Documentation technique

Date : 15/04/2023

SOMMAIRE

1) Routeurs – firewalls

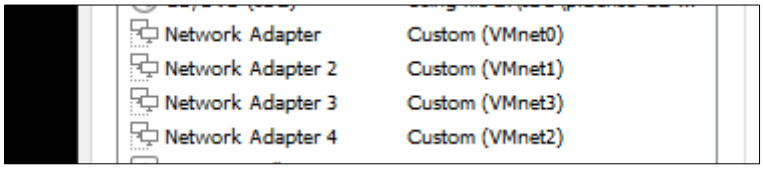
1.1) Configuration système et réseau

Une fois l'installation fini, on configure les adresses IP comme ci-dessous :

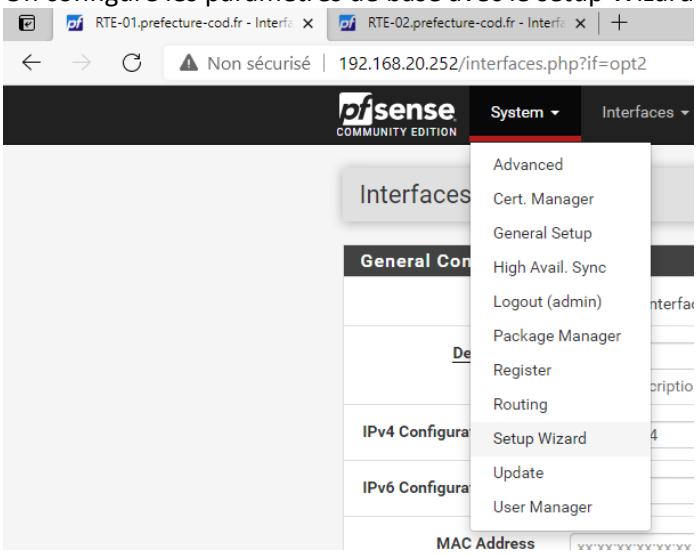
```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on RTE-01 ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.183.143/24
 LAN (lan)       -> em1        -> v4: 192.168.20.252/24
 CARP (opt1)     -> em2        -> v4: 192.168.40.1/30
 DMZ (opt2)      -> em3        -> v4: 192.168.30.252/24
```

On fait pareil sur le 2e routeur en mettant les adresses IP adaptées.

Il ne faut pas oublier de mettre les interfaces réseau de la VM dans le bon réseau :



On configure les paramètres de base avec le setup Wizard :



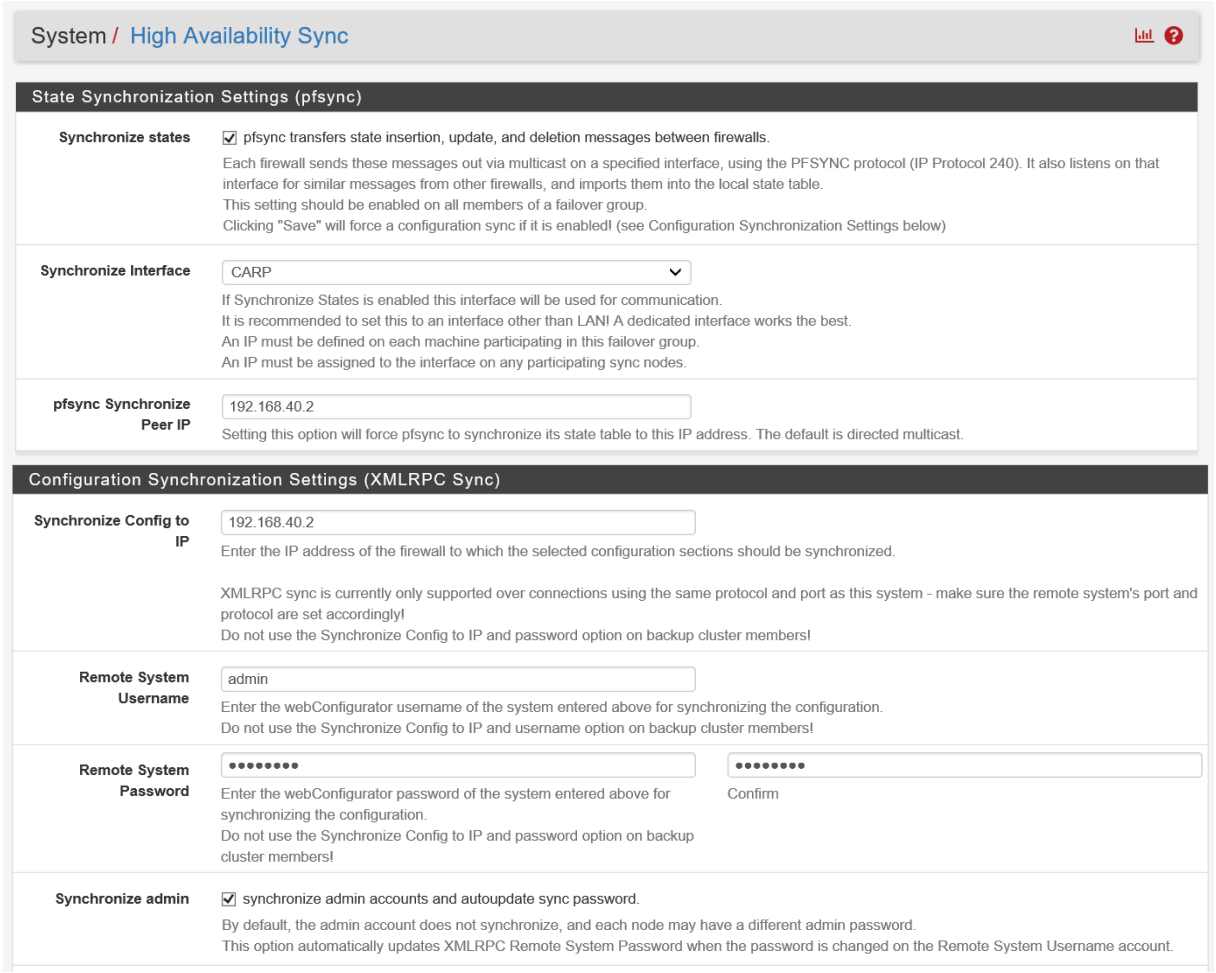
1.2) Redondance des routeurs

On ajoute sur les 2 routeurs une carte réseau. Elle sera dédiée à la synchronisation des 2 routeurs.

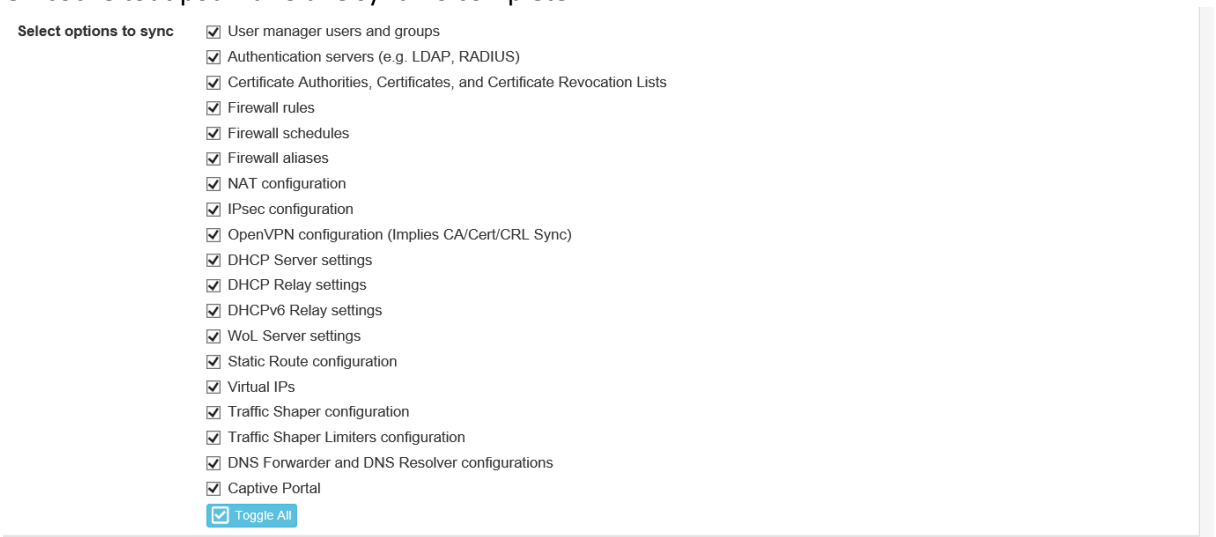
Dans l'onglet interfaces on configure la nouvelle carte réseau avec les paramètres suivants :

RTE-01	**RTE-02**
Nom : CARP	Nom : CARP
192.168.40.1/30	192.168.40.2/30
DNS : /	DNS : /
Passerelle : /	Passerelle : /

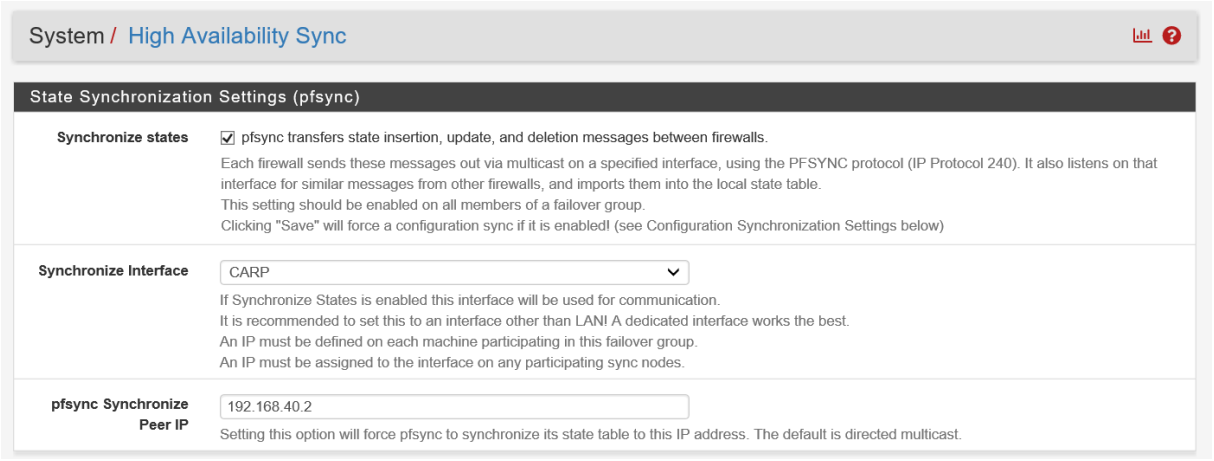
Maintenant on se rend dans System > High Avail Synch depuis le RTE-01 :



On coche tout pour faire une synchro complète :



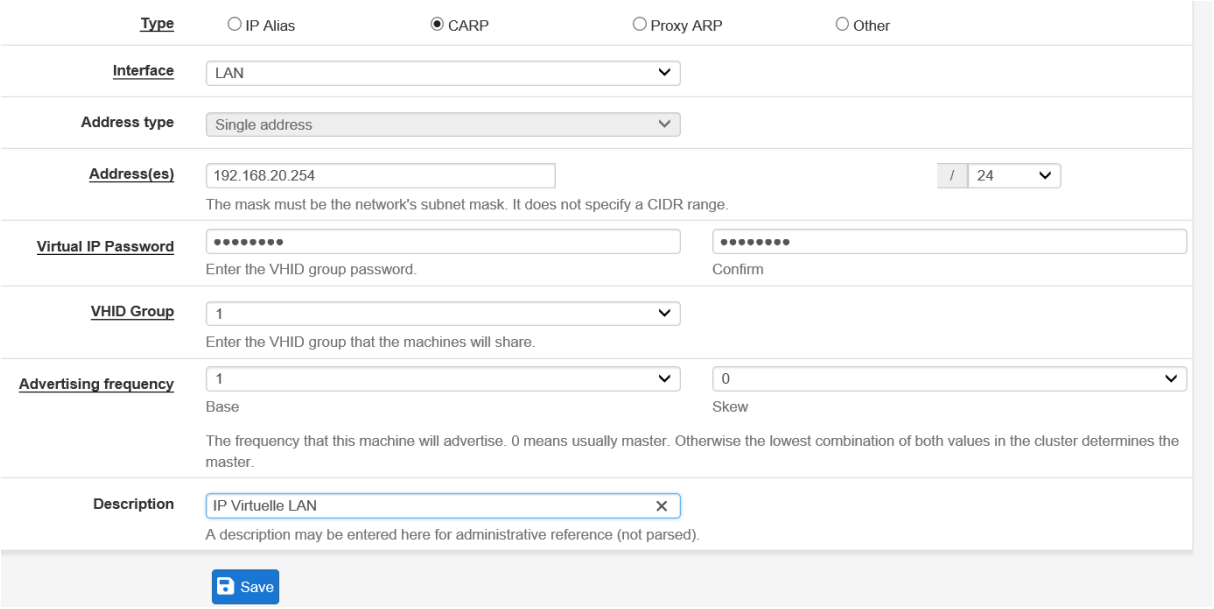
Sur le RTE-02, on se rend au même endroit, et on modifie simplement ces 3 options :



Attention à mettre l'IP en 192.168.40.1 et non en 192.168.40.2.
On ne modifie pas les options qui suivent. Elles doivent être modifiés seulement sur le routeur maitre.

1.3) Adresse IP virtuelle LAN

La manipulation suivante est à faire sur chaque routeur.
On se rend dans Firewall > Virtual IPs. On ajoute une adresse virtuelle avec les paramètres suivants :

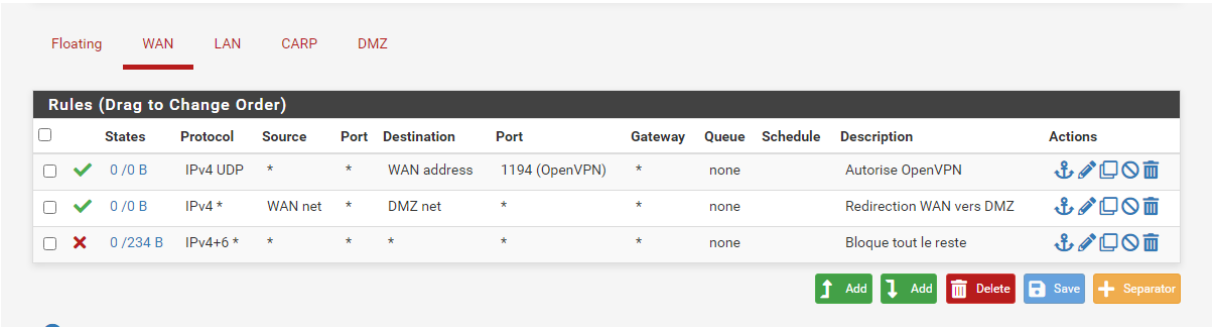


1.4) Adresse IP virtuelle DMZ

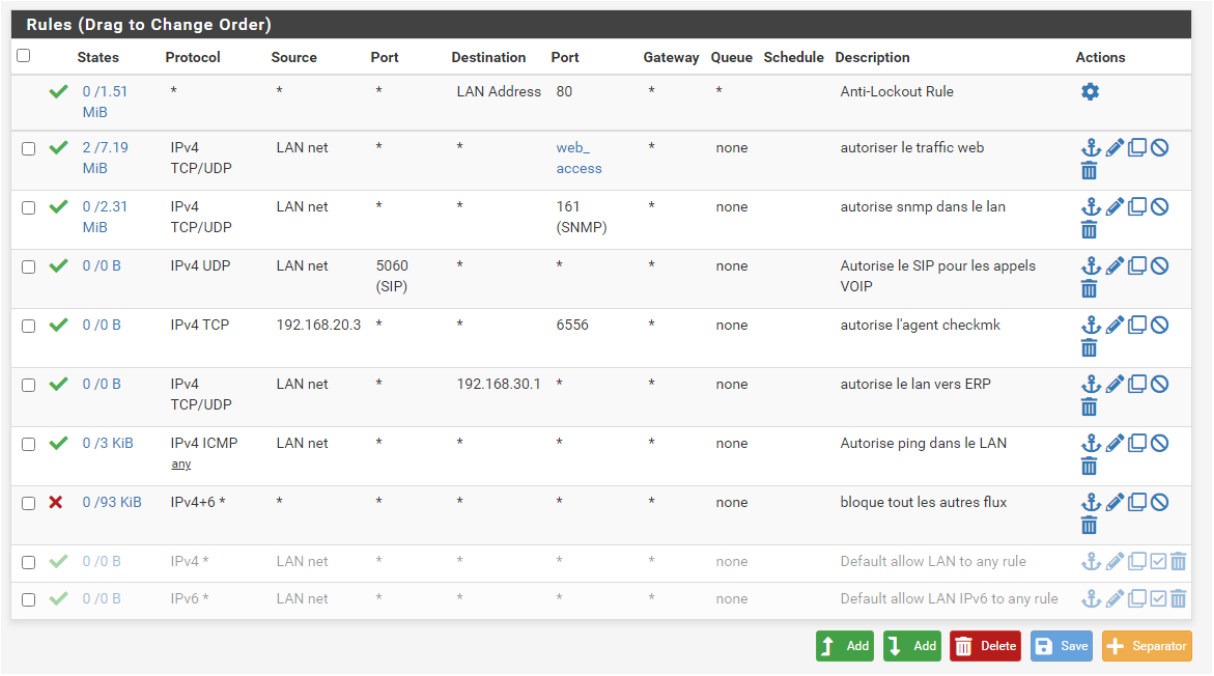
La manipulation est la même que pour l'adresse IP virtuelle LAN. Il faut simplement remplacer :
Interface : mettre DMZ et pas LAN
IP : on met 192.168.30.254 et pas 192.168.20.254

1.5) Règles de pares-feux

Interface WAN :

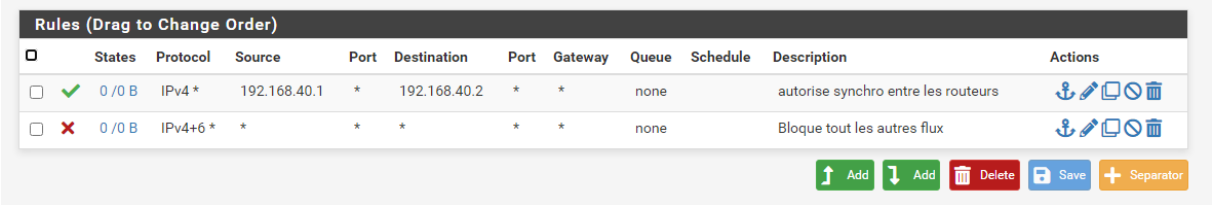


Interface LAN :

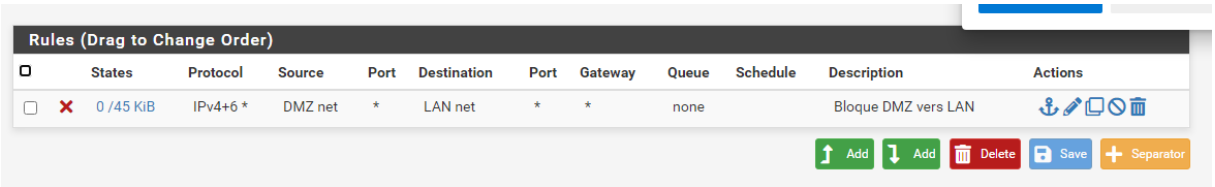


L'alias web_access comprend les ports 53, 80 et 443

Interface CARP :



Interface DMZ :



2) Serveurs Windows

2.1) Installation et configuration de SRV-AD01

Configuration réseau et système :

```
# Définir les variables pour les paramètres de configuration réseau
$InterfaceAlias = "Ethernet0"
$IPAddress = "192.168.20.5"
$PrefixLength = "24"
$DefaultGateway = "192.168.20.254"
$DNSAddresses = "192.168.20.5","192.168.20.6"
$ComputerName = "SRV-AD01"
# Définir l'adresse IP statique, le masque de sous-réseau et la passerelle
New-NetIPAddress -InterfaceAlias $InterfaceAlias -IPAddress $IPAddress -PrefixLength $PrefixLength
-DefaultGateway $DefaultGateway
# Définir les serveurs DNS
Set-DnsClientServerAddress -InterfaceAlias $InterfaceAlias -ServerAddresses $DNSAddresses
# Définir le nom d'hôte
Rename-Computer -NewName $ComputerName
# Redémarrer le serveur pour appliquer les changements
Restart-Computer
```

Définir un mot de passe pour le compte administrateur :

```
$NewPassword = Read-Host "Entrez un nouveau mot de passe pour le compte Administrateur" -
AsSecureString
# Définir le nouveau mot de passe pour le compte Administrateur
Set-LocalUser -Name "Administrateur" -Password (ConvertTo-SecureString -String $NewPassword -
AsPlainText -Force)
```

2.2) Création de l'AD

Depuis le SRV-AD01 :

```
# Installe le rôle AD DS et les outils de gestion AD DS
Install-WindowsFeature AD-Domain-Services, RSAT-AD-AdminCenter
# Configure le nouveau domaine
$domaine = "prefecture-cod.fr"
$domaineNetBios = "PREFECTURE-COD"
Import-Module ADDSDeployment
Install-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomainMode "WinThreshold" `
-DomainName $domaine `
-DomainNetbiosName $domaineNetBios `
-ForestMode "WinThreshold" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

On définit également un mot de passe pour le compte Administrateur, depuis le gestionnaire « Utilisateurs et ordinateurs Active Directory ».

2.3) Installation et configuration de SRV-AD02

Configuration réseau et système :

```
# Définir les variables pour les paramètres de configuration réseau
$InterfaceAlias = "Ethernet0"
$IPAddress = "192.168.20.6"
$PrefixLength = "24"
$DefaultGateway = "192.168.20.254"
$DNSAddresses = "192.168.20.5","192.168.20.6"
$ComputerName = "SRV-AD02"
# Définir l'adresse IP statique, le masque de sous-réseau et la passerelle
New-NetIPAddress -InterfaceAlias $InterfaceAlias -IPAddress $IPAddress -PrefixLength $PrefixLength
-DefaultGateway $DefaultGateway
# Définir les serveurs DNS
Set-DnsClientServerAddress -InterfaceAlias $InterfaceAlias -ServerAddresses $DNSAddresses
# Définir le nom d'hôte
Rename-Computer -NewName $ComputerName
# Redémarrer le serveur pour appliquer les changements
Restart-Computer
```

Définir un mot de passe pour le compte administrateur :

```
$NewPassword = Read-Host "Entrez un nouveau mot de passe pour le compte Administrateur" -
AsSecureString
# Définir le nouveau mot de passe pour le compte Administrateur
Set-LocalUser -Name "Administrateur" -Password (ConvertTo-SecureString -String $NewPassword -
AsPlainText -Force)
```

2.4) Ajout de SRV-AD02 en contrôleur de domaine

```
# Installe le rôle AD DS et les outils de gestion AD DS
Install-WindowsFeature RSAT-AD-PowerShell
Install-WindowsFeature AD-Domain-Services, RSAT-AD-AdminCenter
# Ajout au domaine existant
$domaine = "prefecture-cod.fr"
$nomSite = ""
Install-ADDSDomainController `
-DomainName $domaine `
-Credential (Get-Credential) `
-SiteName $nomSite `
-DatabasePath "C:\Windows\NTDS" `
-LogPath "C:\Windows\NTDS" `
-SYSVOLPath "C:\Windows\SYSVOL" `
```

Une fenêtre apparait et demande un compte Admin du domaine pour valider l'installation. On se connecte avec le compte *Administrateur.*

2.5) Configuration du DCHP

Depuis le SRV-AD01, on installe le role DHCP :

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
```

Configurer l'étendue DHCP :

```
Add-DhcpServerv4Scope
Set-DhcpServerv4OptionValue -DNSServer 192.168.20.5, 192.168.20.6 -DNSDomain prefecture-cod.fr
-Router 192.168.20.254
Add-DhcpServerv4Scope -Name "Pool-PCs" -StartRange 192.168.20.30 -EndRange 192.168.20.250 -
SubnetMask 255.255.255.0 -Description "pool pour PCs du LAN"
```

2.6) Ajout des utilisateurs dans l'AD

```
$FirstName = "Erwann"
$LastName = "Erwann"
$SamAccountName = "erwann"
$Password = "abc123!" | ConvertTo-SecureString -AsPlainText -Force
$Description = "utilisateur du domaine"
$Path = "OU=utilisateurs,DC=préfecture-cod,DC=fr"
New-ADUser -Name "$FirstName $LastName" `
        -SamAccountName $SamAccountName `
        -UserPrincipalName "$SamAccountName@example.com" `
        -AccountPassword $Password `
        -Enabled $true `
        -Description $Description `
        -Path $Path
```

3) Serveur de supervision

3.1) Installation et configuration système réseau

On installe un ubuntu server 22.04
On lance la commande pour mettre à jour le système :

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

Puis on fait la configuration réseau en modifiant le fichier 00-installer-config.yaml comme ci-dessous avec la commande

```
Sudo nano /etc/network/netplan
```

```
  GNU nano 6.2                          00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      addresses:
      - 192.168.20.3/24
      gateway4: 192.168.20.254
      nameservers:
        addresses:
        - 192.168.20.5
        - 192.168.20.6
        search:
        - prefecture-cod.fr
  version: 2
```

Ensuite :

```
Netplan apply
```

3.2) Installer checkmk

On télécharge le paquet debian depuis le site en sélectionnant la version RAW : https://checkmk.com/download. On copie le paquet et on l'installe avec les commandes :

```
mkdir /home/tech/deb
cd /home/tech/deb
cp /mnt/hfgs/share/check-mk-raw-2.1-0p25_0.jammy_amd64.deb checkmk-raw-2.1.deb
apt install ./checkmk-raw-2.1.deb
```

(les commandes ci-dessus nécessitent d'avoir créer un dossier partagé vmware avec l'hote)
On crée un site CheckMK que l'on appelle « préfecture-cod » :

```
omd create prefecture_cod
omd start prefecture_cod
```

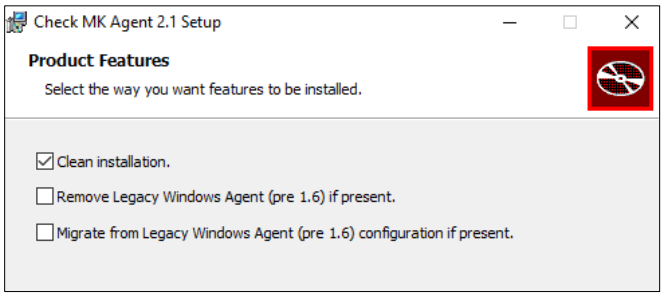
3.3) Configuration de checkmk

On se rend sur le SRV-SUP depuis l'interface web : http://192.168.20.3/prefecture_cod
On se connecte avec
user : cmkadmin
password : le mot de passe est généré automatiquement lors de l'installation
On se rend dans User > Change password (en bas à gauche) et on modifie le mot de passe.

3.4) Installation de l'agent

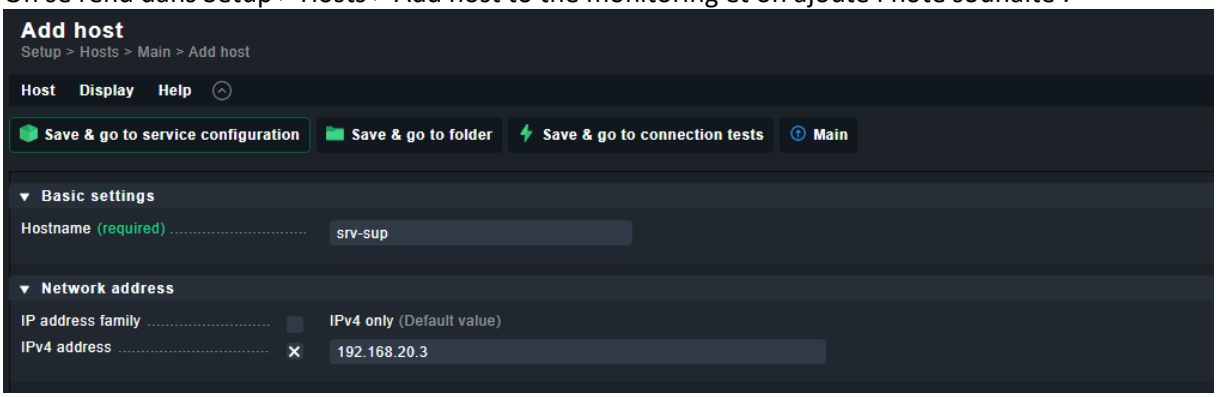
Maintenant nous allons voir comment intégrer des hôtes à notre logiciel de supervision. Tout d'abord il faut installer l'agent sur le système.
Dans Setup > Agents, on télécharge les agents pour les systèmes souhaités (linux, windows, freebsd, macos, …)
Puis on les installe sur les systèmes

Pour l'installation de l'agent sur Windows, on choisit de faire une clean installation :

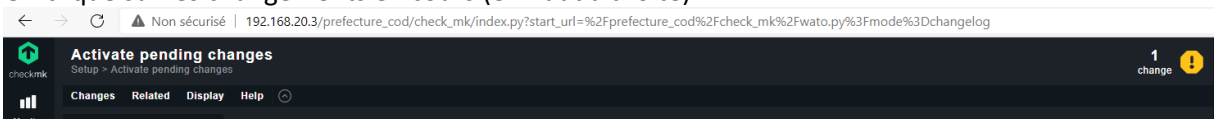


3.5) Ajout de l'hôte

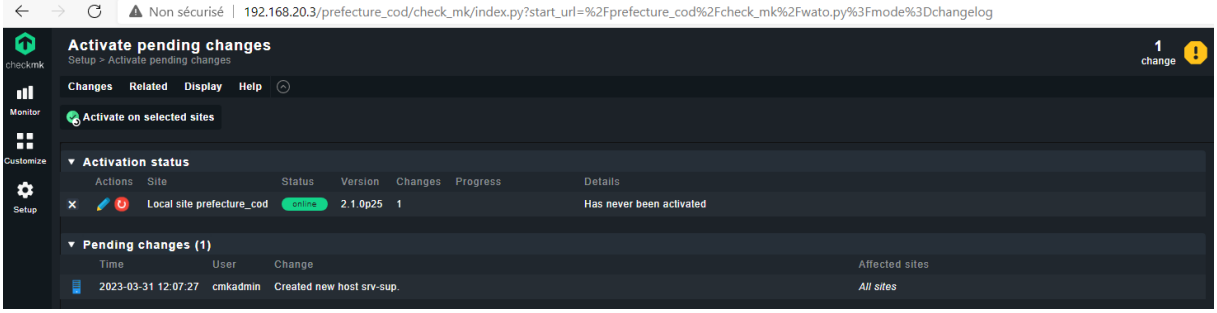
On se rend dans Setup > Hosts > Add host to the monitoring et on ajoute l'hôte souhaité :



On clique sur les changements en cours (en haut à droite) :

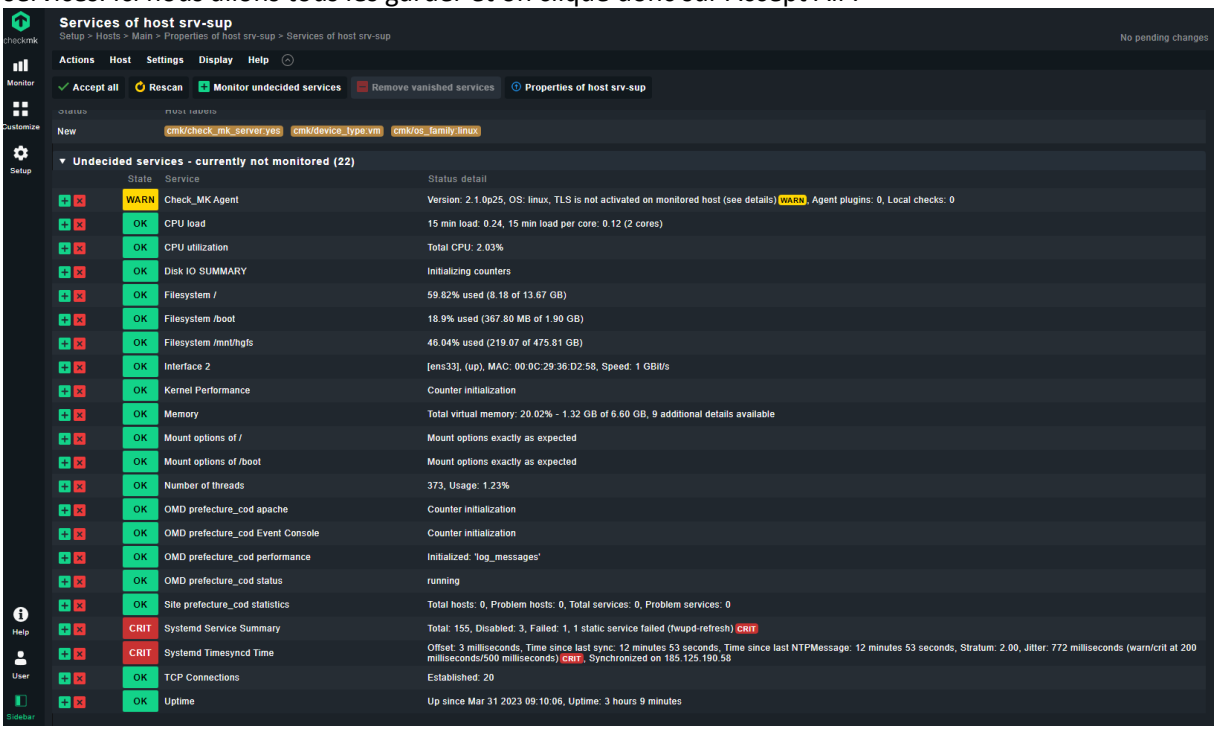


On clique sur Activitate on selected sites



Maintenant on clique sur l'hote, puis sur Services of Host. On choisit de garder ou d'enlever les

services. Ici nous allons tous les garder et on clique donc sur Accept All :

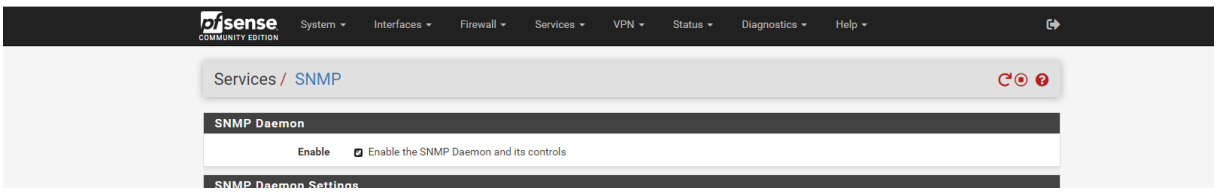


On applique les changements en cliquant sur *Change* puis sur *Activitate on selected sites*

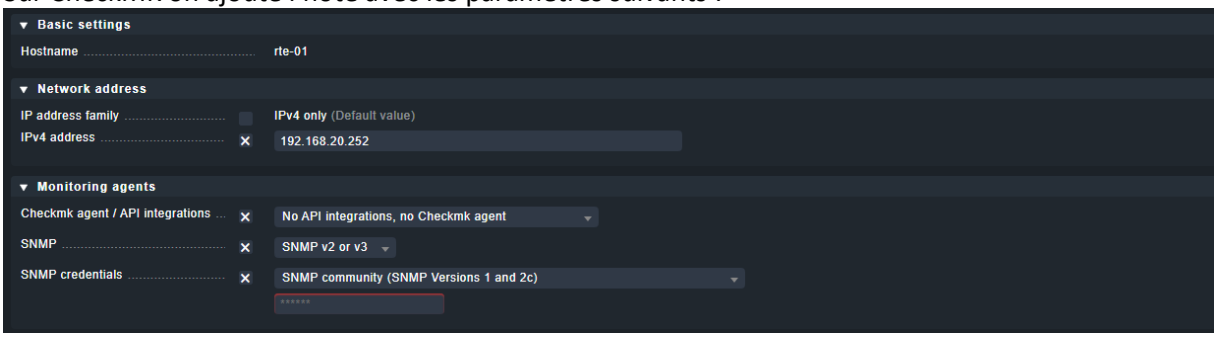
Maintenant sur le *Main dashboard,* on peut voir les alertes.

3.5) Ajouter les pares-feux via SNMP

On active le service SNMP :



Sur CheckMK on ajoute l'hote avec les paramètres suivants :



Puis dans Services of Host on ajoute tous les services.

4) Serveur de messagerie

4.1) Installation Hmail :

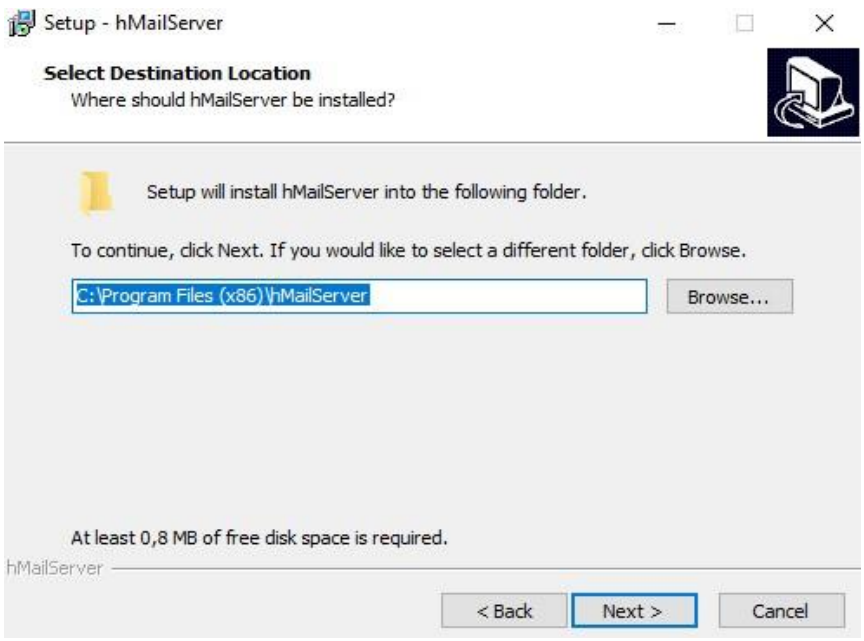
Exécuter le fichier d'installation de hmailserver que l'on télécharge ici :
https://www.hmailserver.com/

(pensez bien à prendre la dernière version et non la béta)

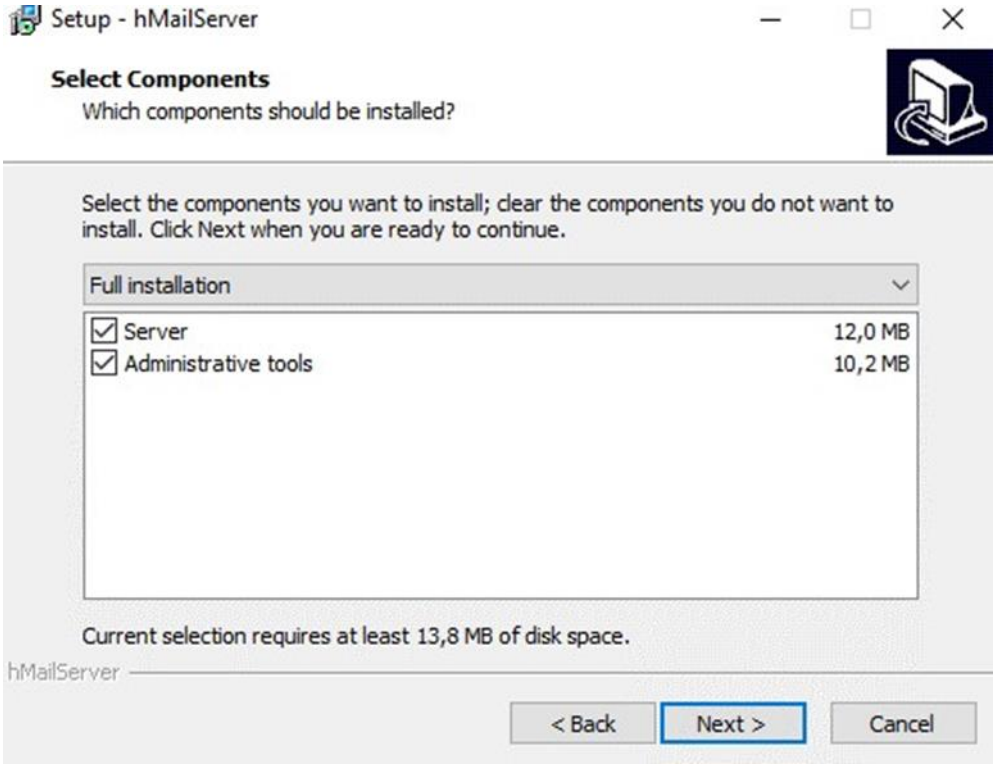
Faites next

Accepter et faites next

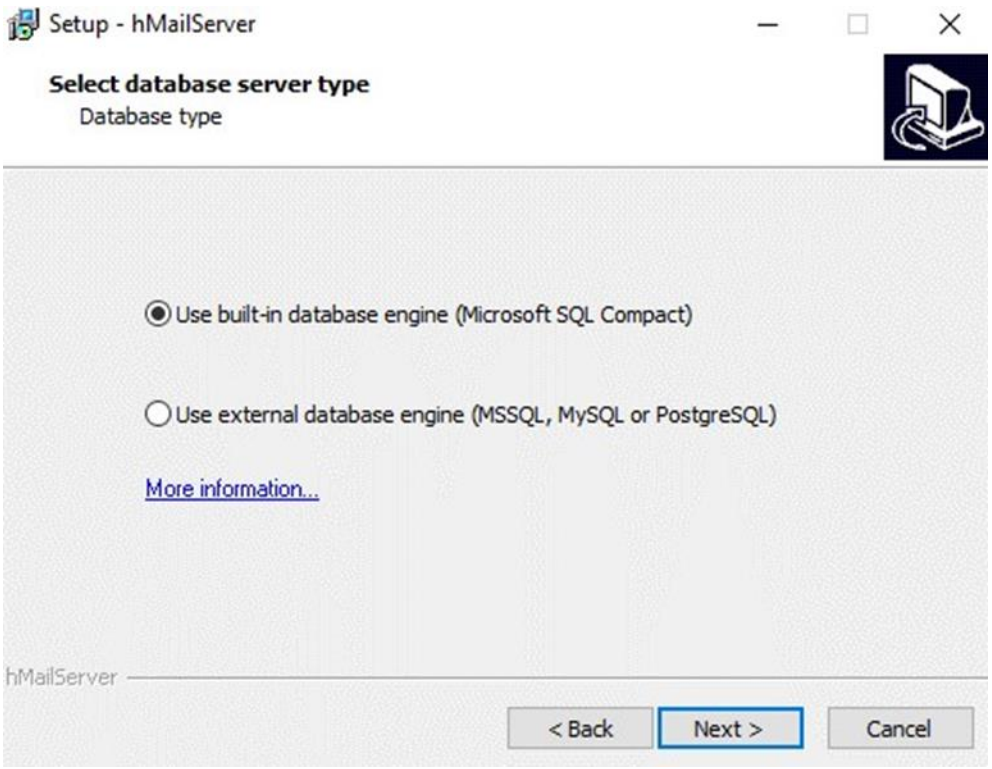
faites next



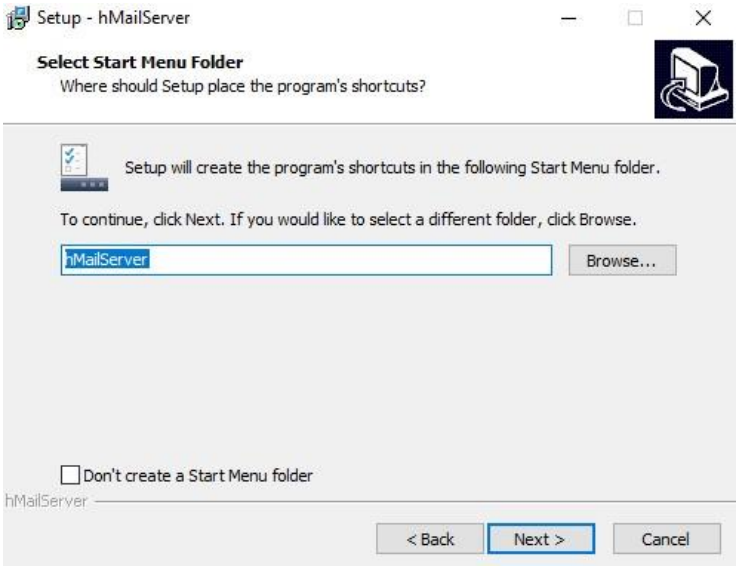
Gardez la full installation et faites next :



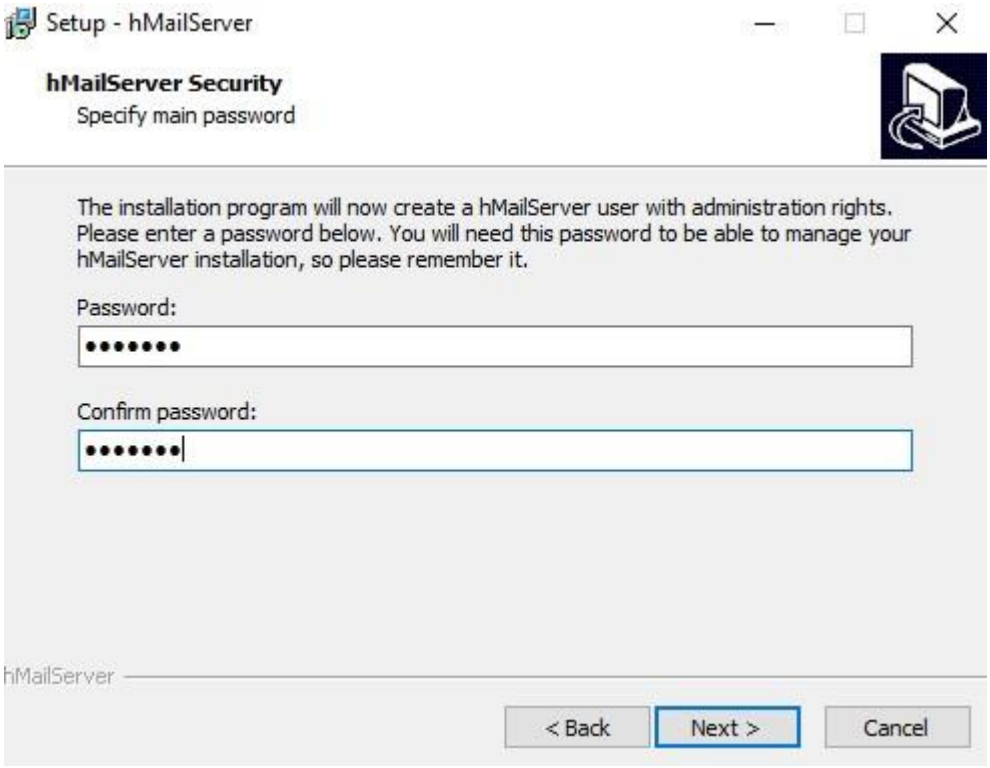
laisser le paramètre par défaut et faites next :



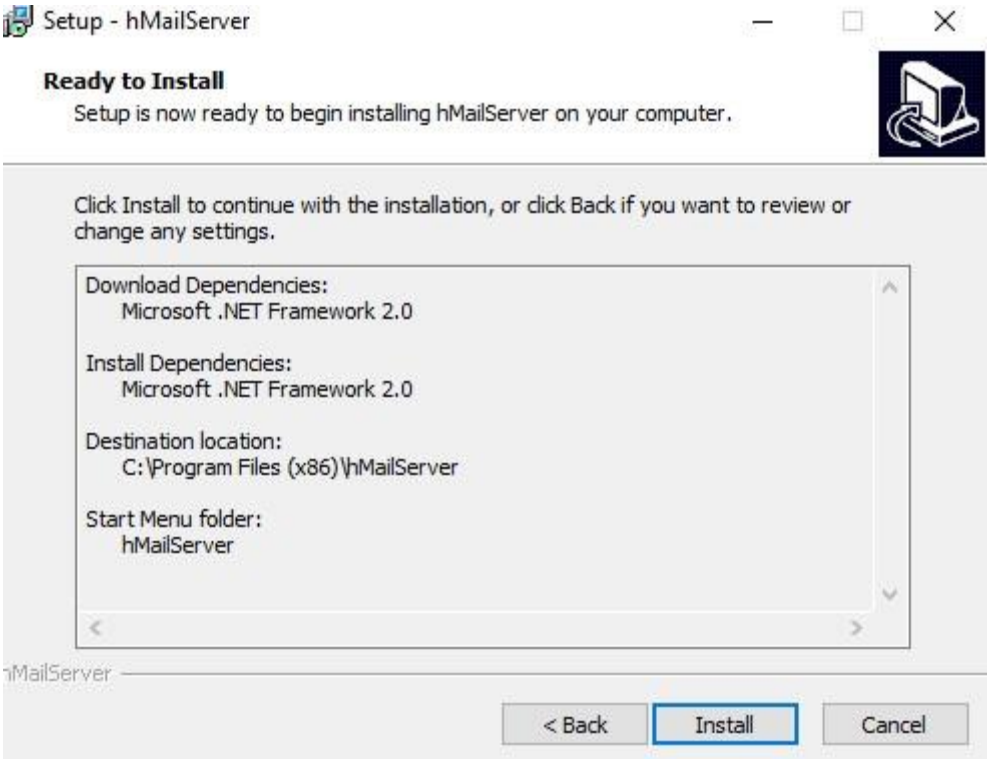
laisser par défaut et faites next :



Choisissez un mot de passe administrateur pour HmailServeur :



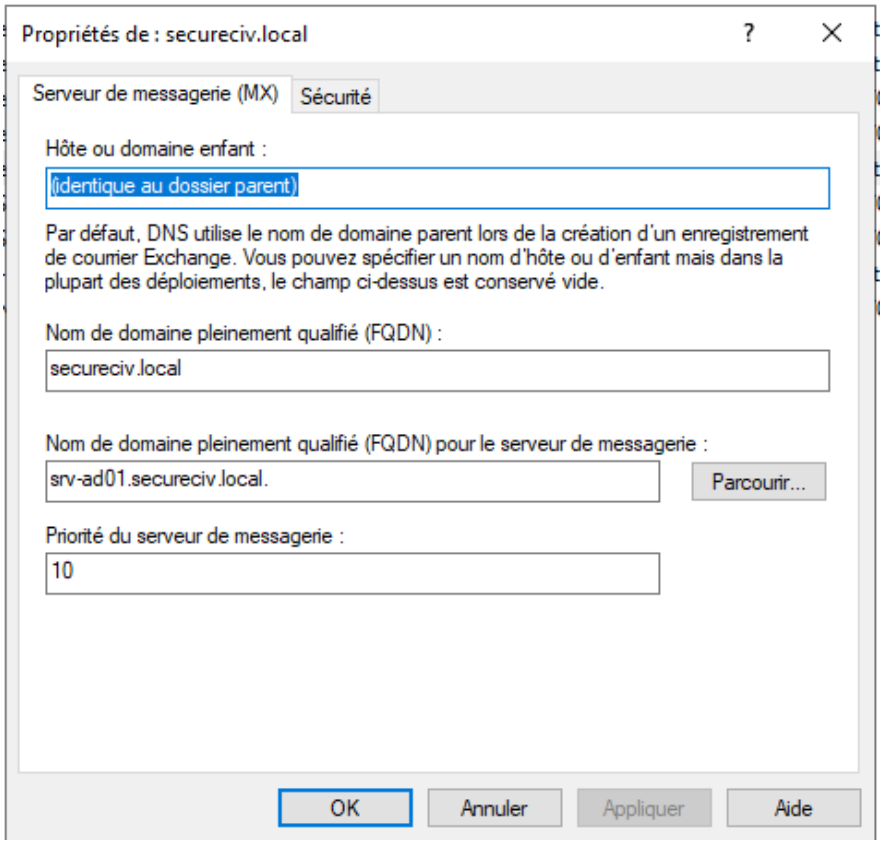
Puis faites Install :



(Penser à installer la fonctionnalité net framework 3.5 sur le serveur)

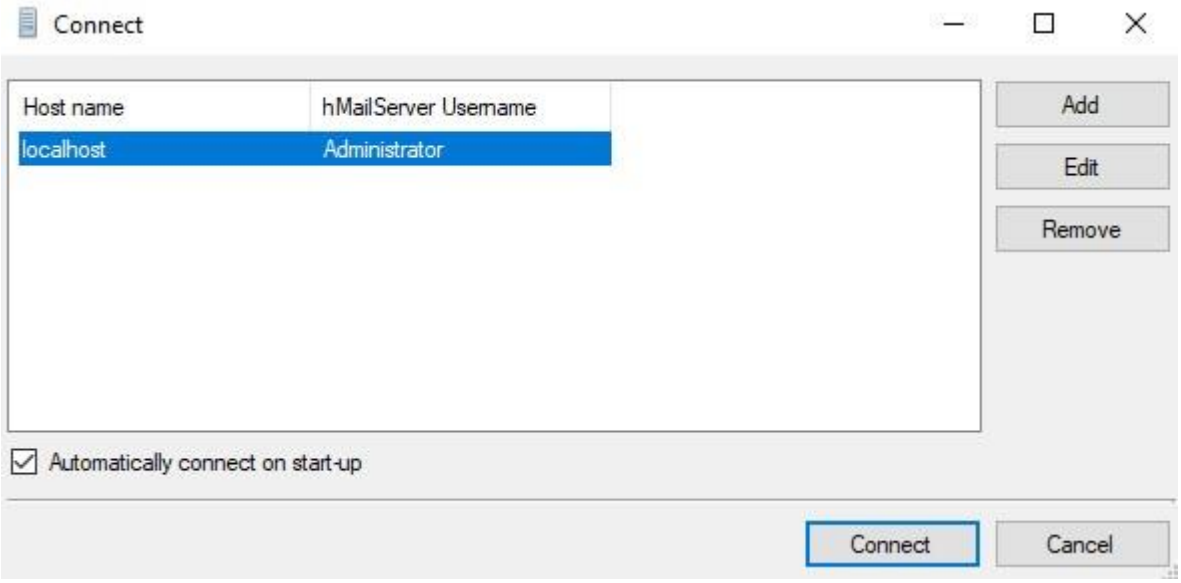
4.2) Configuration DNS pour le serveur de messagerie :

Nous avons ajouté un nouveau serveur de messagerie dans la zone de recherche direct du DNS de notre LAN. Il permettra de définir quel serveur va prendre en charge la gestion des mails.

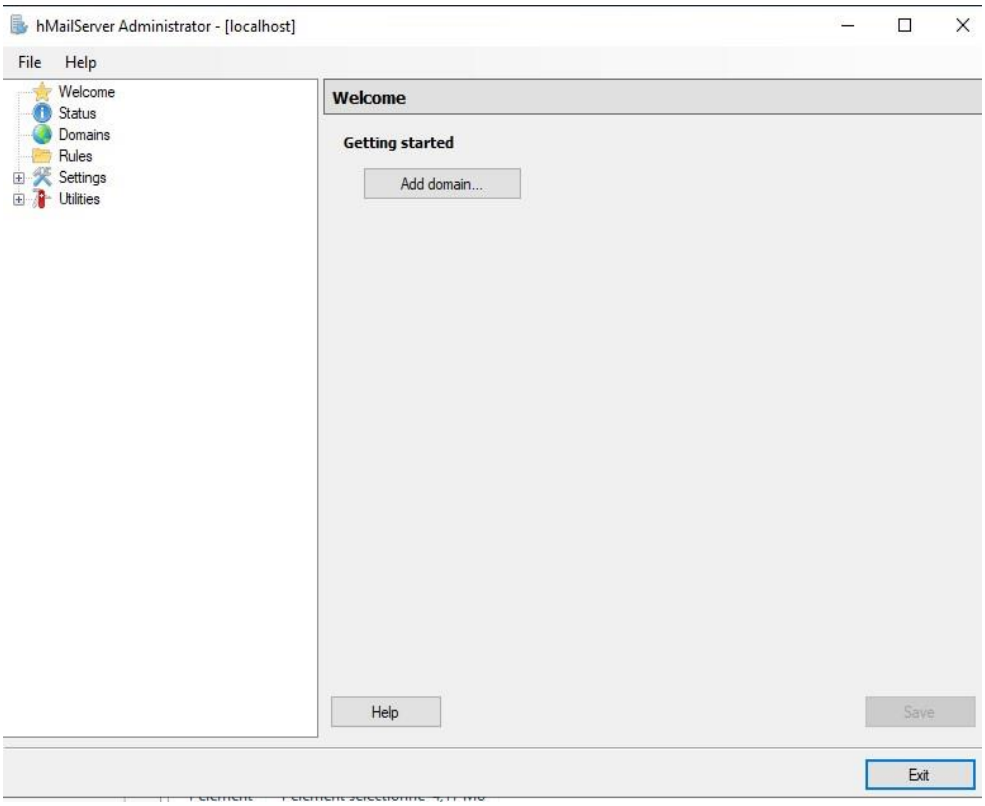


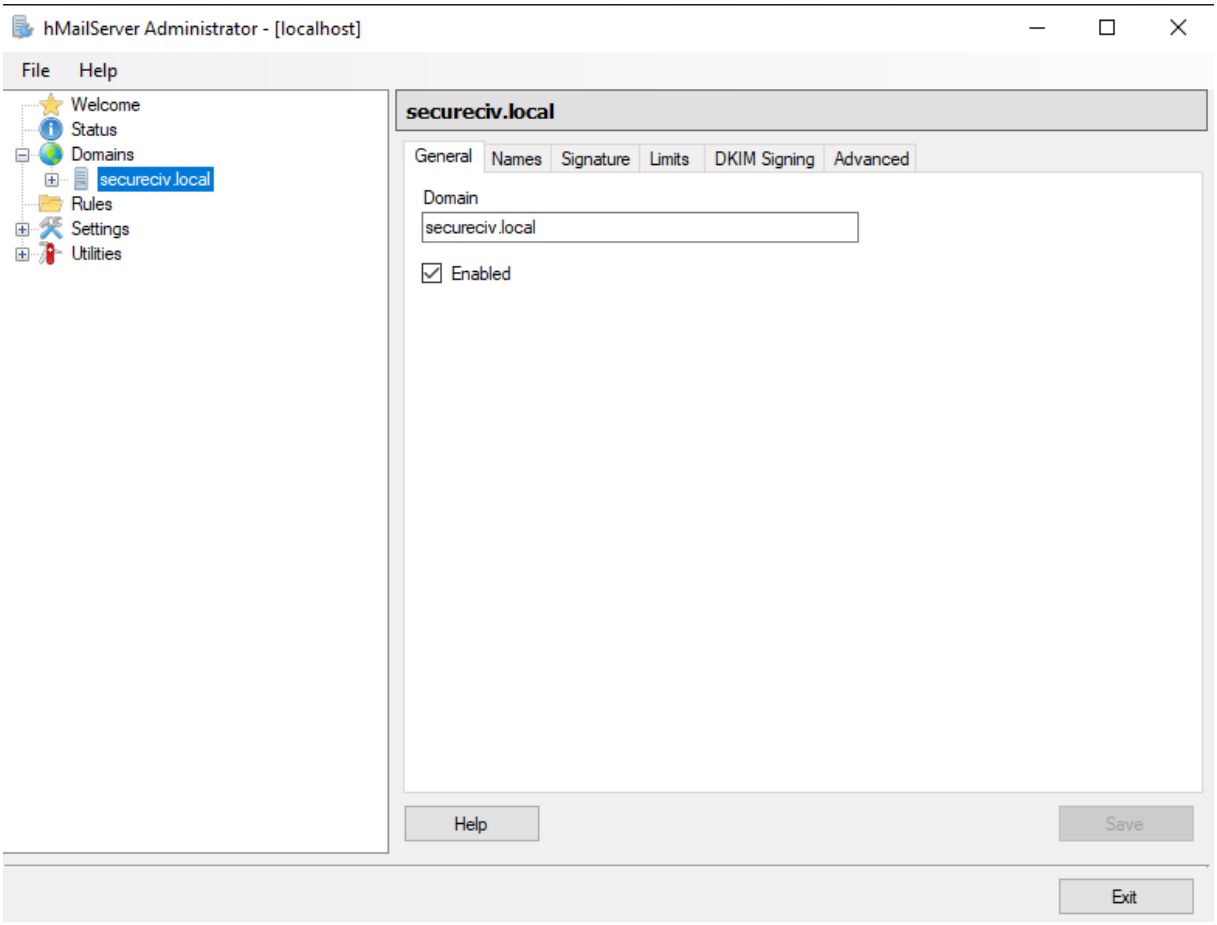
4.3) Configuration Hmailserver

Dans un premier nous devons nous connecter avec le mot de passe définit au moment de l'installation en cliquant sur connect.

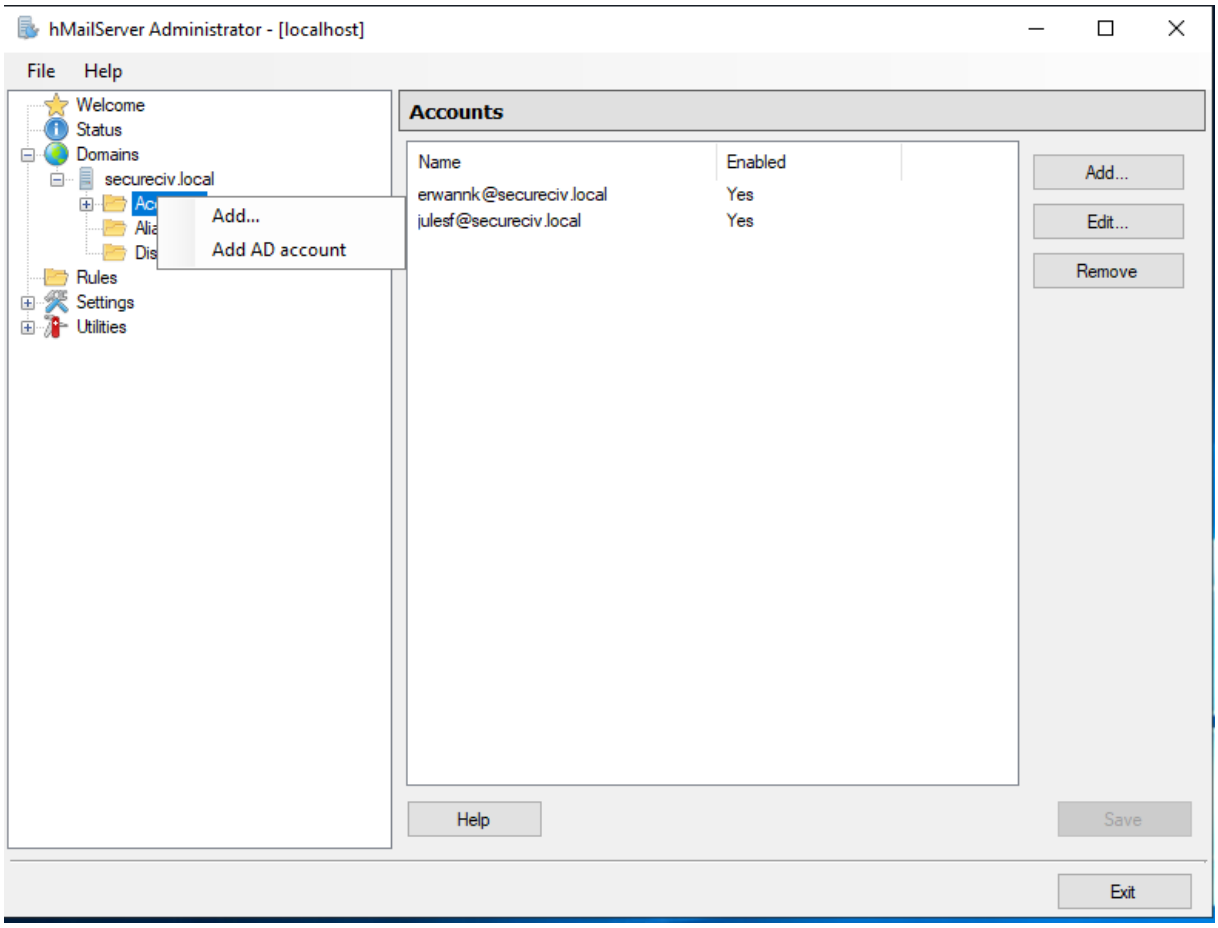


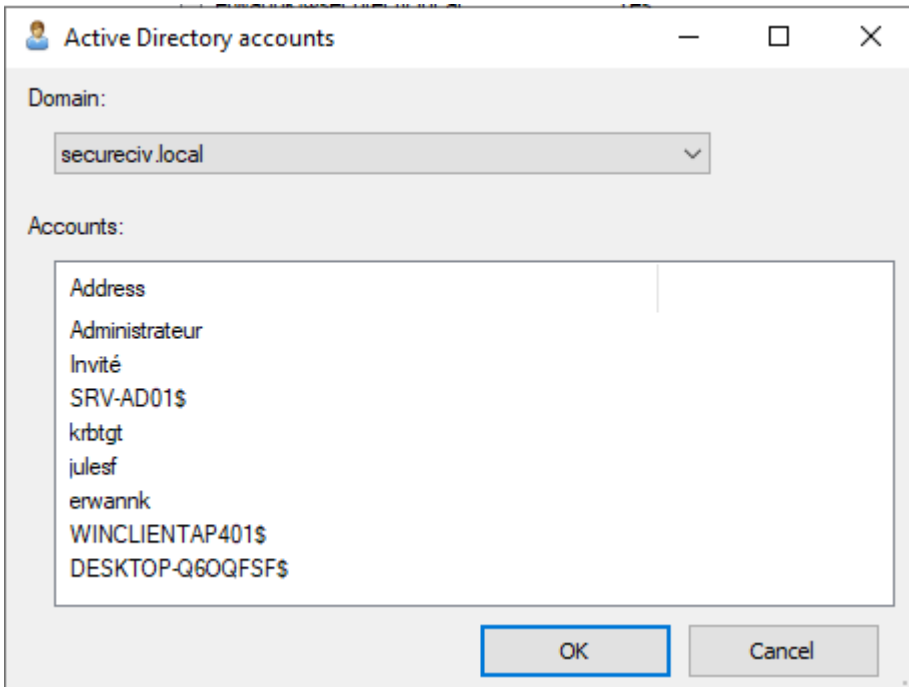
Ensuite nous allons ajouter le domaine en cliquant sur Add domain :

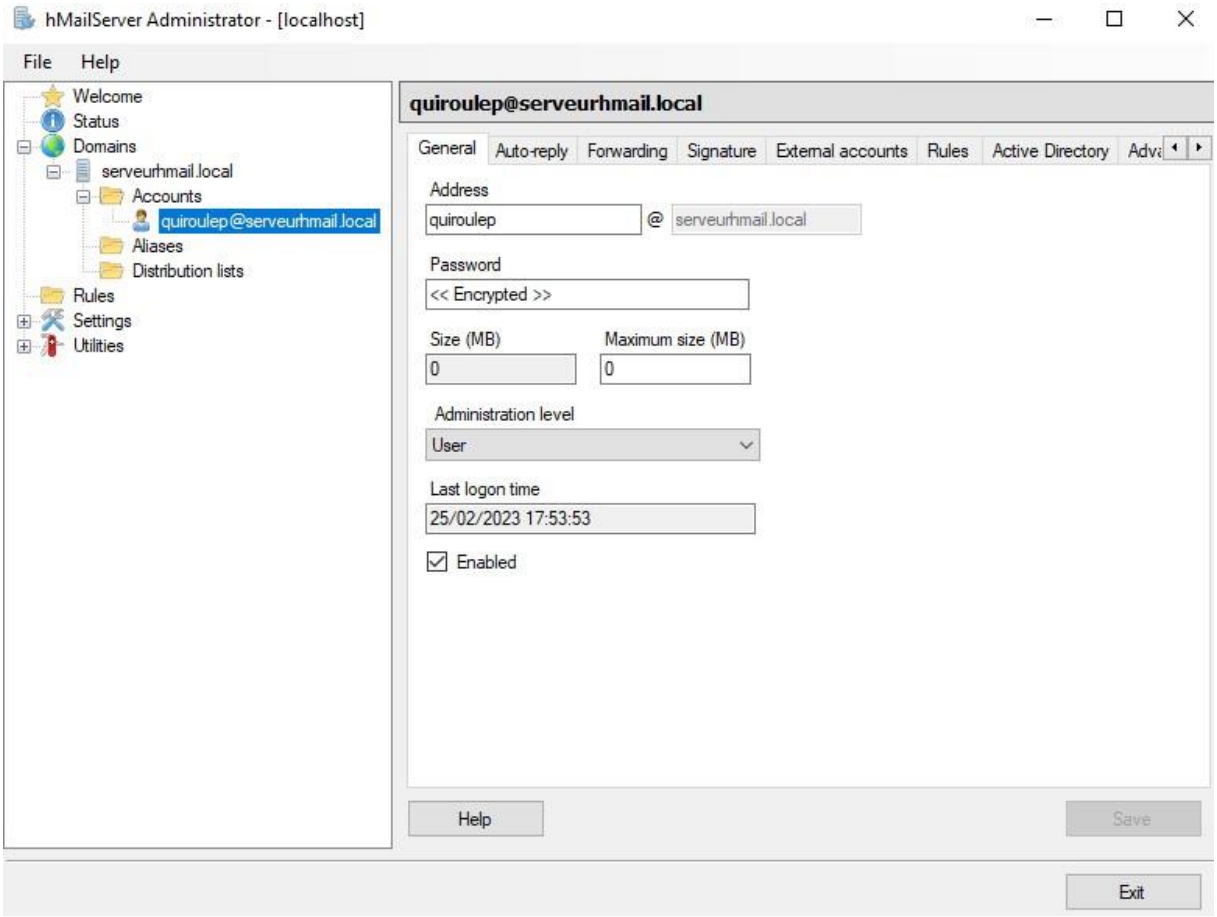




Une fois celui-ci ajouté, faites clic droit sur le nom de domaine et cliquez sur AD account pour ajouter les deux comptes crée au préalable dans l'AD.

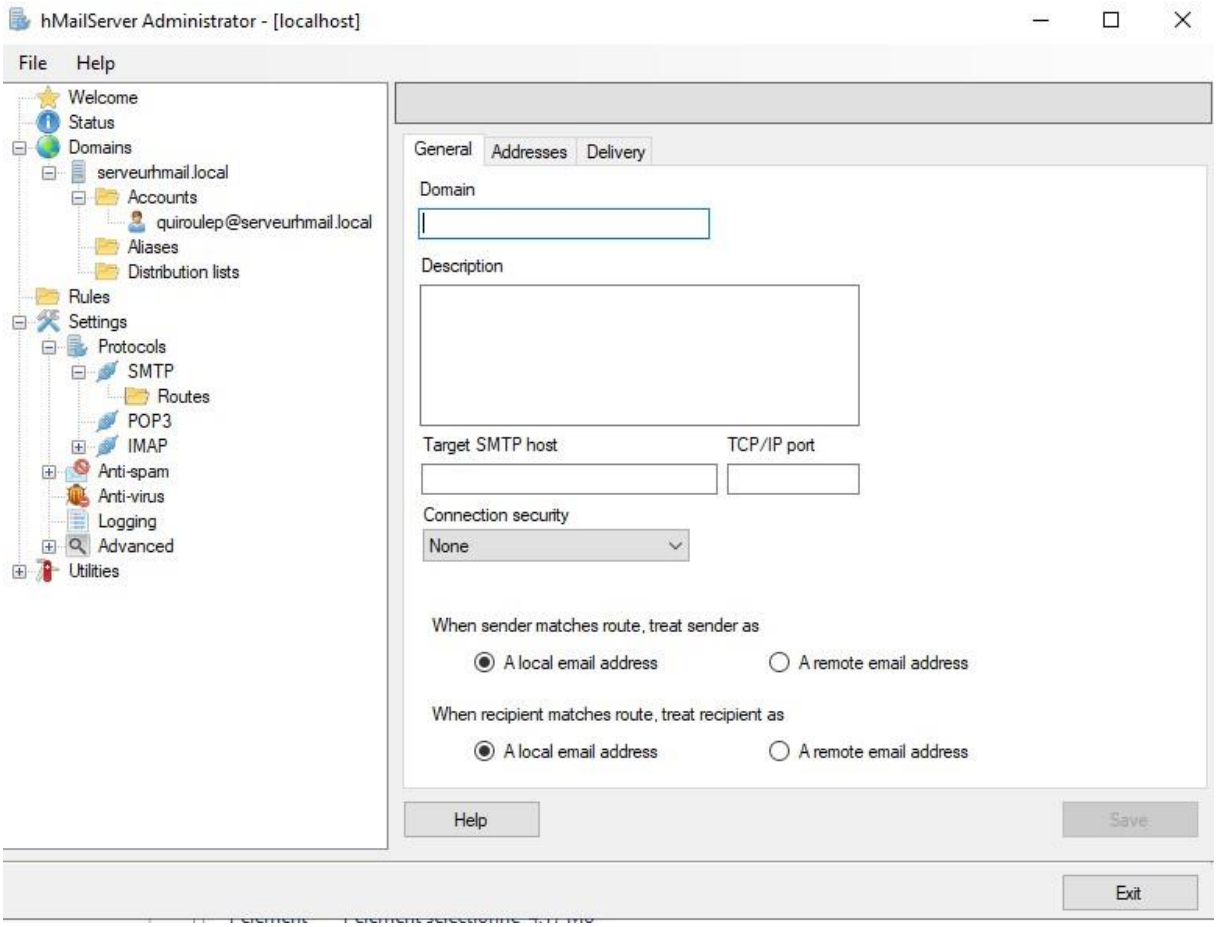

hMailServer Administrator - [localhost]
File
Help
Welcome
Status
Domains
secureciv.local
Add...
Add AD account
Rules
Settings
Utilities
Accounts
Name
Enabled
erwannk@secureciv.local
Yes
julesf@secureciv.local
Yes
Add...
Edit...
Remove
Help
Save
Exit


Active Directory accounts
Domain:
secureciv.local
Accounts:
Address
Administrateur
Invité
SRV-AD01$
krbtgt
julesf
erwannk
WINCLIENTAP401$
DESKTOP-Q6OQFSF$
OK
Cancel



4.4) Configuration SMTP :

Pour cela allez à nouveau dans le HmailServer Administrator
Dans Settings/protocals/SMTP/Routes

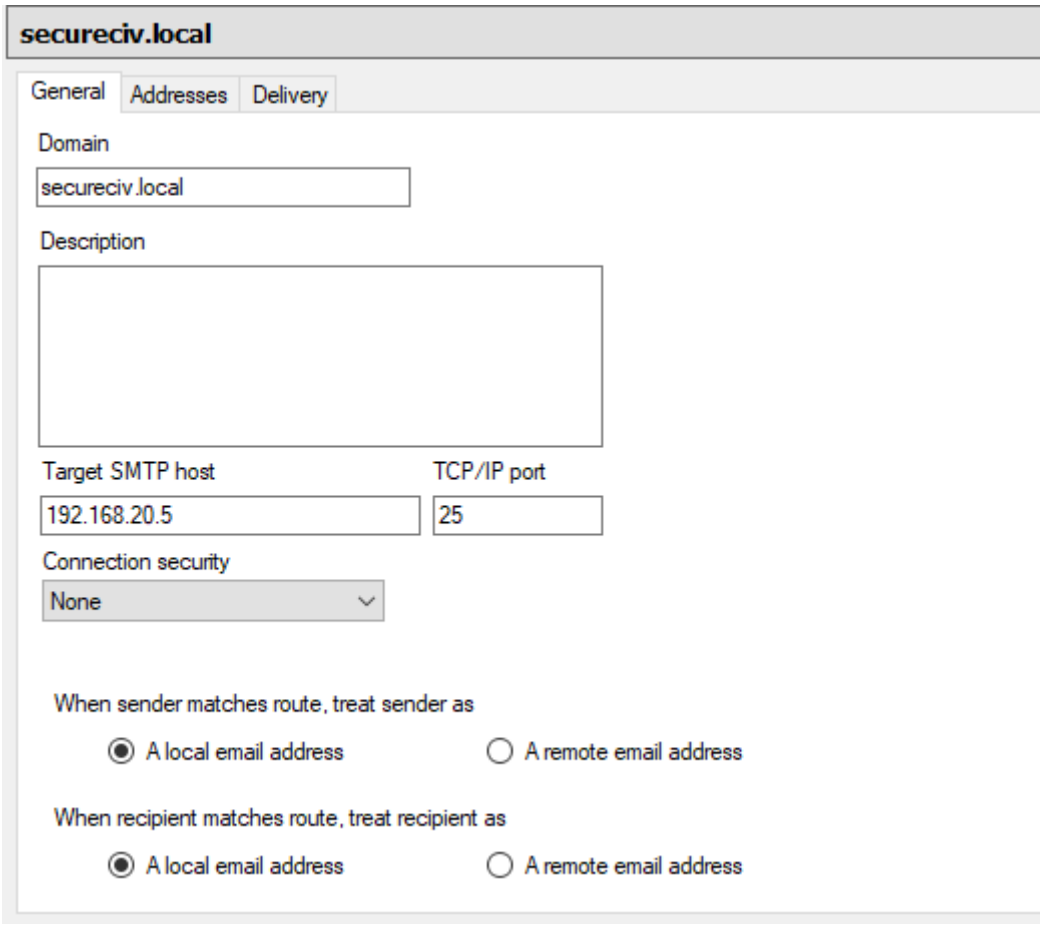


Entrez dans domain le nom de domaine de votre serveur mail.
Ainsi que son adresse IP dans target SMTP host

On utilisera le port 25

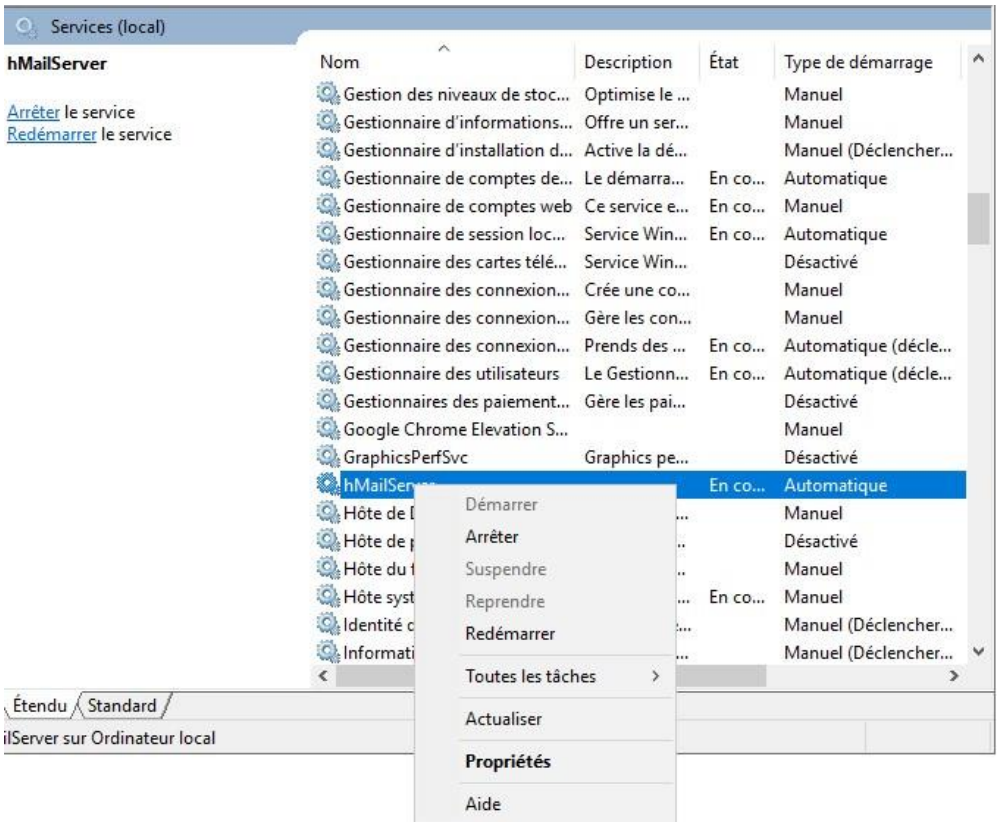
Laissez le reste par défaut

Faites Save



Allez ensuite dans service.msc

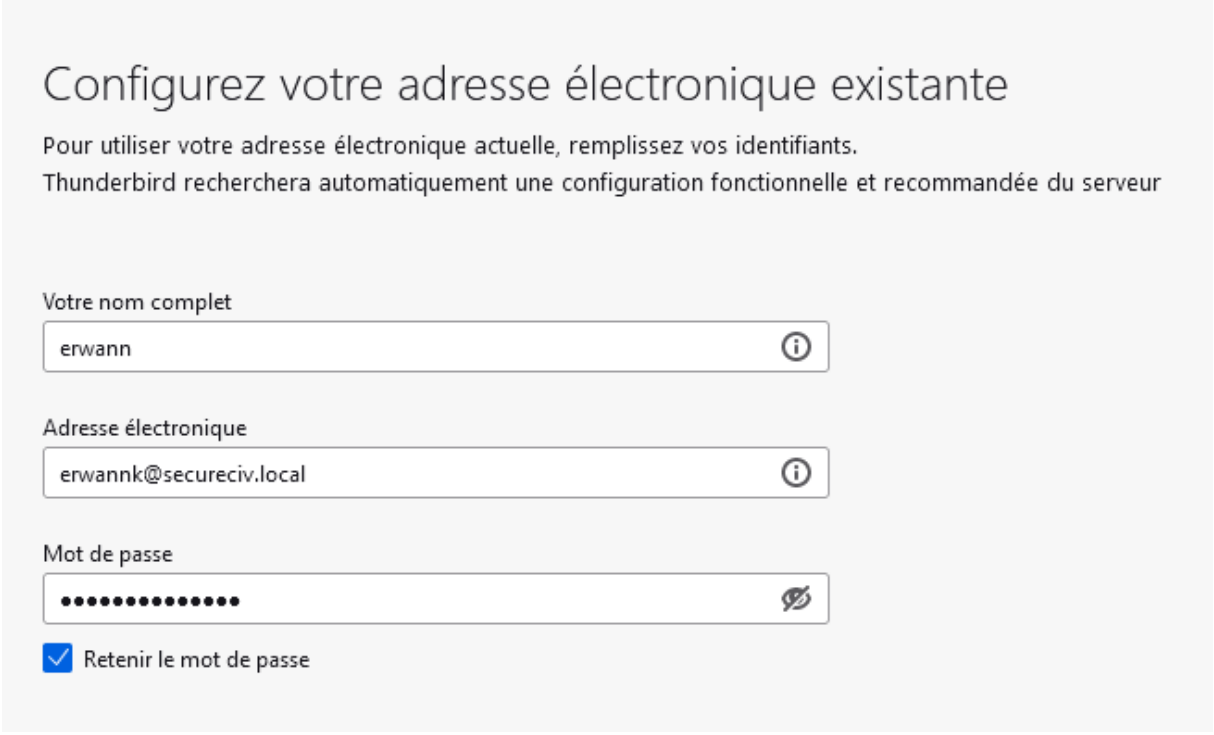
Et redémarrez le service hmail



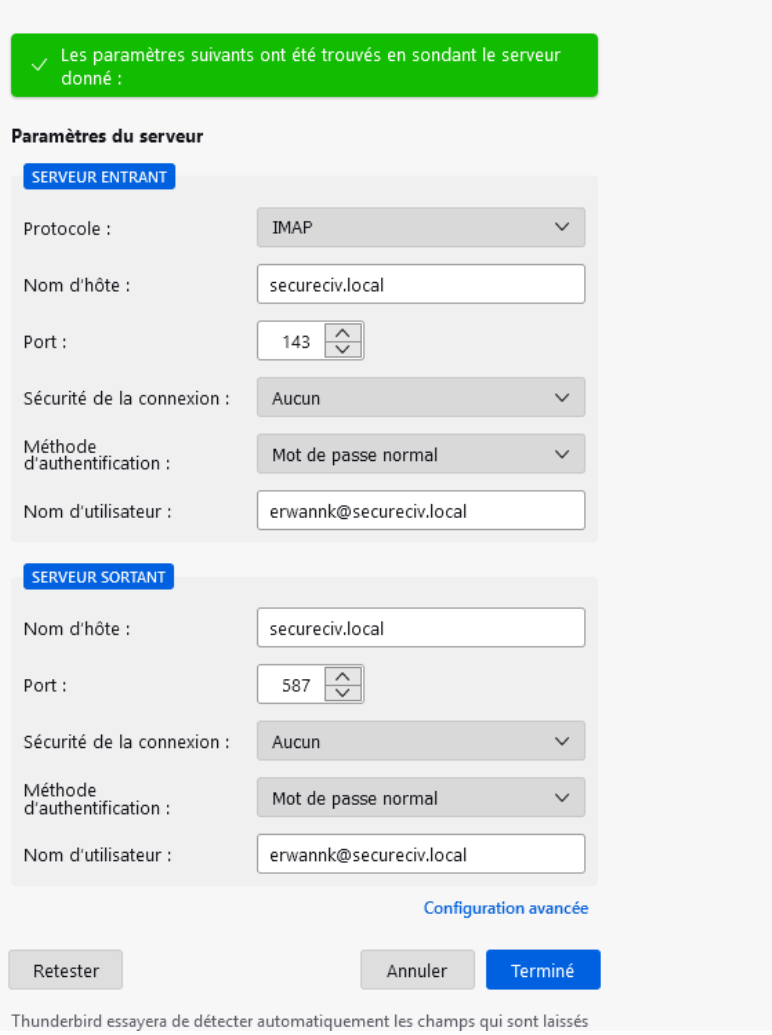
4.5) Connexion au client de messagerie:

Ici nous utiliserons Thunderbird, vous pouvez le trouvez au lien suivant :
https://www.thunderbird.net/fr/

Faites une installation standard et après l'installation de Thunderbird, entrer le nom de la personne et l'adresse mail qui est crée dans l'AD au moment de la création de l'utilisateur ainsi que le mot de passe de l'utilisateur

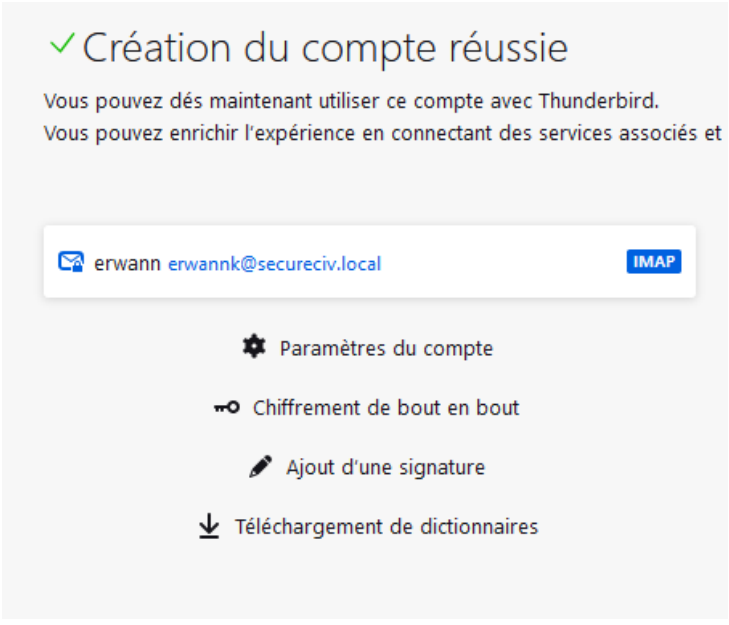


Faites ensuite configuration manuelle,
Vérifier que votre nom de domaine est bien dans la partie « nom d'hote » dans serveur entrant et sortant puis faites tester

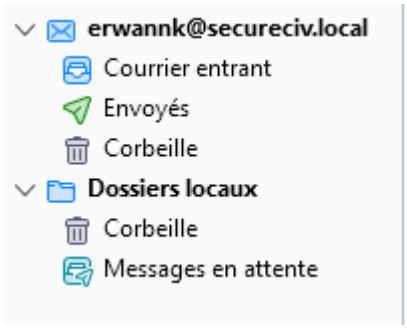


Faites ensuite terminer

Et vous serez connecté au compte

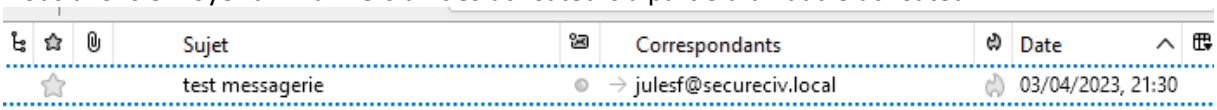


Nous pouvons en effet voir que notre comptes à été crée dans la boite mail Thunderbirth

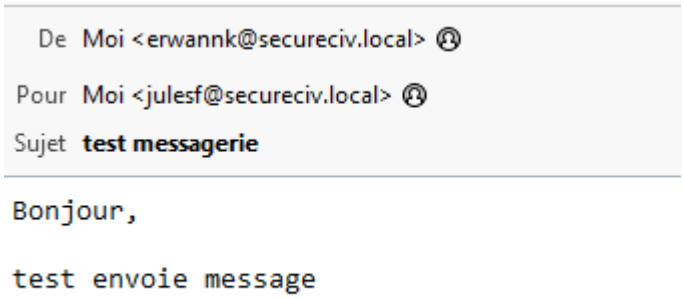


Après l'ajout de deux comptes, nous allons essayer l'envoi et la réception de mail

Nous allons envoyer un mail vers un des utilisateurs a partie d'un autre utilisateur.



Nous pouvons voir après avoir envoyer le mail que celui-ci à correctement été réceptionné



5) Serveur Voip

5.1) Installation et configuration

On installe un ubuntu server 22.04
On lance la commande pour mettre à jour le système :

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

Puis on fait la configuration réseau en modifiant le fichier 00-installer-config.yaml comme ci-dessous avec la commande

```
Sudo nano /etc/netplan
```

```
  GNU nano 6.2                                  00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      addresses:
      - 192.168.20.4/24
      routes:
          - to : default
            via: 192.168.20.254

      nameservers:
        addresses:
        - 192.168.20.5
        - 192.168.20.6
        search:
         - serviceciv.local
  version: 2
```

5.2) Installation d' asterisk:

On installe asterisk via cette commande

```
Sudo install -y asterisk asterisk-core-sounds-fr asterisk-mp3 asterisk-mysql
```

On fais ensuite une commande qui va permettre à asterisk de démarrer à l'allumage de la VM

```
Systemctl enable asterisk
```

5.3) Configuration d'asterisk

Pour la configuration de asterisk on va se rendre dans le fichier sip.conf
Dans un premier temps on ajoute ces lignes dans le fichiers
Elles vont permettre de configuré le protocole utilisé

```
[general]
context=default
allowguest=no
udpinaddr=8.8.8.8
tcpenable=no
transport=udp
```

ensuite sur la ligne 354 on active la ligne en supprimant le point-virgule, on désactive donc tous les codecs, et on active le codec ulaw
(les codec sont des protocoles qui permettent de transformer les enregistrement vocaux en paquet)

```
                                ; limits the other side's codec choice to exactly what we prefer.

disallow=all                    ; First disallow all codecs
allow=ulaw                      ; Allow codecs in order of preference
;allow=ilbc                     ; see https://wiki.asterisk.org/wiki/display/AST/RTP+Packetization
                                ; for framing options
;autoframing=yes                ; Set packetization based on the remote endpoint's (ptime)
                                ; preferences. Defaults to no.
;
; This option specifies a preference for which music on hold class this channel
; should listen to when put on hold if the music class has not been set on the
; channel with Set(CHANNEL(musicclass)=whatever) in the dialplan, and the peer
; channel putting this one on hold did not suggest a music class.
```

5.4) Configuration Users asterisk :

Nous allons créer les utilisateurs sur le fichier users.conf

```
cd /etc/asterisk
nano users.conf
```

```
[1101]
fullname = Jules
username = u1101
host= dynamic
secret =
mailbox = 1101
context = admin
callerid = 1101

[1102]
fullname = erwann
username = u1102
secret =
host = dynamic
mailbox = 1102
context = admin
callerid = 1102
```

[numéro] fait office du numéro du poste à appeler
Fullname= nom de l'utilisateur
Username= nom d'utilisateur dans asterisk
Mailbox = le numéro associer à la boite mail
Secret= le mot de passe de connexion
Host=dynamic l'utilisateur n'est pas associé à une IP fixe
Context= admin l'utilisateur appartient au contexte admin
Callerid=associe le nom au numéro fait ici le nom associé au numéro
On peut alors sauvegarder le fichier

5.5) Création boite vocale :

Pour configurer la boîte vocale c'est le fichier voicemail.conf qu'il faut modifier

```
cd /etc/asterisk
nano voicemail.conf
```

on ajoute les utilisateurs avec les lignes suivantes:

```
[admin]
1101 => ,Jules


[dev]
1102 => ,erwann
```

sauvegarder le fichier une fois la modification faites
On peut également mettre le mot de passe avant la virgule ainsi l'utilisateur devra mettre un mot de passe pour consulter sa messagerie vocale

création du DialPan
On va maintenant modifier le fichier extensions.conf pour mettre en place la boîte vocal

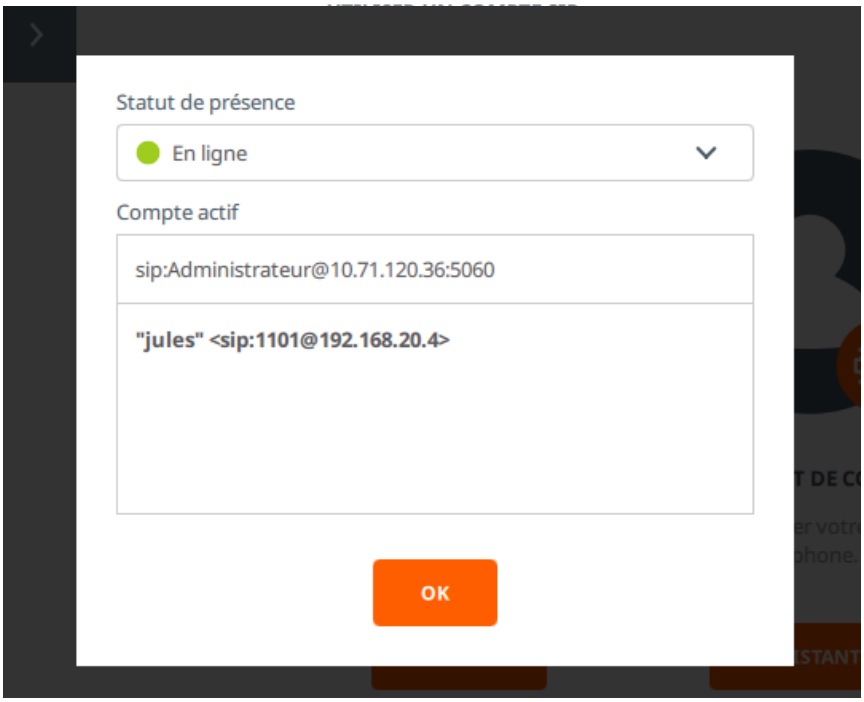
```
cd /etc/asterisk
nano extensions.conf
```

```
[admin]

exten => _110X,1,Dial(SIP/${EXTEN},20)
exten => _110X,2,VoiceMail(${EXTEN}@admin)

exten => 888,1,VoiceMailMain(${CALLERID(num)}@admin)
```

La première ligne dit qu'on appelle un poste commençant par 110 suivis du X numéro du poste, ensuite on prend l'appel et ça sonne pendant 20 secondes.
La deuxième ligne permet de renvoyer sur la boite vocale
la troisième ligne est le numéro 888, pour accéder à sa boîte vocal

Utilisation de la VOIP avec un softphone :
Pour réaliser les tests nous allons avoir besoin de client Windows et d'un softphone, nous allons utiliser linphone qui est open-source Sur Windows installer linphone puis lancer le Sur la page d'accueil linphone cliquer sur utiliser un compte SIP

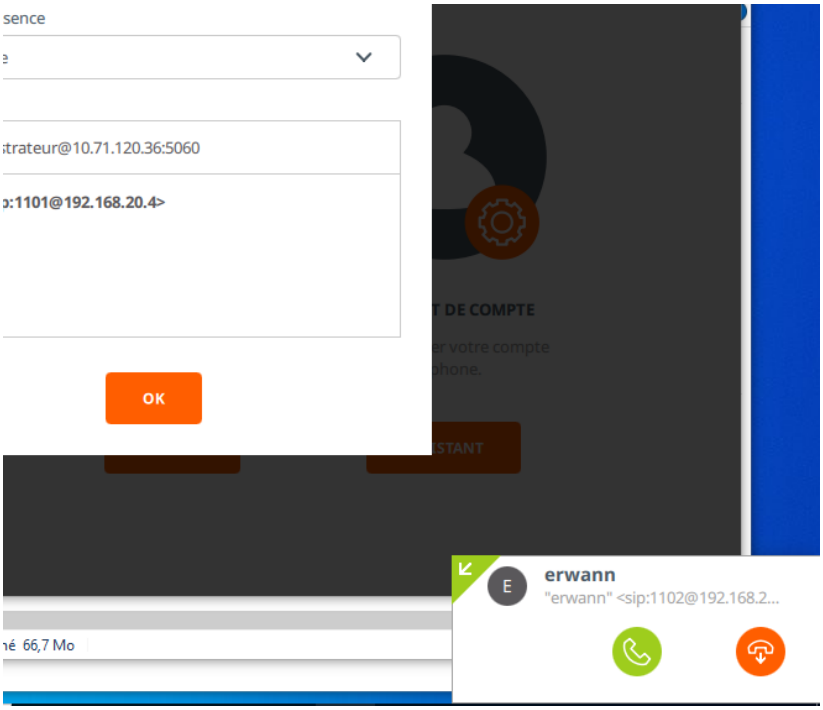
Renseignez ensuite comme ceci
Nom d'utilisateur = le numéro du poste
Nom d'affichage = nom de l'utilisateur
Domaine SIP = adresse IP de notre serveur asterisk
Le mot de passe de l'utilisateur SIP
Puis cliquez sur utiliser

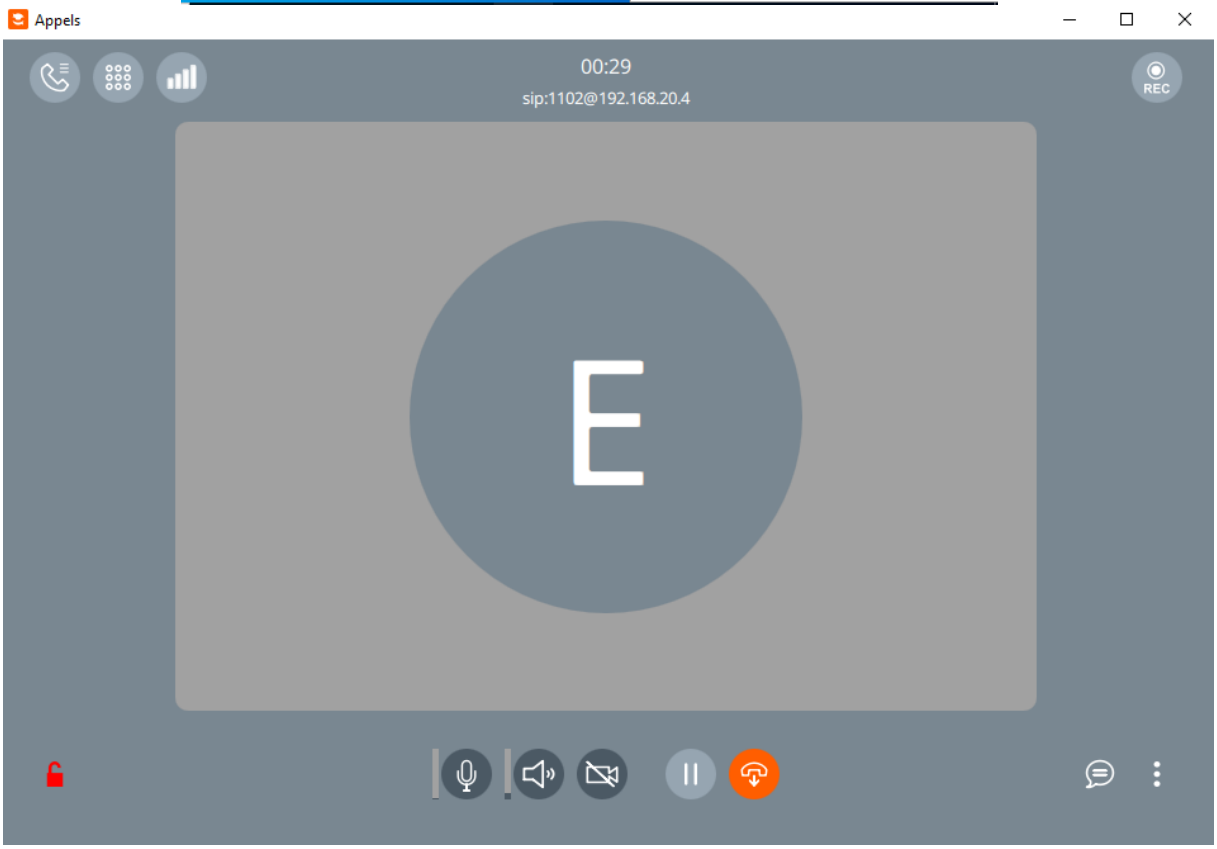


On peut voir que notre compte à bien été ajouté

```
================================================================================
Connected to Asterisk 18.10.0~dfsg+~cs6.10.40431411-2 currently running on srv-voip (pid = 822)
    -- Registered SIP '1102' at 192.168.20.35:5060
       > Saved useragent "Linphone-Desktop/5.0.15 (DESKTOP-Q6OQFSF) windows/10 Qt/5.15.2 LinphoneSDK
/5.2.50" for peer 1102
```

Nous avons maintenant installé linphone sur deux pc du domaine et nous allons tester un appel entre le user 1101 et 1102
Nous pouvons voir que l'appel se déclenche bien et que celui-ci fonctionne





6) ERP et DMZ

6.1) Installation et configuration de eBrigade

On installe un serveur Ubuntu 22.04 et on met à jour le système :

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

On installe les paquets nécessaires :

```
Sudo apt install php mysql-server apache2
```

On supprime le contenu du dossier var/www/html, et on y copie le site eBrigade :

```
Sudo rm -r /var/www/html/
Sudo mv /mnt/hgfs/share/ebrigade /mnt/hgfs/share/html
Sudo cp -r /mnt/hgfs/share/html /var/www/html
```

A present on met l'interface reseau de la VM sur le bon réseau (VMnet2 : celui de la DMZ) et on modifie la configuration réseau en éditant modifiant le fichier 00-installer-config.yaml comme ci-dessous avec la commande

```
Sudo nano /etc/network/netplan
```

```
  GNU nano 6.2                          00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      addresses:
      - 192.168.20.3/24
      gateway4: 192.168.20.254
      nameservers:
        addresses:
        - 192.168.20.5
        - 192.168.20.6
        search:
        - prefecture-cod.fr
  version: 2
```

Attention il faut mettre la bonne adresse : 192.168.30.1/24 et la bonne passerelle : 192.168.30.254.
Ensuite :

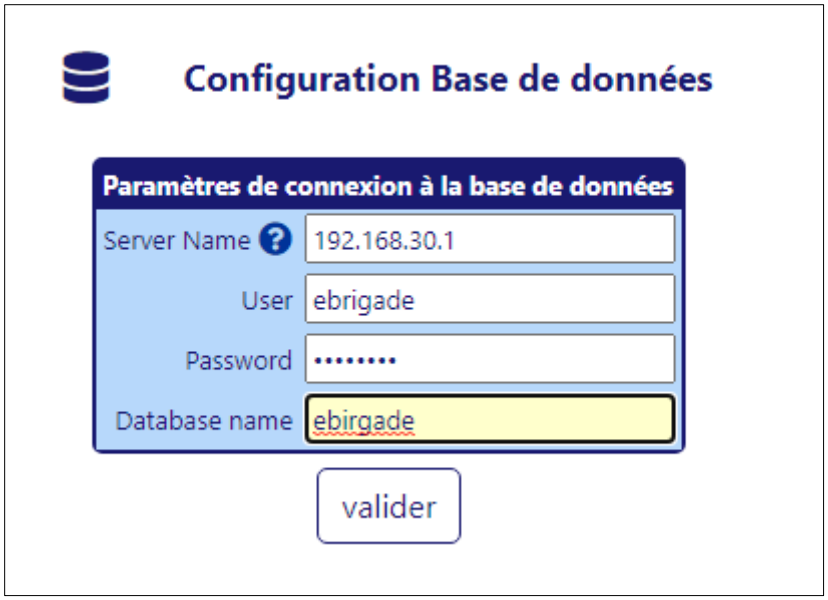
```
Netplan apply
```

6.2) Création de la base de données

On tape les commandes suivantes :

```
Mysql
```

```
mysql> CREATE DATABASE `ebrigade` DEFAULT CHARACTER SET latin1 COLLATE latin1_general_cs;
Query OK, 1 row affected (0,00 sec)

mysql> CREATE USER 'ebrigade'@'localhost' IDENTIFIED BY 'ebrigade';
Query OK, 0 rows affected (0,03 sec)

mysql> GRANT ALL PRIVILEGES ON *.* TO 'ebrigade'@'localhost';
Query OK, 0 rows affected (0,04 sec)

mysql> FLUSH PRIVILEGES
    -> ^C
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,01 sec)
```



6.3) Configuration de la DMZ

La DMZ est configuré avec les règles de pare-feu suivantes :

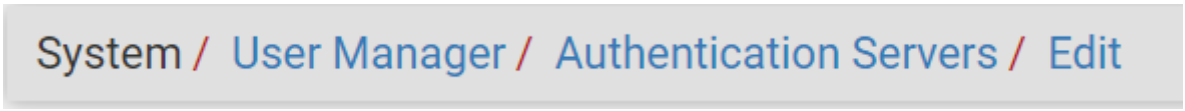
- Rediriger le flux WAN vers la DMZ
- Bloquer le flux DMZ vers LAN
- Autoriser le LAN a accéder au serveur ERP qui est sur la DMZ
-

Voir les règles de pare-feu dans la partie 5.1.6

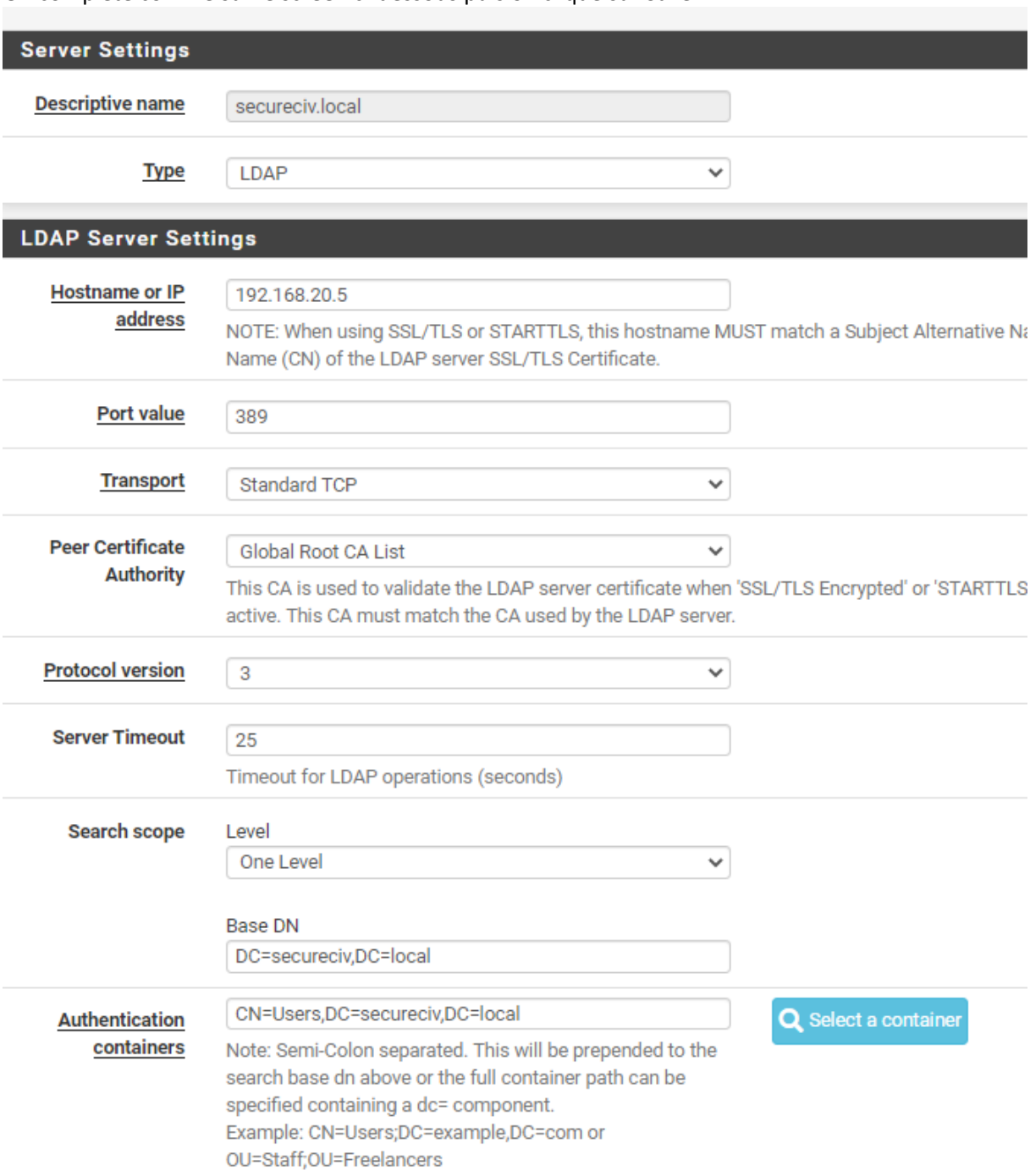
7) Mise en place VPN

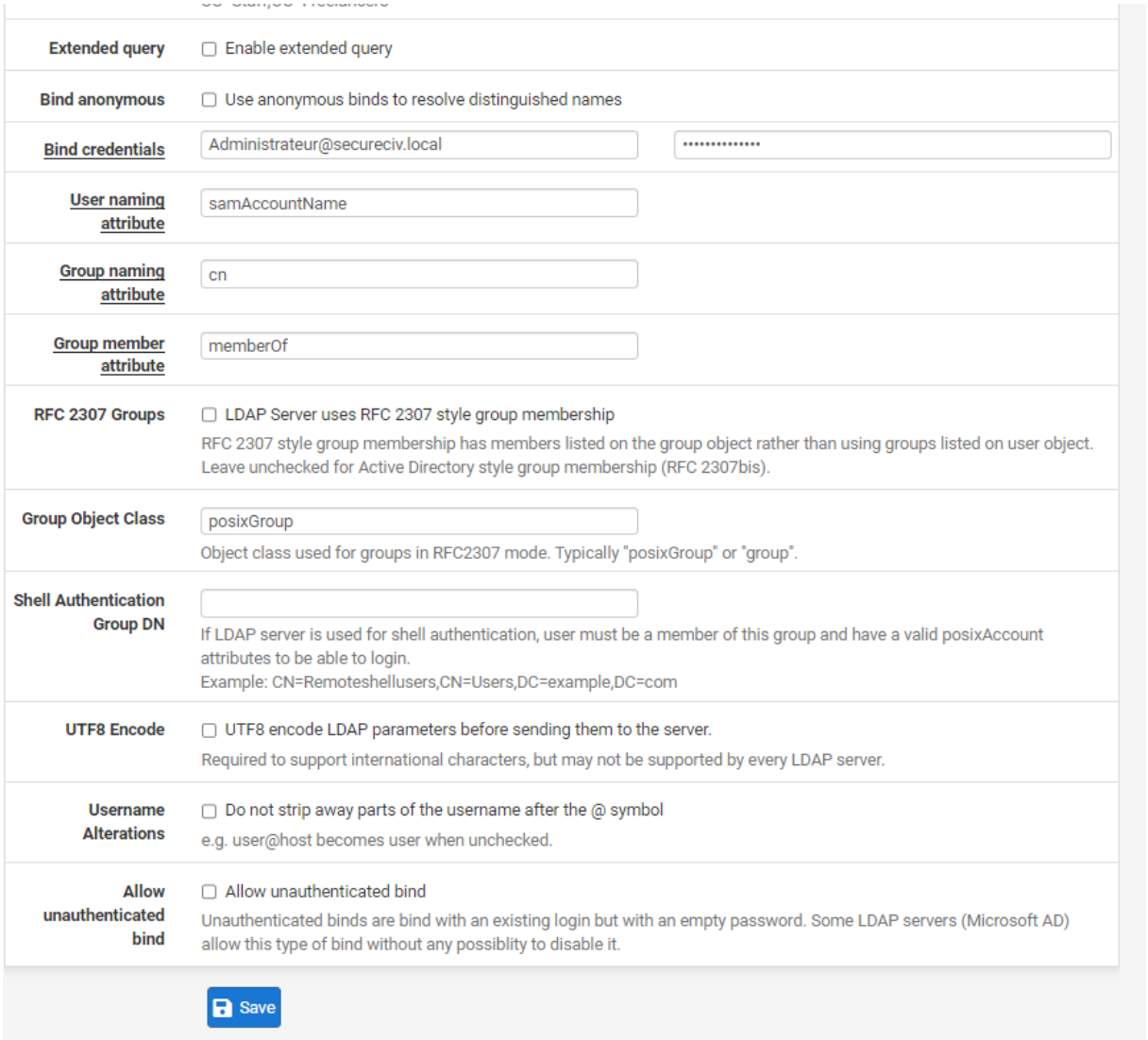
7.1) Liaison pfsense/LDAP :

On se rend sur le pare feu dans system/User manager /authentification Servers/

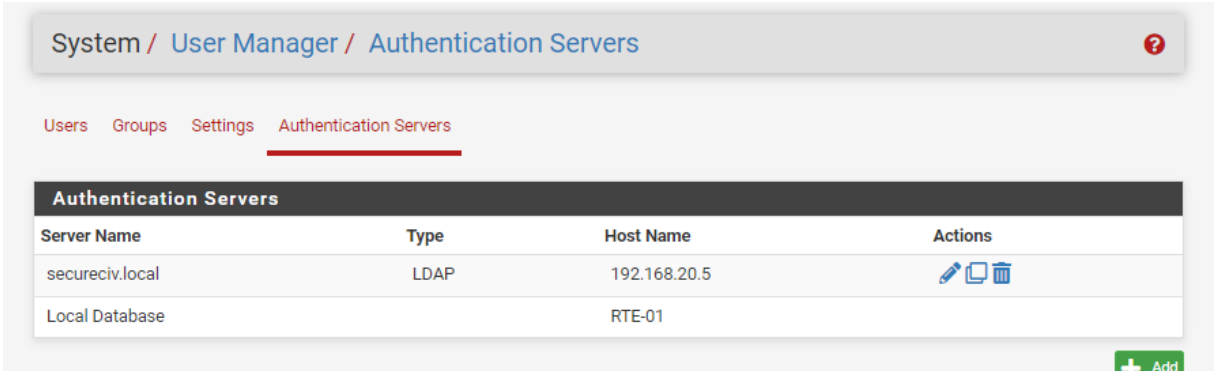


Puis on clique sur ADD
On complète comme sur le screen ci-dessous puis on clique sur Save :



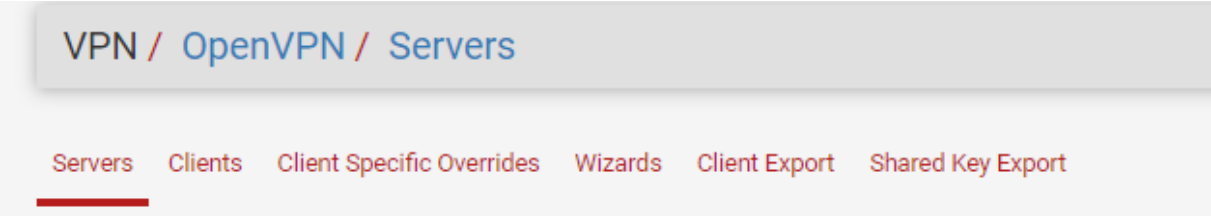


Nous avons maintenant bien lié notre pfsense au LDAP

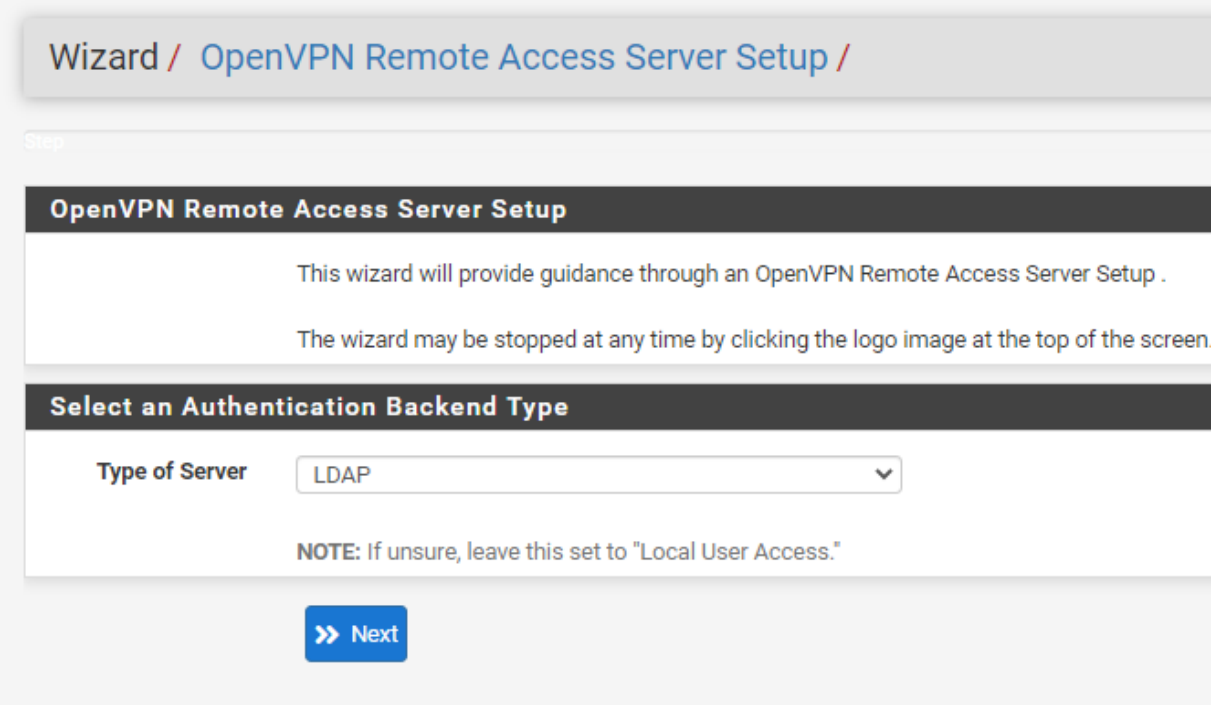


7.2) Mise en place du VPN :

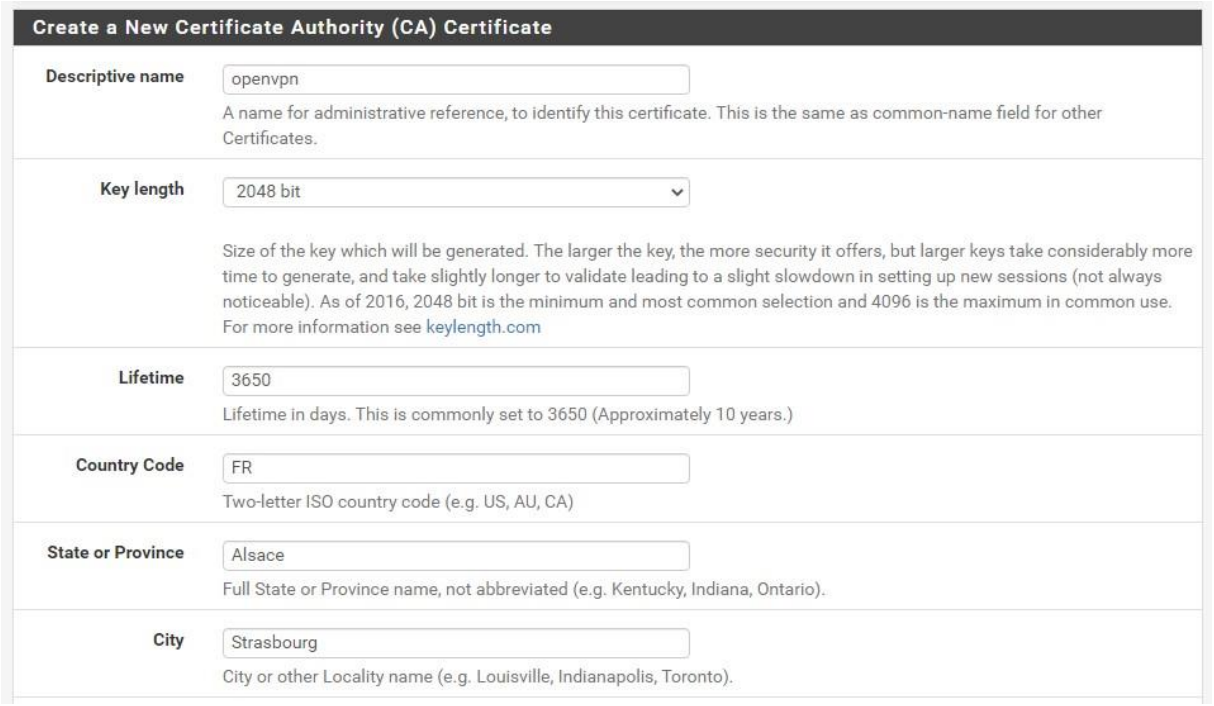
Rendez dans VPN/OpenVPN
Puis allez dans l'onglet « wizards »



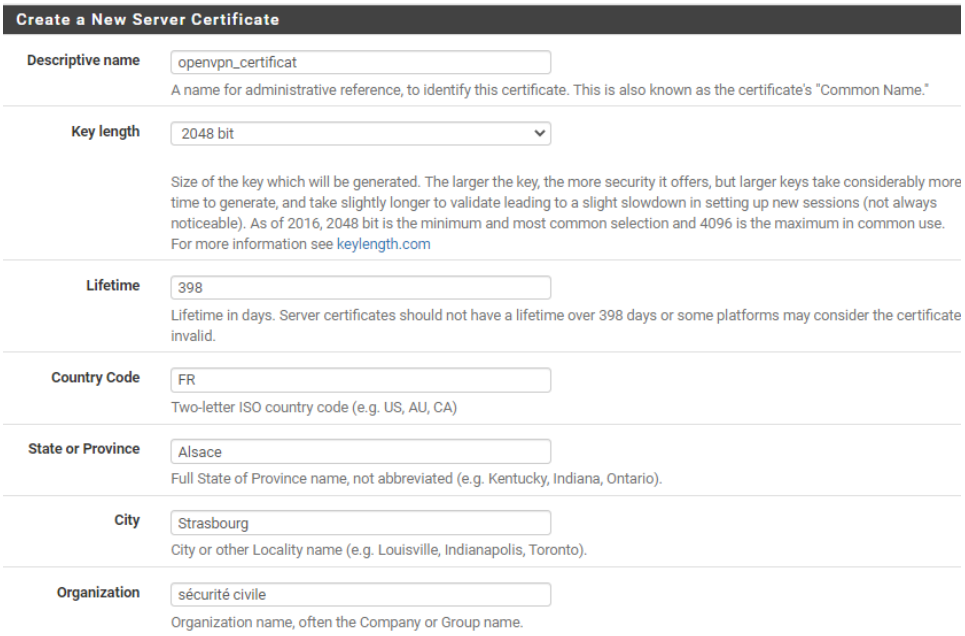
Choisissez « LDAP » dans le type de server :
Sélectionnez le serveur que nous avons au préalablement lié



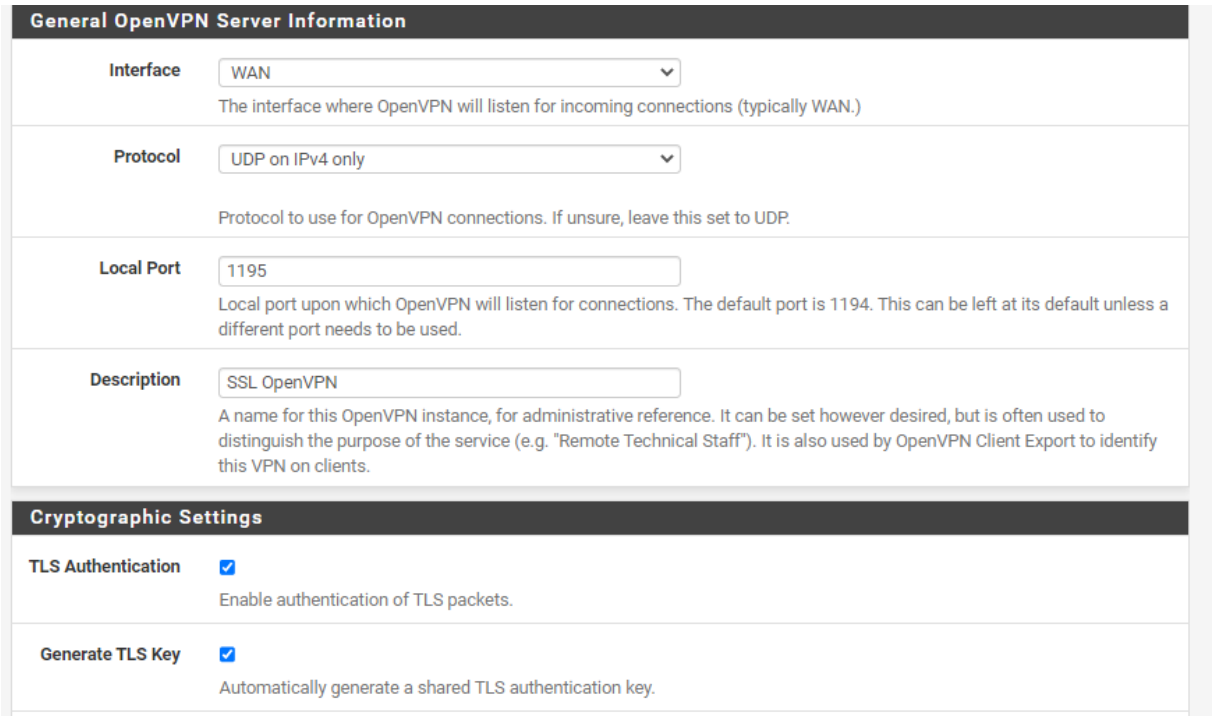
Ensuite complété le Certificat d'autorité comme ci-dessous



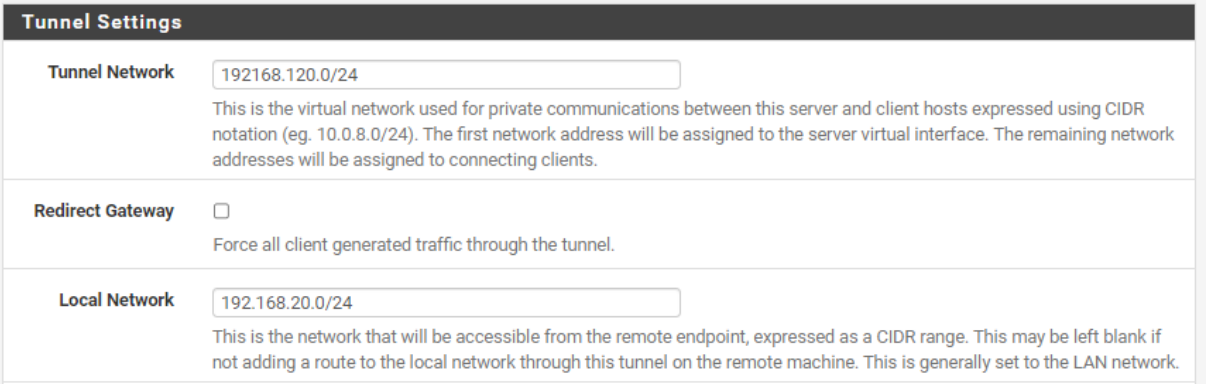
Pareil pour le certificat serveur



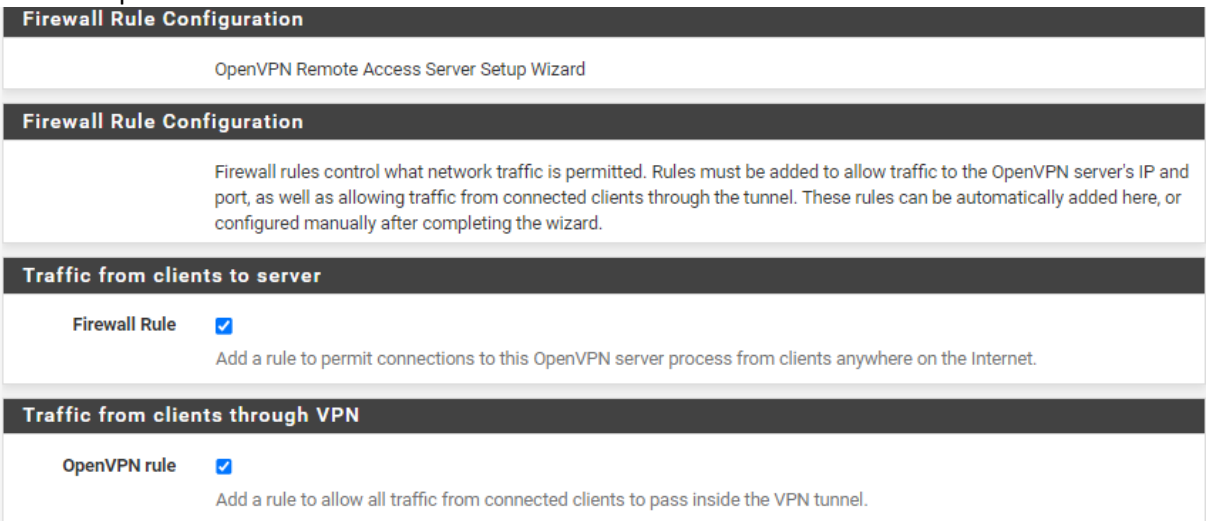
Pour continuer on configure les paramètres généraux de cette manière :



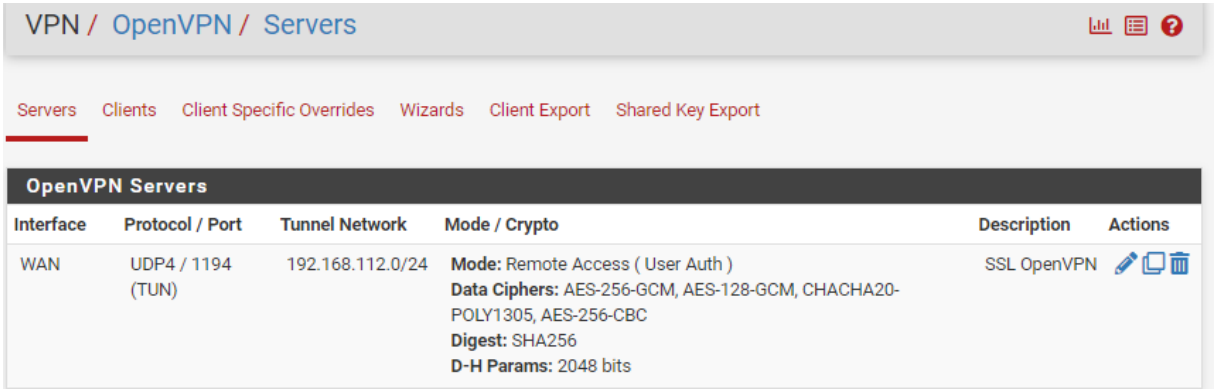
On complète les paramètres pour le tunnel vpn et la liaison à distance, ici on a choisi 192.168.120.0 :



On oublie pas de cocher les deux case ci-dessous

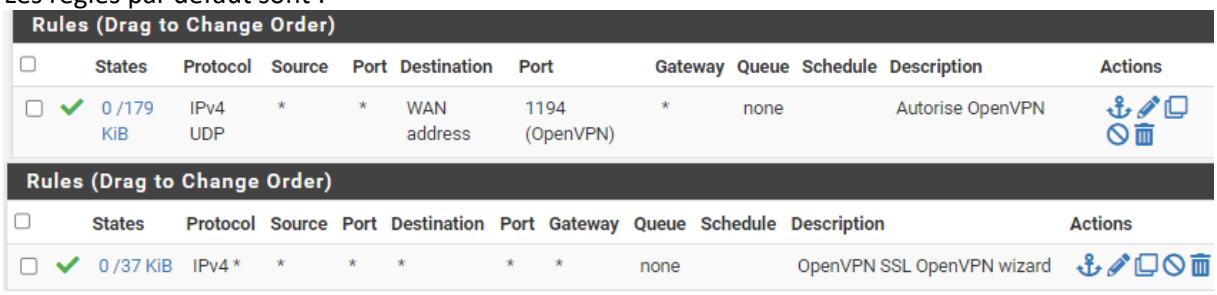


Notre serveur OpenVPN à bien été crée :



7.3) Règle de pare-feu pour openVPN :

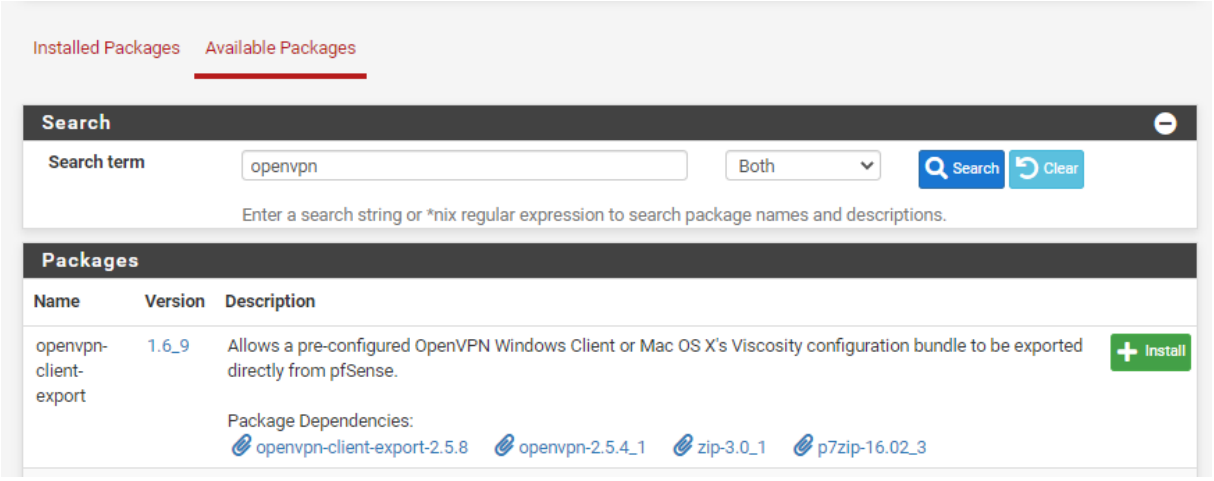
Les règles par défaut sont :



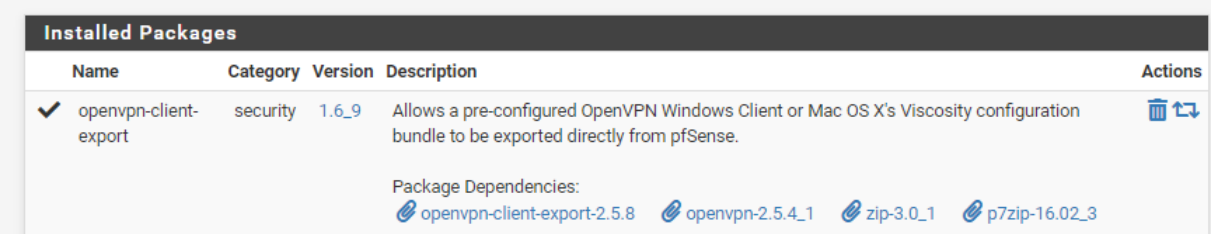
7.4) Installation du paquet OpenVPN

Nous allons allez dans System/Packet manager

Puis dans avalable Packages cherchez OpenVPN et installez le



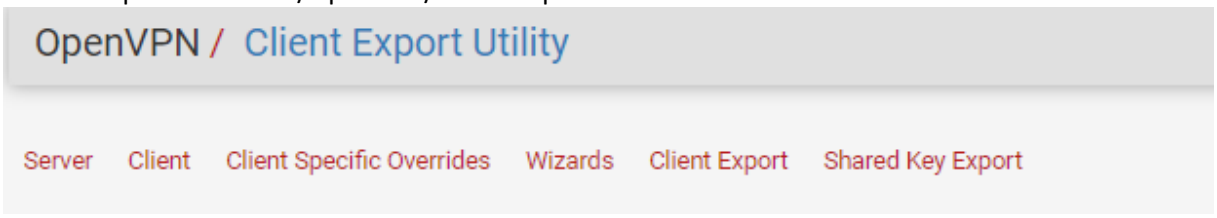
votre package à bien été installé nous allons pouvoir faire les test de connexion distante



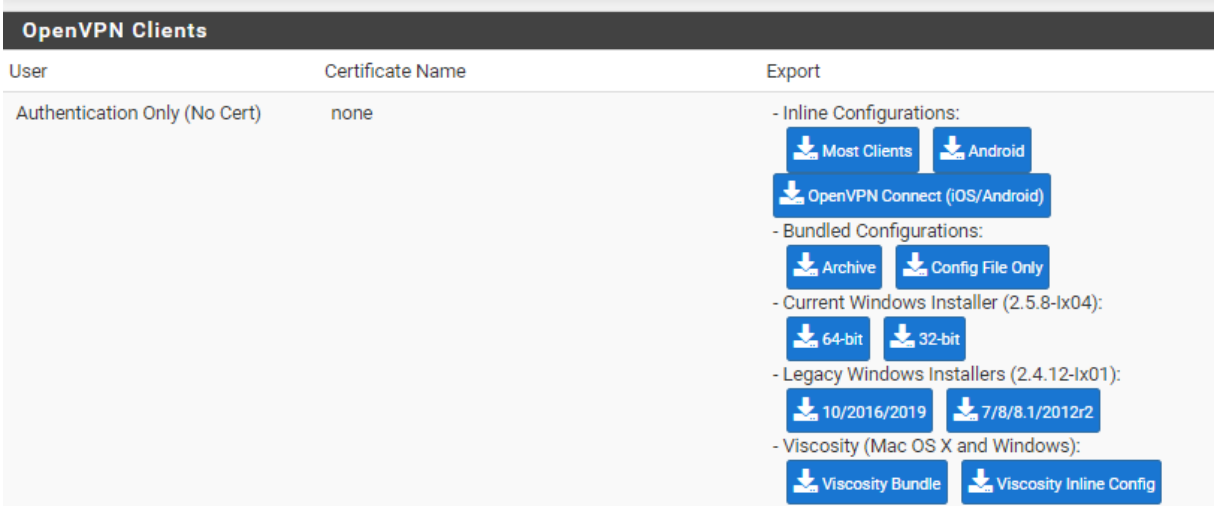
7.5) Connexion VPN à distance :

Nous allons installer OpenVPN sur une machine Windows qui ne se trouve pas dans le même réseau que notre Infra :
Vous pouvez trouver le packet d'installation à cette adresse :
https://openvpn.net/community-downloads/

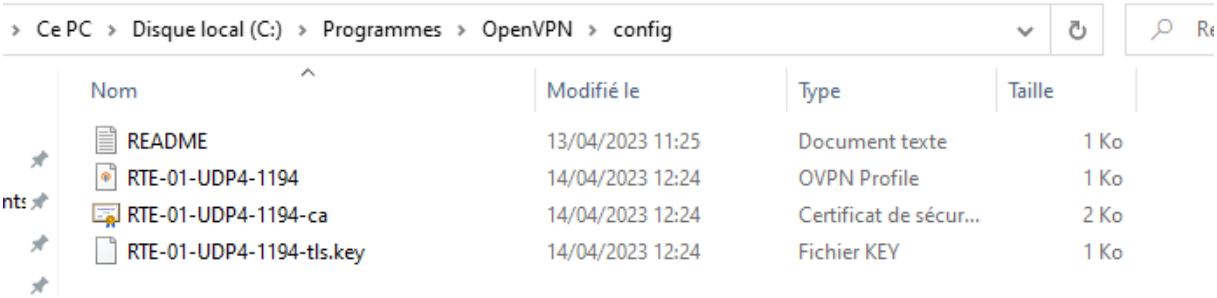
une fois installé, récupérer le fichier donné par pfsense
on le récupère dans VPN/OpenVPN/ client export



Puis on récupère le fichier archive

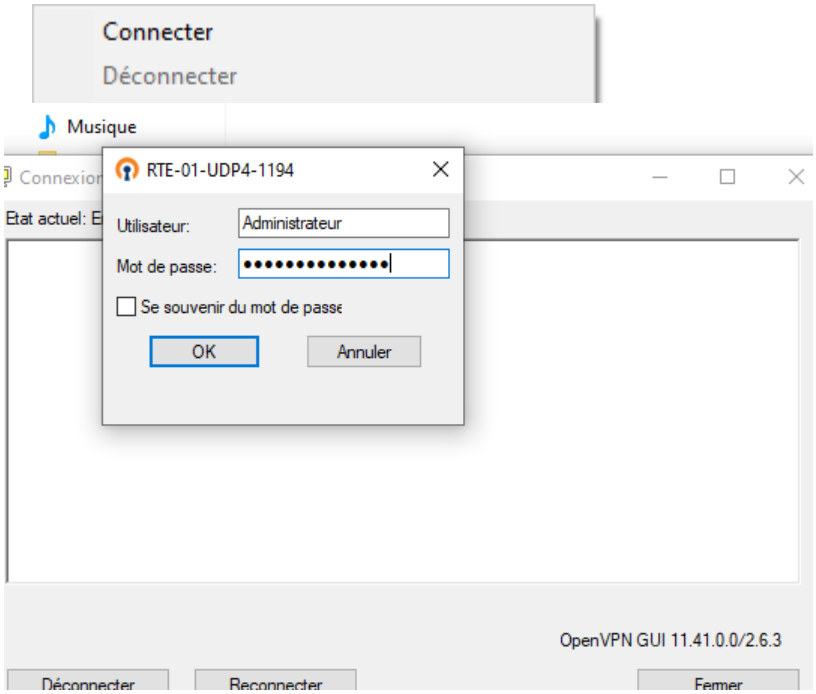


On extrait le fichier et on met les fichier contenu dans le dossier config de OpenVPN qui se trouve dans Programme/OpenVPN/ Config



Puis dans les icones en bas à droit

Cliquez sur connecter



Ensuite entrez le mot de passe et le login de votre compte AD

Nous pouvons maintenant voir que la connexion est bien faites le logo est passé au vert