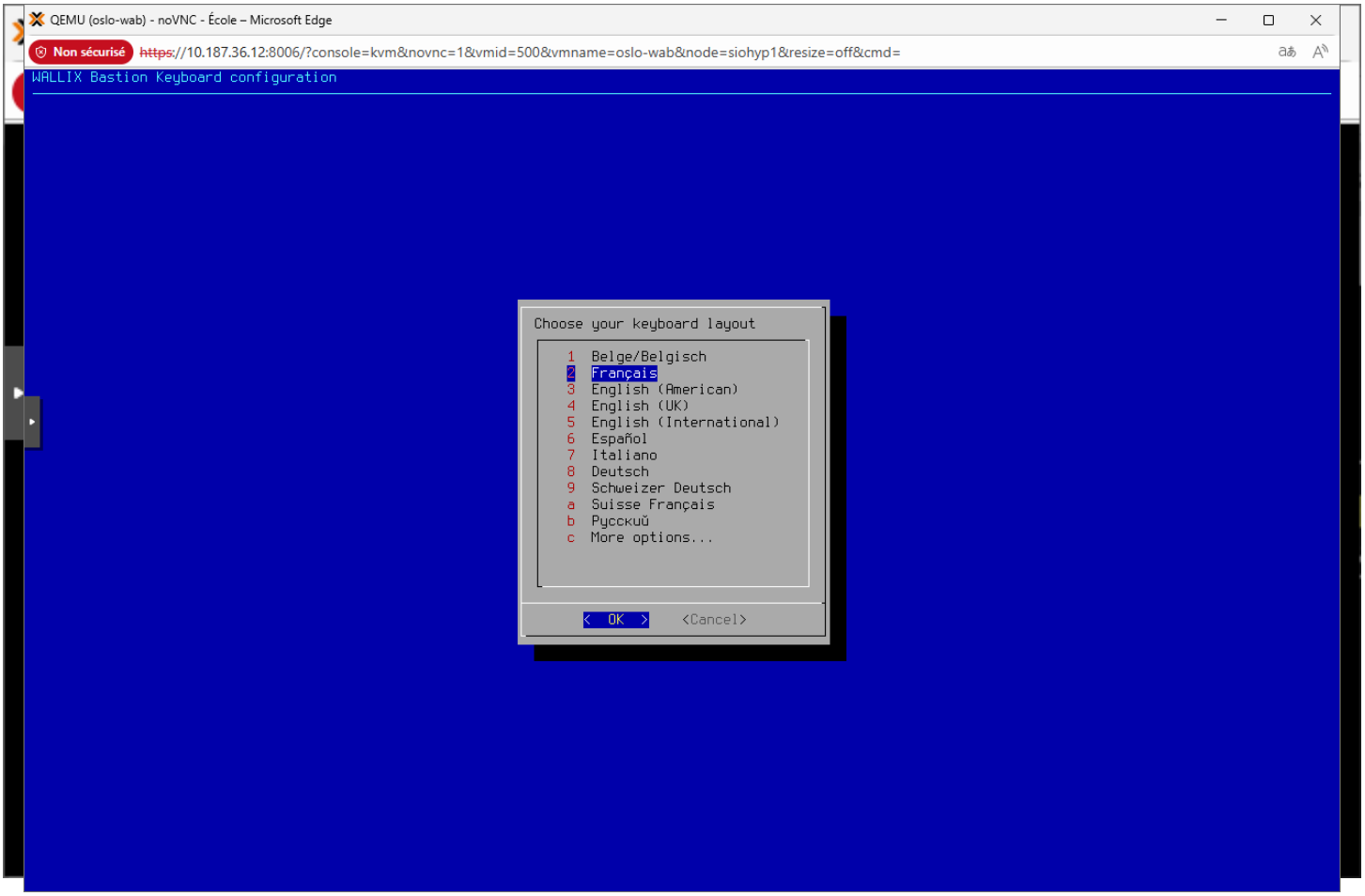
Création d'une VM :

- Nom : Access Manager
- 2 cœurs
- 4 Gio de RAM
- 40 Gio de disque dur
- 1 Interface réseau

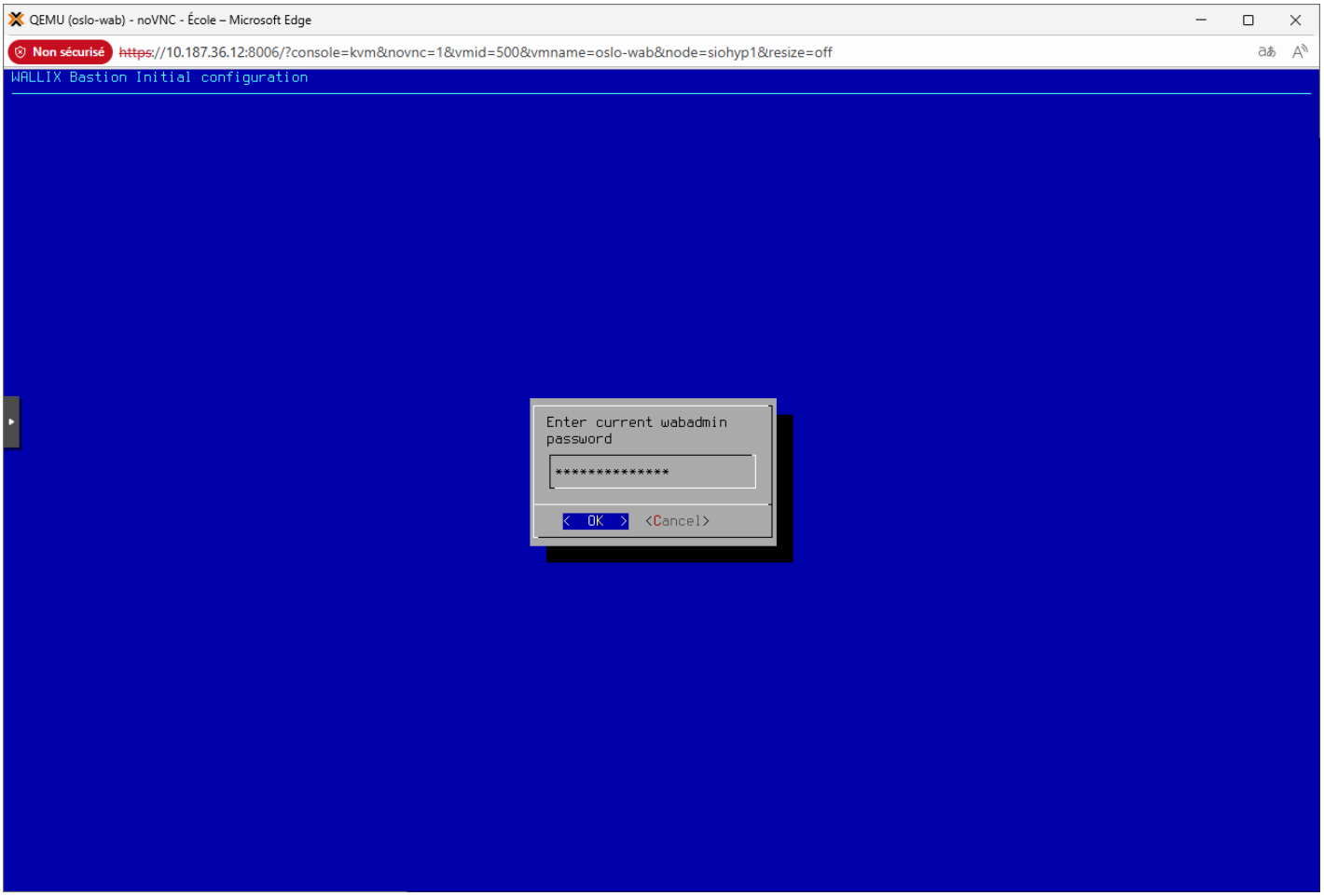
Configuration du Bastion Wallix

Installation du bastion

1re installation



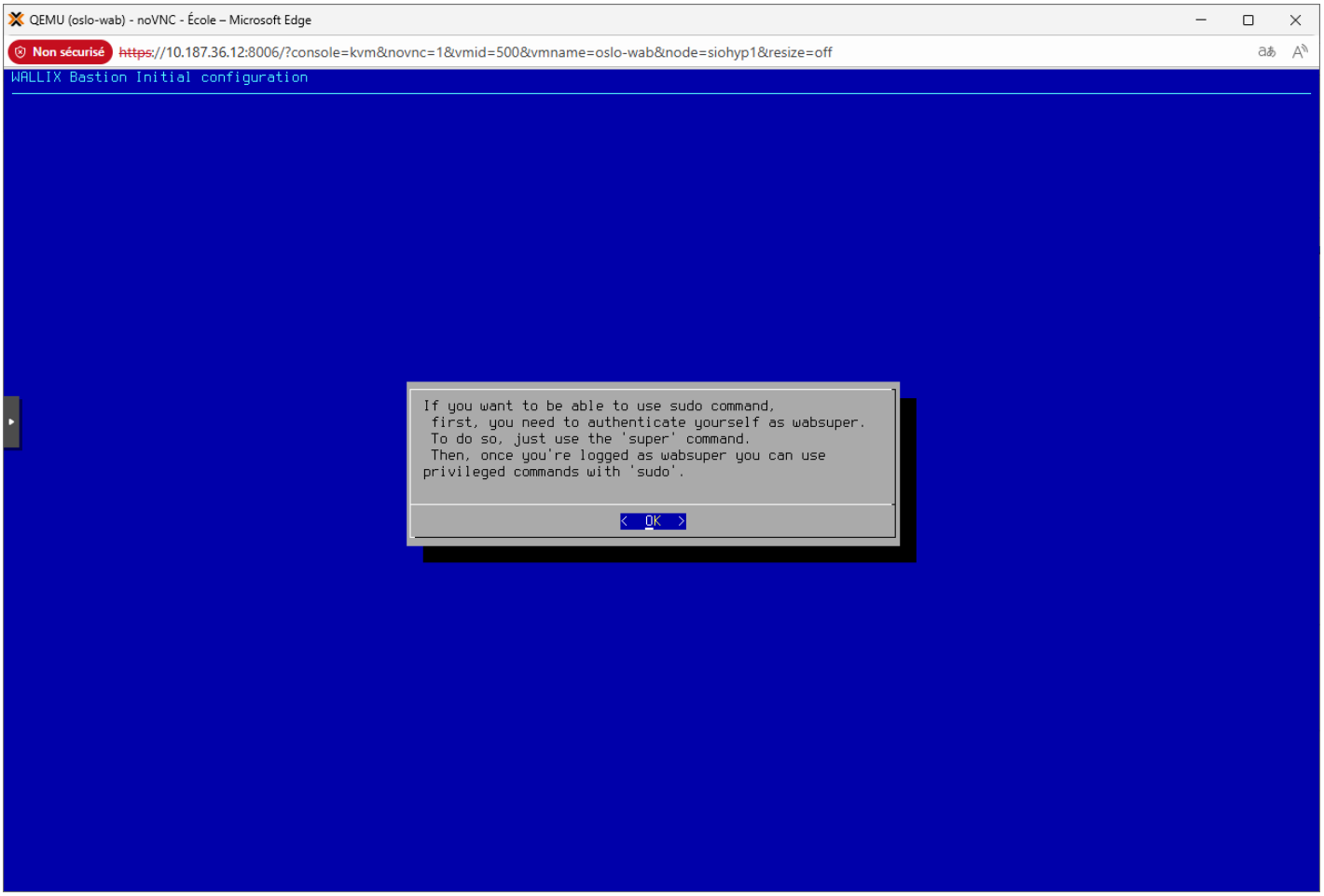
Saisir le mot de passe par défaut **SecureWabAdmin** du compte **wabadmin**



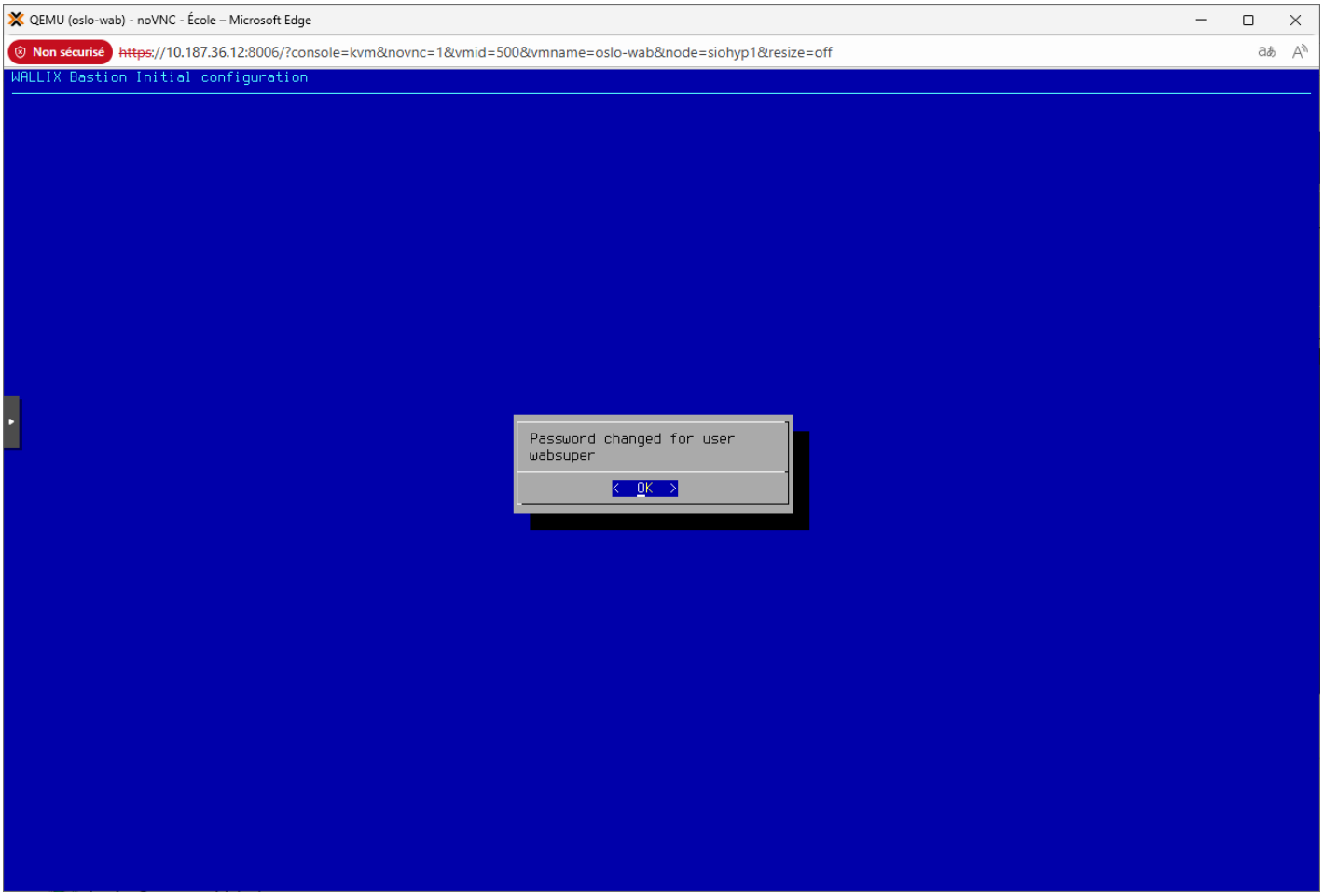
définir un nouveau mot de passe avec les caractéristiques suivantes :

- longueur minimale : 14
- caractère spécial : 1 minimum
- lettre majuscule : 1 minimum
- lettre mininuscle : 1 minimum
- caractère numérique : 1 minimum

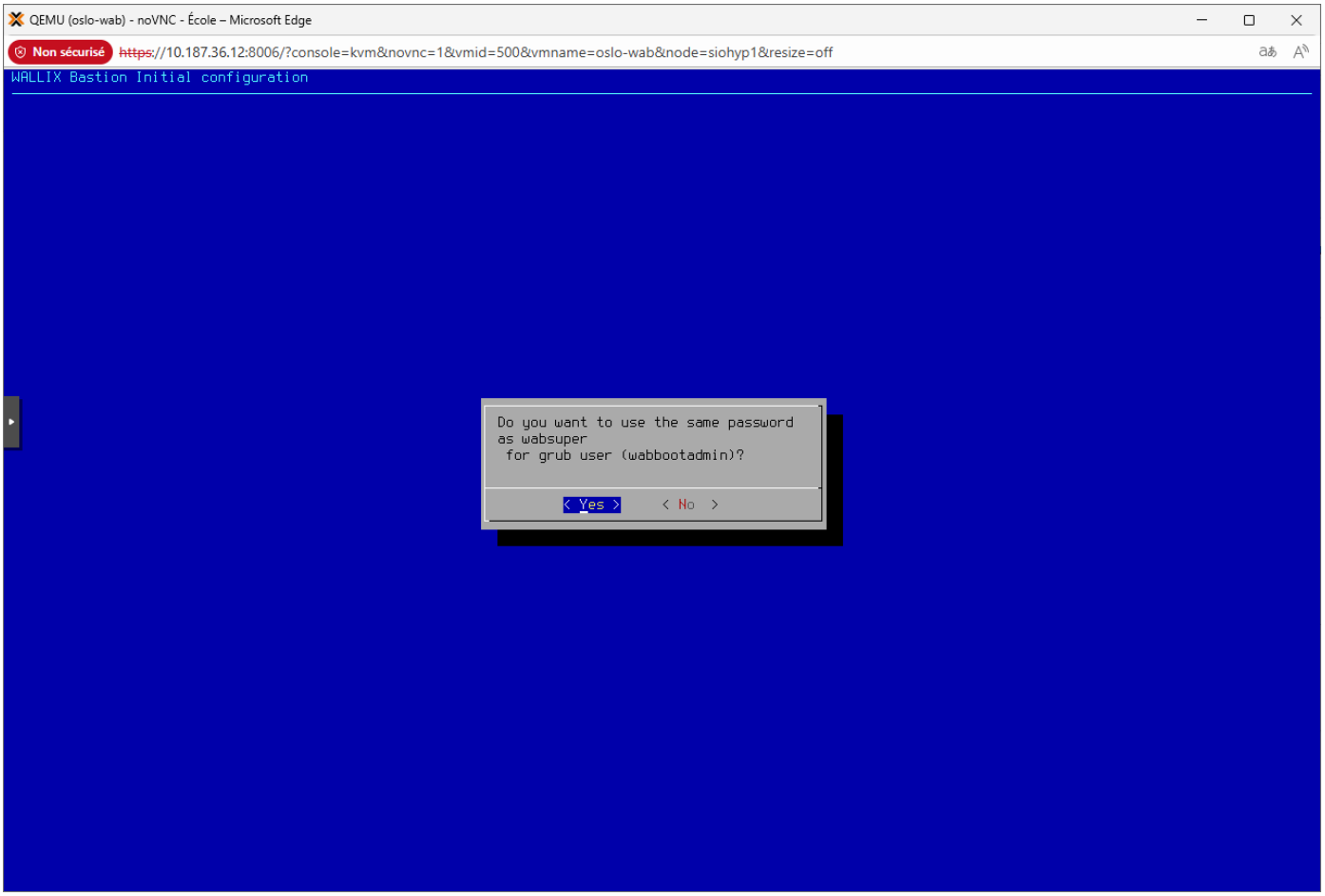
* => P@$$w0rd2025Secure

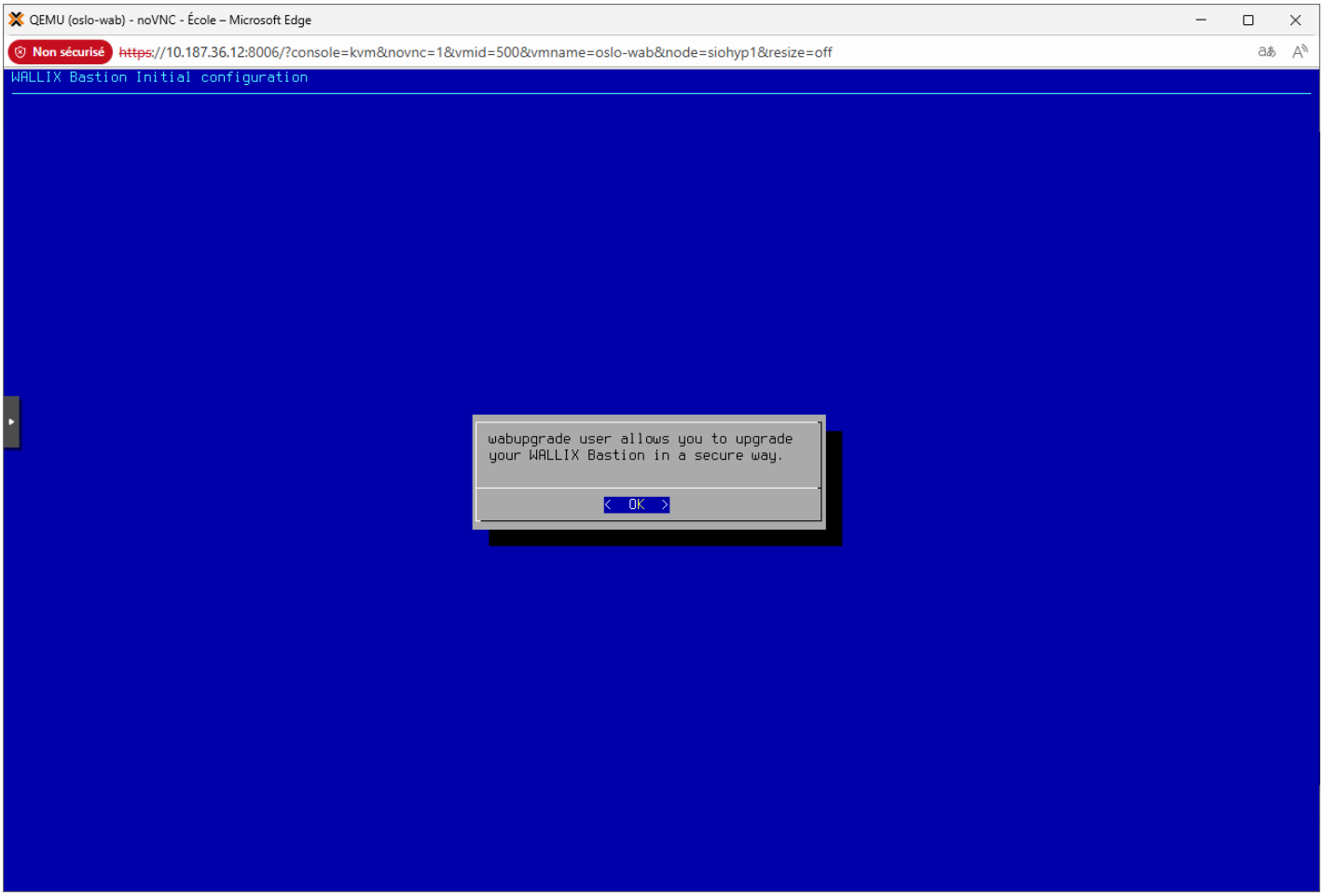


- Définir le mot de passe du compte **wabsuper** ⇒ P@$$w0rd2025Secure

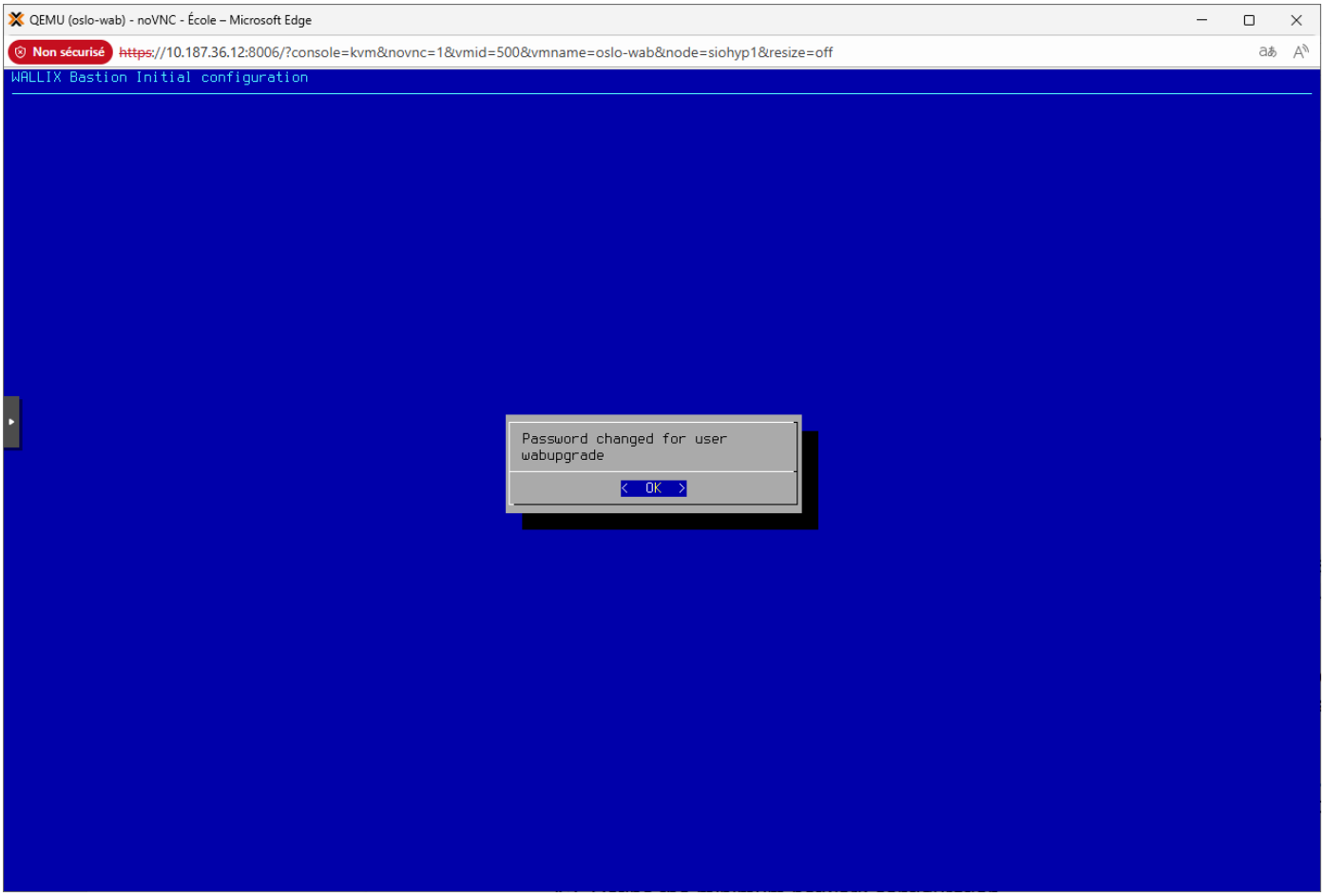


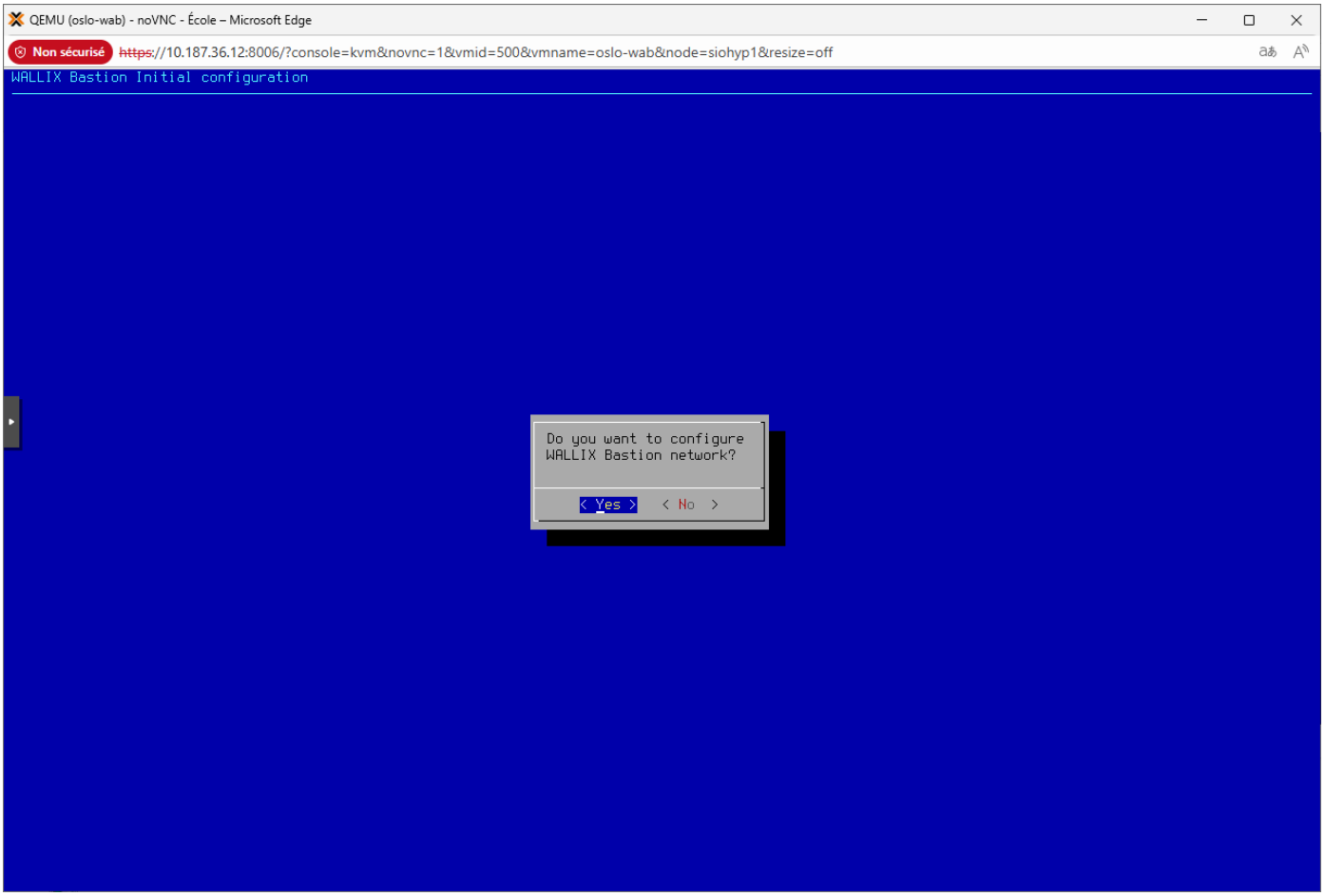
Définir le même mot de passe du compte **wabsuper** pour le compte **wabbootadmin** ⇒ P@$$w0rd2025Secure


QEMU (oslo-wab) - noVNC - École – Microsoft Edge
Non sécurisé
https://10.187.36.12:8006/?console=kvm&novnc=1&vmid=500&vmname=oslo-wab&node=siohyp1&resize=off
WALLIX Bastion Initial configuration
Do you want to use the same password
as wabsuper
for grub user (wabbootadmin)?
< Yes >
< No >



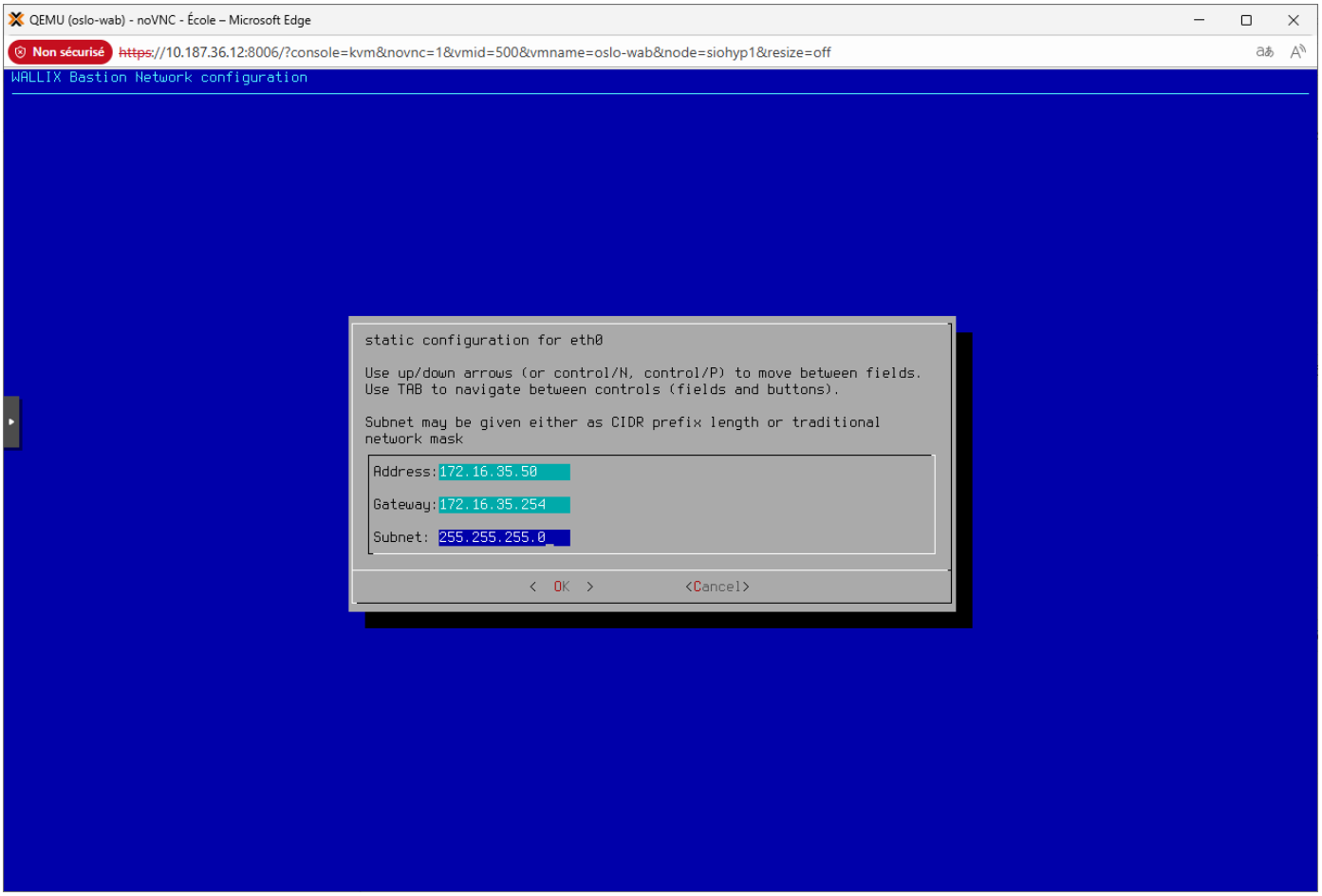
Définir le mot de passe du compte **wabupgrade** ⇒ P@$$w0rd2025Secure


QEMU (oslo-wab) - noVNC - École – Microsoft Edge
Non sécurisé
https://10.187.36.12:8006/?console=kvm&novnc=1&vmid=500&vmname=oslo-wab&node=siohyp1&resize=off
WALLIX Bastion Initial configuration
Password changed for user wabupgrade
< OK >

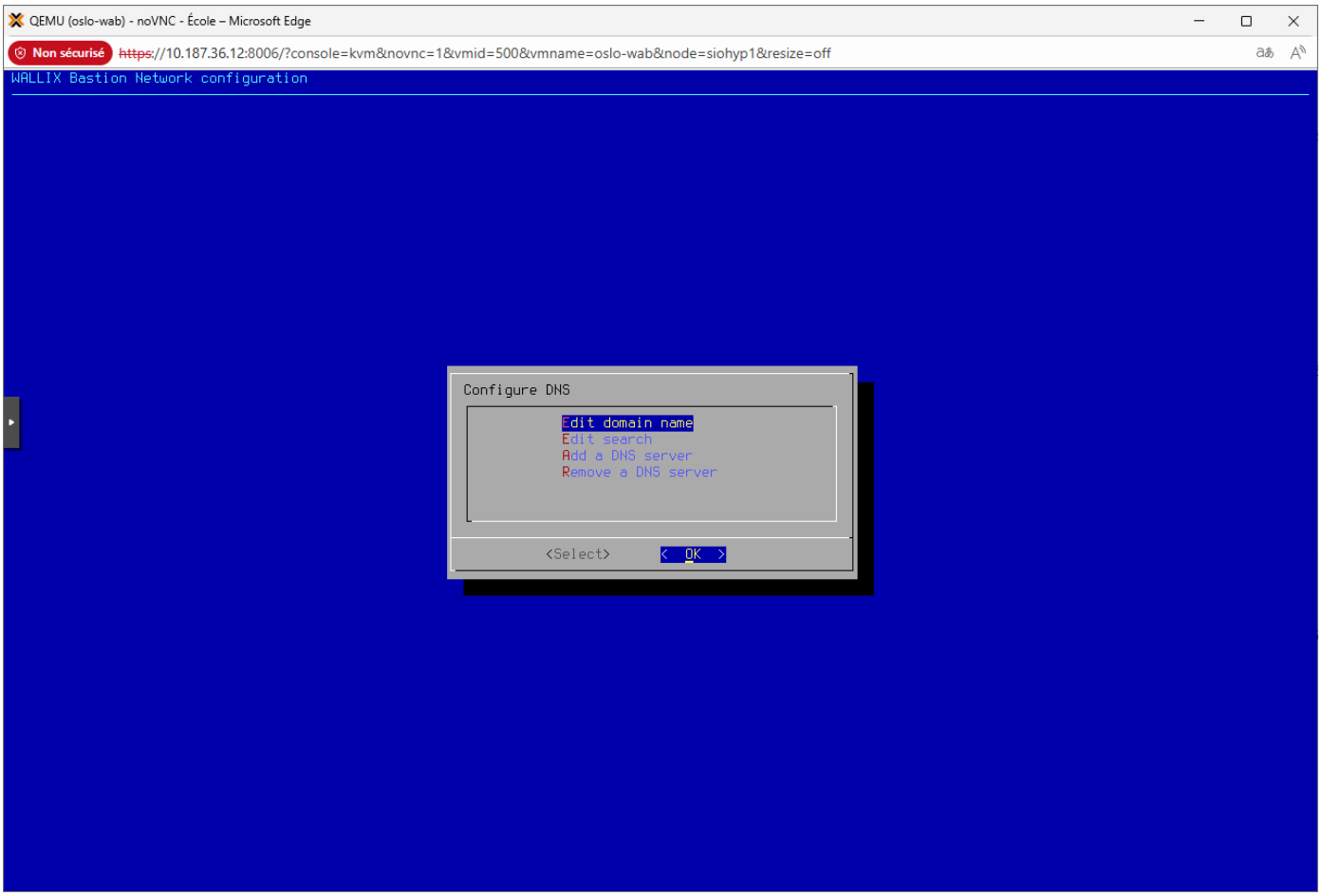

QEMU (oslo-wab) - noVNC - École – Microsoft Edge
Non sécurisé
https://10.187.36.12:8006/?console=kvm&novnc=1&vmid=500&vmname=oslo-wab&node=siohyp1&resize=off
WALLIX Bastion Initial configuration
Do you want to configure
WALLIX Bastion network?
< Yes >
< No >

Configuration réseau du Bastion

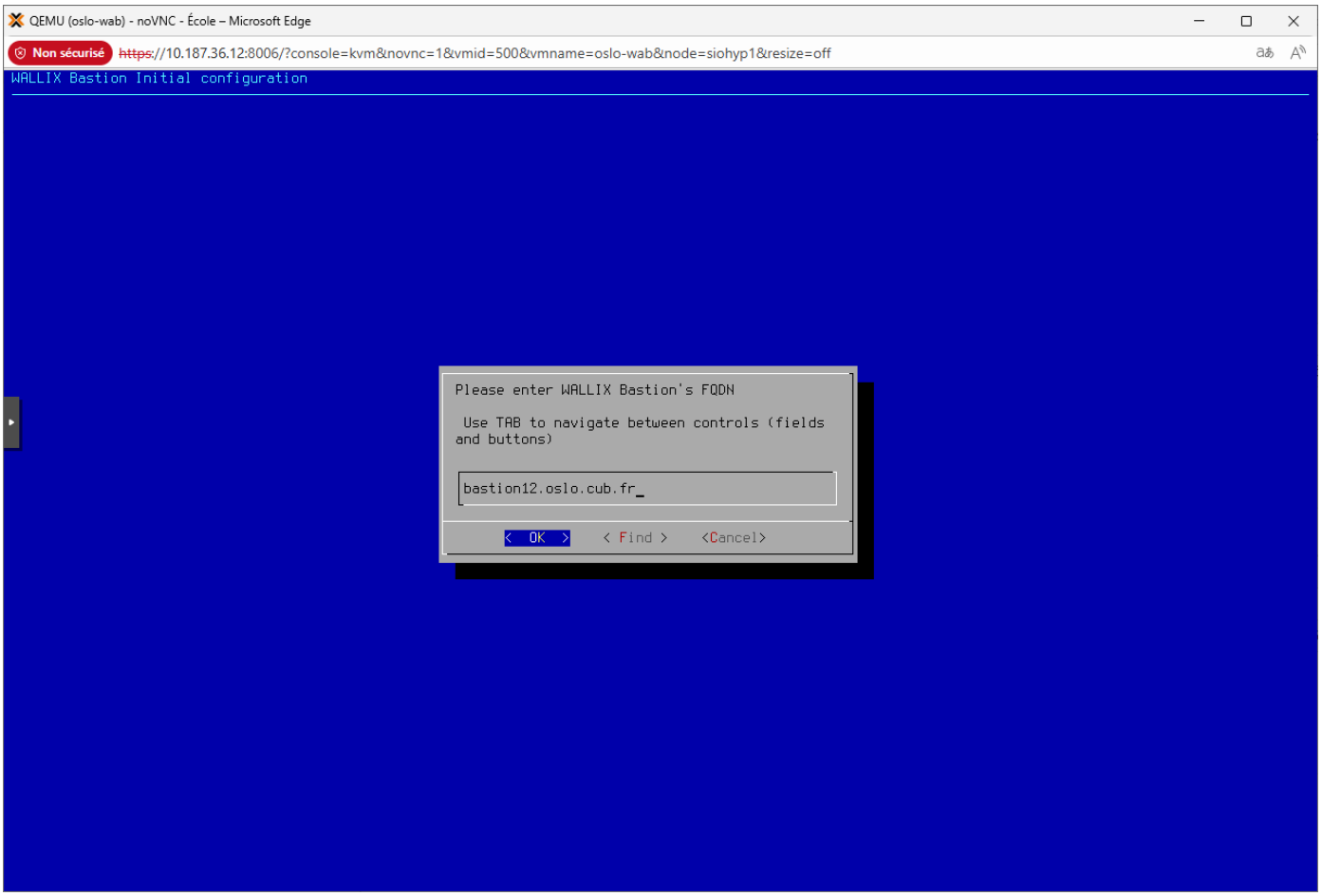
Définition du hostname

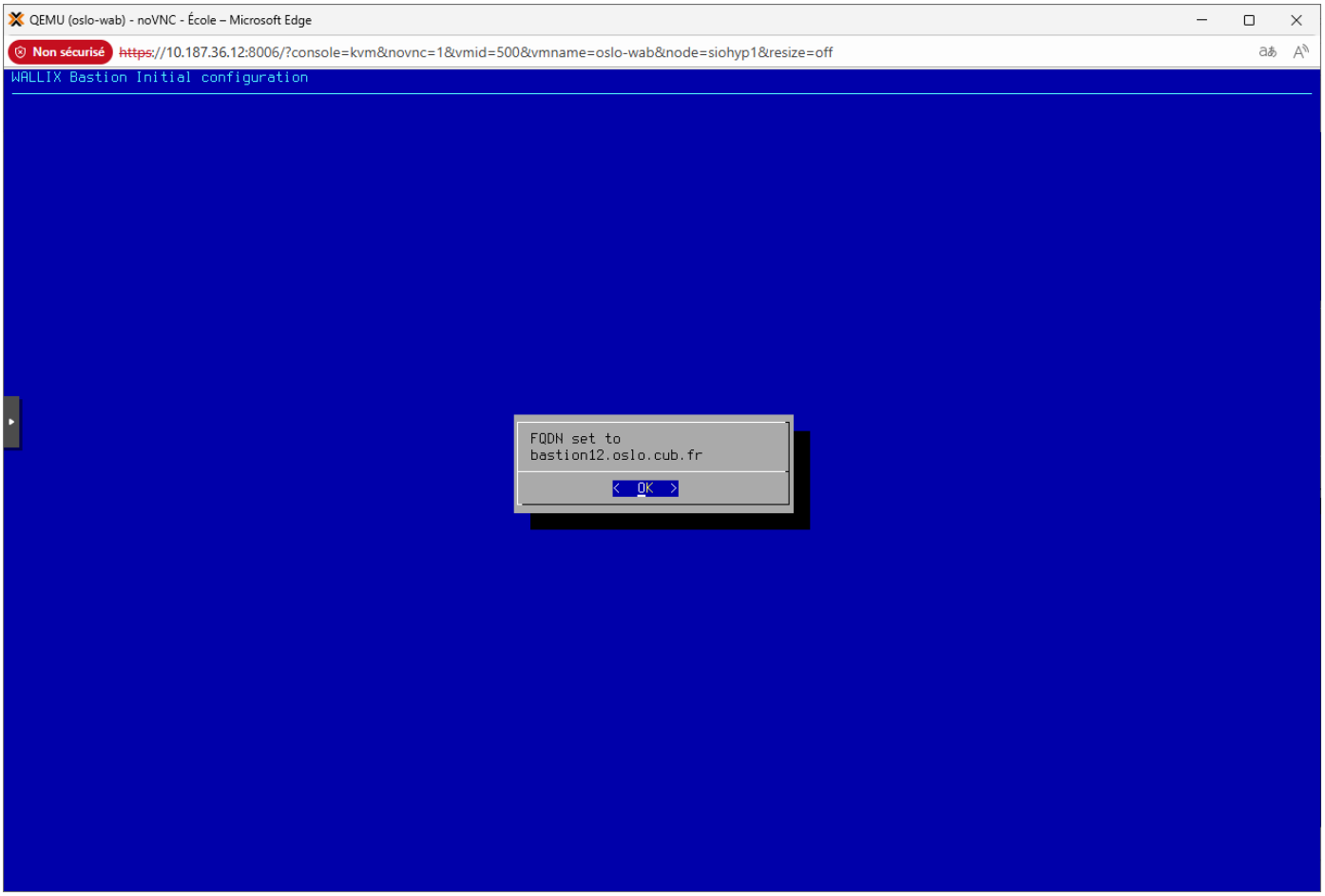


Définition du DNS

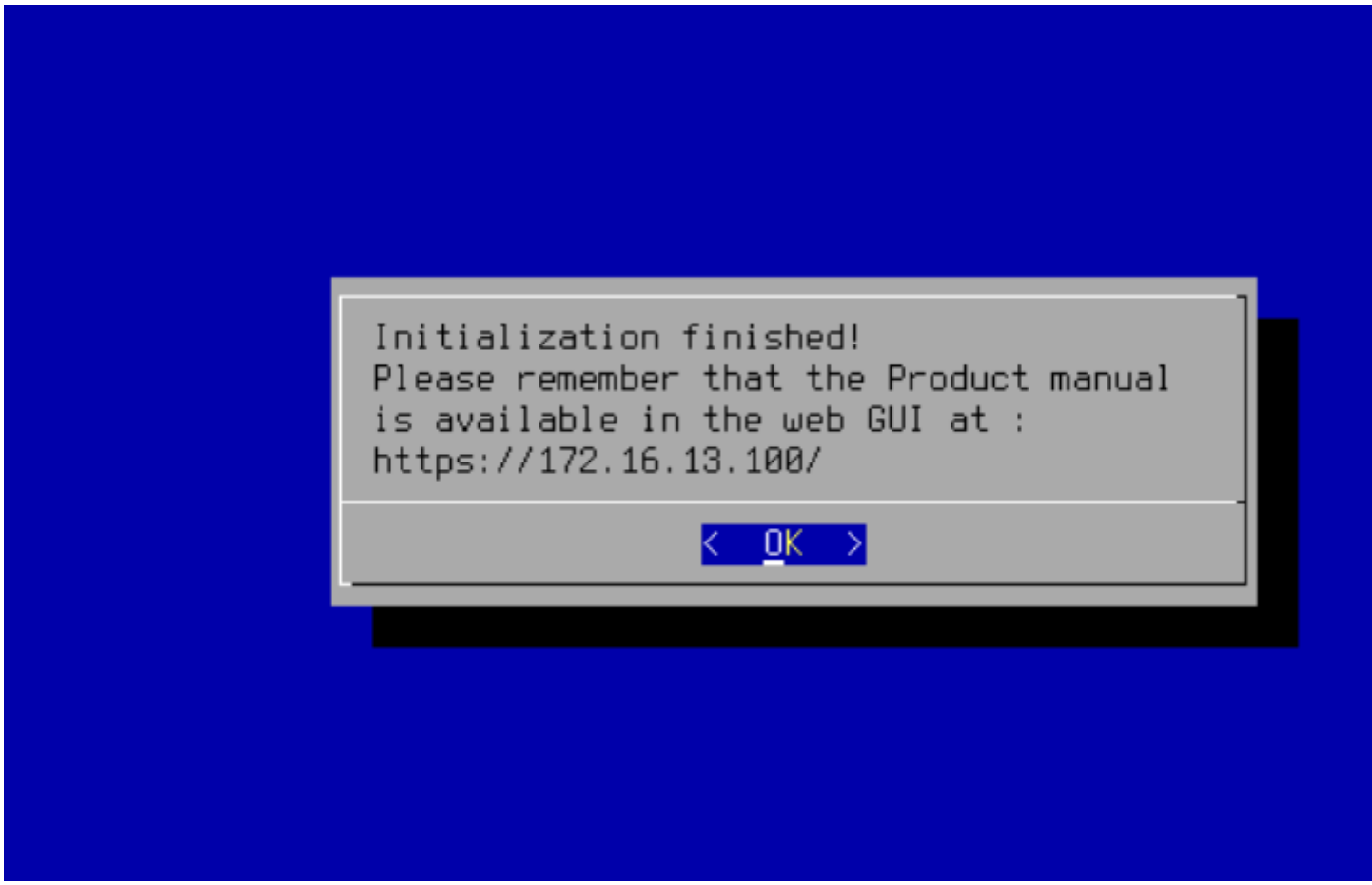


Définition du FQDN

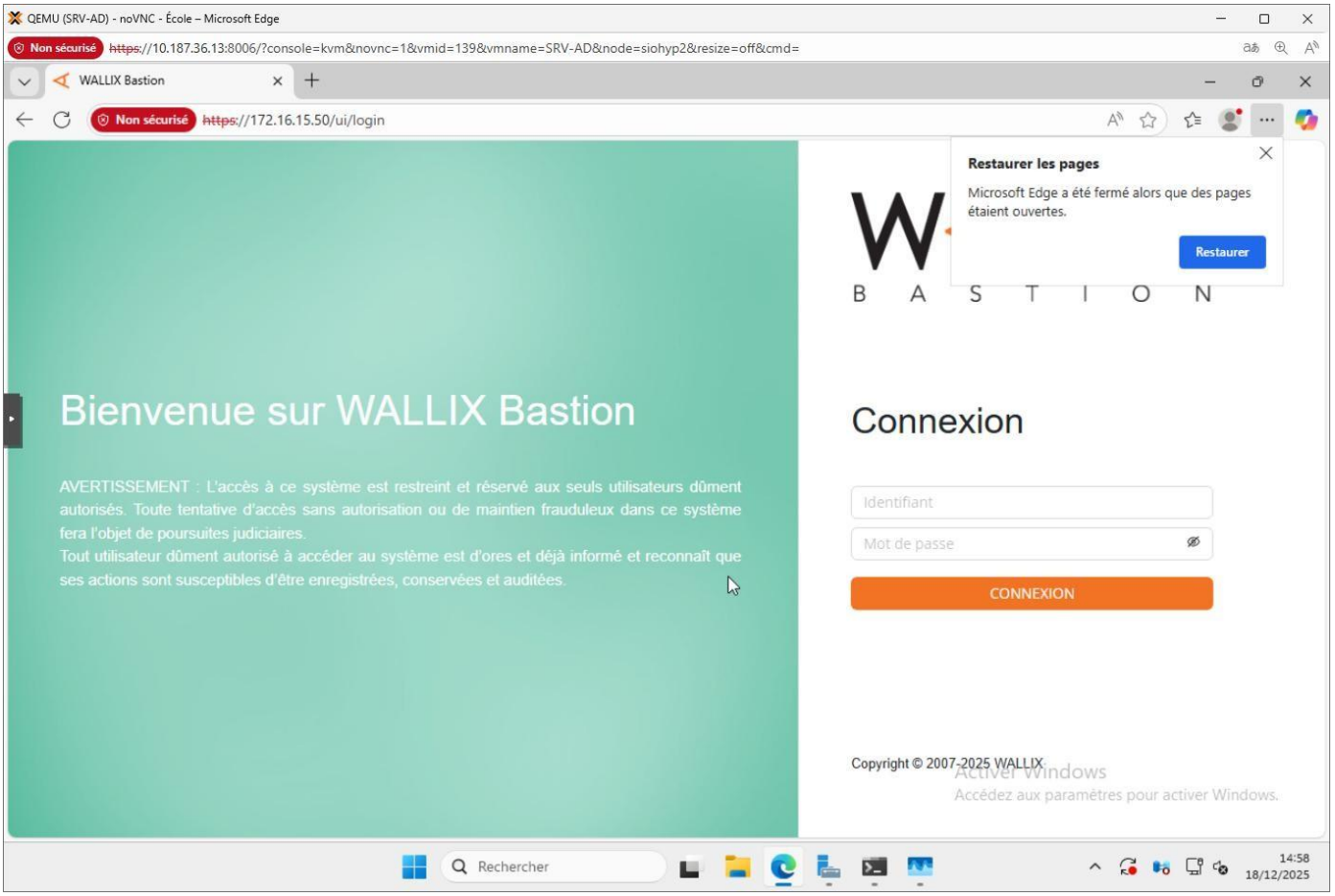


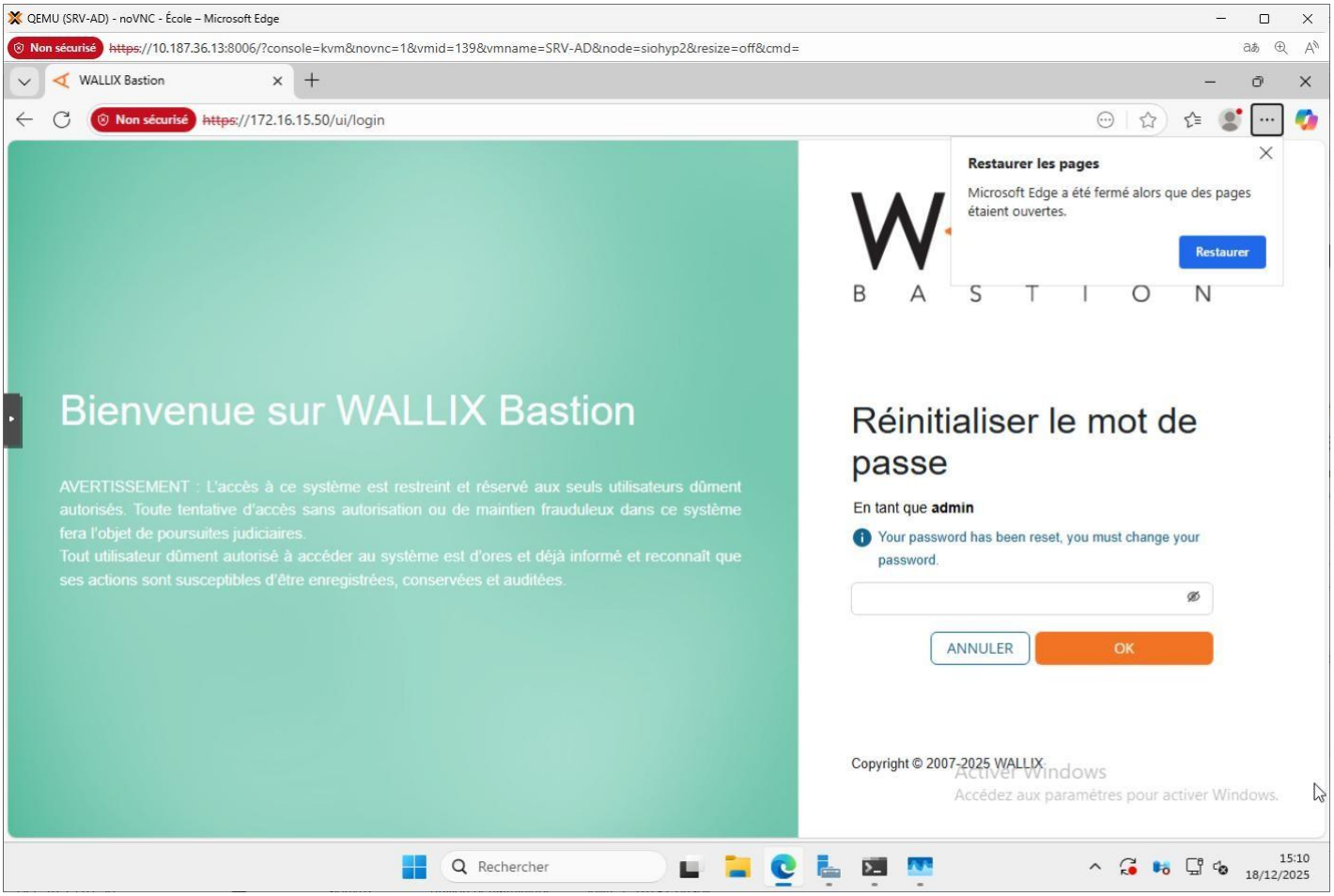

QEMU (oslo-wab) - noVNC - École – Microsoft Edge
Non sécurisé
https://10.187.36.12:8006/?console=kvm&novnc=1&vmid=500&vmname=oslo-wab&node=siohyp1&resize=off
WALLIX Bastion Initial configuration
FQDN set to
bastion12.oslo.cub.fr
< OK >

Fin de la 1re partie de l'installation

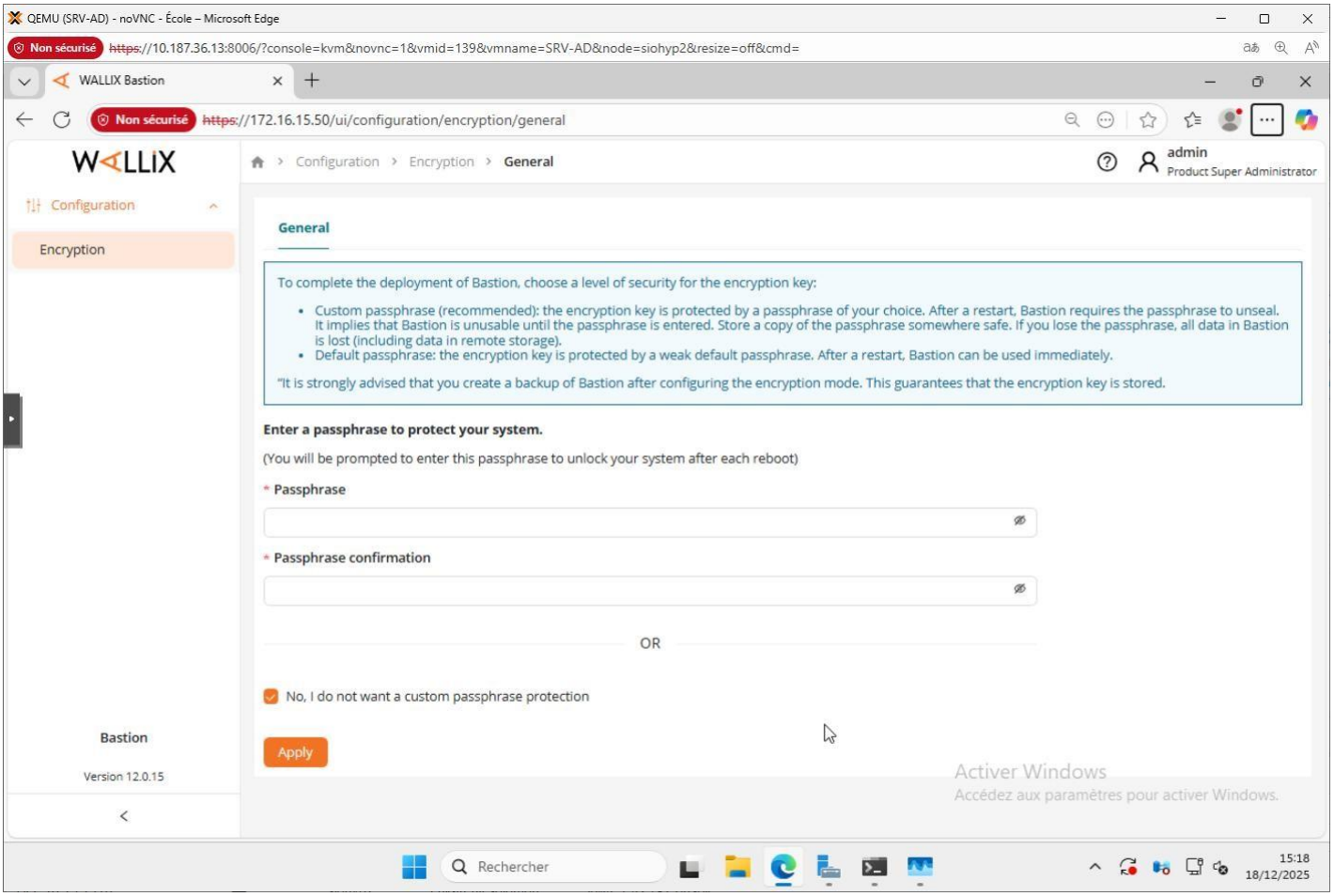


Saisir le mot de passe par défaut **admin** du compte **admin**


QEMU (SRV-AD) - noVNC - École – Microsoft Edge
Non sécurisé https://10.187.36.13:8006/?console=kvm&novnc=1&vmid=139&vmname=SRV-AD&node=siohyp2&resize=off&cmd=
WALLIX Bastion
Non sécurisé https://172.16.15.50/ui/login
Restaurer les pages
Microsoft Edge a été fermé alors que des pages étaient ouvertes.
Restaurer
B A S T I O N
Bienvenue sur WALLIX Bastion
AVERTISSEMENT : L'accès à ce système est restreint et réservé aux seuls utilisateurs dûment autorisés. Toute tentative d'accès sans autorisation ou de maintien frauduleux dans ce système fera l'objet de poursuites judiciaires.
Tout utilisateur dûment autorisé à accéder au système est d'ores et déjà informé et reconnaît que ses actions sont susceptibles d'être enregistrées, conservées et auditées.
Connexion
Identifiant
Mot de passe
CONNEXION
Copyright © 2007-2025 WALLIX
Activer Windows
Accédez aux paramètres pour activer Windows.
Rechercher
14:58
18/12/2025



Définir le mot de passe du compte **admin** ⇒ P@$$w0rd2025Secure



- Ne pas saisir de passphrase
  - https://wallix.groupevalophis.fr/webhelp/fr/Bastion-user-guide/index.html#id-sect-ssh_putty.html
  - https://github.com/wallix/WALLIX-PuTTY/releases
  -

Retour :

- Retour à la Documentation Technique

Supervision avec Zabbix 7.4 (Debian 12 + Apache2 + MariaDB + Agent2)

Présentation

Serveur Zabbix

- Frontend web (Apache2 + PHP)
- Base de données MariaDB
- Agent Zabbix 2

1. Pré-requis

Système :

Debian 12 à jour
- Accès root
- Connexion Internet

Mise à jour du système et installation des packages nécessaires :

apt update && apt upgrade -y
apt install wget curl gnupg2 lsb-release unzip locales -y

Installation d'Apache2 et MariaDB :

apt install apache2 mariadb-server mariadb-client -y
systemctl enable apache2 --now
systemctl enable mariadb --now

2. Sécurisation de MariaDB

Exécuter l'assistant de sécurisation :

mysql_secure_installation

Réponses recommandées :

Définir mot de passe root : **Yes**
- Supprimer utilisateurs anonymes : **Yes**
- Désactiver accès root distant : **Yes**
- Supprimer base de test : **Yes**
- Recharger privilèges : **Yes**
- Unix_socket authentication : **No**
  → nécessaire pour se connecter via mot de passe dans Zabbix.

3. Création de la base et de l'utilisateur Zabbix

Connexion à MariaDB :

mysql -u root -p

Création de la base et de l'utilisateur :

CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'MotDePasseFort';
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
FLUSH PRIVILEGES;
EXIT;

Problème rencontré :
Access denied for user 'zabbix'@'localhost'
Cause : utilisateur mal créé
Solution : recréer l'utilisateur avec les droits complets.

4. Ajout du dépôt Zabbix

Les URLs initiales donnaient une erreur 404.
Paquet correct pour Debian 12 :

wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_7.4-0.1+debian12_all.deb
dpkg -i zabbix-release_7.4-0.1+debian12_all.deb
apt update

5. Installation de Zabbix server, frontend et agent

apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent2 -y

Remarque :
Zabbix Agent 2 est privilégié → plus moderne, modulaire et compatible avec les plugins officiels.

6. Initialisation de la base de données Zabbix

Importer le schéma :

zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | mysql -u zabbix -p zabbix

Vérifier la création des tables :

mysql -u zabbix -p zabbix -e "SHOW TABLES;"

Problème rencontré :
Chemin SQL différent selon version.
Chemin correct Debian 12 :

/usr/share/zabbix/sql-scripts/mysql/server.sql.gz

7. Configuration de Zabbix server

Éditer le fichier :

/etc/zabbix/zabbix_server.conf

Paramètres essentiels :

DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=MotDePasseFort

8. Configuration des locales pour le frontend

Problème constaté :

Locale for language “en_US” is not found on the web server.

Solution : génération des locales :

dpkg-reconfigure locales

Cocher :

en_US.UTF-8 UTF-8

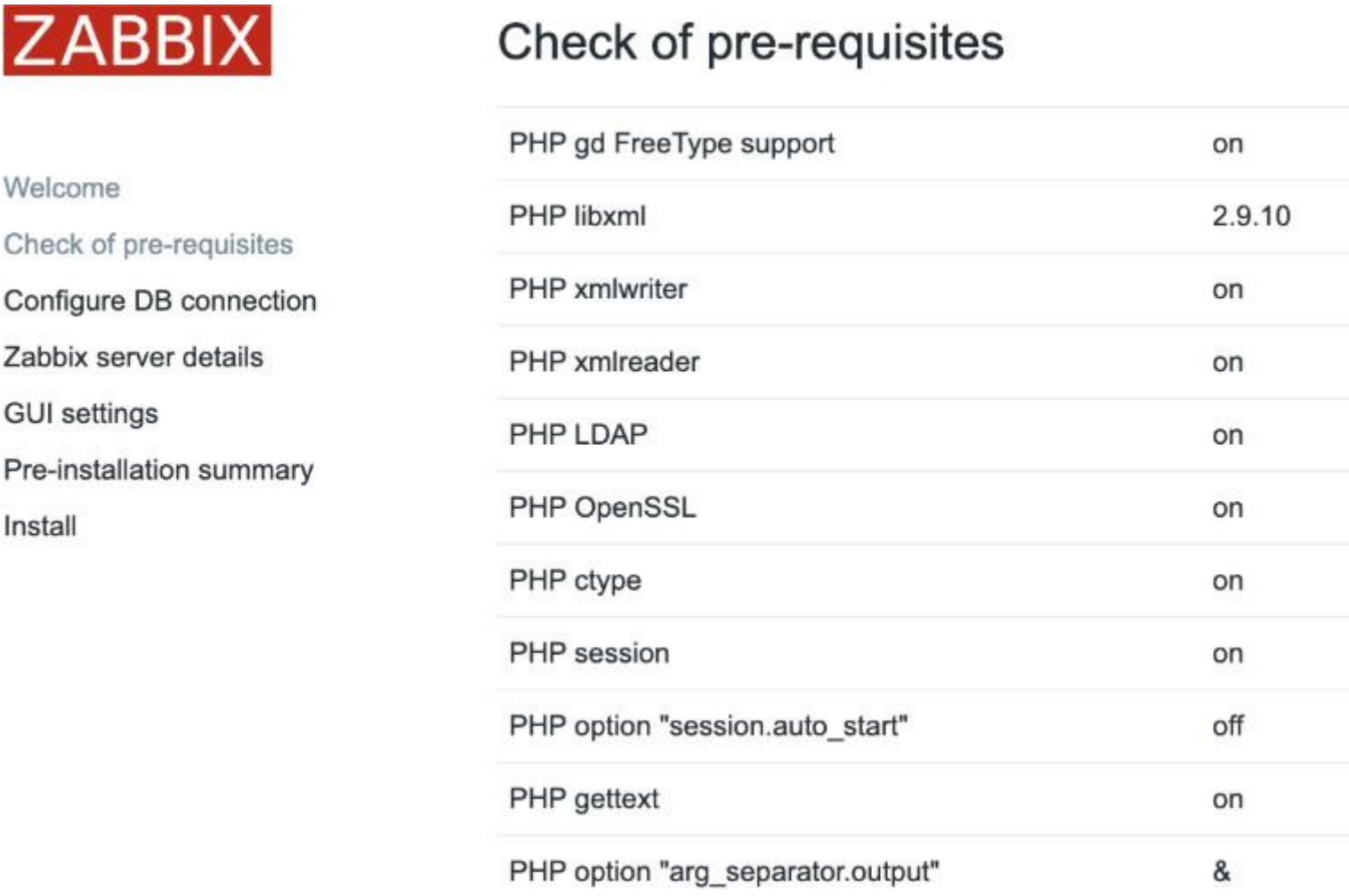
Puis définir en_US.UTF-8 comme locale par défaut.

Vérification :

locale -a | grep en_US

Configurer Apache pour utiliser cette locale :

```
echo 'export LANG=en_US.UTF-8' >> /etc/apache2/envvars
echo 'export LANGUAGE=en_US:en' >> /etc/apache2/envvars
echo 'export LC_ALL=en_US.UTF-8' >> /etc/apache2/envvars
systemctl restart apache2
```



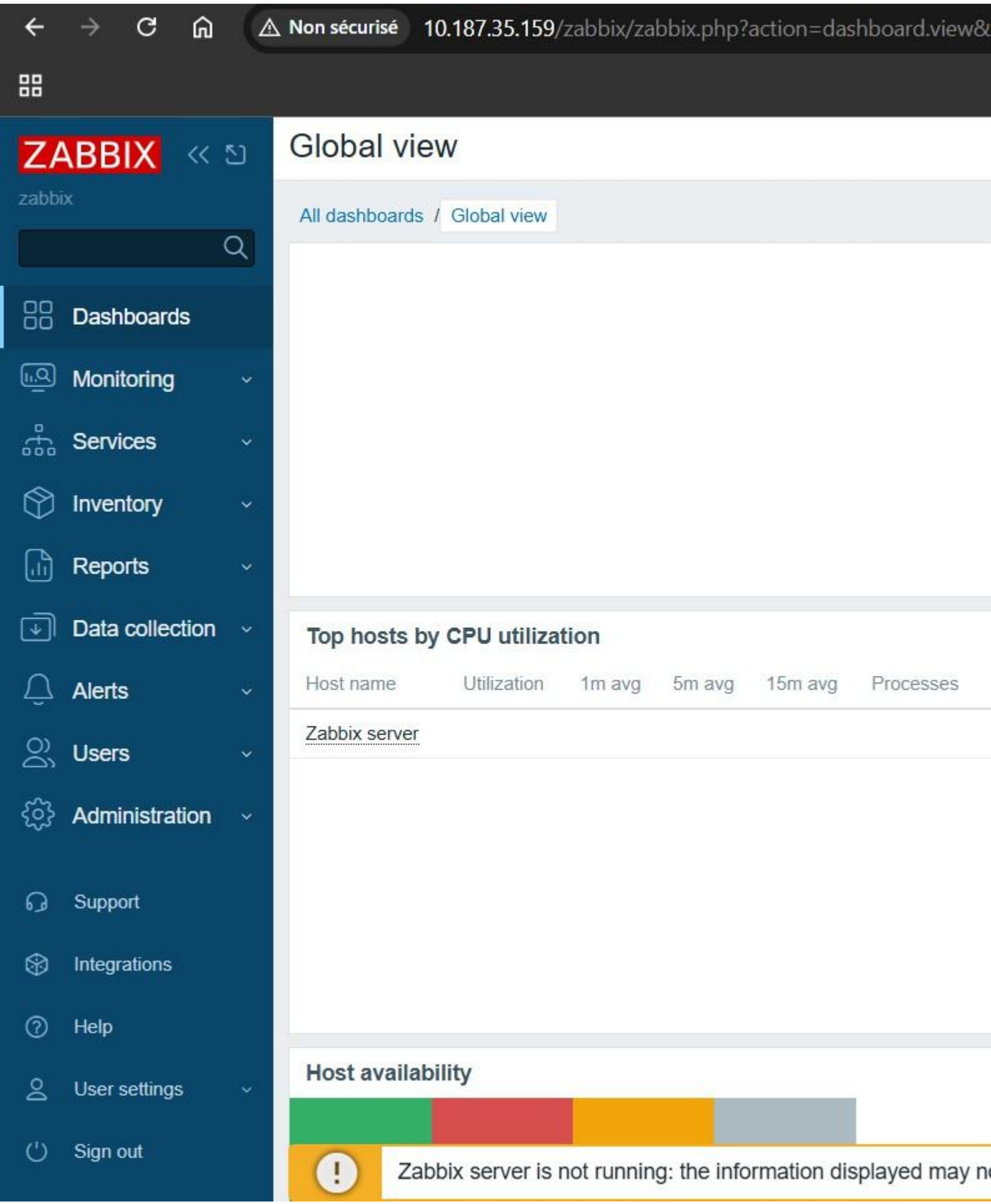
6. Configuration PHP pour le frontend Zabbix

Modifier :

/etc/php/*/apache2/php.ini

Valeurs recommandées :

date.timezone =*



Par défaut: L'identifiant: Admin et le MDP: zabbix

Création agent Zabbix 7.4 :

1 - Installez et configurez Zabbix

Installez le dépôt Zabbix.

```
# wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb
# dpkg -i zabbix-release_latest_7.4+debian12_all.deb
# apt update
```

Installer l'Agent Zabbix

```
apt install zabbix-agent2
```

Configuration de l'agent

```
nano /etc/zabbix/zabbix_agent2.conf
```

Modifier les lignes suivantes:

```
Server=IP_DU_SERVEUR_ZABBIX
ServerActive=IP_DU_SERVEUR_ZABBIX
Hostname=nom_de_la_machine
```

Activer puis redémarrer:

```
systemctl enable zabbix-agent2
systemctl start zabbix-agent2
systemctl status zabbix-agent2
```

Retour :

Retour à la Documentation Technique

Réplication de bases de données

1 - Installer Mariadb sur 2 serveurs Debian :

Après mise en place des 2 conteneurs (**ServeurA** et **ServeurB**) :

Mettre à jour et installer MariaDB :

```
apt update
apt install -y mariadb-server mariadb-client -y
```

Activer et démarrer le service :

```
root@ServeurA:~# systemctl enable --now mariadb
Synchronizing state of mariadb.service with SysV service script with /li
Executing: /lib/systemd/systemd-sysv-install enable mariadb
```

Vérifier l'état de Mariadb :

```
root@ServeurA:~# systemctl status mariadb
* mariadb.service - MariaDB 10.11.14 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; prese
     Active: active (running) since Thu 2025-12-04 10:31:29 UTC; 50s ago
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
   Main PID: 1407 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 12 (limit: 1015189)
     Memory: 80.9M
        CPU: 760ms
     CGroup: /system.slice/mariadb.service
             `-1407 /usr/sbin/mariadbd

Dec 04 10:31:29 ServeurA mariadbd[1407]: 2025-12-04 10:31:29 0 [Note] In
Dec 04 10:31:29 ServeurA mariadbd[1407]: 2025-12-04 10:31:29 0 [Note] In
Dec 04 10:31:29 ServeurA mariadbd[1407]: 2025-12-04 10:31:29 0 [Note] In
Dec 04 10:31:29 ServeurA mariadbd[1407]: 2025-12-04 10:31:29 0 [Note] Pl
Dec 04 10:31:29 ServeurA mariadbd[1407]: 2025-12-04 10:31:29 0 [Note] In
Dec 04 10:31:29 ServeurA mariadbd[1407]: 2025-12-04 10:31:29 0 [Warning]
Dec 04 10:31:29 ServeurA mariadbd[1407]: 2025-12-04 10:31:29 0 [Note] Se
Dec 04 10:31:29 ServeurA mariadbd[1407]: 2025-12-04 10:31:29 0 [Note] /u
Dec 04 10:31:29 ServeurA mariadbd[1407]: Version: '10.11.14-MariaDB-0+de
Dec 04 10:31:29 ServeurA systemd[1]: Started mariadb.service - MariaDB 1
```

Vérifier la version et connexion locale :

```
root@ServeurA:~# mariadb --version
mariadb  Ver 15.1 Distrib 10.11.14-MariaDB, for debian-linux-gnu (x86_64
```

test rapide :

```
root@ServeurA:~# mysql -u root -e "SELECT VERSION(), CURRENT_USER();"
+----------------------------+----------------+
| VERSION()                  | CURRENT_USER() |
+----------------------------+----------------+
| 10.11.14-MariaDB-0+deb12u2 | root@localhost |
+----------------------------+----------------+
```

Sécuriser l'installation :

mysql_secure_installation

Enter current password for root (enter for none): — (appuie sur Entrée)

Switch to unix_socket authentication [Y/n] — y

Change the root password? [Y/n] — y (mdp : **adminsql**)

Remove anonymous users? [Y/n] — y

Disallow root login remotely? [Y/n] — y

Remove test database and access to it? [Y/n] — y

Reload privilege tables now? [Y/n] — y

Vérifier qu'on peut se connecter :

Configuration du serveur Maitre (10.187.35.245) :

Dans le fichier de configuration **/etc/mysql/mariadb.conf.d/50-server.cnf** :

```
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
[mysqld]

server-id            = 1
log_bin              = /var/log/mysql/mysql-bin.log
binlog_do_db         = testdb

user                = mysql
pid-file             = /run/mysqld/mysqld.pid
socket               = /run/mysqld/mysqld.sock
basedir              = /usr
datadir              = /var/lib/mysql
tmpdir               = /tmp
lc-messages-dir      = /usr/share/mysql

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address         = 10.187.35.247


#key_buffer_size       = 128M
#max_allowed_packet     = 1G
#thread_stack          = 192K
#thread_cache_size      = 8
#myisam_recover_options = BACKUP
#max_connections        = 100
#table_cache           = 64
```

```
# $ sudo mkdir -m 2750 /var/log/mysql
# $ sudo chown mysql /var/log/mysql

#general_log_file       = /var/log/mysql/mysql.log
#general_log            = 1

# /etc/mysql/conf.d/mariadb.conf.d/50-mysqld_safe.cnf
#log_error = /var/log/mysql/error.log
#log_slow_query_file     = /var/log/mysql/mariadb-slow.log
#log_slow_query_time     = 10
#log_slow_verbosity      = query_plan,explain
#log-queries-not-using-indexes
#log_slow_min_examined_row_limit = 1000

#server-id              = 1
#log_bin                = /var/log/mysql/mysql-bin.log
expire_logs_days        = 10
#max_binlog_size        = 100M


#ssl-ca = /etc/mysql/cacert.pem
#ssl-cert = /etc/mysql/server-cert.pem
#ssl-key = /etc/mysql/server-key.pem
#require-secure-transport = on

character-set-server  = utf8mb4
collation-server      = utf8mb4_general_ci


# InnoDB is enabled by default with a 10MB datafile in /var/lib/mysql/.
#innodb_buffer_pool_size = 8G

# this is only for embedded server
[embedded]

# This group is only read by MariaDB servers, not by MySQL.
# If you use the same .cnf file for MySQL and MariaDB,
# you can put MariaDB-only options here
[mariadb]

# This group is only read by MariaDB-10.11 servers.
# If you use the same .cnf file for MariaDB of different versions,
# use this group for options that older servers don't understand
[mariadb-10.11]
```

(Note : bind-address souvent périmé, à mettre à jour)

On redémarre les services MariaDB :

```
#systemctl restart mariadb.service
```

Une fois les services redémarrés, on configure les accès pour que le serveur Esclave puisse se connecter :

```
#mysql -u root -p
MariaDB [(none)]> CREATE USER 'replication_user'@'ip_esclave' IDENTIFIED BY 'mdp';
MariaDB [(none)]> GRANT REPLICATION SLAVE ON *.* TO 'replication_user'@'ip_esclave';
MariaDB [(none)]> SHOW MASTER STATUS;
```

```
MariaDB [(none)]> SHOW MASTER STATUS;
+------------------+----------+--------------+------------------+
| File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+------------------+----------+--------------+------------------+
| mysql-bin.000001 |      328 | testdb       |                  |
+------------------+----------+--------------+------------------+
1 row in set (0.000 sec)
```

Configuration du serveur Esclave (10.187.35.247) :

Dans le fichier de configuration /etc/mysql/mariadb.conf.d/50-server.cnf :

```
[server]

# this is only for the mysqld standalone daemon
[mysqld]

server-id            = 2
log_bin              = /var/log/mysql/mysql-bin.log
binlog_do_db         = testdb

user                = mysql
pid-file             = /run/mysqld/mysqld.pid
socket               = /run/mysqld/mysqld.sock
basedir              = /usr
datadir              = /var/lib/mysql
tmpdir               = /tmp
lc-messages-dir      = /usr/share/mysql

bind-address         = 10.187.35.245


#key_buffer_size       = 128M
#max_allowed_packet     = 1G
#thread_stack          = 192K
#thread_cache_size      = 8
#myisam_recover_options = BACKUP
#max_connections        = 100
#table_cache           = 64

# $ sudo mkdir -m 2750 /var/log/mysql
# $ sudo chown mysql /var/log/mysql
```

```
#general_log_file       = /var/log/mysql/mysql.log
#general_log            = 1

# /etc/mysql/conf.d/mariadb.conf.d/50-mysqld_safe.cnf
#log_error = /var/log/mysql/error.log
#log_slow_query_file    = /var/log/mysql/mariadb-slow.log
#log_slow_query_time    = 10
#log_slow_verbosity     = query_plan,explain
#log_slow_min_examined_row_limit = 1000

#server-id              = 1
#log_bin                = /var/log/mysql/mysql-bin.log
expire_logs_days        = 10
#max_binlog_size        = 100M


#ssl-ca = /etc/mysql/cacert.pem
#ssl-cert = /etc/mysql/server-cert.pem
#ssl-key = /etc/mysql/server-key.pem
#require-secure-transport = on


character-set-server  = utf8mb4
collation-server      = utf8mb4_general_ci


# https://mariadb.com/kb/en/innodb-system-variables/#innodb_buffer_pool_size
#innodb_buffer_pool_size = 8G

# this is only for embedded server
[embedded]

# This group is only read by MariaDB servers, not by MySQL.
# If you use the same .cnf file for MySQL and MariaDB,
# you can put MariaDB-only options here
[mariadb]

# This group is only read by MariaDB-10.11 servers.
# If you use the same .cnf file for MariaDB of different versions,
# use this group for options that older servers don't understand
[mariadb-10.11]
```

On redémarre les services MariaDB :

```
#systemctl restart mariadb.service
```

Une fois les services redémarrés, on configurer le serveur Esclave avec le serveur Maitre :

```
MariaDB [(none)]> CHANGE MASTER TO
    -> MASTER_HOST='172.16.33.152',
    -> MASTER_USER='repl',
    -> MASTER_PASSWORD='adminsql',
    -> MASTER_LOG_FILE='mysql-bin.000004',
    -> MASTER_LOG_POS=328;
Query OK, 0 rows affected, 1 warning (0.003 sec)

MariaDB [(none)]>
```

Retour :

Retour à la Documentation Technique