Institut Universitaire de Technologie,
Aix-Marseille Université

ANNEXES
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Développement d'une infrastructure de téléphonie IP

Sébastien ICARD

Groupe SNEF

Responsable entreprise : Mathieu MARZULLO

Responsable académique : Roland DEPEYRE

2021

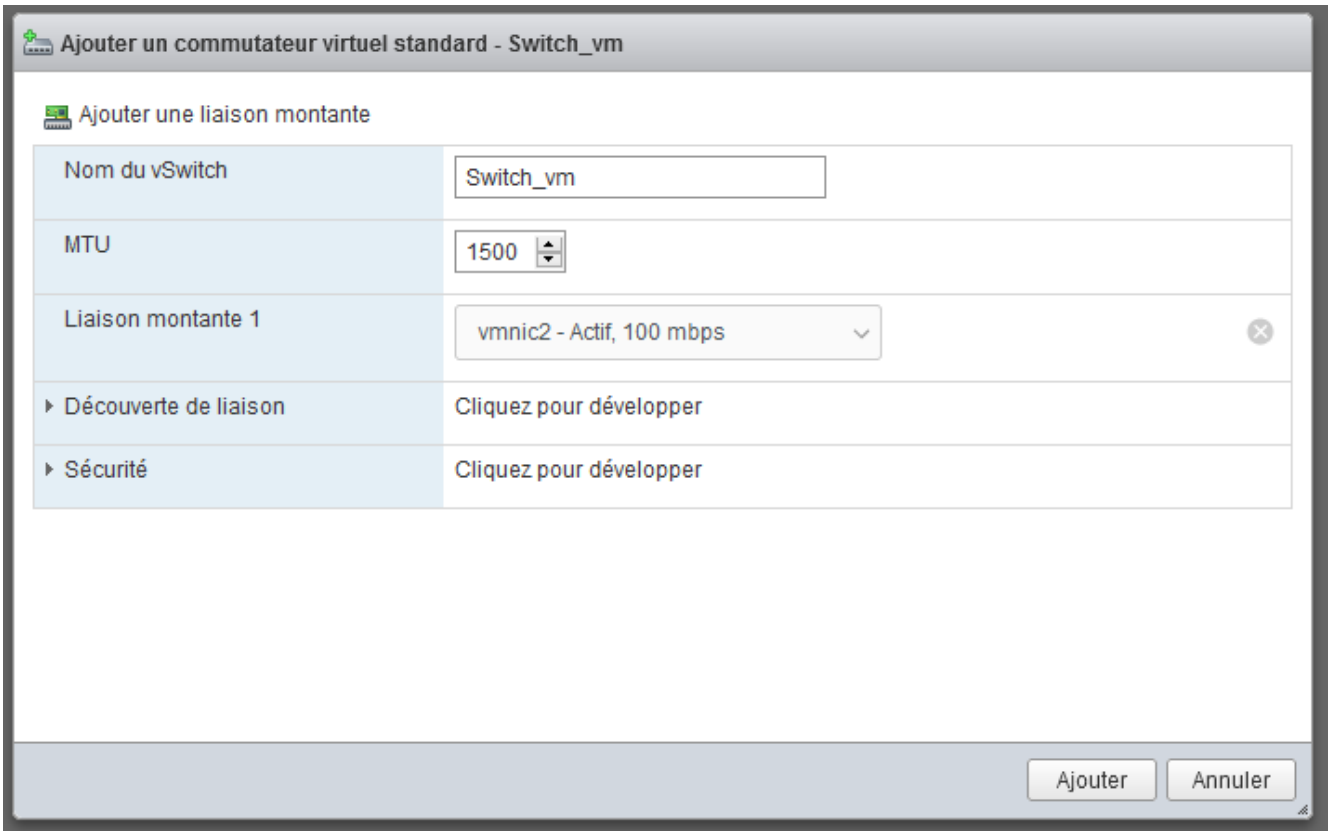
Table des matières

Annexe 1 : Manuel d'installation FreePBX15/Astérisk18

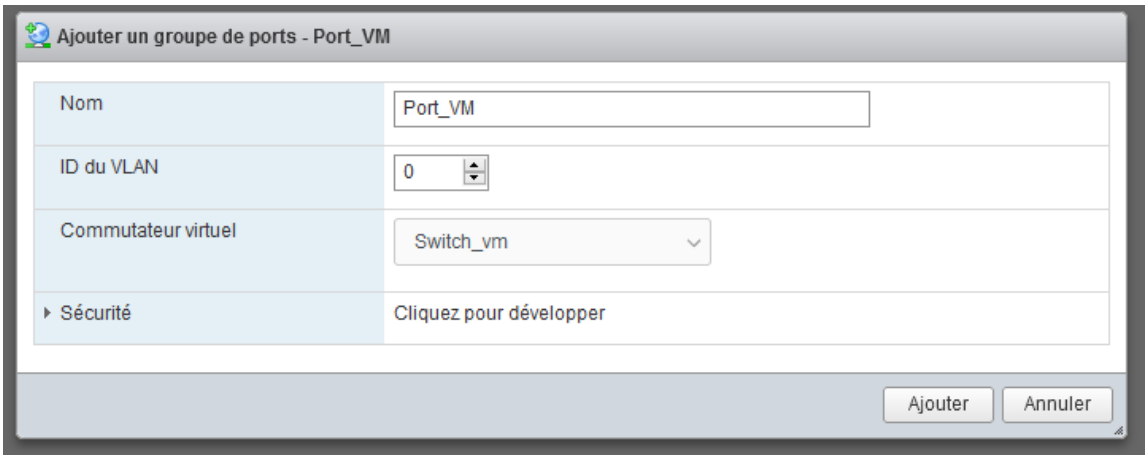
1. Installation d'une VM sur ESXi

1.1. Gestion des réseaux

Après avoir installé l'OS ESXi, se rendre dans : Mise en réseau > Commutateurs virtuels et ajouter un Commutateur Virtuel.

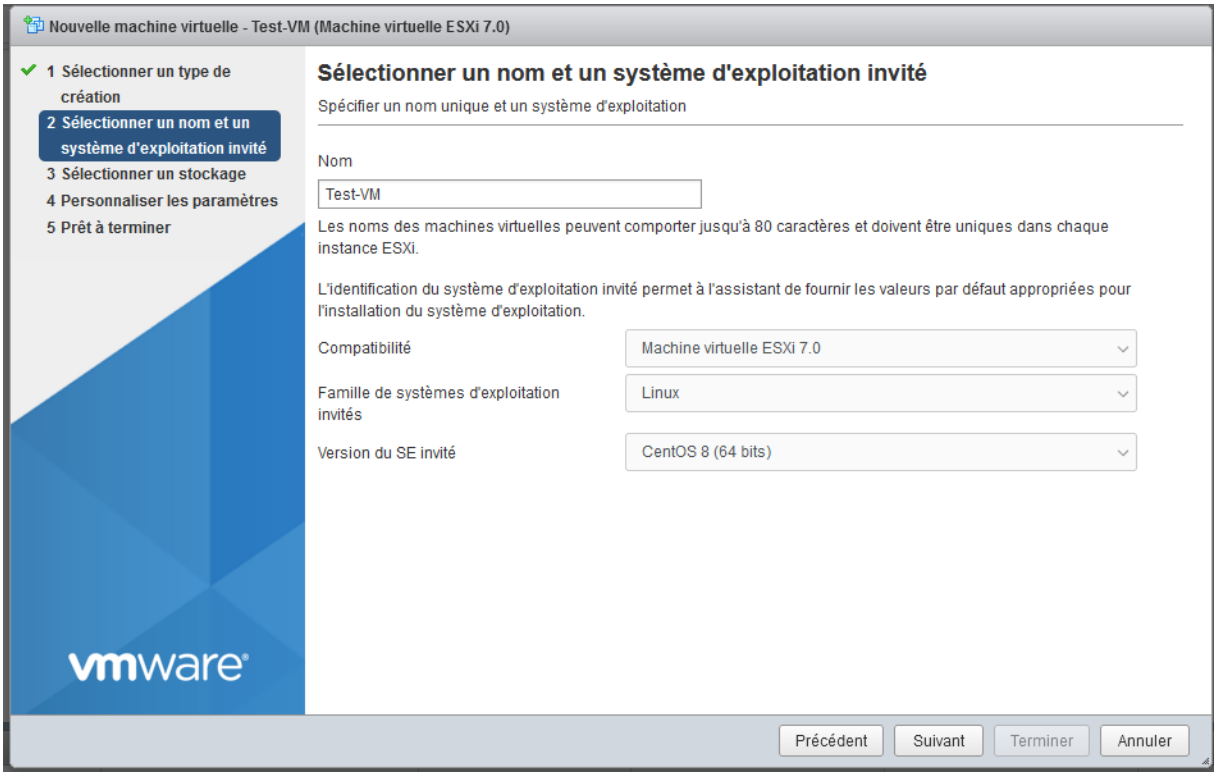


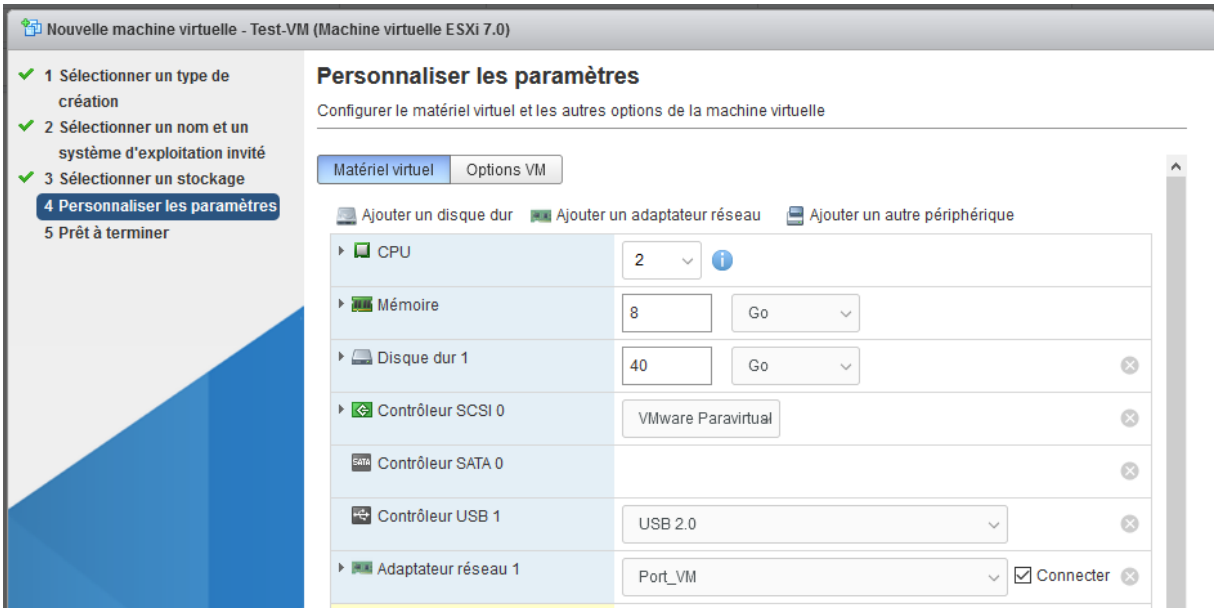
Ensuite se rendre dans Groupe de ports :



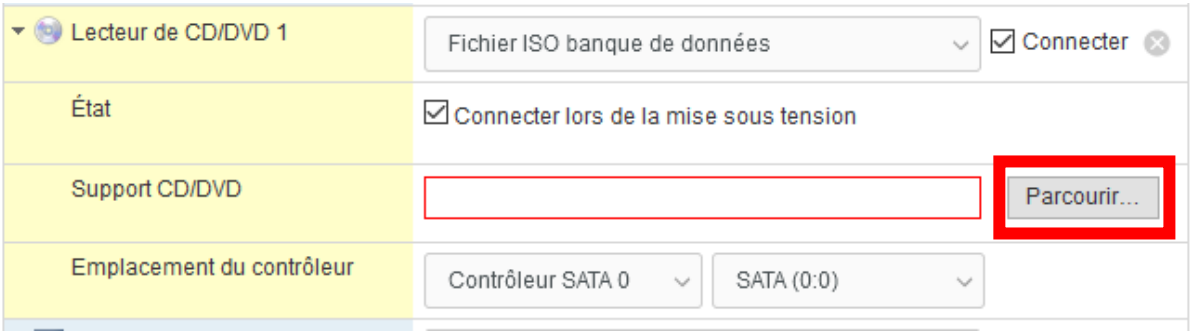
1.2. Création de la Vm

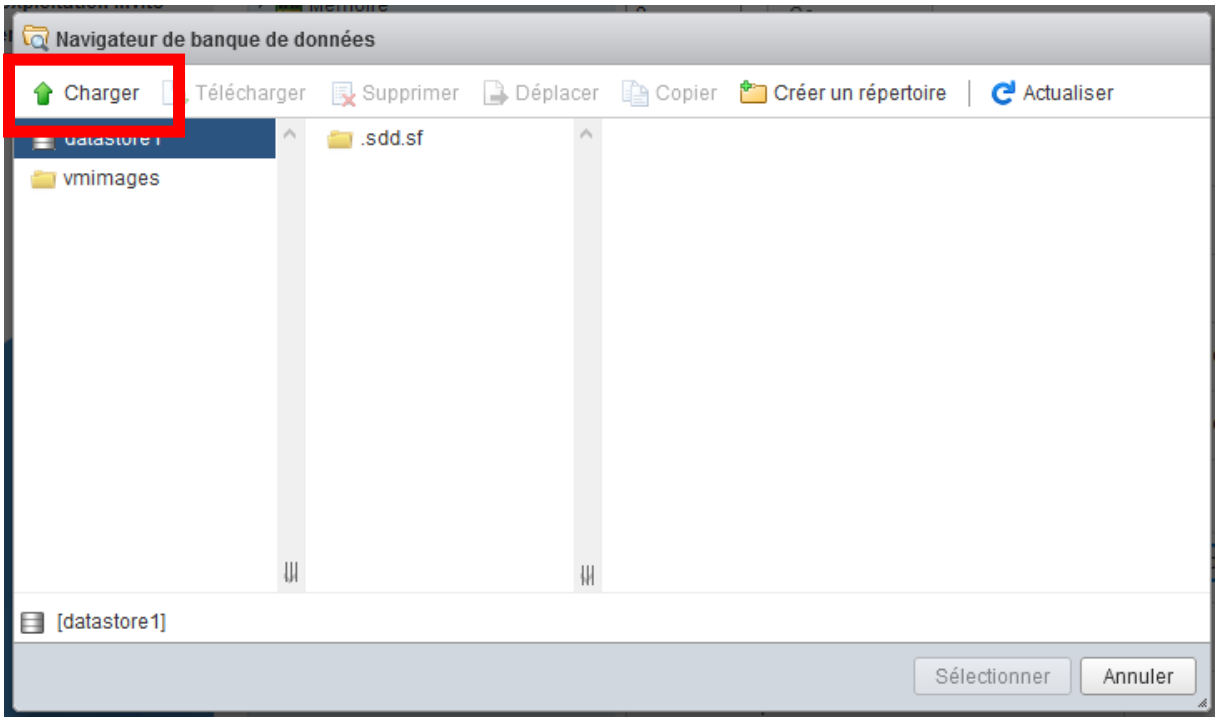
Dans Machines Virtuelles Créer une machine :





Pour insérer l’image iso :





2. Installation Asterisk 18

2.1. Etape 1 : Mettre à jour le système

```
yum -y update
```

Désactiver SELinux :

```
sed -i 's/\(^SELINUX=\).*/\SELINUX=disabled/' /etc/sysconfig/selinux
```

```
sed -i 's/\(^SELINUX=\).*/\SELINUX=disabled/' /etc/selinux/config
```

Ensuite rebooter la machine :

```
reboot
```

Vérifier que SELinux est désactivé avec :

```
sestatus
```

2.2. Etape 2 : Ajouter le Dépôts EPEL

```
yum -y install epel-release
```

```
yum config-manager --set-enabled powertools
```

2.3. Etape 3 : Installer Development Tools

```
yum group -y install "Development Tools"
```

```
yum -y install git wget vim  net-tools sqlite-devel psmisc ncurses-devel libtermcap-devel newt-devel libxml2-devel libtiff-devel gtk2-devel libtool libuuid-devel subversion kernel-devel kernel-devel-$(uname -r) crontabs cronie-anacron libedit libedit-devel
```

2.4. Etape 4 : Télécharger et installer Janson :

```
git clone https://github.com/akheron/jansson.git
```

```
cd jansson
```

```
autoreconf -i
```

```
./configure --prefix=/usr/
```

```
make
```

```
make install
```

2.5. Etape 5 : Télécharger et installer PJSIP

```
cd ~

git clone https://github.com/pjsip/pjproject.git

cd pjproject

./configure CFLAGS="-DNDEBUG -DPJ_HAS_IPV6=1" --prefix=/usr --libdir=/usr/lib64 --enable-shared --disable-video --disable-sound --disable-opencore-amr

make dep

make

make install

ldconfig
```

2.6. Etape 6 : Télécharger et installer Asterisk 18

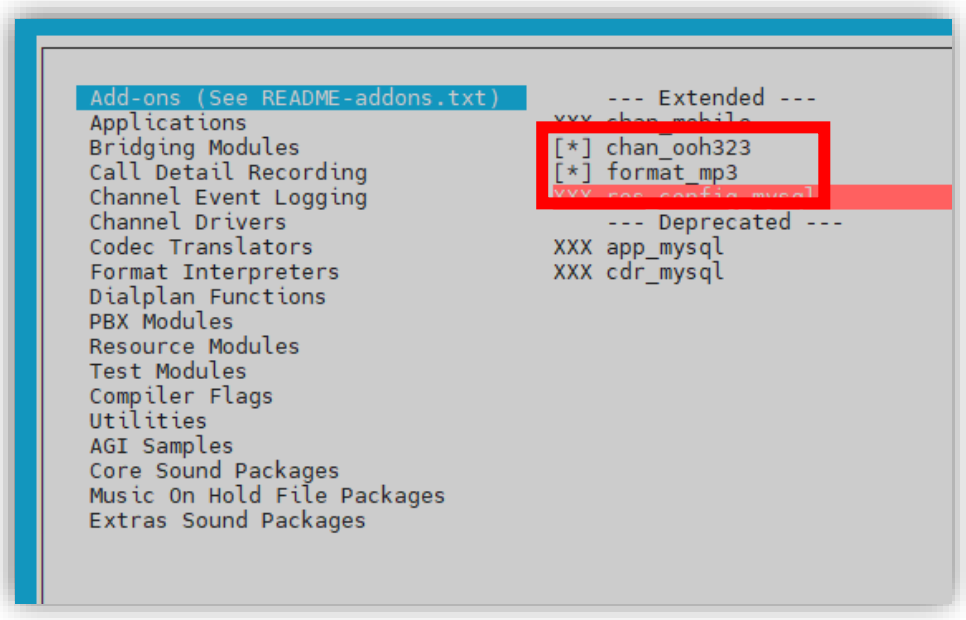
```
cd ~

wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-18-current.tar.gz

tar xvfz asterisk-18-current.tar.gz

cd asterisk-18*/

./configure --libdir=/usr/lib64
```

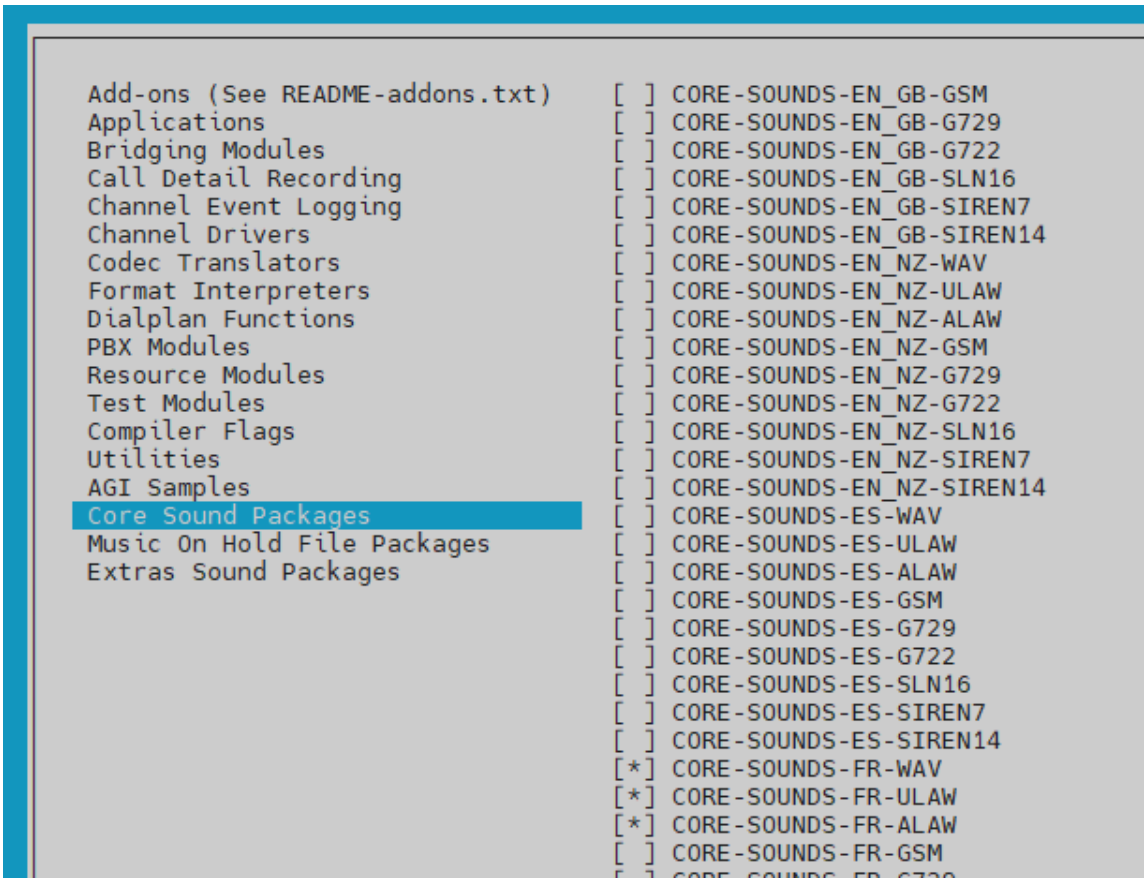
Si tout est bon vous devriez obtenir ceci :

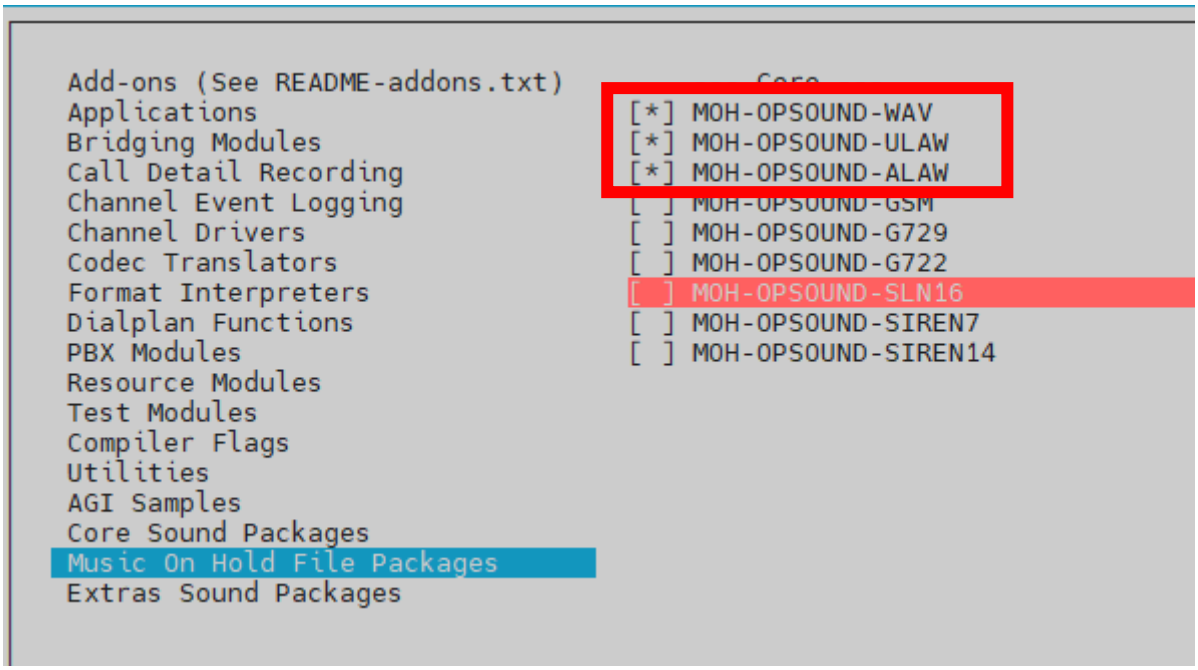
Taper ensuite :

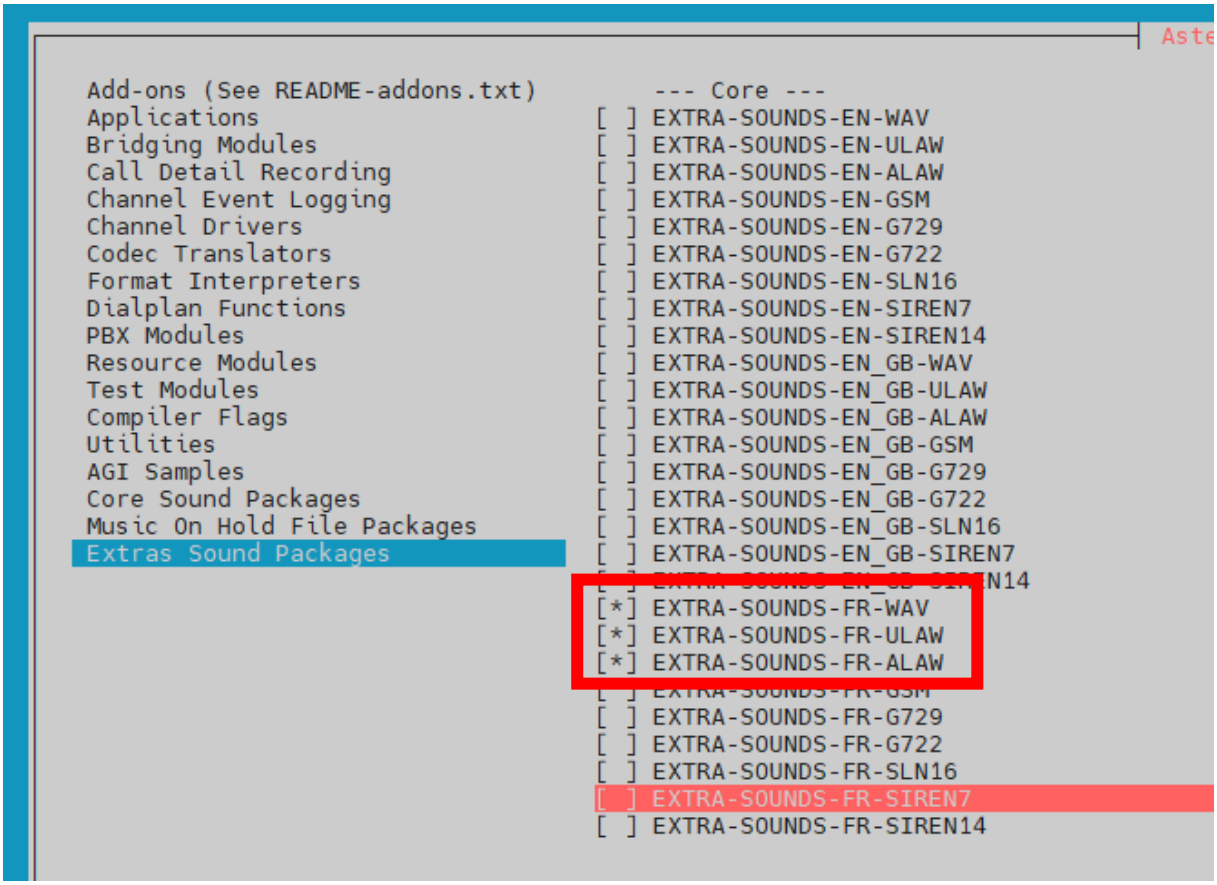
make menuselect

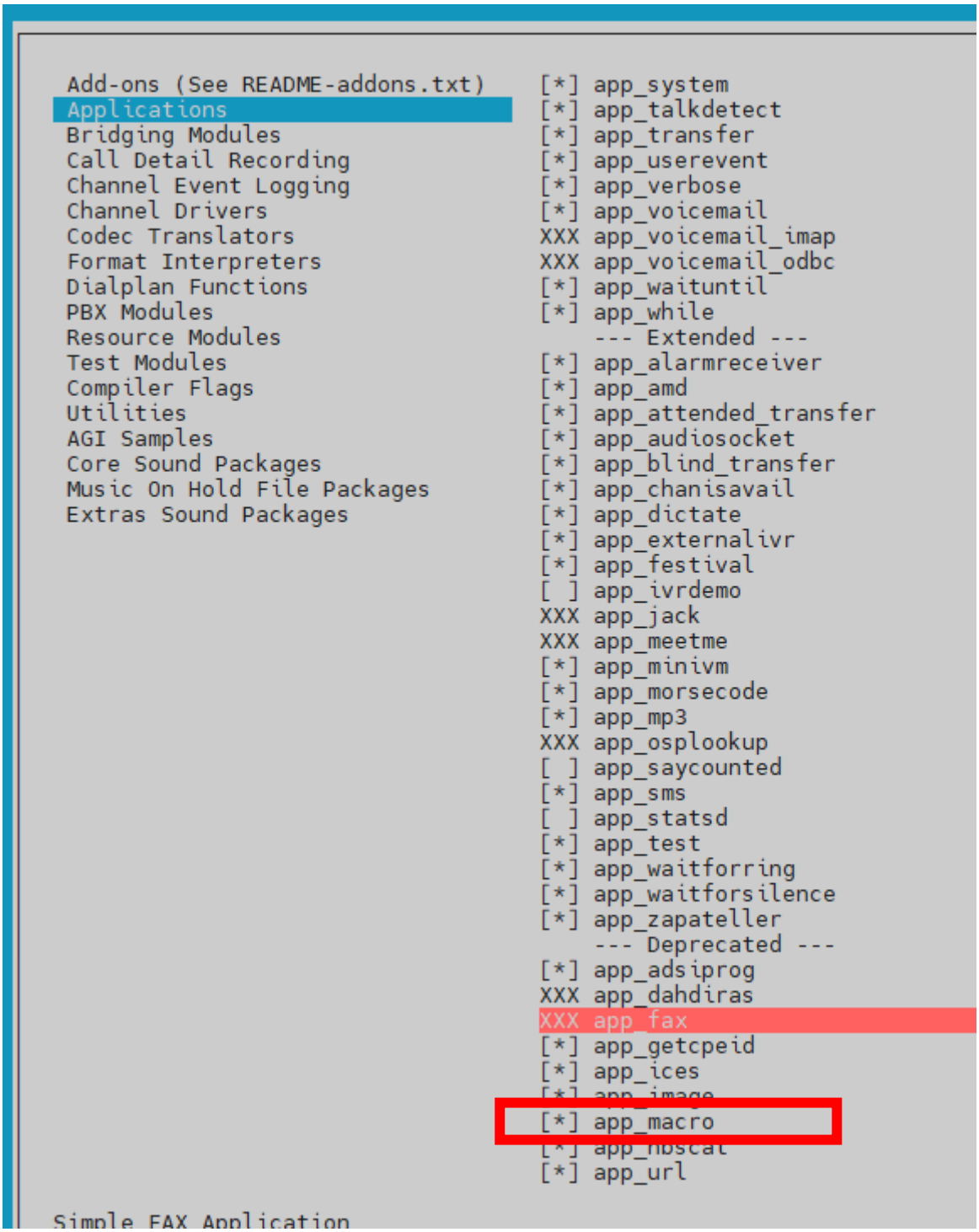
Et sélectionner tous les modules encadrés en rouge :






Add-ons (See README-addons.txt)
Applications
Bridging Modules
Call Detail Recording
Channel Event Logging
Channel Drivers
Codec Translators
Format Interpreters
Dialplan Functions
PBX Modules
Resource Modules
Test Modules
Compiler Flags
Utilities
AGI Samples
Core Sound Packages
Music On Hold File Packages
Extras Sound Packages
[*] MOH-OPSOUND-WAV
[*] MOH-OPSOUND-ULAW
[*] MOH-OPSOUND-ALAW
[ ] MOH-OPSOUND-G729
[ ] MOH-OPSOUND-G722
[ ] MOH-OPSOUND-SLN16
[ ] MOH-OPSOUND-SIREN7
[ ] MOH-OPSOUND-SIREN14


Add-ons (See README-addons.txt)
Applications
Bridging Modules
Call Detail Recording
Channel Event Logging
Channel Drivers
Codec Translators
Format Interpreters
Dialplan Functions
PBX Modules
Resource Modules
Test Modules
Compiler Flags
Utilities
AGI Samples
Core Sound Packages
Music On Hold File Packages
Extras Sound Packages
--- Core ---
[ ] EXTRA-SOUNDS-EN-WAV
[ ] EXTRA-SOUNDS-EN-ULAW
[ ] EXTRA-SOUNDS-EN-ALAW
[ ] EXTRA-SOUNDS-EN-GSM
[ ] EXTRA-SOUNDS-EN-G729
[ ] EXTRA-SOUNDS-EN-G722
[ ] EXTRA-SOUNDS-EN-SLN16
[ ] EXTRA-SOUNDS-EN-SIREN7
[ ] EXTRA-SOUNDS-EN-SIREN14
[ ] EXTRA-SOUNDS-EN_GB-WAV
[ ] EXTRA-SOUNDS-EN_GB-ULAW
[ ] EXTRA-SOUNDS-EN_GB-ALAW
[ ] EXTRA-SOUNDS-EN_GB-GSM
[ ] EXTRA-SOUNDS-EN_GB-G729
[ ] EXTRA-SOUNDS-EN_GB-G722
[ ] EXTRA-SOUNDS-EN_GB-SLN16
[ ] EXTRA-SOUNDS-EN_GB-SIREN7
[*] EXTRA-SOUNDS-FR-WAV
[*] EXTRA-SOUNDS-FR-ULAW
[*] EXTRA-SOUNDS-FR-ALAW
[ ] EXTRA-SOUNDS-FR-G729
[ ] EXTRA-SOUNDS-FR-G722
[ ] EXTRA-SOUNDS-FR-SLN16
[ ] EXTRA-SOUNDS-FR-SIREN7
[ ] EXTRA-SOUNDS-FR-SIREN14



Après cela « Save & Exit » grâce à la touche « Tab »

Maintenant :

contrib/scripts/get_mp3_source.sh

make

make install

make samples

make config

ldconfig

2.7. Etape 7 : Configuration finale et démarrage d'Asterisk

Suppression du Firewall :

systemctl stop firewalld.service

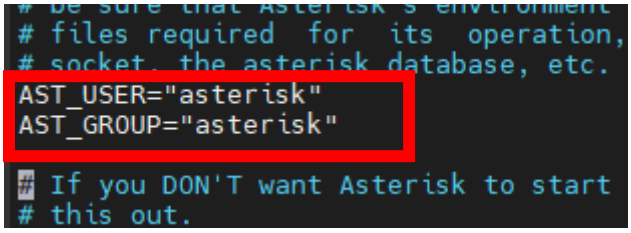
systemctl disable firewalld.service

Ajout de l'utilisateur et du groupe Asterisk et accord des permissions :

```
groupadd asterisk
useradd -r -d /var/lib/asterisk -g asterisk asterisk
usermod -aG audio,dialout asterisk
chown -R asterisk.asterisk /etc/asterisk /var/{lib,log,spool}/asterisk /usr/lib64/asterisk
```

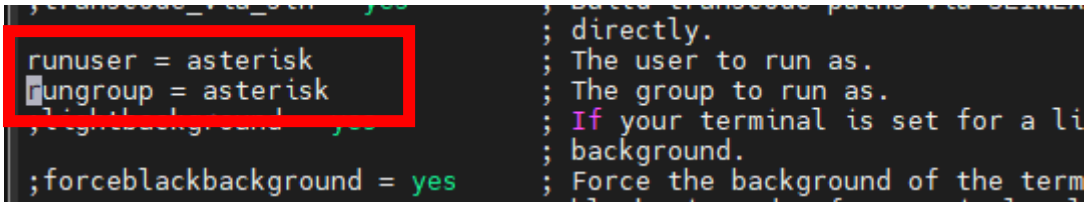
Taper : **nano /etc/sysconfig/asterisk**

Et décommenter les lignes :



De même taper : **nano /etc/asterisk/asterisk.conf**

Et décommenter les lignes :



Après cela on redémarre Asterisk et on l'active pour les prochains reboot :

systemctl restart asterisk

systemctl enable asterisk

3. Installation de FreePBX 15

3.1. Installation des dépendances

dnf -y install lynx tftp-server unixODBC mariadb-server mariadb httpd ncurses-devel sendmail sendmail-cf newt-devel libxml2-devel libtiff-devel gtk2-devel subversion git wget vim uuid-devel sqlite-devel net-tools gnutls-devel texinfo libuuid-devel libedit-devel

dnf config-manager --set-disabled powertools

dnf install -y https://repo.mysql.com/yum/mysql-connectors-community/el/8/x86_64/mysql-connector-odbc-8.0.19-1.el8.x86_64.rpm

dnf install -y epel-release

dnf install -y libid3tag

dnf install -y https://forensics.cert.org/cert-forensics-tools-release-el8.rpm

dnf --enablerepo=forensics install -y sox

dnf install -y audiofile-devel

dnf install -y python3-devel

3.2. Installation de php7.2 :

dnf remove php*
dnf install -y php php-pdo php-mysqlnd php-mbstring php-pear php-process php-xml php-opcache php-ldap php-intl php-soap php-json

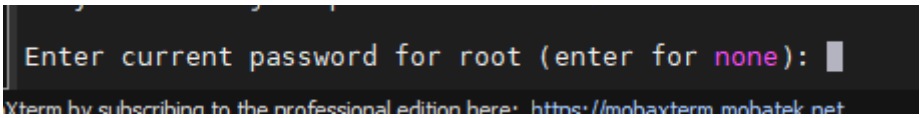
3.3. Installation de nodejs :

curl -sL https://rpm.nodesource.com/setup_12.x | bash -

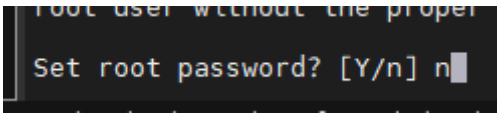
dnf install -y nodejs

3.4. Activation et démarrage de MariaDB :

```
systemctl enable mariadb.service
systemctl start mariadb
mysql_secure_installation
```



Laisser vide et appuyer sur la touche Entrée



Taper « n »

Vous pouvez taper « y » pour toutes les autres questions.

3.5. Démarrage de Appache :

```
systemctl enable httpd.service
systemctl start httpd.service
pear install Console_Getopt
```

3.6. Installation et configuration de FreePBX

```
sed -i 's/\(^upload_max_filesize = \).*/\120M/' /etc/php.ini
sed -i 's/\(^memory_limit = \).*/\1256M/' /etc/php.ini
sed -i 's/^\(User\|Group\).*/\1 asterisk/' /etc/httpd/conf/httpd.conf
sed -i 's/AllowOverride None/AllowOverride All/' /etc/httpd/conf/httpd.conf
sed -i 's/\(^user = \).*/\1asterisk/' /etc/php-fpm.d/www.conf
sed -i 's/\(^group = \).*/\1asterisk/' /etc/php-fpm.d/www.conf
sed -i 's/\(^listen.acl_users = apache,nginx\).*/\1,asterisk/' /etc/php-fpm.d/www.conf
systemctl restart httpd.service
systemctl restart php-fpm
```

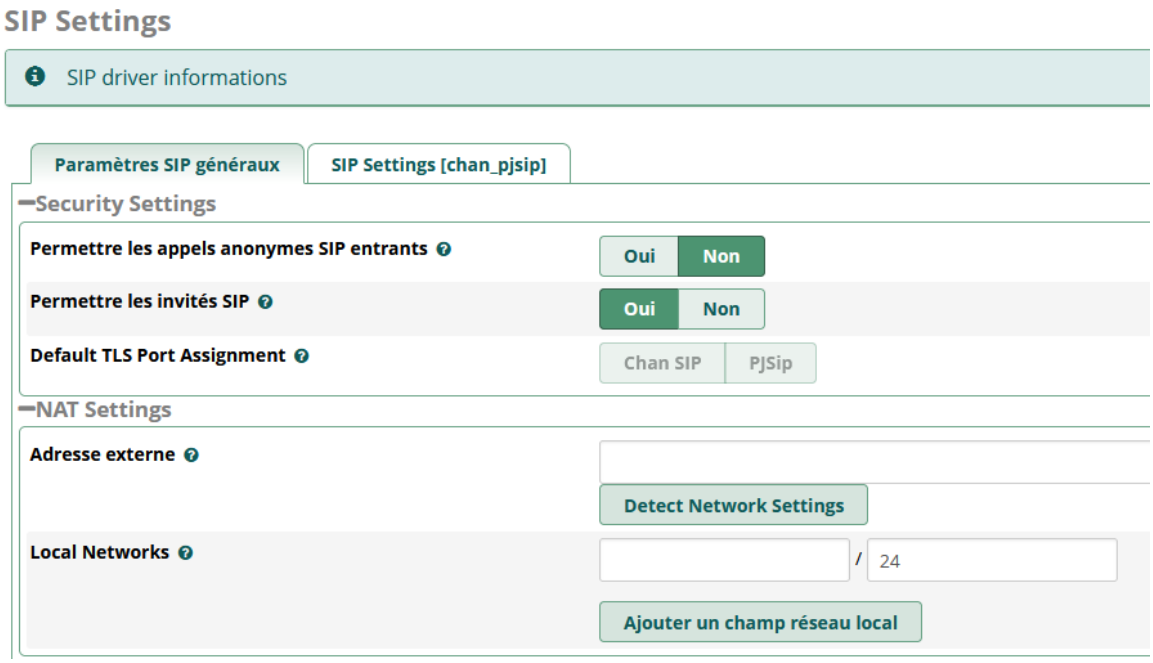
Téléchargement et installation de FreePBX :

```
cd /usr/src
wget http://mirror.freepbx.org/modules/packages/freepbx/freepbx-15.0-latest.tgz
tar xfz freepbx-15.0-latest.tgz
rm -f freepbx-15.0-latest.tgz
cd freepbx
./start_asterisk start
./install -n
```

4. Administration et installation des téléphones ip à travers FreePBX

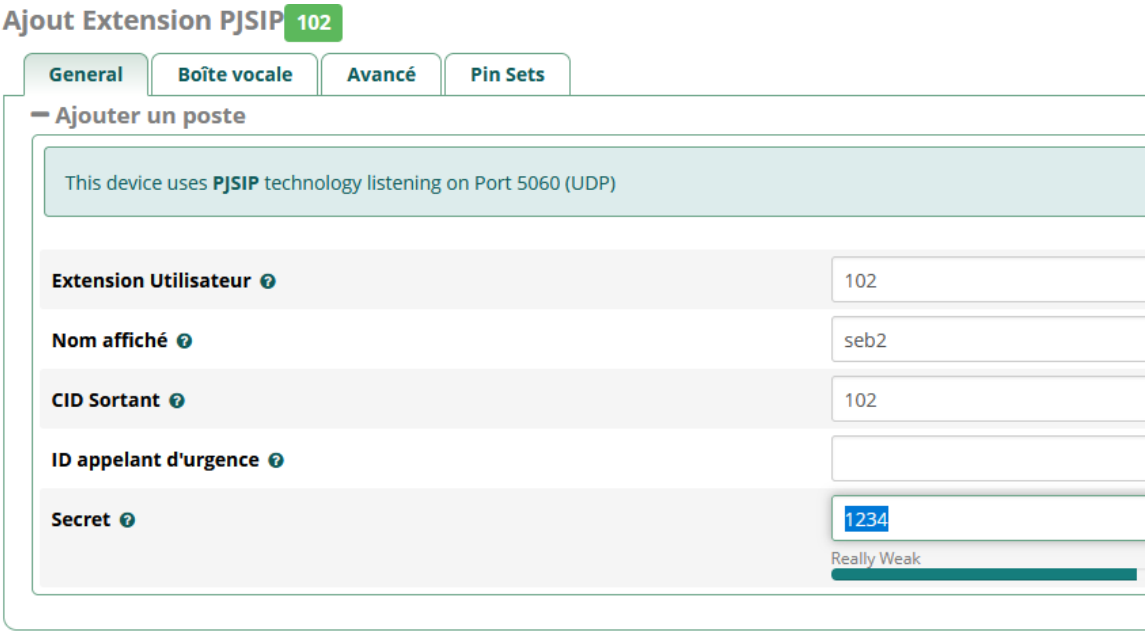
Dans Paramètres > Paramètres SIP d'Asterisk

Rajouter le réseaux Local



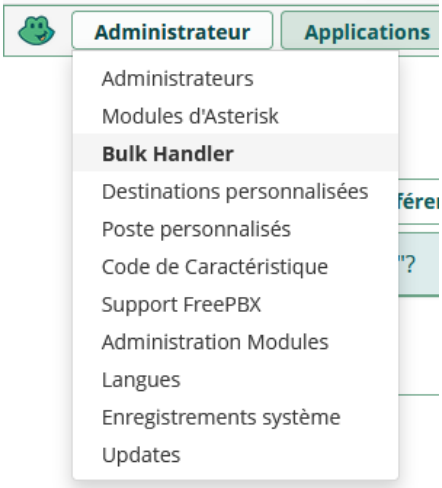
Dans application>Postes :

Créer un utilisateur :

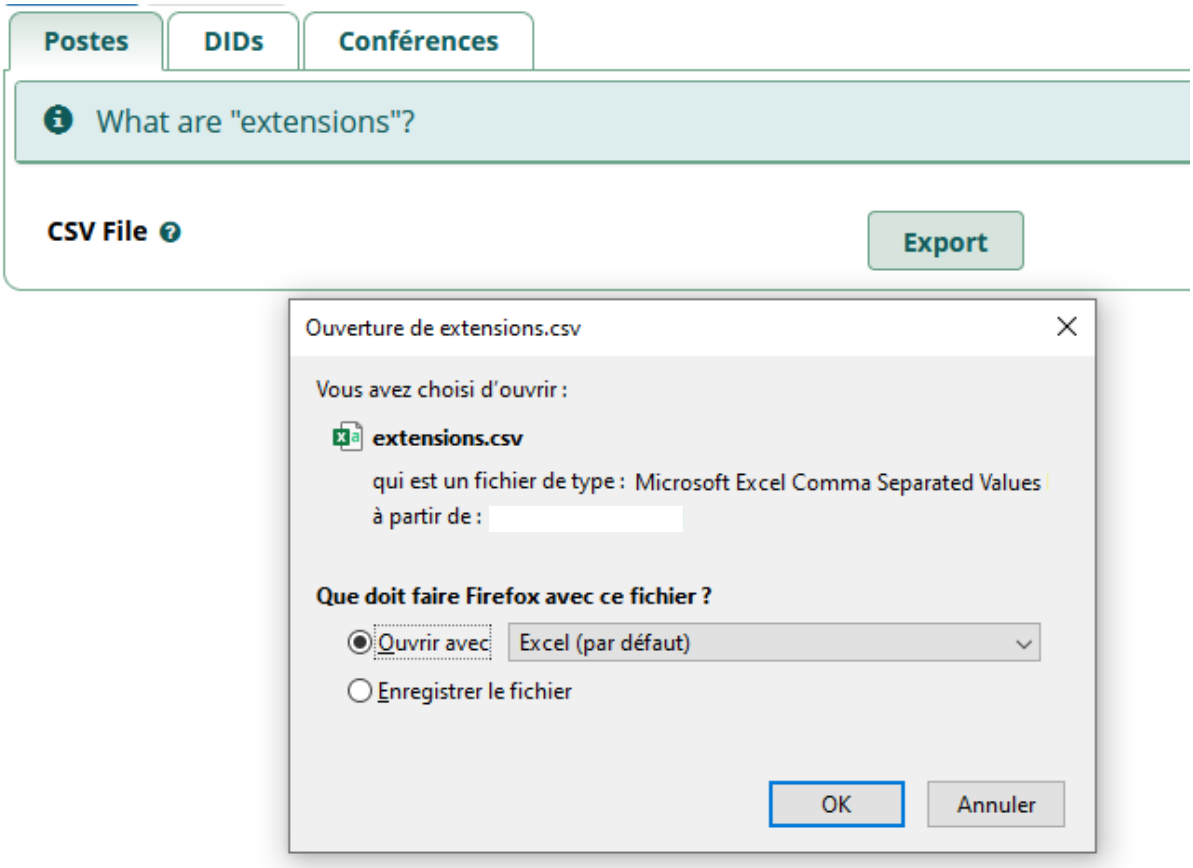


5. Convertir une configuration SIP en PJSIP

5.1. Exporter la configuration de l'ancien serveur



Se rendre dans Administrateur>Bulk Handler



Exporter la configuration au format CSV.

5.2. Importer la configuration sur le nouveau serveur :

De même se rendre dans Bulk Handler.

Puis dans Import et importer le fichier CSV récupéré sur l'ancien serveur

5.3. Conversion des profils

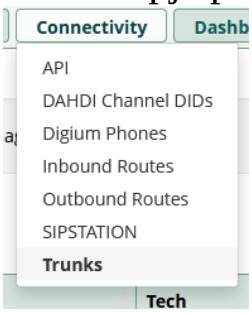
Sur le nouveau serveur taper les commandes :

fwconsole convert2pjsip -a

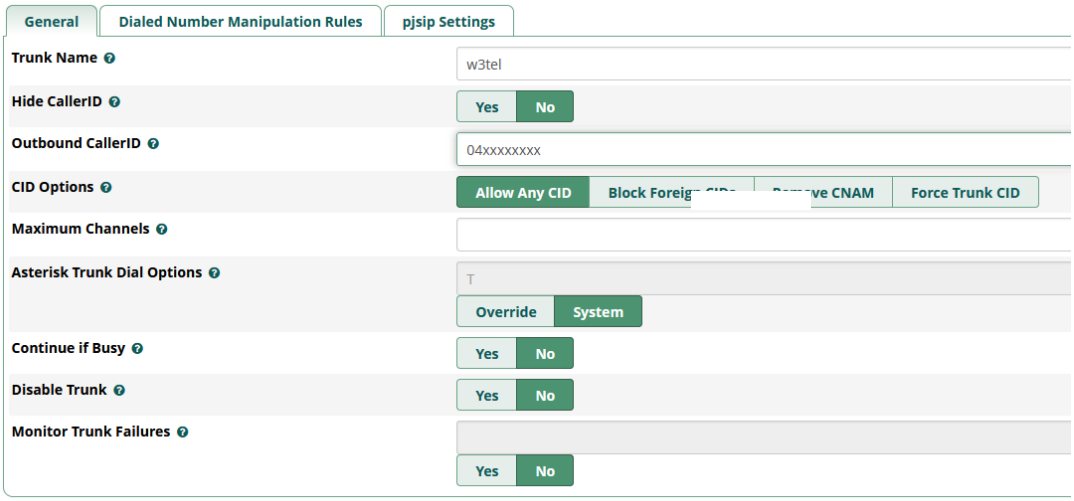
fwconsole reload

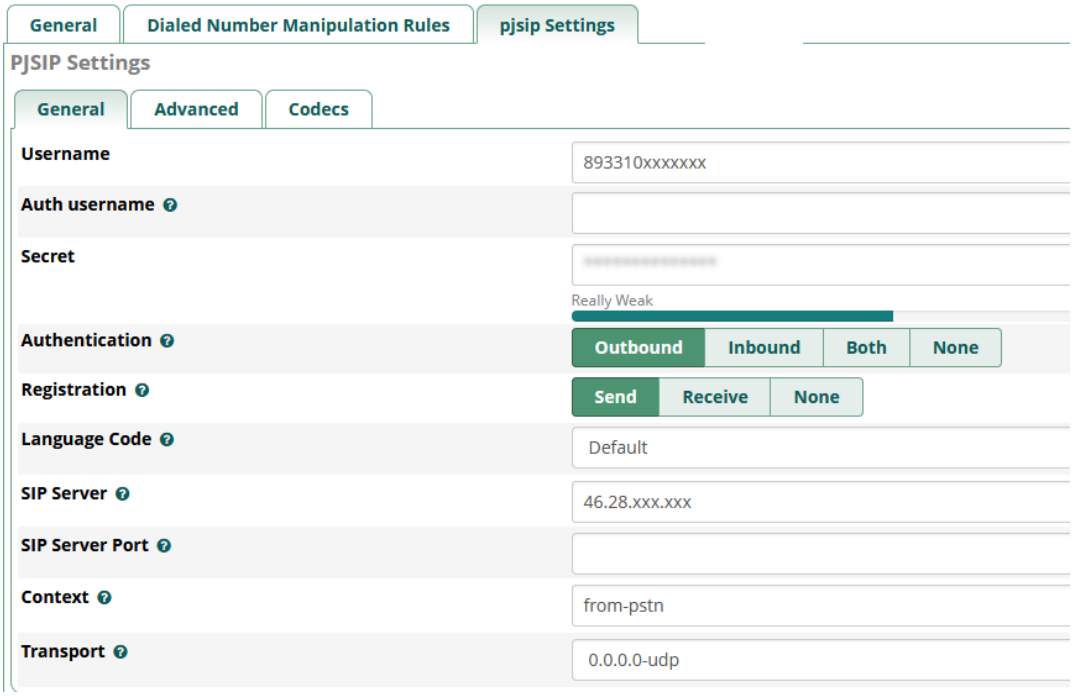
6. Configurer un Trunk pjsip

Se rendre dans :

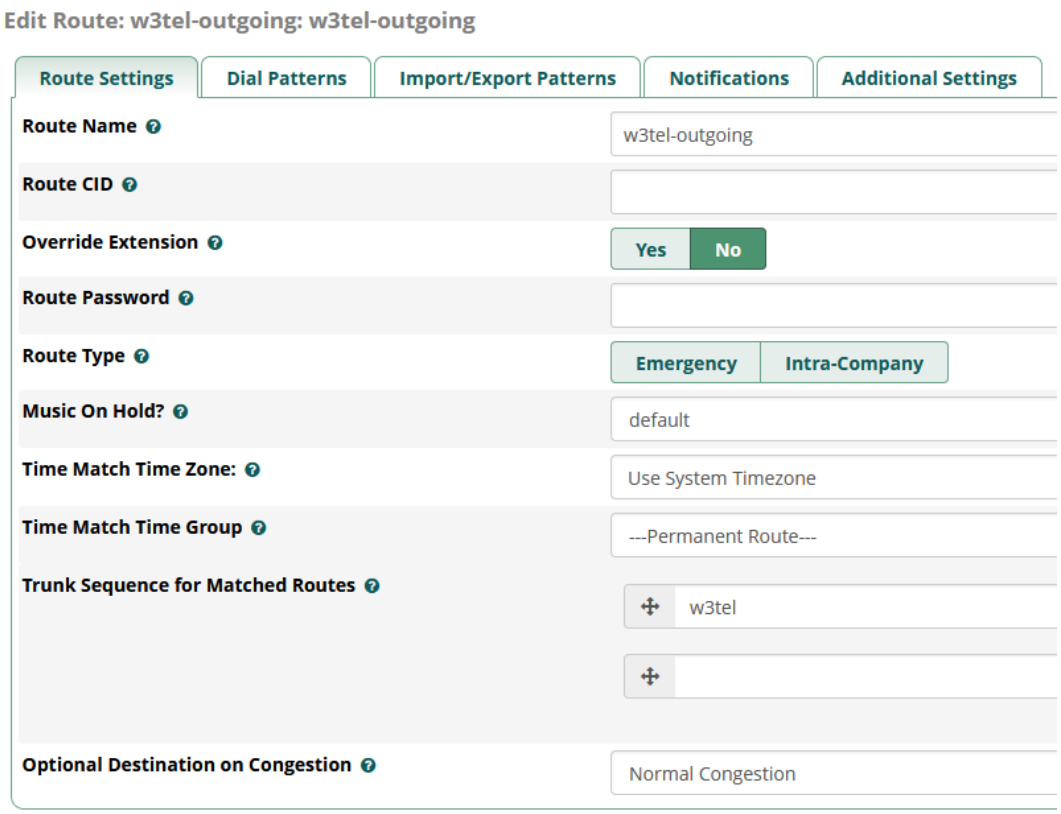


Ensuite :

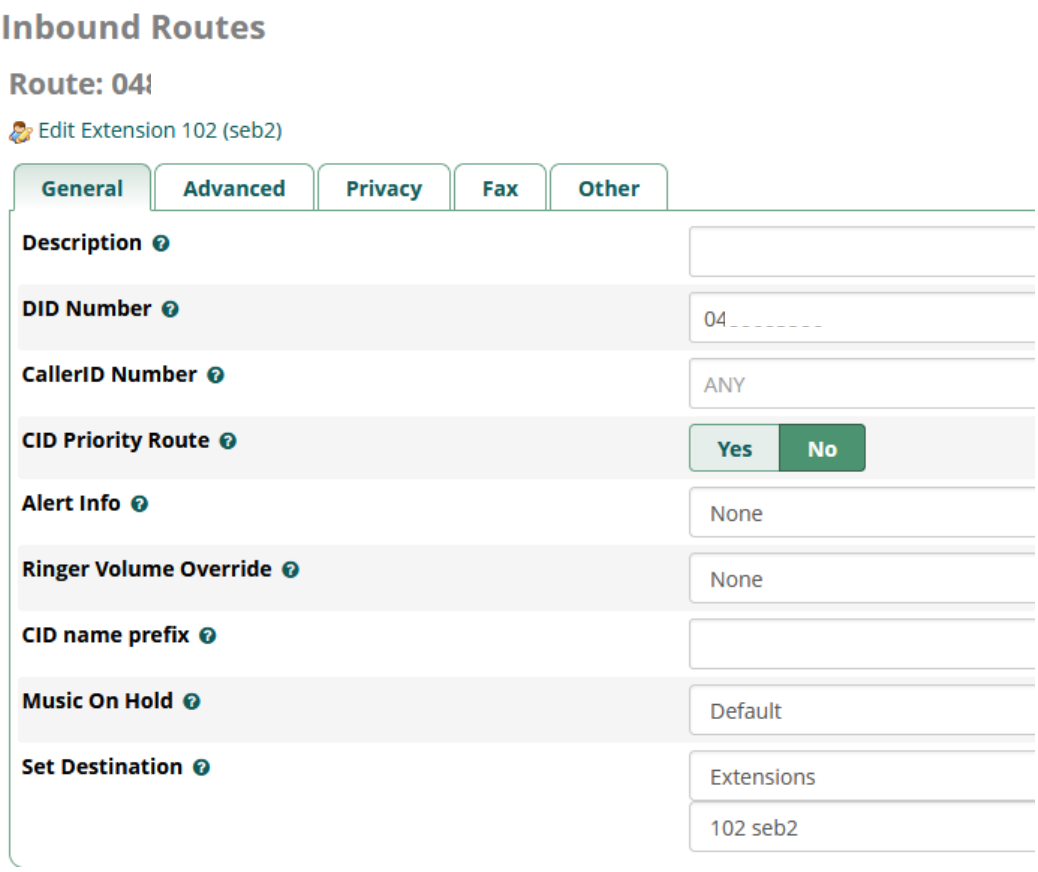




Il faut ensuite configurer la route sortante et la faire pointer vers le trunk :



Et enfin configurer les routes entrantes pour relier les postes interne à un numéro de l'extérieur :



7. Configuration du switch pour le voice vlan

```
config-file-header
switch31c77f
v1.4.2.4 / R800_NIK_1_4_194_194
CLI v1.0
set system mode switch queues-mode 4

file SSD indicator encrypted
@
ssd-control-start
ssd config
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
!
vlan database
vlan 10,50,90,250,254
exit
voice vlan id 50
voice vlan state oui-enabled
voice vlan oui-table add 0001e3 Siemens_AG_phone________
voice vlan oui-table add 00036b Cisco_phone______________
voice vlan oui-table add 00096e Avaya____________________
voice vlan oui-table add 000b82 GS2
voice vlan oui-table add 000fe2 H3C_Aolynk_______________
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone
voice vlan oui-table add 00d01e Pingtel_phone____________
voice vlan oui-table add 00e075 Polycom/Veritel_phone___
voice vlan oui-table add 00e0bb 3Com_phone_______________
voice vlan oui-table add c074ad GS
qos advanced
qos trust cos-dscp
ip access-list extended test
exit
hostname switch31c77f
ip ssh server
ip ssh password-auth
!
interface vlan 10
 name utilisateurs
!
interface vlan 50
 name voix
!
interface vlan 90
 name admin
```

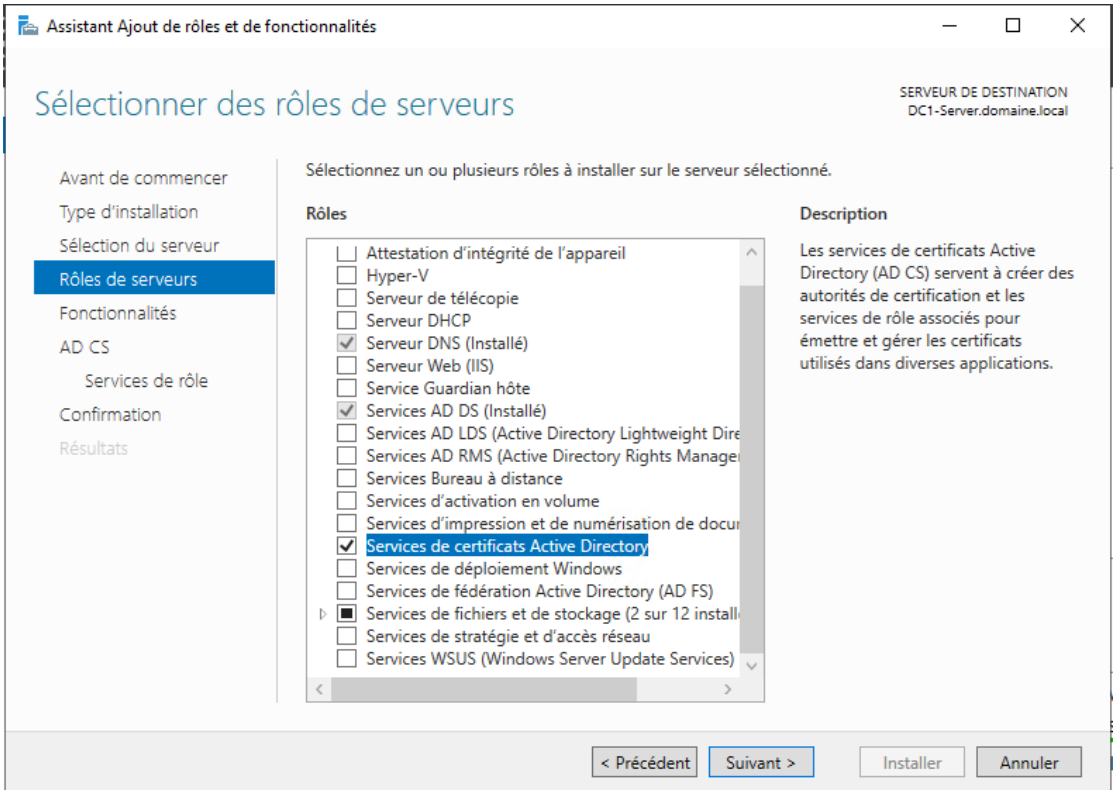
```
 ip address 10.xxx.xxx.xxx 255.255.255.0
 no ip address dhcp
!
interface vlan 250
 name DMZ
!
interface vlan 254
 name DMZ_Service
!
interface gigabitethernet1/1/1
 description "Firewall - Trunk"
 channel-group 1 mode auto
!
interface gigabitethernet1/1/2
 description "Firewall - Trunk"
 channel-group 1 mode auto
!
interface gigabitethernet1/1/3
 description user
 switchport trunk native vlan 10
 voice vlan enable
!
interface gigabitethernet1/1/4
 description user
 switchport trunk native vlan 10
 voice vlan enable
!
interface gigabitethernet1/1/5
 description user
 switchport trunk native vlan 10
 voice vlan enable
!
interface gigabitethernet1/1/6
 description user
 switchport trunk native vlan 10
 voice vlan enable
!
interface gigabitethernet1/1/7
 description user
 switchport trunk native vlan 10
 voice vlan enable
!
interface gigabitethernet1/1/8
 description user
 switchport trunk native vlan 10
 voice vlan enable
!
interface gigabitethernet1/1/9
```

```
 description user
 switchport trunk native vlan 10
 voice vlan enable
!
interface gigabitethernet1/1/10
 description user
 switchport trunk native vlan 10
 voice vlan enable
!
interface gigabitethernet1/1/25
 description ESXi
 switchport mode access
 switchport access vlan 90
!
interface gigabitethernet1/1/26
 description FreePBX
 switchport mode access
 switchport access vlan 250
!
interface gigabitethernet1/1/27
 description AD
 switchport mode access
 switchport access vlan 254
!
interface gigabitethernet1/1/28
 description "Aruba Access Point Wifi"
 switchport trunk allowed vlan add 10
 switchport trunk native vlan 90
!
interface Port-channel1
 description LACP
 switchport trunk allowed vlan add 10,50,90,250,254
!
exit
macro auto disabled
ip default-gateway 10.xxx.xxx.xxx
```

Annexe 2 : Mise en place d'une authentification par AD aux bornes wifi Aruba.

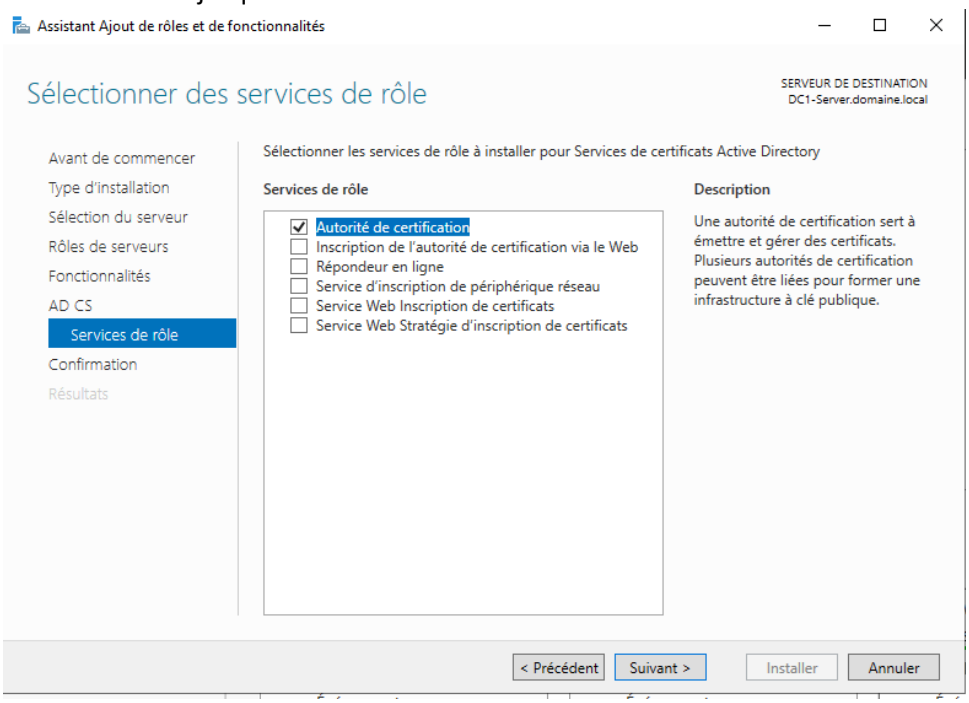
8. AD CS
9. Installation du rôle

Ajouter des rôles et des fonctionnalités :

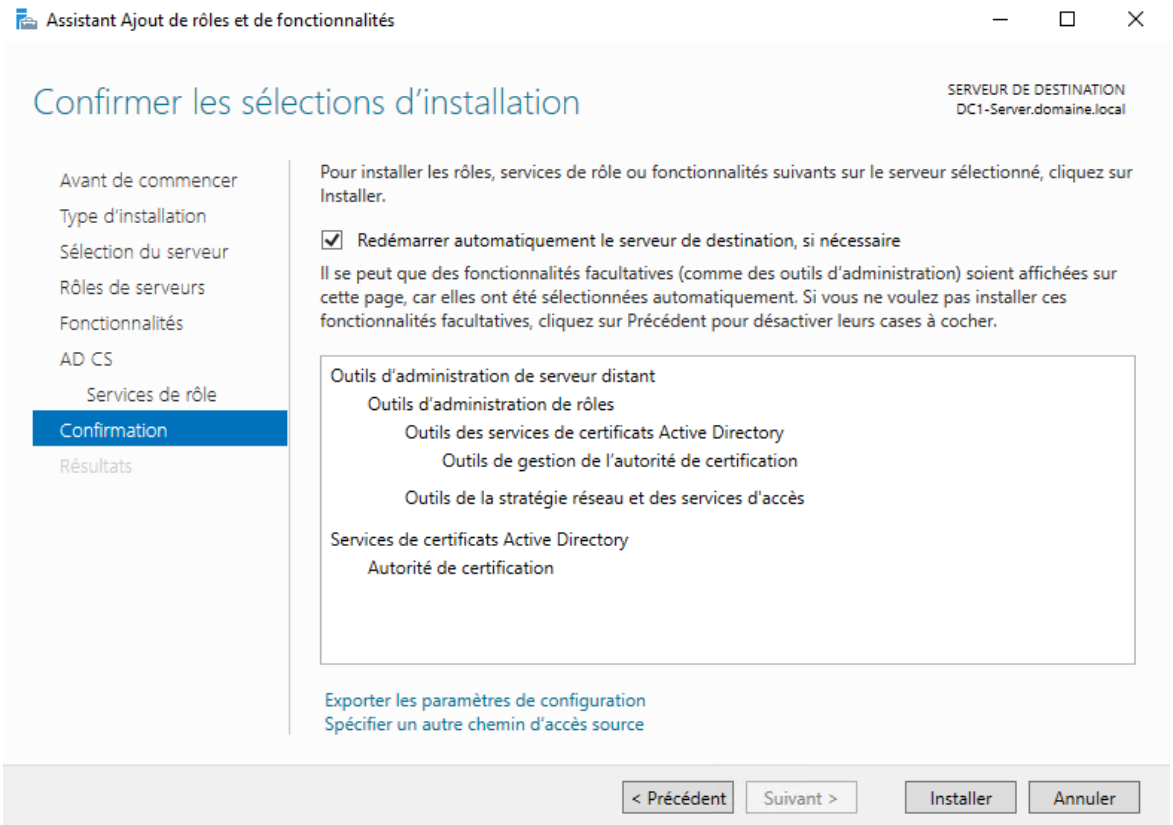


Sélectionner le Service de certificats Active Directory

Puis « Suivant » jusqu'à :

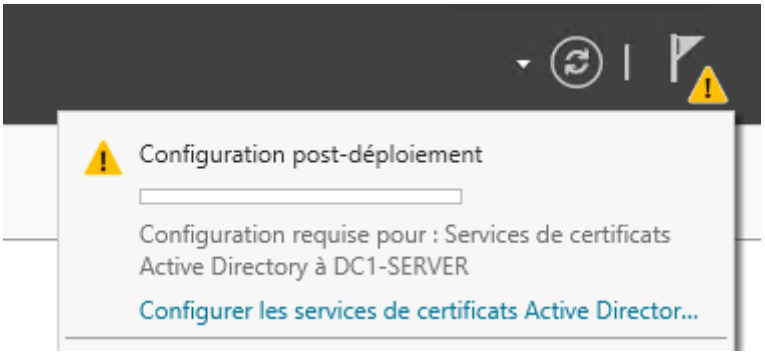


Sélectionner « Autorité de certification »

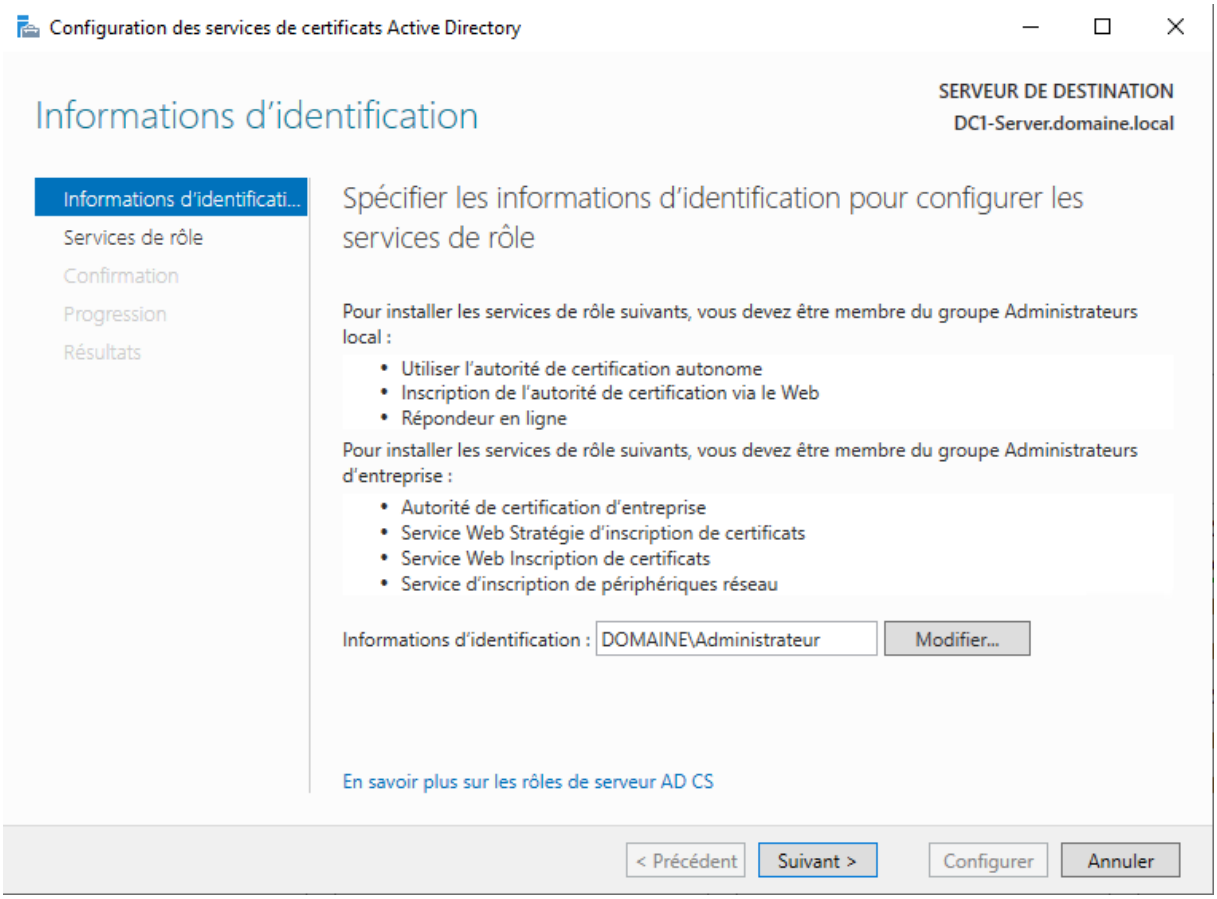


Puis confirmer et installer.

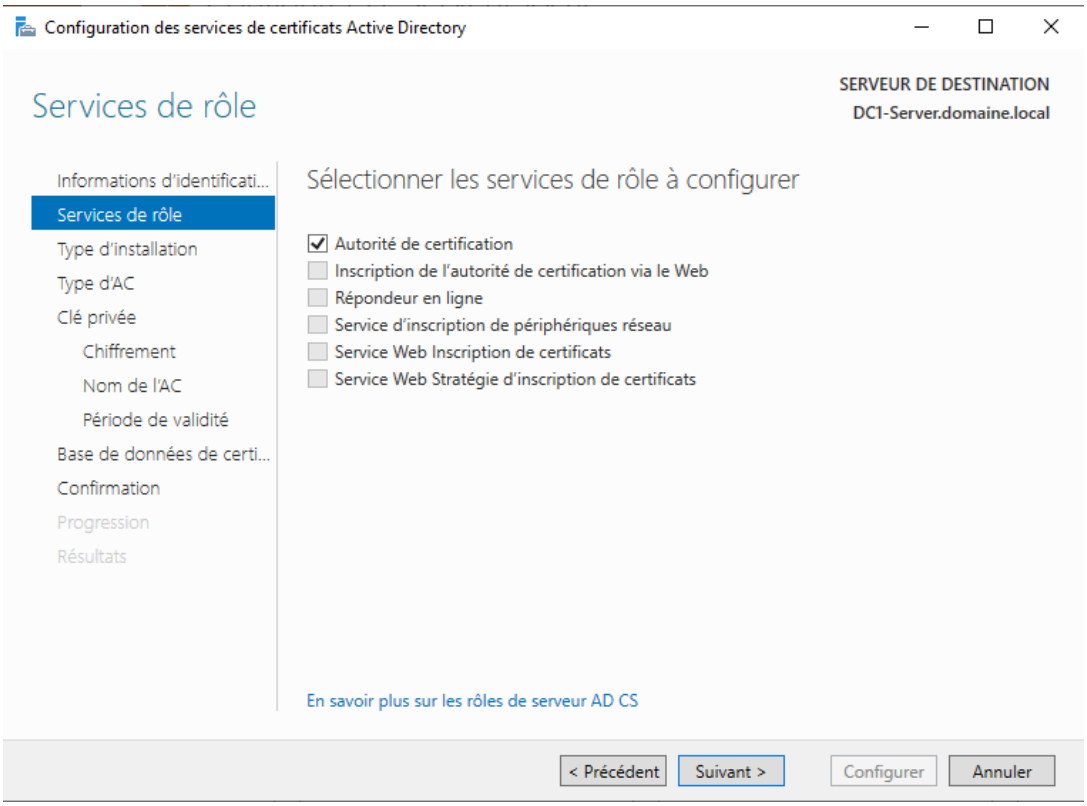
10. Configuration du rôle



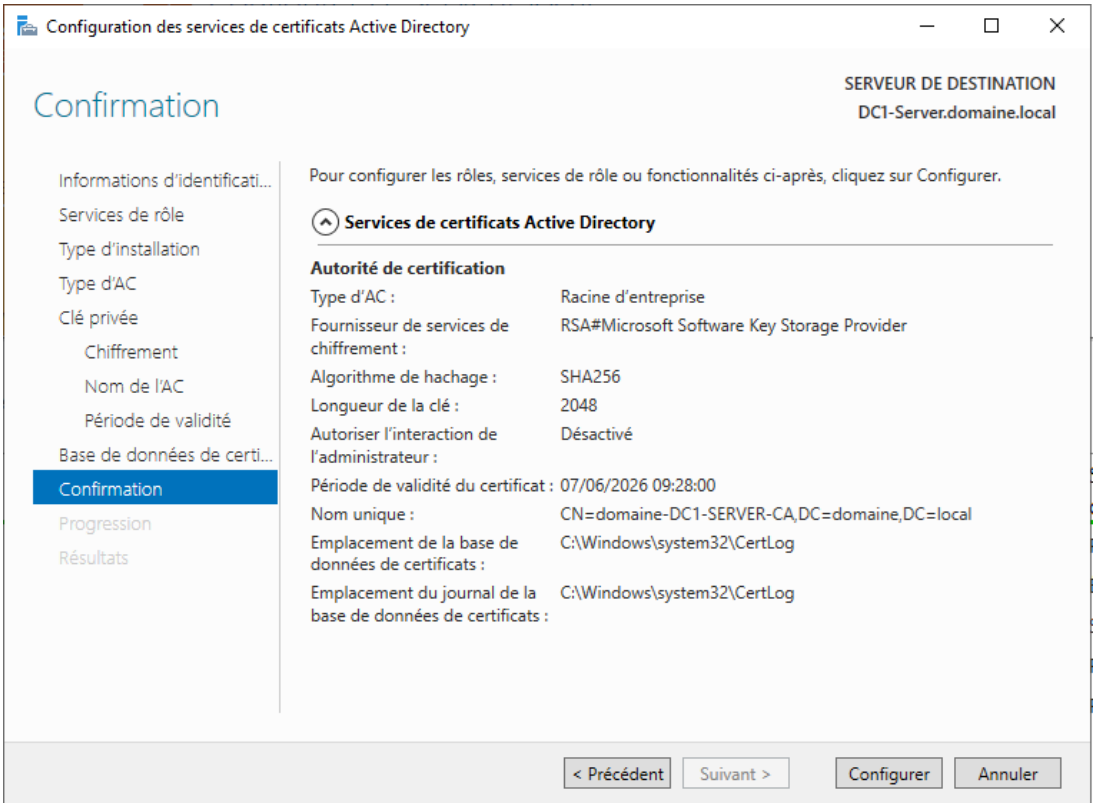
Configurer les services



Ensuite sélectionner « Autorité de certification » :



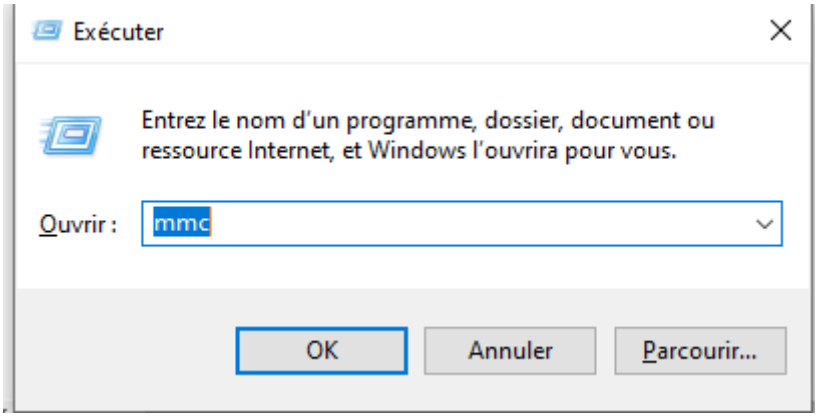
Sélectionner Suivant jusqu'à :



Et enfin cliquer sur « Configurer »

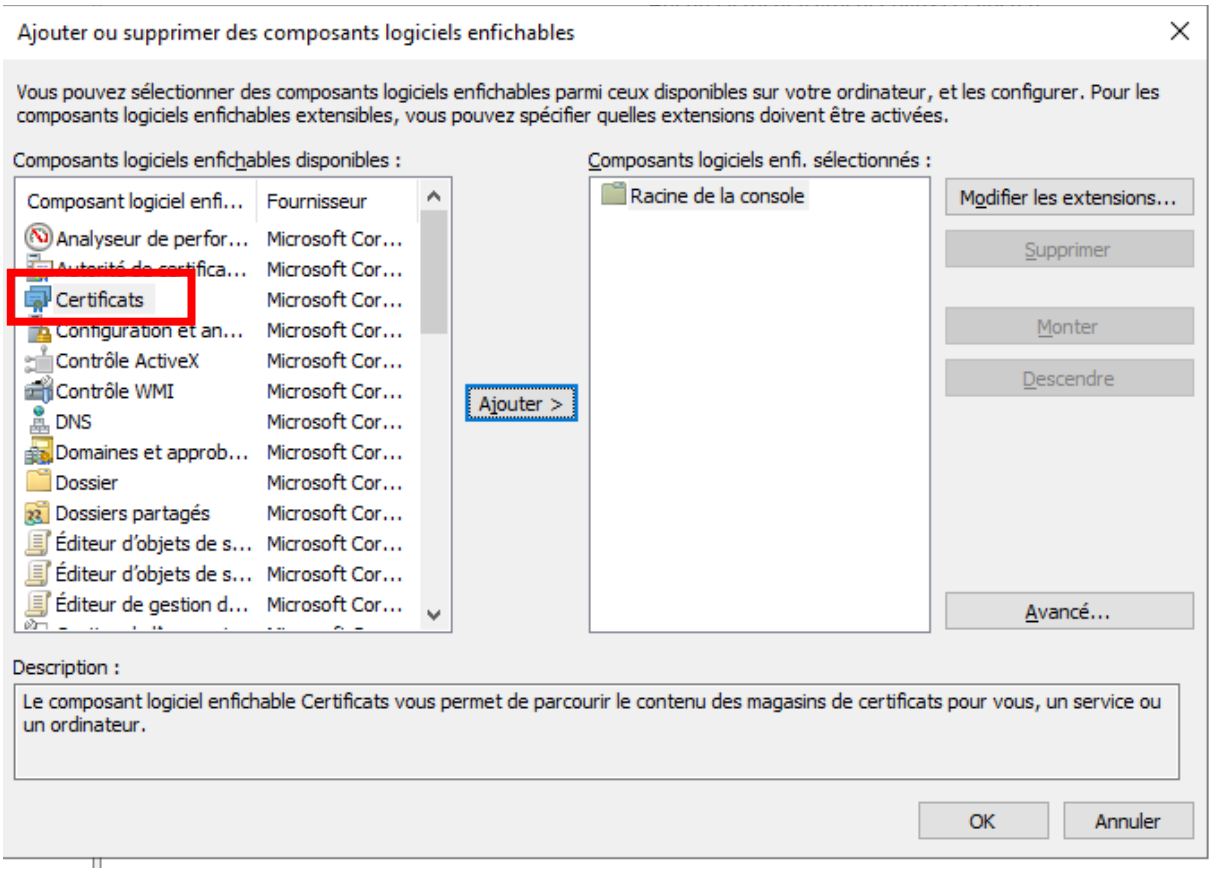
Nous allons maintenant créer un certificat.

Windows + R :

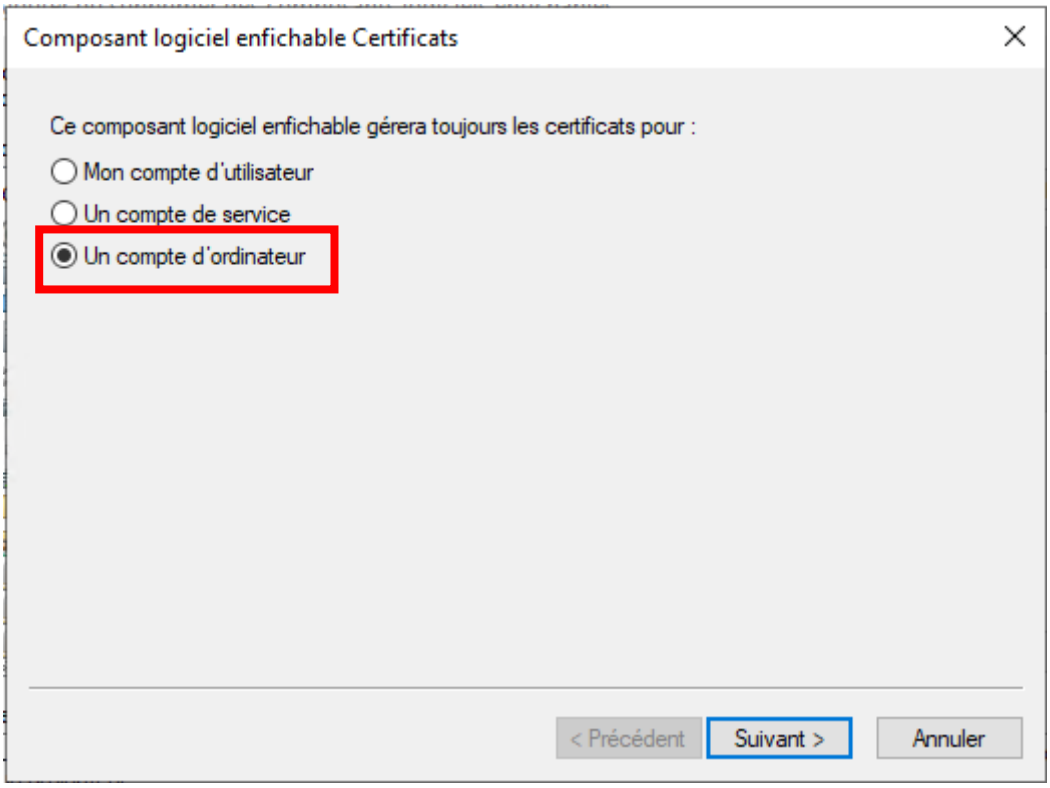


Ensuite dans la fenêtre qui s'ouvre cliquer sur : Fichier > Ajouter/Supprimer un composant logiciel enfichable…

Dans la fenêtre qui s'ouvre :

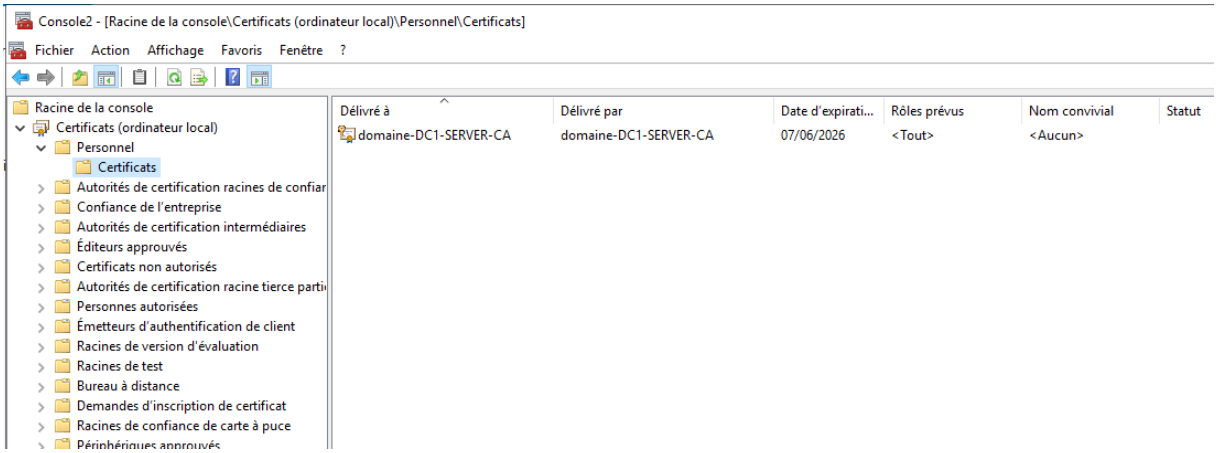


Cliquer sur Certificats puis Ajouter :

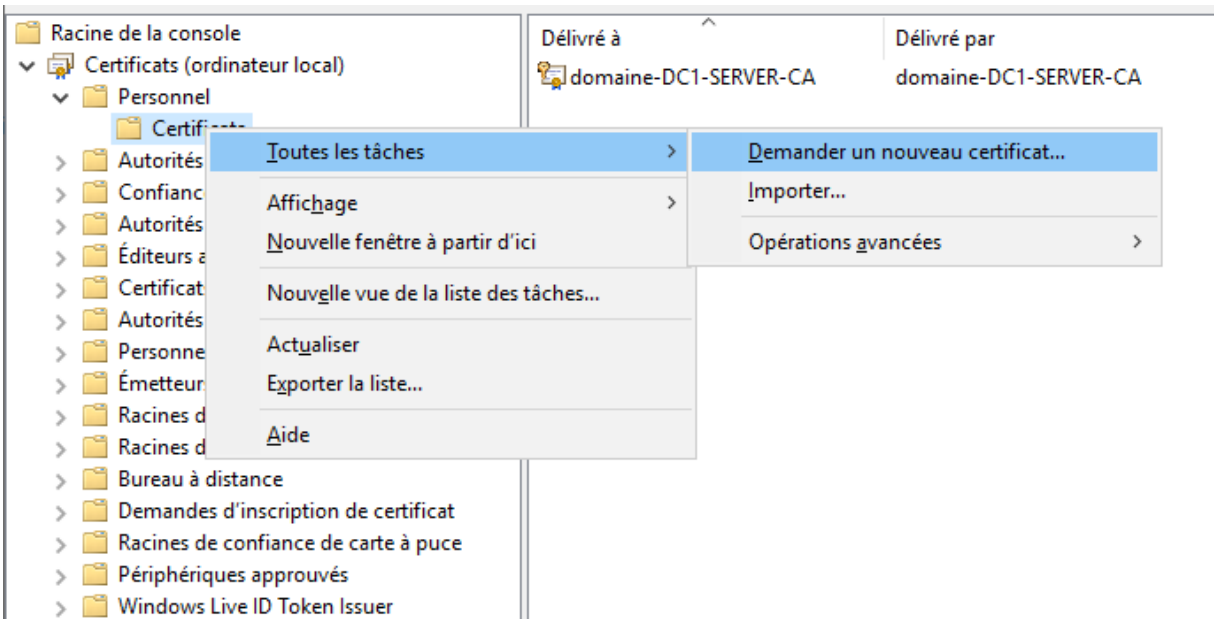


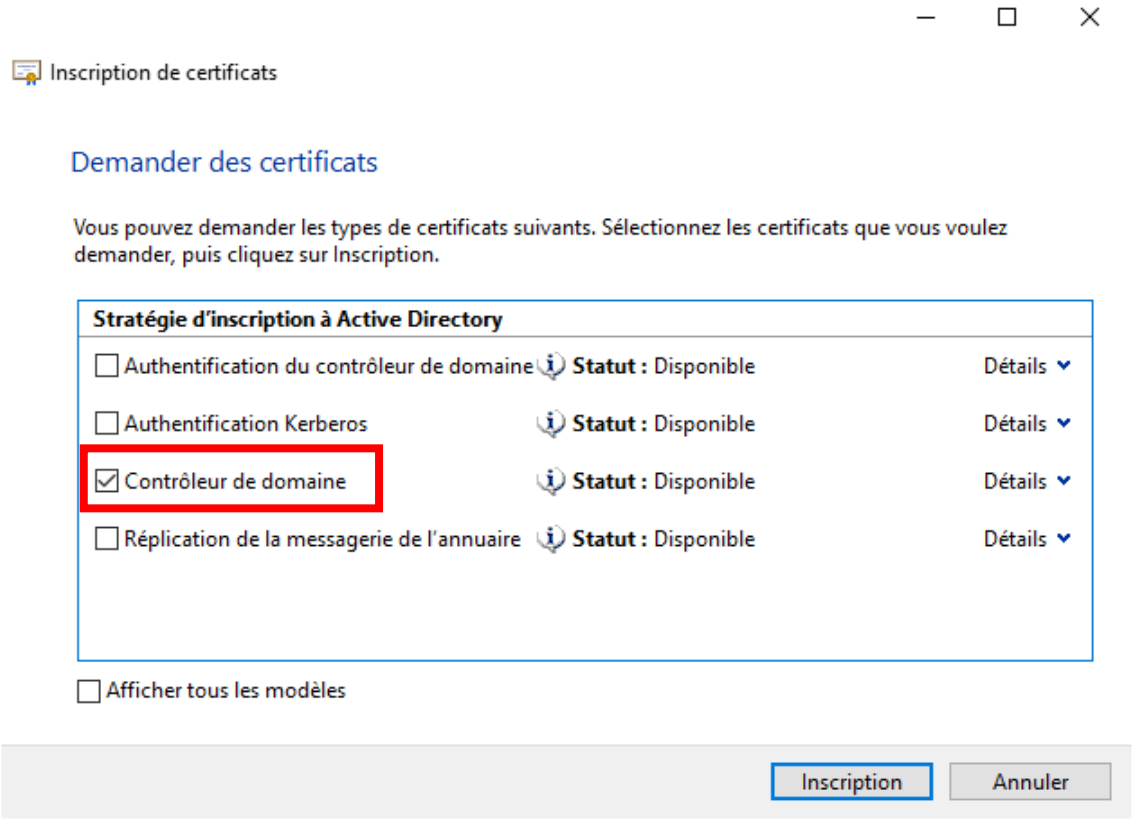
Puis valider

Dans l'arborescence se placer dans Certificats (ordinateur local) > Personnel > Certificats :

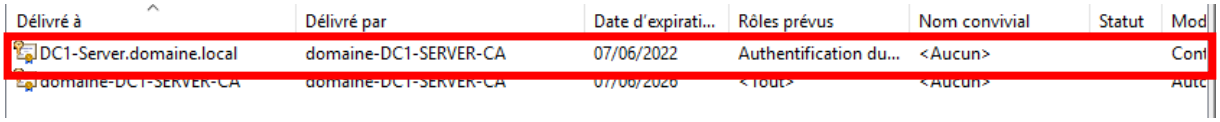


Puis clic droit sur certificat et demander un nouveau certificat :

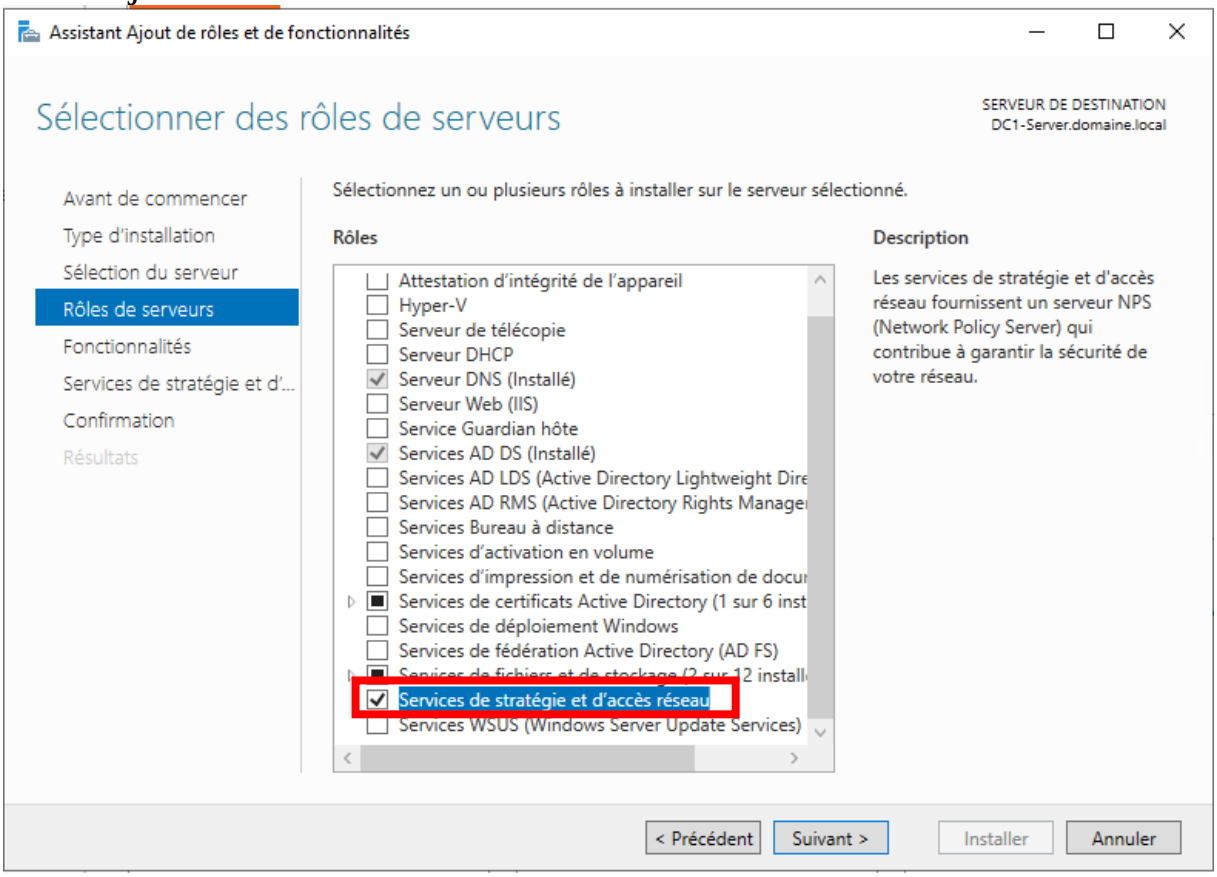




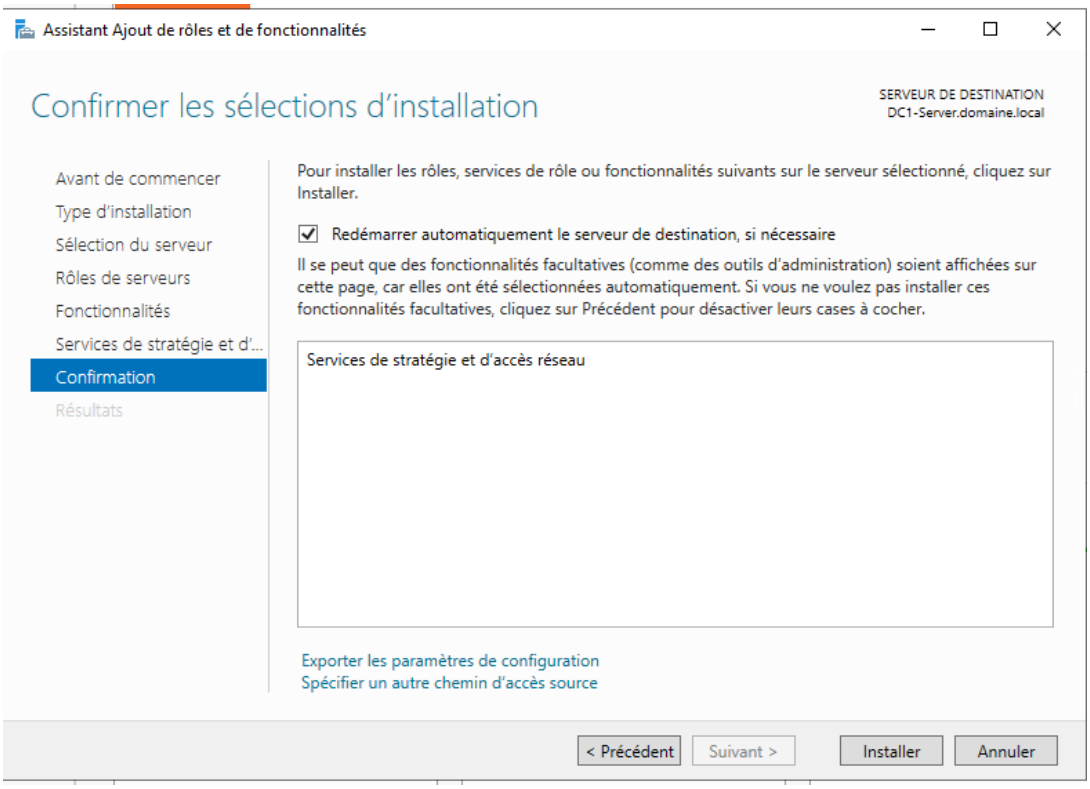
Nous pouvons voir sur la première ligne notre certificat :



11. NPS (Serveur Radius)
12. Ajout du rôle

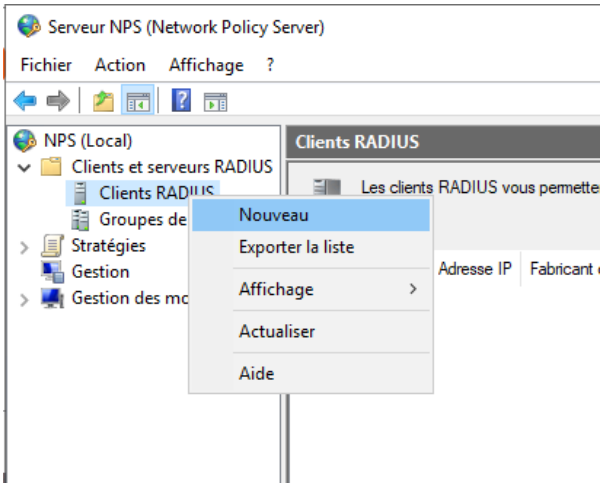


Et l'installer



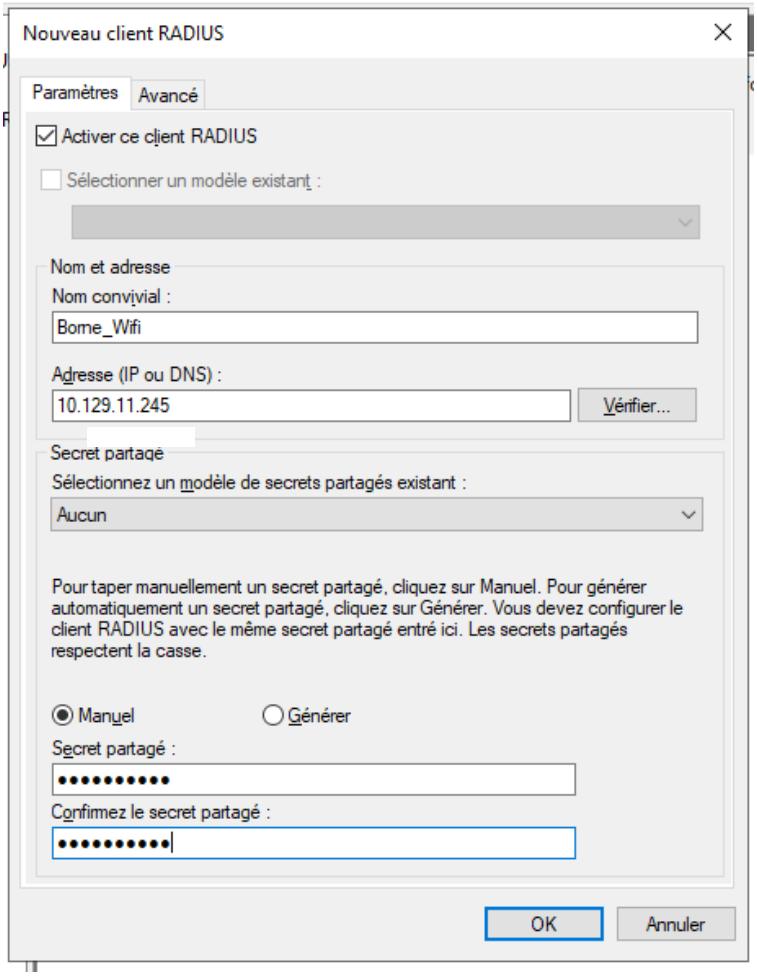
13. Configuration du serveur radius

Ouvrir Serveur NPS et se rendre dans Clients et serveurs RADIUS > Clients RADIUS



et ajouter un client radius

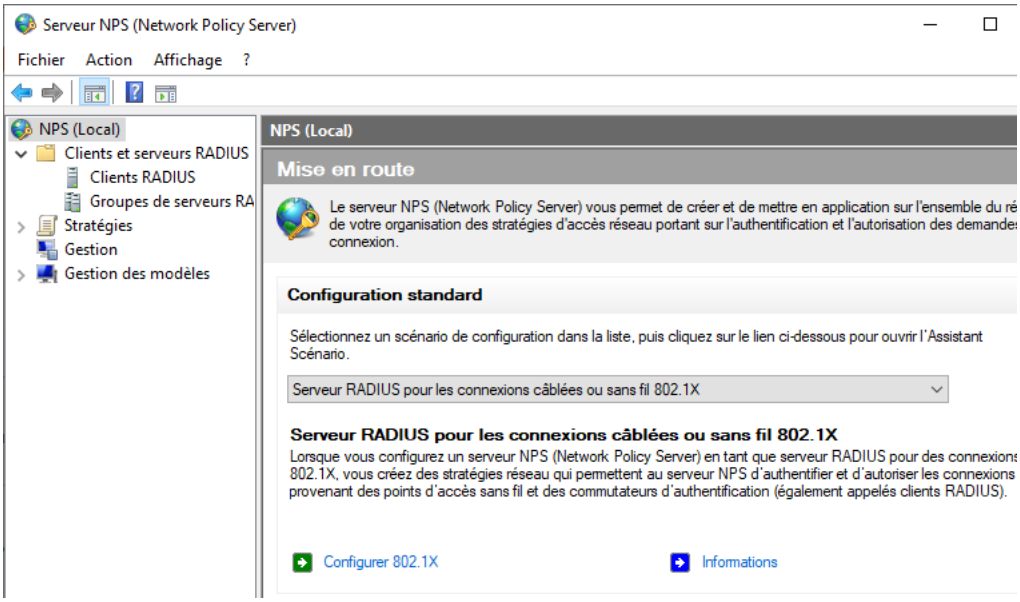
Configurer le client :



Indiquer l'adresse ip de la borne wifi et rentrer un mot de passe qu'il faudra aussi indiquer à la borne ultérieurement.

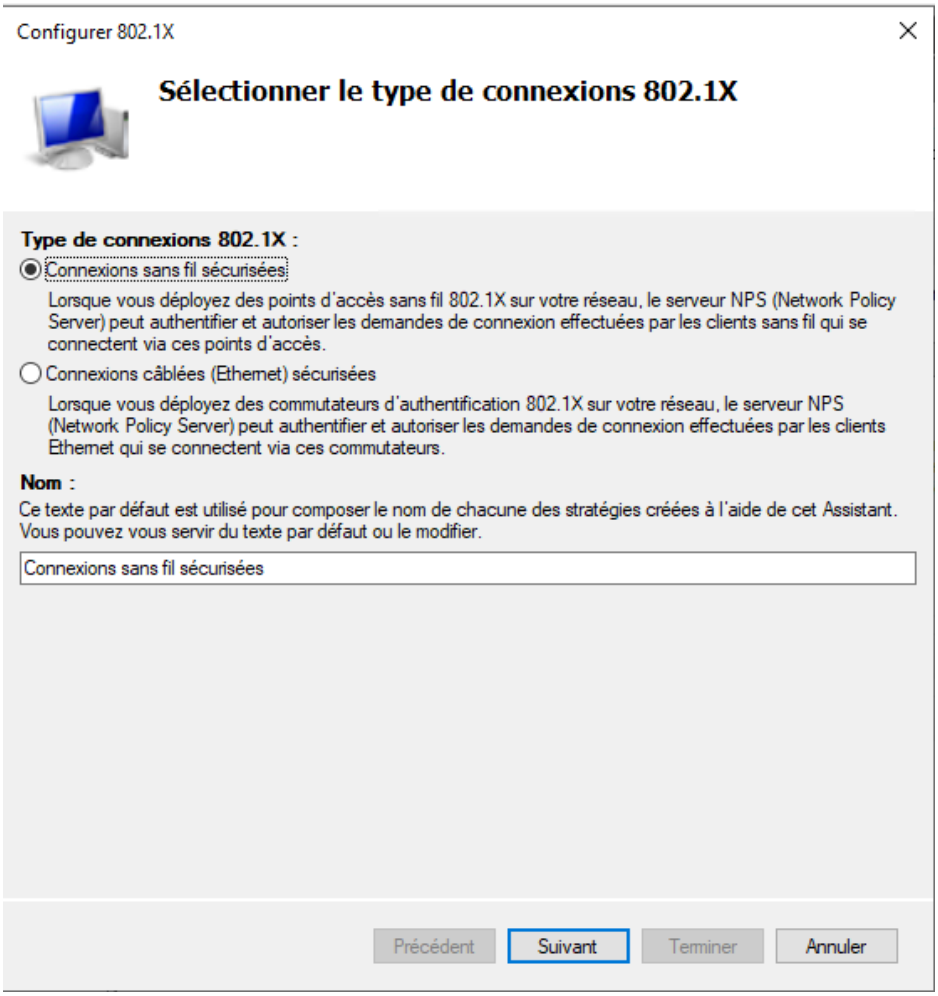
Ensuite cliquer sur NPS(Local) dans l'arborescence à droite.

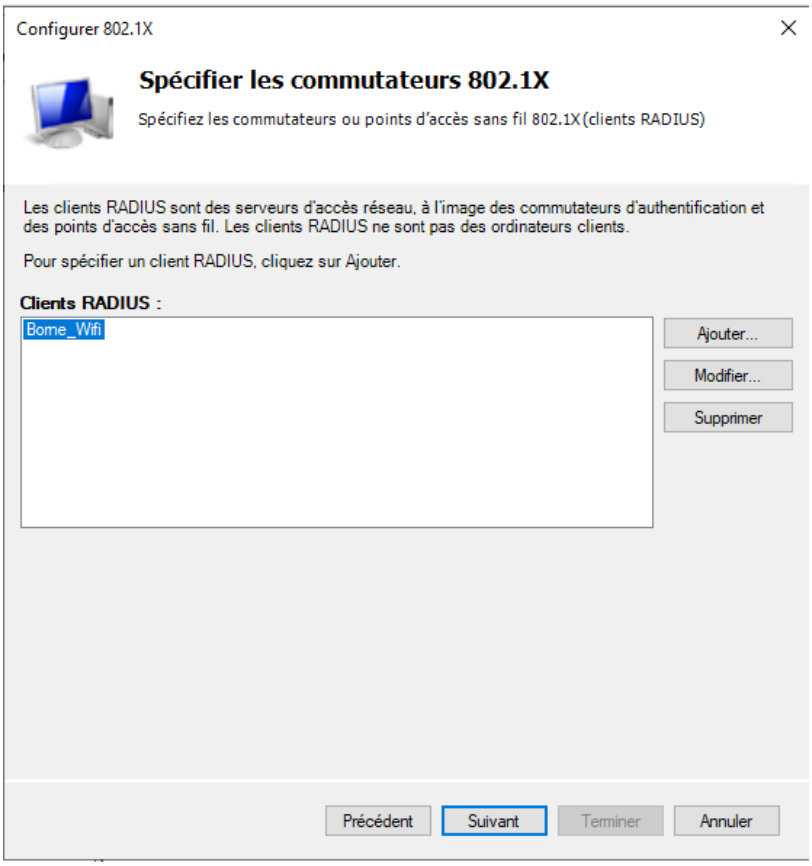
Dans configuration standard choisisser :

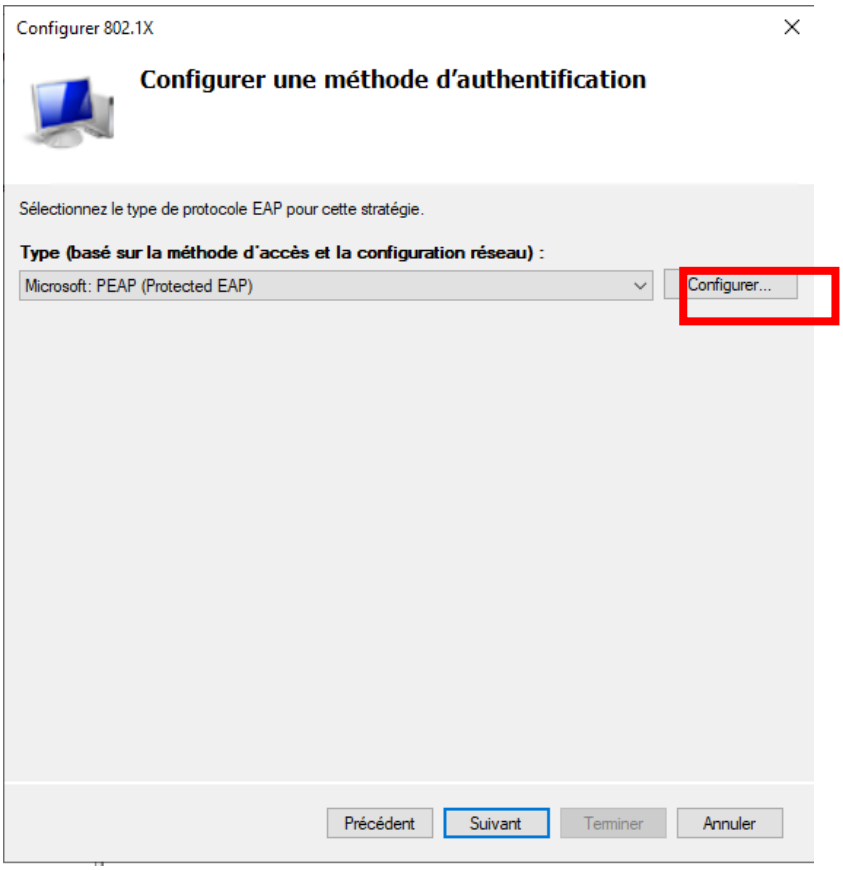


Cliquer sur « Configurer 802.1X »

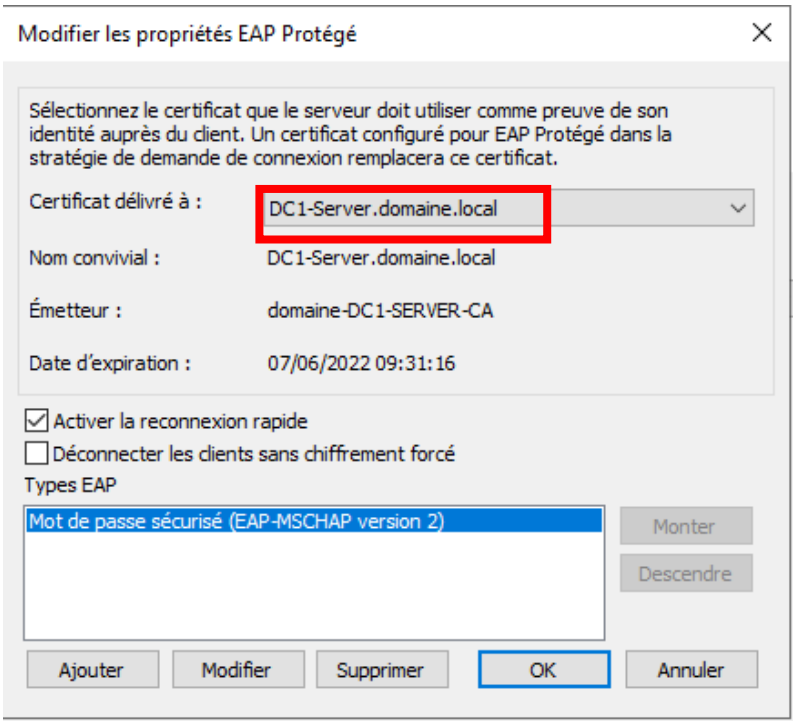
Et suivre les étapes suivantes :



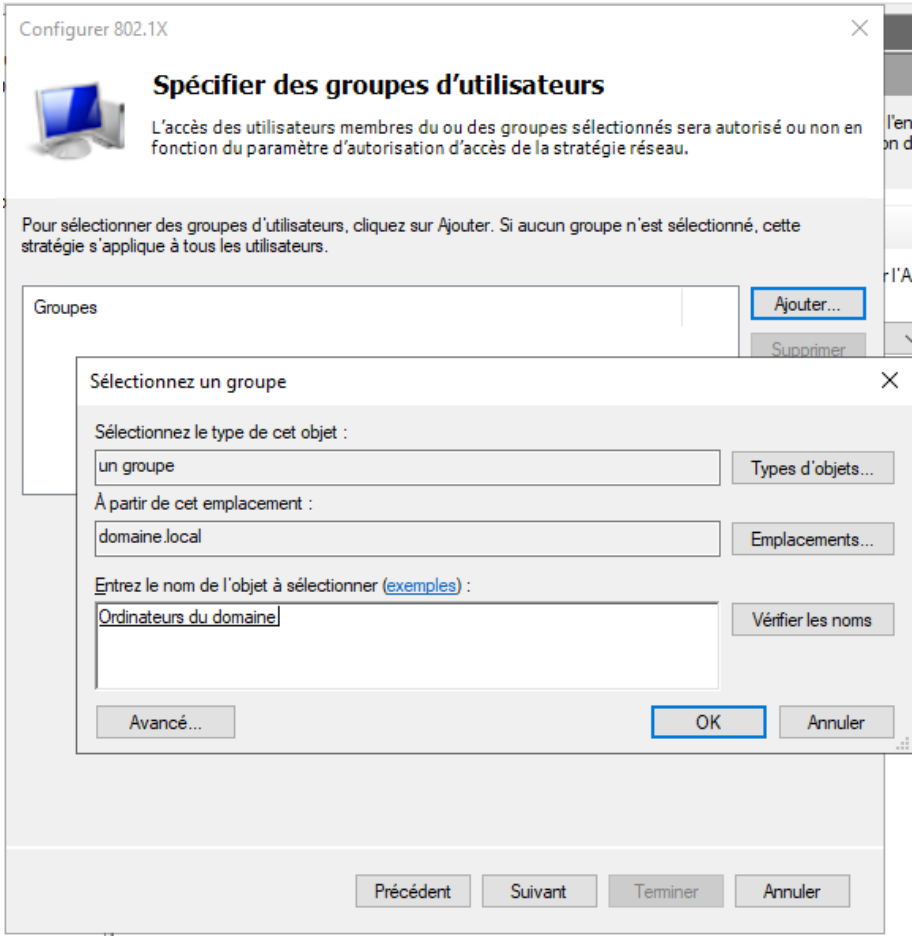




Cliquer sur « Configurer » le protocole PEAP



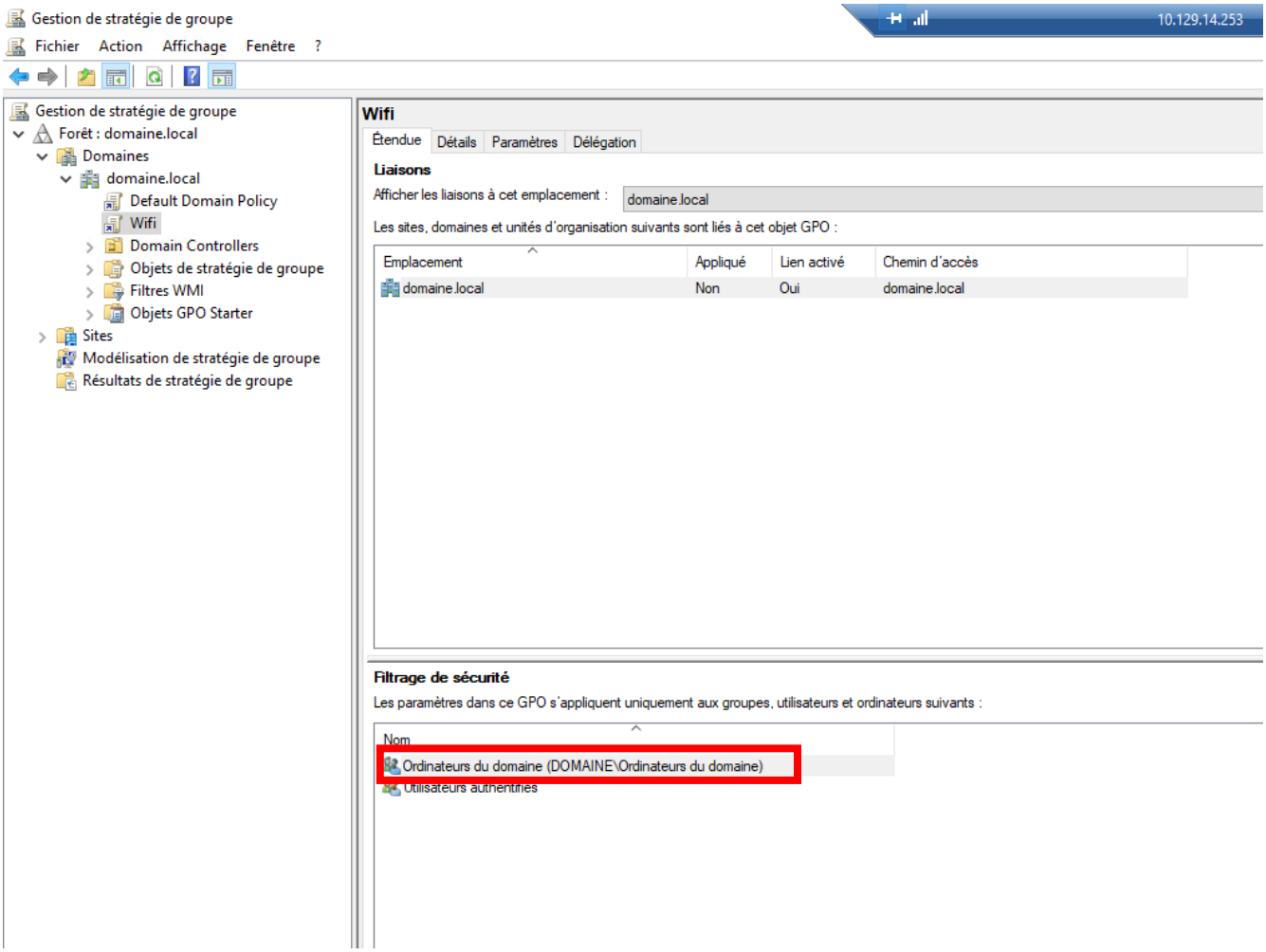
Sélectionner le certificat créé dans les étapes précédentes.



Ajouter un groupe, ici nous allons configurer une connexion pour tous les ordinateurs du domaine.
Vous pouvez maintenant cliquer sur « Suivant » jusqu'à pouvoir « Terminer »

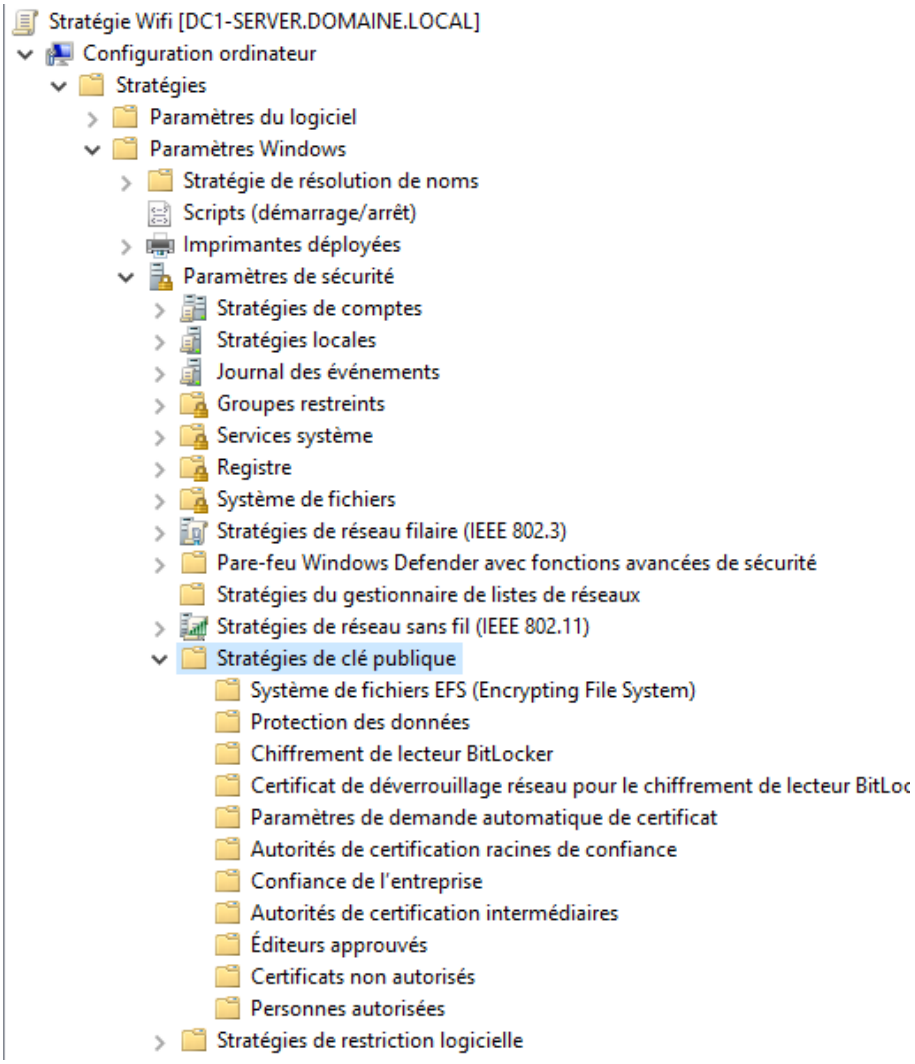
14. Création d'une GPO pour la gestion des certificats

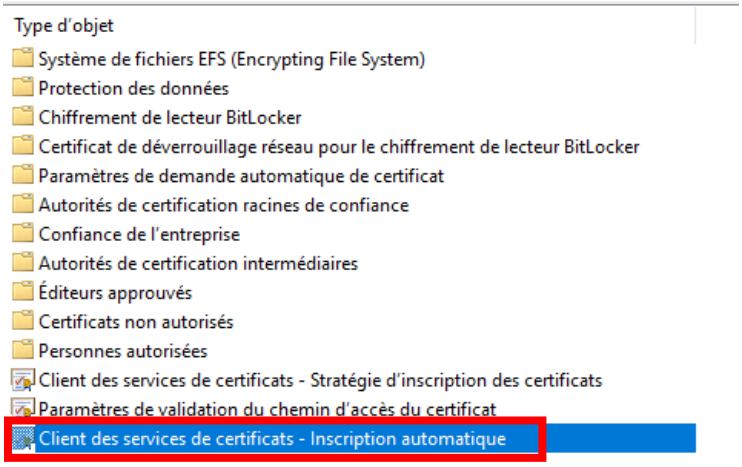
Dans « Gestion de stratégie de groupe », créer une nouvelle GPO qui affectera le groupe visé par la stratégie wifi :



Dans l' « Editeur de gestion des stratégies de groupe »

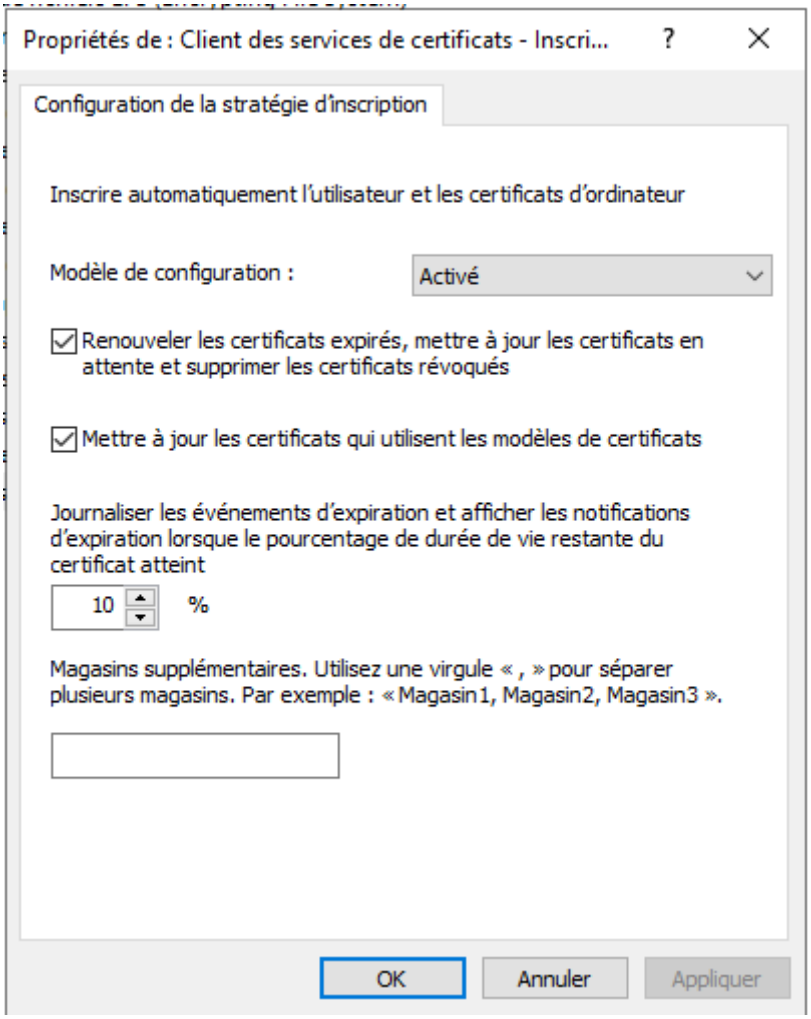
Sélectionner dans l'arborescence : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique



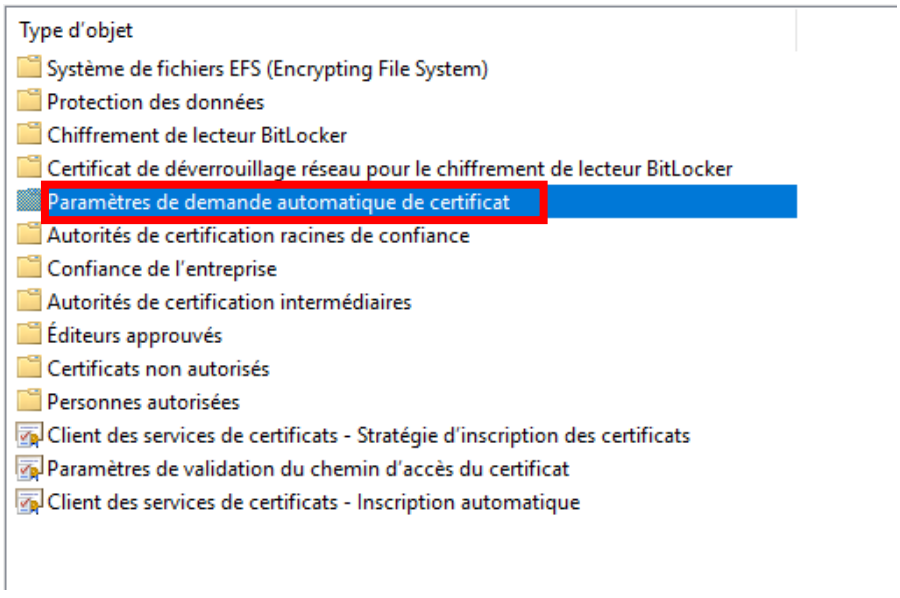


Configurer Client des services de certificats – Inscription automatique

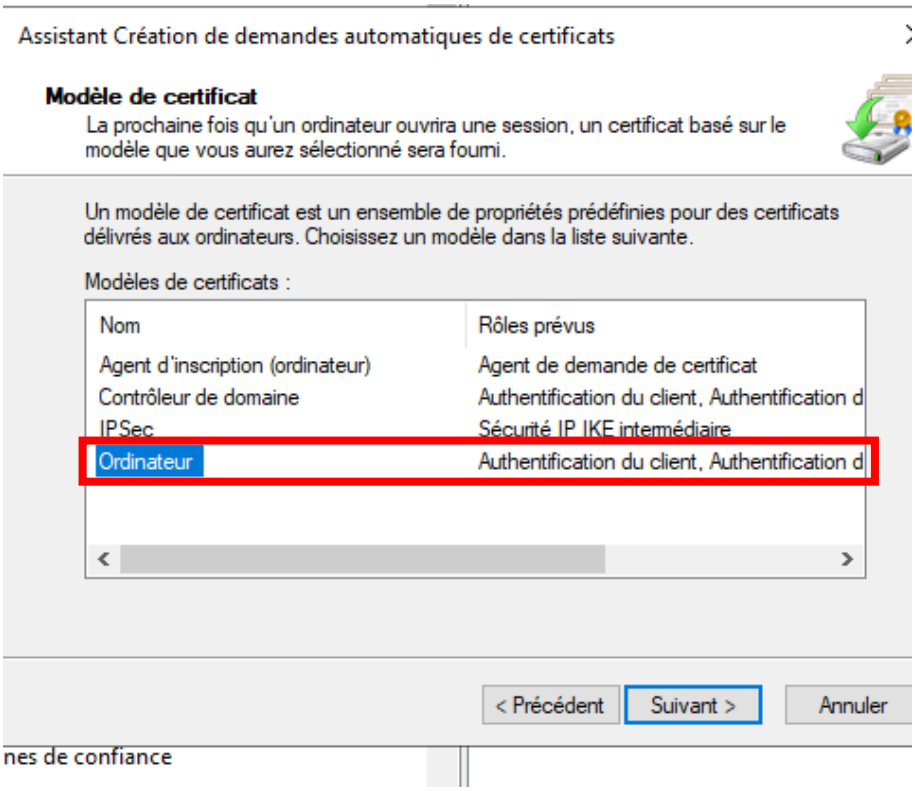
Comme ceci :



Puis sélectionner :



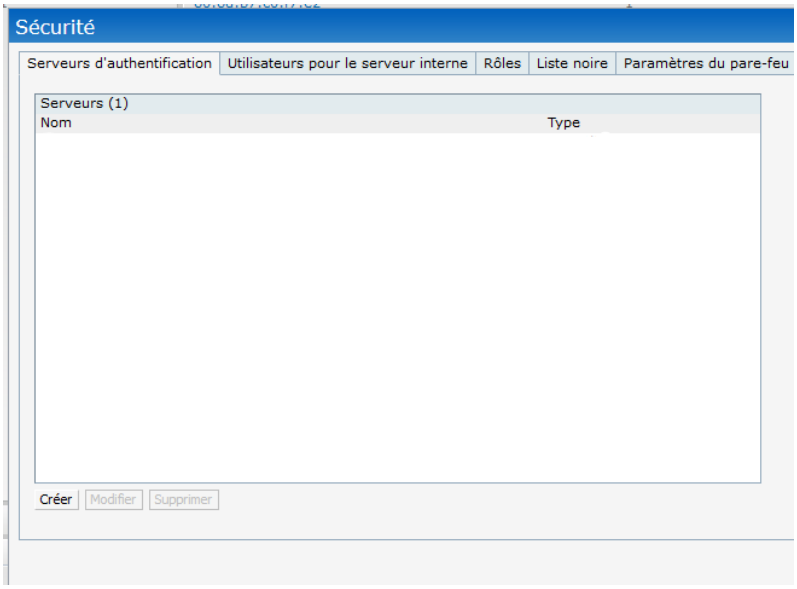
Clic droit > Nouveau > Demande automatique de certificat …



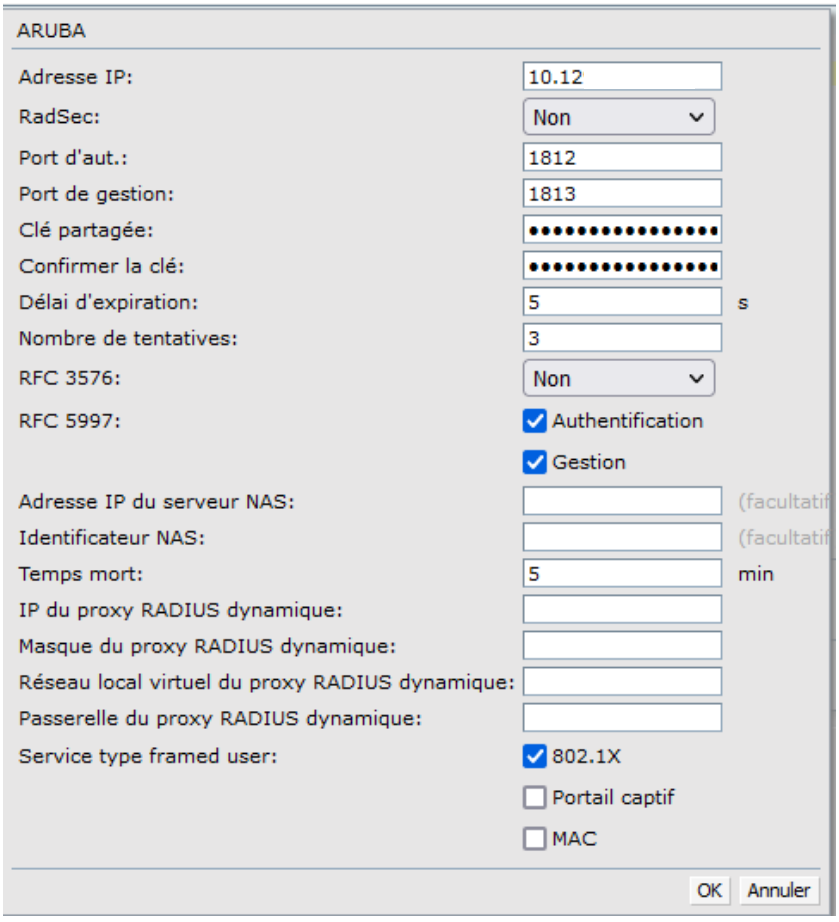
15. Configuration de la borne ARUBA

Se rendre sur la page configuration de la borne.

Puis se rendre dans Sécurité > Serveur d'authentification :



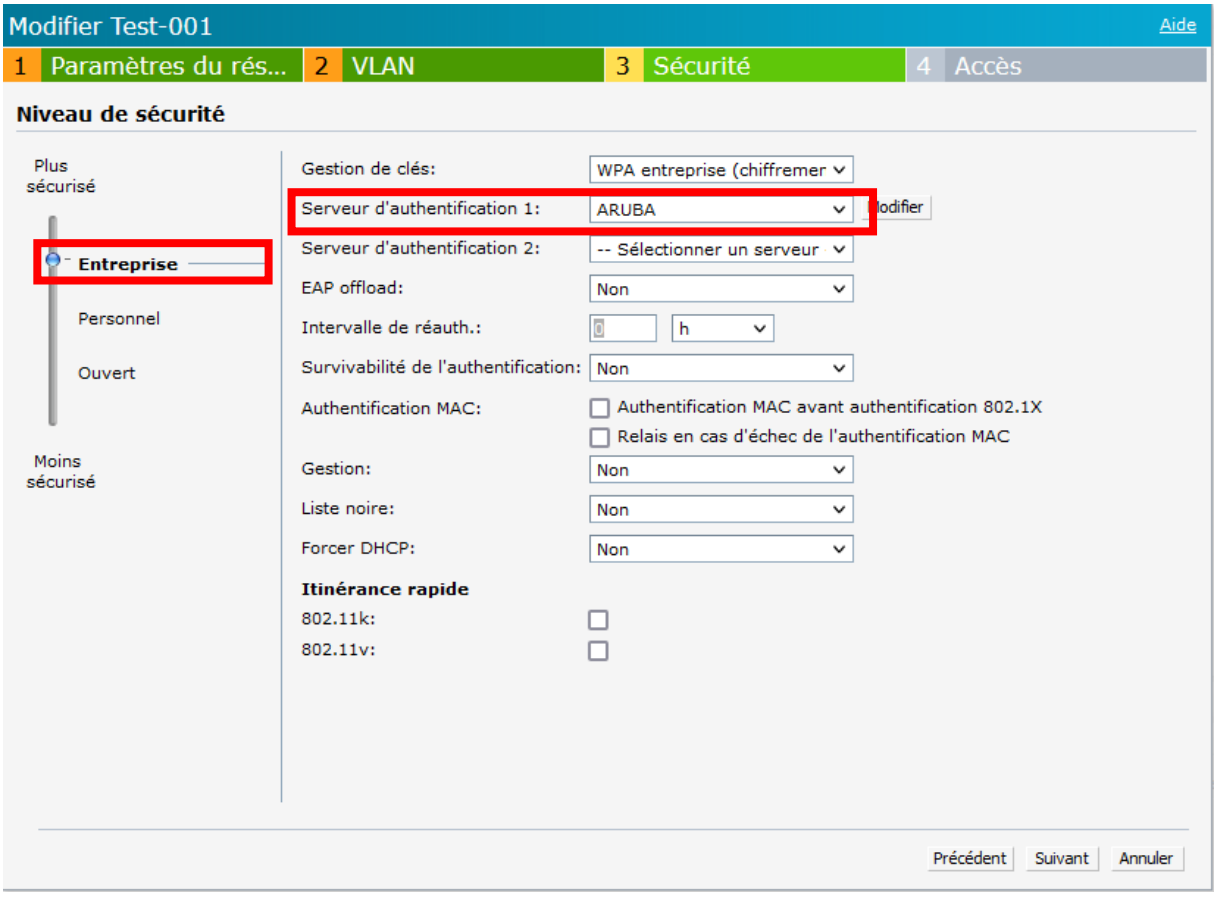
Et créer un serveur :



Indiquer l'adresse Ip du serveur NPS, la clé partager créée pendant la création du client Radius, puis valider.

Se rendre ensuite dans la configuration de son Réseau (Point d'accès), dans l'onglet Sécurité.

Il faut maintenant sélectionner entreprise dans le niveau de sécurité à droite :



Il faut sélectionner ici notre serveur d'authentification qui a été créé à l'étape précédente.

La configuration est terminée.

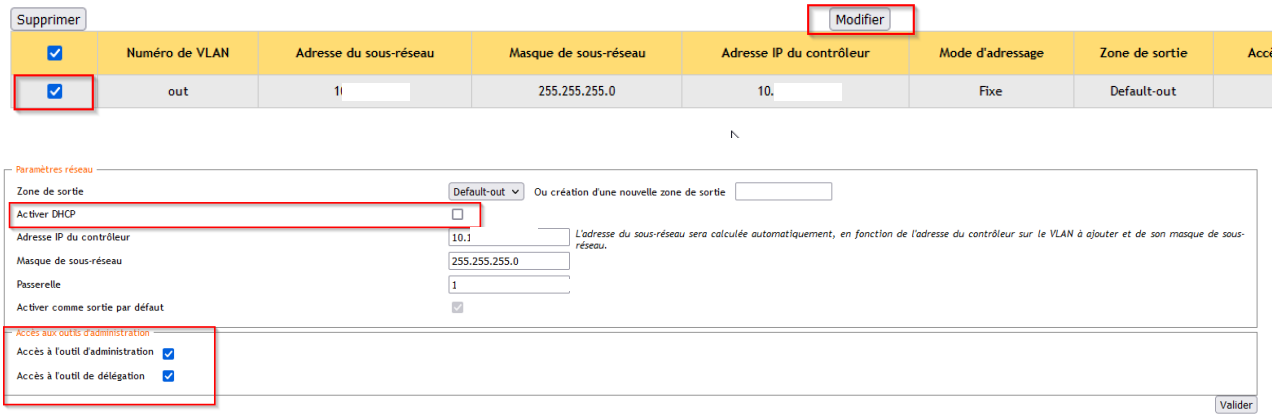
Annexe 3 : Configuration Ucopia Aruba en mode Out of Band architecture

1. Configuration réseau

La page de configuration est disponible à l'adresse : https://@Ip-ucopia/admin

1.1. Fixer l'adresse ip

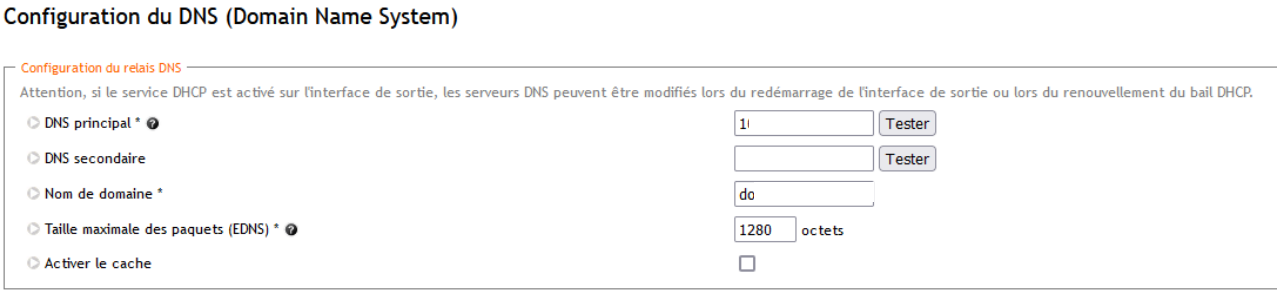
Se rendre dans Configuration > Réseau > Réseaux de sortie :



Ne pas cocher « Activer DHCP» et cocher les dernières cases comme ci-dessus.

1.2. Configuration du serveur DNS

Se rendre dans Configuration > Réseau > Serveur DNS :



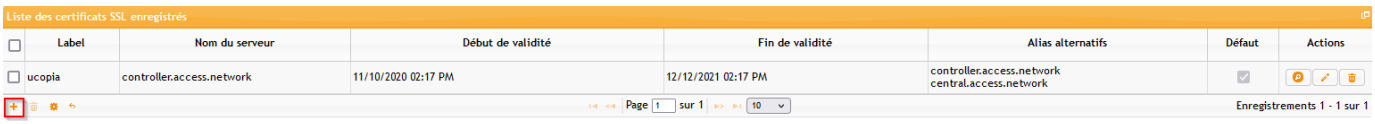
Renseigner les données relatives au DNS.

16. Authentification

1.3. Certificats

Si un certificat est à ajouter pour l'établissement de la connexion https entre le client et le Ucopia :

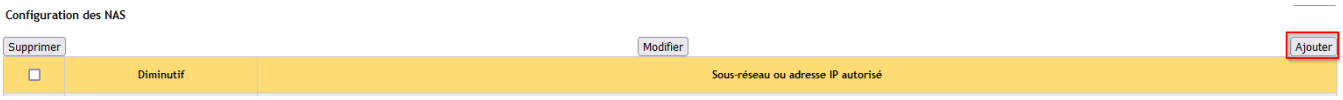
Se rendre dans Configuration > Authentification > Certificats :



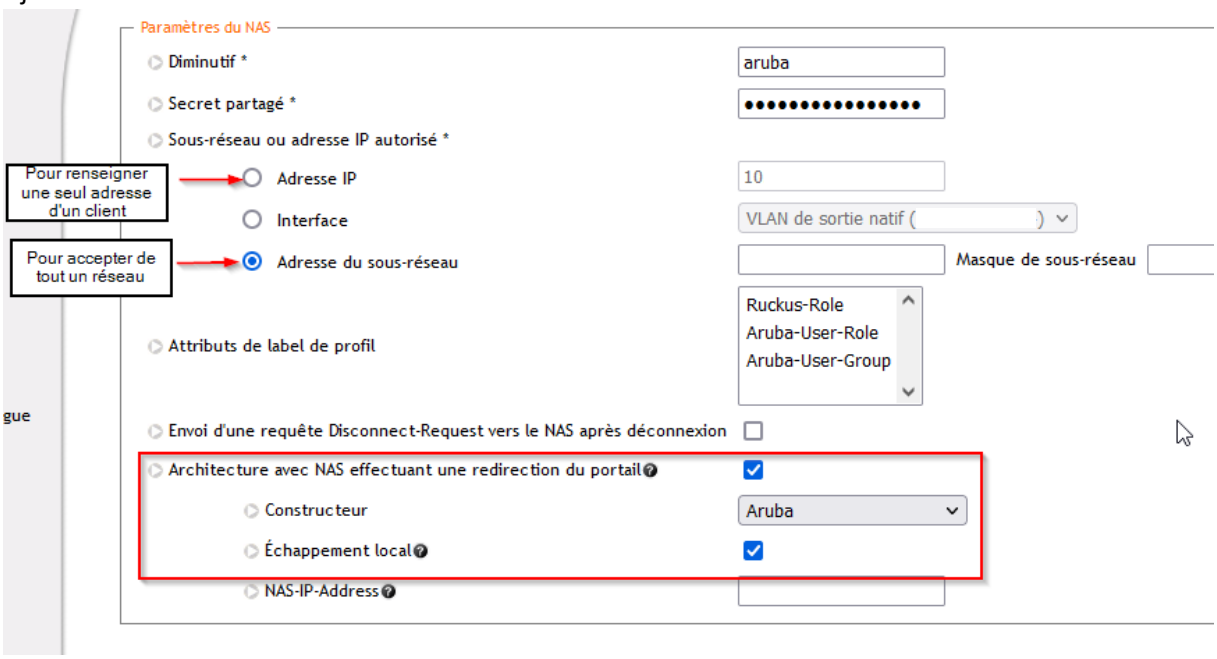
Et le définir par défaut.

1.4. Radius

Se rendre dans Configuration > Authentification > Radius



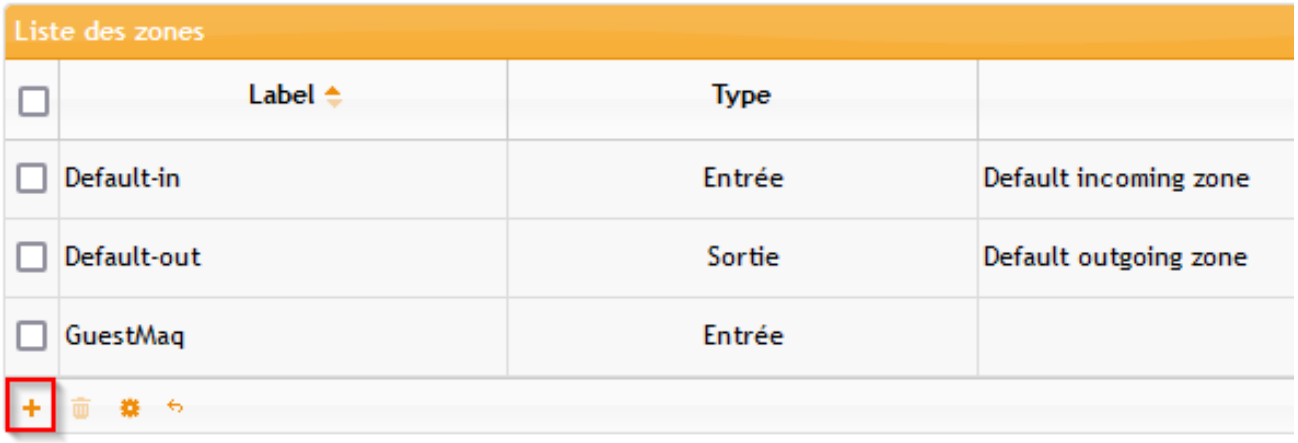
Ajouter un NAS



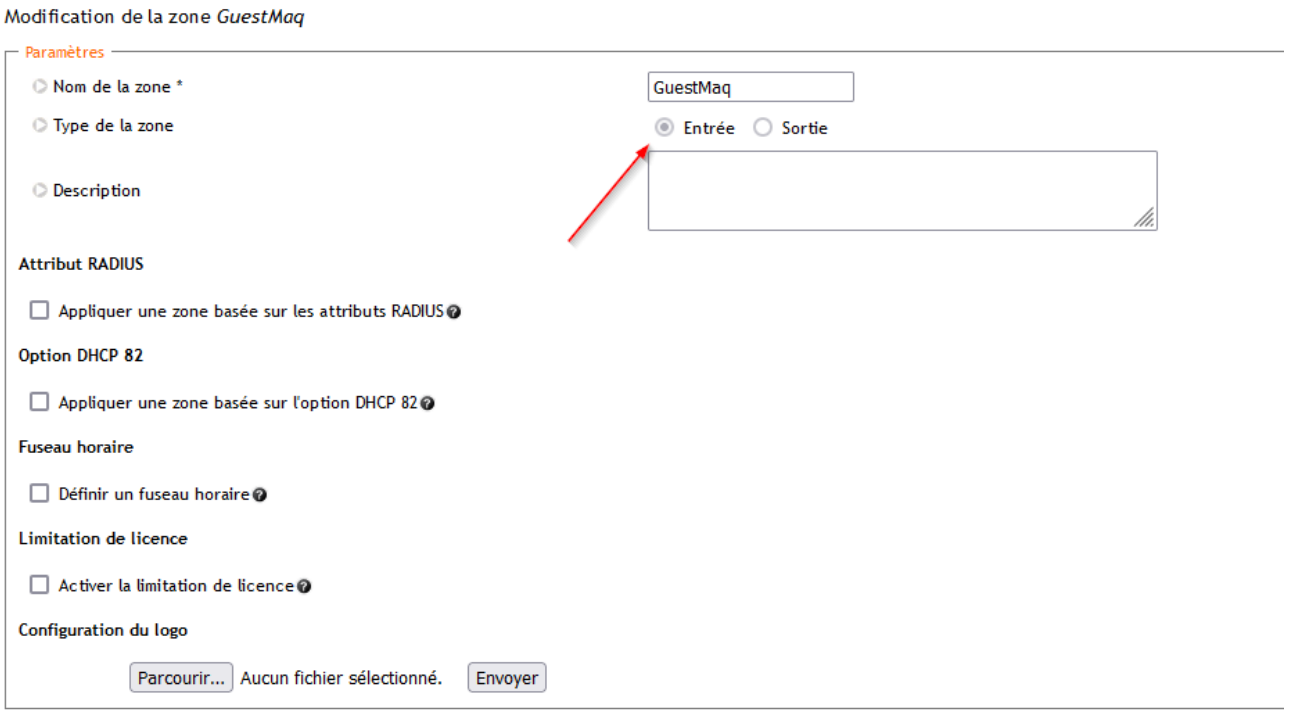
Renseigner les informations liées à la borne Aruba et créer un mot de passe partagé.

17. Création de zone :

Se rendre dans Administration > Politiques > Zones :



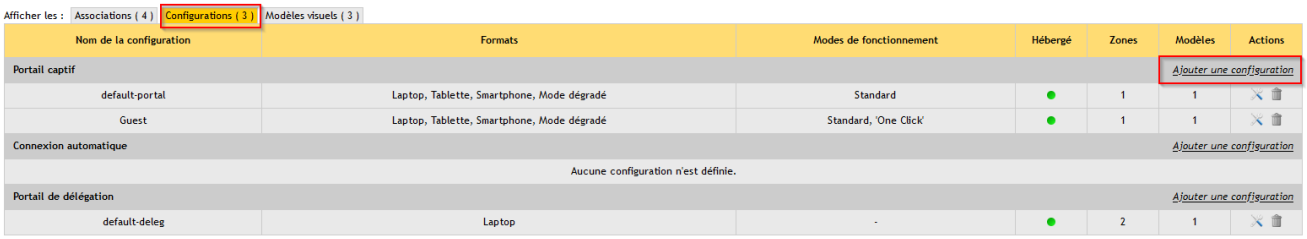
Créer une zone



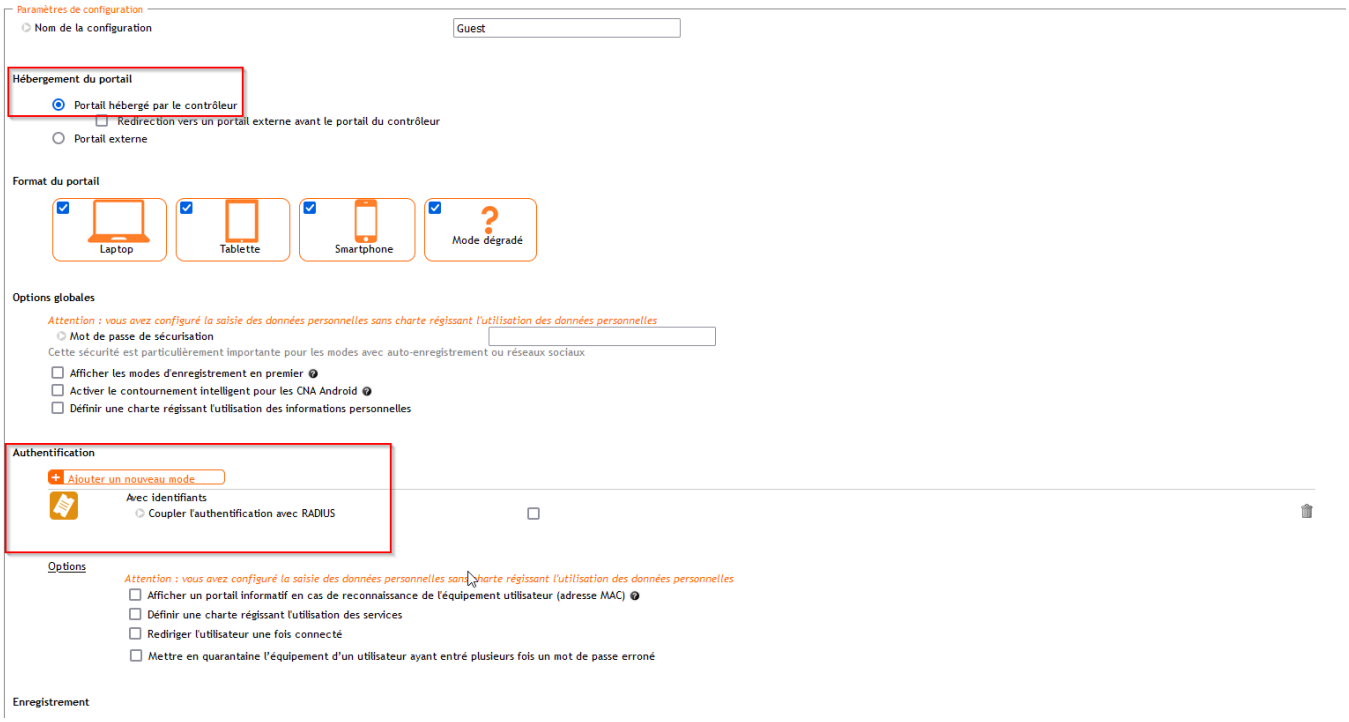
La définir comme zone d'entrée et lui donner un nom.

18. Portail captif

Se rendre dans Configuration > Personnalisation > Portails

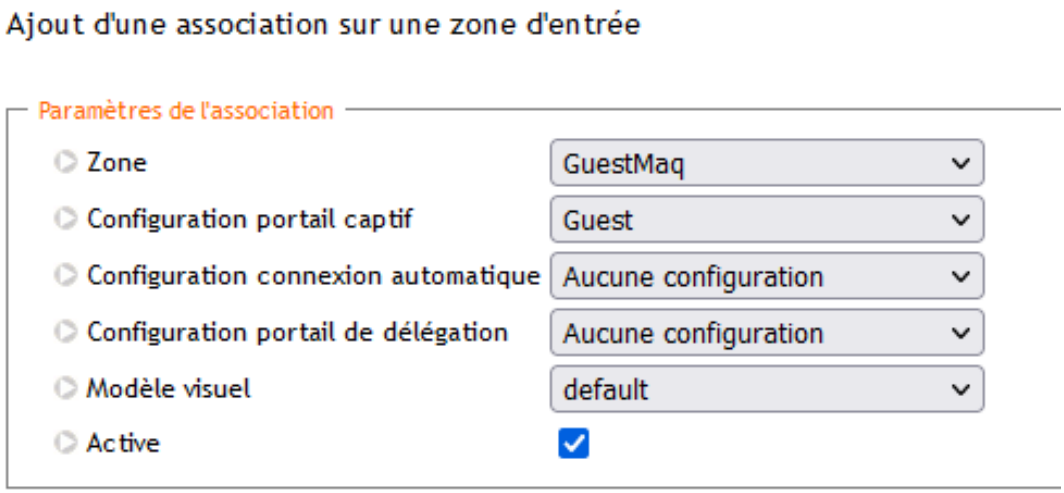


Sur configuration, ajouter une configuration. Cette configuration sera associée à la zone d'entrée.



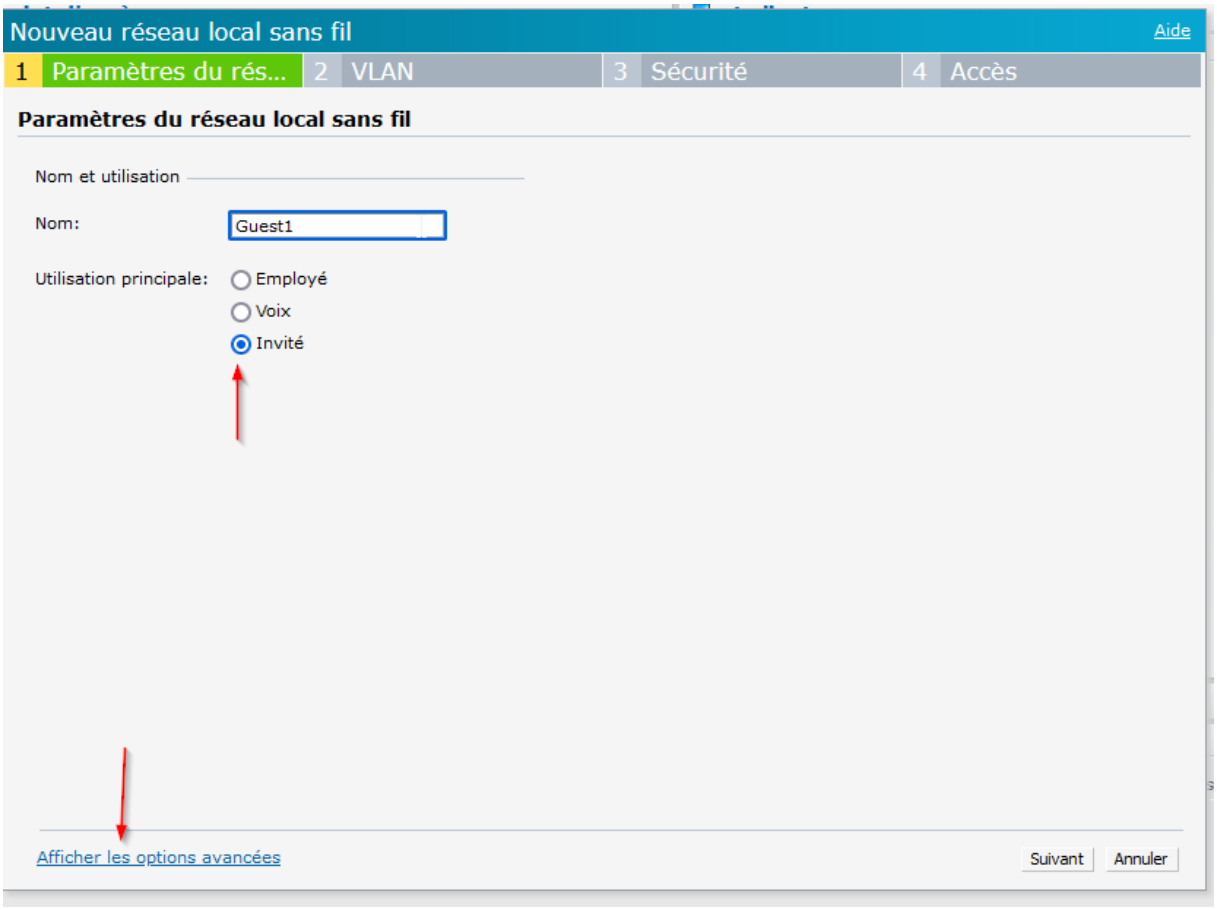
On peut ici choisir la méthode d'authentification et d'autres paramètres.

Maintenant on associe la configuration du portail à une zone

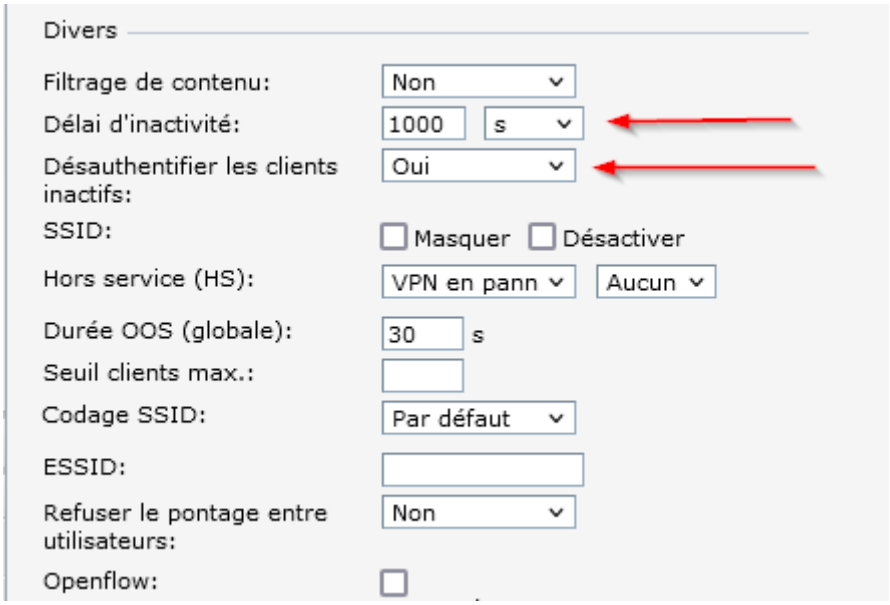


19. Configuration de la borne Aruba

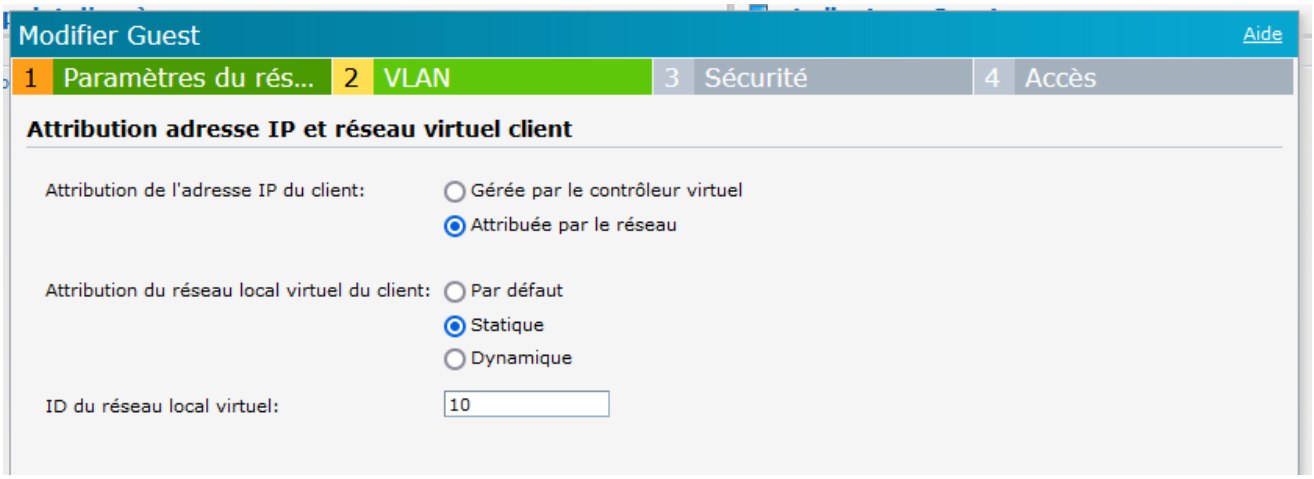
On ajoute un nouveau réseau local sans fil sur la borne.



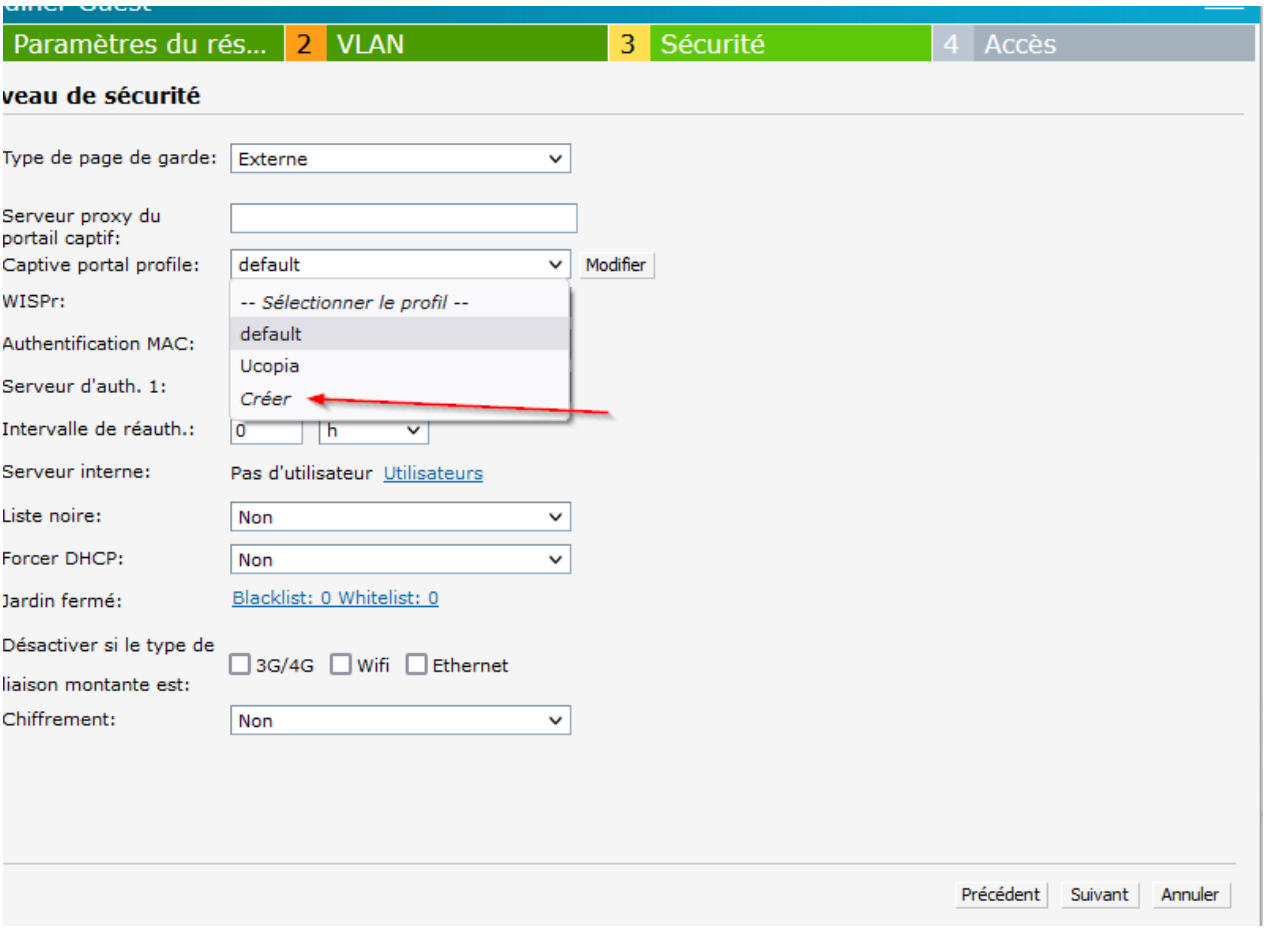
On peut sélectionner une période d'inactivité afin de déconnecter les clients inactifs.

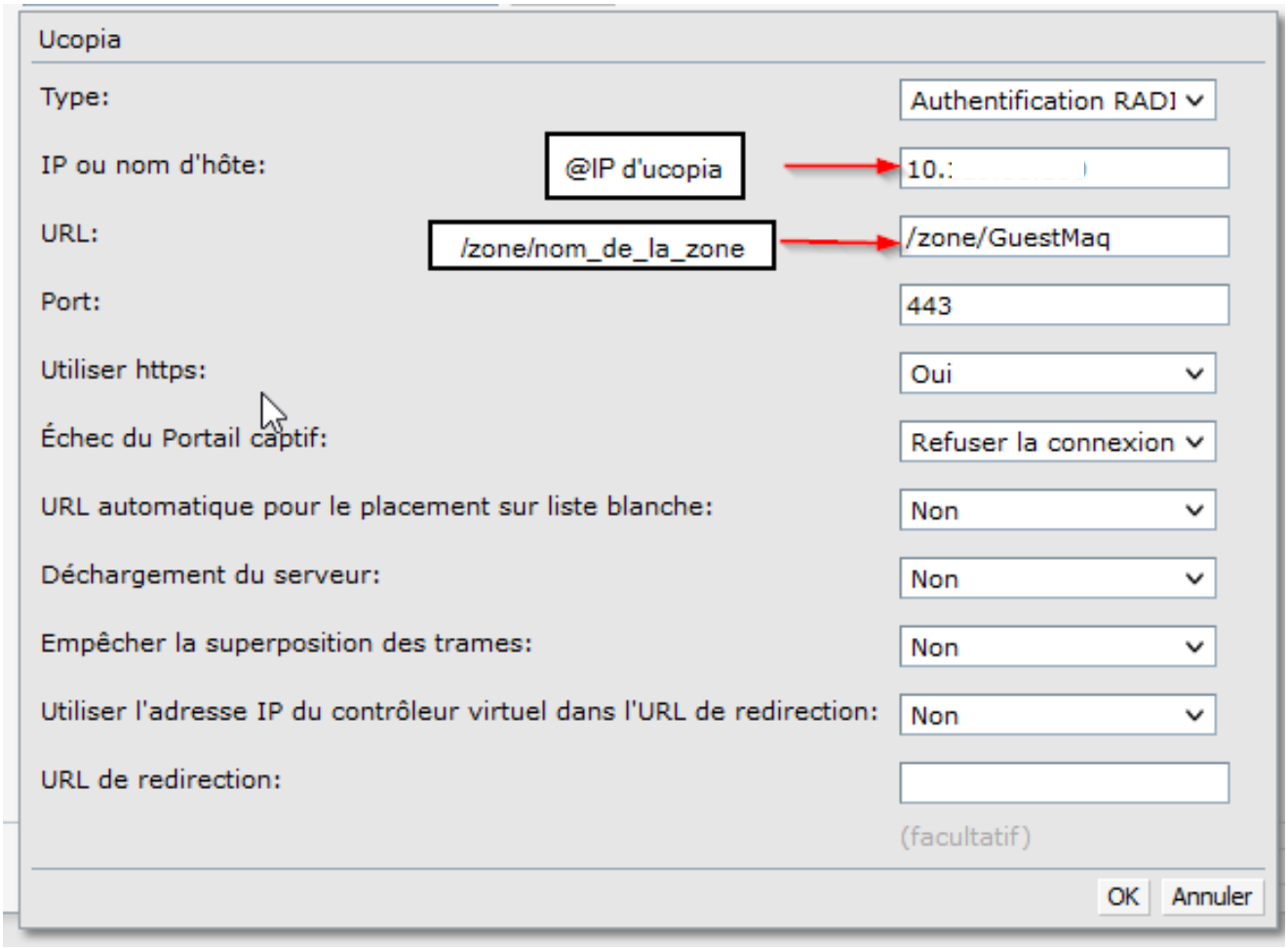


on sélectionne le vlan et la gestion de l'attribution d'adresse ip.



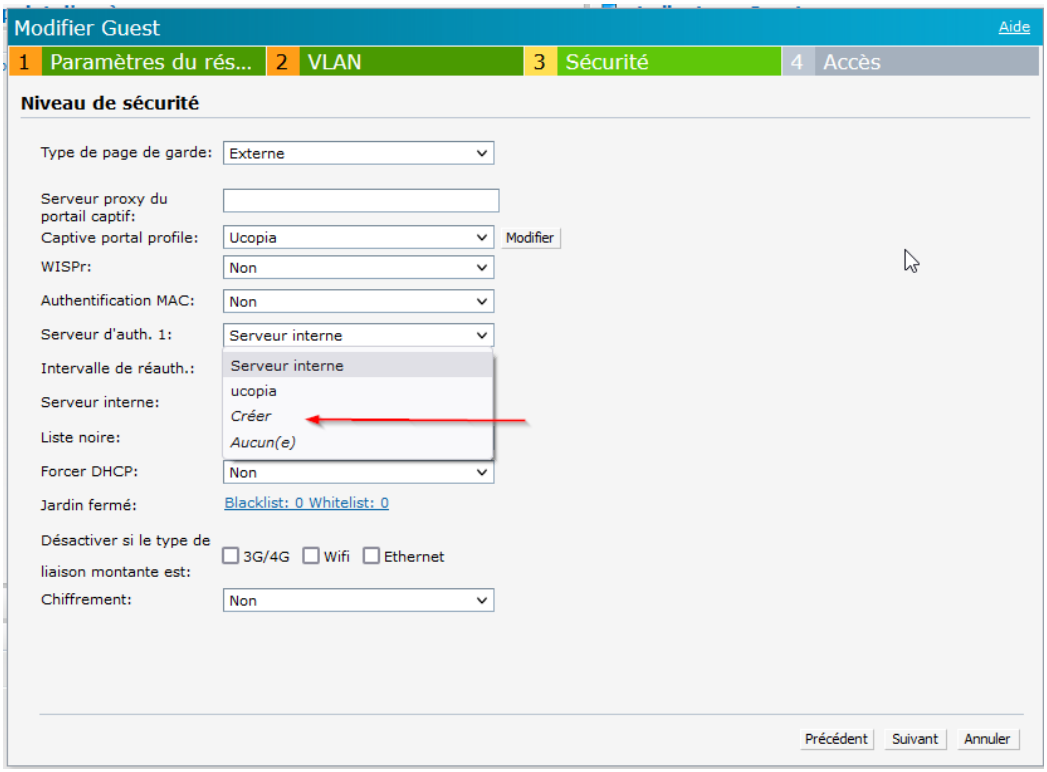
Ensuite on ajoute un profil pour le portail captif :

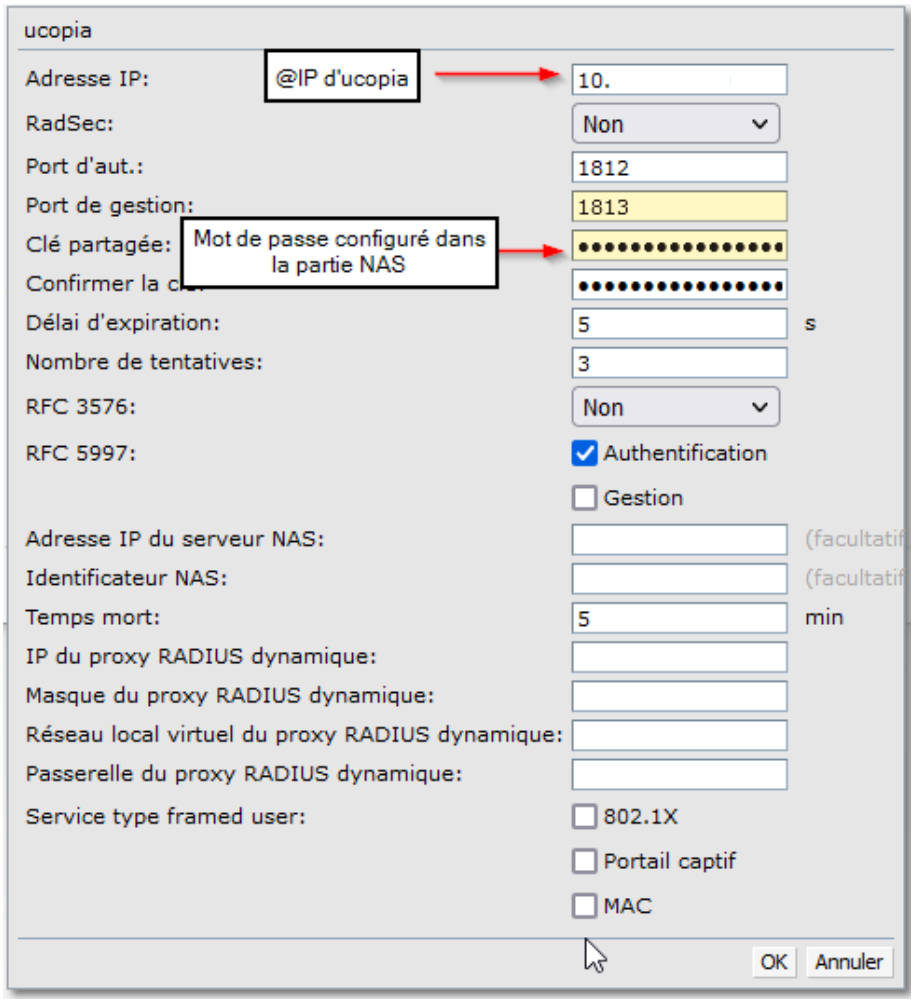


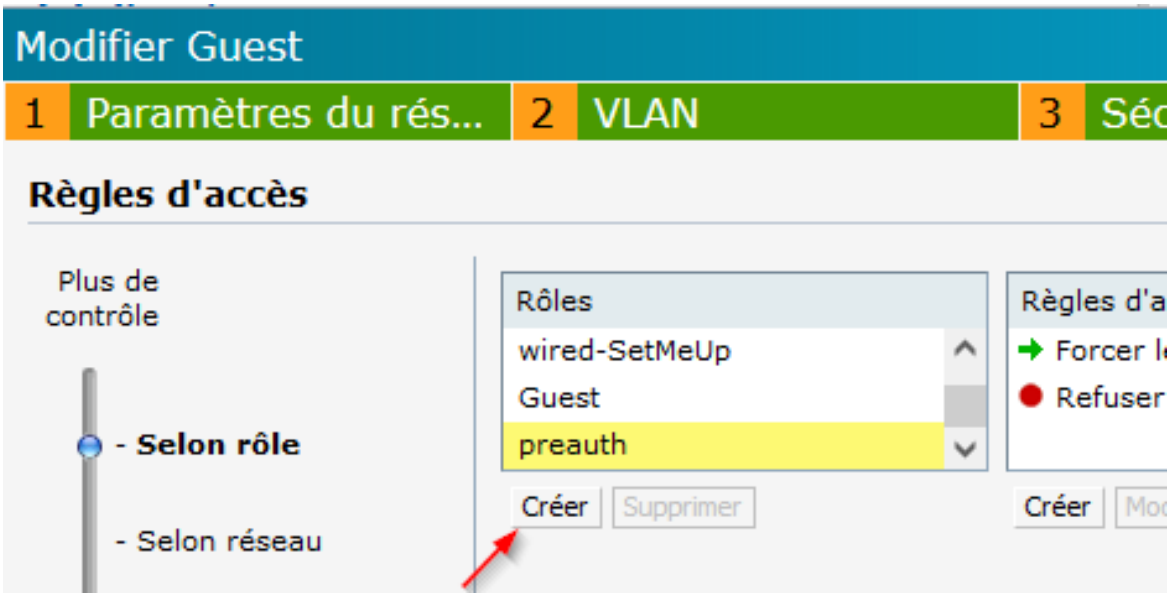


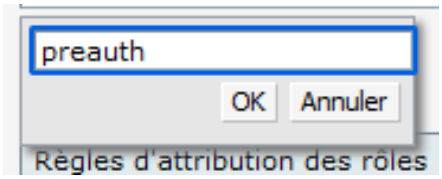
On spécifie l'adresse ip d'ucopia le nom de l'url et le type d'authentification.

On ajoute un serveur d'authentification

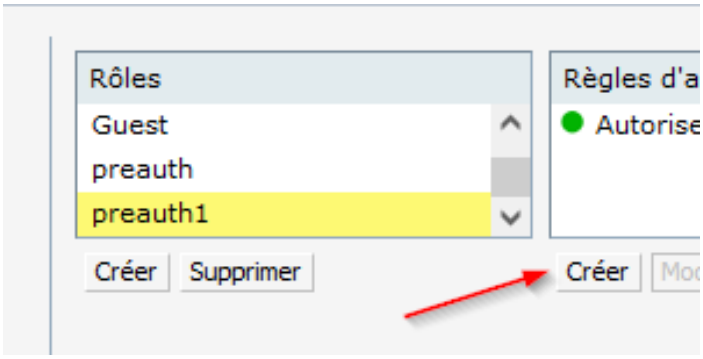


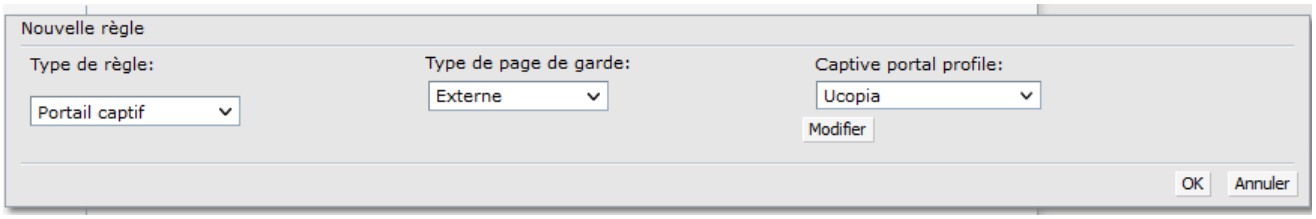


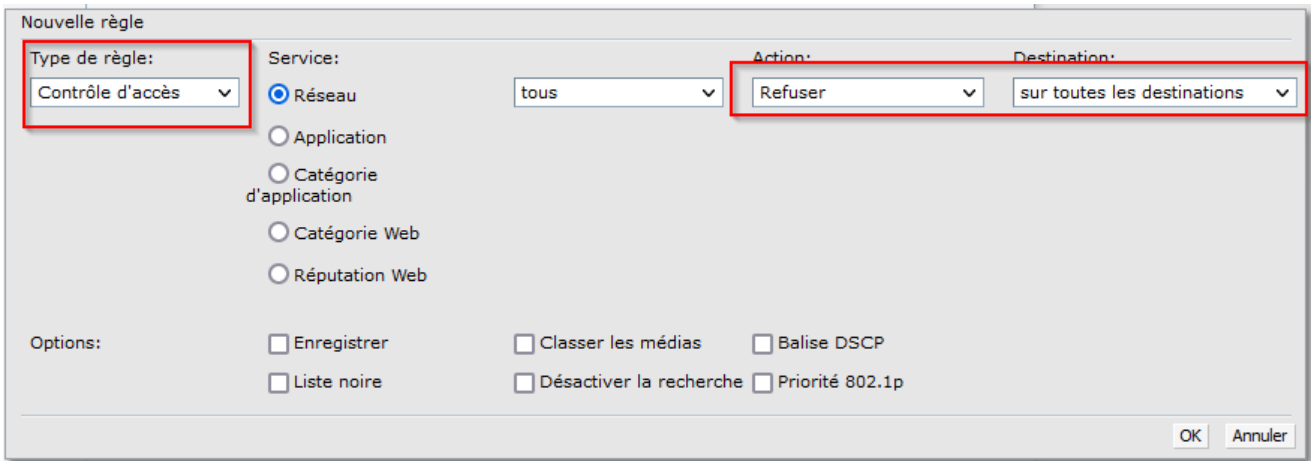


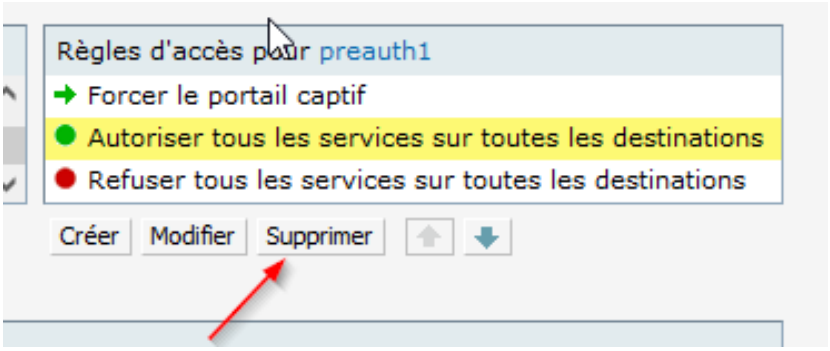


On ajoute un profil pour placer les clients avant l'authentification.

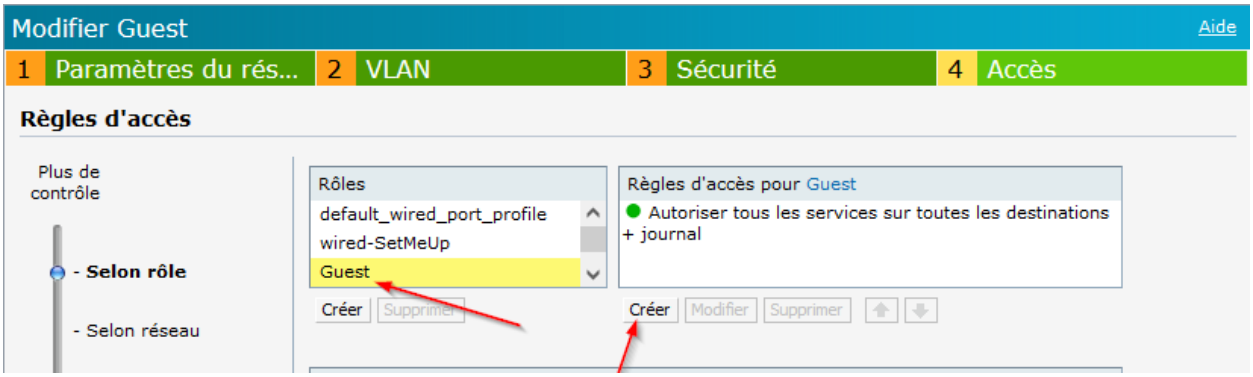




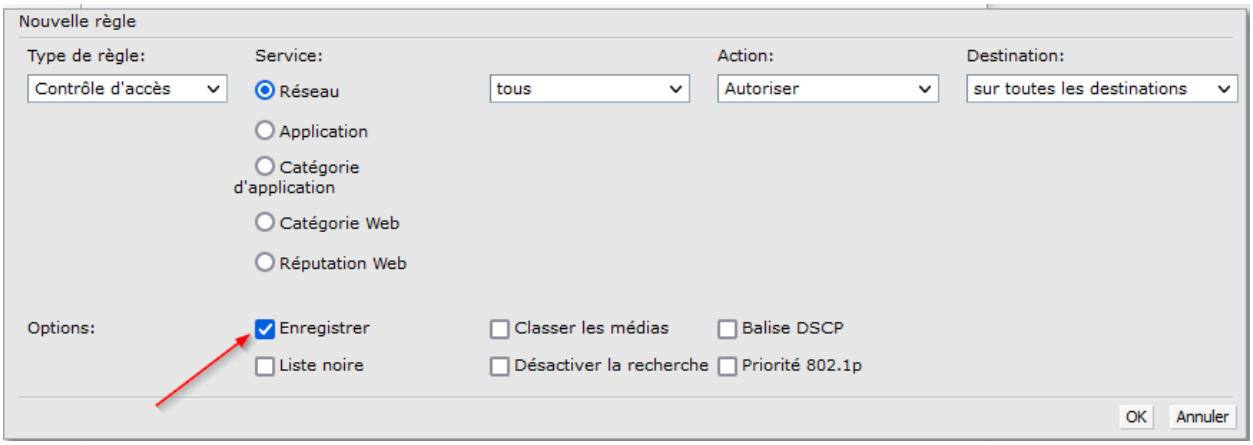


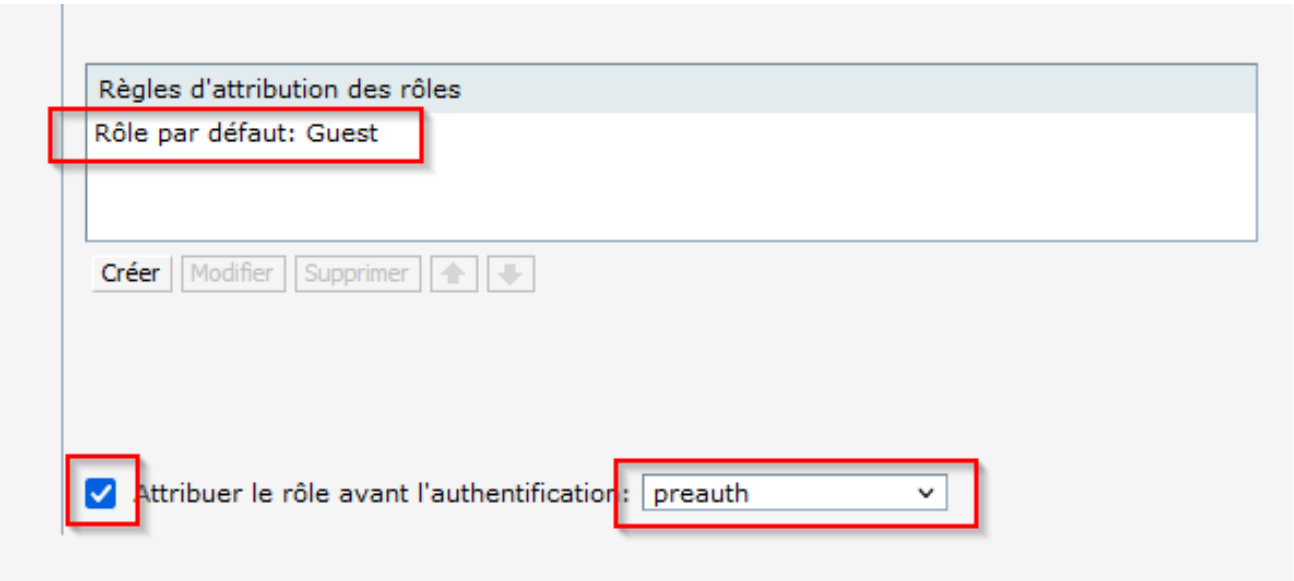


On enlève tous les droits afin que le client ne puisse pas naviguer avant de s'être authentifié.



On ajoute la journalisation au profil par défaut afin de pouvoir suivre les logs.

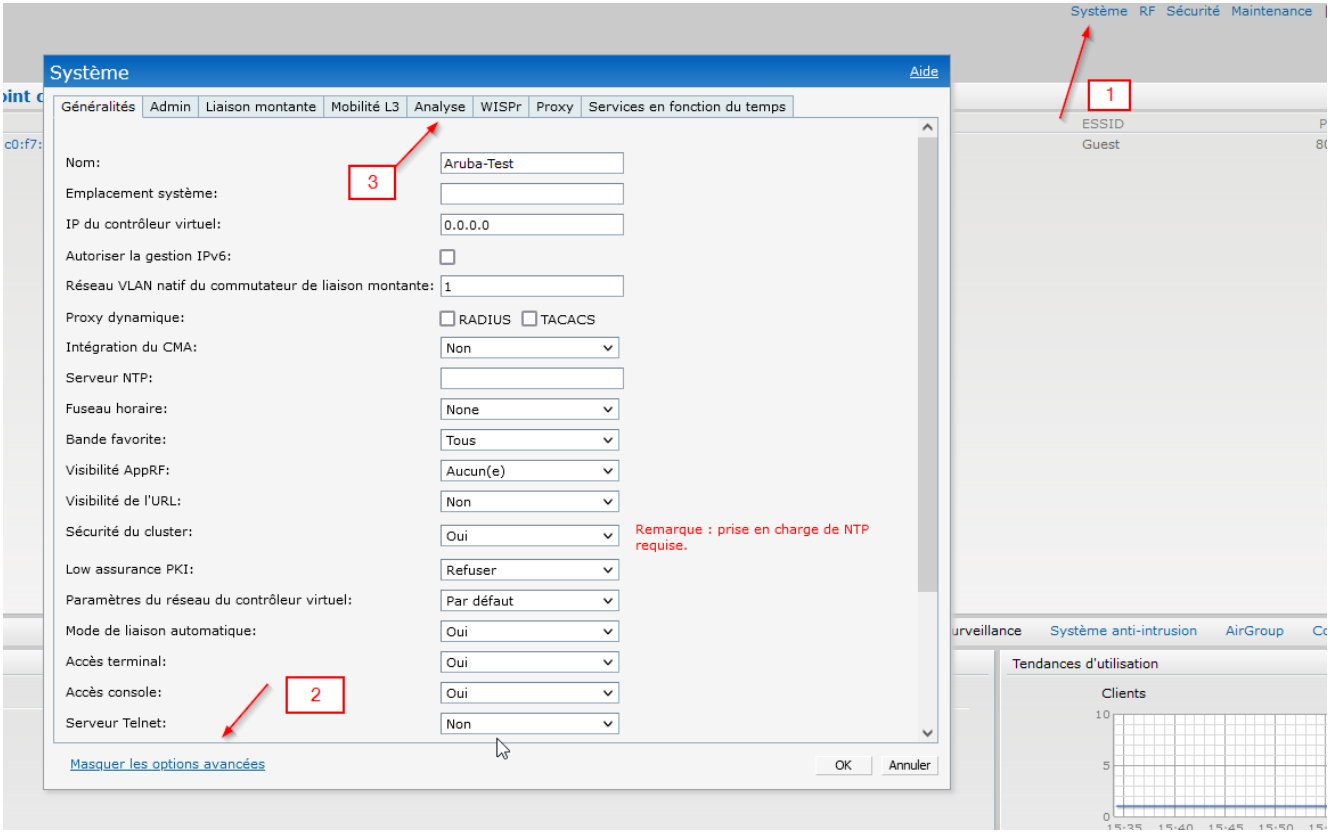


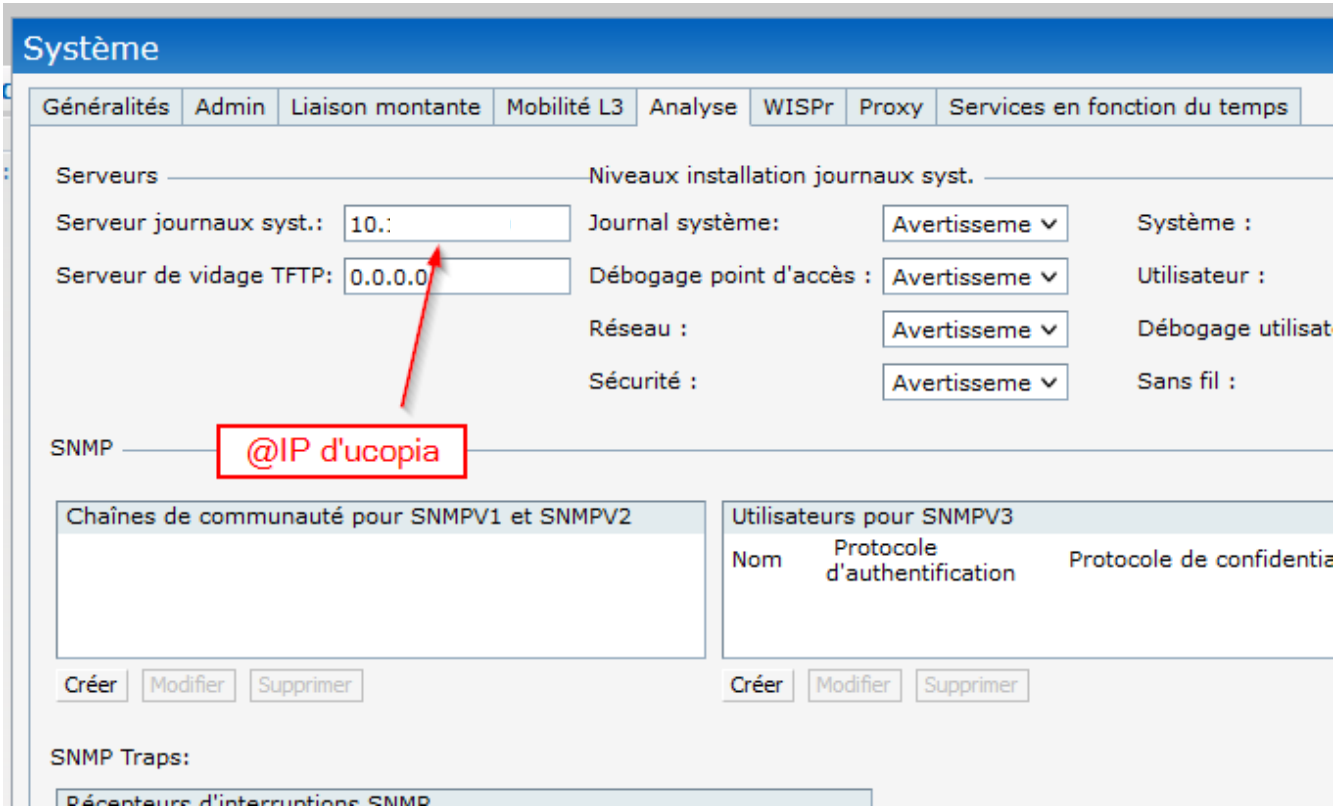


On définit le rôle avant l'authentification.

20. Configuration du serveur Syslog

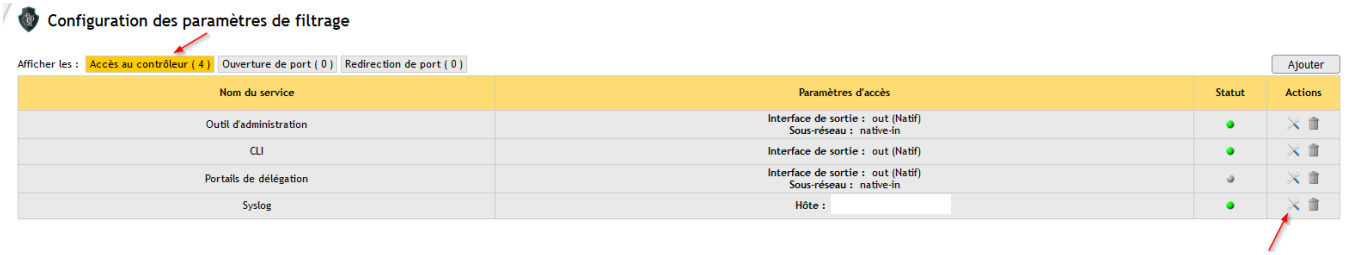
Sur la borne Aruba

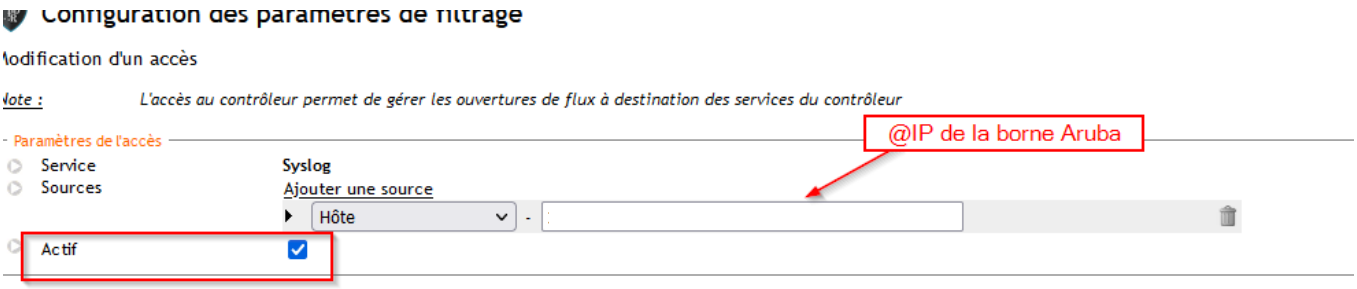




Sur l'UCOPIA :

Se rendre sur Configuration > Réseau > Filtrage :

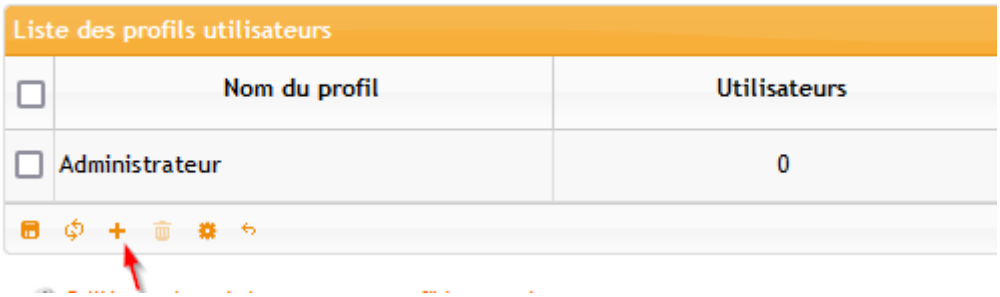




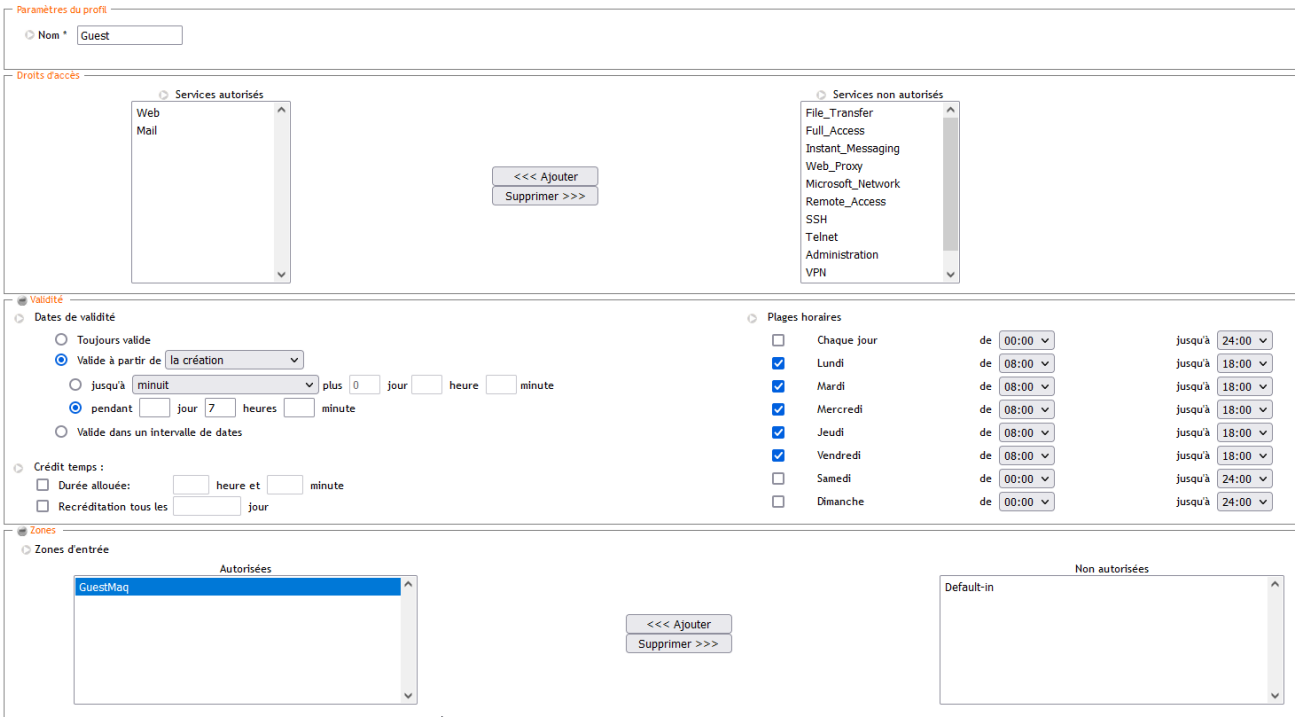
On renseigne l'adresse de la borne Aruba.

21. Création des comptes utilisateurs

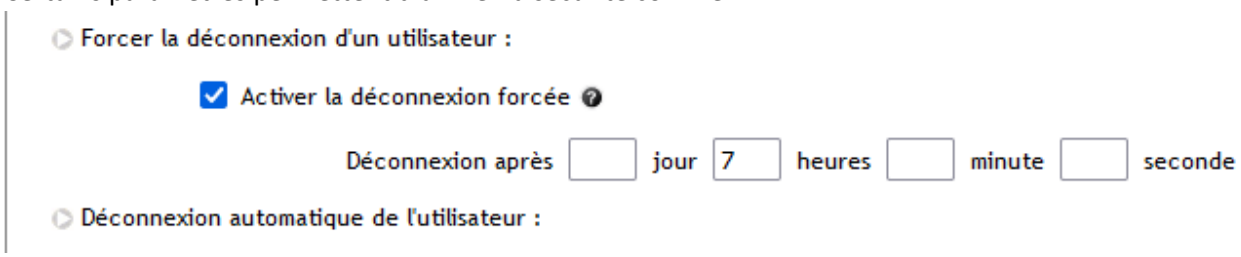
Dans Administration > Utilisateurs > Profils



Dans notre exemple nous allons créer un profil pour les invités :



Certains paramètres permettent d'affiner la sécurité comme :

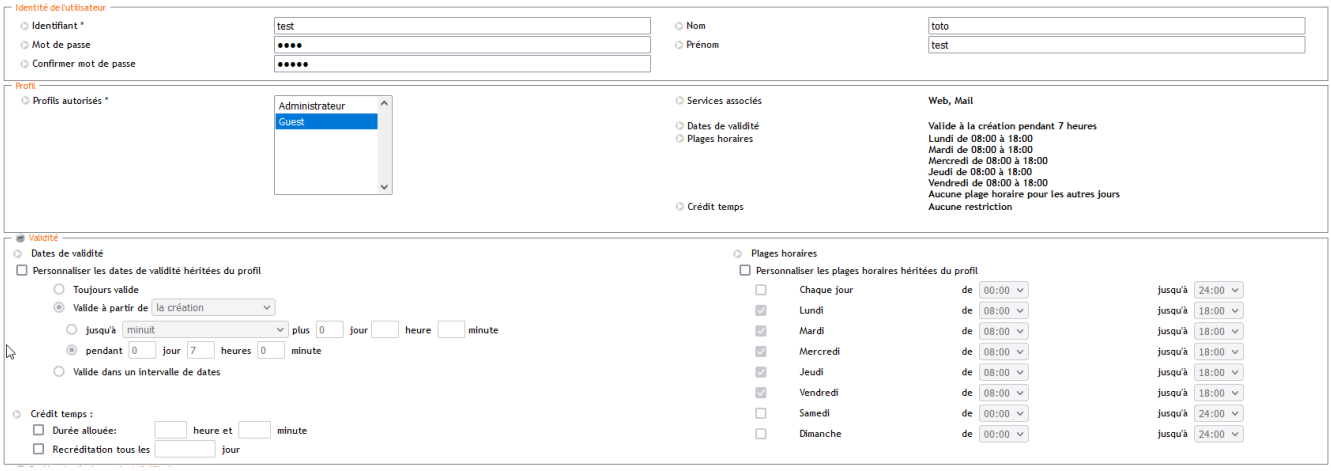


Une fois le profil créé il y a deux façons de créer des comptes :

- Directement depuis l'espace d'administration (admin)
- Depuis un espace dédié (standardiste, etc…)

21.1. Création pour un admin

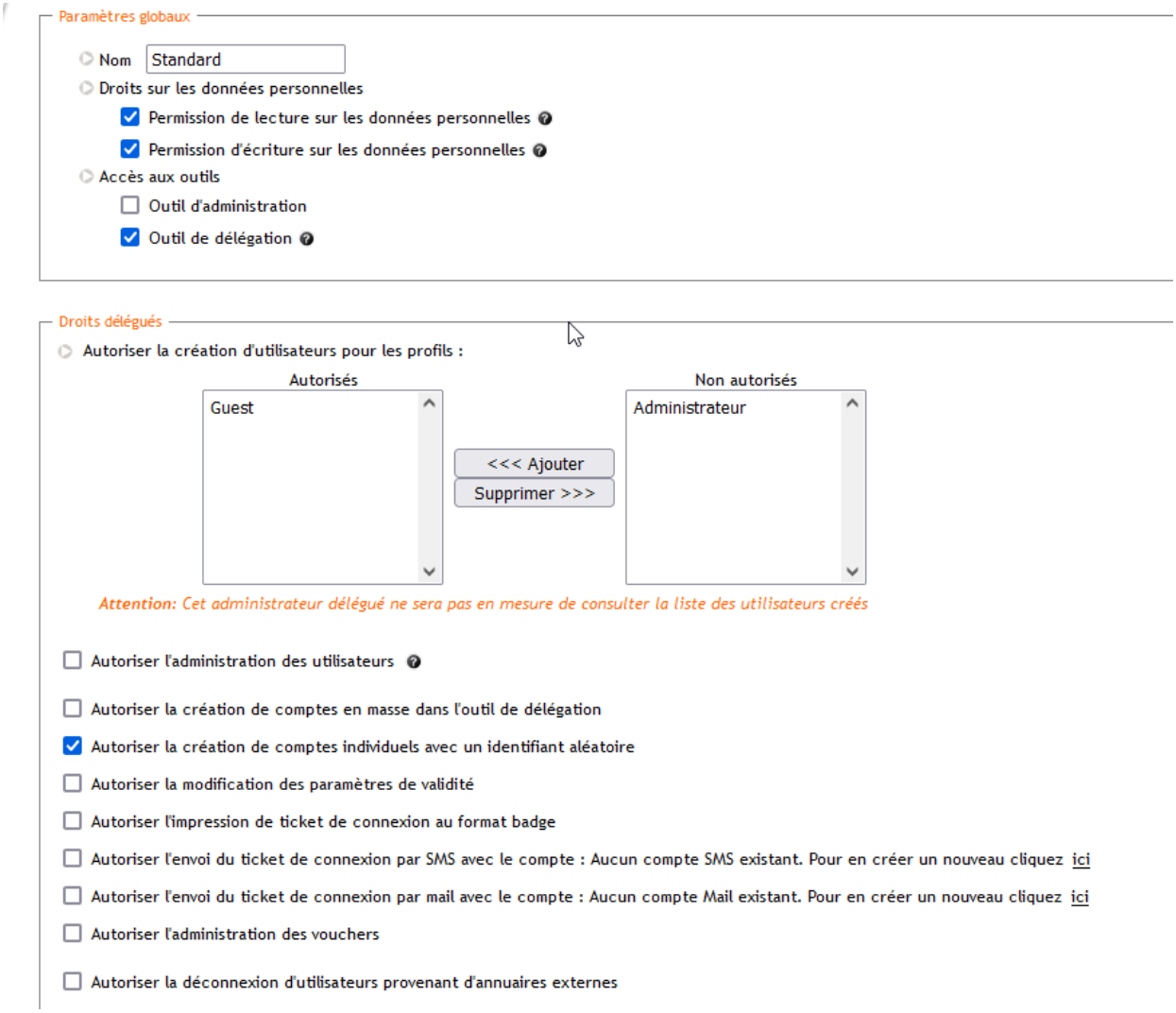
Se rendre dans Administration > Utilisateurs > Comptes :



Remplir les champs nécessaires.

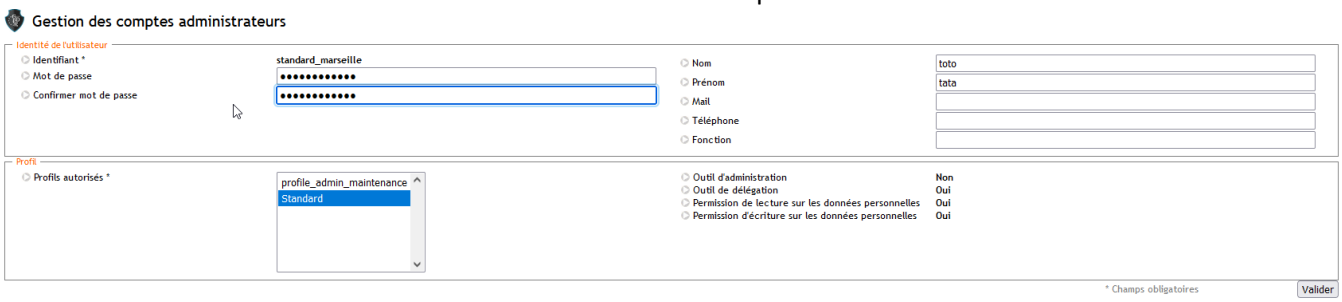
21.2. Création pour un standardiste

Se rendre dans Administration > Administrateurs >Profils



Créer un profil.

Ensuite se rendre dans Administration > Administrateurs > Comptes



Indiquer les informations relatives à la personne concernée.

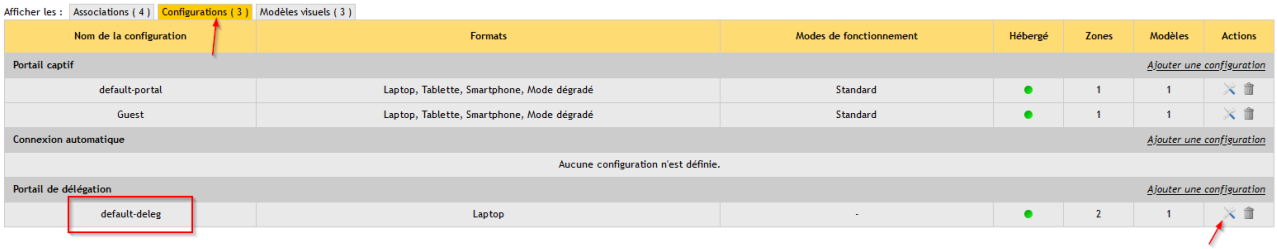
Espace dédié

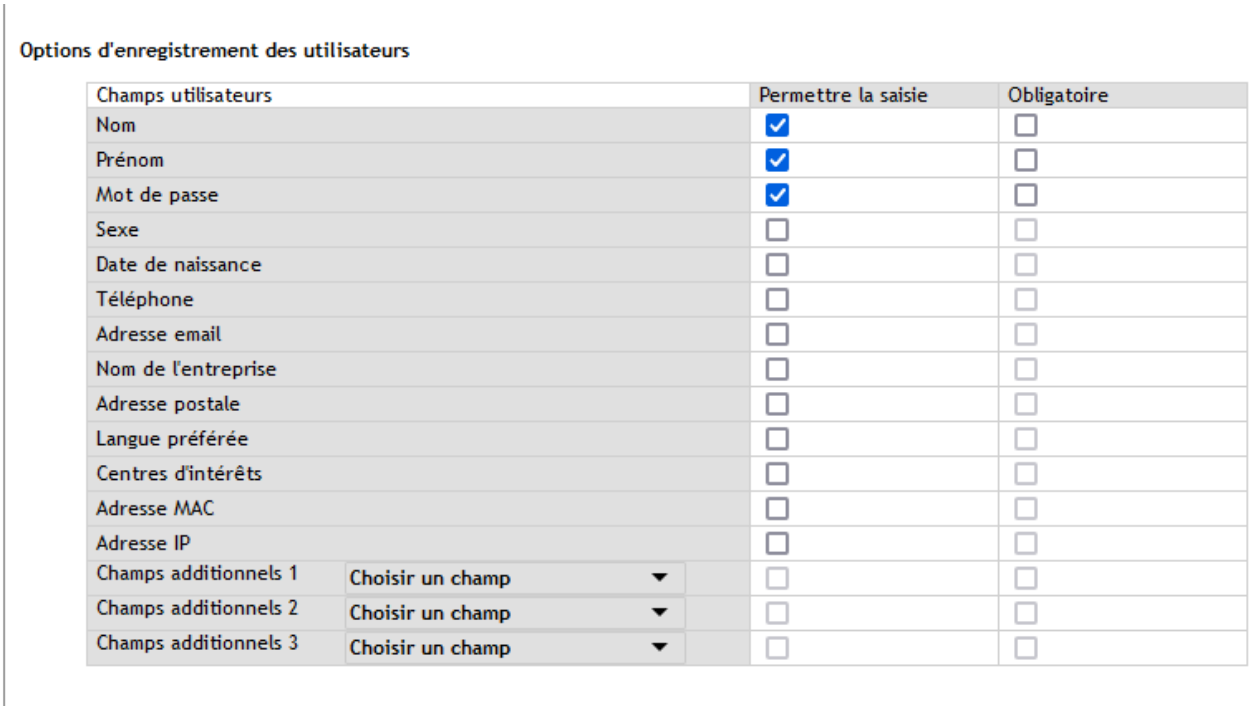
Se rendre à l'adresse https://@ip_ucopia/deleg

Nous pouvons maintenant créer un profil.

Pour personnaliser les infos demandées au standardiste pendant la création d'un compte invité :

se rendre dans Configuration > Personnalisation > Portails :





Choisir les options désirées.