

**AP4**

**Documentation Technique**

Date : 15/04/2023

Les résultats, opinions et recommandations exprimés dans ce rapport émanent de l’auteur ou des auteurs et n’engagent aucunement CCI Campus

**SOMMAIRE**

[1) Routeurs – firewalls 4](#_Toc132809317)

[1.1) Configuration système et réseau 4](#_Toc132809318)

[1.2) Redondance des routeurs 4](#_Toc132809319)

[1.3) Adresse IP virtuelle LAN 6](#_Toc132809320)

[1.4) Adresse IP virtuelle DMZ 6](#_Toc132809321)

[1.5) Règles de pares-feux 6](#_Toc132809322)

[2) Serveurs Windows 8](#_Toc132809323)

[2.1) Installation et configuration de SRV-AD01 8](#_Toc132809324)

[2.2) Création de l’AD 8](#_Toc132809325)

[2.3) Installation et configuration de SRV-AD02 9](#_Toc132809326)

[2.4) Ajout de SRV-AD02 en contrôleur de domaine 9](#_Toc132809327)

[2.5) Configuration du DCHP 9](#_Toc132809328)

[2.6) Ajout des utilisateurs dans l’AD 10](#_Toc132809329)

[3) Serveur de supervision 10](#_Toc132809330)

[3.1) Installation et configuration système réseau 10](#_Toc132809331)

[3.2) Installer checkmk 10](#_Toc132809332)

[3.3) Configuration de checkmk 11](#_Toc132809333)

[3.4) Installation de l’agent 11](#_Toc132809334)

[3.5) Ajout de l’hôte 11](#_Toc132809335)

[3.6) Ajouter les pares-feux via SNMP 12](#_Toc132809336)

[4) Serveur de messagerie 13](#_Toc132809337)

[4.1) Installation Hmail : 13](#_Toc132809338)

[4.2) Configuration DNS pour le serveur de messagerie : 17](#_Toc132809339)

[4.3) Configuration Hmailserver 18](#_Toc132809340)

[4.4) Configuration SMTP : 21](#_Toc132809341)

[4.5) Connexion au client de messagerie: 24](#_Toc132809342)

[5) Serveur Voip 27](#_Toc132809343)

[5.1) Installatio net configuration 27](#_Toc132809344)

[5.2) Installation d’ asterisk: 27](#_Toc132809345)

[5.3) Configuration d’asterisk 27](#_Toc132809346)

[5.4) Configuration Users asterisk : 28](#_Toc132809347)

[5.5) Création boite vocale : 28](#_Toc132809348)

[6) ERP et DMZ 32](#_Toc132809349)

[6.1) Installation et configuration de eBrigade 32](#_Toc132809350)

[6.2) Création de la base de données 32](#_Toc132809351)

[6.3) Configuration de la DMZ 33](#_Toc132809352)

[7) Mise en place VPN 34](#_Toc132809353)

[7.1) Liaison pfsense/LDAP : 34](#_Toc132809354)

[7.2) Mise en place du VPN : 35](#_Toc132809355)

[7.3) Règle de pare-feu pour openVPN : 39](#_Toc132809356)

[7.4) Installation du paquet OpenVPN 39](#_Toc132809357)

[7.5) Connexion VPN à distance : 40](#_Toc132809358)

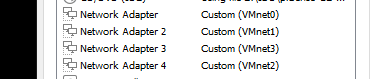
## 1) Routeurs – firewalls

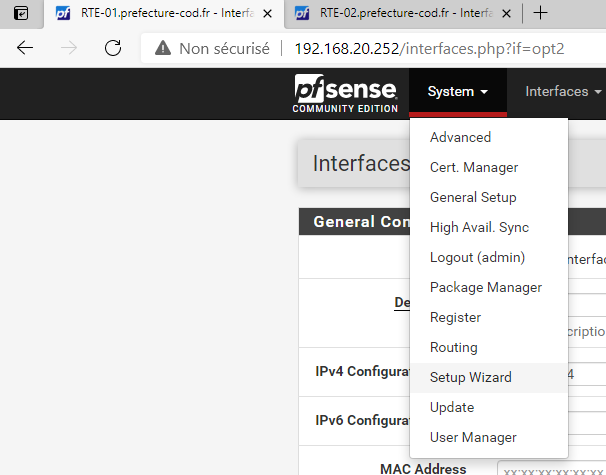
### 1.1) Configuration système et réseau

Une fois l’installation fini, on configure les adresses IP comme ci-dessous :  
Une image contenant texte

Description générée automatiquement

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 :

Une image contenant texte

Description générée automatiquement

Une image contenant texte, table

Description générée automatiquement

On coche tout pour faire une synchro complète :  
Une image contenant texte

Description générée automatiquement

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

Description générée automatiquement

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 :Une image contenant texte

Description générée automatiquement

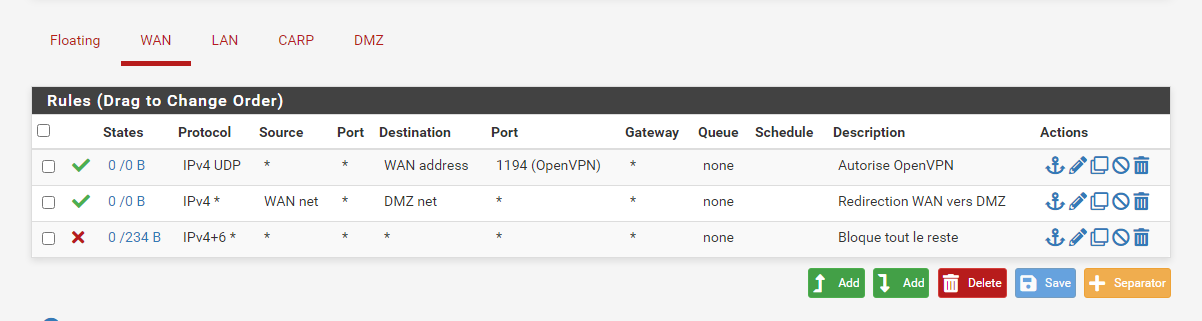
### 1.4) Adresse IP virtuelle DMZ

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 :

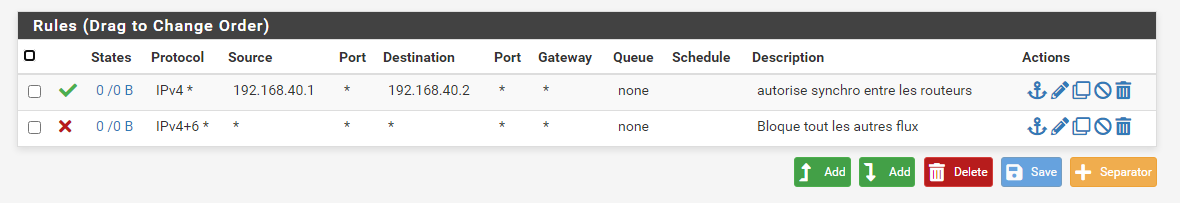


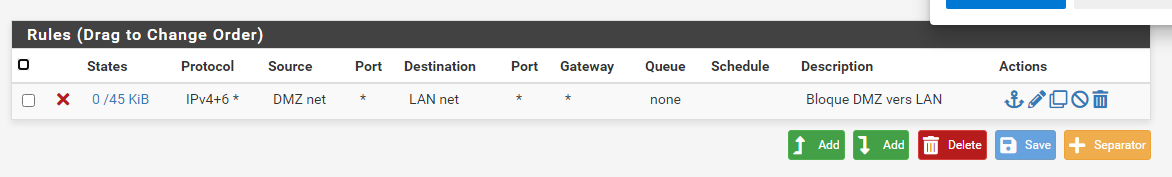
Interface LAN :

Une image contenant calendrier

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

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

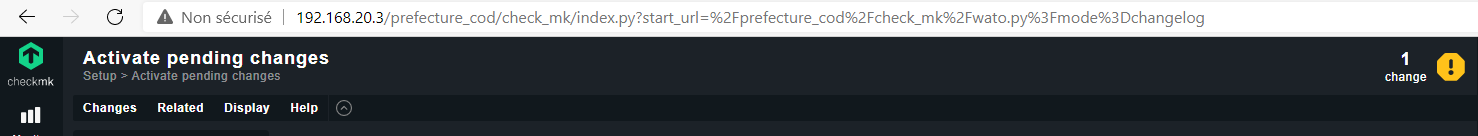
Pour l’installation de l’agent sur Windows, on choisit de faire une clean installation :  
Une image contenant texte

Description générée automatiquement

### 3.5) Ajout de l’hôte

On se rend dans Setup > Hosts > Add host to the monitoring et on ajoute l’hôte souhaité :  
Une image contenant texte, capture d’écran, écran, noir

Description générée automatiquement

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


On clique sur Activitate on selected sites   
Une image contenant texte, capture d’écran, écran, intérieur

Description générée automatiquement

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 :  
Une image contenant texte

Description générée automatiquement

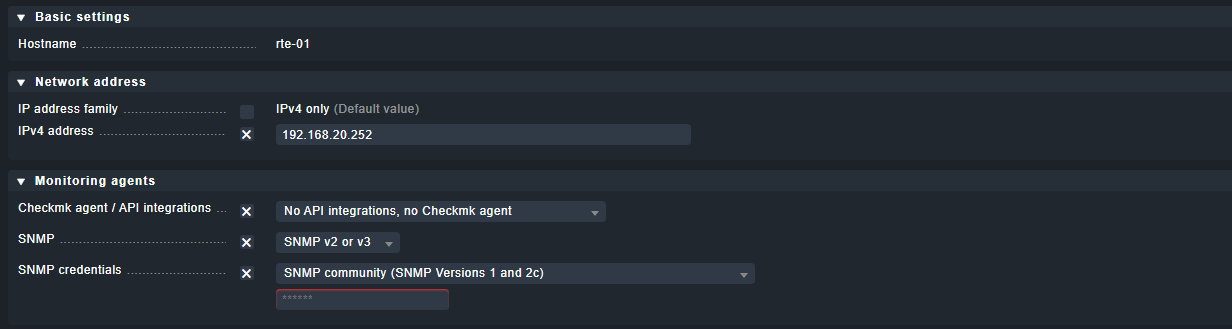
On applique les changements en cliquant sur *Change* puis sur *Activitate on selected sites*

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

### 3.6) Ajouter les pares-feux via SNMP

On active le service SNMP :  
Une image contenant texte, capture d’écran, écran, télévision

Description générée automatiquement

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

Puis dans Services of Host on ajoute tous les services.

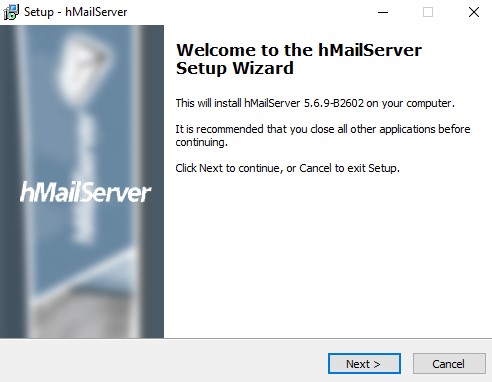
## 4) Serveur de messagerie

### 4.1) Installation Hmail :

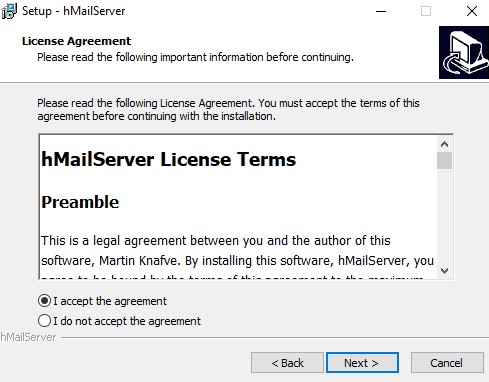
Exécuter le fichier d’installation de hmailserver que l’on télécharge ici : <https://www.hmailserver.com/>

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

Faites next



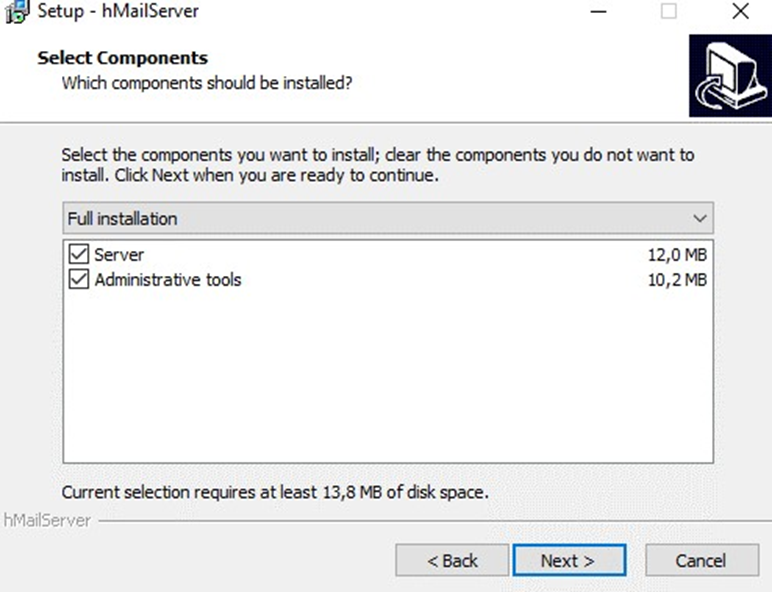
Accepter et faites next

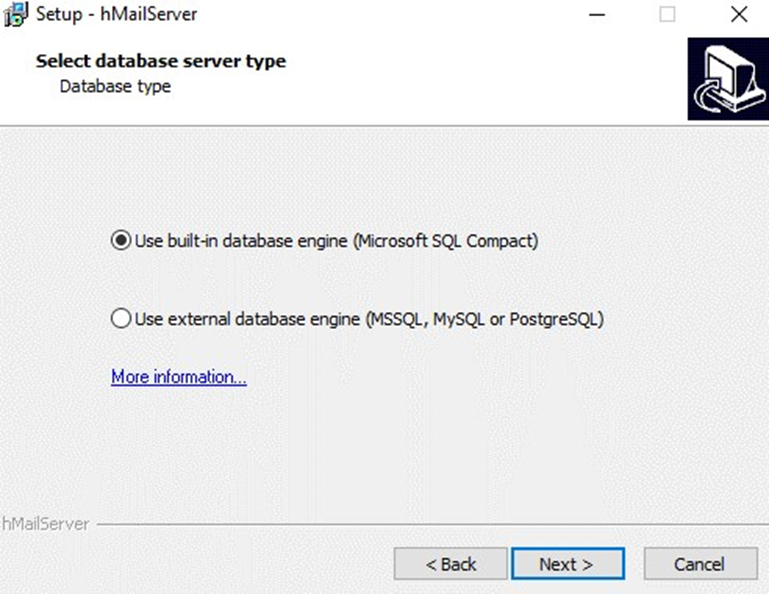


Une image contenant texte

Description générée automatiquementfaites next

Gardez la full installation et faites next :



laisser le paramètre par défaut et faites next :

Une image contenant texte

Description générée automatiquementlaisser par défaut et faites next :

Une image contenant texte

Description générée automatiquementChoisissez un mot de passe administrateur pour HmailServeur :

Puis faites Install :

Une image contenant texte

Description générée automatiquement

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

### 4.2) Configuration DNS pour le serveur de messagerie :

Une image contenant texte

Description générée automatiquementNous 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.

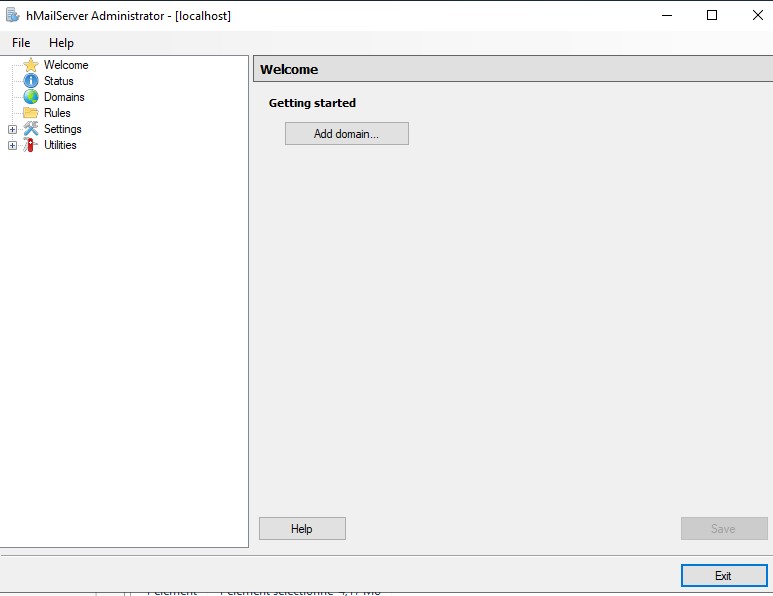
### 4.3) Configuration Hmailserver

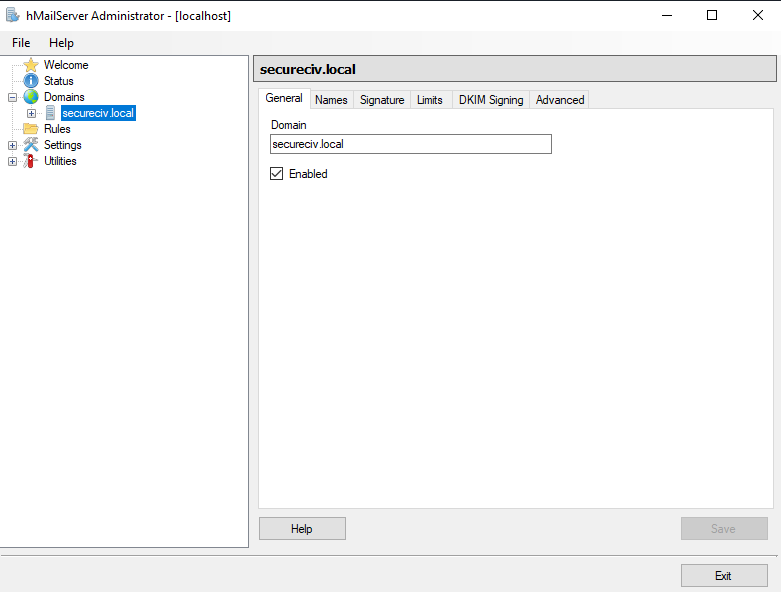
Dans un premier nous devons nous connecter avec le mot de passe définit au moment de l’installation en cliquant sur connect.

Une image contenant texte

Description générée automatiquement

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





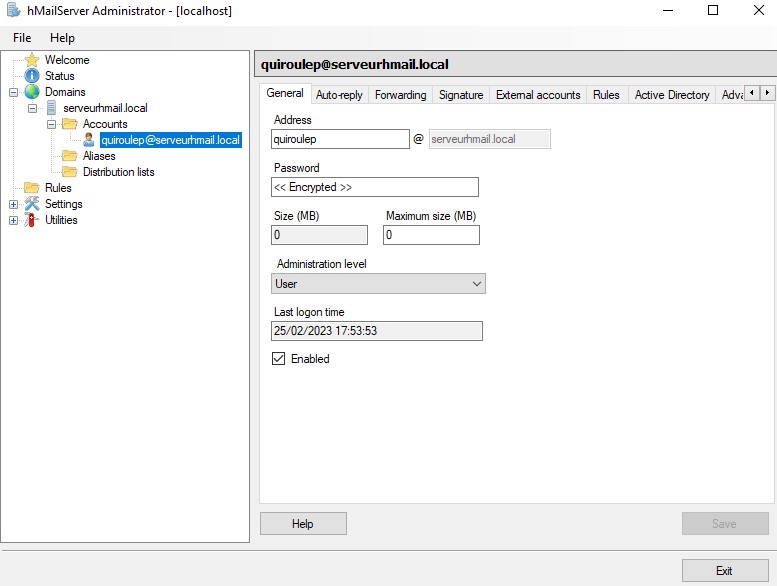
Une fois celui-ci ajouté, faites clic droit sur le nom de domaine et cliquez sur AD account pour ajouter les deux comptes crée au préalable dans l’AD.

Une image contenant texte

Description générée automatiquement

Une image contenant texte

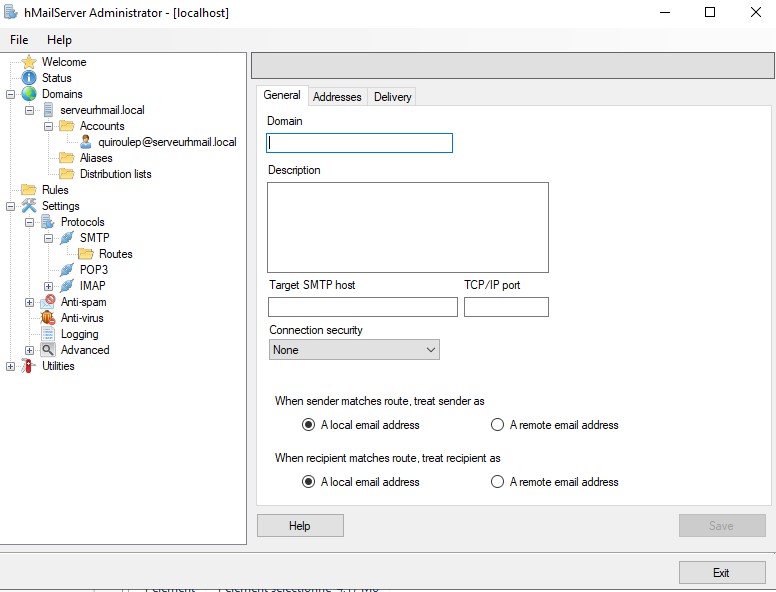
Description générée automatiquement



### 4.4) Configuration SMTP :

Pour cela allez à nouveau dans le HmailServer Administrator

Dans Settings/protocals/SMTP/Routes



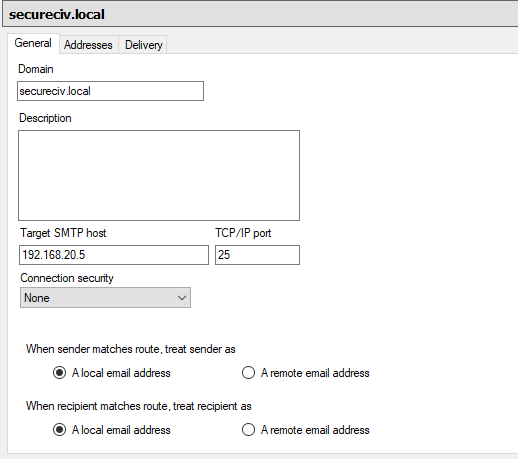
Entrez dans domain le nom de domaine de votre serveur mail.

Ainsi que son adresse IP dans target SMTP host

On utilisera le port 25

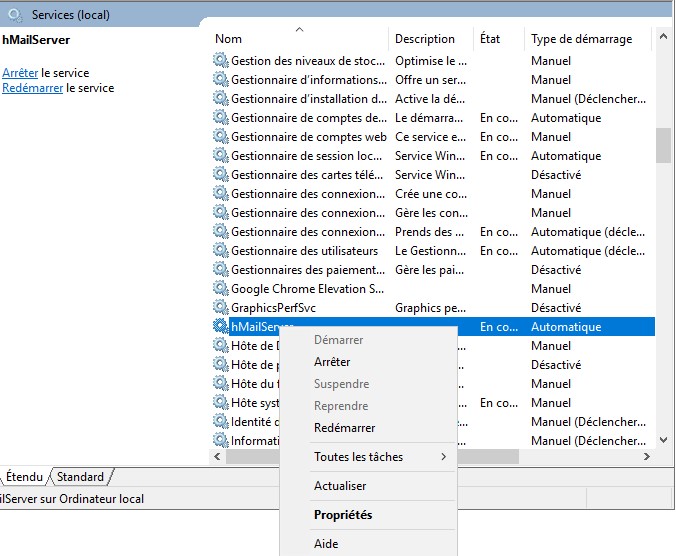
Laissez le reste par défaut

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/>

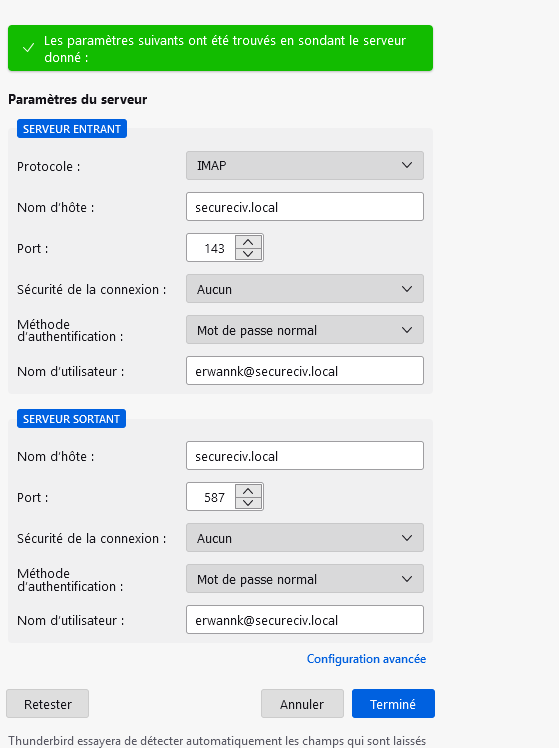
Faites une installation standard et après l’installation de Thunderbird, entrer le nom de la personne et l’adresse mail qui est crée dans l’AD au moment de la création de l’utilisateur ainsi que le mot de passe de l’utilisateur

Une image contenant texte

Description générée automatiquement

Faites ensuite configuration manuelle,

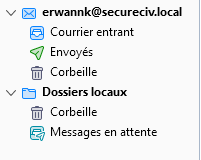
Vérifier que votre nom de domaine est bien dans la partie « nom d’hote » dans serveur entrant et sortant puis faites tester



Faites ensuite terminer

Une image contenant texte

Description générée automatiquementEt 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.

Une image contenant graphique

Description générée automatiquement

Nous pouvons voir après avoir envoyer le mail que celui-ci à correctement été réceptionnéUne image contenant texte

Description générée automatiquement

## 5) Serveur Voip

### 5.1) Installatio net 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

Une image contenant texte

Description générée automatiquementSudo nano /etc/netplan

### 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

Une image contenant texte

Description générée automatiquementElles vont permettre de configuré le protocole utilisé

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)

Une image contenant texte

Description générée automatiquement

### 5.4) Configuration Users asterisk :

Nous allons créer les utilisateurs sur le fichier users.conf

cd /etc/asterisk

nano users.conf

Une image contenant texte

Description générée automatiquement

[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:

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquementnano extensions.conf

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

Une image contenant texte

Description générée automatiquement

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

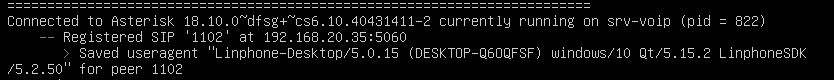
Le mot de passe de l’utilisateur SIP

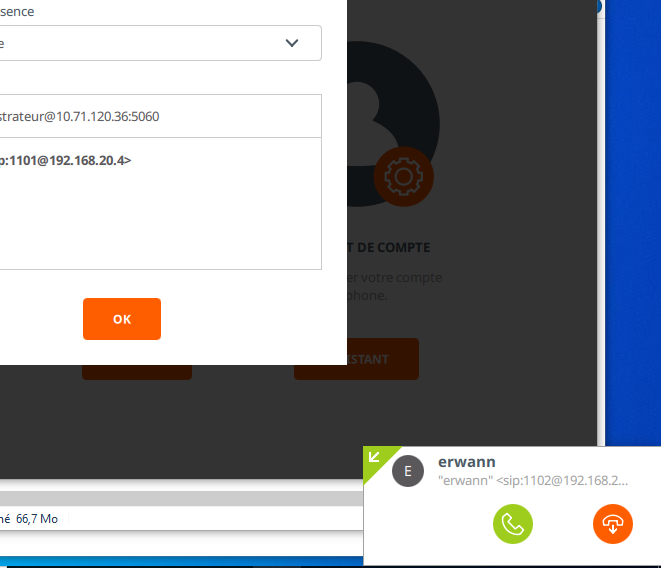
Une image contenant Site web

Description générée automatiquementPuis cliquez sur utiliser

Une image contenant texte

Description générée automatiquementOn peut voir que notre compte à bien été ajouté



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

Une image contenant texte, capture d’écran, Appareils électroniques

Description générée automatiquement

## 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

Une image contenant texte

Description générée automatiquement

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

Ensuite :

Netplan apply

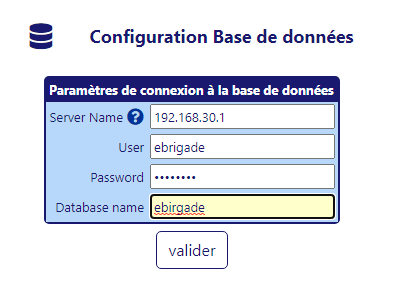
### 6.2) Création de la base de données

On tape les commandes suivantes :

Mysql

Une image contenant texte

Description générée automatiquement



### 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

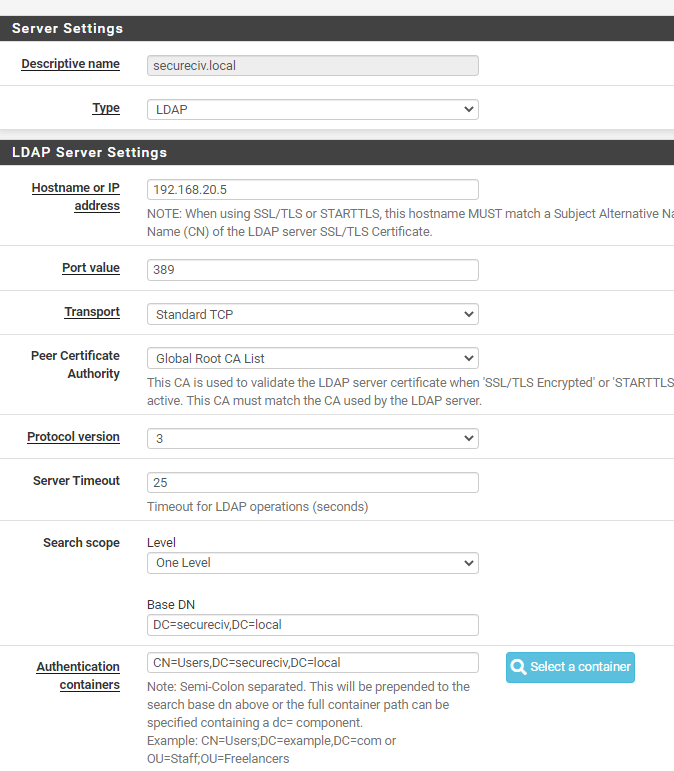
## 7) Mise en place VPN

### 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 :



Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquementNous 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 »

Une image contenant texte

Description générée automatiquement

Choisissez « LDAP » dans le type de server :

Sélectionnez le serveur que nous avons au préalablement lié

Une image contenant texte

Description générée automatiquement

Ensuite complété le Certificat d’autorité comme ci-dessous

Une image contenant table

Description générée automatiquement

Une image contenant texte

Description générée automatiquementPareil pour le certificat serveur

Pour continuer on configure les paramètres généraux de cette manière :

Une image contenant texte

Description générée automatiquement

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

Une image contenant texte

Description générée automatiquement

On oublie pas de cocher les deux case ci-dessous

Une image contenant texte

Description générée automatiquement

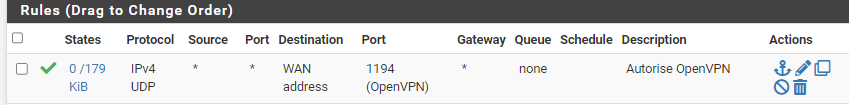
Notre serveur OpenVPN à bien été crée :

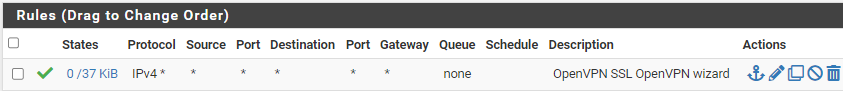
Une image contenant texte

Description générée automatiquement

### 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

Une image contenant texte

Description générée automatiquementPuis dans avalable Packages cherchez OpenVPN et installez le

Une image contenant texte

Description générée automatiquementvotre package à bien été installé nous allons pouvoir faire les test de connexion distante

### 7.5) Connexion VPN à distance :

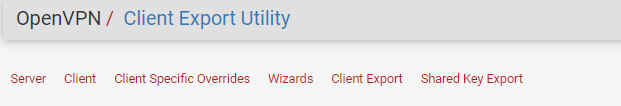
Nous allons installer OpenVPN sur une machine Windows qui ne se trouve pas dans le même réseau que notre Infra :

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

Une image contenant texte

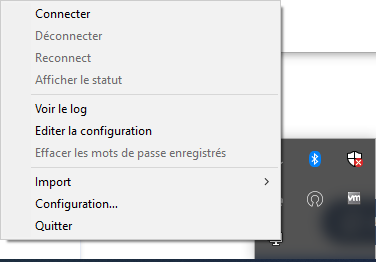
Description générée automatiquement

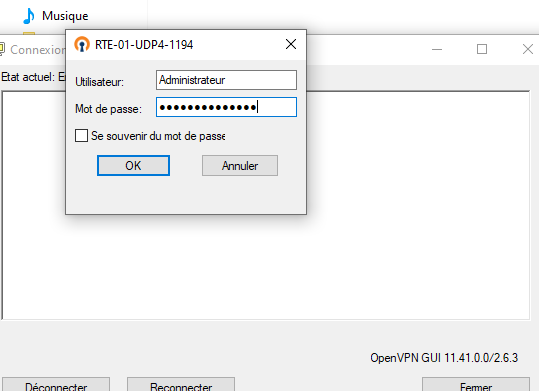
On extrait le fichier et on met les fichier contenu dans le dossier config de OpenVPN qui se trouve dans Programme/OpenVPN/ Config

Une image contenant texte

Description générée automatiquement

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