

**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/Asterisk18.....	3
1. Installation d'une VM sur ESXi	3
1.1. Gestion des réseaux	3
1.2. Création de la Vm	4
2. Installation Asterisk 18	6
2.1. Etape 1 : Mettre à jour le système	6
2.2. Etape 2 : Ajouter le Dépôts EPEL.....	6
2.3. Etape 3 : Installer Development Tools	6
2.4. Etape 4 : Télécharger et installer Janson :.....	6
2.5. Etape 5 : Télécharger et installer PJSIP	7
2.6. Etape 6 : Télécharger et installer Asterisk 18.....	7
2.7. Etape 7 : Configuration finale et démarrage d'Asterisk	11
3. Installation de FreePBX 15.....	12
3.1. Installation des dépendances.....	12
3.2. Installation de php7.2 :.....	12
3.3. Installation de nodejs :	12
3.4. Activation et démarrage de MariaDB :.....	13
3.5. Démarrage de Apache :.....	13
3.6. Installation et configuration de FreePBX.....	13
4. Administration et installation des téléphones ip à travers FreePBX.....	14
5. Convertir une configuration SIP en PJSIP	15
5.1. Exporter la configuration de l'ancien serveur	15
5.2. Importer la configuration sur le nouveau serveur :	16
5.3. Conversion des profils	16
6. Configurer un Trunk pjsip.....	17
7. Configuration du switch pour le voice vlan.....	19
Annexe 2 : Mise en place d'une authentification par AD aux bornes wifi Aruba.	23
8. AD CS	23
9. Installation du rôle	23
10. Configuration du rôle	25
11. NPS (Serveur Radius).....	30
12. Ajout du rôle.....	30
13. Configuration du serveur radius.....	31
14. Création d'une GPO pour la gestion des certificats	35

15.	Configuration de la borne ARUBA	39
Annexe 3 : Configuration Ucopia Aruba en mode Out of Band architecture.....		42
1.	Configuration réseau	42
1.1.	Fixer l'adresse ip.....	42
1.2.	Configuration du serveur DNS.....	42
16.	Authentification.....	42
1.3.	Certificats.....	42
1.4.	Radius	43
17.	Création de zone :	43
18.	Portail captif	44
19.	Configuration de la borne Aruba.....	46
20.	Configuration du serveur Syslog.....	52
21.	Création des comptes utilisateurs.....	54
21.1.	Création pour un admin	55
21.2.	Création pour un standardiste	55

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.

Ajouter un commutateur virtuel standard - Switch_vm

Ajouter une liaison montante

Nom du vSwitch	Switch_vm
MTU	1500
Liaison montante 1	vmnic2 - Actif, 100 mbps
▸ Découverte de liaison	Cliquez pour développer
▸ Sécurité	Cliquez pour développer

Ajouter Annuler

Ensuite se rendre dans Groupe de ports :

Ajouter un groupe de ports - Port_VM

Nom	Port_VM
ID du VLAN	0
Commutateur virtuel	Switch_vm
▸ Sécurité	Cliquez pour développer

Ajouter Annuler

1.2. Création de la Vm

Dans Machines Virtuelles Créer une machine :

Nouvelle machine virtuelle - Test-VM (Machine virtuelle ESXi 7.0)

- 1 Sélectionner un type de création
- 2 Sélectionner un nom et un système d'exploitation invité**
- 3 Sélectionner un stockage
- 4 Personnaliser les paramètres
- 5 Prêt à terminer

Sélectionner un nom et un système d'exploitation invité

Spécifier un nom unique et un système d'exploitation

Nom:

Les noms des machines virtuelles peuvent comporter jusqu'à 80 caractères et doivent être uniques dans chaque instance ESXi.

L'identification du système d'exploitation invité permet à l'assistant de fournir les valeurs par défaut appropriées pour l'installation du système d'exploitation.

Compatibilité:

Famille de systèmes d'exploitation invités:

Version du SE invité:

Précédent Suivant Terminer Annuler

Nouvelle machine virtuelle - Test-VM (Machine virtuelle ESXi 7.0)

- 1 Sélectionner un type de création
- 2 Sélectionner un nom et un système d'exploitation invité
- 3 Sélectionner un stockage
- 4 Personnaliser les paramètres**
- 5 Prêt à terminer

Personnaliser les paramètres

Configurer le matériel virtuel et les autres options de la machine virtuelle

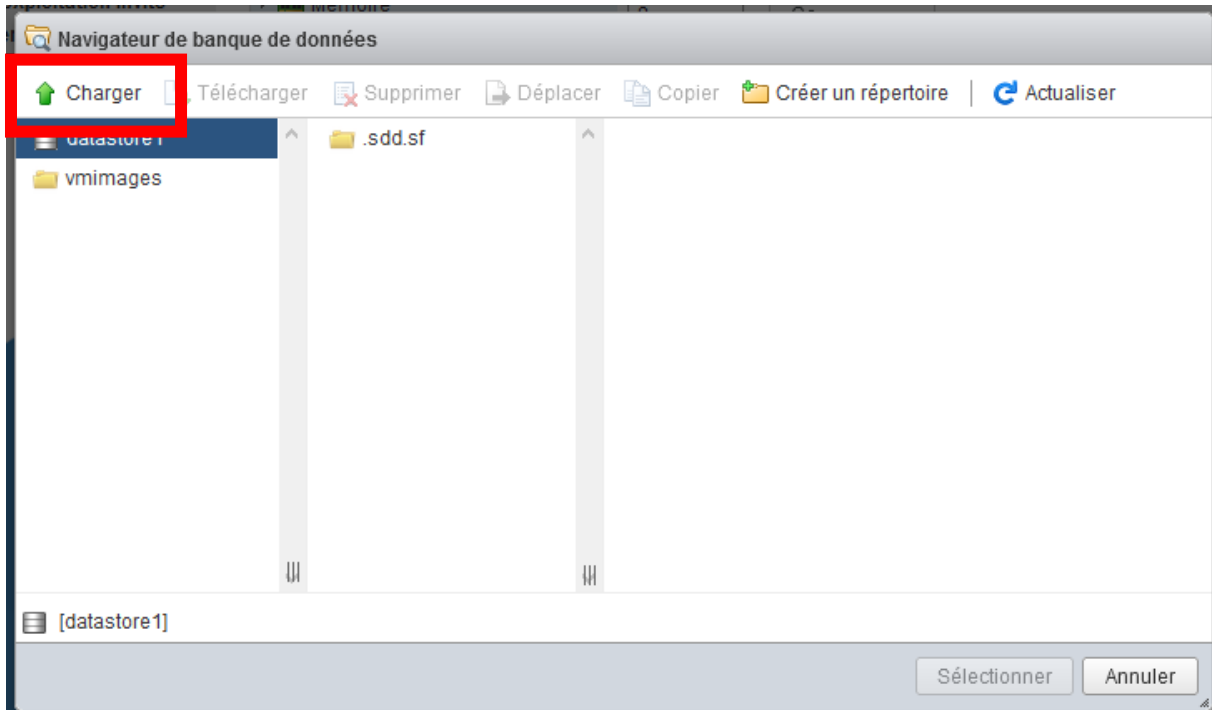
Matériel virtuel Options VM

Ajouter un disque dur Ajouter un adaptateur réseau Ajouter un autre périphérique

CPU	<input type="text" value="2"/>	<input type="button" value="i"/>
Mémoire	<input type="text" value="8"/>	<input type="button" value="Go"/>
Disque dur 1	<input type="text" value="40"/>	<input type="button" value="Go"/>
Contrôleur SCSI 0	<input type="text" value="VMware Paravirtual"/>	<input type="button" value="x"/>
Contrôleur SATA 0		<input type="button" value="x"/>
Contrôleur USB 1	<input type="text" value="USB 2.0"/>	<input type="button" value="x"/>
Adaptateur réseau 1	<input type="text" value="Port_VM"/>	<input checked="" type="checkbox"/> Connecter <input type="button" value="x"/>

Pour insérer l'image iso :

Lecteur de CD/DVD 1	Fichier ISO banque de données	<input checked="" type="checkbox"/> Connecter
État	<input checked="" type="checkbox"/> Connecter lors de la mise sous tension	
Support CD/DVD	<input type="text"/>	<input type="button" value="Parcourir..."/>
Emplacement du contrôleur	Contrôleur SATA 0	SATA (0:0)



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 :

```
config.status: creating autoconfig.h
configure: Menuselect build configuration successfully completed

      .$$$$$$$$$$$$$$$$$.
     .7$7..          .7$7:..
    .$$:.           ,7.7
   .7.      7$$$$      .777
  .$.      .$$$      .$$$7
 .7$      ?.      $$$$.      ?.      7$$$
$.      .$$7. $$$7 .7$$$      .$$$
.777.      .$$$$77$$$$77$$$$7.      $$$
$$$~      .7$$$$$$$$7.      .$$$
.$7      .7$$$$$7:      ?$$$
$$$      ?7$$$$$$$I      .77
$$$      .7$$$$$$$$$$$$$      :$$$
$$$      $$$$$7$$$$$$$$$      .$$$
$$$      $$$ 7$$$7 .$$$      .$$$
$$$$$      $$$7      .$$$
7$$$7      7$$$      7$$$
$$$$$      $$$
$$$7.      $$ (TM)
$$$$$.      .7$$$$$ $$
$$$$$$$$7$$$$$$$$.
$$$$$$$$$$$$$.

configure: Package configured for:
configure: OS type : linux-gnu
configure: Host CPU : x86_64
configure: build-cpu:vendor:os: x86_64 : pc : linux-gnu :
configure: host-cpu:vendor:os: x86_64 : pc : linux-gnu :
[root@localhost asterisk-18.3.0]#
```

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

--- Extended ---
XXX chan_mobile
[*] chan_oo323
[*] format_mp3
XXX app_mysql

--- Deprecated ---
XXX app_mysql
XXX cdr_mysql
```

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

```

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 ---
[*] MOH-OPSOUND-WAV
[*] MOH-OPSOUND-ULAW
[*] MOH-OPSOUND-ALAW
[ ] MOH-OPSOUND-GSM
[ ] 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-EN_GB-SIREN14
[*] EXTRA-SOUNDS-FR-WAV
[*] EXTRA-SOUNDS-FR-ULAW
[*] EXTRA-SOUNDS-FR-ALAW
[ ] EXTRA-SOUNDS-FR-GSM
[ ] EXTRA-SOUNDS-FR-G729
[ ] EXTRA-SOUNDS-FR-G722
[ ] EXTRA-SOUNDS-FR-SLN16
[ ] EXTRA-SOUNDS-FR-SIREN7
[ ] EXTRA-SOUNDS-FR-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

[*] app_system
[*] app_talkdetect
[*] app_transfer
[*] app_userevent
[*] app_verbose
[*] app_voicemail
XXX app_voicemail_imap
XXX app_voicemail_odbc
[*] app_waituntil
[*] app_while
--- Extended ---
[*] app_alarmreceiver
[*] app_amd
[*] app_attended_transfer
[*] app_audiosocket
[*] app_blind_transfer
[*] app_chanisavail
[*] app_dictate
[*] app_externalivr
[*] app_festival
[ ] app_ivrdemo
XXX app_jack
XXX app_meetme
[*] app_minivm
[*] app_morsecode
[*] app_mp3
XXX app_osplookup
[ ] app_saycounted
[*] app_sms
[ ] app_statsd
[*] app_test
[*] app_waitforring
[*] app_waitforsilence
[*] app_zapateller
--- Deprecated ---
[*] app_adsiprog
XXX app_dahdiras
XXX app_fax
[*] app_getcpeid
[*] app_ices
[*] app_image
[*] app_macro
[*] app_nbscat
[*] app_url

Simple FAX Application
```

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 :

```
# Be sure that Asterisk's environment
# files required for its operation,
# socket, the asterisk database, etc.
AST_USER="asterisk"
AST_GROUP="asterisk"

# If you DON'T want Asterisk to start
# this out.
```

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

Et décommenter les lignes :

```
;runuser = asterisk  
;rungroup = asterisk  
;forceblackbackground = yes
```

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
```

```
Enter current password for root (enter for none): █  
Xterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
```

Laisser vide et appuyer sur la touche Entrée

```
root user without the proper  
Set root password? [Y/n] n █
```

Taper « n »

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

3.5. Démarrage de Apache :

```
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 xzf 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

SIP Settings

SIP driver informations

Paramètres SIP généraux | SIP Settings [chan_pjsip]

—Security Settings

Permettre les appels anonymes SIP entrants [?](#) Oui Non

Permettre les invités SIP [?](#) Oui Non

Default TLS Port Assignment [?](#) Chan SIP PJSip

—NAT Settings

Adresse externe [?](#)

Local Networks [?](#) /

Dans application>Postes :

Créer un utilisateur :

Ajout Extension PJSIP 102

General Boîte vocale Avancé Pin Sets

— Ajouter un poste

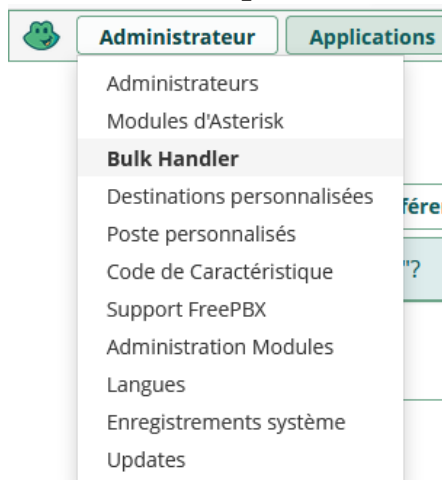
This device uses **PJSIP** technology listening on Port 5060 (UDP)

Extension Utilisateur ?	102
Nom affiché ?	seb2
CID Sortant ?	102
ID appelant d'urgence ?	
Secret ?	1234

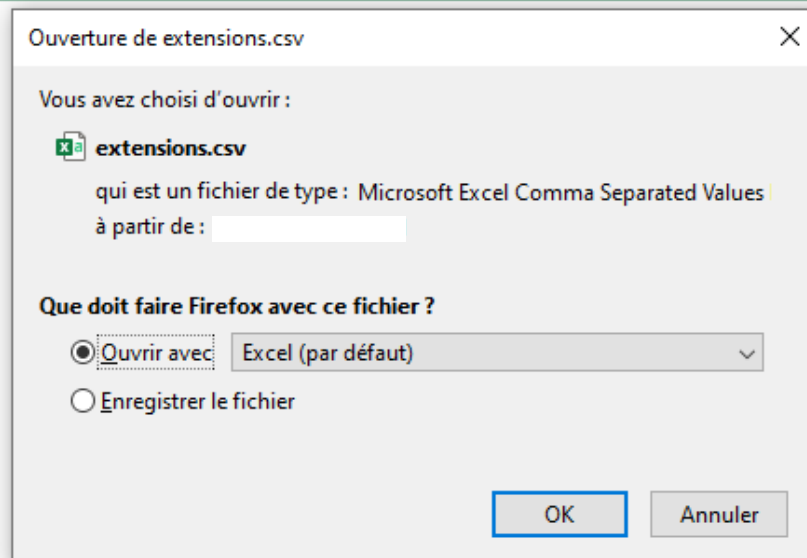
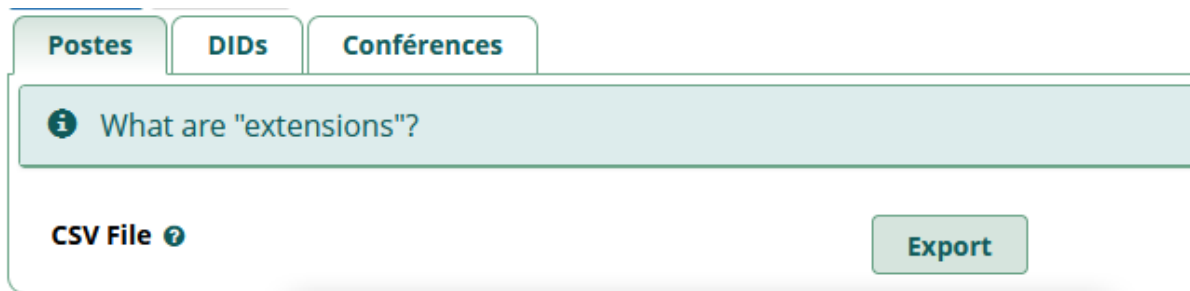
Really Weak

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

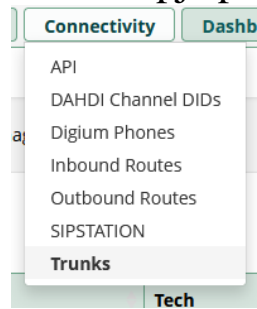
Sur le nouveau serveur taper les commandes :

```
fwconsole convert2pjsip -a
```

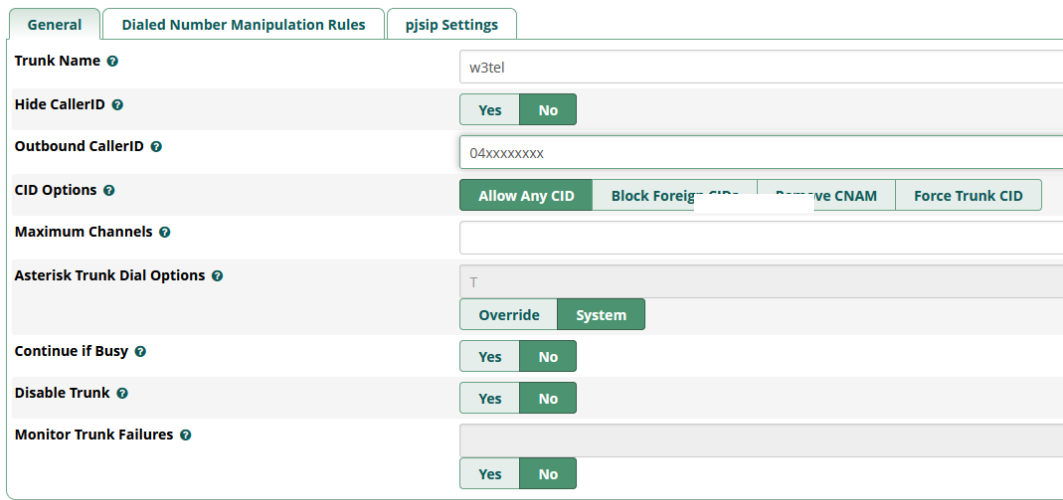
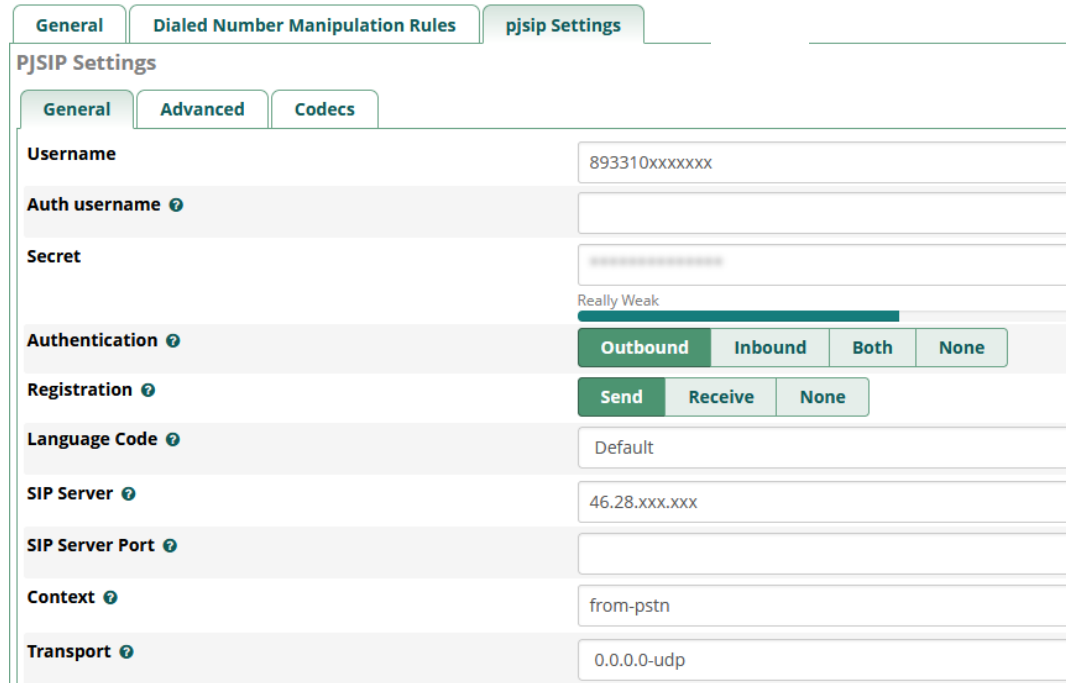
```
fwconsole reload
```

6. Configurer un Trunk pjsip

Se rendre dans :



Ensuite :

A screenshot of the Asterisk management interface showing the 'pjsip Settings' tab for a trunk. The 'Trunk Name' is 'w3tel'. The 'Hide CallerID' is set to 'No'. The 'Outbound CallerID' is '04xxxxxxxx'. The 'CID Options' are 'Allow Any CID', 'Block Foreign CID', 'Remove CNAM', and 'Force Trunk CID'. The 'Maximum Channels' is empty. The 'Asterisk Trunk Dial Options' is 'T'. The 'Continue if Busy' is set to 'No'. The 'Disable Trunk' is set to 'No'. The 'Monitor Trunk Failures' is set to 'No'.A screenshot of the Asterisk management interface showing the 'PJSIP Settings' tab for a trunk. The 'Username' is '893310xxxxxxxx'. The 'Auth username' is empty. The 'Secret' is masked with asterisks. The 'Authentication' is set to 'Outbound'. The 'Registration' is set to 'Send'. The 'Language Code' is 'Default'. The 'SIP Server' is '46.28.xxx.xxx'. The 'SIP Server Port' is empty. The 'Context' is 'from-pstn'. The 'Transport' is '0.0.0.0-udp'.

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


Edit Route: w3tel-outgoing: w3tel-outgoing

Route Settings	Dial Patterns	Import/Export Patterns	Notifications	Additional Settings
Route Name ?	w3tel-outgoing			
Route CID ?				
Override Extension ?	<input type="radio"/> Yes <input checked="" type="radio"/> No			
Route Password ?				
Route Type ?	<input checked="" type="radio"/> Emergency <input type="radio"/> Intra-Company			
Music On Hold? ?	default			
Time Match Time Zone: ?	Use System Timezone			
Time Match Time Group ?	---Permanent Route---			
Trunk Sequence for Matched Routes ?	<input type="button" value="+"/> w3tel <input type="button" value="+"/>			
Optional Destination on Congestion ?	Normal Congestion			

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

Inbound Routes

Route: 04!

 Edit Extension 102 (seb2)

General	Advanced	Privacy	Fax	Other
Description ?				
DID Number ?	04			
CallerID Number ?	ANY			
CID Priority Route ?	<input checked="" type="radio"/> Yes <input type="radio"/> No			
Alert Info ?	None			
Ringer Volume Override ?	None			
CID name prefix ?				
Music On Hold ?	Default			
Set Destination ?	Extensions 102 seb2			

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
```

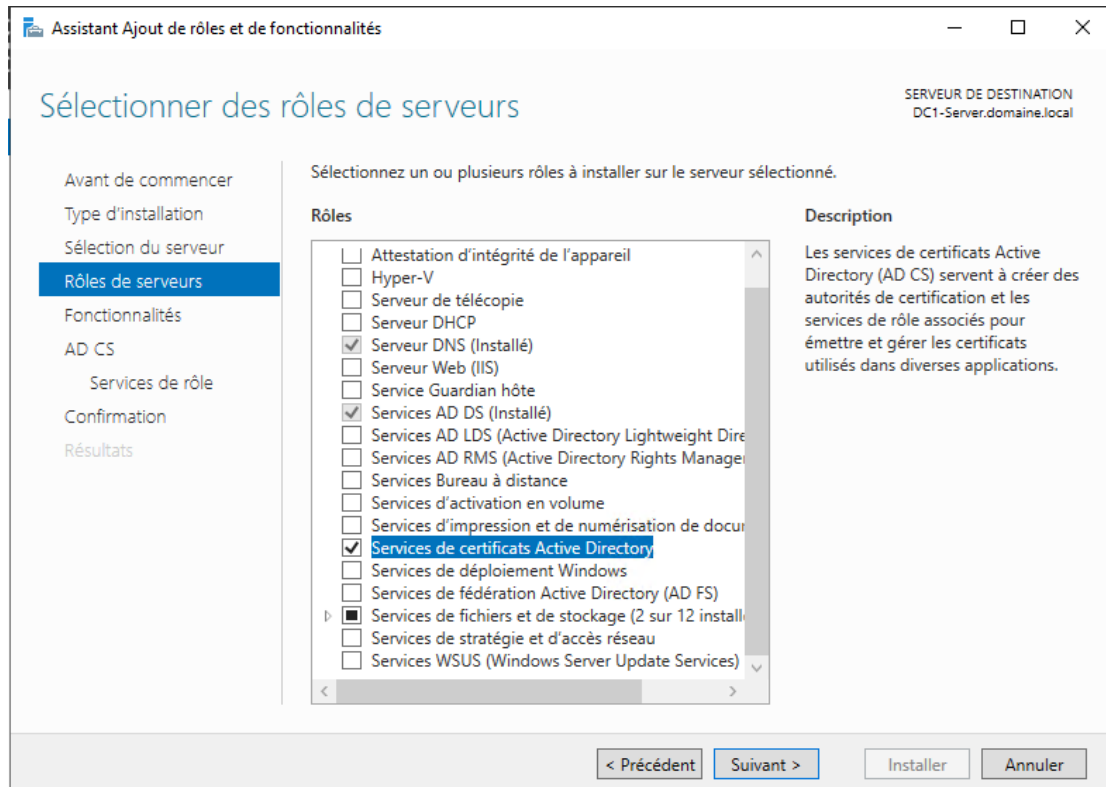
```
description user
switchport trunk native vlan 10
voice vlan enable
!
interface gigabitethernet1/1/10
description user
switchport trunk native vlan 10
voice vlan enable
!
interface gigabitethernet1/1/25
description ESXi
switchport mode access
switchport access vlan 90
!
interface gigabitethernet1/1/26
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

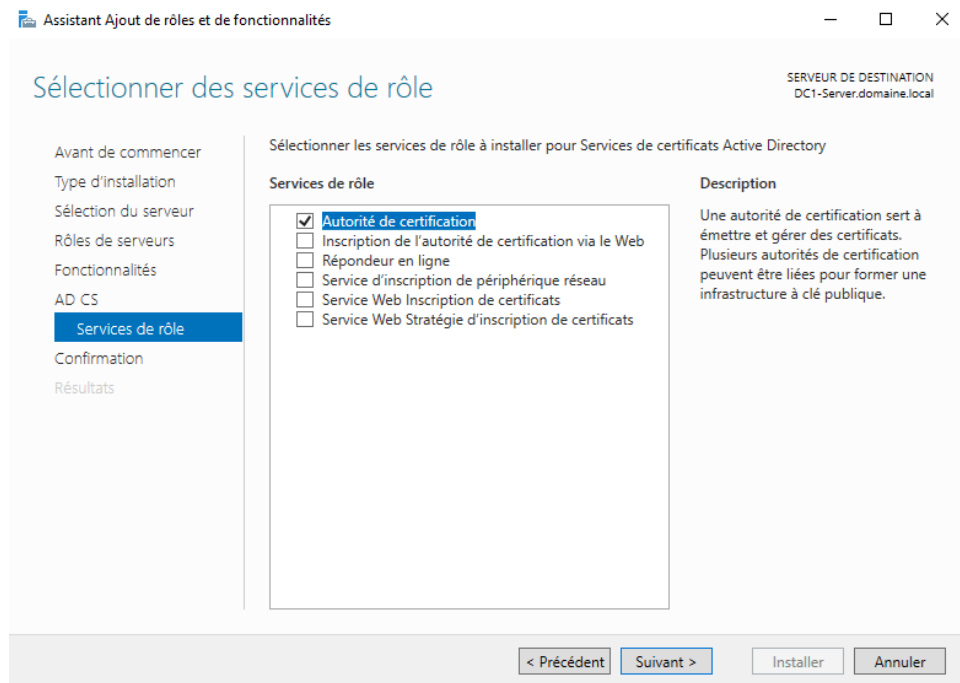
9. Installation du rôle

Ajouter des rôles et des fonctionnalités :

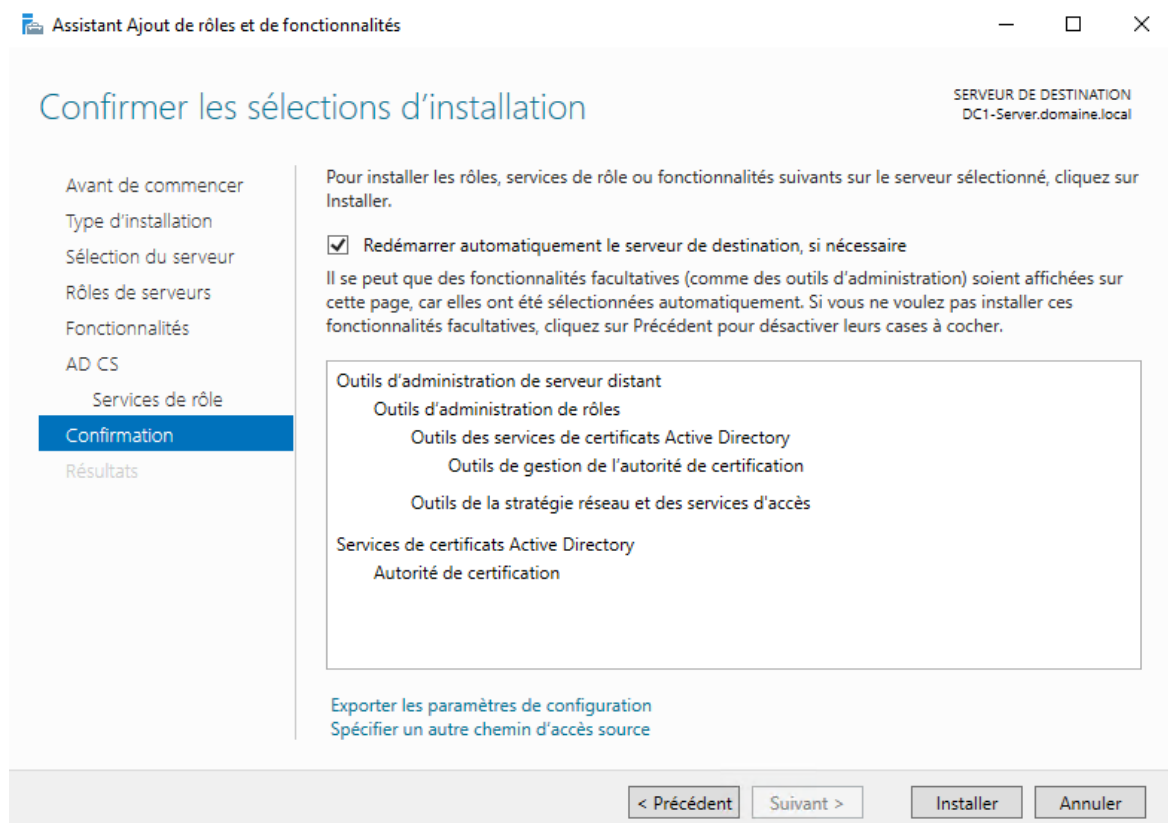


Sélectionner le Service de certificats Active Directory

Puis « Suivant » jusqu'à :

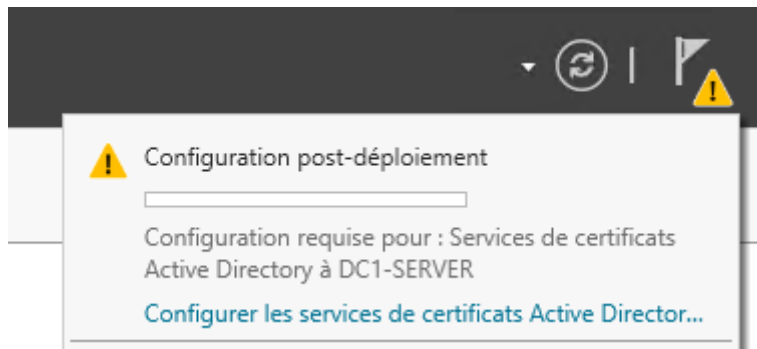


Sélectionner « Autorité de certification »

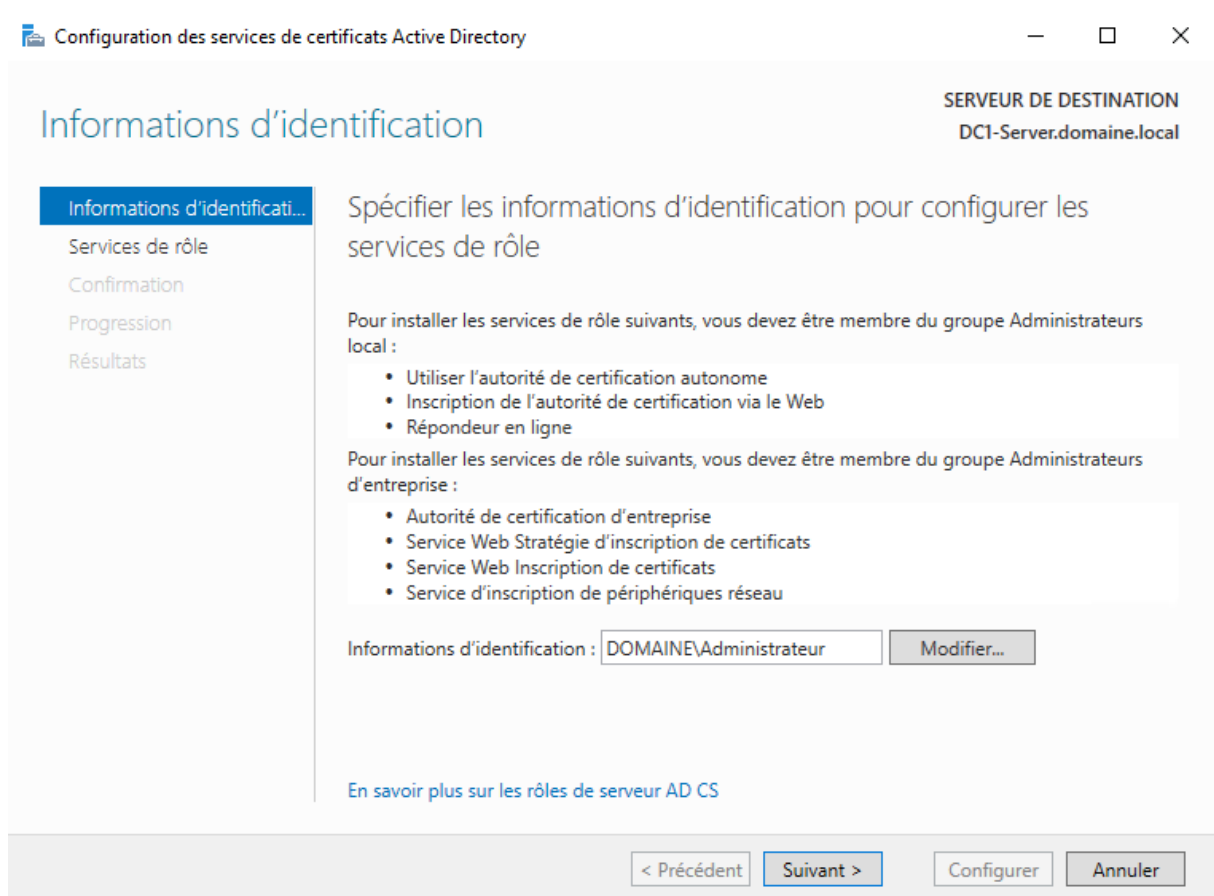


Puis confirmer et installer.

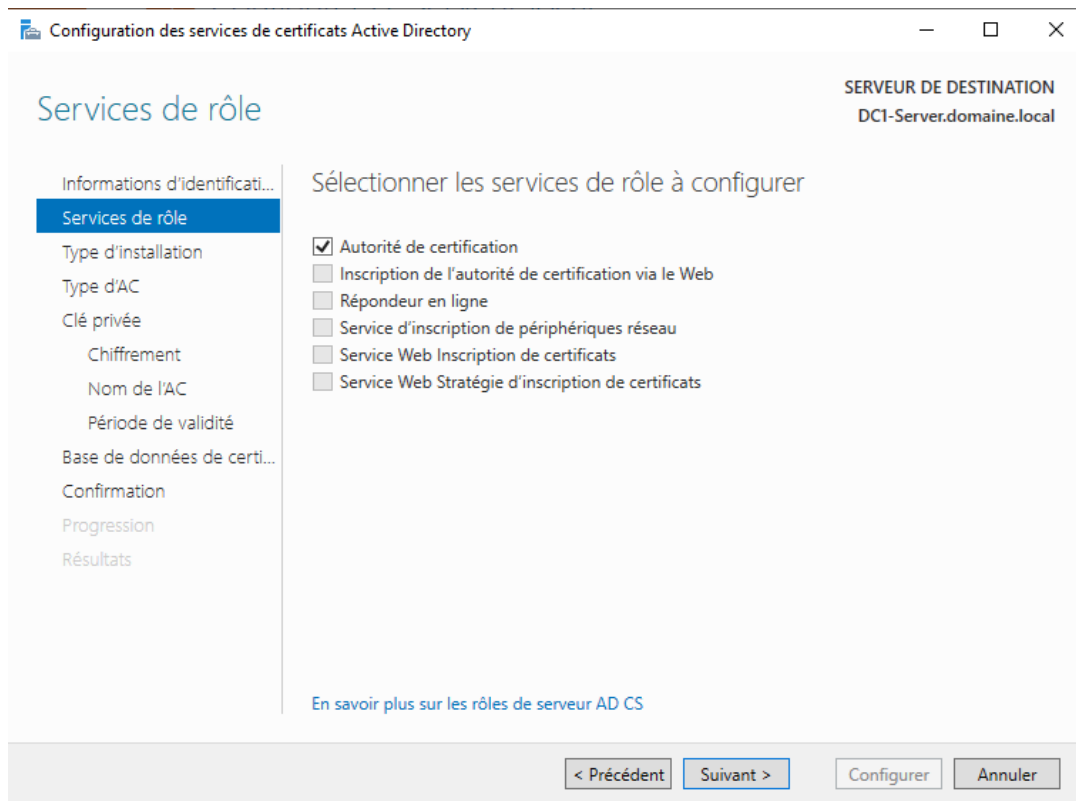
10. Configuration du rôle



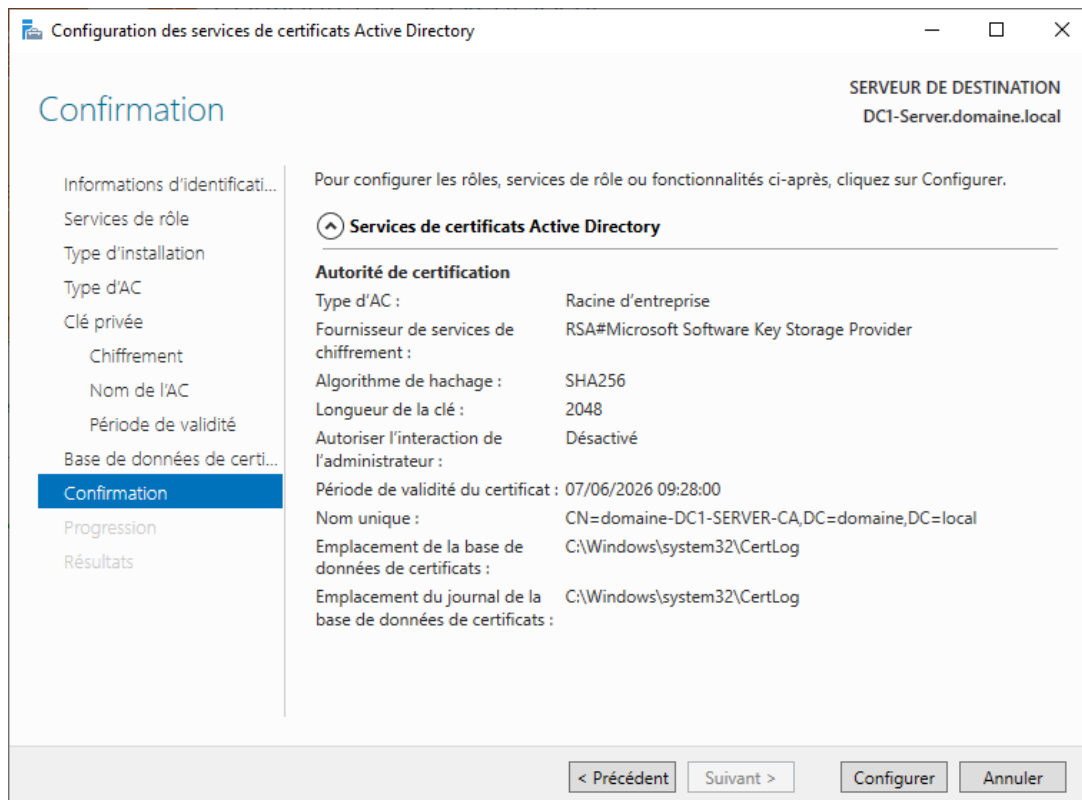
Configurer les services



Ensuite sélectionner « Autorité de certification » :



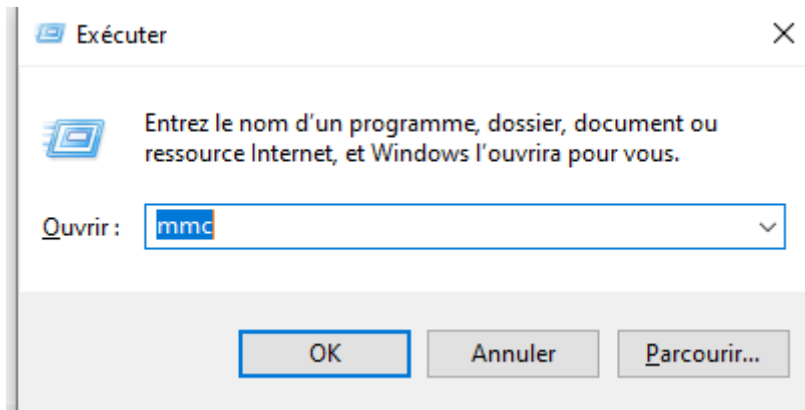
Sélectionner Suivant jusqu'à :



Et enfin cliquer sur « Configurer »

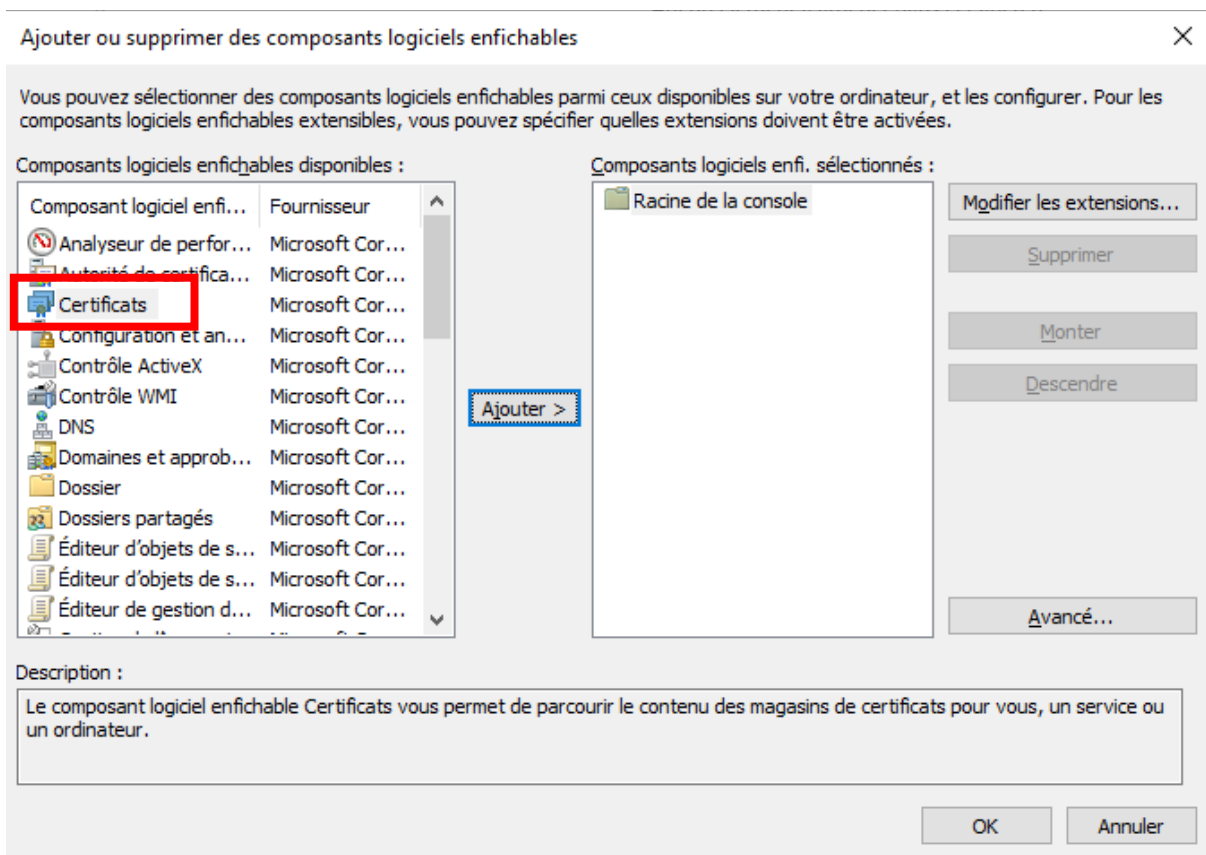
Nous allons maintenant créer un certificat.

Windows + R :

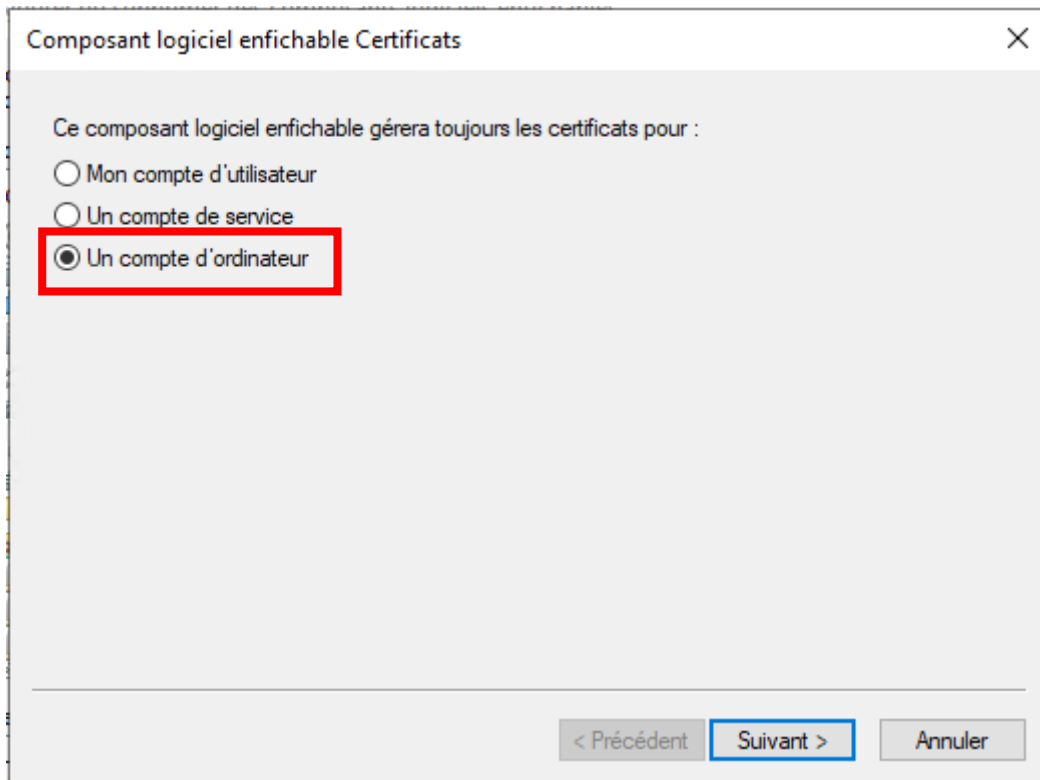


Ensuite dans la fenêtre qui s'ouvre cliquer sur : Fichier > Ajouter/Supprimer un composant logiciel enfichable...

Dans la fenêtre qui s'ouvre :

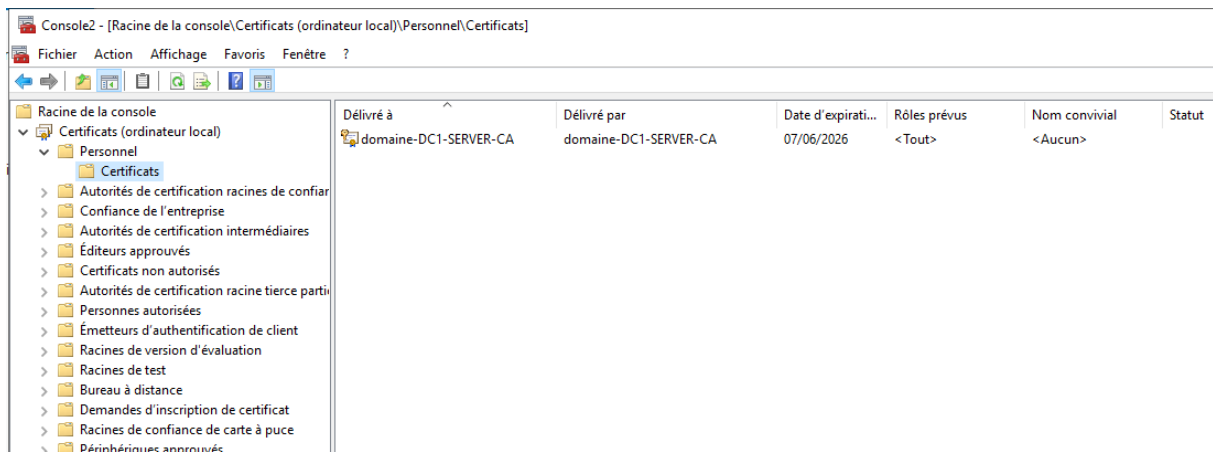


Cliquer sur Certificats puis Ajouter :

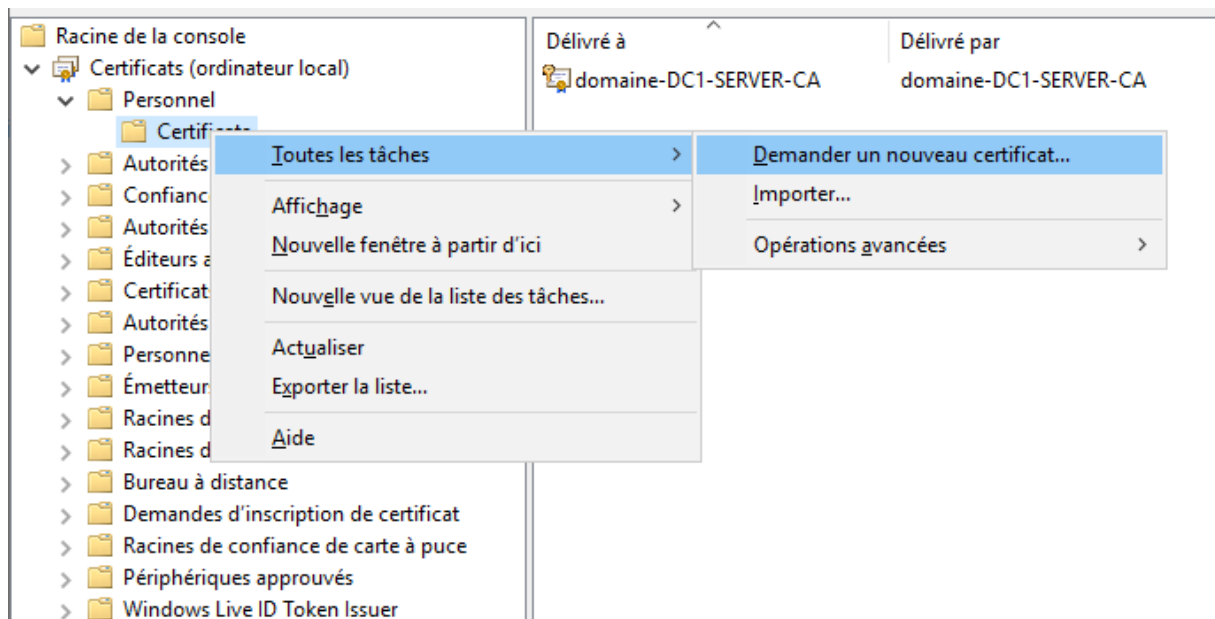


Puis valider

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



Puis clic droit sur certificat et demander un nouveau certificat :



Inscription de certificats

Demander des certificats

Vous pouvez demander les types de certificats suivants. Sélectionnez les certificats que vous voulez demander, puis cliquez sur Inscription.

Stratégie d'inscription à Active Directory			
<input type="checkbox"/>	Authentification du contrôleur de domaine	Statut : Disponible	Détails ▾
<input type="checkbox"/>	Authentification Kerberos	Statut : Disponible	Détails ▾
<input checked="" type="checkbox"/>	Contrôleur de domaine	Statut : Disponible	Détails ▾
<input type="checkbox"/>	Réplication de la messagerie de l'annuaire	Statut : Disponible	Détails ▾

Afficher tous les modèles

Inscription

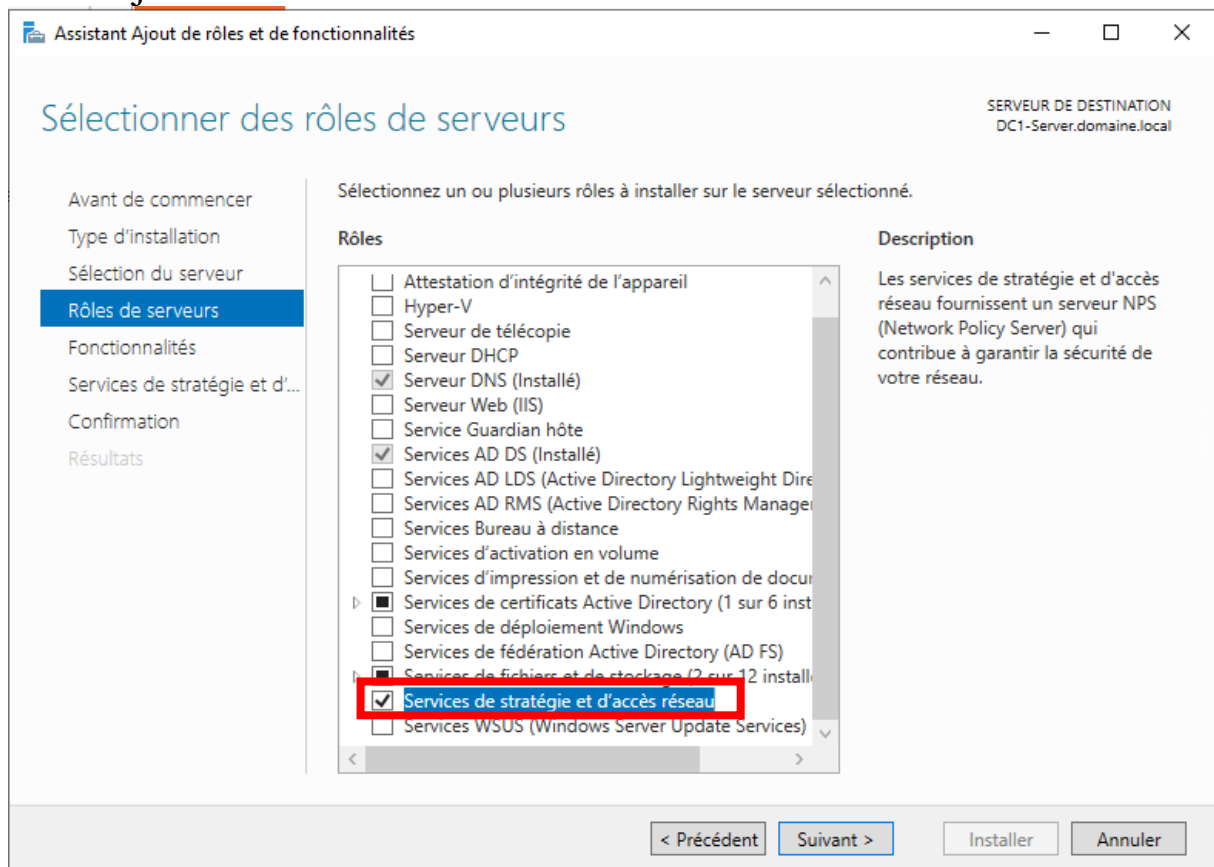
Annuler

Nous pouvons voir sur la première ligne notre certificat :

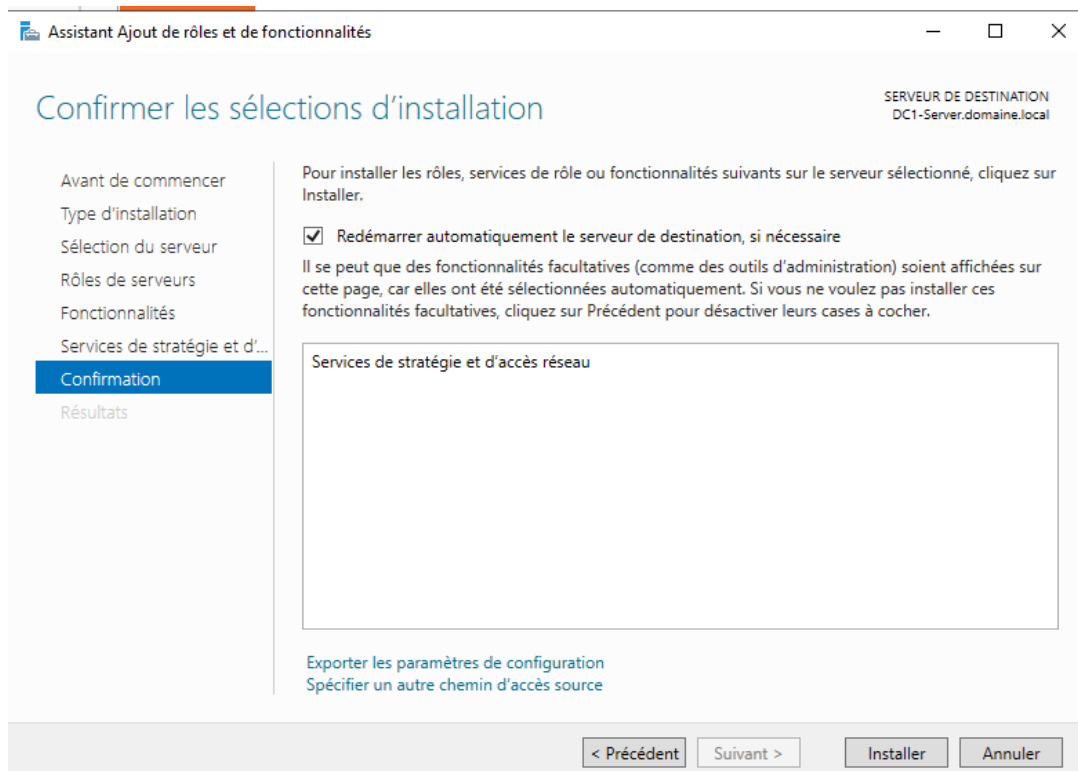
Délivré à	Délivré par	Date d'expirati...	Rôles prévus	Nom convivial	Statut	Mod
DC1-Server.domaine.local	domaine-DC1-SERVER-CA	07/06/2022	Authentification du...	<Aucun>	Conf	
domaine-DC1-SERVER-CA	domaine-DC1-SERVER-CA	07/06/2020	<Tout>	<Aucun>	Aut	

11. NPS (Serveur Radius)

12. Ajout du rôle

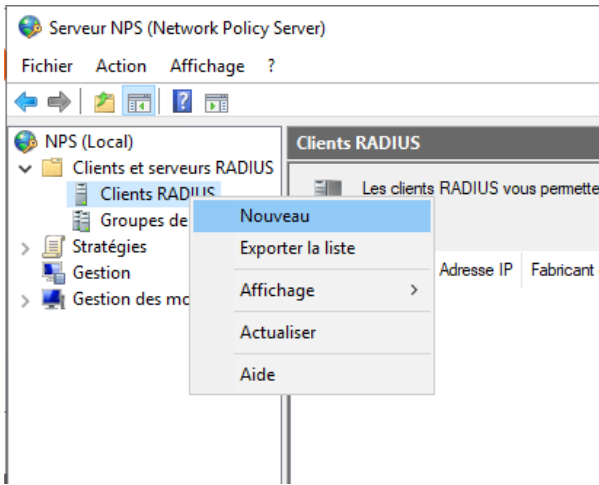


Et l'installer



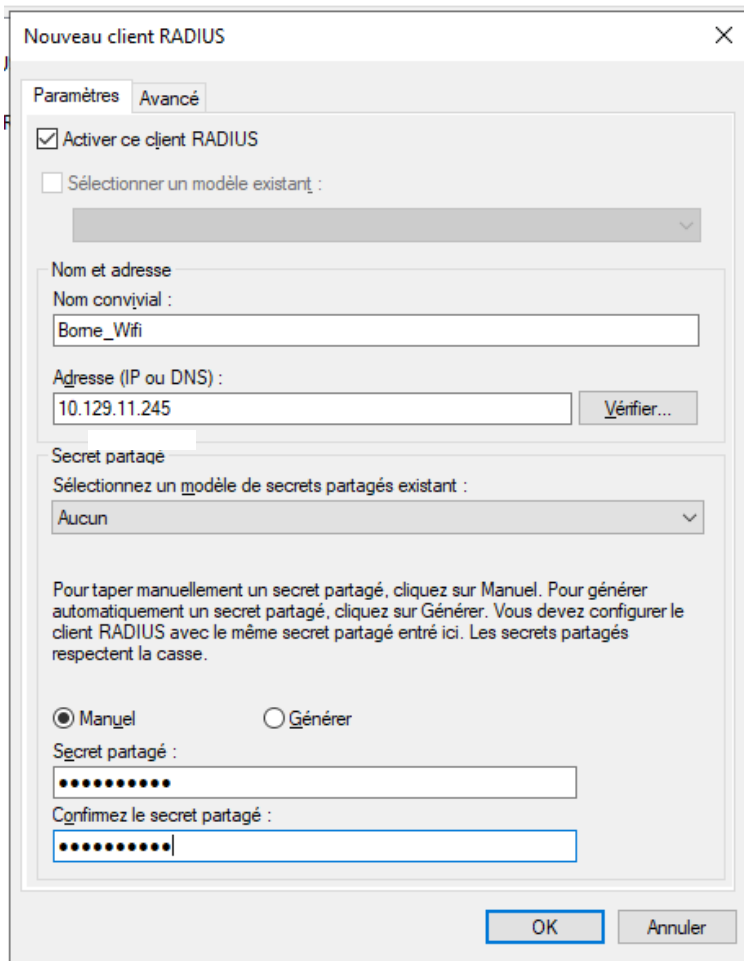
13. Configuration du serveur radius

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



et ajouter un client radius

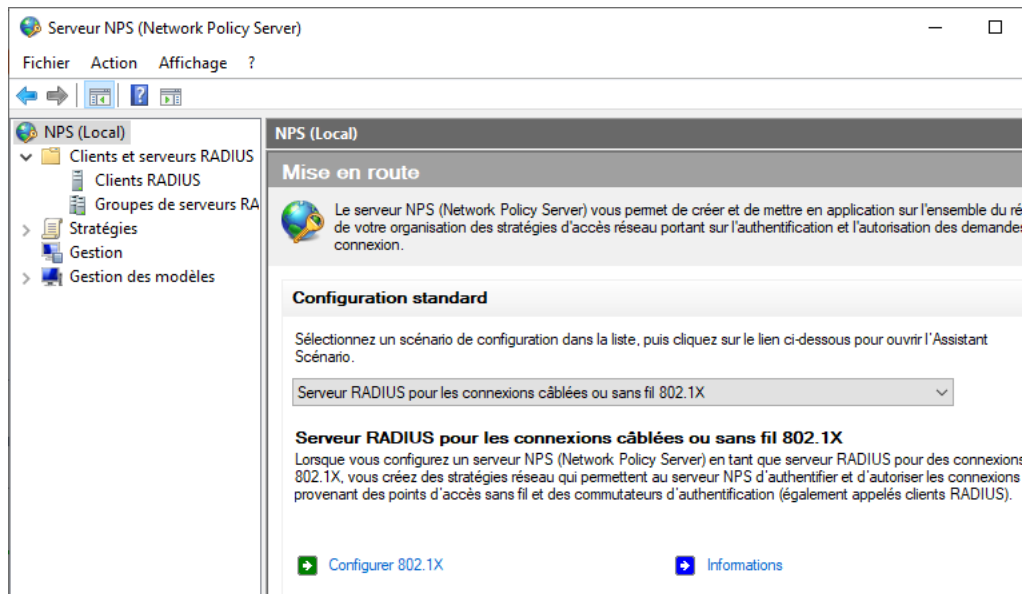
Configurer le client :



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

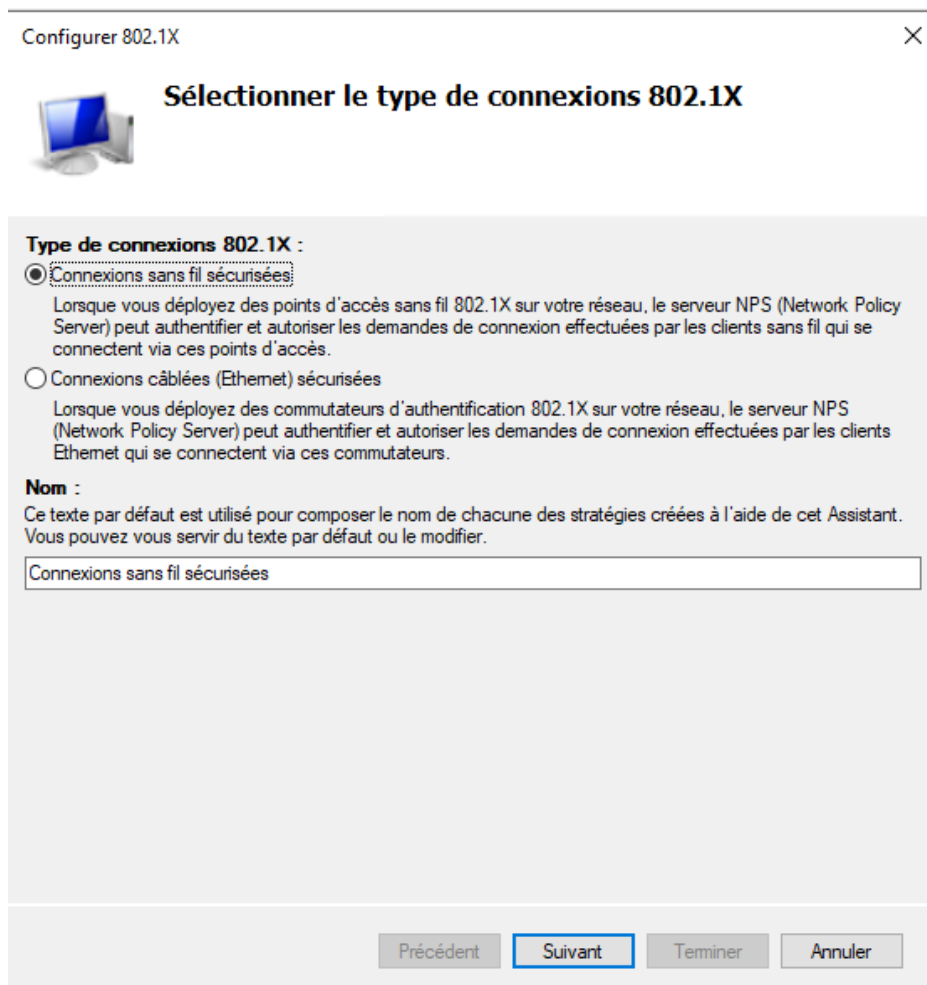
Ensuite cliquer sur NPS(Local) dans l'arborescence à droite.

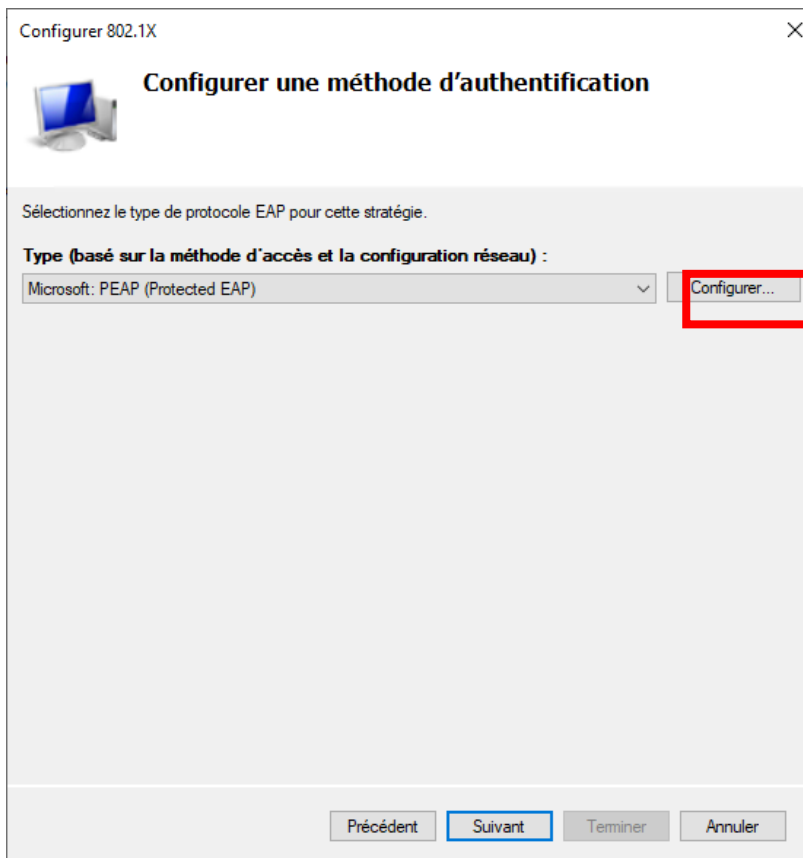
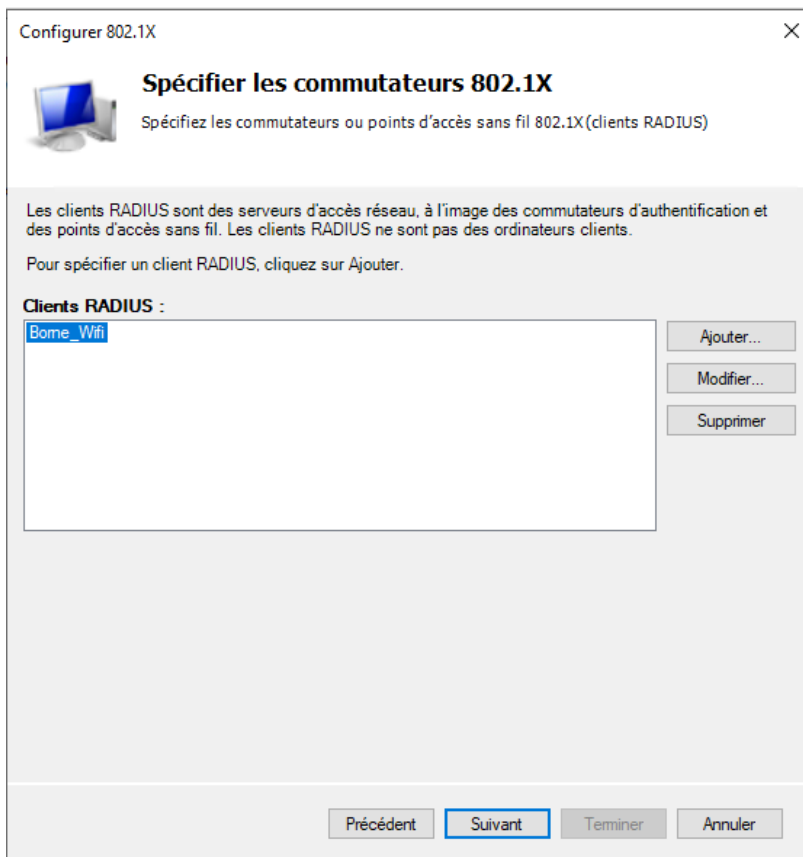
Dans configuration standard choisir :



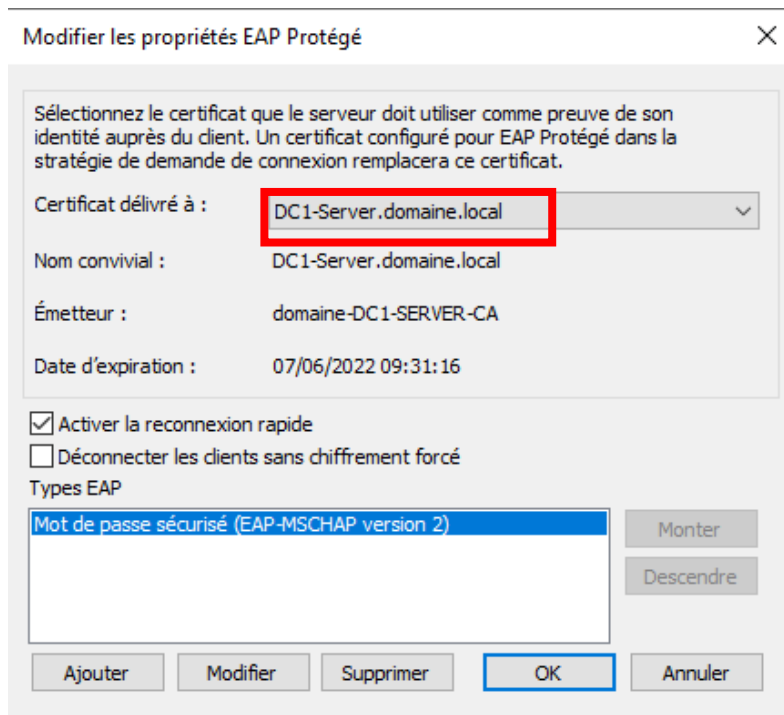
Cliquer sur « Configurer 802.1X »

Et suivre les étapes suivantes :

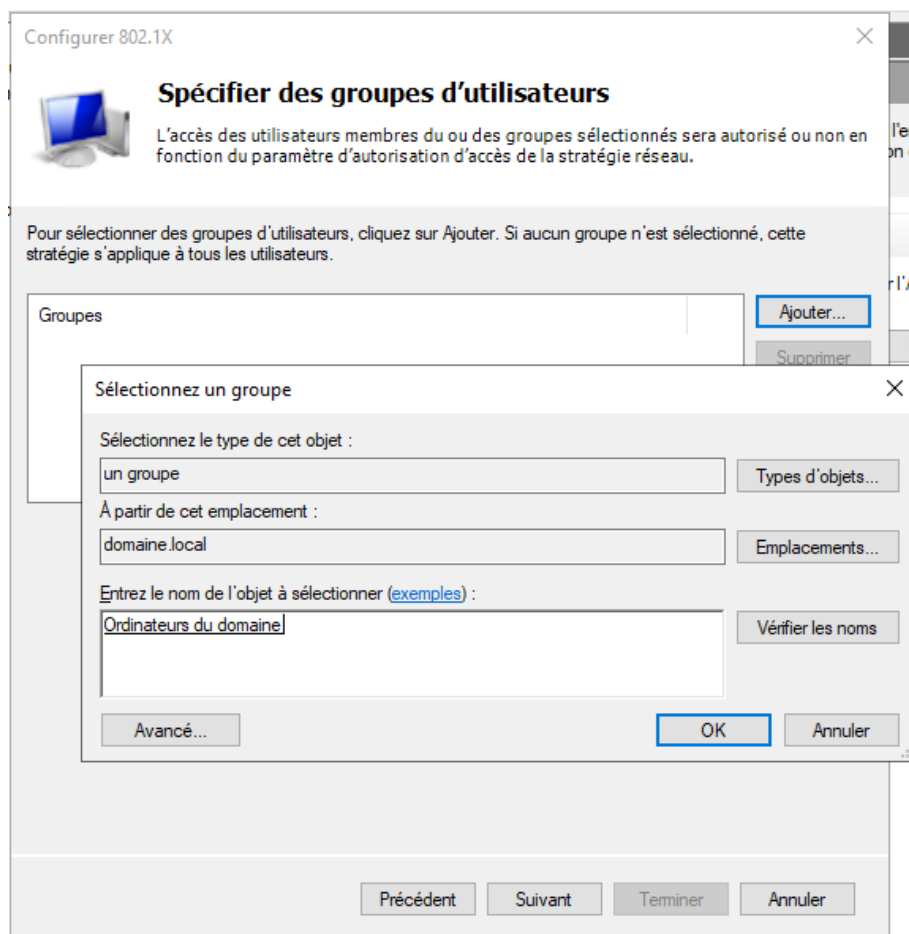




Cliquer sur « Configurer » le protocole PEAP



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 :

Gestion de stratégie de groupe

Fichier Action Affichage Fenêtre ?

10.129.14.253

Gestion de stratégie de groupe

- Forêt : domaine.local
 - Domaines
 - domaine.local
 - Default Domain Policy
 - Wifi
 - Domain Controllers
 - Objets de stratégie de groupe
 - Filtres WMI
 - Objets GPO Starter
 - Sites
 - Modélisation de stratégie de groupe
 - Résultats de stratégie de groupe

Wifi

Étendue Détails Paramètres Délégation

Liaisons

Afficher les liaisons à cet emplacement : domaine.local

Les sites, domaines et unités d'organisation suivants sont liés à cet objet GPO :

Emplacement	Appliqué	Lien activé	Chemin d'accès
domaine.local	Non	Oui	domaine.local

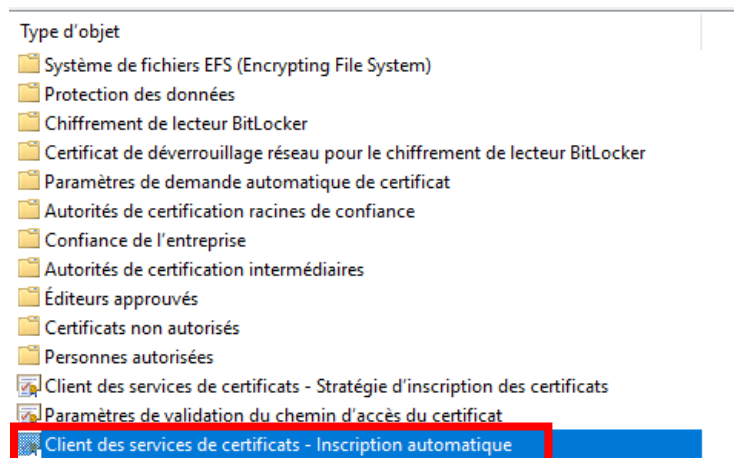
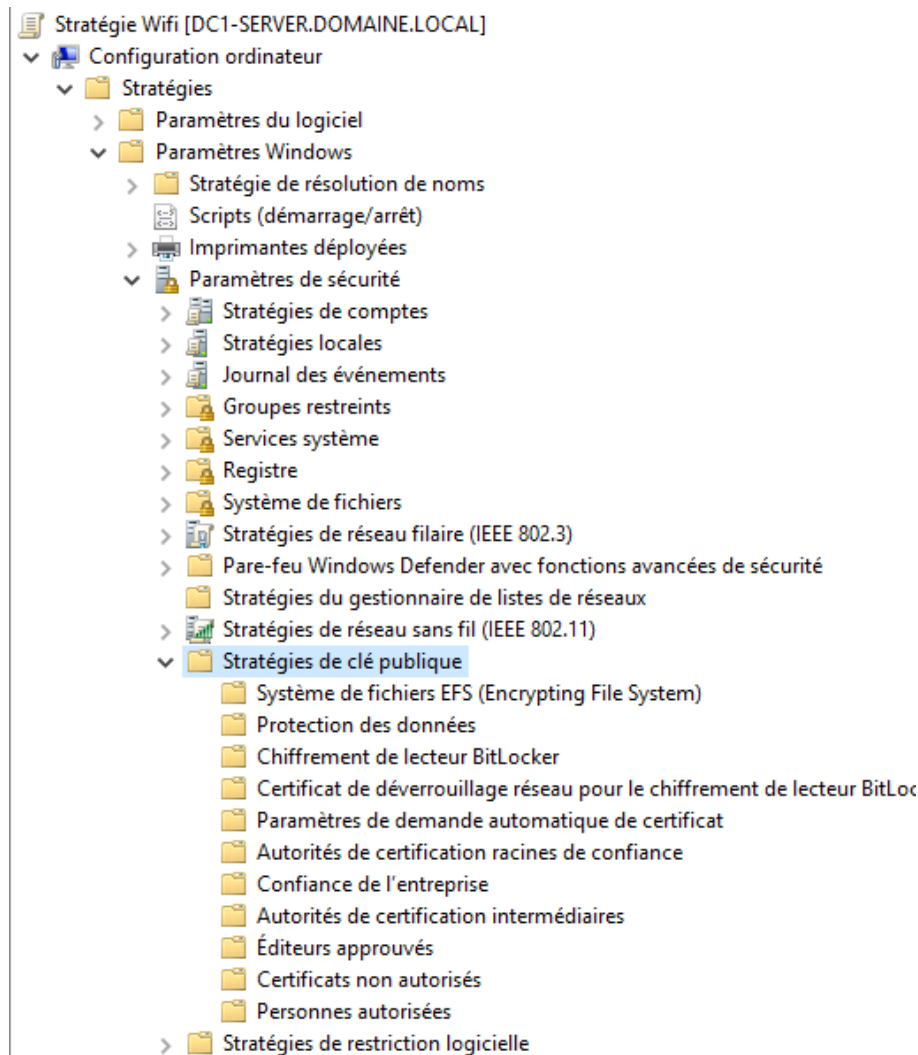
Filtrage de sécurité

Les paramètres dans ce GPO s'appliquent uniquement aux groupes, utilisateurs et ordinateurs suivants :

Nom
Ordinateurs du domaine (DOMAINE\Ordinateurs du domaine)
Utilisateurs authentifiés

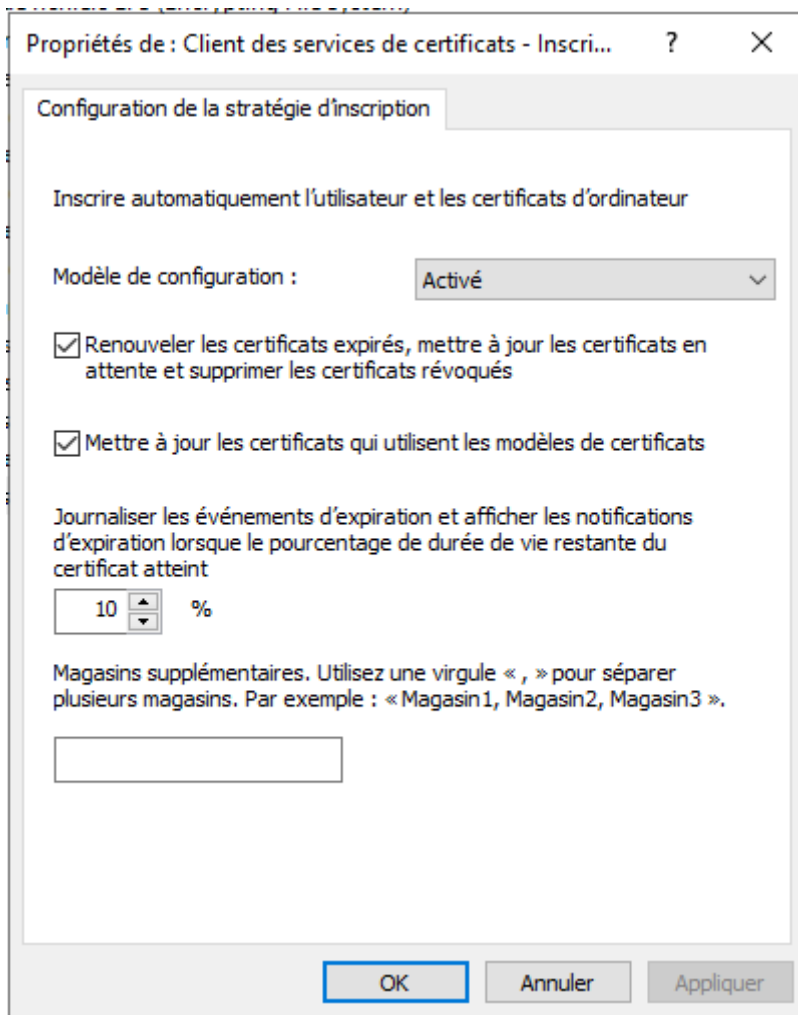
Dans l' « Editeur de gestion des stratégies de groupe »

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

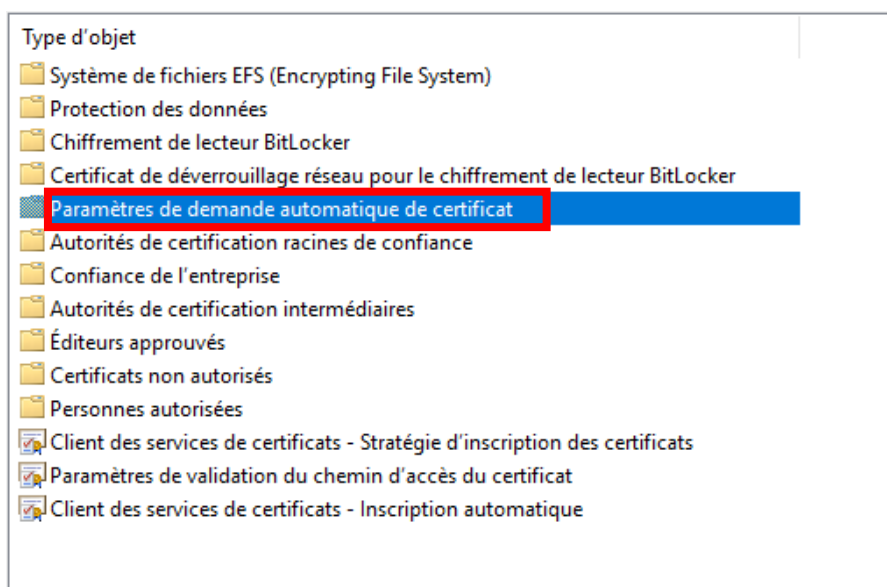


Configurer Client des services de certificats – Inscription automatique

Comme ceci :



Puis sélectionner :



Clic droit > Nouveau > Demande automatique de certificat ...

Assistant Création de demandes automatiques de certificats

Modèle de certificat

La prochaine fois qu'un ordinateur ouvrira une session, un certificat basé sur le modèle que vous aurez sélectionné sera fourni.



Un modèle de certificat est un ensemble de propriétés prédéfinies pour des certificats délivrés aux ordinateurs. Choisissez un modèle dans la liste suivante.

Modèles de certificats :

Nom	Rôles prévus
Agent d'inscription (ordinateur)	Agent de demande de certificat
Contrôleur de domaine	Authentification du client, Authentification d
IPSec	Sécurité IP IKE intermédiaire
Ordinateur	Authentification du client, Authentification d

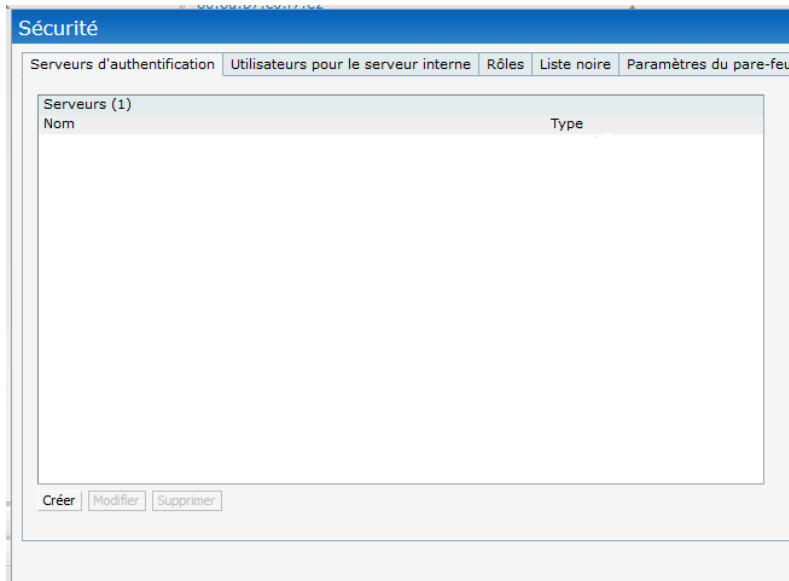
< Précédent Suivant > Annuler

nes de confiance

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 :

The screenshot shows the configuration interface for 'Modifier Test-001' with the 'Sécurité' tab selected. The 'Niveau de sécurité' section features a vertical slider with three positions: 'Plus sécurisé' at the top, 'Personnel' in the middle, and 'Ouvert' at the bottom. The 'Entreprise' level is currently selected. To the right, the 'Gestion de clés' section is configured with 'WPA entreprise (chiffremer)' as the key management method. The 'Serveur d'authentification 1' dropdown menu is set to 'ARUBA', which is highlighted with a red box. Other settings include 'Serveur d'authentification 2' set to '-- Sélectionner un serveur', 'EAP offload' set to 'Non', 'Intervalle de réauth.' set to '0 h', and 'Survivabilité de l'authentification' set to 'Non'. The 'Authentification MAC' section has two unchecked checkboxes: 'Authentification MAC avant authentification 802.1X' and 'Relais en cas d'échec de l'authentification MAC'. The 'Gestion' dropdown is set to 'Non', and 'Liste noire' and 'Forcer DHCP' are also set to 'Non'. The 'Itinérance rapide' section has two unchecked checkboxes for '802.11k' and '802.11v'. At the bottom right, there are buttons for 'Précédent', 'Suivant', and 'Annuler'.

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 :

	Numéro de VLAN	Adresse du sous-réseau	Masque de sous-réseau	Adresse IP du contrôleur	Mode d'adressage	Zone de sortie	Acc
<input checked="" type="checkbox"/>	out	10.1	255.255.255.0	10.1	Fixe	Default-out	

Paramètres réseau

Zone de sortie: Default-out | Ou création d'une nouvelle zone de sortie: []

Activer DHCP:

Adresse IP du contrôleur: 10.1 | L'adresse du sous-réseau sera calculée automatiquement, en fonction de l'adresse du contrôleur sur le VLAN à ajouter et de son masque de sous-réseau.

Masque de sous-réseau: 255.255.255.0

Passerelle: 1

Activer comme sortie par défaut:

Accès aux outils d'administration

Accès à l'outil d'administration:

Accès à l'outil de délégation:

Valider

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 :

Configuration du DNS (Domain Name System)

Configuration du relais DNS

Attention, si le service DHCP est activé sur l'interface de sortie, les serveurs DNS peuvent être modifiés lors du redémarrage de l'interface de sortie ou lors du renouvellement du bail DHCP.

DNS principal * 10.1 [Tester]

DNS secondaire [] [Tester]

Nom de domaine * do

Taille maximale des paquets (EDNS) * 1280 octets

Activer le cache

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 :

	Label	Nom du serveur	Début de validité	Fin de validité	Alias alternatifs	Défaut	Actions
<input checked="" type="checkbox"/>	ucopia	controller.access.network	11/10/2020 02:17 PM	12/12/2021 02:17 PM	controller.access.network central.access.network	<input checked="" type="checkbox"/>	[] [] []

Page 1 sur 1

Enregistrements 1 - 1 sur 1

Import/visualisation des certificats pour le portail captif

- Label
- Certificat de l'Autorité de certification (CA) Aucun fichier sélectionné.
- Certificat du contrôleur Aucun fichier sélectionné.
- Clé privée du contrôleur Aucun fichier sélectionné.
- Mot de passe de la clé privée
- Défaut

Et le définir par défaut.

1.4. Radius

Se rendre dans Configuration > Authentification > Radius

Configuration des NAS

Diminutif Sous-réseau ou adresse IP autorisé

Ajouter un NAS

Paramètres du NAS

- Diminutif *
- Secret partagé *
- Sous-réseau ou adresse IP autorisé *
 - Adresse IP
 - Interface
 - Adresse du sous-réseau
 - VLAN de sortie natif ()
 - Masque de sous-réseau
- Attributs de label de profil
 - Ruckus-Role
 - Aruba-User-Role
 - Aruba-User-Group
- Envoi d'une requête Disconnect-Request vers le NAS après déconnexion
- Architecture avec NAS effectuant une redirection du portail
 - Constructeur
 - Échappement local
 - NAS-IP-Address

Annotations :
 - Pour renseigner une seule adresse d'un client : Adresse IP
 - Pour accepter de tout un réseau : Adresse du sous-réseau

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 :

Liste des zones			
<input type="checkbox"/>	Label	Type	
<input type="checkbox"/>	Default-in	Entrée	Default incoming zone
<input type="checkbox"/>	Default-out	Sortie	Default outgoing zone
<input type="checkbox"/>	GuestMaq	Entrée	

Créer une zone

Modification de la zone *GuestMaq*

Paramètres

Nom de la zone *

Type de la zone Entrée Sortie

Description

Attribut RADIUS

Appliquer une zone basée sur les attributs RADIUS ?

Option DHCP 82

Appliquer une zone basée sur l'option DHCP 82 ?

Fuseau horaire

Définir un fuseau horaire ?

Limitation de licence

Activer la limitation de licence ?

Configuration du logo

Aucun fichier sélectionné.

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

18. Portail captif

Se rendre dans Configuration > Personnalisation > Portails

Afficher les : Associations (4) **Configurations (3)** Modèles visuels (3)

Nom de la configuration	Formats	Modes de fonctionnement	Hébergé	Zones	Modèles	Actions
Portail captif						
default-portal	Laptop, Tablette, Smartphone, Mode dégradé	Standard	●	1	1	Ajouter une configuration
Guest	Laptop, Tablette, Smartphone, Mode dégradé	Standard, One Click	●	1	1	Ajouter une configuration
Connexion automatique						
Aucune configuration n'est définie.						
Portail de délégation						
default-deleg	Laptop	-	●	2	1	Ajouter une configuration

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

Paramètres de configuration

Nom de la configuration: Guest

Hébergement du portail

Portail hébergé par le contrôleur

Redirection vers un portail externe avant le portail du contrôleur

Portail externe

Format du portail

Laptop

Tablette

Smartphone

Mode dégradé

Options globales

Attention : vous avez configuré la saisie des données personnelles sans charte régissant l'utilisation des données personnelles

Mot de passe de sécurisation

Cette sécurité est particulièrement importante pour les modes avec auto-enregistrement ou réseaux sociaux

Afficher les modes d'enregistrement en premier

Activer le contournement intelligent pour les CNA Android

Définir une charte régissant l'utilisation des informations personnelles

Authentification

[Ajouter un nouveau mode](#)

Avec identifiants

Coupler l'authentification avec RADIUS

Options

Attention : vous avez configuré la saisie des données personnelles sans charte régissant l'utilisation des données personnelles

Afficher un portail informatif en cas de reconnaissance de l'équipement utilisateur (adresse MAC)

Définir une charte régissant l'utilisation des services

Rediriger l'utilisateur une fois connecté

Mettre en quarantaine l'équipement d'un utilisateur ayant entré plusieurs fois un mot de passe erroné

Enregistrement

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

Afficher les : Associations (4) Configurations (3) Modèles visuels (3)

Nom de la zone	Type de portail	Nom de la configuration	Nom du modèle visuel	Statut	Actions
Zones d'entrée					Ajouter une association
Default-in	Portail captif	default-portal	default	●	✕ 🗑️
	Portail de délégation	default-deleg	default	●	✕ 🗑️
GuestMaq	Portail captif	Guest	snef	●	✕ 🗑️
Zones de sortie Attention, seul des portails de délégation peuvent être associés aux zones de sortie.					Ajouter une association
Default-out	Portail de délégation	default-deleg	default	●	✕ 🗑️

Maintenant on associe la configuration du portail à une zone

Ajout d'une association sur une zone d'entrée

Paramètres de l'association

Zone: GuestMaq

Configuration portail captif: Guest

Configuration connexion automatique: Aucune configuration

Configuration portail de délégation: Aucune configuration

Modèle visuel: default

Active:

19. Configuration de la borne Aruba

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

The screenshot shows the 'Nouveau réseau local sans fil' (New wireless network) configuration page. The page has a blue header with the title and an 'Aide' link. Below the header is a navigation bar with four tabs: '1 Paramètres du rés...', '2 VLAN', '3 Sécurité', and '4 Accès'. The 'Paramètres du réseau local sans fil' section is active. It contains a form with the following fields:

- Nom et utilisation** (Section header)
- Nom:** A text input field containing 'Guest1'.
- Utilisation principale:** Three radio buttons: 'Employé', 'Voix', and 'Invité'. The 'Invité' option is selected, indicated by a red arrow pointing to it.
- Afficher les options avancées:** A blue link at the bottom left, with a red arrow pointing to it.
- Suivant** and **Annuler** buttons at the bottom right.

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

The screenshot shows the 'Divers' (Miscellaneous) configuration section. It contains the following fields:

- Filtrage de contenu:** A dropdown menu set to 'Non'.
- Délai d'inactivité:** A text input field containing '1000' and a dropdown menu set to 's'. A red arrow points to this field.
- Désauthentifier les clients inactifs:** A dropdown menu set to 'Oui'. A red arrow points to this field.
- SSID:** Two checkboxes: 'Masquer' and 'Désactiver', both unchecked.
- Hors service (HS):** Two dropdown menus: 'VPN en pann' and 'Aucun'.
- Durée OOS (globale):** A text input field containing '30' and a dropdown menu set to 's'.
- Seuil clients max.:** An empty text input field.
- Codage SSID:** A dropdown menu set to 'Par défaut'.
- ESSID:** An empty text input field.
- Refuser le pontage entre utilisateurs:** A dropdown menu set to 'Non'.
- Openflow:** An unchecked checkbox.

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

Modifier Guest Aide

1 Paramètres du rés... 2 **VLAN** 3 Sécurité 4 Accès

Attribution adresse IP et réseau virtuel client

Attribution de l'adresse IP du client: Gérée par le contrôleur virtuel
 Attribuée par le réseau

Attribution du réseau local virtuel du client: Par défaut
 Statique
 Dynamique

ID du réseau local virtuel:

Ensuite on ajoute un profil pour le portail captif :

Paramètres du rés... 2 VLAN 3 **Sécurité** 4 Accès

veau de sécurité

Type de page de garde:

Serveur proxy du portail captif:

Captive portal profile:

WISPr:

Authentification MAC:

Serveur d'auth. 1:

Intervalle de réauth.: h

Serveur interne: Pas d'utilisateur [Utilisateurs](#)

Liste noire:

Forcer DHCP:

Jardin fermé: [Blacklist: 0 Whitelist: 0](#)

Désactiver si le type de liaison montante est: 3G/4G Wifi Ethernet

Chiffrement:

Ucopia

Type: ▾

IP ou nom d'hôte: →

URL: →

Port:

Utiliser https: ▾

Échec du Portail captif: ▾

URL automatique pour le placement sur liste blanche: ▾

Déchargement du serveur: ▾

Empêcher la superposition des trames: ▾

Utiliser l'adresse IP du contrôleur virtuel dans l'URL de redirection: ▾

URL de redirection:

(facultatif)

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

On ajoute un serveur d'authentification

Modifier Guest Aide

1 Paramètres du rés... 2 VLAN 3 Sécurité 4 Accès

Niveau de sécurité

Type de page de garde: Externe

Serveur proxy du portail captif:

Captive portal profile: Ucopia Modifier

WISPr: Non

Authentification MAC: Non

Serveur d'auth. 1: Serveur interne

Intervalle de réauth.: Serveur interne

Serveur interne: ucopia

Liste noire: Créer ← Aucun(e)

Forcer DHCP: Non

Jardin fermé: [Blacklist: 0](#) [Whitelist: 0](#)

Désactiver si le type de liaison montante est: 3G/4G Wifi Ethernet

Chiffrement: Non

Précédent Suivant Annuler

ucopia

Adresse IP: @IP d'ucopia → 10.

RadSec: Non

Port d'aut.: 1812

Port de gestion: 1813

Clé partagée: Mot de passe configuré dans la partie NAS →

Confirmer la clé:

Délai d'expiration: 5 s

Nombre de tentatives: 3

RFC 3576: Non

RFC 5997: Authentification Gestion

Adresse IP du serveur NAS: (facultatif)

Identificateur NAS: (facultatif)

Temps mort: 5 min

IP du proxy RADIUS dynamique:

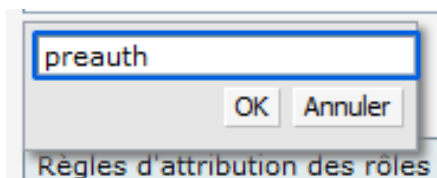
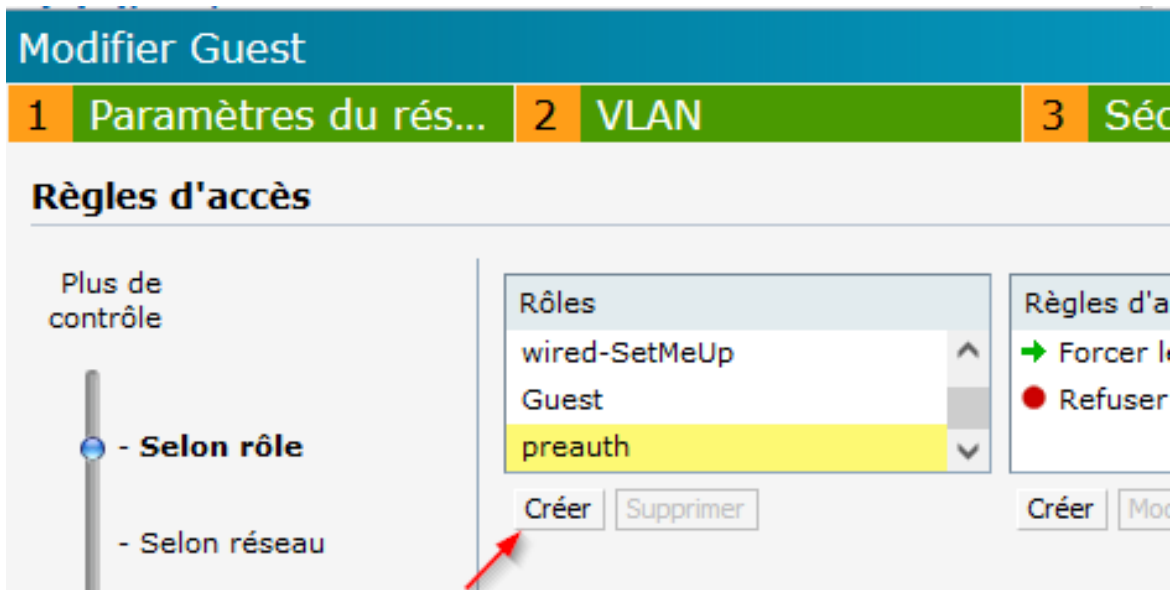
Masque du proxy RADIUS dynamique:

Réseau local virtuel du proxy RADIUS dynamique:

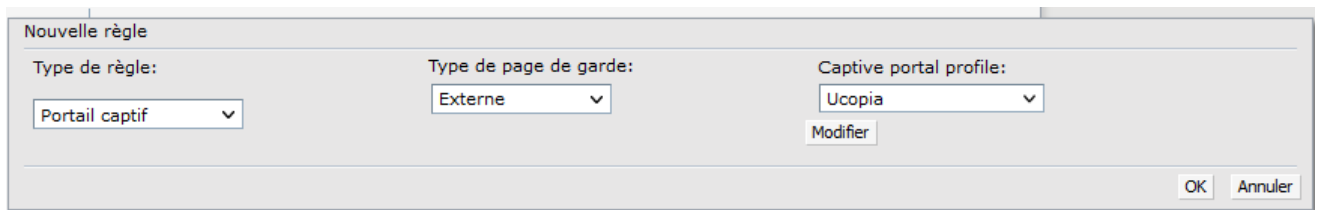
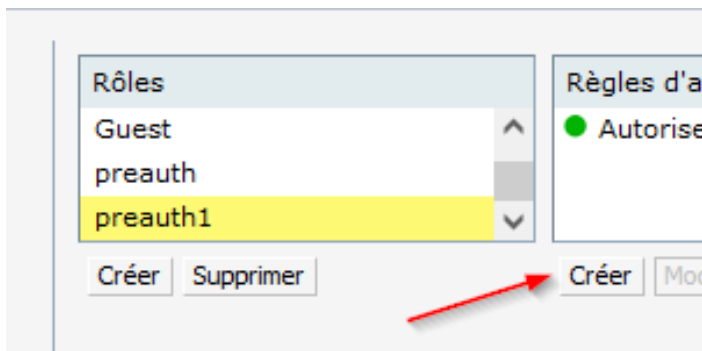
Passerelle du proxy RADIUS dynamique:

Service type framed user: 802.1X Portail captif MAC

OK Annuler



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



Nouvelle règle

Type de règle: **Contrôle d'accès**

Service: Réseau Application Catégorie d'application Catégorie Web Réputation Web

Action: **Refuser**

Destination: **sur toutes les destinations**

Options: Enregistrer Classer les médias Balise DSCP Liste noire Désactiver la recherche Priorité 802.1p

OK Annuler

Règles d'accès pour **preauth1**

- Forcer le portail captif
- Autoriser tous les services sur toutes les destinations
- Refuser tous les services sur toutes les destinations

Créer Modifier Supprimer ↑ ↓

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

Modifier Guest Aide

1 Paramètres du rés... 2 VLAN 3 Sécurité 4 Accès

Règles d'accès

Plus de contrôle

- Selon rôle - Selon réseau

Rôles: default_wired_port_profile, wired-SetMeUp, **Guest**

Règles d'accès pour **Guest**: ● Autoriser tous les services sur toutes les destinations + journal

Créer Supprimer

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

Nouvelle règle

Type de règle: **Contrôle d'accès**

Service: Réseau Application Catégorie d'application Catégorie Web Réputation Web

Action: **Autoriser**

Destination: **sur toutes les destinations**

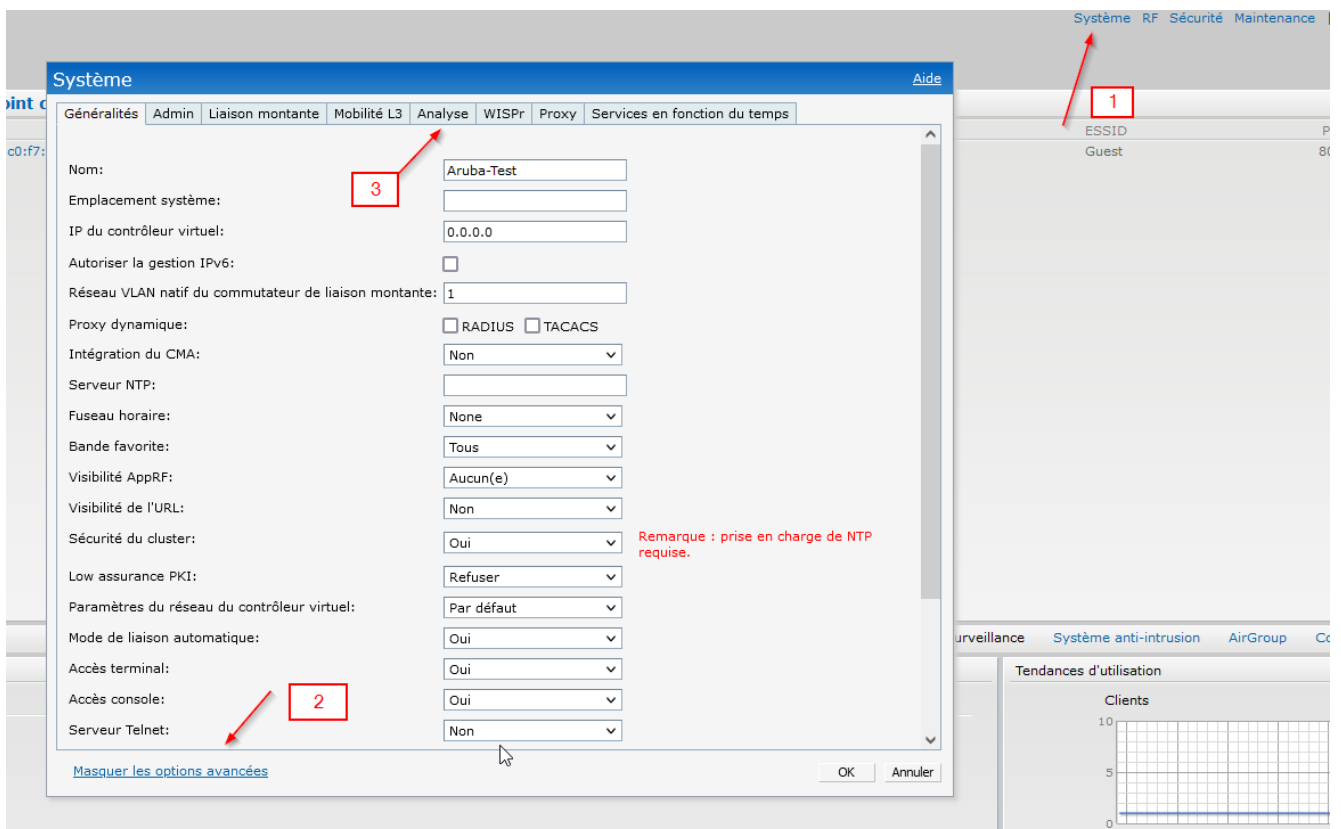
Options: Enregistrer Classer les médias Balise DSCP Liste noire Désactiver la recherche Priorité 802.1p

OK Annuler



On définit le rôle avant l'authentification.

20. Configuration du serveur Syslog Sur la borne Aruba



Système

Généralités Admin Liaison montante Mobilité L3 Analyse WISPr Proxy Services en fonction du temps

Serveurs — Niveaux installation journaux syst. —

Serveur journaux syst.: 10.:
 Serveur de vidage TFTP: 0.0.0.0
 Journal système: Avertisseme
 Débogage point d'accès: Avertisseme
 Réseau: Avertisseme
 Sécurité: Avertisseme
 Système:
 Utilisateur:
 Débogage utilisat:
 Sans fil:

SNMP — @IP d'ucopia

Chaînes de communauté pour SNMPV1 et SNMPV2

Utilisateurs pour SNMPV3

Nom	Protocole d'authentification	Protocole de confidentialité

Créer Modifier Supprimer

Créer Modifier Supprimer

SNMP Traps:

Récepteurs d'interruptions SNMP

Sur l'UCOPIA :

Se rendre sur Configuration > Réseau > Filtrage :

Configuration des paramètres de filtrage

Afficher les : Accès au contrôleur (4) Ouverture de port (0) Redirection de port (0)

Nom du service	Paramètres d'accès	Statut	Actions
Outil d'administration	Interface de sortie : out (Natif) Sous-réseau : natve-in	●	✕ 🗑️
CLI	Interface de sortie : out (Natif)	●	✕ 🗑️
Portails de délégation	Interface de sortie : out (Natif) Sous-réseau : natve-in	●	✕ 🗑️
Syslog	Hôte : <input type="text"/>	●	✕ 🗑️

Configuration des paramètres de filtrage

Modification d'un accès

Note : L'accès au contrôleur permet de gérer les ouvertures de flux à destination des services du contrôleur

Paramètres de l'accès

Service Sources

Syslog

Ajouter une source

Hôte : @IP de la borne Aruba

Actif

On renseigne l'adresse de la borne Aruba.

21. Création des comptes utilisateurs

Dans Administration > Utilisateurs > Profils

Liste des profils utilisateurs		
<input type="checkbox"/>	Nom du profil	Utilisateurs
<input type="checkbox"/>	Administrateur	0

📁 ⚙️ + 🗑️ ⚙️ ↩️

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

Paramètres du profil

Nom *

Droits d'accès

Services autorisés: Web, Mail

Services non autorisés: File_Transfer, Full_Access, Instant_Messaging, Web_Proxy, Microsoft_Network, Remote_Access, SSH, Telnet, Administration, VPN

<<< Ajouter / Supprimer >>>

Validité

Dates de validité: Toujours valide, Valide à partir de la création, Jusqu'à [minuit], pendant [7] jour [] heures [] minute, Valide dans un intervalle de dates

Crédit temps: Durée allouée: [] heure et [] minute, Recrédition tous les [] jour

Plages horaires: Chaque jour, Lundi, Mardi, Mercredi, Jeudi, Vendredi, Samedi, Dimanche

Zones

Zones d'entrée: Autorisées: GuestMaq, Non autorisées: Default-in

<<< Ajouter / Supprimer >>>

Certains paramètres permettent d'affiner la sécurité comme :

🔍 Forcer la déconnexion d'un utilisateur :

Activer la déconnexion forcée ?

Déconnexion après [] jour [7] heures [] minute [] seconde

🔍 Déconnexion automatique de l'utilisateur :

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 :

Identité de l'utilisateur

Identifiant * Nom
 Mot de passe Prénom
 Confirmer mot de passe

Profil

Profils autorisés *
 Services associés Web, Mail
 Dates de validité Plages horaires Crédit temps

Valable à la création pendant 7 heures
Lundi de 08:00 à 18:00
Mardi de 08:00 à 18:00
Mercredi de 08:00 à 18:00
Jeudi de 08:00 à 18:00
Vendredi de 08:00 à 18:00
Aucune plage horaire pour les autres jours
Aucune restriction

Validité

Dates de validité
 Personnaliser les dates de validité héritées du profil
 Toujours valide
 Valide à partir de la création
 jusqu'à [minuit] plus 0 jour [] heure [] minute
 pendant 0 jour 7 heures 0 minute
 Valide dans un intervalle de dates

Crédit temps :
 Durée allouée: [] heure et [] minute
 Recréation tous les [] jour

Plages horaires
 Personnaliser les plages horaires héritées du profil

	de	de	de	de	de	de
<input type="checkbox"/> Chaque jour	00:00					24:00
<input checked="" type="checkbox"/> Lundi	08:00					18:00
<input checked="" type="checkbox"/> Mardi	08:00					18:00
<input checked="" type="checkbox"/> Mercredi	08:00					18:00
<input checked="" type="checkbox"/> Jeudi	08:00					18:00
<input checked="" type="checkbox"/> Vendredi	08:00					18:00
<input type="checkbox"/> Samedi	00:00					24:00
<input type="checkbox"/> Dimanche	00:00					24:00

Remplir les champs nécessaires.

21.2. Création pour un standardiste

Se rendre dans Administration > Administrateurs > Profils

Paramètres globaux

Nom
 Droits sur les données personnelles
 Permission de lecture sur les données personnelles
 Permission d'écriture sur les données personnelles
 Accès aux outils
 Outil d'administration
 Outil de délégation

Droits délégués

Autoriser la création d'utilisateurs pour les profils :

Autorisés:
Non autorisés:
<<< Ajouter
Supprimer >>>

Attention: Cet administrateur délégué ne sera pas en mesure de consulter la liste des utilisateurs créés

Autoriser l'administration des utilisateurs
 Autoriser la création de comptes en masse dans l'outil de délégation
 Autoriser la création de comptes individuels avec un identifiant aléatoire
 Autoriser la modification des paramètres de validité
 Autoriser l'impression de ticket de connexion au format badge
 Autoriser l'envoi du ticket de connexion par SMS avec le compte : Aucun compte SMS existant. Pour en créer un nouveau cliquez [ici](#)
 Autoriser l'envoi du ticket de connexion par mail avec le compte : Aucun compte Mail existant. Pour en créer un nouveau cliquez [ici](#)
 Autoriser l'administration des vouchers
 Autoriser la déconnexion d'utilisateurs provenant d'annuaires externes

Créer un profil.

Ensuite se rendre dans Administration > Administrateurs > Comptes

Gestion des comptes administrateurs

Identité de l'utilisateur

Identifiant *
 Mot de passe
 Confirmer mot de passe

Nom
 Prénom
 Mail
 Téléphone
 Fonction

Profil

Profils autorisés *

Outil d'administration Non
 Outil de délégation Oui
 Permission de lecture sur les données personnelles Oui
 Permission d'écriture sur les données personnelles Oui

* Champs obligatoires Valider

Indiquer les informations relatives à la personne concernée.

Espace dédié

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

UCOPIA
TURN YOUR WI-FI UP

Langue

Identification

Identifiant
Mot de passe

Connexion

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 :

Afficher les : Associations (4) Configurations (3) Modèles visuels (3)

Nom de la configuration	Formats	Modes de fonctionnement	Hébergé	Zones	Modèles	Actions
Portail captif						
default-portal	Laptop, Tablette, Smartphone, Mode dégradé	Standard	●	1	1	Ajouter une configuration
Guest	Laptop, Tablette, Smartphone, Mode dégradé	Standard	●	1	1	Ajouter une configuration
Connexion automatique						
Aucune configuration n'est définie.						
Portail de délégation						
default-deleg	Laptop	-	●	2	1	Ajouter une configuration

Options d'enregistrement des utilisateurs

Champs utilisateurs	Permettre la saisie	Obligatoire
Nom	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Prénom	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mot de passe	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sexe	<input type="checkbox"/>	<input type="checkbox"/>
Date de naissance	<input type="checkbox"/>	<input type="checkbox"/>
Téléphone	<input type="checkbox"/>	<input type="checkbox"/>
Adresse email	<input type="checkbox"/>	<input type="checkbox"/>
Nom de l'entreprise	<input type="checkbox"/>	<input type="checkbox"/>
Adresse postale	<input type="checkbox"/>	<input type="checkbox"/>
Langue préférée	<input type="checkbox"/>	<input type="checkbox"/>
Centres d'intérêts	<input type="checkbox"/>	<input type="checkbox"/>
Adresse MAC	<input type="checkbox"/>	<input type="checkbox"/>
Adresse IP	<input type="checkbox"/>	<input type="checkbox"/>
Champs additionnels 1	Choisir un champ ▼	<input type="checkbox"/>
Champs additionnels 2	Choisir un champ ▼	<input type="checkbox"/>
Champs additionnels 3	Choisir un champ ▼	<input type="checkbox"/>

Choisir les options désirées.