-

BTS SIO 2025 Option SISR

Epreuve E6

-

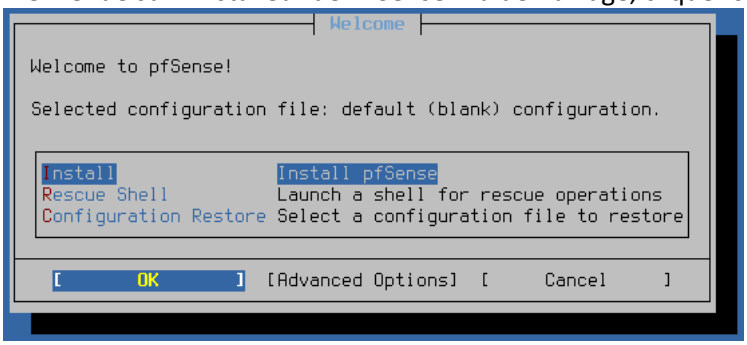
Situation professionnelle 2 – Documentation Technique

Table des matières

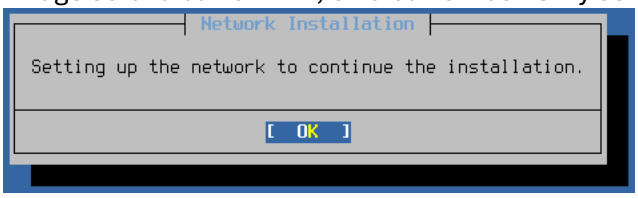
Documentation d’installation

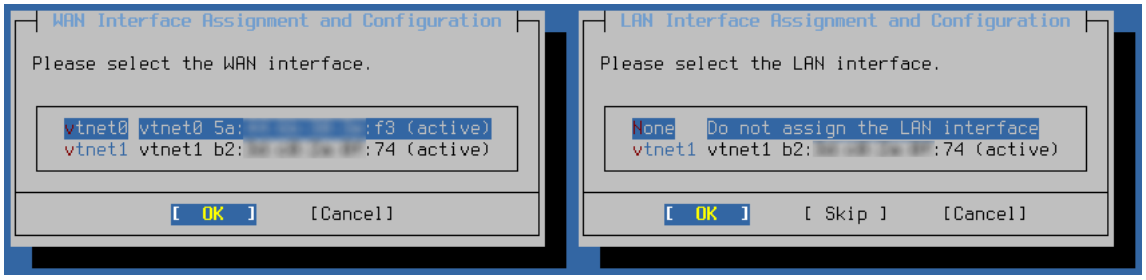
Installation d’un routeur PfSense avec la mise en place d’un VPN Road Warrior

Bienvenue sur l’installeur de PFSense. Au démarrage, cliquez sur Install.

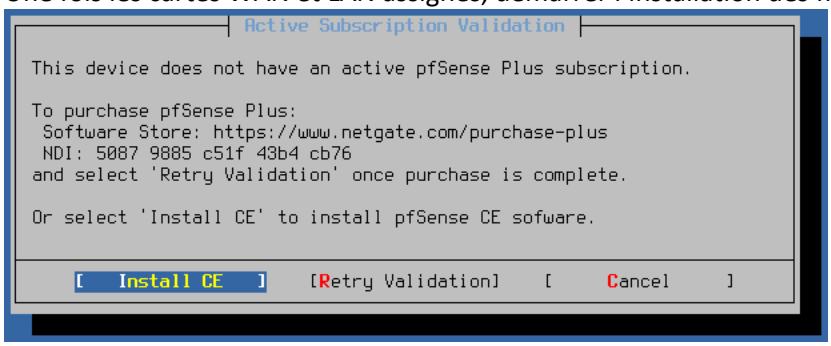


Après avoir démarré l’installation, assigner les interfaces WAN et LAN aux cartes réseaux, la carte Bridge sera la carte WAN, et la carte Host-Only sera la carte LAN.

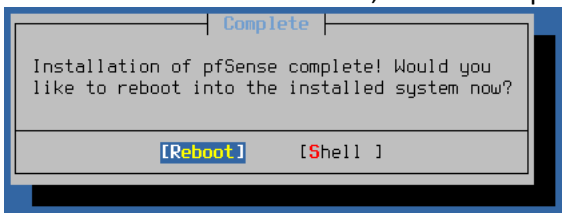




Il est recommandé d'attribuer une adresse IP fixe pour l'adresse LAN, pour éviter les problèmes d'accès à l'interface WEB de PFSense.
Une fois les cartes WAN et LAN assignés, démarrer l'installation des fichiers de pfSense.



Une fois l'installation terminée, redémarrer pfSense, et l'installations sera alors terminée.



Installation d'un serveur Windows SERVER 2022 avec les services AD DNS DHCP (avec basculement)

Prérequis :

- 1 Windows SERVER 2022 avec interface graphique (Carte réseau VMNet1)
- 1 Windows SERVER 2022 Core (Carte réseau VMNet1)
- 1 Routeur (Carte réseau VMNet1, et VMNet2) (optionnel, utilisé dans le cadre du projet M2i)

Description des cartes réseau dans ce cas :

- VMNet 1 : Carte Host-only (réseau LAN)
- VMNet2 : Carte NAT / Bridge (réseau WAN)

Cet exemple utilisera 2 serveurs mentionnés auparavant. Nous passerons par un routeur (PFSense) qui fera office de passerelle entre le réseau local et le réseau WAN. Nous allons voir comment installer les fonctionnalités AD DS, DNS (fonctionnalité obligatoire avec AD DS), ainsi que DHCP. Nous allons également voir comment répliquer tout cela sur le serveur Core pour assurer la disponibilité en cas de panne du serveur 1.
L'installation du rôle DNS ne sera pas mentionnée explicitement car elle est automatiquement installée avec l'Active Directory. Aucune configuration n'est alors requise pour que DNS fonctionne.

Étape 1 : Installation des rôles / fonctionnalités sur le serveur 1 :

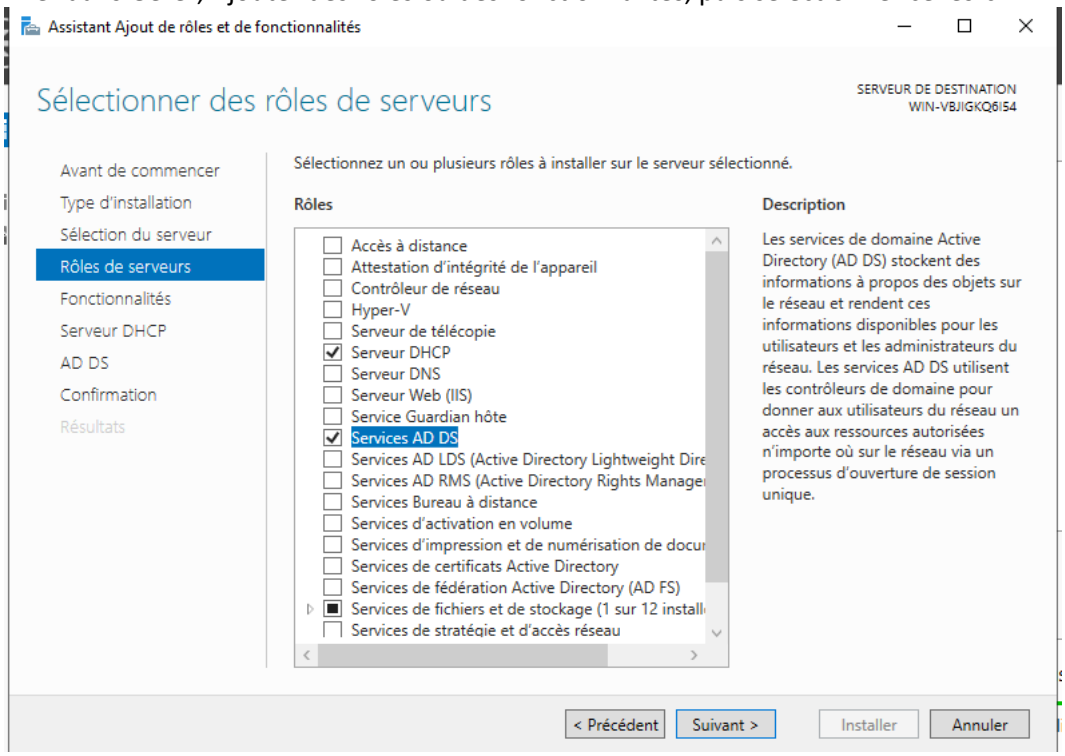
Installation du rôle sur le serveur

Pour commencer, nous allons définir une adresse IP fixe sur le serveur :

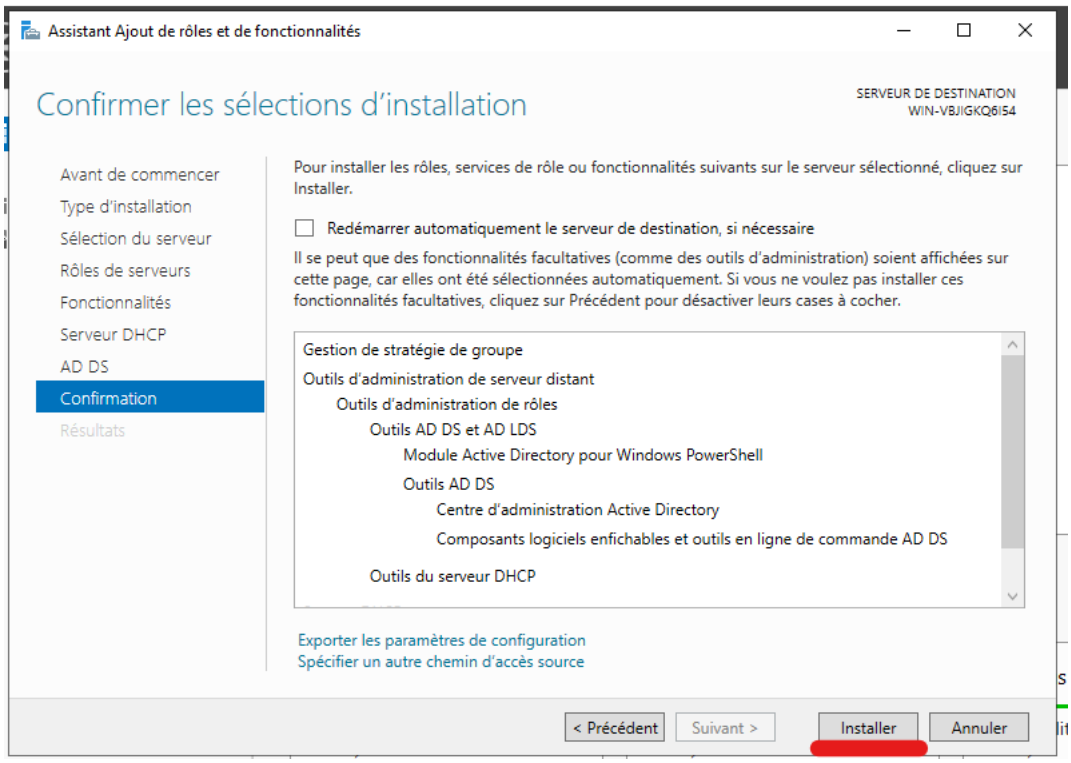
- Aller dans le gestionnaire de serveur sous Serveur Local
- Double cliquer sur Adresse IPv4 attribuée par DHCP
- Cliquer sur sa carte réseau *EthernetX*
- Aller dans les propriétés, puis Protocole Internet version 4
- Dans cette interface il sera alors possible de définir une adresse IP fixe.

Configuration du rôle AD avec mise en place d'une forêt

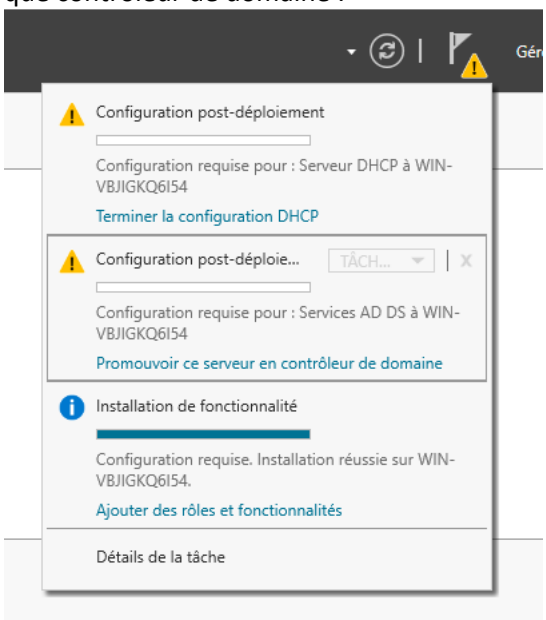
Aller dans Gérer, Ajouter des rôles ou des fonctionnalités, puis sélectionner celles-ci



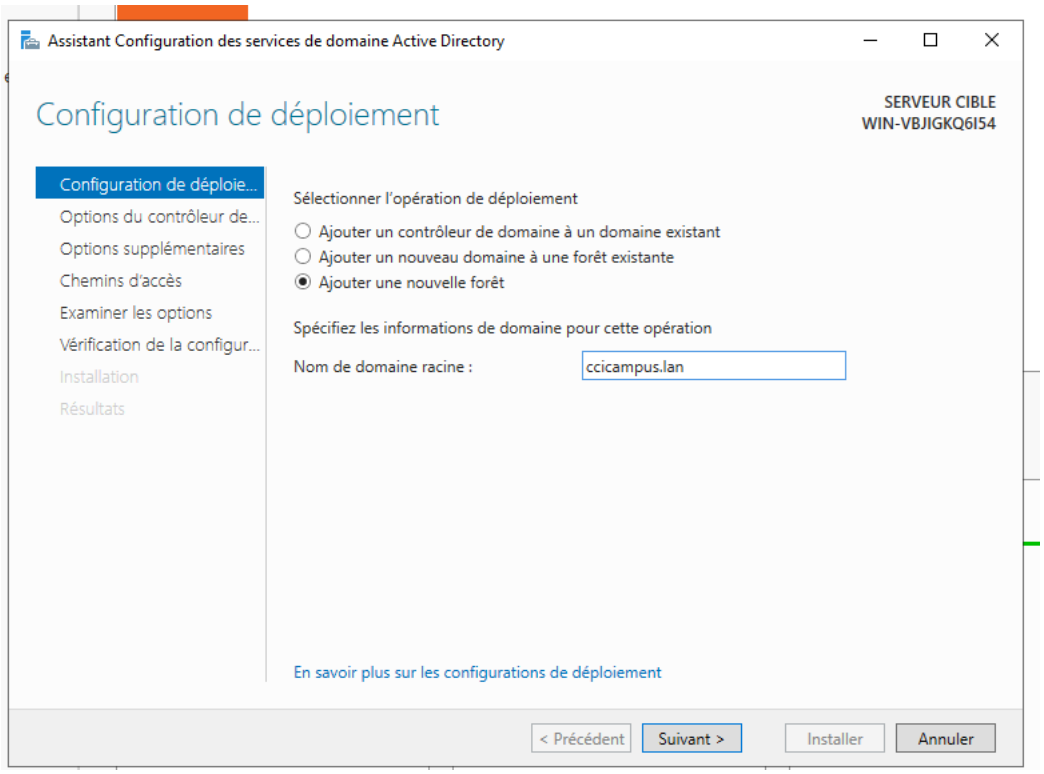
Lancer l'installation des rôles :



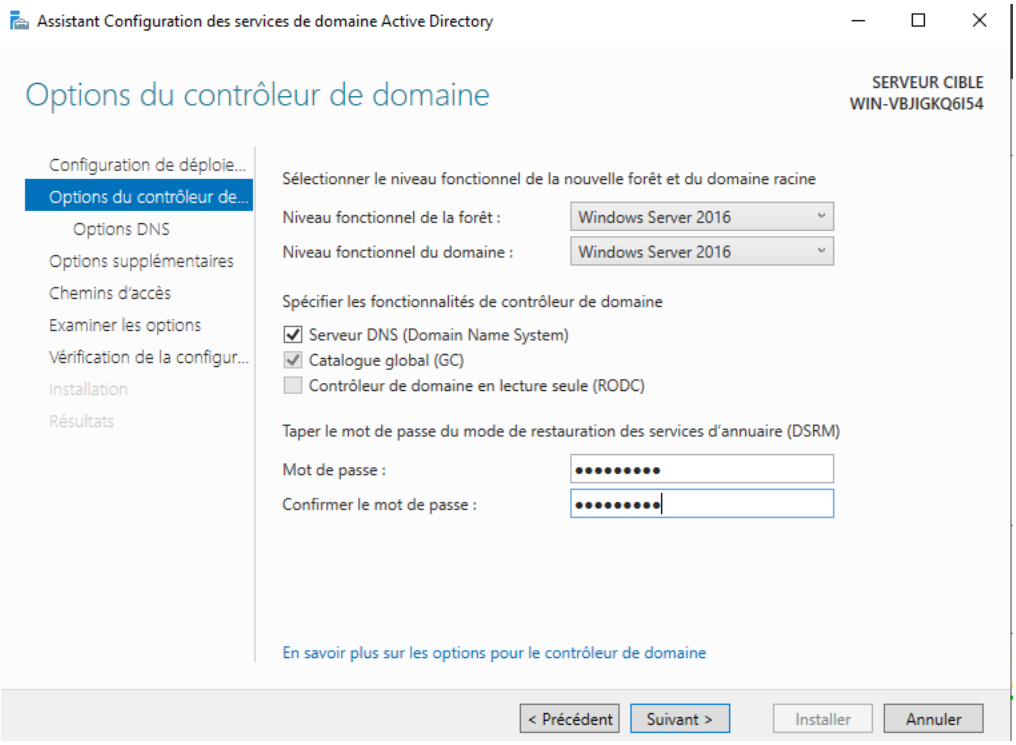
Ensuite, nous allons lancer la création de la forêt Active Directory en cliquant sur Promouvoir ce serveur en tant que contrôleur de domaine :



Nous allons définir le nom du domaine que nous voulons créer.



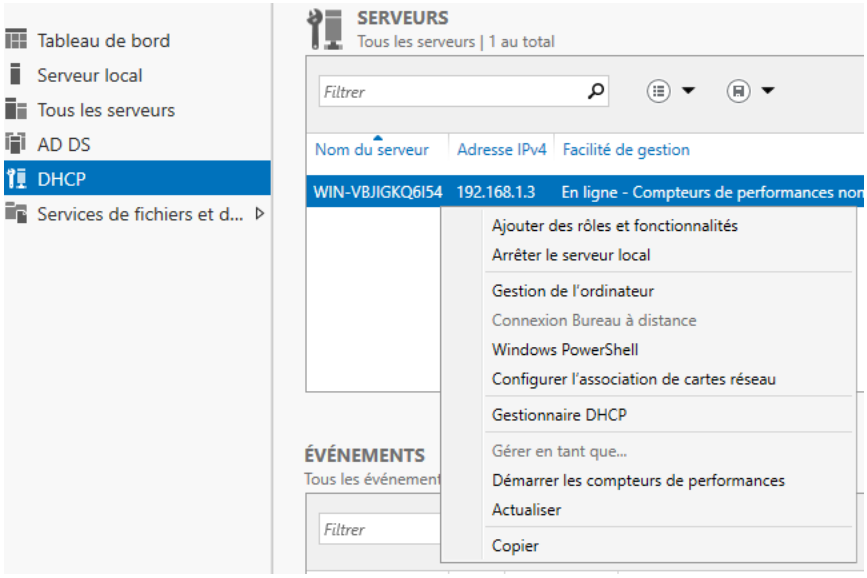
Nous allons également définir un mot de passe de restauration des services.



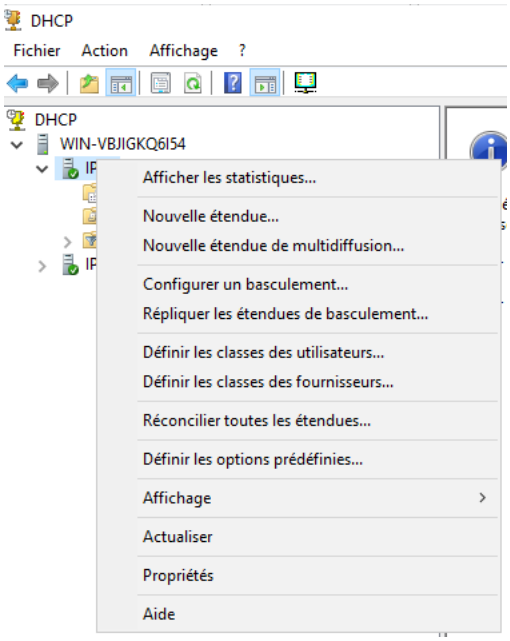
Une fois cela fait, l'AD sera complétement installé, prêt à l'usage.

Configuration du rôle DHCP avec création d'une étendue de test

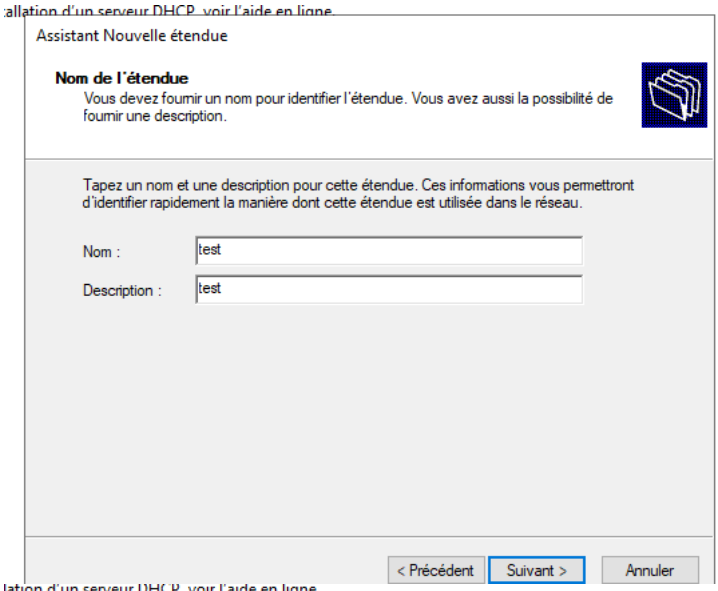
Pour compléter l'installation de DHCP, il suffira de se rendre dans le drapeau en haut à droite, cliquer sur Terminer la configuration DHCP. Il y aura juste à cliquer sur Suivant pour terminer la configuration.
Pour la création d'un bail DHCP, il va falloir se rendre sur le Gestionnaire DHCP :

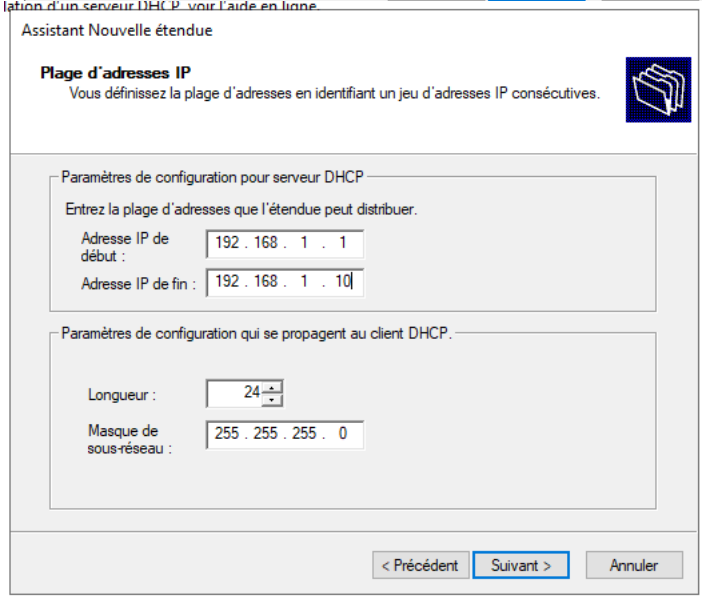


Une fois dessus, il faudra aller dans : *ServerName/IPv4* puis faire clic droit sur IPv4 pour créer une nouvelle étendue.



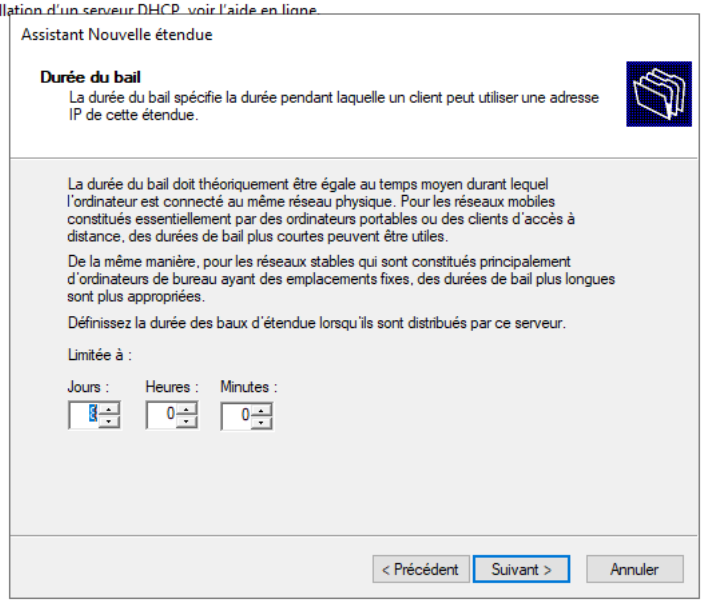
Nous allons ensuite la nommer, puis définir une plage d'adresse que l'on souhaite allouer à la plage.





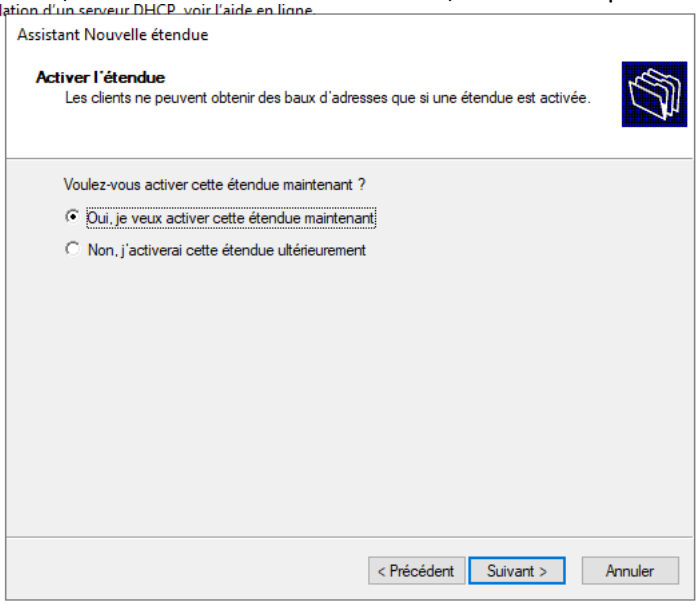
Il est également possible de modifier la durée du bail afin que les adresses utilisées puissent être reprises et ne restent pas bloqués pendant le temps par défaut (8 jours)

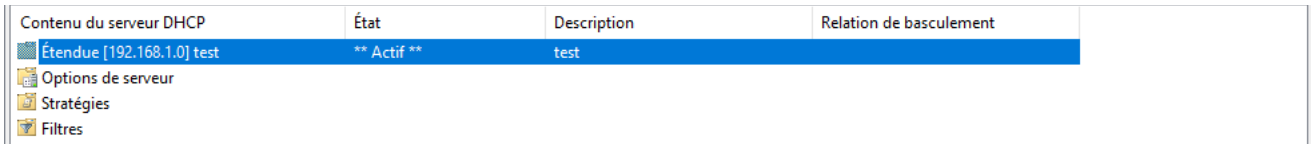
allation d'un serveur DHCP, voir l'aide en ligne.



A la fin, il faudra alors activer l'étendue, et tout sera prêt à la connexion d'un potentiel client.

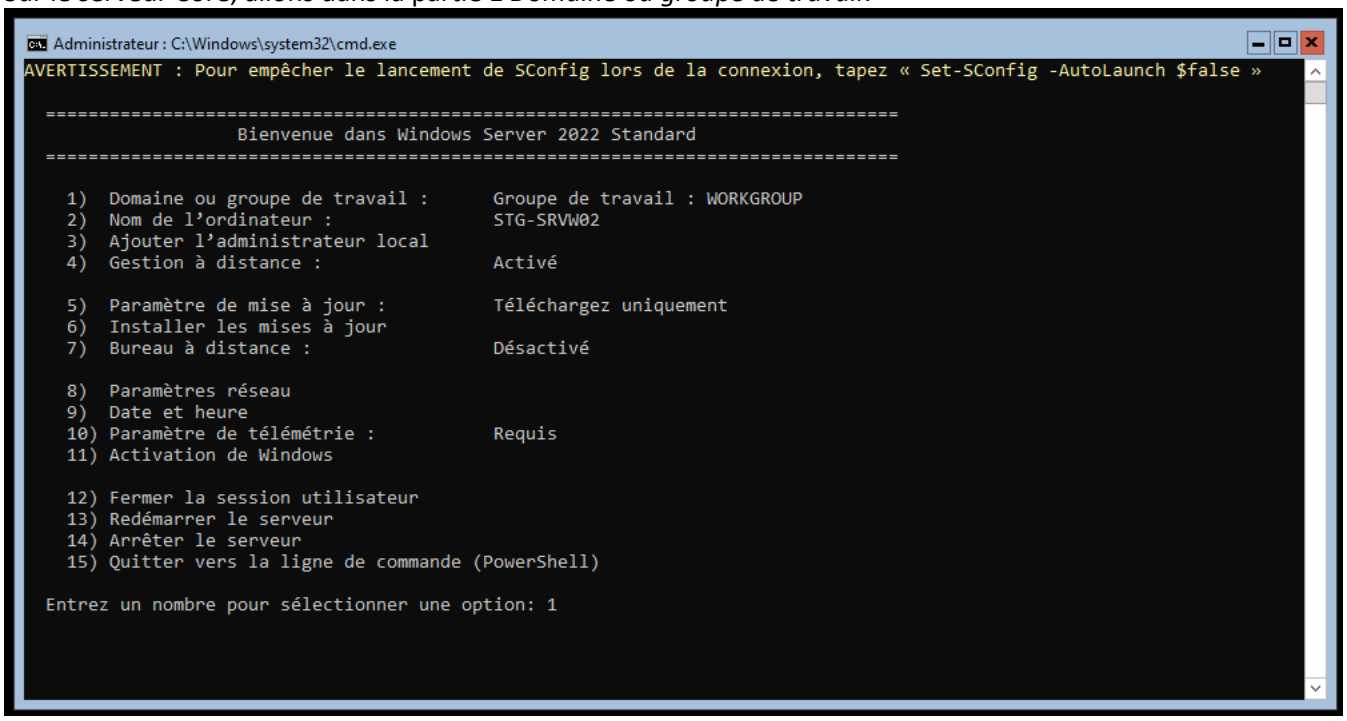
tallation d'un serveur DHCP, voir l'aide en ligne.



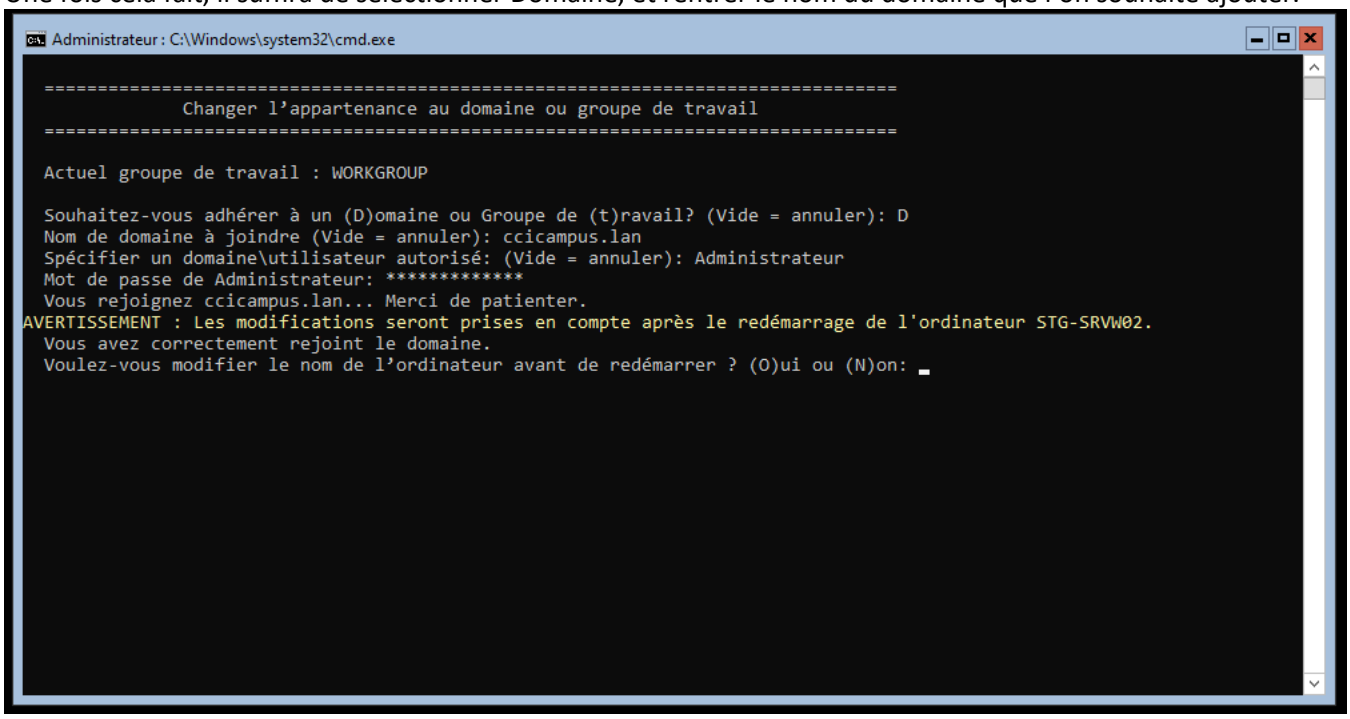


Étape 2 : Installation des rôles / fonctionnalités sur le serveur 2 :

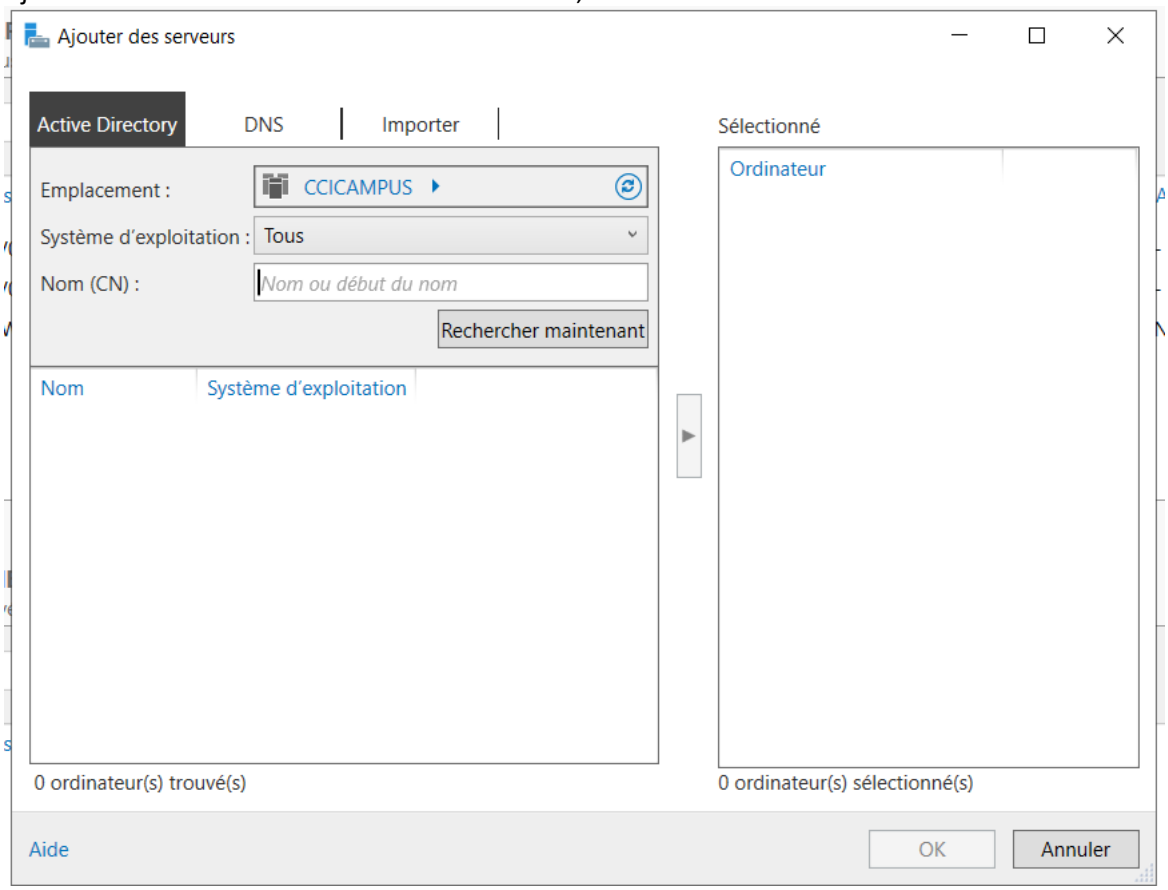
Sur le serveur Core, allons dans la partie 1 *Domaine ou groupe de travail*.



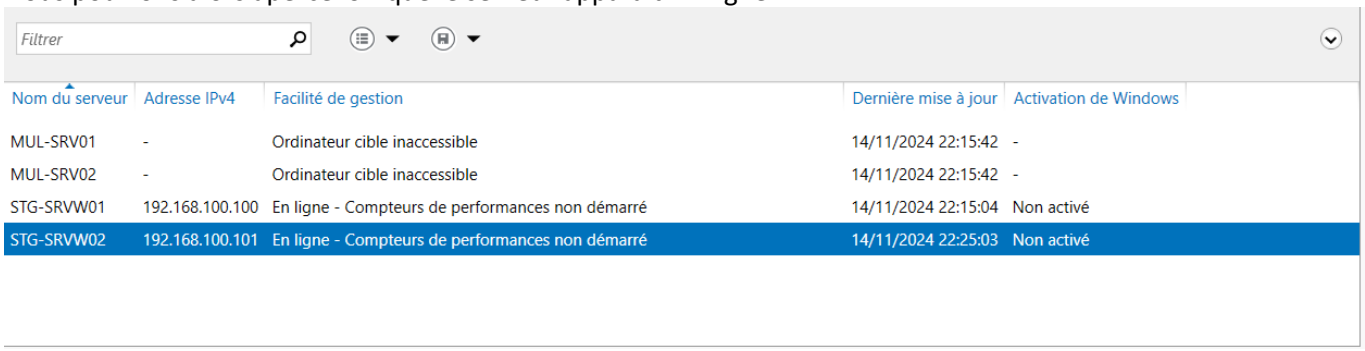
Une fois cela fait, il suffira de sélectionner Domaine, et rentrer le nom du domaine que l'on souhaite ajouter.



Une fois que le serveur sera dans le domaine, il sera possible de l'administrer depuis le serveur 1, pour cela, nous allons nous rendre dans la section Tous les serveurs du gestionnaire de serveur, puis faire Clic droit dessus, et Ajouter un serveur. Il suffira de rentrer son nom, le sélectionner et ce sera bon.

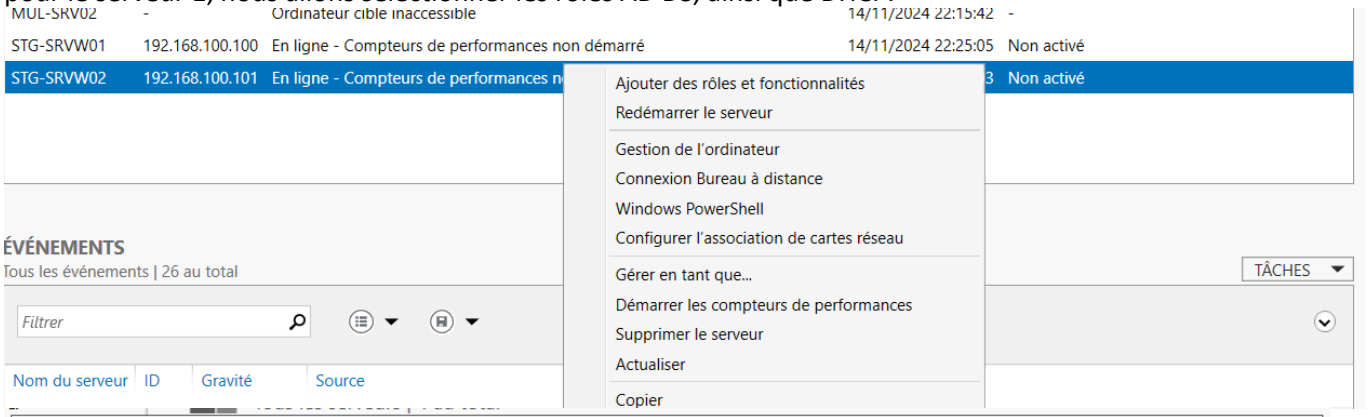


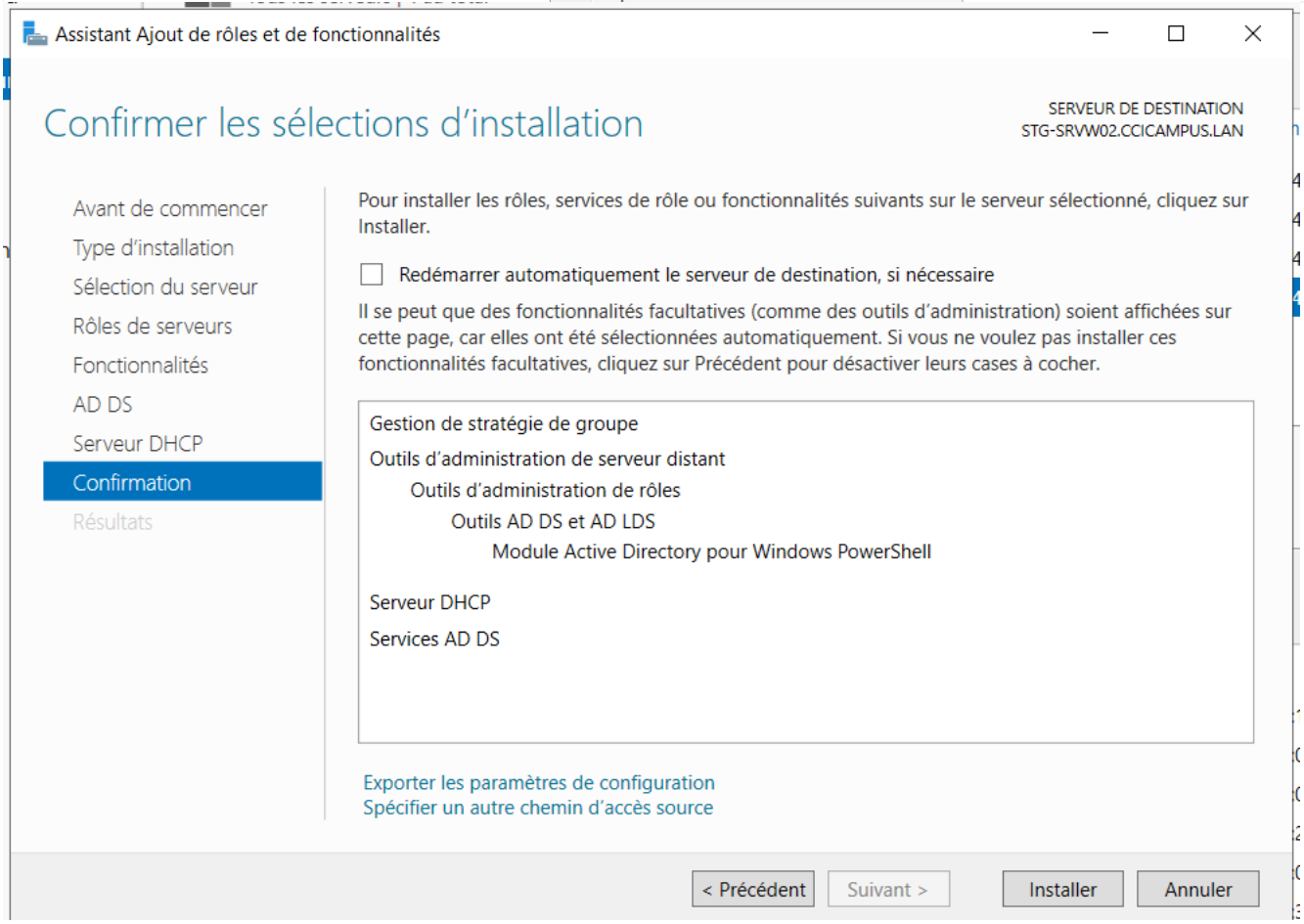
Nous pourrons alors apercevoir que le serveur apparaît En Ligne.



Installation des rôles AD DS et DHCP sur le second serveur.

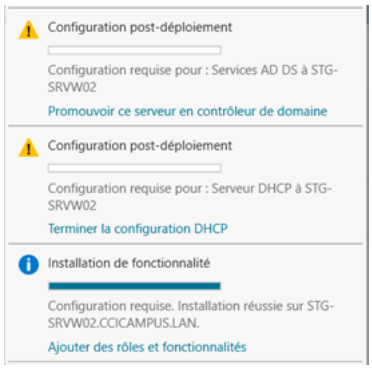
Pour commencer, nous allons faire clic droit sur le serveur 2, puis ajouter des rôles ou des fonctionnalités. Comme pour le serveur 1, nous allons sélectionner les rôles AD DS, ainsi que DHCP.



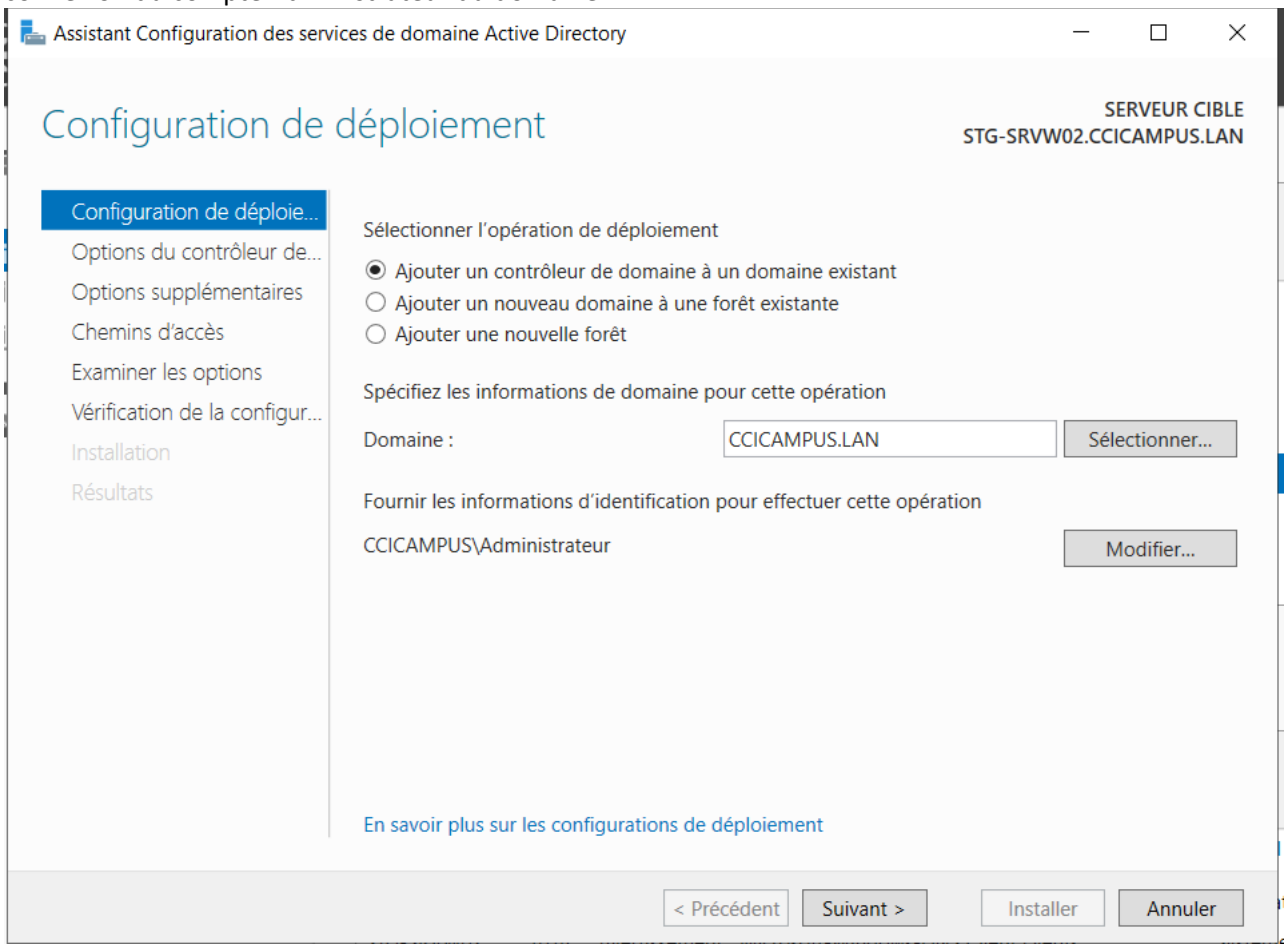


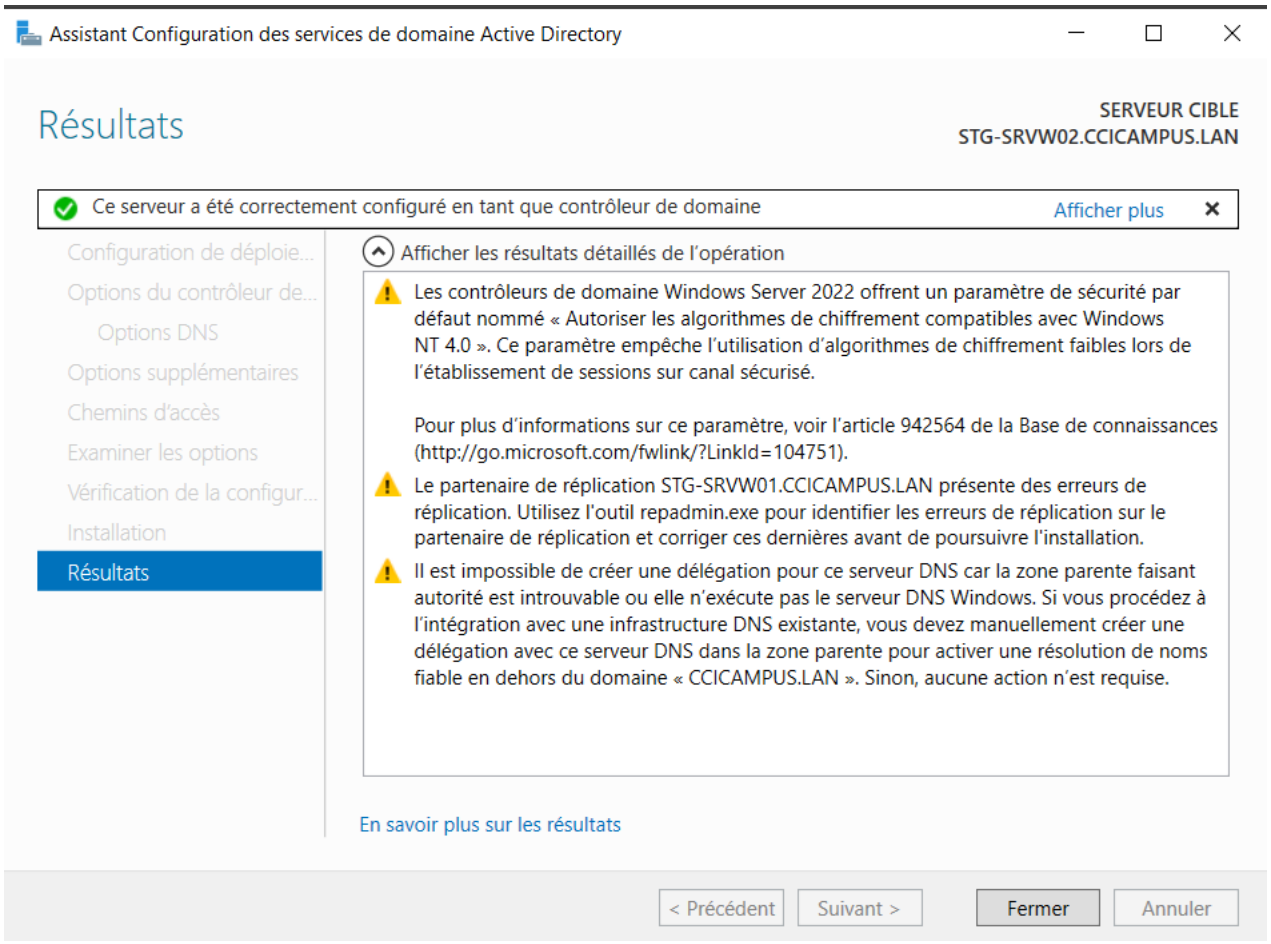
Concernant la configuration du DHCP, elle est identique à celle réalisée auparavant sur le premier serveur.

Pour la configuration de la réplication de l'AD, il faudra se rendre dans le petit drapeau d'information, puis cliquer sur Promouvoir ce serveur en tant que contrôleur de domaine.



Une fois cela fait, nous allons rentrer le domaine déjà existant ici, il faudra également rentrer les informations de connexion du compte Administrateur du domaine.

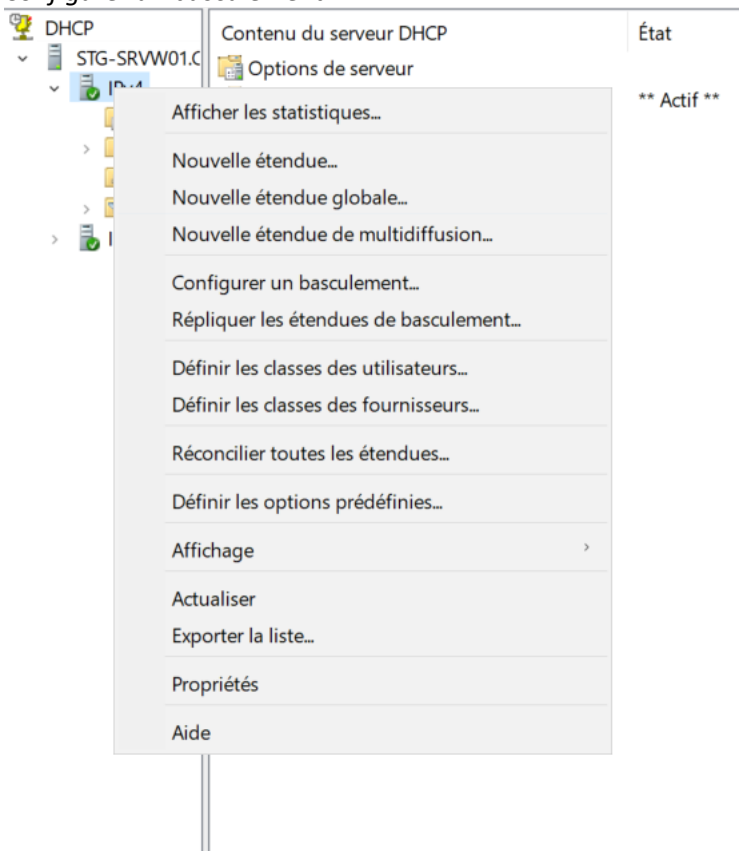




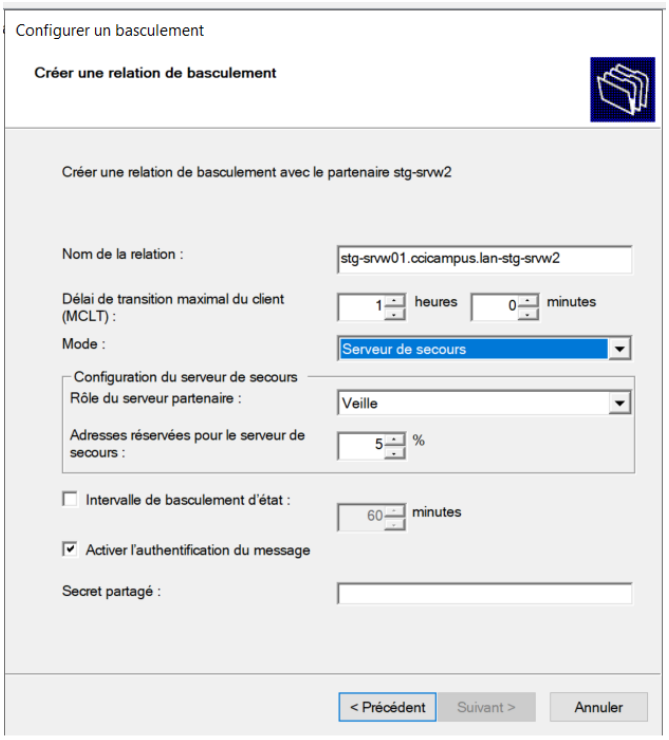
Cette étape nous montre que le serveur est désormais bien contrôleur de domaine secondaire du domaine CCICAMPUS.LAN.

Configuration du basculement DHCP

Nous allons nous rendre sur le gestionnaire DHCP du premier serveur, puis clic droit sur IPv4 pour afficher l'option *Configurer un basculement*.



Une fois dans l'interface, nous allons rentrer les informations du serveur 2 pour définir qui va gérer le basculement, et comment.



Installation d'un serveur de téléphonie VOIP

1. Installation d'Asterisk

Cette section détaille la procédure d'installation d'Asterisk 22.3.0 par **compilation des sources** sur Debian 11. Cette méthode offre une flexibilité optimale pour sélectionner les modules nécessaires à notre environnement VOIP.

Préparation du système

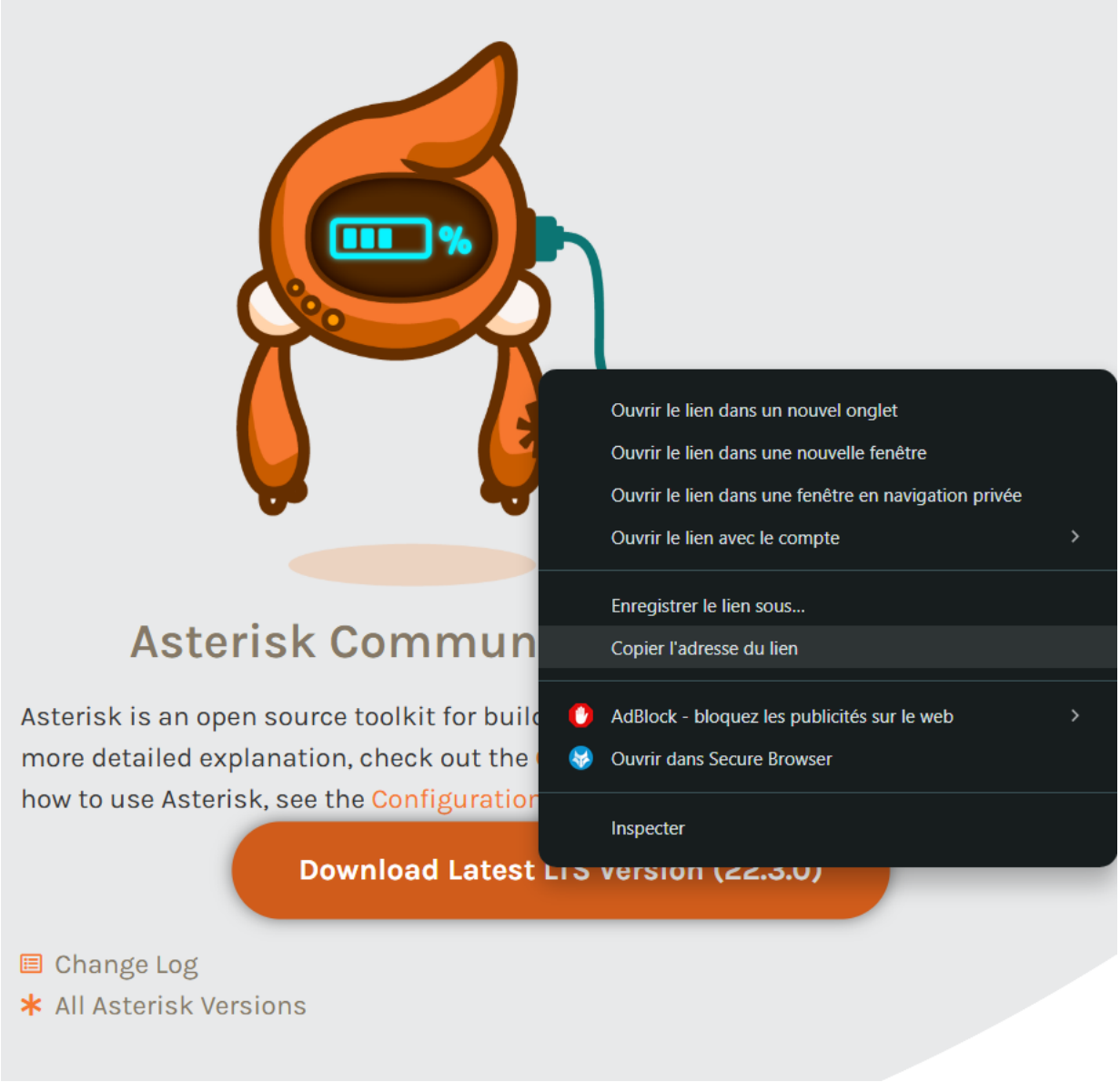
Avant de commencer l'installation, assurez-vous que tous les paquets système sont à jour :

```
root@E-SRV-VOIP:~# sudo apt update && sudo apt upgrade -y
```

Installez ensuite les dépendances requises pour la compilation :

```
root@E-SRV-VOIP:~# sudo apt install -y build-essential wget git curl subvers
ion \
  libjansson-dev libxml2-dev libsqlite3-dev uuid-dev
```

Récupérez les sources d'Asterisk depuis le site officiel. Et sur le bouton pour télécharger la dernière version faite clique doit puis « Copier l'adresse du lien ».



Téléchargement de Asterisk

Créée un dossier que vous allez nommer « VOIP »

```
root@E-SRV-VOIP:~/test# mkdir VOIP
```

Puis allé dans le dossier VOIP et coller l'adresse du lien de Asterisk pour le télécharger

```
root@E-SRV-VOIP:~# cd VOIP
root@E-SRV-VOIP:~/VOIP# wget https://downloads.asterisk.org/pub/telephony/as
terisk/asterisk-22-current.tar.gz
```

Maintenant il faudra unzip l'archive.

```
root@E-SRV-VOIP:~/VOIP# tar -xvzf asterisk-22-current.tar.gz
```

Configuration de la compilation

Exécutez le script de configuration pour vérifier les dépendances manquantes :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# ./configure
```

***Attention** : Notez toute dépendance manquante signalée à cette étape et installez-la avant de continuer.*

Pour sélectionner les modules à compiler, utilisez l'outil de configuration interactif :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# make menuconfig
```

Dans l'interface qui s'affiche, assurez-vous d'activer les modules suivants, essentiels pour notre configuration VOIP :

- **chan_pjsip** (Canal SIP basé sur PJSIP)
- **res_rtp_asterisk** (Gestion des flux RTP)
- Autres modules de base pour la téléphonie IP

Compilation et installation

Lancez la compilation avec les commandes suivantes :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# make
make install
make samples
make config
```

Cette étape peut prendre plusieurs minutes selon les performances de votre machine.

Vérification de l'installation

Vérifiez que le service Asterisk fonctionne correctement :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# systemctl status asterisk
● asterisk.service - LSB: Asterisk PBX
     Loaded: loaded (/etc/init.d/asterisk; generated)
     Active: active (running) since Thu 2025-04-10 10:59:16 CEST; 43min ago
       Docs: man:systemd-sysv-generator(8)
    Process: 814 ExecStart=/etc/init.d/asterisk start (code=exited, status=>
      Tasks: 65 (limit: 2264)
     Memory: 122.0M
        CPU: 20.803s
     CGroup: /system.slice/asterisk.service
             └─866 /usr/sbin/asterisk

avril 10 10:59:16 E-SRV-VOIP systemd[1]: Starting LSB: Asterisk PBX...
avril 10 10:59:16 E-SRV-VOIP asterisk[814]: Starting Asterisk PBX: asterisk.
avril 10 10:59:16 E-SRV-VOIP systemd[1]: Started LSB: Asterisk PBX.
lines 1-14/14 (END)
```

Vous devriez voir une sortie indiquant que le service est actif (running).

Paramétrage initial du service

Assurez-vous que le service Asterisk démarre automatiquement au démarrage du système sinon faites les commandes ci-dessous.

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# systemctl enable asterisk
```

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# systemctl start asterisk
```

2. Configuration de base

Cette section décrit la configuration initiale d'Asterisk après l'installation pour établir une plateforme VOIP opérationnelle. Nous nous concentrons sur les deux fichiers de configuration essentiels qui nécessitent des modifications pour une première mise en service fonctionnelle.

Emplacement des fichiers de configuration

Les fichiers de configuration d'Asterisk se trouvent dans le répertoire **/etc/asterisk** . Dans notre configuration de base, seuls deux fichiers nécessitent des modifications :

Fichier	Fonction
pjsip.conf	Configuration des comptes SIP et transports
extensions.conf	Plan de numérotation et logique d'appel

Configuration du transport SIP

La première étape consiste à configurer le transport SIP dans le fichier **pjsip.conf**. Cette configuration permet à Asterisk d'écouter les requêtes SIP entrantes.

Ouvrez le fichier avec votre éditeur :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# nano /etc/asterisk/pjsip.conf
```

Ajoutez la section de transport UDP suivante :

```
[transport-udp]
type=transport
protocol=udp
bind=0.0.0.0:5060
```

L'utilisation de 0.0.0.0 permet d'écouter sur toutes les interfaces réseau. Dans un environnement de production, limitez cette écoute à des interfaces spécifiques pour des raisons de sécurité.

Création des comptes PJSIP

Notre configuration minimale comprend deux comptes SIP (1001 et 1002) pour permettre des tests d'appels entre deux postes téléphoniques. Toujours dans le fichier **pjsip.conf**, ajoutez les sections suivantes :

```
[1001]
type=endpoint
transport=transport-udp
context=internal
disallow=all
allow=ulaw,alaw,g722
auth=auth1001
aors=1001
max_contacts=1

[1001]
type=auth
auth_type=userpass
password=P@ssword10
username=admin1

[1001]
type=aor
max_contacts=1
;contact=sip:1001@192.168.100.30:5060
```

Cette configuration définit pour chaque utilisateur :

- Un **endpoint** : point de terminaison SIP
- Une **authentification** : identifiants de connexion
- Un **AoR** (Address of Record) : gestion de l'enregistrement

Configuration du plan de numérotation

Le plan de numérotation définit le comportement d'Asterisk lorsqu'un numéro est composé. Ouvrez le fichier extensions.conf :

```
root@E-SRV-VOIP:/etc/asterisk# nano /etc/asterisk/extensions.conf
root@E-SRV-VOIP:/etc/asterisk#
```

Ajoutez la configuration suivante pour permettre aux comptes de s'appeler mutuellement :

```
[default]
exten => 1001,1,Answer()
exten => 1001,n,Dial(PJSIP/1001,20)
exten => 1001,n,Hangup()

exten => 1002,1,Answer()
exten => 1002,n,Dial(PJSIP/1002,20)
exten => 1002,n,Hangup()
```

Explication du plan de numérotation

Chaque ligne du plan de numérotation suit la syntaxe :

Exten => numéro,priorité,Application(paramètres)

Application des modifications

Après avoir modifié les fichiers de configuration, rechargez-les dans Asterisk sans redémarrer le service :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# asterisk -rx "core reload"
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
```

Pour vérifier que les configurations sont correctement chargées :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# asterisk -rx "pjsip show endpoints"

 Endpoint:  <Endpoint/CID.....................................>  <State.....
>  <Channels.>
    I/OAuth:  <AuthId/UserName.................................................
.............>
        Aor:  <Aor.........................................>  <MaxContact
>
      Contact:  <Aor/ContactUri.........................> <Hash....> <Statu
s> <RTT(ms)..>
  Transport:  <TransportId........>  <Type>  <cos>  <tos>  <BindAddress.....
.............>
   Identify:  <Identify/Endpoint.............................................
.............>
        Match:  <criteria.........................>
    Channel:  <ChannelId.....................................>  <State.....
>  <Time.....>
        Exten: <DialedExten...........>  CLCID: <ConnectedLineCID.......>
==============================================================================
==============

 Endpoint:  1001                                                 Unavailable
   0 of inf
     InAuth:  1001/1001
        Aor:  1001                                               1

 Endpoint:  1002                                                 Unavailable
   0 of inf
     InAuth:  1002/1002
        Aor:  1002                                               1


Objects found: 2

root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
```

Vous devriez voir les endpoints 1001 et 1002 listés dans la sortie.

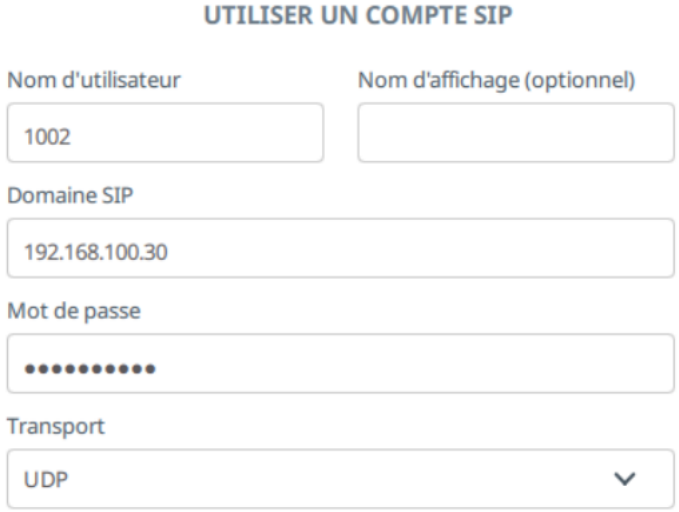
Vérification des transports
Vérifiez que le transport SIP est correctement configuré :

```
root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0# asterisk -rx "pjsip show transports"

Transport:  <TransportId........>  <Type>  <cos>  <tos>  <BindAddress.......
.............>
===============================================================================
==============

Transport:  transport-udp             udp      0      0  0.0.0.0:5060

Objects found: 1

root@E-SRV-VOIP:~/VOIP/asterisk-22.3.0#
```

Le transport UDP doit apparaître comme actif et en écoute sur l'adresse spécifiée.

3. Tests et validation du système

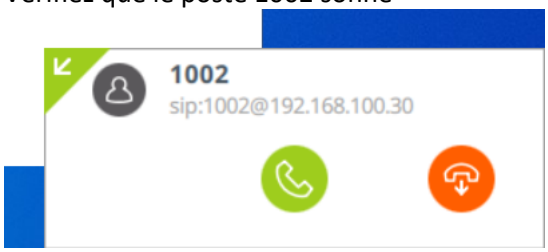
Configuration du softphone Linphone
Configurez Linphone sur les postes de test avec les paramètres suivants :



Une fois cliqué sur enregistrer vous devriez voir l'adresse IP du poste client et le port utilisé. Faite la même manipulation sur un ordinateur différents du même réseau avec le 2ème compte SIP.
Test d'appel basique
Pour valider la configuration complète, effectuez un appel entre les extensions :

Depuis le poste 1002, composez le 1001

Vérifiez que le poste 1002 sonne

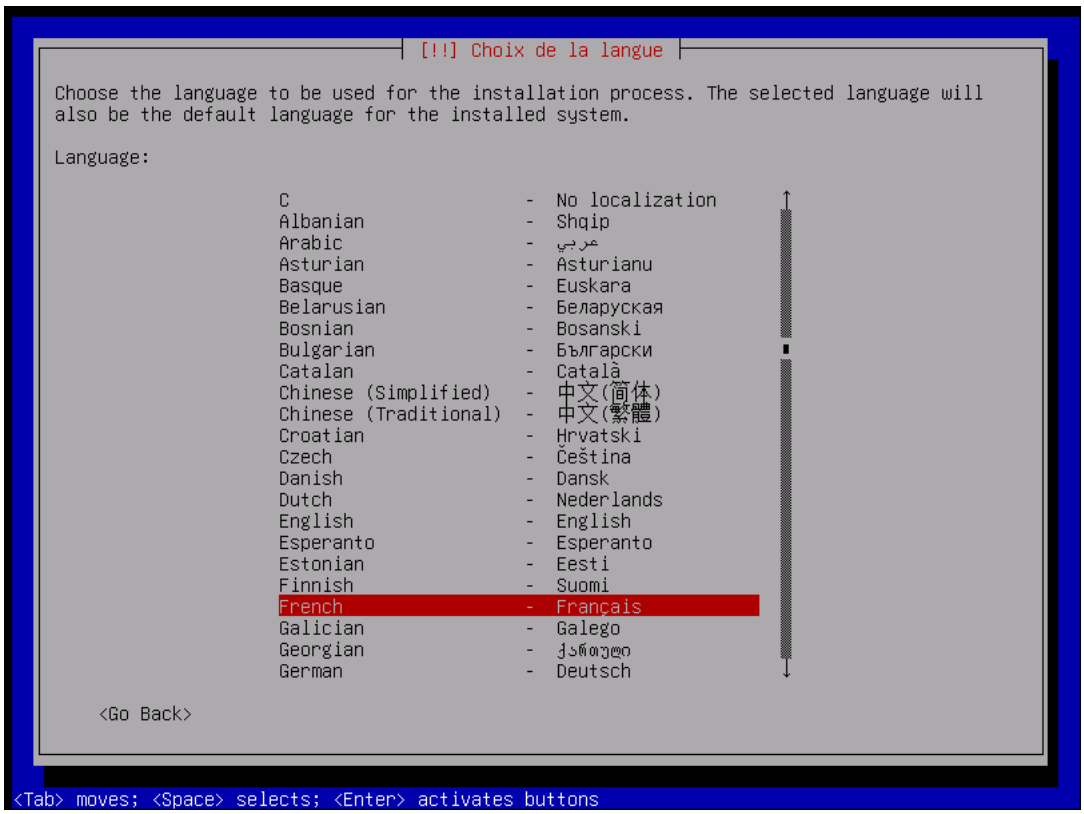


Comme vous pouvez l'apercevoir ci-dessus, je reçois bien l'appelle de 1002. Et en décrochant j'ai bien un retour audio du compte sans latence et bug.

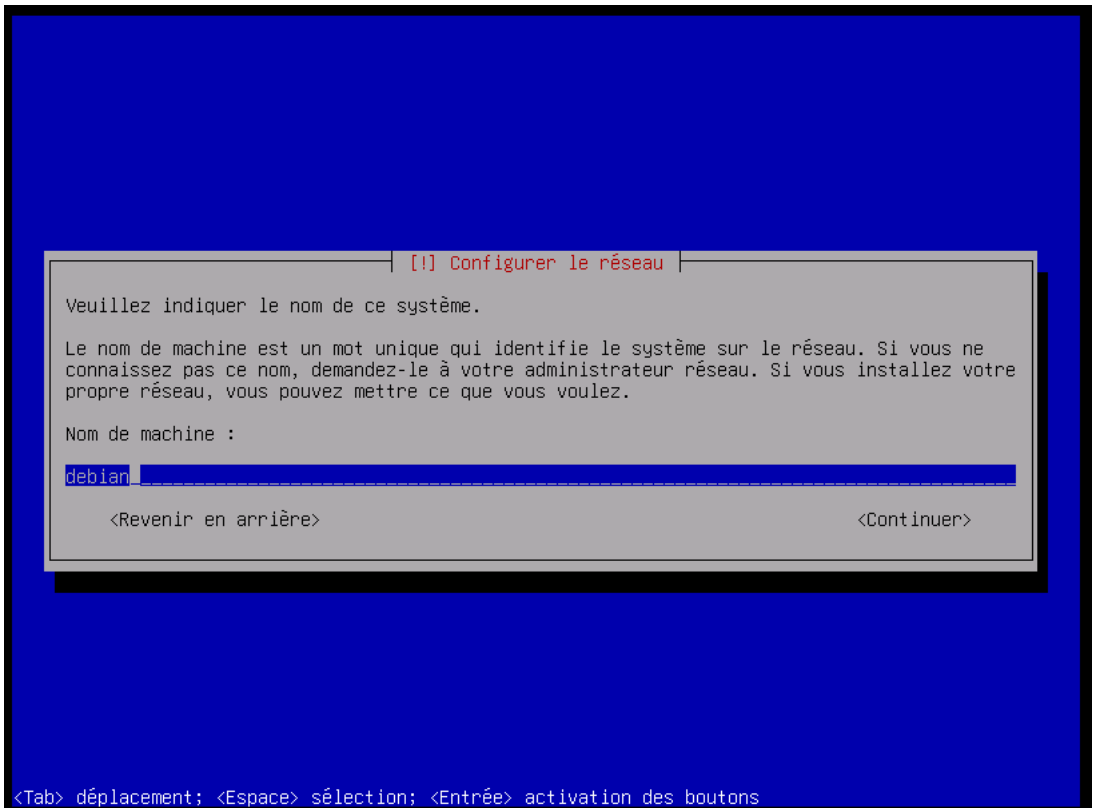
Installation d’un serveur de messagerie sur Debian 12

Partie 1 : Installation de Debian

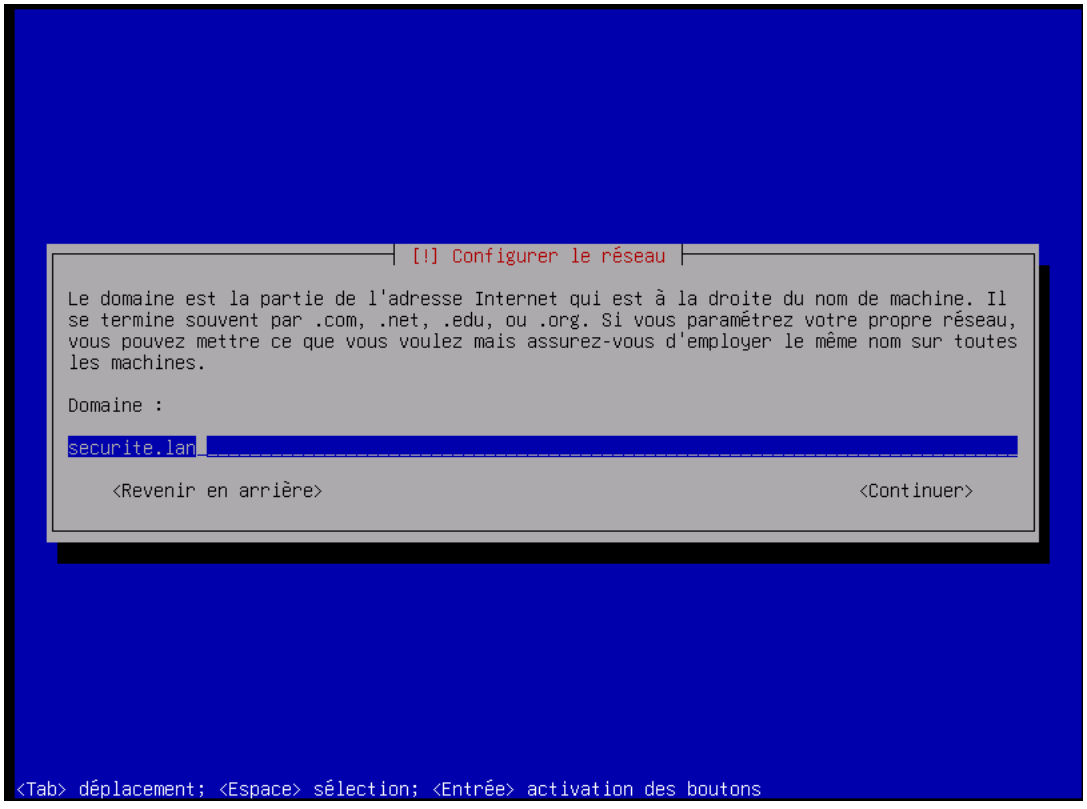
Bienvenue sur l’installeur de Debian 12, pour commencer, choisissez la langue de votre choix :



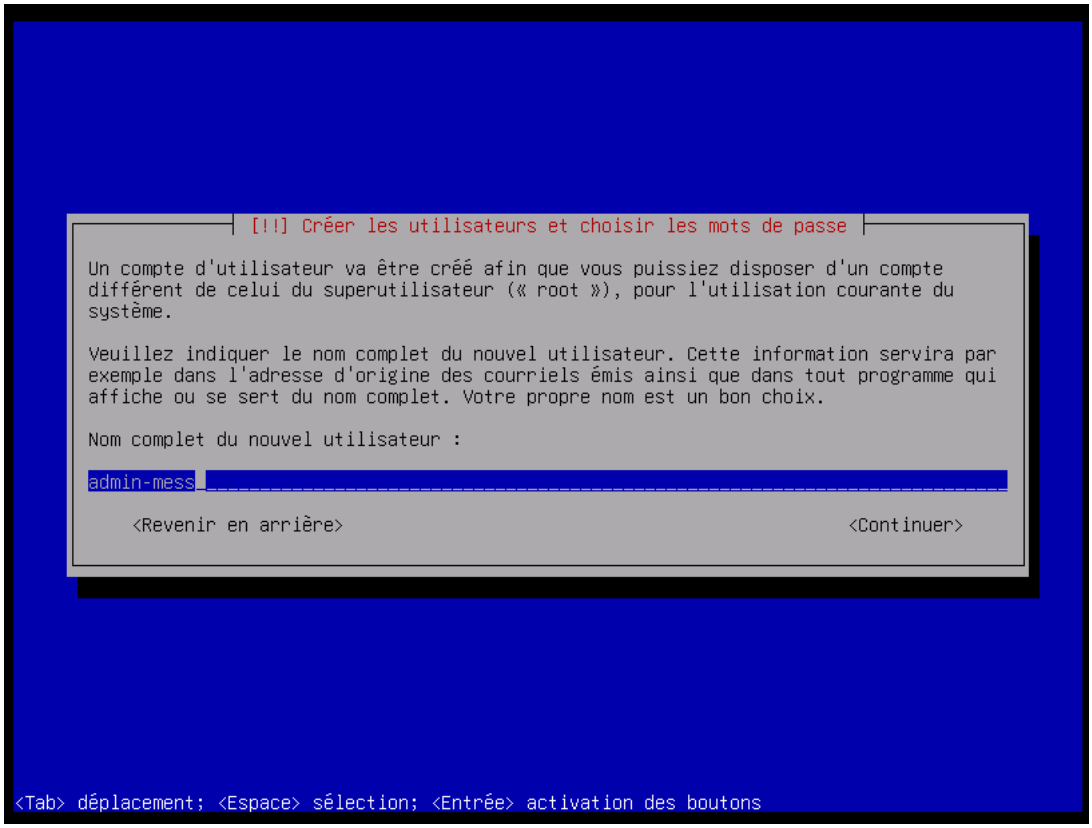
Ensuite, définissez un nom de machine pour votre serveur Debian.



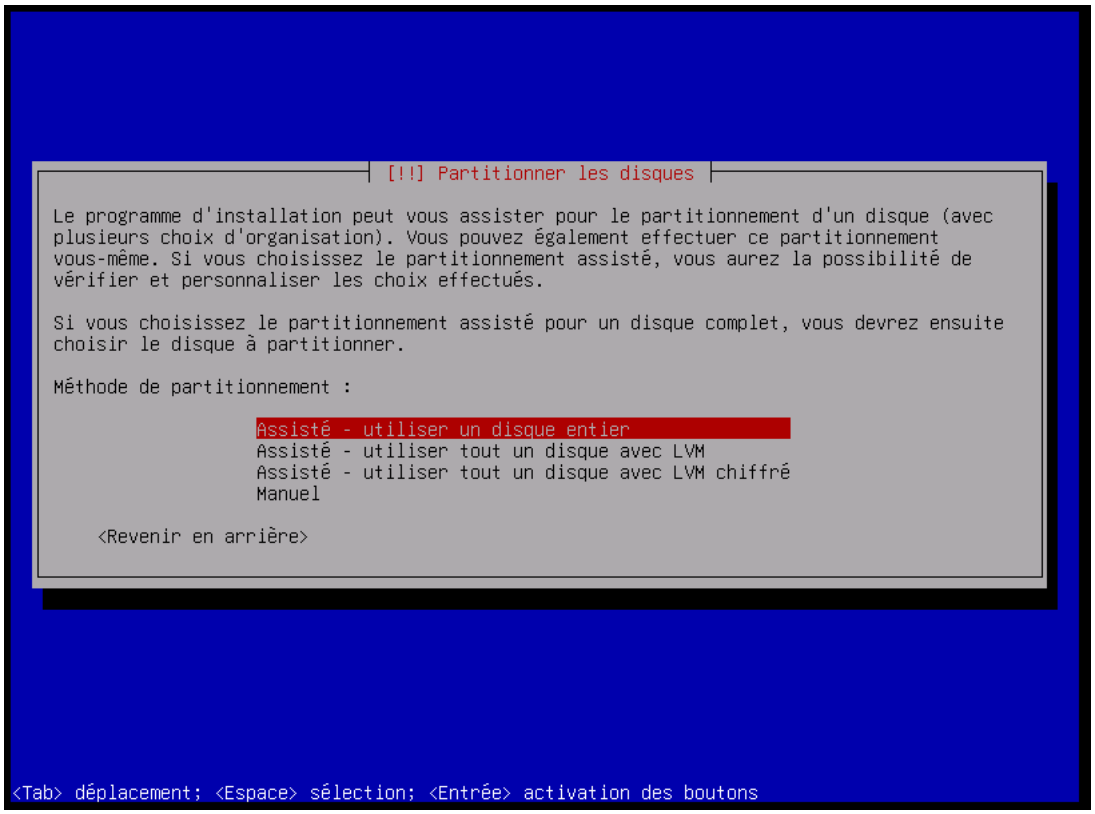
Vous pouvez, si vous le souhaitez déjà rentrer le nom du domaine à cette étape



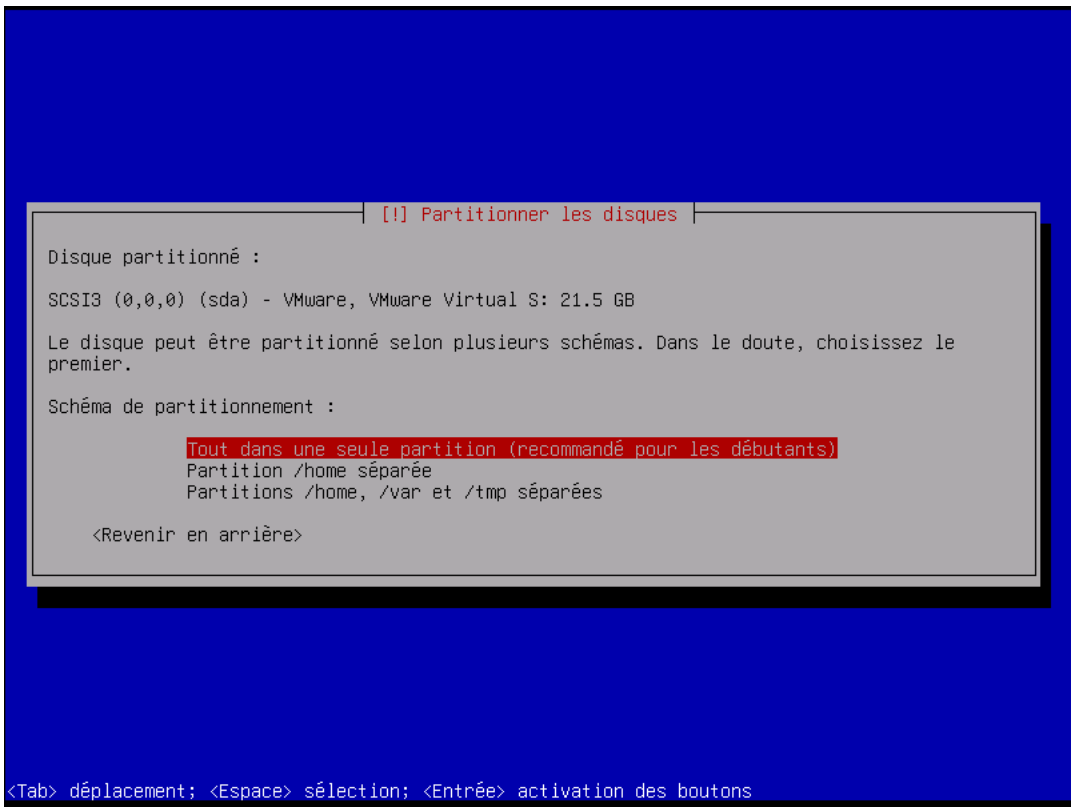
Maintenant, nous allons définir un nom d'utilisateur et un mot de passe pour l'utilisateur que l'on va utiliser avec le serveur :



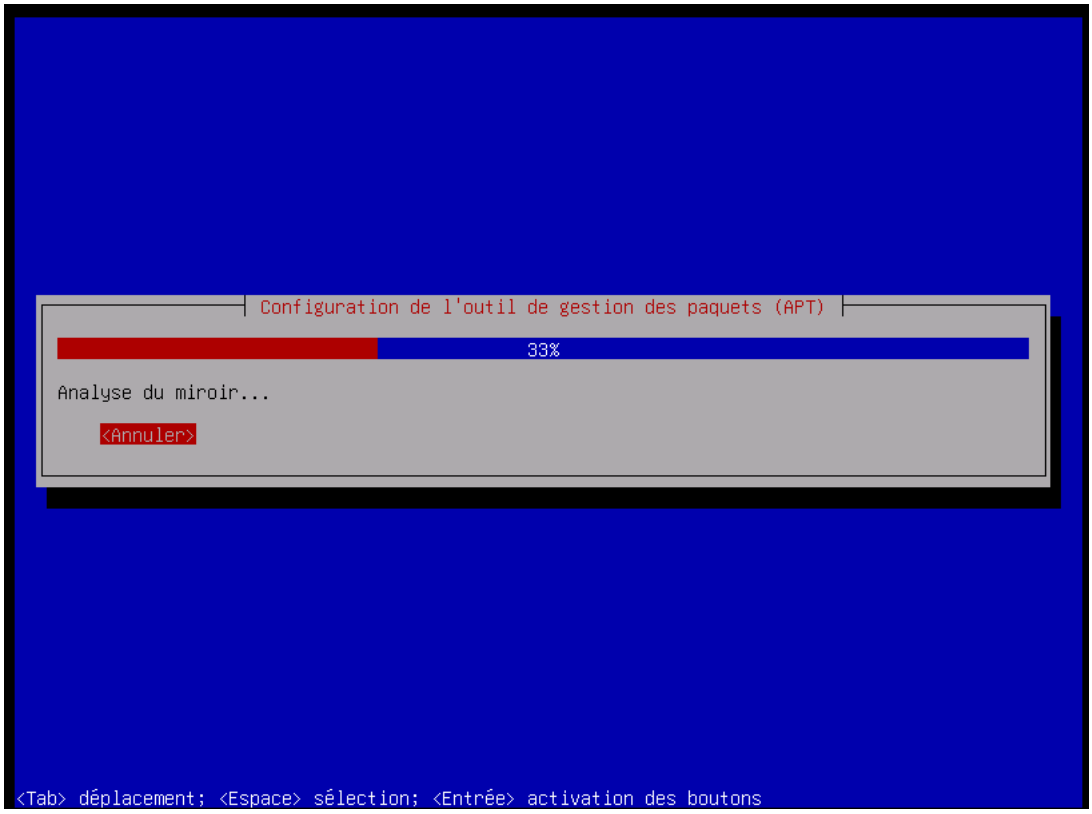
Nous allons continuer avec un disque entier, le partitionnement du disque n'est pas forcément nécessaire pour cet usage.



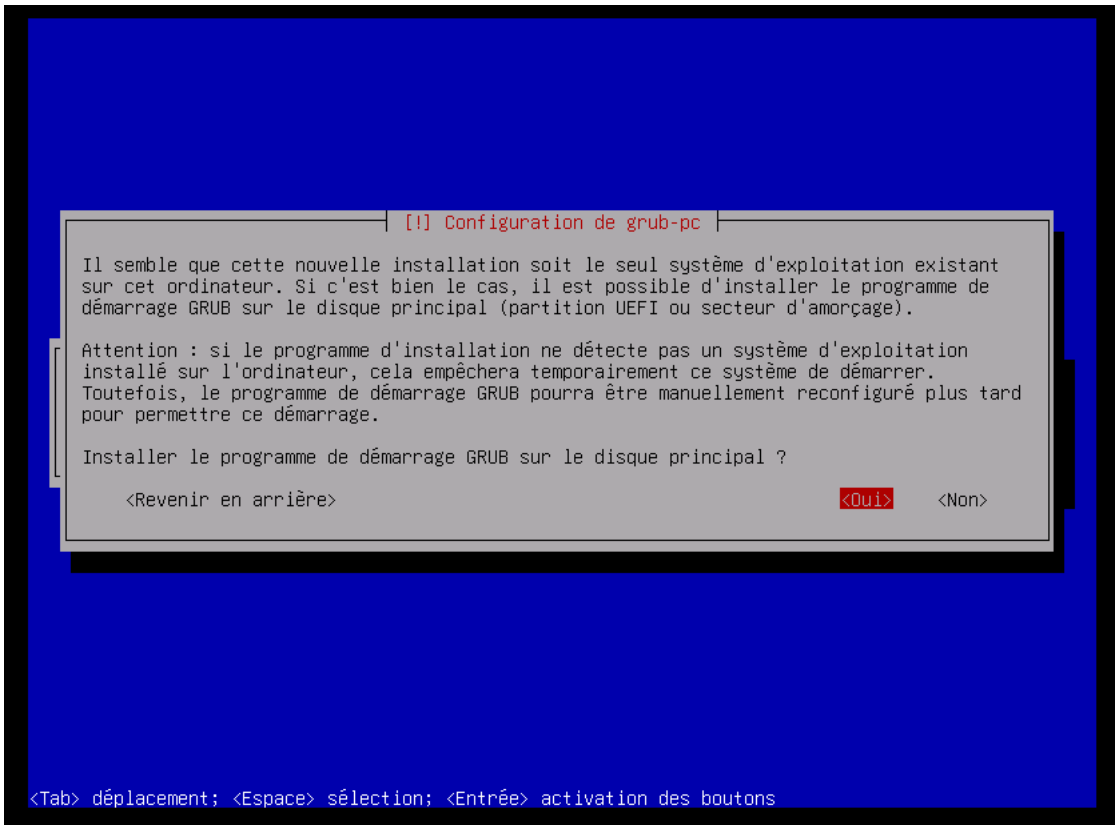
En conséquent, nous allons tout mettre dans la même partition



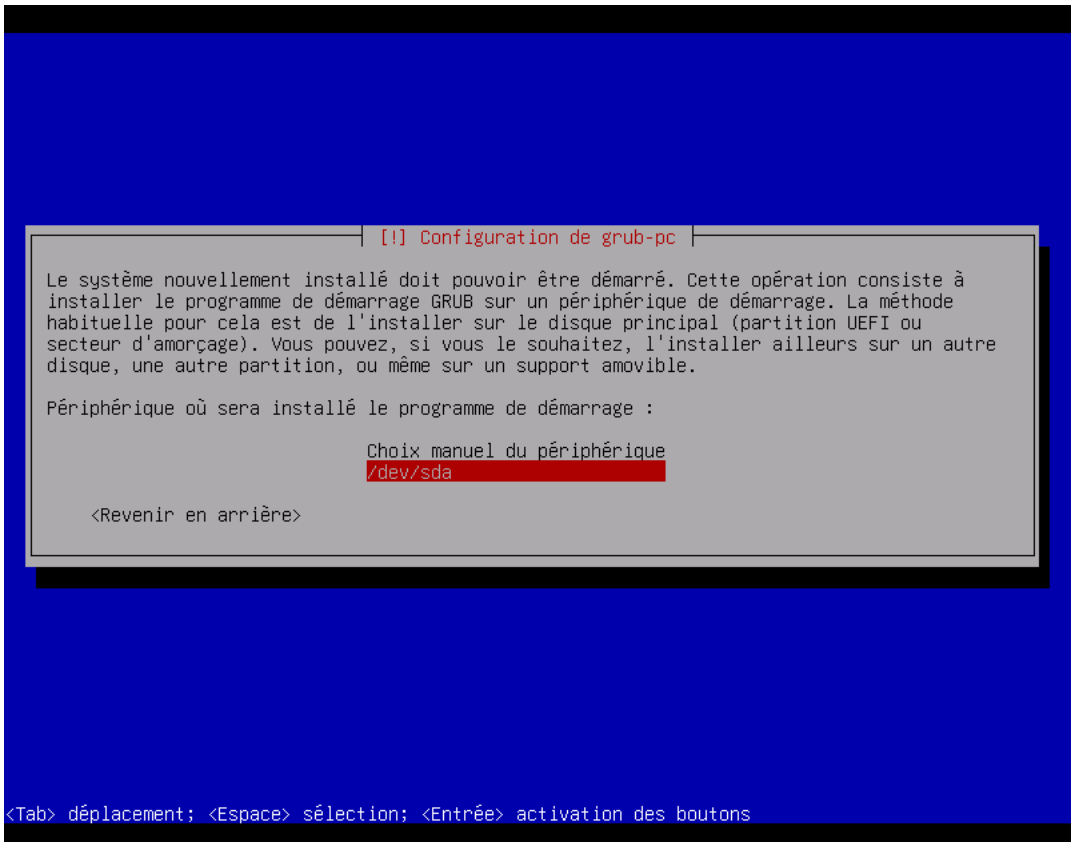
Après avoir appliqué les changements et terminé le partitionnement, comme sur Ubuntu, un test de connexion via un miroir Debian s'effectuera. Après cela, l'installeur va installer les utilitaires de base.



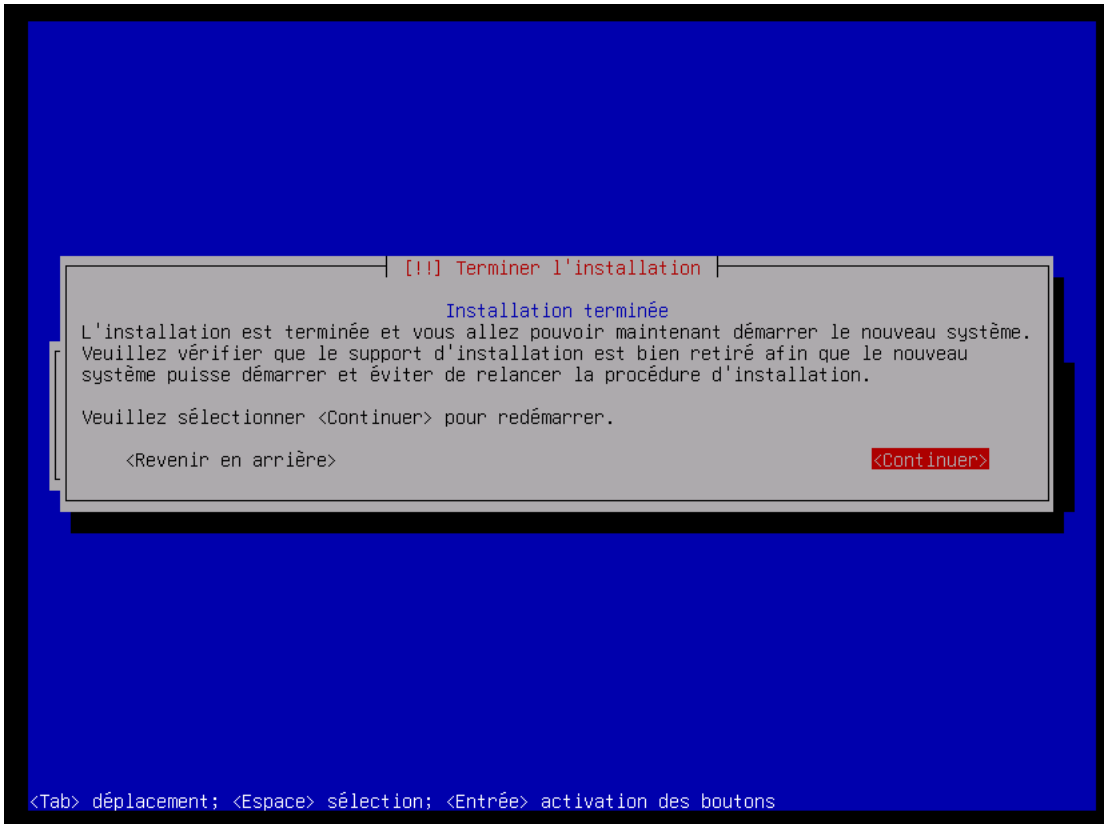
Maintenant, nous allons installer GRUB, ce qui permet d'arriver sur Debian au démarrage de la machine :



Nous allons également lui indiquer ou doit-il démarrer. Le chemin de base ci-dessous :



Debian est désormais installé !



Partie 2 : Installation de Modoboa

Pour commencer, connectons-nous et mettons à jour le système :

```
root@srv-mess:~# apt update
Réception de :1 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Réception de :2 http://deb.debian.org/debian bookworm InRelease [151 kB]
Réception de :3 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Réception de :4 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [254 kB]
Réception de :5 http://security.debian.org/debian-security bookworm-security/main Translation-en [150 kB]
Réception de :6 http://security.debian.org/debian-security bookworm-security/contrib amd64 Packages [896 B]
Réception de :7 http://security.debian.org/debian-security bookworm-security/contrib Translation-en [652 B]
Réception de :8 http://security.debian.org/debian-security bookworm-security/non-free-firmware amd64 Packages [688 B]
Réception de :9 http://security.debian.org/debian-security bookworm-security/non-free-firmware Translation-en [472 B]
Réception de :10 http://deb.debian.org/debian bookworm/main amd64 Packages [8 792 kB]
40% [10 Packages 4 699 kB/8 792 kB 53%]
```

Une fois cela fait, nous allons commencer par lier notre serveur Debian au domaine Securite.lan, dans ce cas. Nous allons le définir dans le fichier hosts qui se trouve dans /etc/hosts

```
  GNU nano 7.2                                                    /et
127.0.0.1       localhost
127.0.1.1       srv-mess.securite.lan   srv-mess
```

Maintenant, nous allons installer les paquets nécessaires pour joindre le serveur au domaine :

```
root@srv-mess:~# apt install -y realmd sssd sssd-tools libnss-sss libpam-sss adcli samba-common-bin oddjob oddjob-mkhomedir packagekit krb5-user
```

Une fois l'installation terminée, nous allons vérifier si le serveur Debian peut voir le domaine avec la commande suivante :

```
root@srv-mess:~# realm discover securite.lan
securite.lan
  type: kerberos
  realm-name: SECURITE.LAN
  domain-name: securite.lan
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
  login-formats: %U@securite.lan
  login-policy: allow-realm-logins
root@srv-mess:~# _
```

Si cela fonctionne, nous allons alors lier au domaine le serveur avec la commande suivante :
Sudo realm join –user=Administrateur securite.lan

Nous allons maintenant passer à l'installation de modoboa, pour cela, nous allons cloner le dépôt en ligne.

```
admin-mess@srv-mess:~$ git clone https://github.com/modoboa/modoboa-installer
Clonage dans 'modoboa-installer'...
remote: Enumerating objects: 3434, done.
remote: Counting objects: 100% (961/961), done.
remote: Compressing objects: 100% (251/251), done.
remote: Total 3434 (delta 810), reused 790 (delta 703), pack-reused 2473 (from 3)
Réception d'objets: 100% (3434/3434), 695.96 Kio | 3.48 Mio/s, fait.
Résolution des deltas: 100% (2387/2387), fait.
admin-mess@srv-mess:~$
```

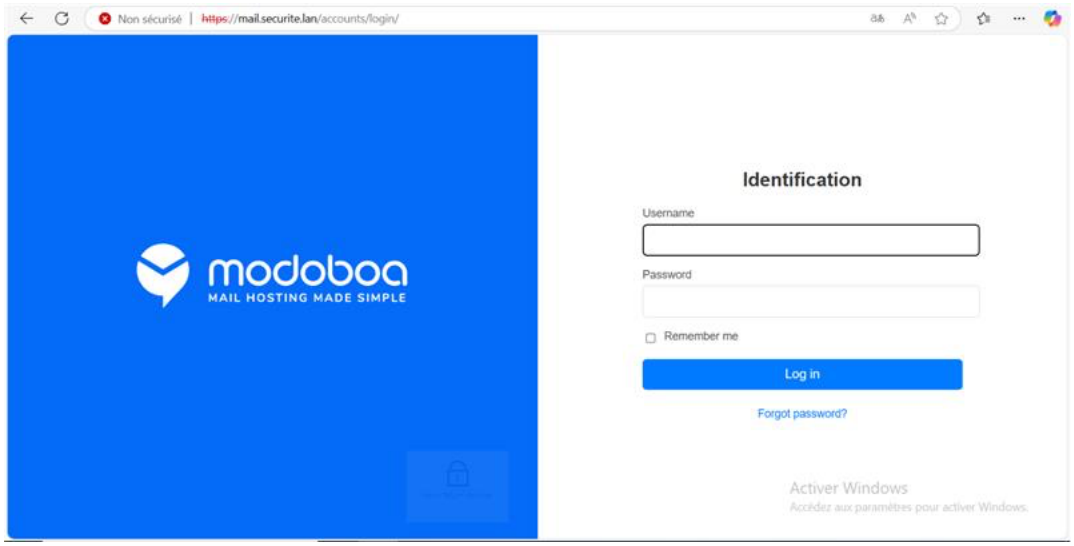
Nous allons maintenant rentrer dans le dossier « Modoboa-installer » et nous allons exécuter le script run.py

```
admin-mess@srv-mess:~/modoboa-installer$ sudo ./run.py mail.securite.lan
Welcome to Modoboa installer!

Checking the installer...
Installer seems up to date!
Checks complete

Configuration file installer.cfg not found, creating new one.
Notice:
It is recommanded to run this installer on a FRESHLY installed server.
(ie. with nothing special already installed on it)

Warning:
Before you start the installation, please make sure the following DNS records exist for domain 'mail.securite.lan':
  mail IN A   <IP ADDRESS OF YOUR SERVER>
     @ IN MX  mail.mail.securite.lan.

Your mail server will be installed with the following components:
fail2ban modoboa automx amavis clamav dovecot nginx razor postfix postwhite spamassassin uwsgi radicale opendkim
Do you confirm? (Y/n)
```

```
Your mail server will be installed with the following components:
fail2ban modoboa automx amavis clamav dovecot nginx razor postfix postwhite spamassassin uwsgi radic
ale opendkim
Do you confirm? (Y/n) y
The process can be long, feel free to take a coffee and come back later ;)
Starting...
Generating new certificate using letsencrypt
Installing amavis
Installing spamassassin
Installing razor
Installing clamav
Installing fail2ban
Installing modoboa
Installing automx
Installing radicale
Installing uwsgi
Installing nginx
Installing opendkim
Installing postfix
Installing postwhite
Installing dovecot
User dovecot already exists, skipping creation but please make sure the /srv/vmail directory exists.
Congratulations! You can enjoy Modoboa at https://mail.henrybroadway.com (admin:password)

Modoboa is a free software maintained by volunteers.
You like the project and want it to be sustainable?
Then don't wait anymore and go sponsor it here:

https://github.com/sponsors/modoboa

Thank you for your help :-)
```

Une fois l'installation terminée, vous voila fin prêt pour utiliser votre serveur de messagerie !

Nous allons alors nous rendre sur l'interface web depuis le lien qui nous ait donné ; en l'occurrence mail.securite.lan dans ce cas.



Nous allons rentrer les identifiants de base, donné à la fin de l'installation : admin / password.
Il est très important de les modifier juste après ; et de créer un second compte d'administration avec uniquement les droits nécessaires pour éviter toute mauvaise manipulation.

Une fois connecté, vous allez pouvoir ajouter un domaine, en l'occurrence sécurité.lan dans mon cas, veuillez bien faire attention à avoir créé toutes les entrées DNS afin que le lien puisse se faire.

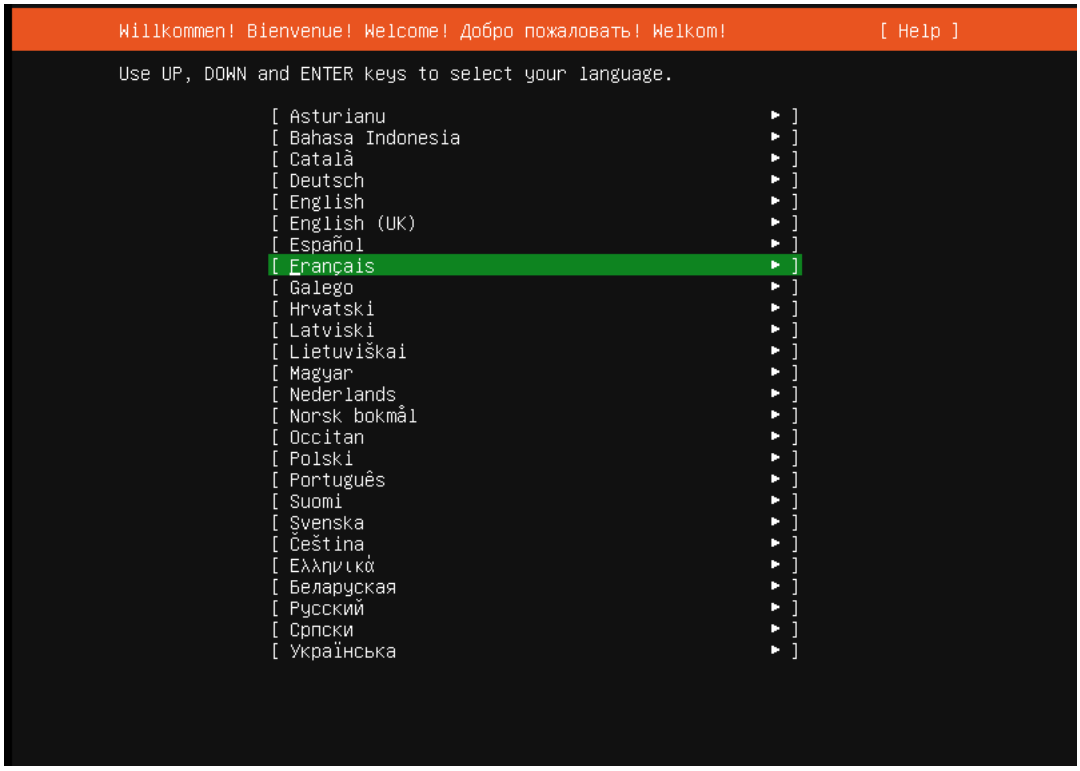
Il est également possible de créer des comptes utilisateurs, pour les différents utilisateurs du domaine. Nous pouvons aussi leur définir des quotas d'envoi de mail.

Une fois un compte créé, nous pouvons alors faire un test en essayant d'envoyer un mail au compte administrateur depuis notre compte test depuis un MUA, Thunderbird est un bon outil.

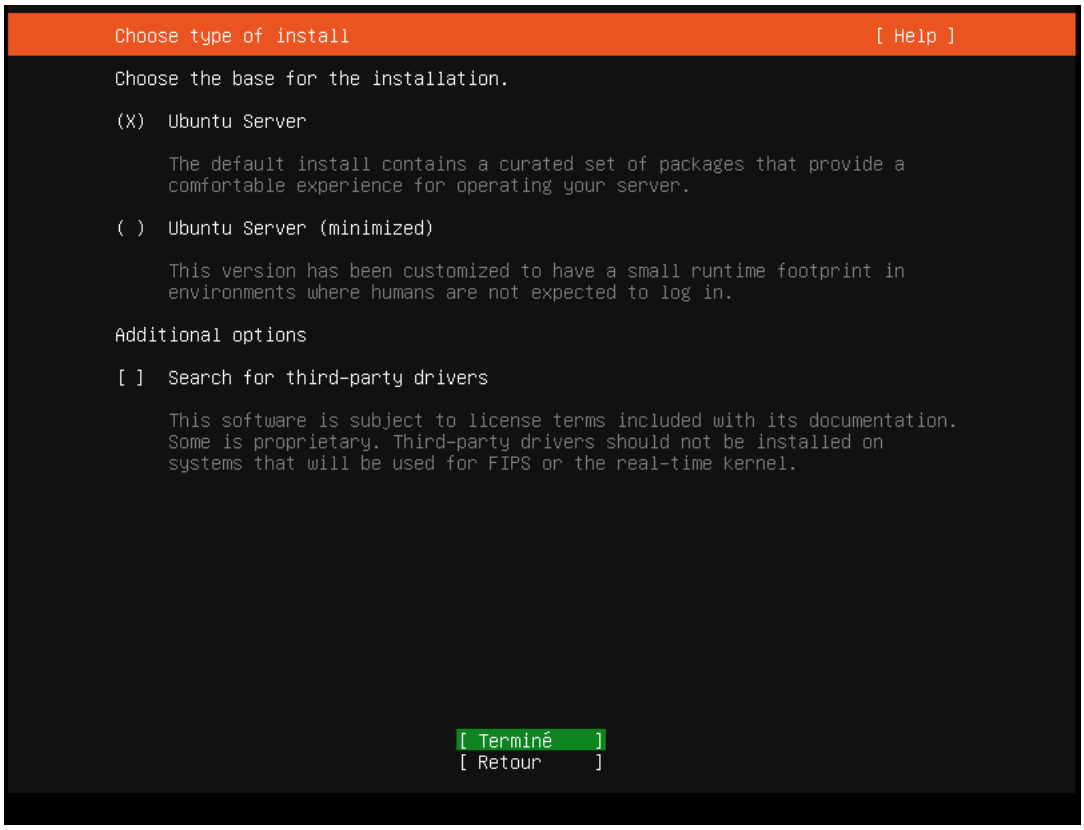
Installation d’un serveur web Apache sur Ubuntu 22.04

Partie 1 : Installation d’Ubuntu 22.04

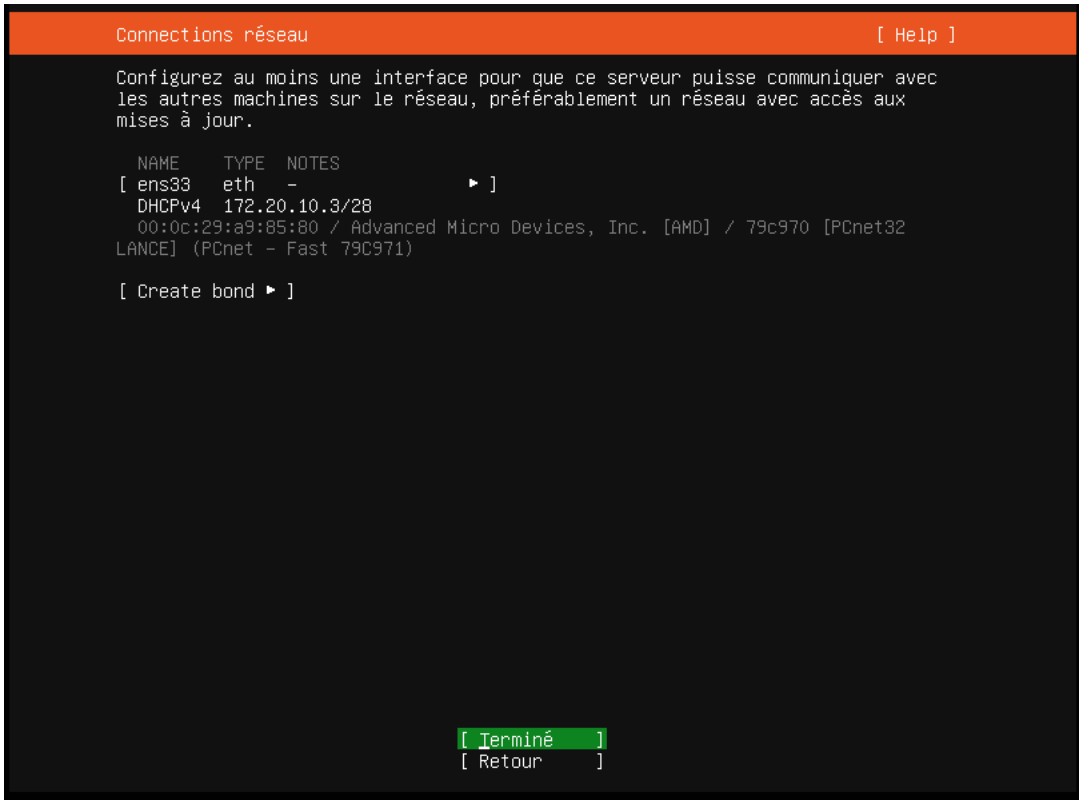
Bienvenue sur l’installeur d’Ubuntu 22.04 ; pour commencer, choisissez la langue du système d’exploitation.



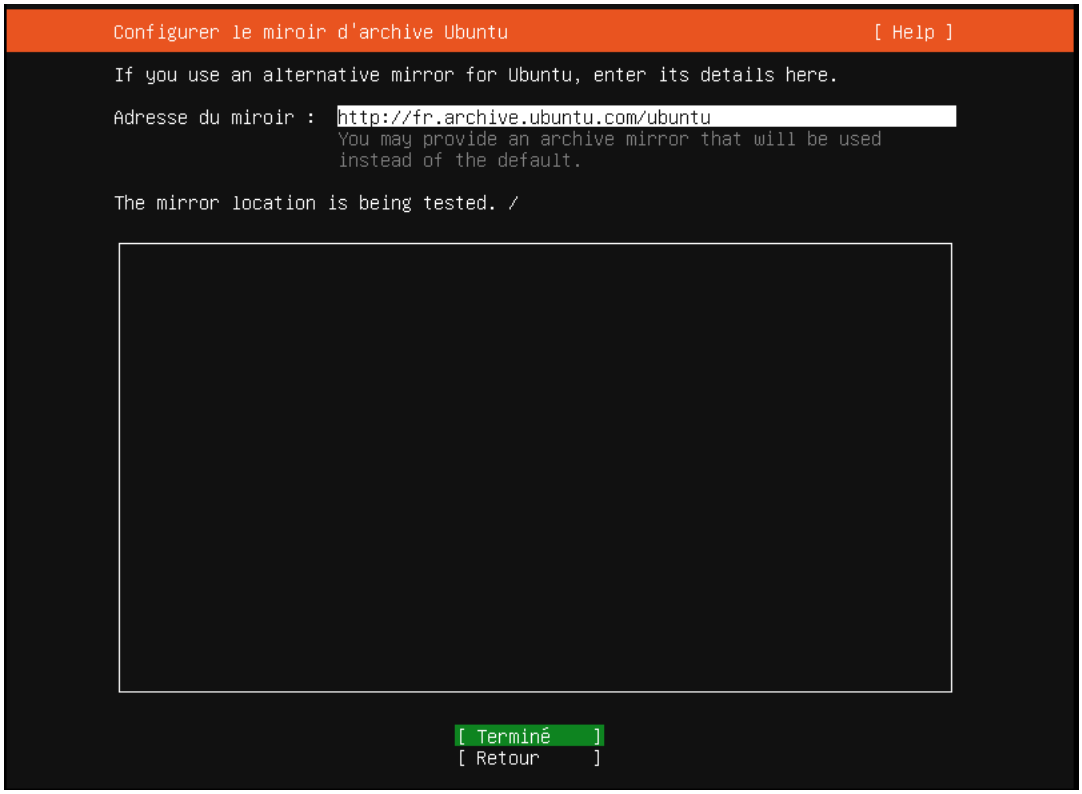
Nous allons choisir la version Ubuntu Server complète, un environnement en ligne de commande un peu plus gourmand que la version (minimized) mais adaptée au besoin.



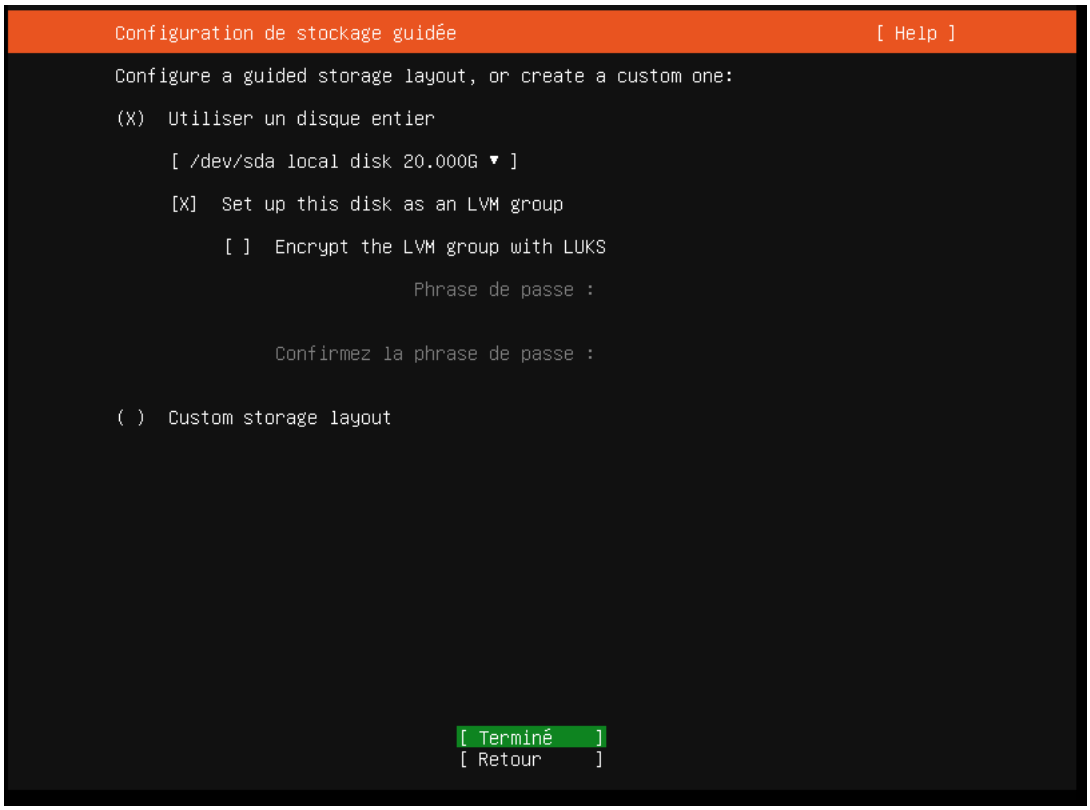
Nous allons désormais définir les paramètres réseaux du serveur pour lui permettre de récupérer les mises à jour sur les dépôts en ligne



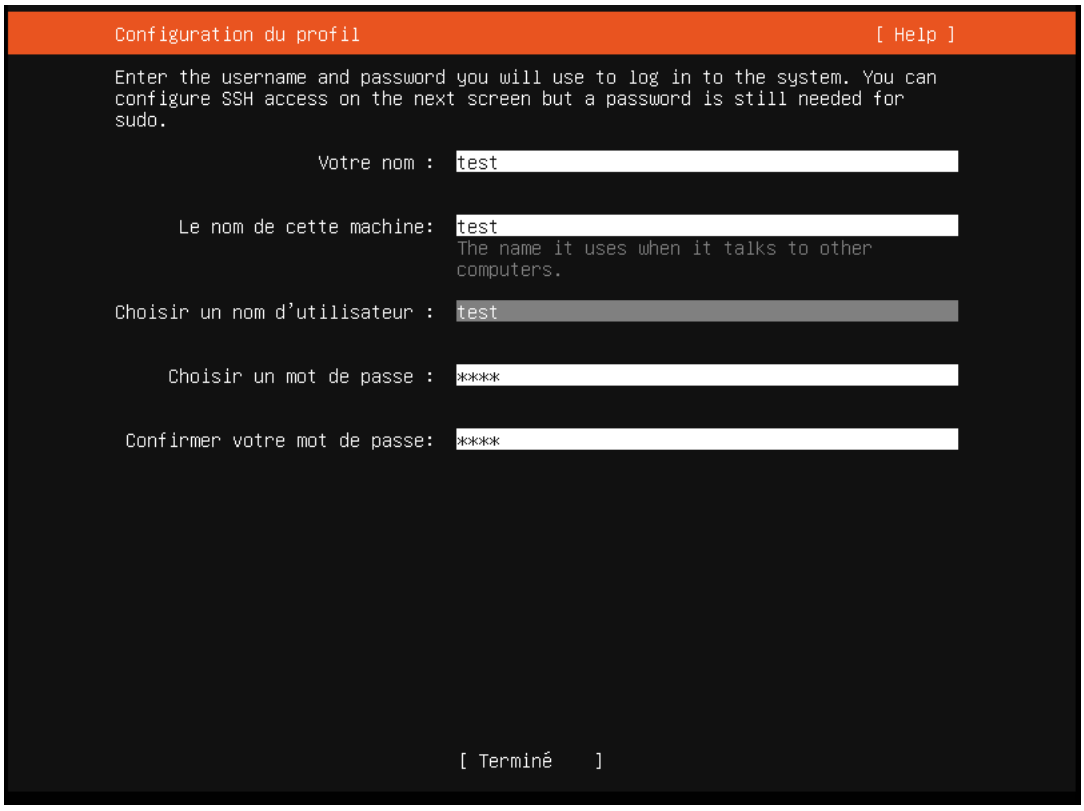
Après les paramètres réseaux définis, un test va être réalisé ce qui va permettre de voir si le serveur a bien un accès vers internet pour récupérer des paquets :



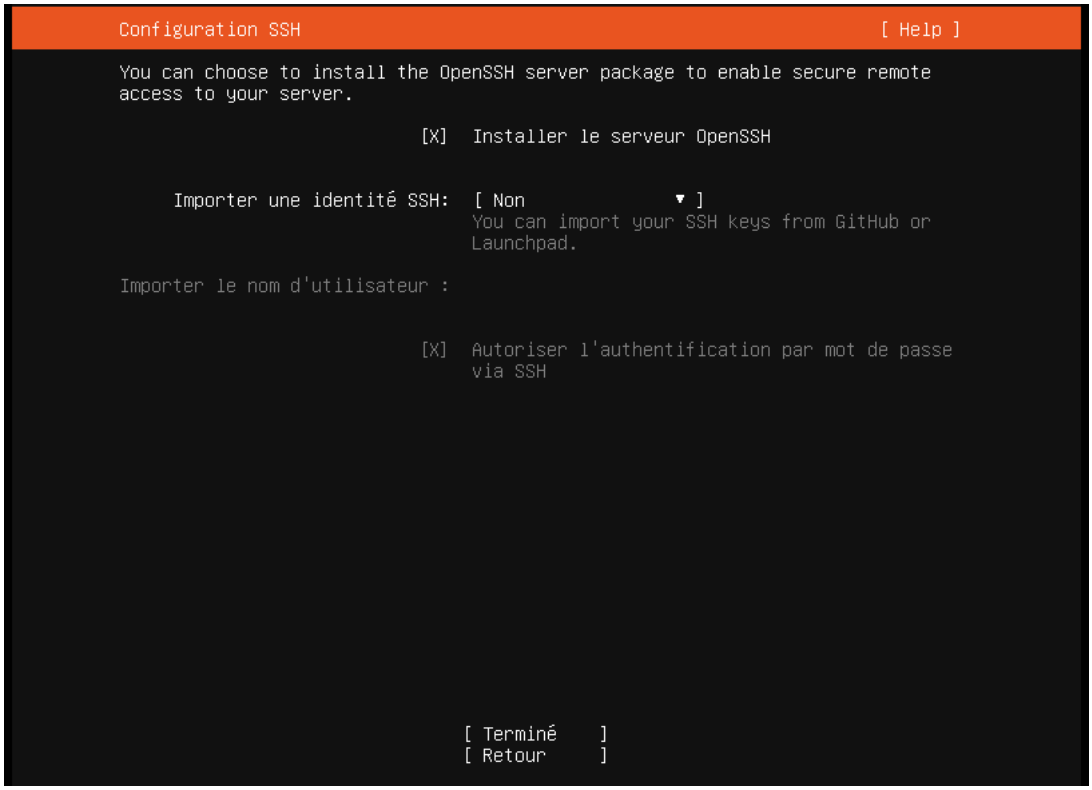
Concernant la taille du disque, un disque de 20Go peut être amplement suffisant, Ubuntu étant basé sur Linux, le système d'exploitation est très léger.



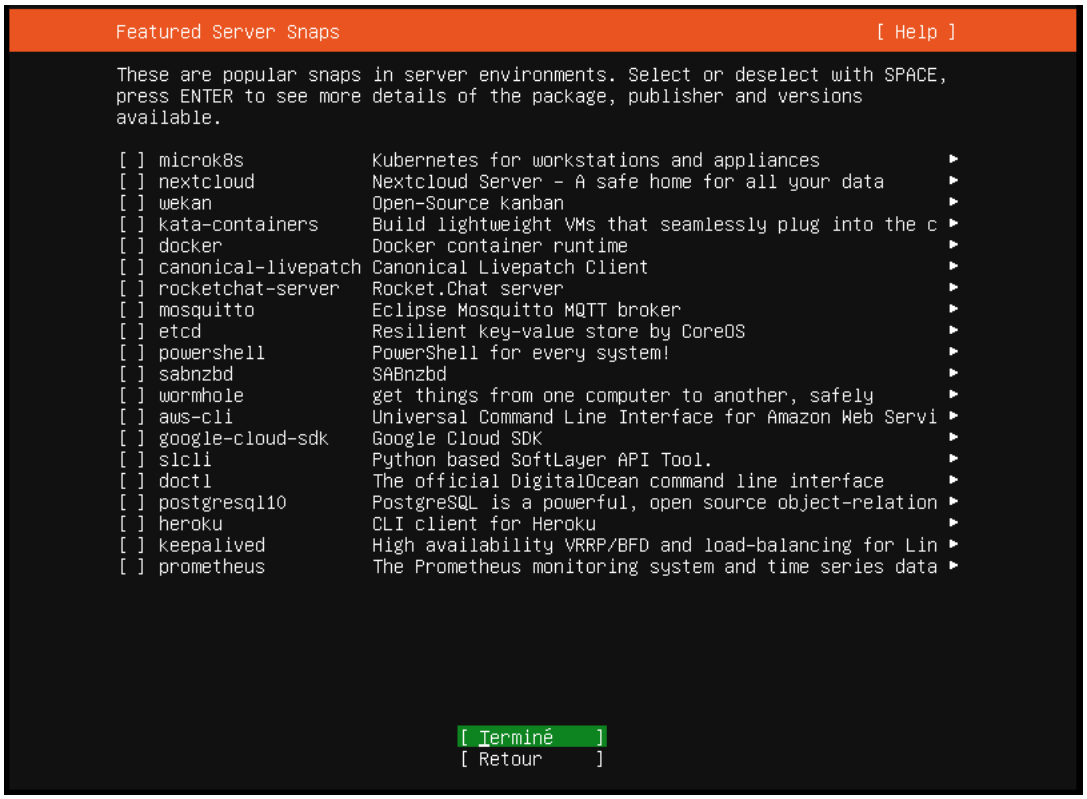
Désormais, nous allons définir un utilisateur de base qui va nous servir à nous connecter après la configuration et l'installation de l'OS. Un nom de machine va également être demandé.



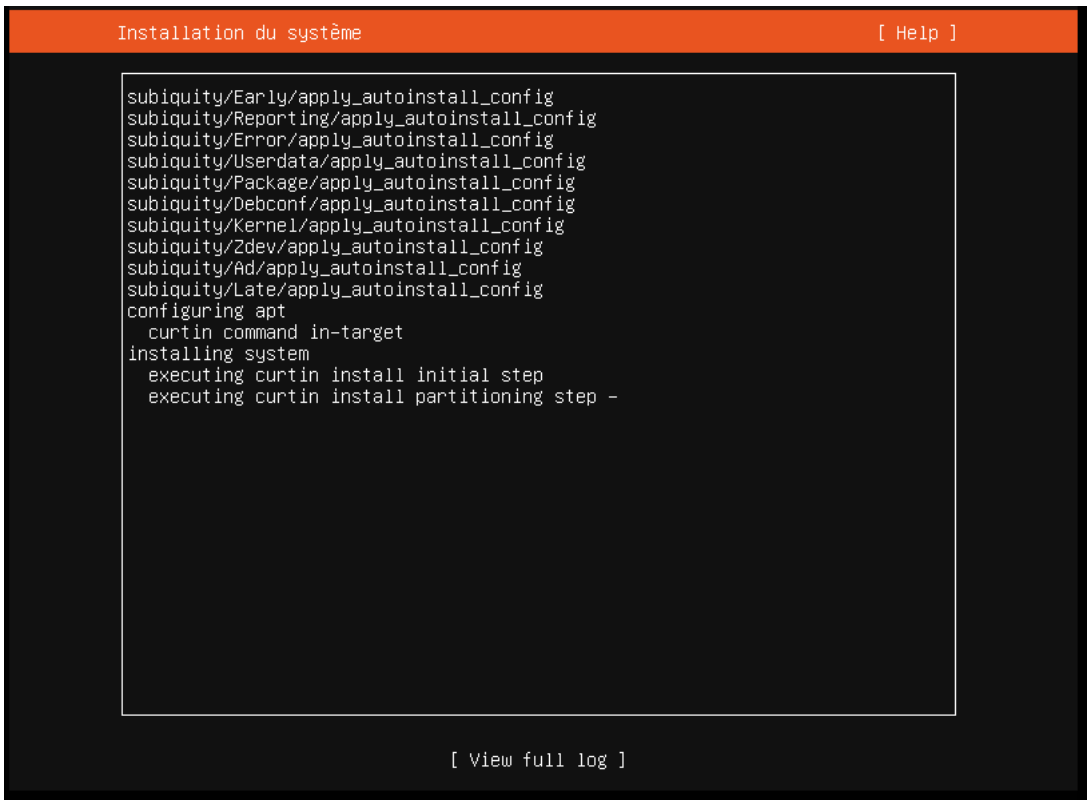
Pour une question de pratique, nous pouvons cocher l'option d'installation d'un serveur SSH, le service SSH sera alors installé, et configuré pour faire en sorte que seul l'utilisateur créé auparavant puisse se connecter. Il est également possible d'importer une clé SSH depuis GitHub.



Pour finir, nous allons pouvoir choisir des packages à installer en supplément, suivant l'utilisation du serveur. En l'occurrence, nous n'allons pas en choisir pour installer Apache.



Nous y sommes, le serveur Ubuntu est désormais en train de s'installer. Après l'installation, il suffira de le redémarrer pour arriver à l'interface de connexion.



Partie 2 : Installation d'Apache sur le serveur Ubuntu 22.04

Pour commencer, connectons-nous avec l'utilisateur que nous avons défini auparavant

```
Ubuntu 22.04.3 LTS test tty1

test login: test
Password: _
```

Avant n'importe quelle installation, il est important de vérifier que le système soit à jour. Il faut donc exécuter la commande suivant qui va rechercher les mises à jour, les télécharger et les appliquer.

```
admin-apache@srv-apache:~$ sudo apt upgrade && sudo_apt upgrade
```

Cette opération peut être longue, en fonction du nombre de mises à jour que Ubuntu doit récupérer.
Après cette mise à jour, nous allons pouvoir installer Apache2 avec la commande suivante

```
test@test:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser bzip2-doc
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils bzip2 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap liblua5.3-0 mailcap mime-support ssl-cert
0 upgraded, 13 newly installed, 0 to remove and 226 not upgraded.
Need to get 2142 kB of archives.
After this operation, 8528 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

Après l'installation, nous allons vérifier que l'installation s'est bien déroulée, et que apache est bien démarré :

```
admin-apache@ebrigade:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-04-14 08:01:51 UTC; 17min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 815 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 913 (apache2)
      Tasks: 6 (limit: 4519)
     Memory: 26.0M
        CPU: 387ms
     CGroup: /system.slice/apache2.service
             ├─913 /usr/sbin/apache2 -k start
             ├─954 /usr/sbin/apache2 -k start
             ├─955 /usr/sbin/apache2 -k start
             ├─956 /usr/sbin/apache2 -k start
             ├─957 /usr/sbin/apache2 -k start
             └─958 /usr/sbin/apache2 -k start

avril 14 08:01:50 ebrigade systemd[1]: Starting The Apache HTTP Server...
avril 14 08:01:51 ebrigade apachectl[877]: AH00558: apache2: Could not reliably determine the serve>
avril 14 08:01:51 ebrigade systemd[1]: Started The Apache HTTP Server.
lines 1-20/20 (END)_
```

Dans ce cas, apache a le statut 'active', il est donc fonctionnel. Pour afficher ce qui est partagé avec apache, il suffira d'aller sur un navigateur comme Edge, et rentrer http://AdresseIP/

Partie 3 : Faire marcher e-brigade sur apache

Pour faire fonctionner e-brigade, nous allons d'abord transférer les fichiers sources via sftp avec FileZilla par exemple.

Une fois cela fait, nous allons définir dans le fichier de configuration d'apache le chemin de la source d'E-brigade :

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/ebrigade

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
~
~
~
~
<c/apache2/sites-available/000-default.conf" [lecture-seule] 31L, 1336B          1,1          Tout
```

Désormais, Apache affichera la page de configuration d'E-brigade sur l'interface web. **ATTENTION, EBRIGADE nécessite une version de php 7.4 ou plus.**

Nous allons maintenant installer mysql, ce qui va permettre d'ajouter une base de données pour ebrigade avec les commandes suivantes :
``sudo apt install mysql-server
Une fois mysql installé, nous allons nous y connecter avec l'utilisateur root, puis nous allons créer une base de données, un utilisateur spécifique à la base, et nous allons lui mettre les droits sur la base.
CREATE DATABASE database;
CREATE USER 'nom_utilisateur'@'localhost' IDENTIFIED BY 'mot_de_passe';
GRANT ALL PRIVILEGES ON database* TO 'nom_utilisateur'@'localhost';
FLUSH PRIVILEGES;

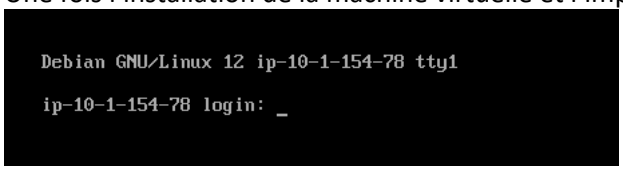
Une fois la création de la base de données faite, nous allons désormais pouvoir finaliser la configuration d'e-brigade :
Sur l'interface WEB, rentrez simplement 'localhost' comme hôte, le nom de la base, l'utilisateur et le mot de passe, puis cliquez sur continuer.

Nous y sommes, bienvenue sur e-brigade !

Installation d'un serveur de supervision Centreon

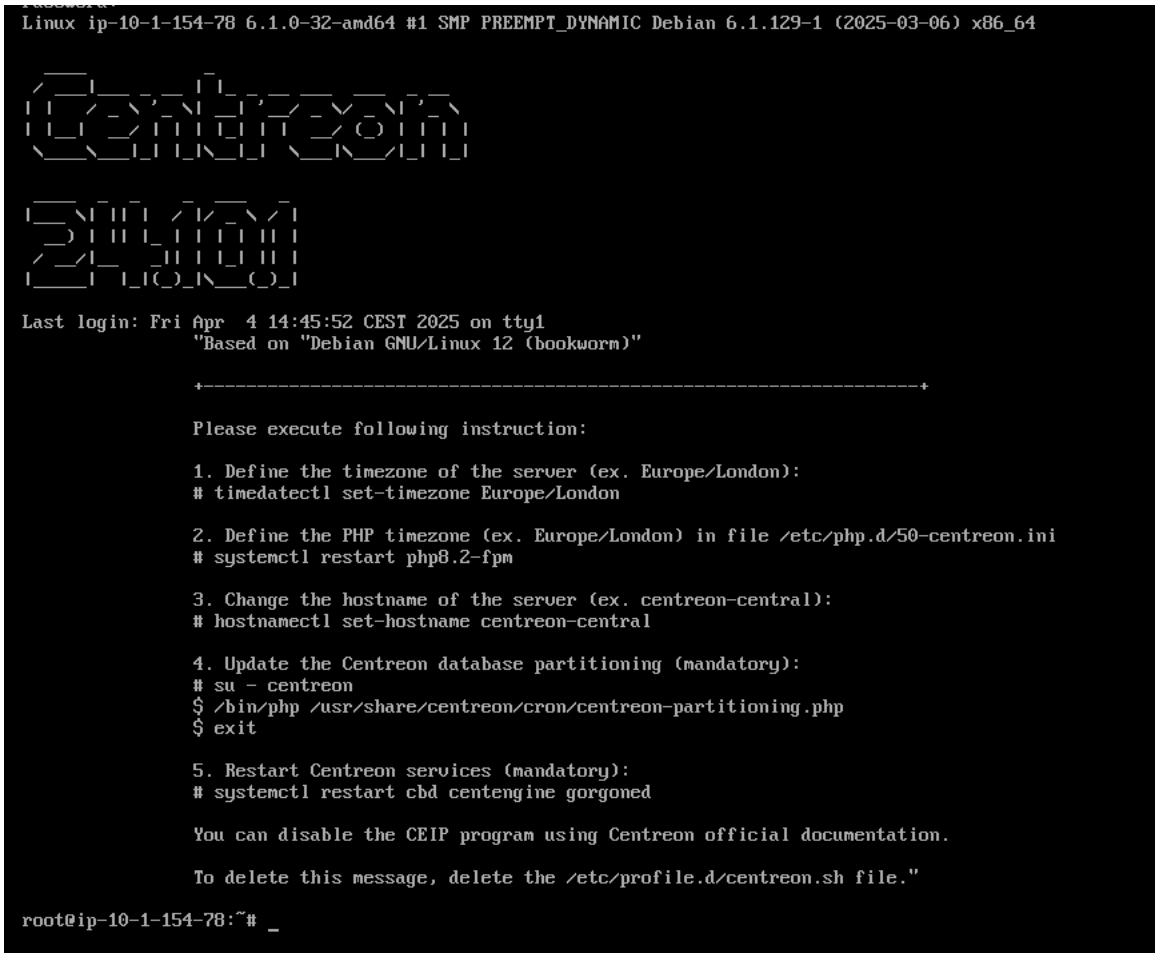
L'installation de Centreon passe par l'installation d'une machine virtuelle directement sur le site officiel de Centreon. C'est un fichier OVA qui va s'installer, qu'il va falloir importer sur le logiciel utilisé (VMWare ou VirtualBOX).

Une fois l'installation de la machine virtuelle et l'import fait, nous allons pouvoir démarrer notre machine :



Une fois ici, nous allons rentrer les identifiants fournis par Centreon, l'utilisateur est root, et le mot de passe *centreon*.

A l'arrivée sur le serveur, une liste de choses à faire avant l'utilisation nous ai donné, nous allons alors la suivre.



Dans un premier temps, nous allons devoir se synchroniser sur des serveurs de temps afin d'éviter les incohérences entre les autres machines. Le serveur PHP lui aussi aura besoin de synchronisation du temps.

Nous allons ensuite renommer le serveur avec la commande hostnamectl, Centreon nous donne directement les arguments à rentrer pour les différentes commandes à exécuter.

Pour finir, nous allons mettre à jour la base de données de Centreon avec les commandes données à l'étape 4, puis nous allons redémarrer les services, il peut également être conseillé de redémarrer le serveur complétement afin qu'il se mette à jour au niveau des fuseaux horaires.

Après toutes ces étapes, Centreon est désormais prêt à l'utilisation et a la supervision des équipements !

Mise en place d'un VPN RoadWarrior OpenVPN

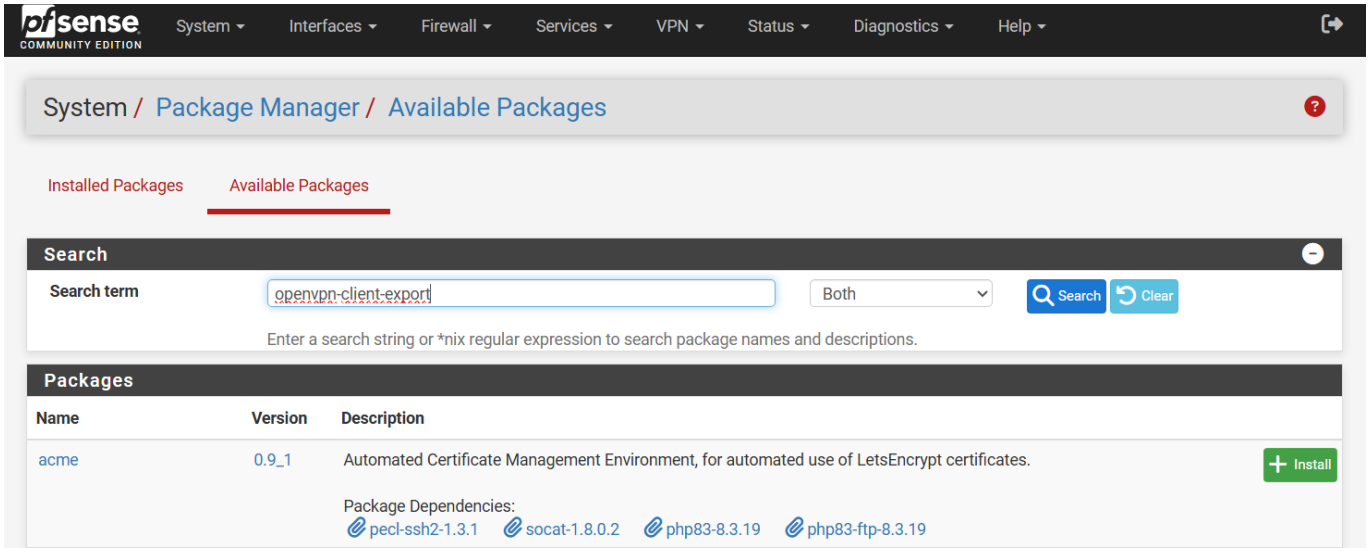
Configuration du VPN

La mise en place d'un VPN (RW) sur pfSense constitue une étape cruciale dans notre architecture sécurisée. Cette configuration permettra aux utilisateurs distants d'accéder de manière sécurisée aux ressources du réseau interne en s'authentifiant via leurs comptes Active Directory existants.

Installation du package OpenVPN

L'installation du service OpenVPN a été réalisée via l'interface d'administration de pfSense :

1. Navigation vers **System > Package Manager**
2. Sélection de l'onglet **Available Packages**
3. Recherche et installation du package **openvpn-client-export**

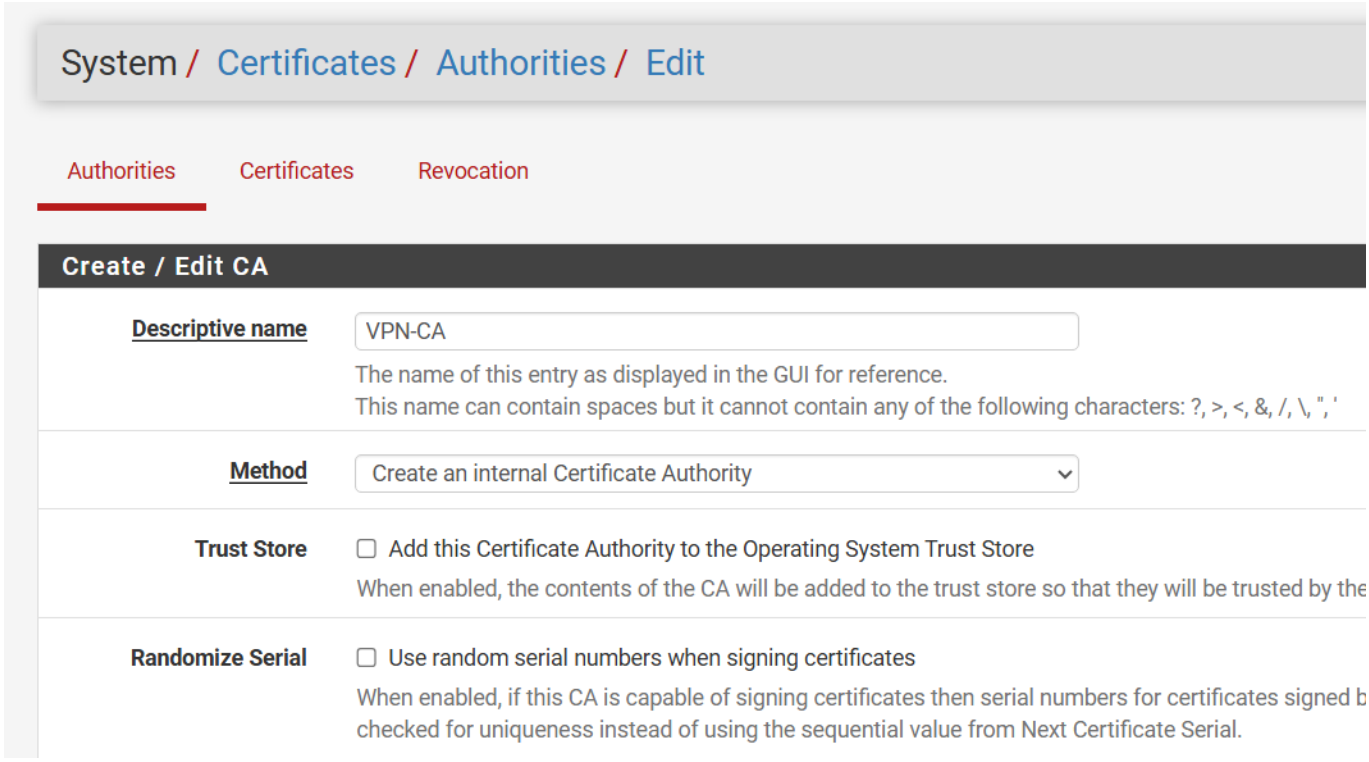


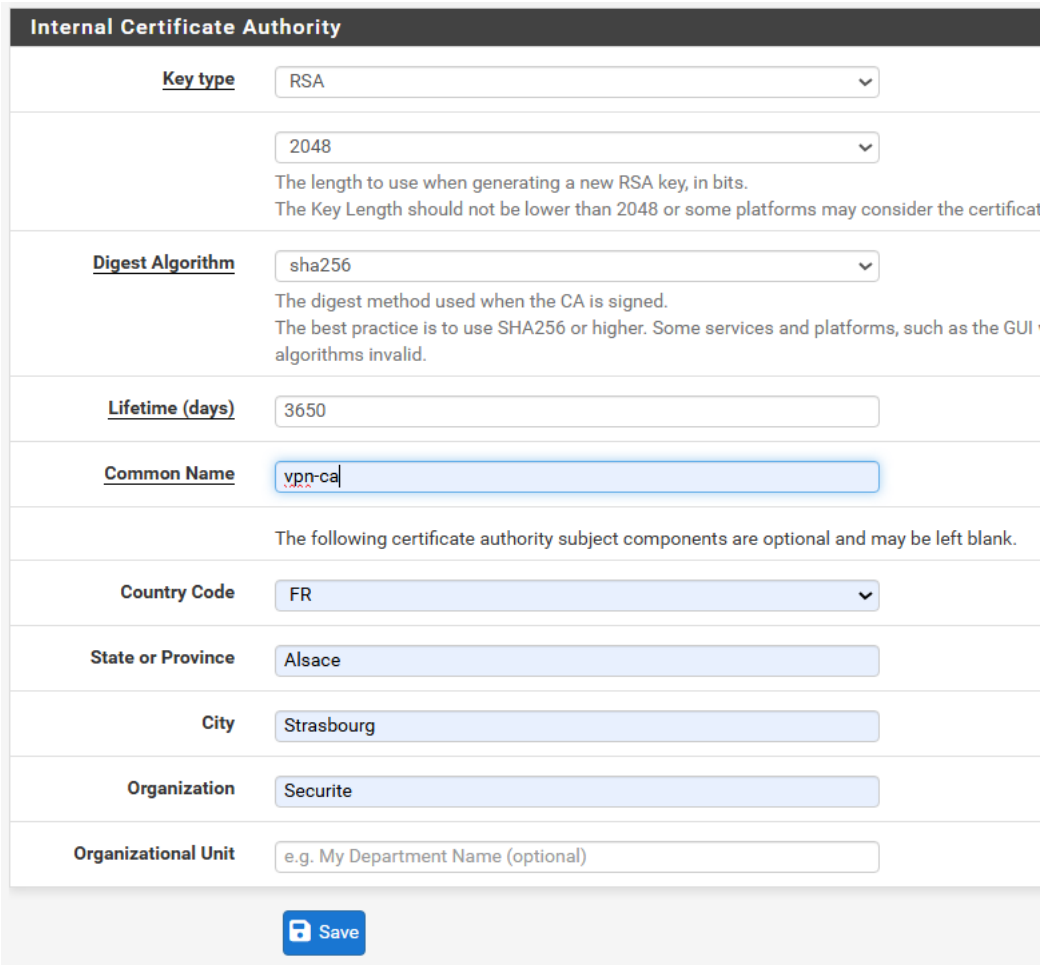
Ce package additionnel simplifie la génération des configurations clients et permet l'exportation des paramètres nécessaires à la connexion.

Création de l'autorité de certification

Avant de configurer le serveur VPN, nous avons généré une infrastructure de clés publiques (PKI) via le gestionnaire de certificats intégré à pfSense :

1. Navigation vers **System > Certificates**
2. Création d'une nouvelle autorité de certification. Cliqué sur Add et compléter avec les paramètres suivants :

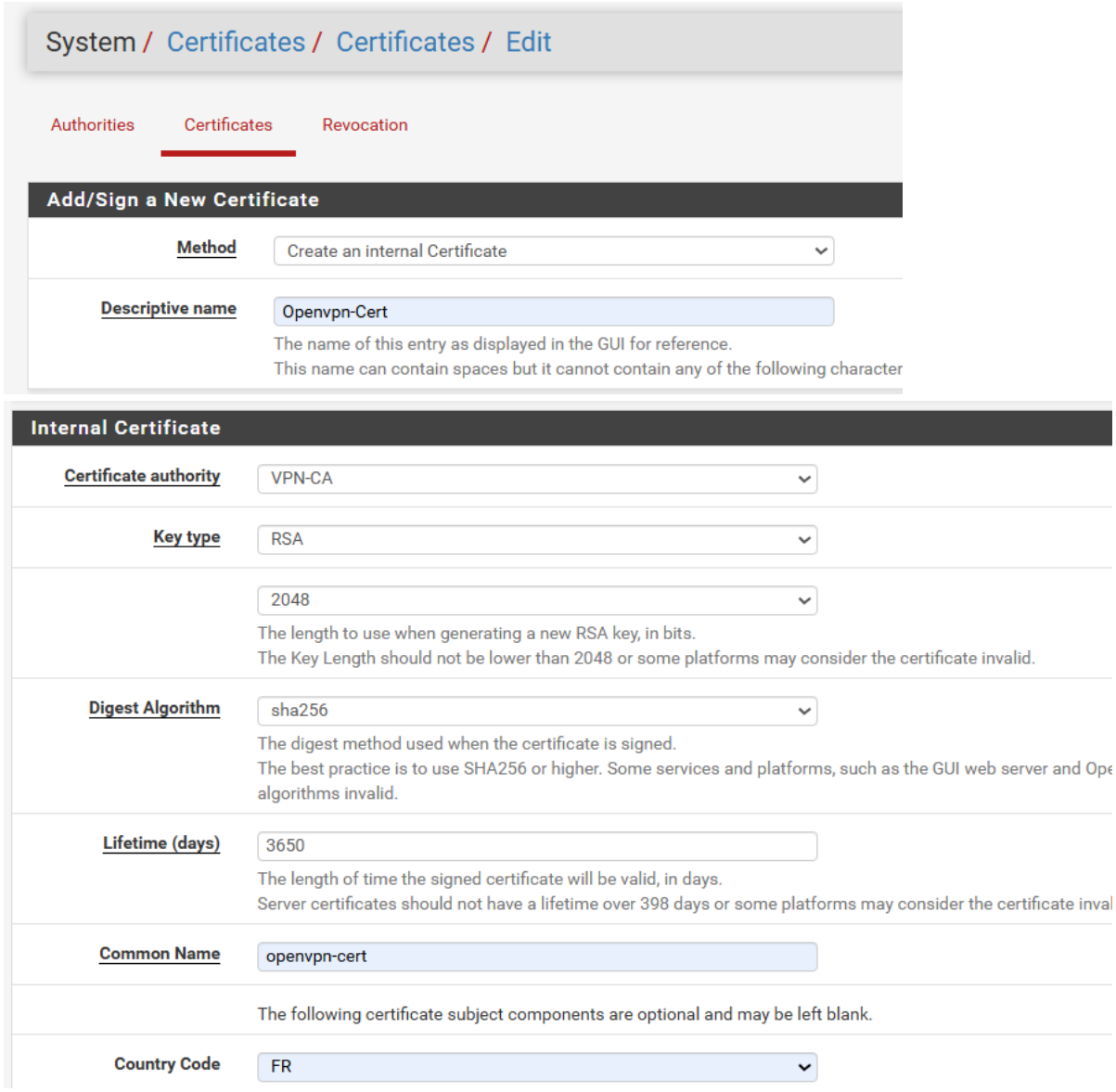

System / Certificates / Authorities / Edit
Authorities
Certificates
Revocation
Create / Edit CA
Descriptive name
VPN-CA
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '
Method
Create an internal Certificate Authority
Trust Store
Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the
Randomize Serial
Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed b
checked for uniqueness instead of using the sequential value from Next Certificate Serial.

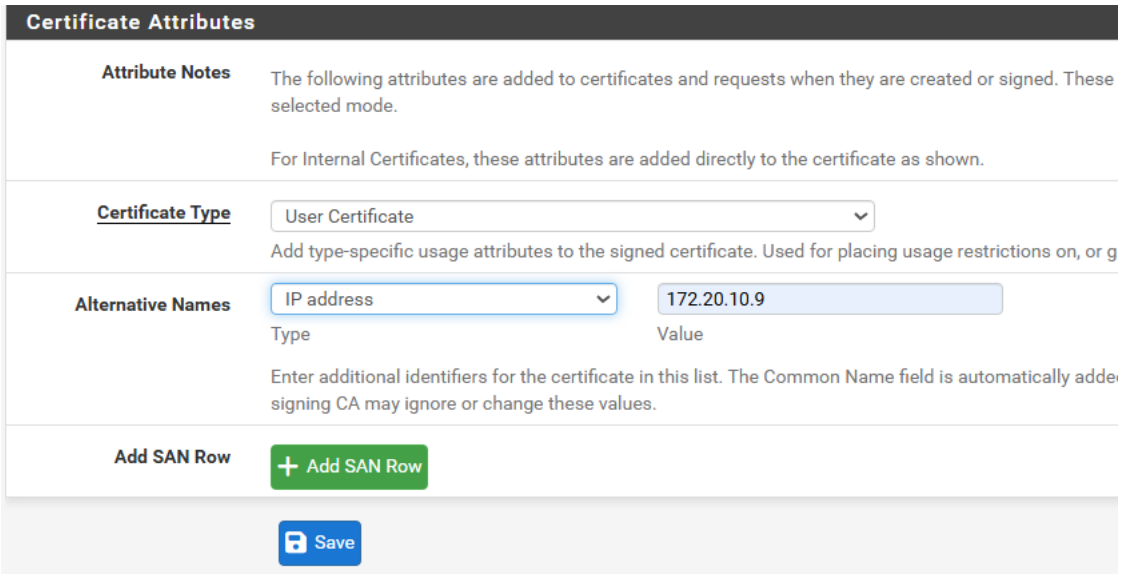


Génération du certificat serveur

Après la création de l'autorité de certification, nous avons généré un certificat spécifique pour le serveur VPN :

1. Toujours dans **System > Certificates**, sélection de l'onglet **Certificates**
2. Création d'un nouveau certificat avec les paramètres suivants :


System / Certificates / Certificates / Edit
Authorities
Certificates
Revocation
Add/Sign a New Certificate
Method
Create an internal Certificate
Descriptive name
Openvpn-Cert
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following character
Internal Certificate
Certificate authority
VPN-CA
Key type
RSA
2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm
sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and Ope
algorithms invalid.
Lifetime (days)
3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate inval
Common Name
openvpn-cert
The following certificate subject components are optional and may be left blank.
Country Code
FR

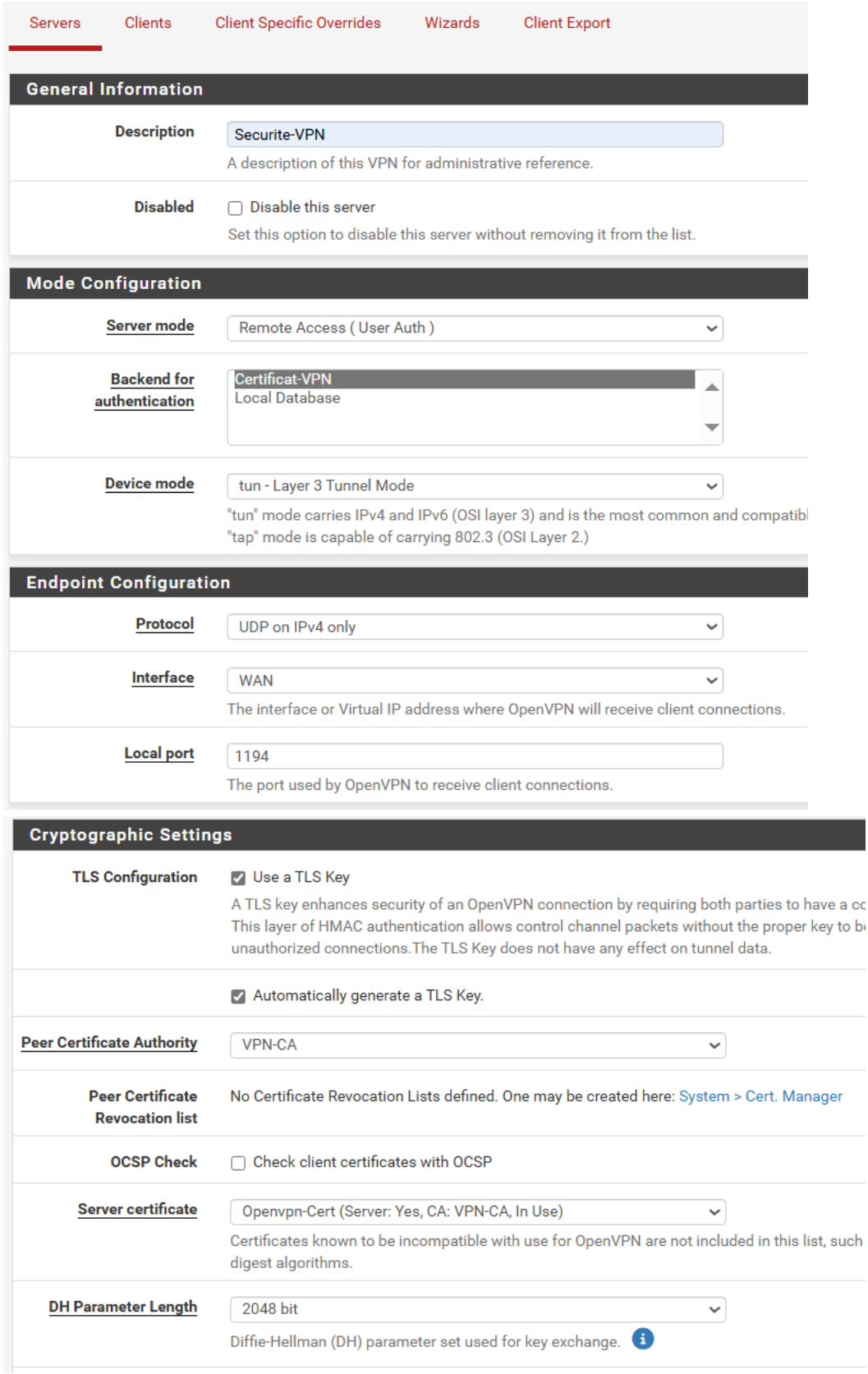


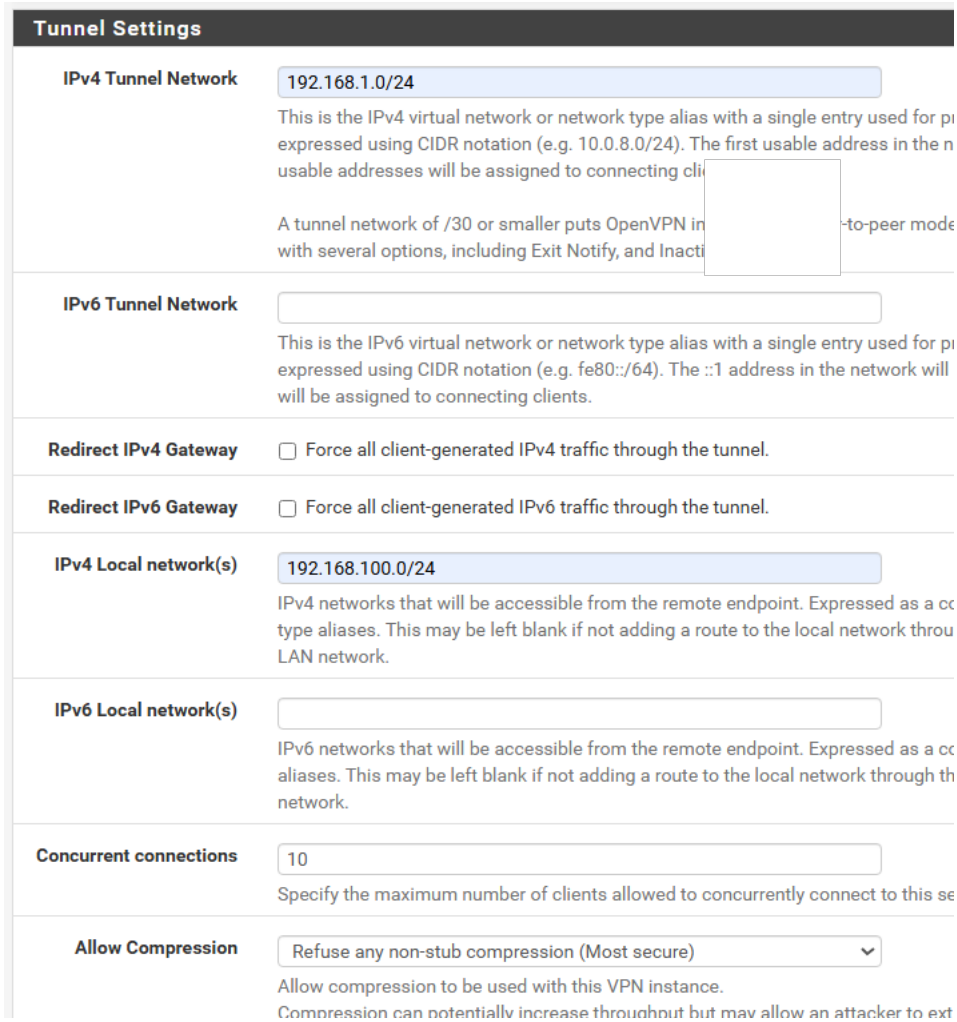
Et cliqué sur Save

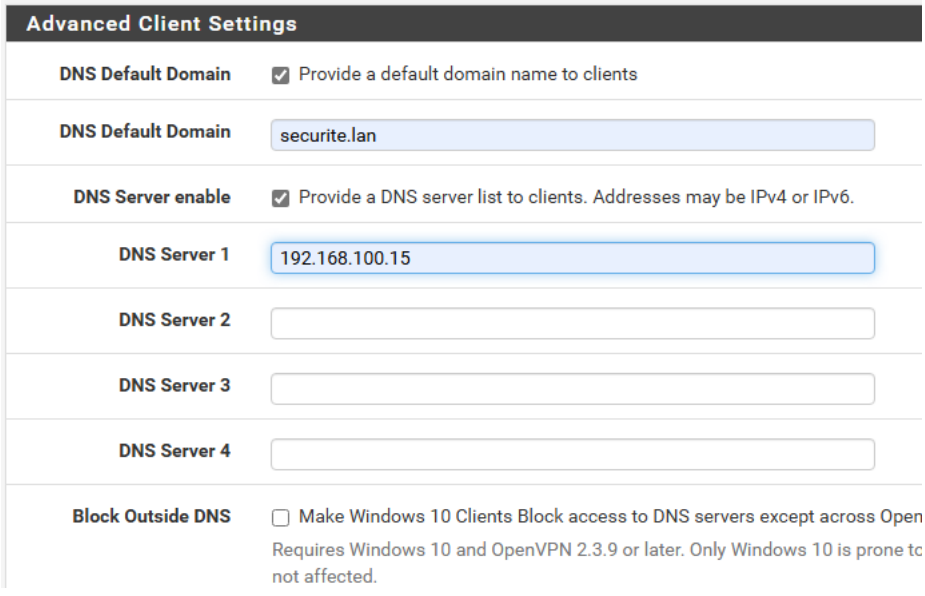
Configuration du serveur OpenVPN

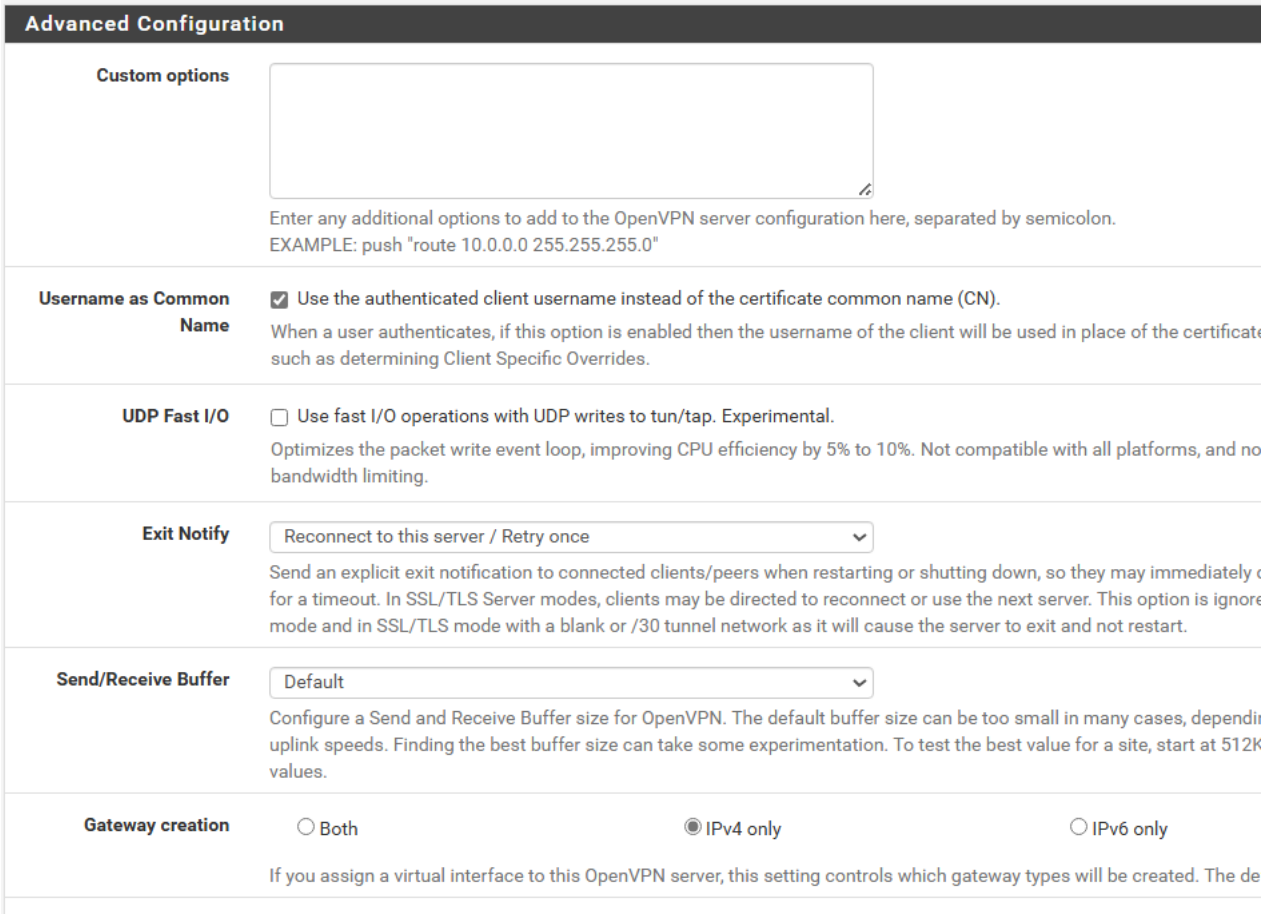
La configuration du serveur OpenVPN a été réalisée via l'interface graphique de pfSense :

1. Navigation vers **VPN > OpenVPN**, onglet **Servers**
2. Création d'un nouveau serveur avec les paramètres suivants :


Servers
Clients
Client Specific Overrides
Wizards
Client Export
General Information
Description
Securite-VPN
A description of this VPN for administrative reference.
Disabled
Disable this server
Set this option to disable this server without removing it from the list.
Mode Configuration
Server mode
Remote Access (User Auth)
Backend for authentication
Certificat-VPN
Local Database
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatibl
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration
Protocol
UDP on IPv4 only
Interface
WAN
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port
1194
The port used by OpenVPN to receive client connections.
Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a cc
This layer of HMAC authentication allows control channel packets without the proper key to b
unauthorized connections.The TLS Key does not have any effect on tunnel data.
Automatically generate a TLS Key.
Peer Certificate Authority
VPN-CA
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check
Check client certificates with OCSP
Server certificate
Openvpn-Cert (Server: Yes, CA: VPN-CA, In Use)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such
digest algorithms.
DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.


Tunnel Settings
IPv4 Tunnel Network
192.168.1.0/24
This is the IPv4 virtual network or network type alias with a single entry used for pr
expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the n
usable addresses will be assigned to connecting cli
A tunnel network of /30 or smaller puts OpenVPN in
-to-peer mode
with several options, including Exit Notify, and Inacti
IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for pr
expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will
will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway
Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)
192.168.100.0/24
IPv4 networks that will be accessible from the remote endpoint. Expressed as a cc
type aliases. This may be left blank if not adding a route to the local network throu
LAN network.
IPv6 Local network(s)
IPv6 networks that will be accessible from the remote endpoint. Expressed as a cc
aliases. This may be left blank if not adding a route to the local network through th
network.
Concurrent connections
10
Specify the maximum number of clients allowed to concurrently connect to this se
Allow Compression
Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to ext


Advanced Client Settings
DNS Default Domain
Provide a default domain name to clients
DNS Default Domain
securite.lan
DNS Server enable
Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1
192.168.100.15
DNS Server 2
DNS Server 3
DNS Server 4
Block Outside DNS
Make Windows 10 Clients Block access to DNS servers except across Open
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to
not affected.



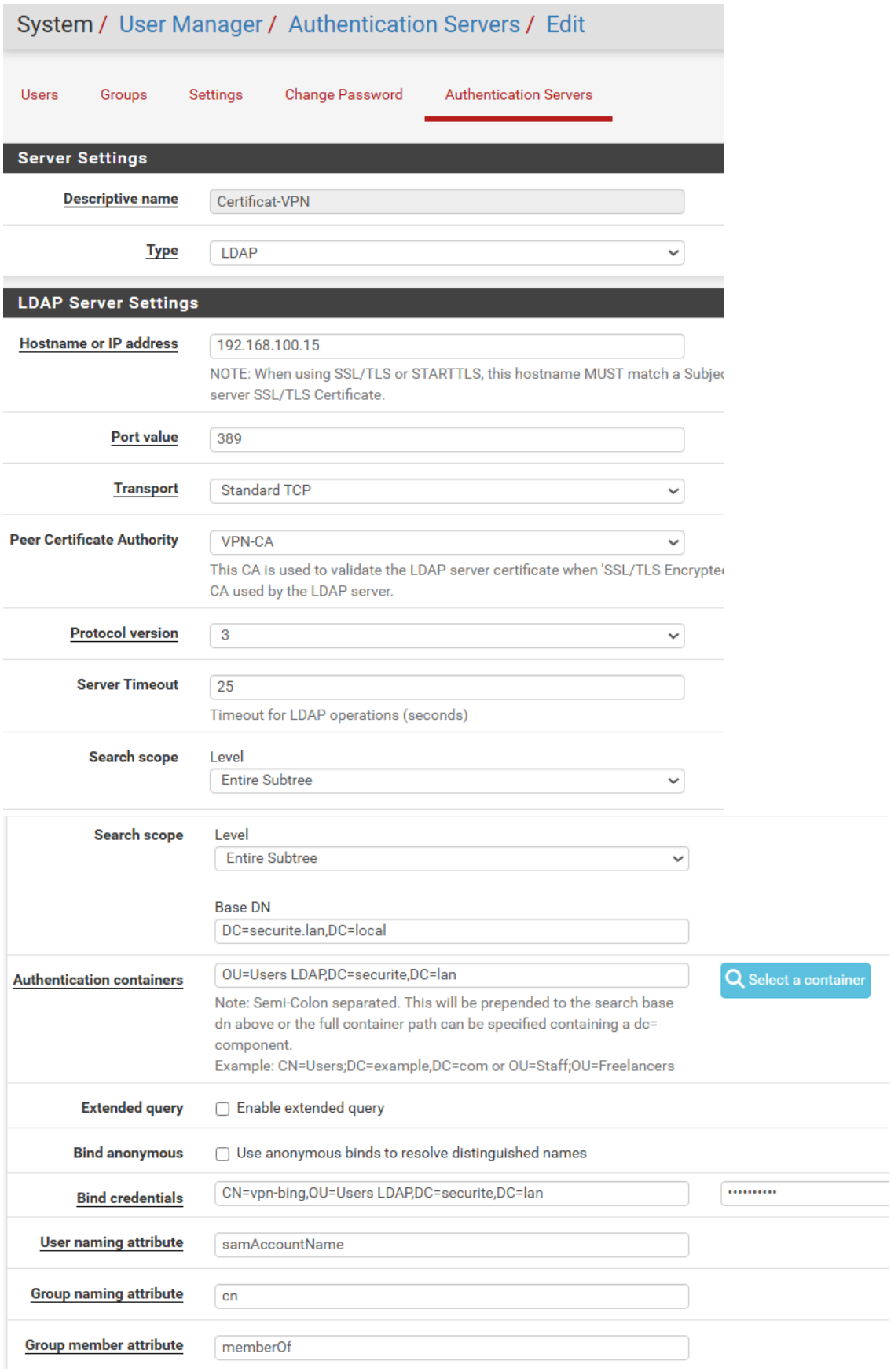
Et cliqué sur Save.

Intégration avec l'Active Directory

Configuration du serveur OpenVPN

La configuration du serveur OpenVPN a été réalisée via l'interface graphique de pfSense :

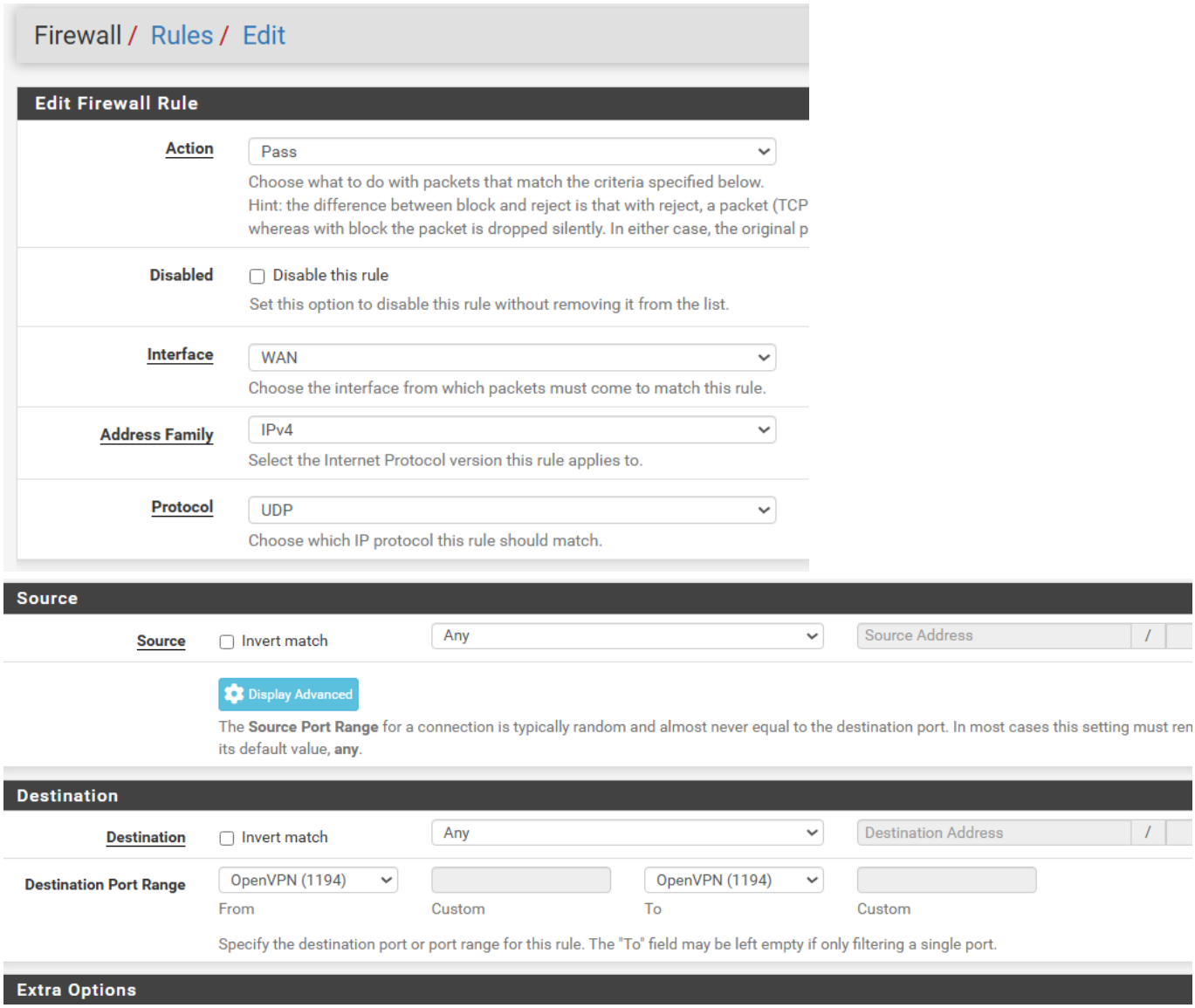
1. Navigation vers **System > User Manager**, onglet **Authentication Servers**
2. Création de l’autorisation pour la communication entre le serveur pfsense et le serveur AD



Configuration des règles de pare-feu

Pour permettre l'accès au serveur VPN depuis Internet, les règles de pare-feu suivantes ont été ajoutées :

1. Navigation vers **Firewall > Rules**, onglet **WAN**
2. Création d'une règle permettant le trafic UDP entrant sur le port 1194 :



Et cliqué sur Save.

Export du client

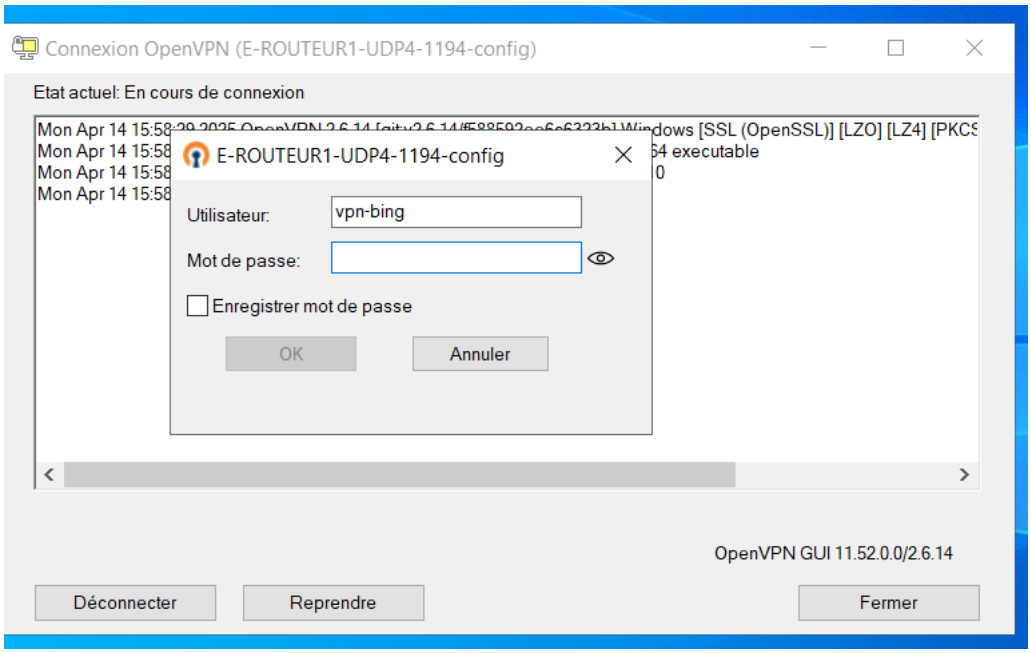
Pour permettre l'accès au serveur VPN depuis Internet, Il faut exporter un « client » pour pouvoir l'importer dans OpenVPN pour qu'il puisse récupérer toutes les infos de connexions.

1. Navigation vers **VPN > OpenVPN**, onglet **Client Export**
2. Exportation du client avec les paramètres suivants :

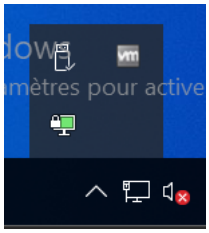
Cliquer sur « Most Clients » pour l'exportation

Tests et validation du VPN

1. Télécharger et installer OpenVPN GUI
2. Lancez OpenVPN et importe le .ovpn télécharger précédemment.



Il va donc vous demander de vous connecter avec un de vos utilisateurs de l'AD qui est autorisée de se connecter en VPN.



Si l'icône affiche vert vous êtes belle est bien connecter en VPN.