



SÉCURITÉ CIVILE

Documentation technique

Date : 15/04/2023

SOMMAIRE

1) Routeurs – firewalls	4
1.1) Configuration système et réseau	4
1.2) Redondance des routeurs	4
1.3) Adresse IP virtuelle LAN	6
1.4) Adresse IP virtuelle DMZ	6
1.5) Règles de pares-feux	7
2) Serveurs Windows	8
2.1) Installation et configuration de SRV-AD01.....	8
2.2) Création de l'AD	8
2.3) Installation et configuration de SRV-AD02.....	9
2.4) Ajout de SRV-AD02 en contrôleur de domaine.....	9
2.5) Configuration du DHCP	9
2.6) Ajout des utilisateurs dans l'AD	10
3) Serveur de supervision	10
3.1) Installation et configuration système réseau.....	10
3.2) Installer checkmk	10
3.3) Configuration de checkmk	11
3.4) Installation de l'agent.....	11
3.5) Ajout de l'hôte.....	11
3.5) Ajouter les pares-feux via SNMP	12
4) Serveur de messagerie	13
4.1) Installation Hmail :	13
4.2) Configuration DNS pour le serveur de messagerie :	17
4.3) Configuration Hmailserver	18
4.4) Configuration SMTP :	21
4.5) Connexion au client de messagerie:.....	24
5) Serveur Voip	27
5.1) Installation et configuration.....	27
5.2) Installation d' asterisk:	27
5.3) Configuration d'asterisk	27
5.4) Configuration Users asterisk :	28
5.5) Crédit boîte vocale :	28

6) ERP et DMZ.....	32
6.1) Installation et configuration de eBrigade.....	32
6.2) Création de la base de données	32
6.3) Configuration de la DMZ	33
7) Mise en place VPN	34
7.1) Liaison pfsense/LDAP :	34
7.2) Mise en place du VPN :	36
7.3) Règle de pare-feu pour openVPN :	39
7.4) Installation du paquet OpenVPN.....	39
7.5) Connexion VPN à distance :	40

1) Routeurs – firewalls

1.1) Configuration système et réseau

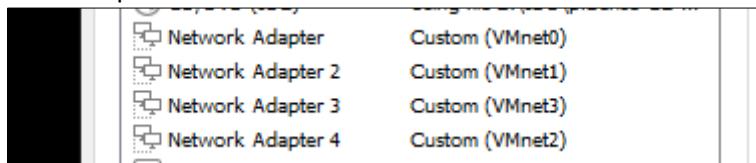
Une fois l'installation fini, on configure les adresses IP comme ci-dessous :

```
*** 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 2^e 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 :

State Synchronization Settings (pfsync)

Synchronize states pfsync transfers state insertion, update, and deletion messages between firewalls.
 Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
 This setting should be enabled on all members of a failover group.
 Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface CARP

If Synchronize States is enabled this interface will be used for communication.
 It is recommended to set this to an interface other than LAN1 A dedicated interface works the best.
 An IP must be defined on each machine participating in this failover group.
 An IP must be assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP 192.168.40.2
 Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP 192.168.40.2
 Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
 XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
 Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username admin
 Enter the webConfigurator username of the system entered above for synchronizing the configuration.
 Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password Confirm
 Enter the webConfigurator password of the system entered above for synchronizing the configuration.
 Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize admin synchronize admin accounts and autoupdate sync password.
 By default, the admin account does not synchronize, and each node may have a different admin password.
 This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

On coche tout pour faire une synchro complète :

Select options to sync

- User manager users and groups
- Authentication servers (e.g. LDAP, RADIUS)
- Certificate Authorities, Certificates, and Certificate Revocation Lists
- Firewall rules
- Firewall schedules
- Firewall aliases
- NAT configuration
- IPsec configuration
- OpenVPN configuration (Implies CA/Cert/CRL Sync)
- DHCP Server settings
- DHCP Relay settings
- DHCPv6 Relay settings
- WoL Server settings
- Static Route configuration
- Virtual IPs
- Traffic Shaper configuration
- Traffic Shaper Limiters configuration
- DNS Forwarder and DNS Resolver configurations
- Captive Portal

Toggle All

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

State Synchronization Settings (pfsync)

Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize Interface	CARP If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.
pfsync Synchronize Peer IP	192.168.40.2 Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

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 modifiées seulement sur le routeur maître.

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 :

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	LAN			
Address type	Single address			
Address(es)	192.168.20.254	/	24	<input type="button"/>
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP Password	*****	*****	Confirm	
VHID Group	1	Enter the VHID group that the machines will share.		
Advertising frequency	1	0	<input type="button"/>	
Base Skew				
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.				
Description	IP Virtuelle LAN <input type="button"/>			
A description may be entered here for administrative reference (not parsed).				

 Save

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 pare-feux

Interface WAN :

Floating	WAN	LAN	CARP	DMZ							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Autorise OpenVPN	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	WAN net	*	DMZ net	*	*	none		Redirection WAN vers DMZ	
<input type="checkbox"/>	✗ 0 / 234 B	IPv4+6 *	*	*	*	*	*	none		Bloque tout le reste	

Add Add Delete Save

Interface LAN :

Floating	WAN	LAN	CARP	DMZ							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0 / 1.51 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 2 / 7.19 MiB	IPv4 TCP/UDP	LAN net	*	*	web_access	*	none		autoriser le traffic web	
<input type="checkbox"/>	✓ 0 / 2.31 MiB	IPv4 TCP/UDP	LAN net	*	*	161 (SNMP)	*	none		autorise snmp dans le lan	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 UDP	LAN net	5060 (SIP)	*	*	*	none		Autorise le SIP pour les appels VOIP	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	192.168.20.3	*	*	6556	*	none		autorise l'agent checkmk	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LAN net	*	192.168.30.1	*	*	none		autorise le lan vers ERP	
<input type="checkbox"/>	✓ 0 / 3 KiB	IPv4 ICMP any	LAN net	*	*	*	*	none		Autorise ping dans le LAN	
<input type="checkbox"/>	✗ 0 / 93 KiB	IPv4+6 *	*	*	*	*	*	none		bloque tout les autres flux	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save

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

Interface CARP :

Floating	WAN	LAN	CARP	DMZ							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 *	192.168.40.1	*	192.168.40.2	*	*	none		autorise synchro entre les routeurs	
<input type="checkbox"/>	✗ 0 / 0 B	IPv4+6 *	*	*	*	*	*	none		Bloque tous les autres flux	

Add Add Delete Save

Interface DMZ :

Floating	WAN	LAN	CARP	DMZ							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0 / 45 KiB	IPv4+6 *	DMZ net	*	LAN net	*	*	none		Bloque DMZ vers LAN	

Add Add Delete Save

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

2.5) Configuration du DHCP

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:
        - préfecture-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'hôte)

On crée un site CheckMK que l'on appelle « préfecture-cod » :

```
omd create préfecture_cod
omd start préfecture_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.

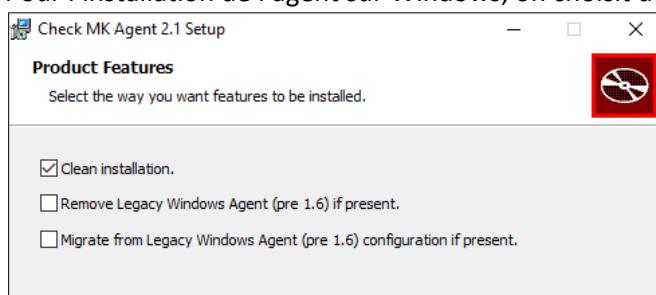
3.4) Installation de l'agent

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 :

Hostname (required) srv-sup

IP address family IPv4 only (Default value)

IPv4 address 192.168.20.3

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

1 change

On clique sur Activate on selected sites

Action	Site	Status	Version	Changes	Progress	Details
x	Local site prefecture_cod	online	2.1.0p25	1		Has never been activated

Pending changes (1)

Time	User	Change	Affected sites
2023-03-31 12:07:27	cmkadmin	Created new host srv-sup.	All sites

Maintenant on clique sur l'hôte, 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 :

The screenshot shows the 'Services of host srv-sup' page in CheckMK. At the top, there are tabs for Actions, Host, Settings, Display, Help, and a status bar indicating 'No pending changes'. Below the tabs, there are buttons for Accept all, Rescan, Monitor undecided services, Remove vanished services, and Properties of host srv-sup. A 'Status' dropdown menu is open, showing 'New' and three filters: cmk/check_mk_server=yes, cmk/device_type=vm, and cmk/os_family=linux. The main area displays a table titled 'Undecided services - currently not monitored (22)'. The table has two columns: 'State' and 'Service'. The 'State' column uses color-coded icons: yellow for WARN, green for OK, and red for CRIT. The 'Service' column lists various system components like 'Check_MK Agent', 'CPU load', 'CPU utilization', etc. Each service entry includes a brief status summary. At the bottom right of the table, it says 'Up since Mar 31 2023 09:10:06, Uptime: 3 hours 9 minutes'.

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 pare-feux via SNMP

On active le service SNMP :

The screenshot shows the 'Services / SNMP' page in pfSense. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'SNMP Daemon'. It contains a single configuration item: 'Enable' with a checkbox followed by the text 'Enable the SNMP Daemon and its controls'. Below this is a link labeled 'SNMP Daemon Settings'.

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

The screenshot shows the 'Basic settings' and 'Network address' sections of the 'Host properties' page in CheckMK. In the 'Basic settings' section, the 'Hostname' is set to 'rte-01'. In the 'Network address' section, the 'IP address family' is set to 'IPv4 only' (Default value), and the 'IPv4 address' is '192.168.20.252'. Below these, under 'Monitoring agents', there are fields for 'Checkmk agent / API integrations', 'SNMP', and 'SNMP credentials'. The 'Checkmk agent / API integrations' dropdown is set to 'No API integrations, no Checkmk agent'. The 'SNMP' dropdown is set to 'SNMP v2 or v3'. The 'SNMP credentials' dropdown is set to 'SNMP community (SNMP Versions 1 and 2c)' with a password field containing '*****'.

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 bêta)

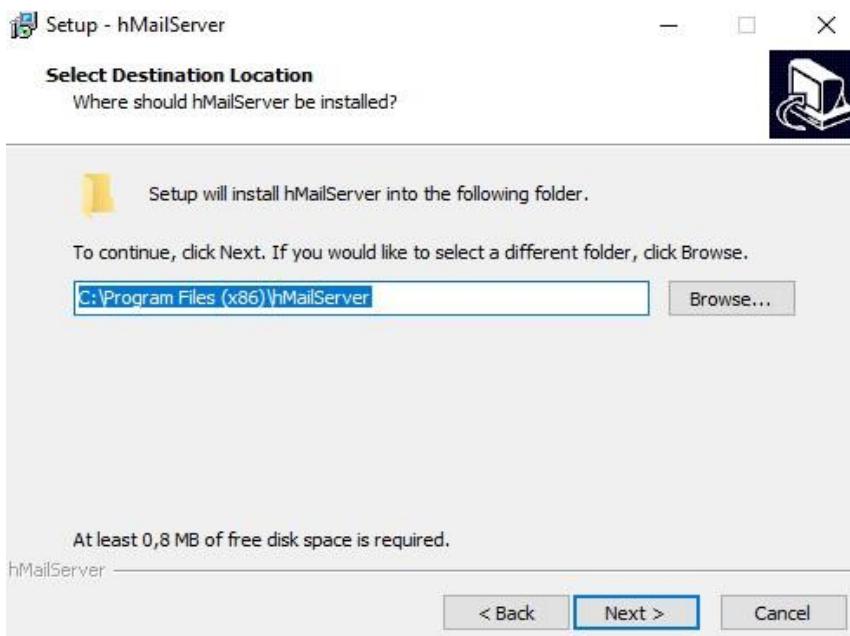
Faites next



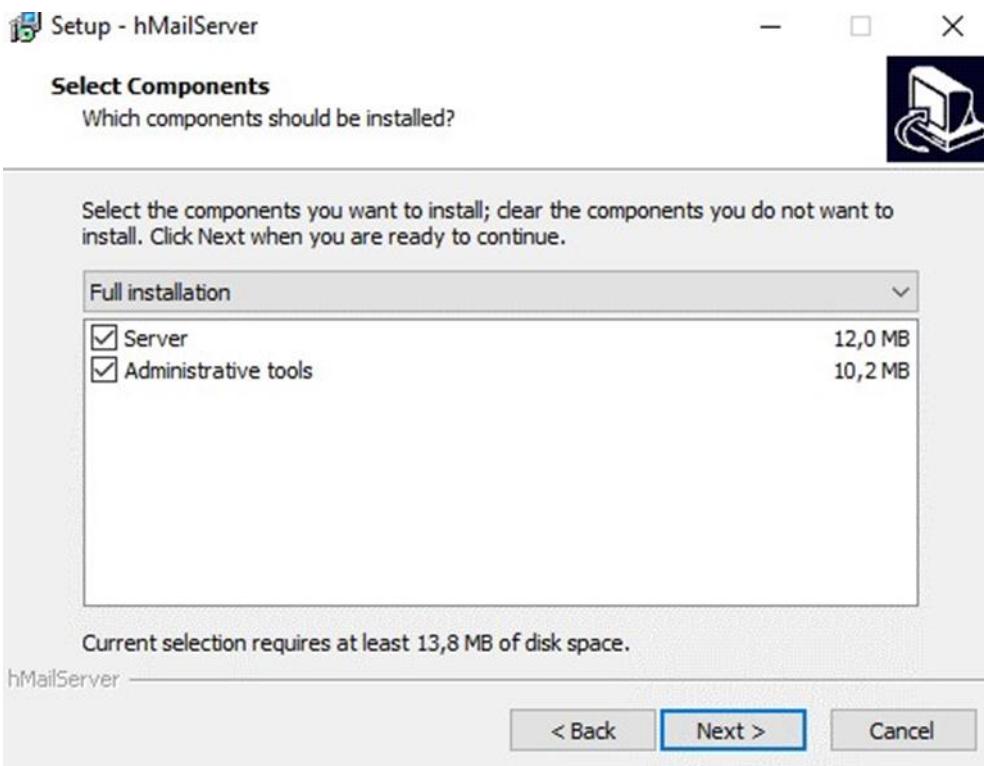
Accepter et faites next



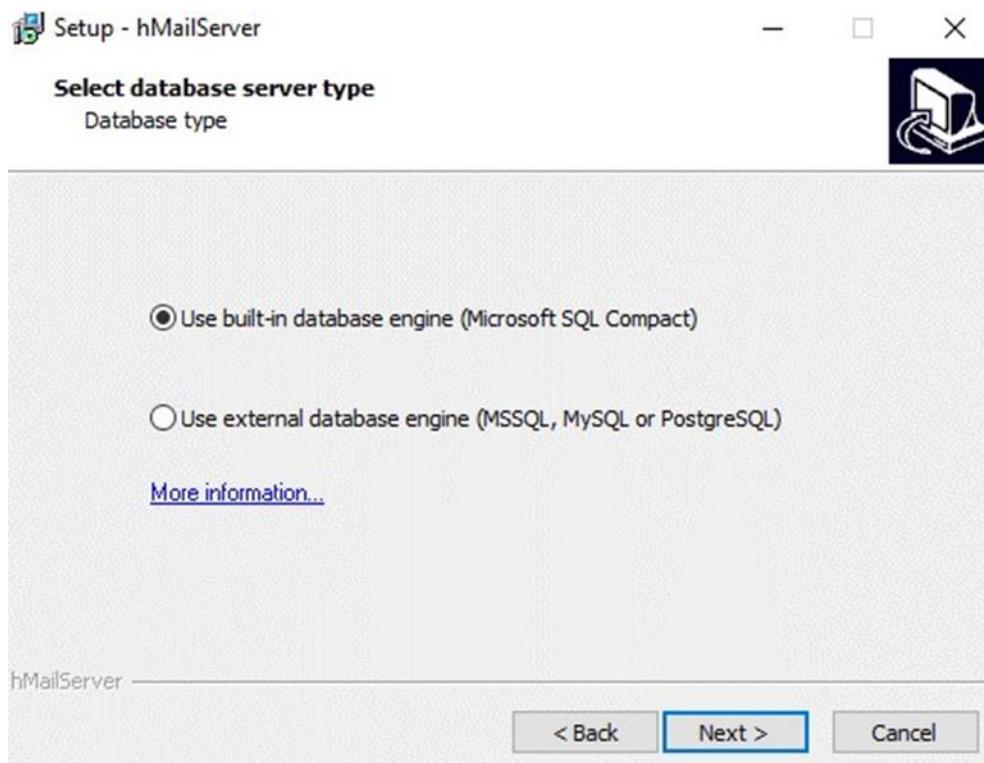
faites next



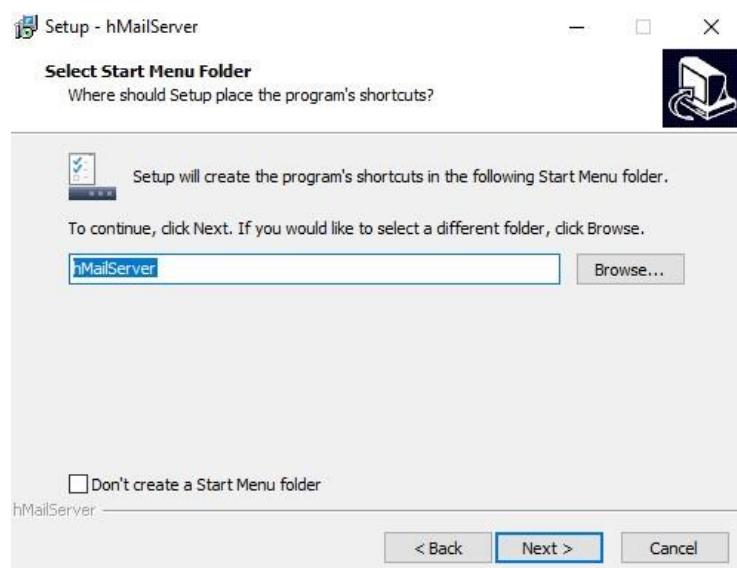
Gardez la full installation et faites next :



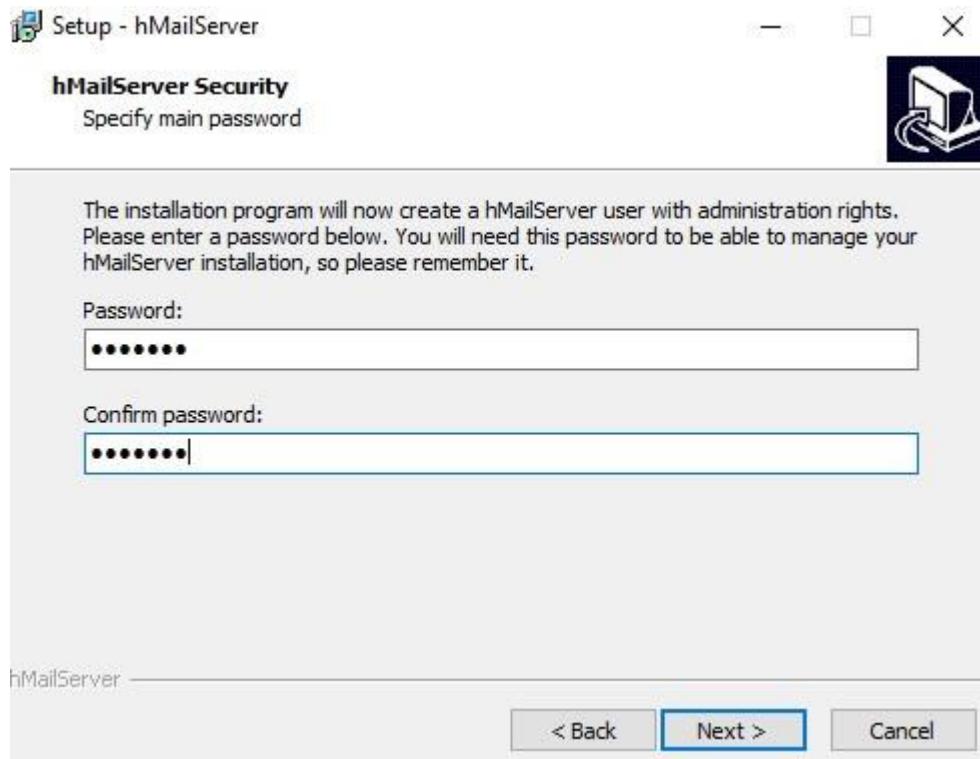
laisser le paramètre par défaut et faites next :



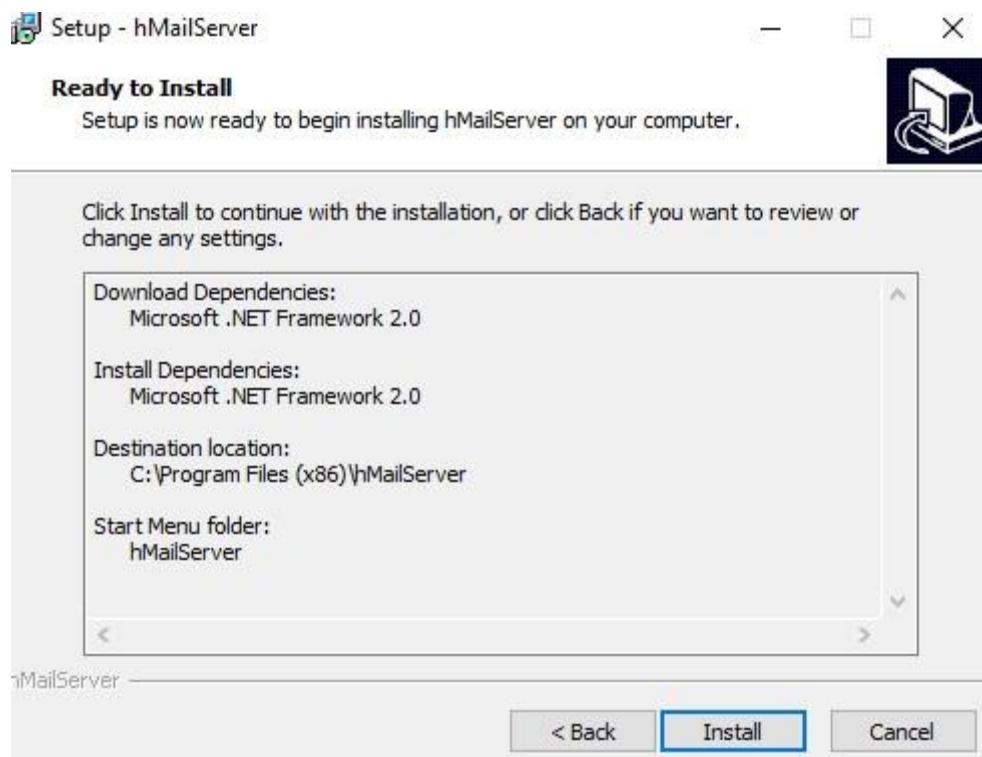
laisser par défaut et faites next :



Choisissez un mot de passe administrateur pour HmailServeur :



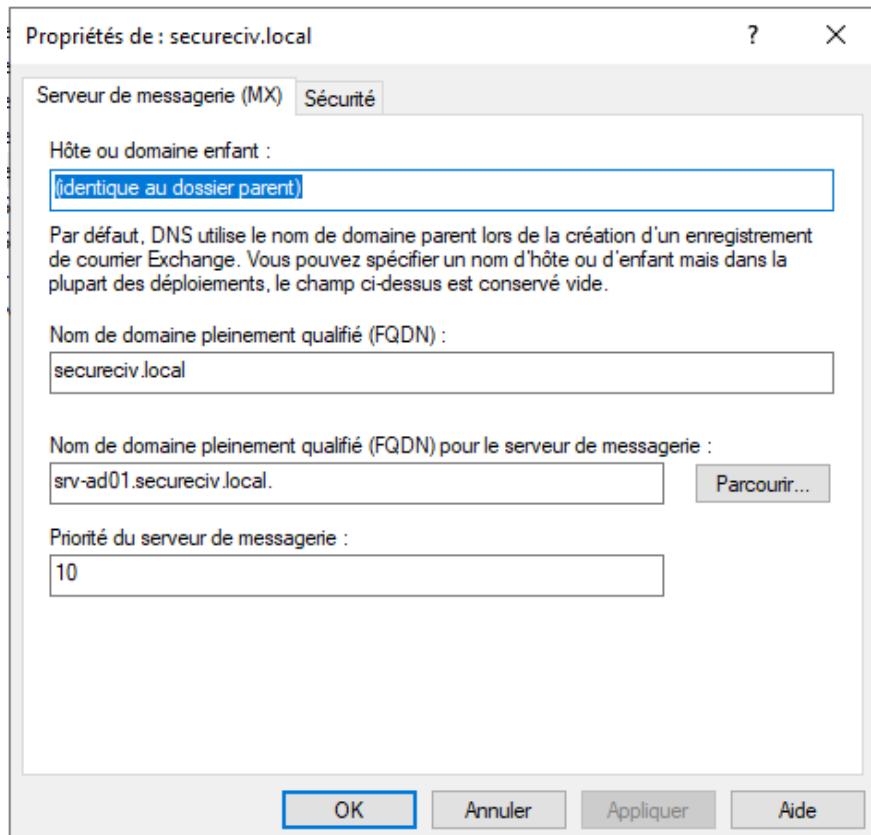
Puis faites Install :



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

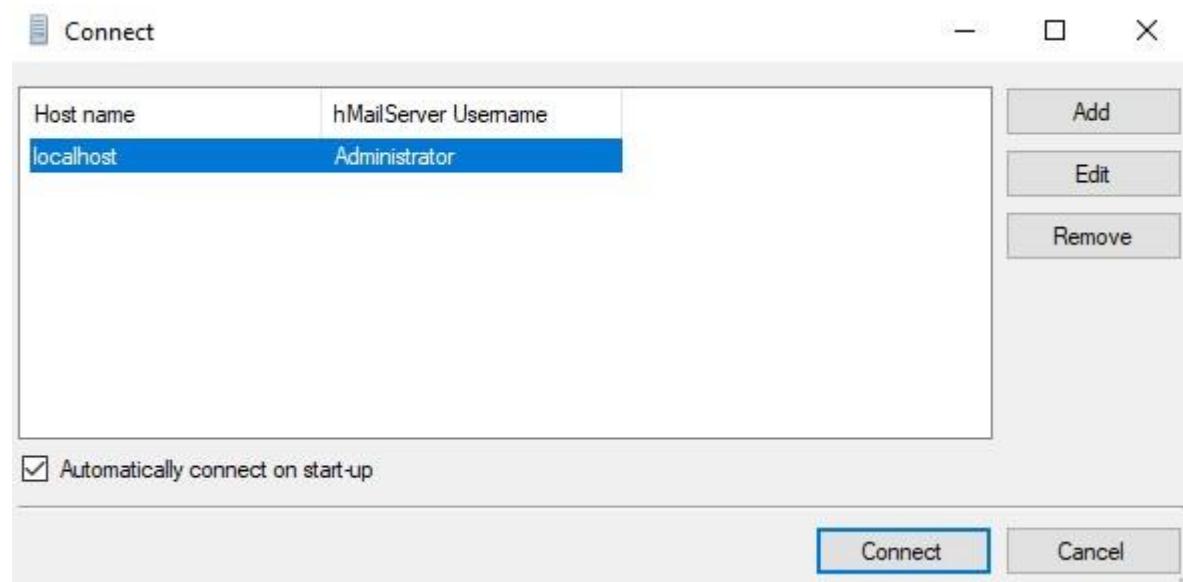
4.2) Configuration DNS pour le serveur de messagerie :

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.

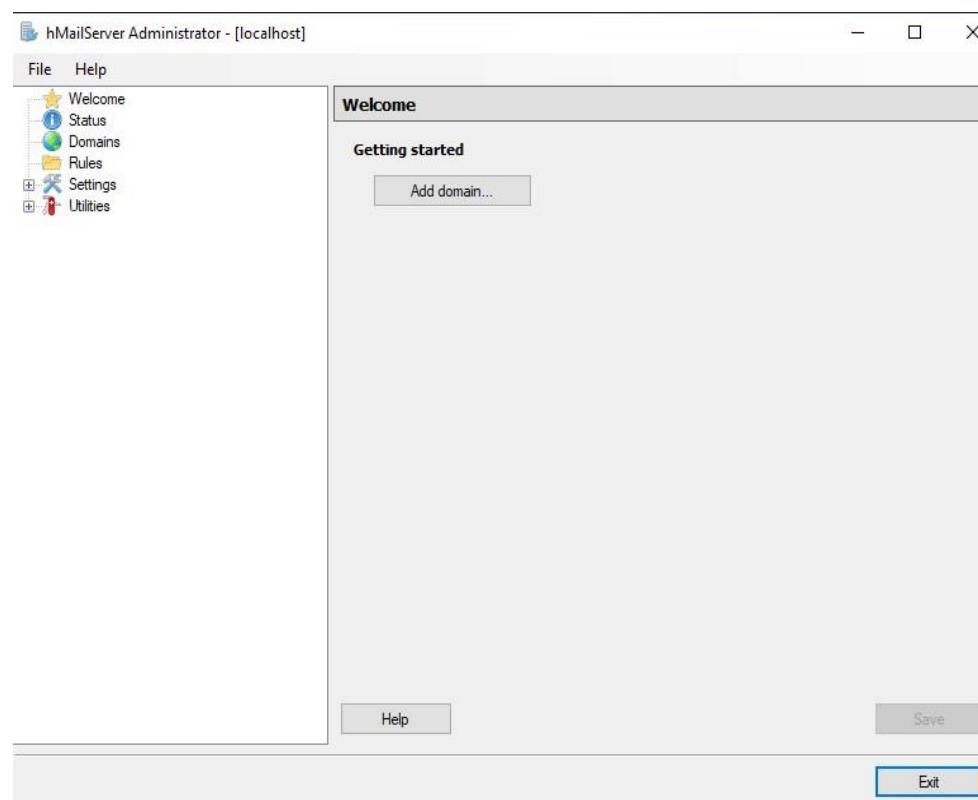


4.3) Configuration Hmailserver

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



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



hMailServer Administrator - [localhost]

File Help

Welcome Status Domains secureciv.local Rules Settings Utilities

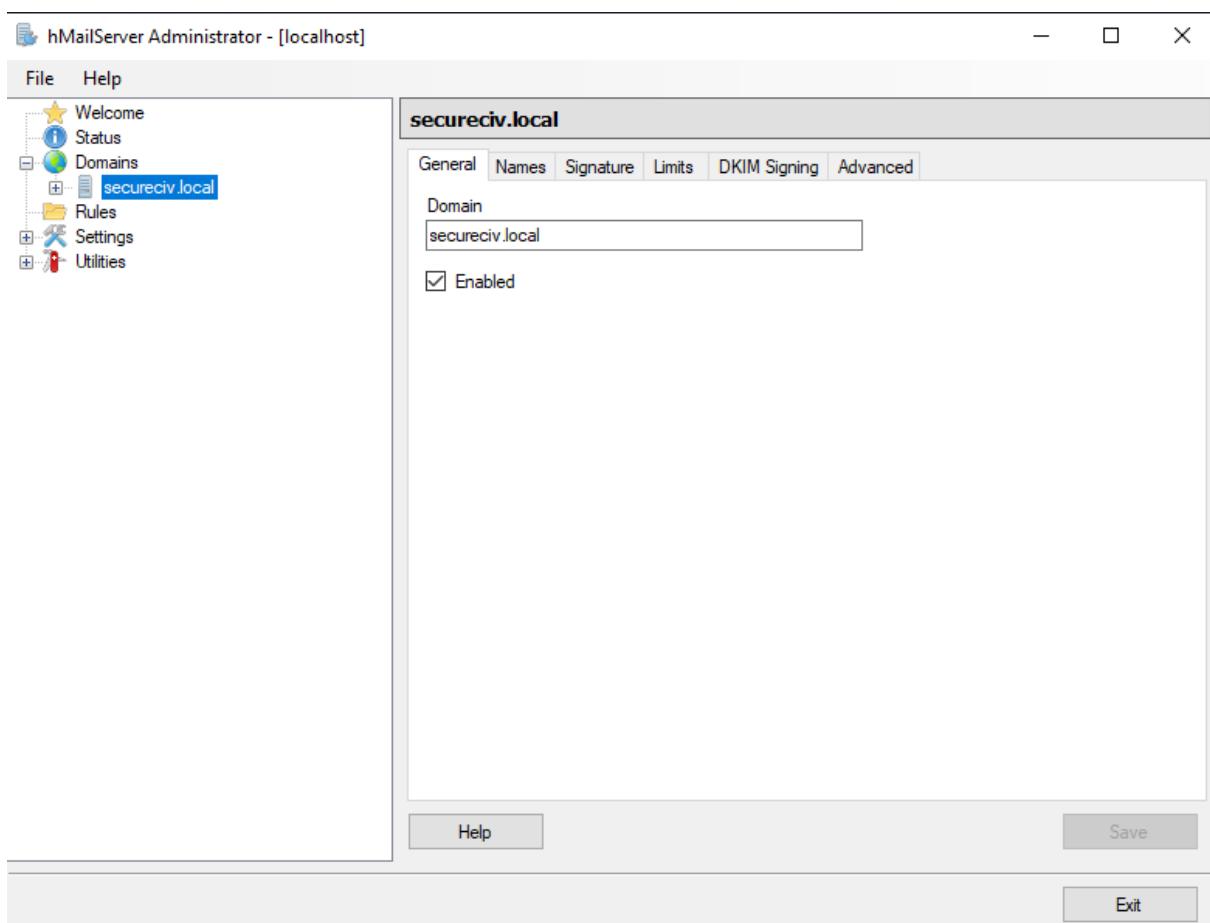
secureciv.local

General Names Signature Limits DKIM Signing Advanced

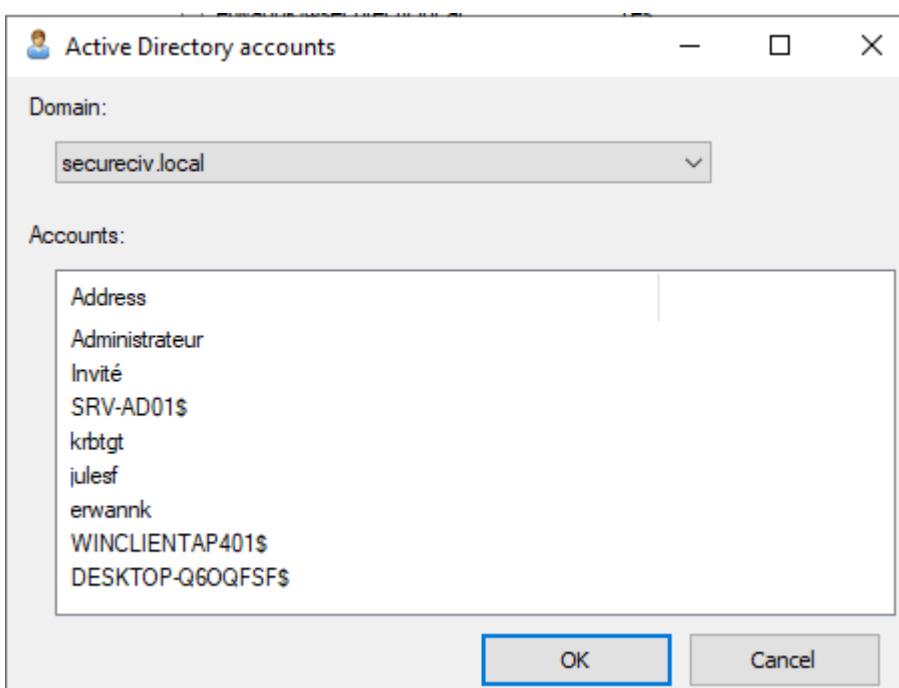
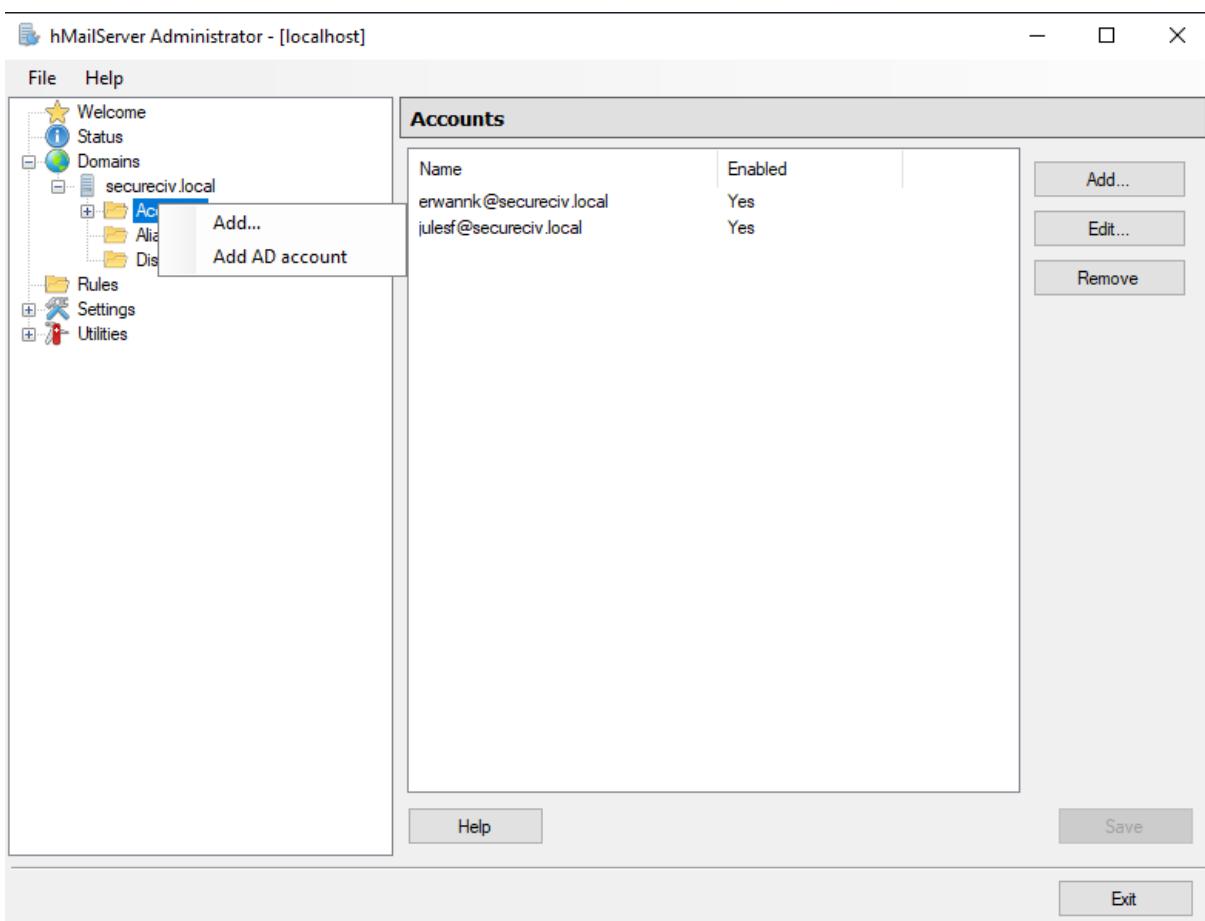
Domain: secureciv.local

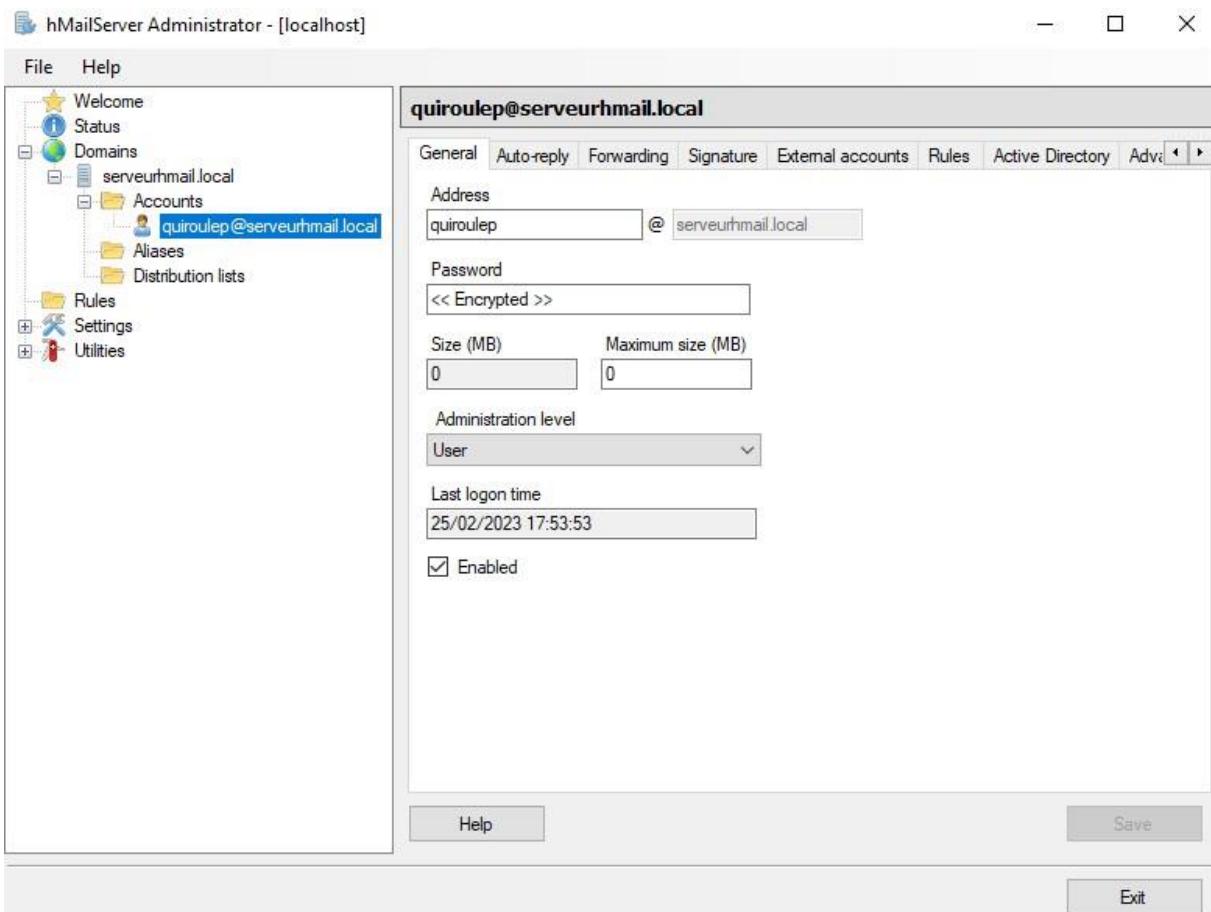
Enabled

Help Save Exit



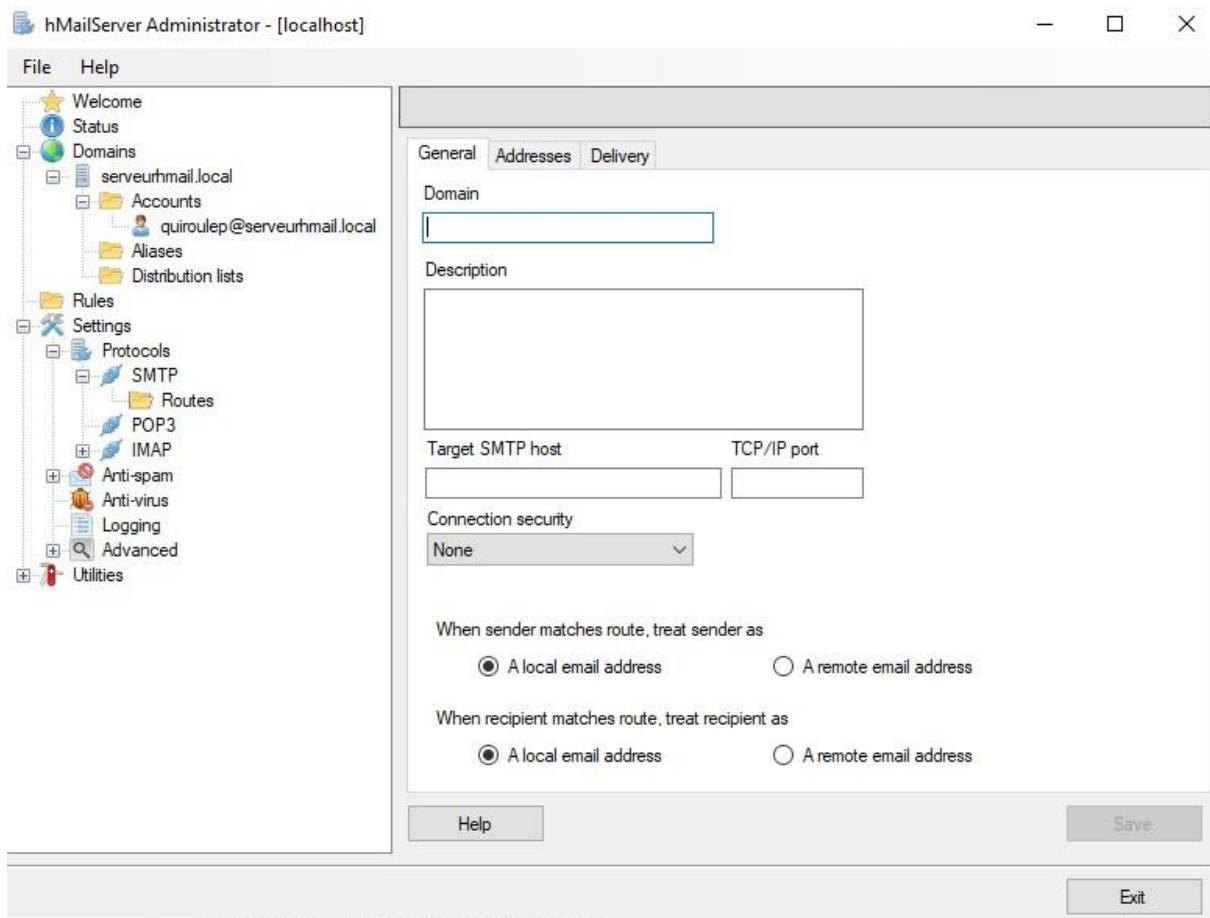
Une fois celui-ci ajouté, faites clic droit sur le nom de domaine et cliquez sur AD account pour ajouter les deux comptes crée au préalable dans l'AD.





4.4) Configuration SMTP :

Pour cela allez à nouveau dans le HmailServer Administrator
Dans Settings/protocols/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

secureciv.local

General Addresses Delivery

Domain
secureciv.local

Description

Target SMTP host TCP/IP port
192.168.20.5 25

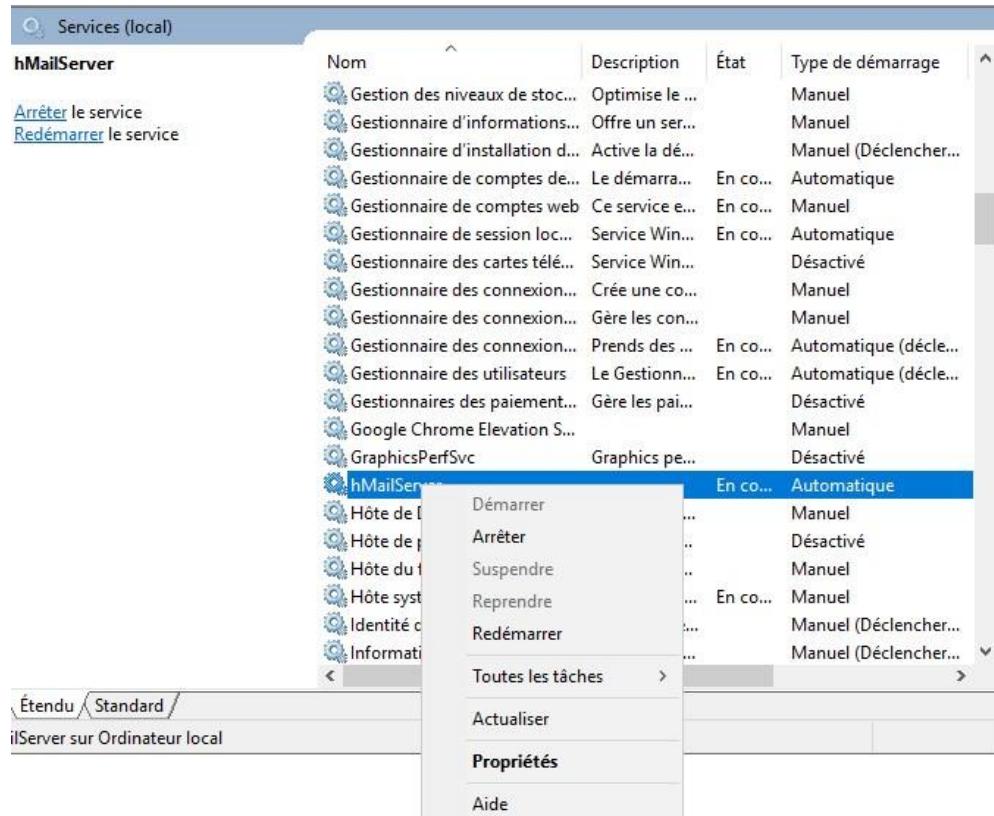
Connection security
None

When sender matches route, treat sender as
 A local email address A remote email address

When recipient matches route, treat recipient as
 A local email address A remote email address

Allez ensuite dans service.msc

Et redémarrez le service hmail



4.5) Connexion au client de messagerie:

Ici nous utiliserons Thunderbird, vous pouvez le trouver 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 créée dans l'AD au moment de la création de l'utilisateur ainsi que le mot de passe de l'utilisateur

Configurez votre adresse électronique existante

Pour utiliser votre adresse électronique actuelle, remplissez vos identifiants.

Thunderbird recherchera automatiquement une configuration fonctionnelle et recommandée du serveur

Votre nom complet

erwann



Adresse électronique

erwannk@secureciv.local



Mot de passe



Retenir le mot de passe

Faites ensuite configuration manuelle,

Vérifier que votre nom de domaine est bien dans la partie « nom d'hôte » dans serveur entrant et sortant puis faites tester

✓ Les paramètres suivants ont été trouvés en sondant le serveur donné :

Paramètres du serveur

SERVEUR ENTRANT

Protocole :	IMAP
Nom d'hôte :	secureciv.local
Port :	143
Sécurité de la connexion :	Aucun
Méthode d'authentification :	Mot de passe normal
Nom d'utilisateur :	erwannk@secureciv.local

SERVEUR SORTANT

Nom d'hôte :	secureciv.local
Port :	587
Sécurité de la connexion :	Aucun
Méthode d'authentification :	Mot de passe normal
Nom d'utilisateur :	erwannk@secureciv.local

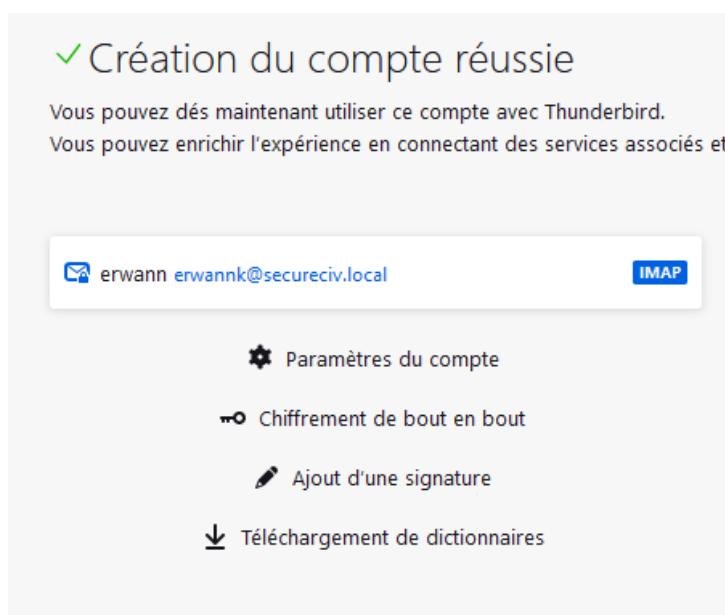
[Configuration avancée](#)

[Retester](#) [Annuler](#) [Terminé](#)

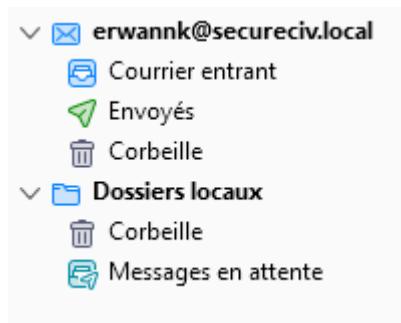
Thunderbird essaiera de détecter automatiquement les champs qui sont laissés

Faites ensuite terminer

Et vous serez connecté au compte



Nous pouvons en effet voir que notre compte a été créé dans la boîte mail Thunderbird



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 à partie d'un autre utilisateur.

	Sujet	Correspondants	Date
★	test messagerie	→ julesf@secureciv.local	03/04/2023, 21:30

Nous pouvons voir après avoir envoyé le mail que celui-ci a correctement été réceptionné

De Moi <erwannk@secureciv.local> ⓘ
Pour Moi <julesf@secureciv.local> ⓘ
Sujet **test messagerie**

Bonjour,

test envoie message

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 configurer 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
allow=ulaw
:allow=ilbc
:autoframing=yes
;
; 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

Fullscreen= 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) Crédit boîte 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



BIENVENUE

Cet assistant va vous aider à configurer et utiliser votre compte SIP.

J'accepte [les conditions d'utilisation](#) et [la politique de confidentialité](#) de Belledonne Communications

[CRÉER UN COMPTE LINPHONE](#)

[UTILISER UN COMPTE LINPHONE](#)

[UTILISER UN COMPTE SIP](#)

[TÉLÉCHARGER UNE CONFIGURATION](#)

Renseignez ensuite comme ceci

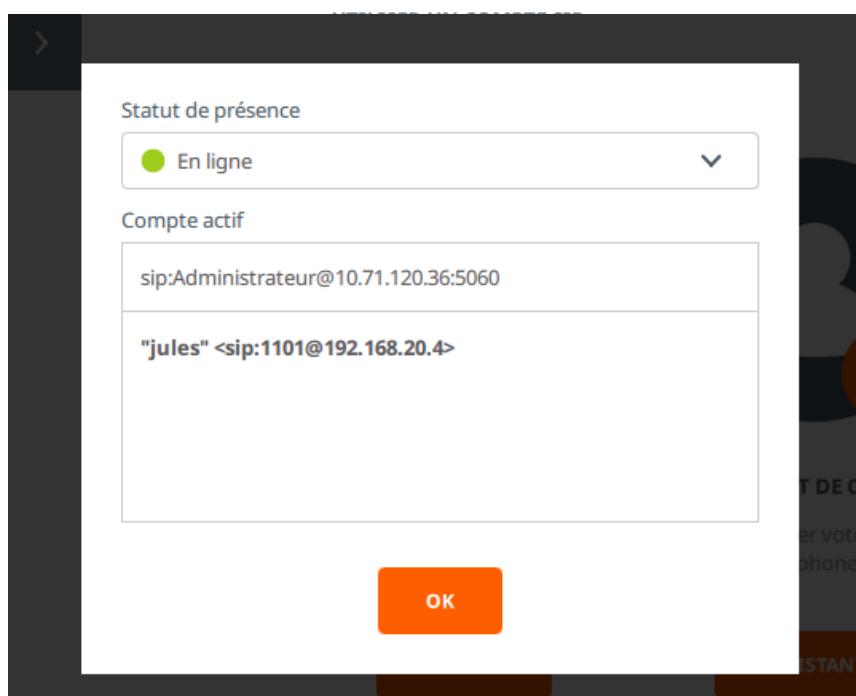
Nom d'utilisateur = le numéro du poste

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

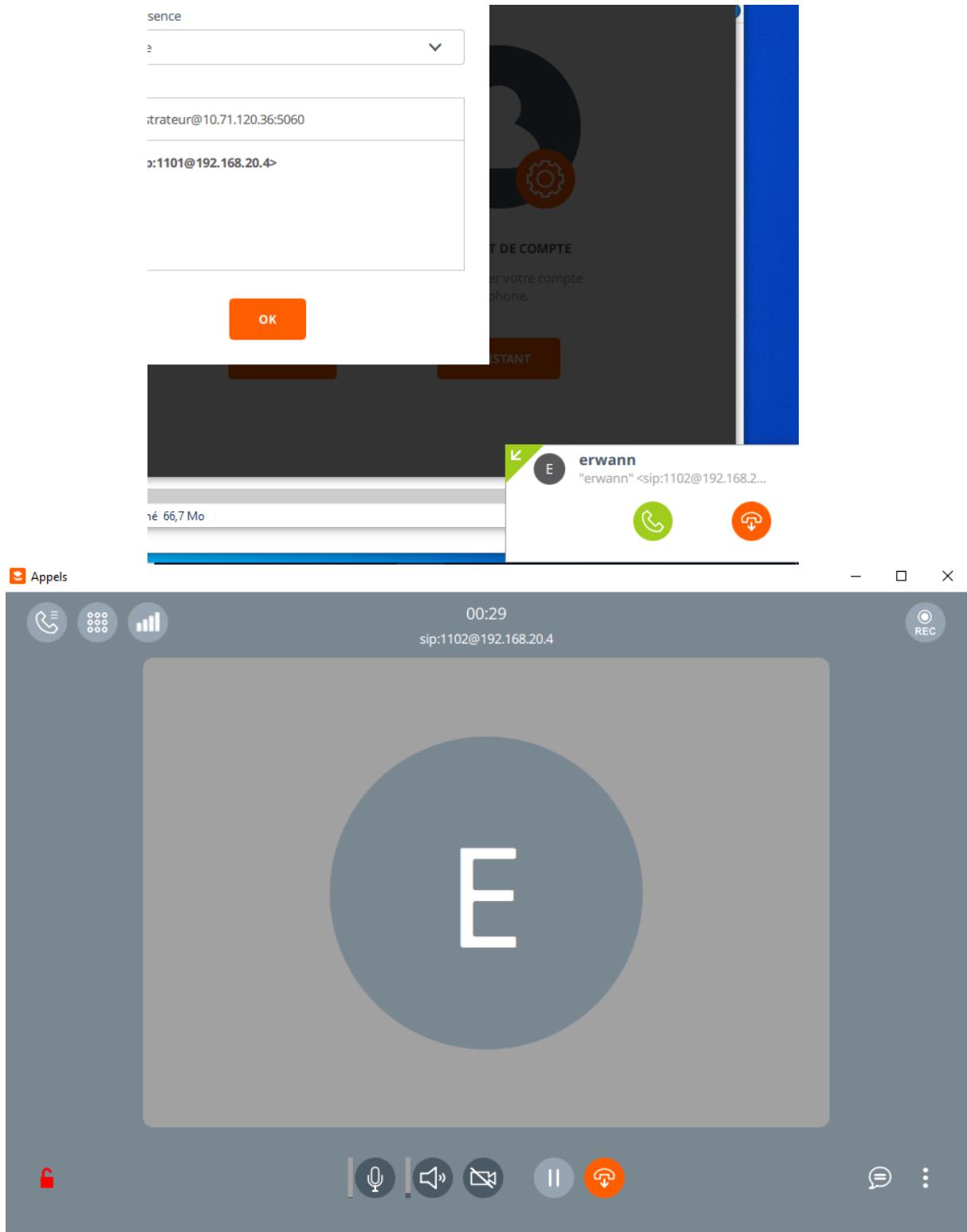


On peut voir que notre compte a bien été ajouté

```
=====
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-Q60QFSF) 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 présent on met l'interface réseau 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_ci;
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)
```

 Configuration Base de données

Paramètres de connexion à la base de données

Server Name	<input type="text" value="192.168.30.1"/>
User	<input type="text" value="ebrigade"/>
Password	<input type="password" value="....."/>
Database name	<input type="text" value="ebirgade"/>

valider

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 à 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 /authentication Servers/

System / User Manager / Authentication Servers / Edit

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

Server Settings	
<u>Descriptive name</u>	secureciv.local
<u>Type</u>	LDAP

LDAP Server Settings

<u>Hostname or IP address</u>	192.168.20.5
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (CN) of the LDAP server SSL/TLS Certificate.	
<u>Port value</u>	389
<u>Transport</u>	Standard TCP
<u>Peer Certificate Authority</u>	Global Root CA List
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS active. This CA must match the CA used by the LDAP server.	
<u>Protocol version</u>	3
<u>Server Timeout</u>	25
Timeout for LDAP operations (seconds)	
<u>Search scope</u>	Level
<u>One Level</u>	
<u>Base DN</u>	
DC=secureciv,DC=local	
<u>Authentication containers</u>	CN=Users,DC=secureciv,DC=local
Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component. Example: CN=Users;DC=example,DC=com or OU=Staff,OU=Freelancers	
<input type="button" value="Select a container"/>	

CCi campus

Extended query Enable extended query

Bind anonymous Use anonymous binds to resolve distinguished names

Bind credentials Administrateur@secureciv.local
User naming attribute samAccountName
Group naming attribute cn
Group member attribute memberOf

RFC 2307 Groups LDAP Server uses RFC 2307 style group membership
 RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object.
 Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class posixGroup
 Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN
 If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.
 Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

UTF8 Encode UTF8 encode LDAP parameters before sending them to the server.
 Required to support international characters, but may not be supported by every LDAP server.

Username Alterations Do not strip away parts of the username after the @ symbol
 e.g. user@host becomes user when unchecked.

Allow unauthenticated bind Allow unauthenticated bind
 Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

Nous avons maintenant bien lié notre pfsense au LDAP

System / User Manager / Authentication Servers

Users Groups Settings **Authentication Servers**

Authentication Servers			
Server Name	Type	Host Name	Actions
secureciv.local	LDAP	192.168.20.5	
Local Database		RTE-01	

7.2) Mise en place du VPN :

Rendez dans VPN/OpenVPN

Puis allez dans l'onglet « wizards »

The screenshot shows a top navigation bar with tabs: 'VPN / OpenVPN / Servers', 'Clients', 'Client Specific Overrides', 'Wizards', 'Client Export', and 'Shared Key Export'. The 'Servers' tab is highlighted with a red underline.

Choisissez « LDAP » dans le type de server :

Sélectionnez le serveur que nous avons au préalablement lié

The screenshot shows a wizard titled 'OpenVPN Remote Access Server Setup'. The first step is 'Select an Authentication Backend Type'. A dropdown menu labeled 'Type of Server' is set to 'LDAP'. A note below says: 'NOTE: If unsure, leave this set to "Local User Access."'. A blue 'Next' button is at the bottom.

Ensuite complété le Certificat d'autorité comme ci-dessous

Create a New Certificate Authority (CA) Certificate

Descriptive name	openvpn	A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.
Key length	2048 bit	Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Lifetime	3650	Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code	FR	Two-letter ISO country code (e.g. US, AU, CA)
State or Province	Alsace	Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	Strasbourg	City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Pareil pour le certificat serveur

Create a New Server Certificate

Descriptive name	openvpn_certificate	A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."
Key length	2048 bit	Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Lifetime	398	Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Country Code	FR	Two-letter ISO country code (e.g. US, AU, CA)
State or Province	Alsace	Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	Strasbourg	City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization	sécurité civile	Organization name, often the Company or Group name.

Pour continuer on configure les paramètres généraux de cette manière :

General OpenVPN Server Information	
Interface	WAN
The interface where OpenVPN will listen for incoming connections (typically WAN.)	
Protocol	UDP on IPv4 only
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.	
Local Port	1195
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.	
Description	SSL OpenVPN
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.	
Cryptographic Settings	
TLS Authentication	<input checked="" type="checkbox"/>
Enable authentication of TLS packets.	
Generate TLS Key	<input checked="" type="checkbox"/>
Automatically generate a shared TLS authentication key.	

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

Tunnel Settings	
Tunnel Network	192.168.120.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.	
Redirect Gateway	<input type="checkbox"/>
Force all client generated traffic through the tunnel.	
Local Network	192.168.20.0/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.	

On oublie pas de cocher les deux case ci-dessous

Firewall Rule Configuration	
OpenVPN Remote Access Server Setup Wizard	
Firewall Rule Configuration	
Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.	
Traffic from clients to server	
Firewall Rule	<input checked="" type="checkbox"/>
Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.	
Traffic from clients through VPN	
OpenVPN rule	<input checked="" type="checkbox"/>
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.	

Notre serveur OpenVPN à bien été crée :

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

OpenVPN Servers									Description	Actions		
Interface	Protocol / Port	Tunnel Network	Mode / Crypto									
WAN	UDP4 / 1194 (TUN)	192.168.112.0/24	Mode: Remote Access (User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits						SSL OpenVPN			

7.3) Règle de pare-feu pour openVPN :

Les règles par défaut sont :

Rules (Drag to Change Order)												Actions	
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description			
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /179 KiB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Autorise OpenVPN			

Rules (Drag to Change Order)												Actions	
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description			
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /37 KiB	IPv4 *	*	*	*	*	*	*	none	OpenVPN SSL OpenVPN wizard			

7.4) Installation du paquet OpenVPN

Nous allons allez dans System/Package manager

Puis dans available Packages cherchez OpenVPN et installez le

Installed Packages Available Packages

Search

Search term: openvpn Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages			
Name	Version	Description	Actions
openvpn-client-export	1.6_9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	
Package Dependencies: openvpn-client-export-2.5.8 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3			

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

Installed Packages

Name	Category	Version	Description	Actions
openvpn-client-export	security	1.6_9	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	
Package Dependencies: openvpn-client-export-2.5.8 openvpn-2.5.4_1 zip-3.0_1 p7zip-16.02_3				

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

The screenshot shows the 'OpenVPN / Client Export Utility' interface. At the top, there are tabs: Server, Client, Client Specific Overrides, Wizards, Client Export (which is highlighted in blue), and Shared Key Export. Below the tabs, there is a section titled 'Client Export' with several download links:

- Inline Configurations:
 - [Most Clients](#)
 - [Android](#)
 - [OpenVPN Connect \(iOS/Android\)](#)
- Bundled Configurations:
 - [Archive](#)
 - [Config File Only](#)
- Current Windows Installer (2.5.8-ix04):
 - [64-bit](#)
 - [32-bit](#)
- Legacy Windows Installers (2.4.12-ix01):
 - [10/2016/2019](#)
 - [7/8/8.1/2012r2](#)
- Viscosity (Mac OS X and Windows):
 - [Viscosity Bundle](#)
 - [Viscosity Inline Config](#)

Puis on récupère le fichier archive

The screenshot shows the 'OpenVPN Clients' interface. In the 'Client Export' section, there is a table with columns: User, Certificate Name, and Export. One row is visible:

User	Certificate Name	Export
Authentication Only (No Cert)	none	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Archive Config File Only - Current Windows Installer (2.5.8-ix04): <ul style="list-style-type: none"> 64-bit 32-bit - Legacy Windows Installers (2.4.12-ix01): <ul style="list-style-type: none"> 10/2016/2019 7/8/8.1/2012r2 - Viscosity (Mac OS X and Windows): <ul style="list-style-type: none"> Viscosity Bundle Viscosity Inline Config

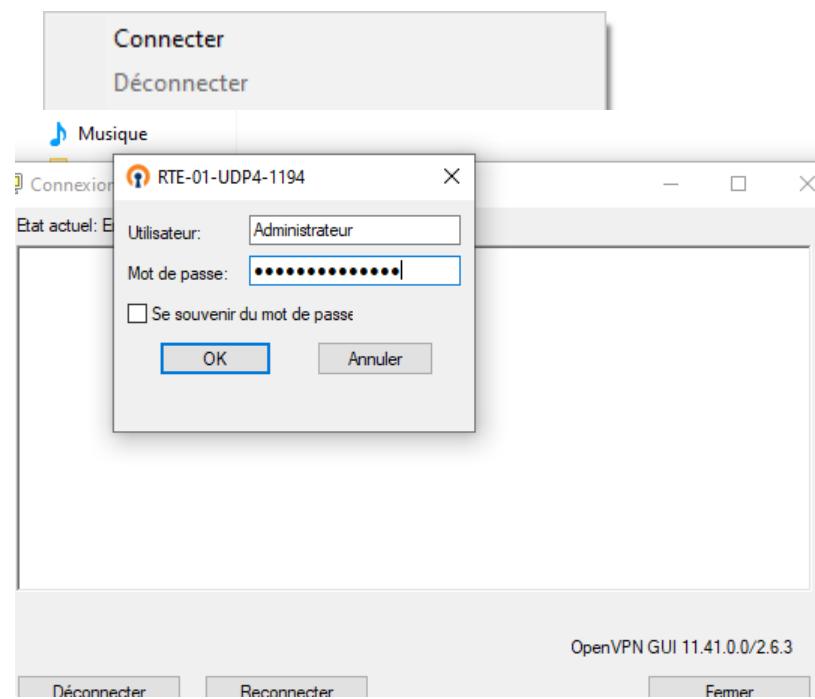
On extrait le fichier et on met les fichiers contenu dans le dossier config de OpenVPN qui se trouve dans Programme/OpenVPN/ Config

The screenshot shows a Windows File Explorer window with the path: Ce PC > Disque local (C:) > Programmes > OpenVPN > config. The folder contains the following files:

Nom	Modifié le	Type	Taille
README	13/04/2023 11:25	Document texte	1 Ko
RTE-01-UDP4-1194	14/04/2023 12:24	OVPN Profile	1 Ko
RTE-01-UDP4-1194-ca	14/04/2023 12:24	Certificat de sécur...	2 Ko
RTE-01-UDP4-1194-tls.key	14/04/2023 12:24	Fichier KEY	1 Ko

Puis dans les icônes 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

