AP4 - LIVRABLE 2

La mise en œuvre d'une connexion distante permettant l'accès aux ressources et outils métiers par les agents de terrain.

GROUPE 7

Victor WARTH / Nicolas TANT

DOCUMENTATION TECHNIQUE

Table des matières

1) INSTALLATION D'UN WINDOWS SERVER 2022 AVEC AD, DHCP ET DNS

1.1) Prérequis

Prérequis pour la Configuration du Serveur Windows avec Active Directory, Serveur DHCP et Serveur DNS

1.1.1) Serveur Windows Server 2022 (VM)

- **Configuration minimale recommandée :**
  - Processeur : 2 cœurs ou plus
  - Mémoire : 2 Go de RAM
  - Espace de stockage : 20 Go d'espace disque disponible

1.1.2) Client Windows 10/11 (VM)

- **Configuration minimale recommandée :**
  - Processeur : 2 cœurs ou plus
  - Mémoire : 2 Go de RAM
  - Espace de stockage : 20 Go d'espace disque disponible

1.1.3) Carte Réseau VMware

- Assurez-vous que la carte réseau de chaque machine virtuelle est correctement configurée dans VMware.
- Désactivez toute configuration de serveur DHCP sur la carte réseau VMware.

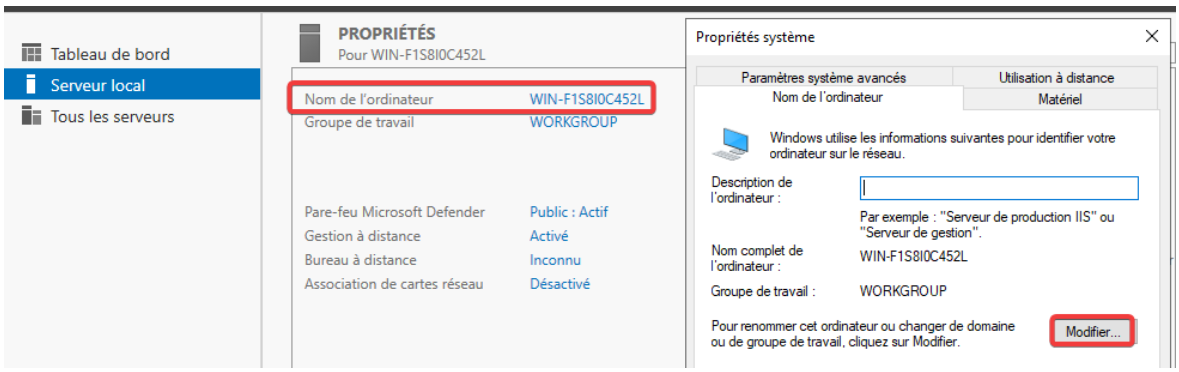
1.2) Pré configuration

<u>Remarque :</u> Il est important de vérifier et changer si besoin le nom du serveur ainsi que d'attribuer une adresse IP statique au serveur avant toute installation. En effet, cela peut créer des conflits si ces paramètres sont changés plus tard après installation de l'AD par exemple.

1.2.1) Changer le nom de l'ordinateur

Pour changer le nom de l'ordinateur il faut cliquer sur le nom de l'ordinateur inscrit dans la section Serveur local du gestionnaire de serveur, puis dans l'onglet « Nom de l'ordinateur » cliquer sur modifier et inscrire le nouveau nom de l'ordinateur.

NB: Il faut redémarrer le serveur pour que le changement de nom soit pris en compte. Dans notre cas nous le redémarreront par la suite.

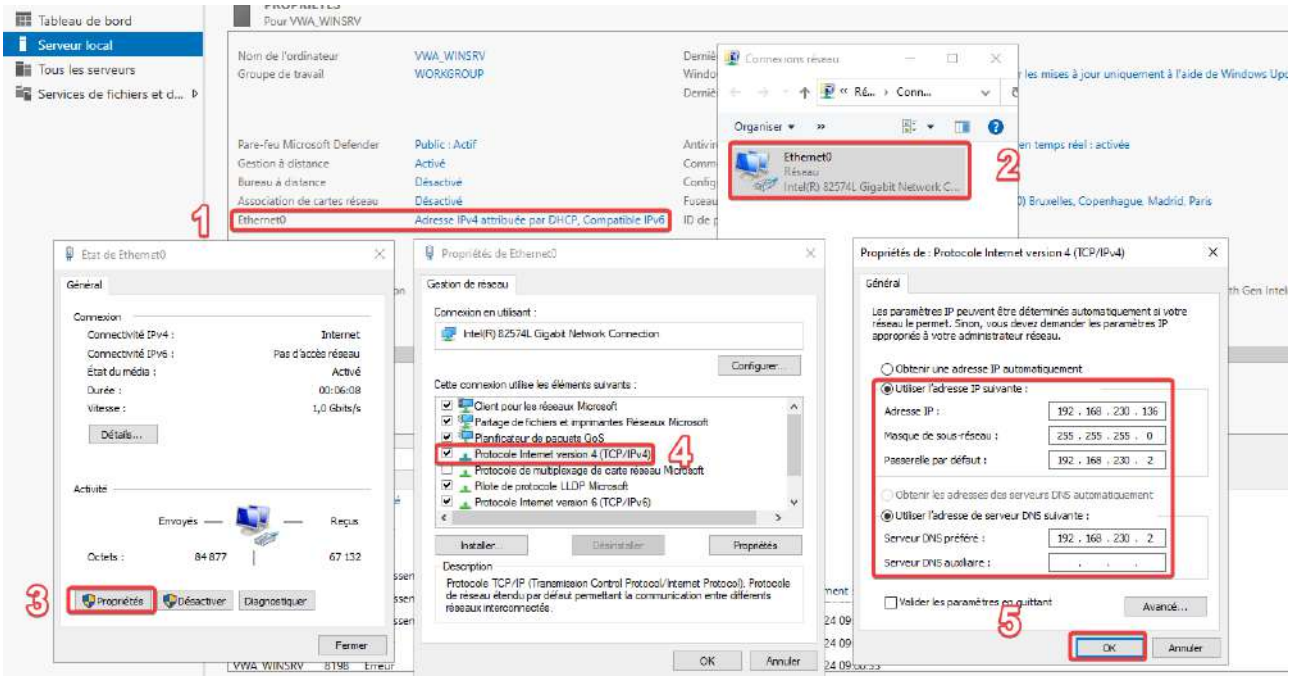


Gestionnaire de serveur > Serveur local > %Nom de l'ordinateur% > Nom de l'ordinateur > Modifier

1.2.2) Configurer une adresse IP statique

L'utilisation d'une adresse IP statique sur un serveur assure une stabilité d'accès et simplifie la gestion, évitant les changements d'adresse dynamique et facilitant la configuration réseau.

Pour attribuer manuellement une adresse IPv4 au serveur il faut cliquer sur la carte réseau **(1)** dans la section Serveur local du gestionnaire de serveur. Ensuite, sélectionné la carte réseau concernée, ici « Ethernet0 » **(2)** puis cliquer sur « Propriétés » **(3)**, « Protocole Internet version 4 » **(4)** enfin, sélectionner « Utiliser l'adresse IP suivante » et renseigner l'adresse IP désirée **(5)**.

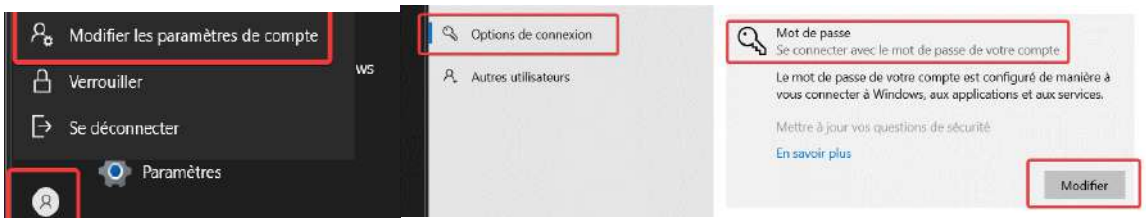


%Ethernet0% > %Ethernet0% > Propriétés > Protocole IPv4

1.2.3) Modification du mot de passe administrateur

Il faut modifier le mot de passe du compte Administrateur et utilisateur, si ce n'est pas fait cela peut créer des erreurs plus tard. (Mot de passe robuste nécessaire → L'utilisation d'un générateur de mot de passe s'avère être une bonne idée.)

Pour modifier le mot de passe d'un compte, il faut aller dans le menu Windows, puis cliquer sur l'icône de l'utilisateur en bas à gauche, puis sur « Modifier les paramètres de compte » puis dans la nouvelle page qui s'est ouverte cliquer sur l'onglet « Options de connexion », enfin, il faut développer la partie « Mot de passe » puis cliquer sur « Modifier »



Menu Windows > Utilisateur > Modifier les paramètres de compte > Options de connexion > Mot de passe

NB: Il ne faut pas oublier de modifier aussi le mot de passe sur le compte Administrateur (Se déconnecter puis se reconnecter sur la session administrateur)

Redémarrer le serveur.

1.3) Installation de l’Active Directory et du DHCP

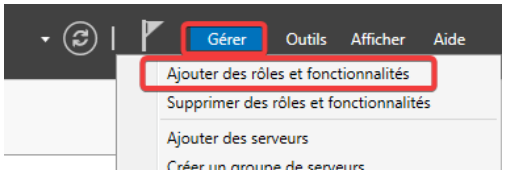
L'Active Directory (AD) est un service de répertoire développé par Microsoft, utilisé pour stocker des informations sur les ressources réseau, tels que les utilisateurs, les groupes, les ordinateurs, et les imprimantes, dans un environnement Windows. Il facilite l'organisation et la gestion des objets réseau, tout en permettant l'authentification et l'autorisation des utilisateurs et des services.

Le serveur DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP et d'autres paramètres de configuration réseau aux dispositifs connectés à un réseau. Il simplifie la gestion des adresses IP en évitant les conflits et en permettant une configuration automatique, ce qui est particulièrement utile dans les réseaux où les dispositifs se connectent et se déconnectent fréquemment.

1.3.1) Ajout des rôles et fonctionnalités

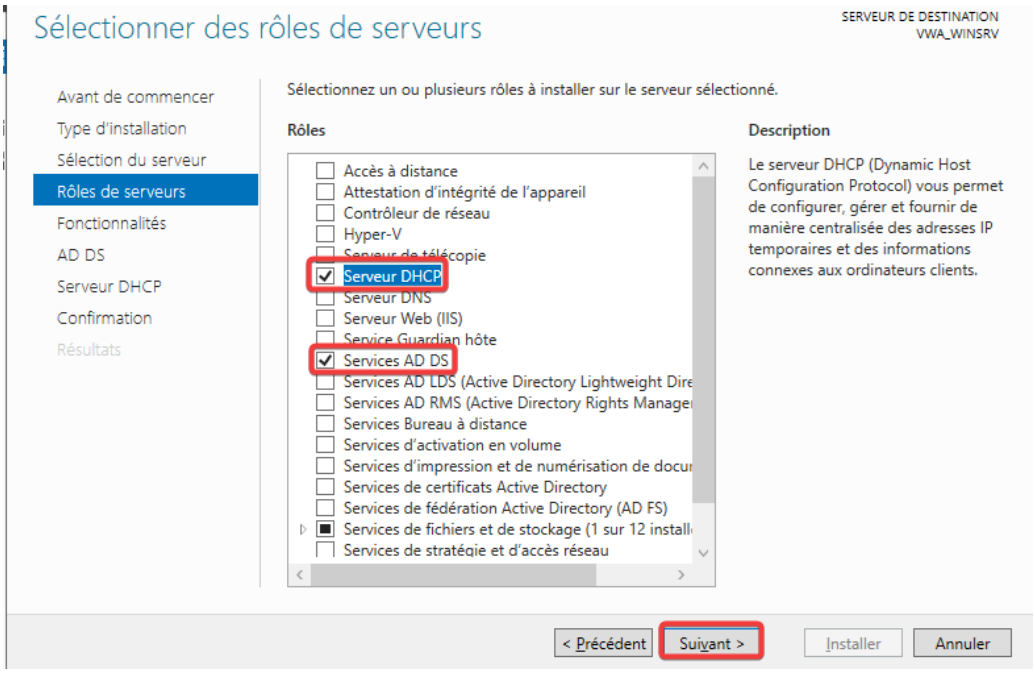
NB: L'Active Directory Domain Services (AD DS) regroupe un annuaire LDAP, un service DNS pour la gestion des domaines, et utilise le protocole Kerberos pour l'authentification des utilisateurs. Il n'est donc **pas nécessaire d'installer le rôle Serveur DNS** (cela peut même créer des conflits).

Pour ajouter les services AD DS et de serveur DHCP il faut cliquer sur « Gérer » puis « Ajouter des rôles et fonctionnalités » dans le gestionnaire de serveur.



Pour le « Type d'installation » on peut laisser par défaut, puis dans « Sélection du serveur » il faut sélectionner notre serveur.

Ensuite dans l'onglet « Rôles de serveurs » il faut sélectionner « Serveur DHCP » et « Services AD DS ». Ensuite cliquer sur suivant.



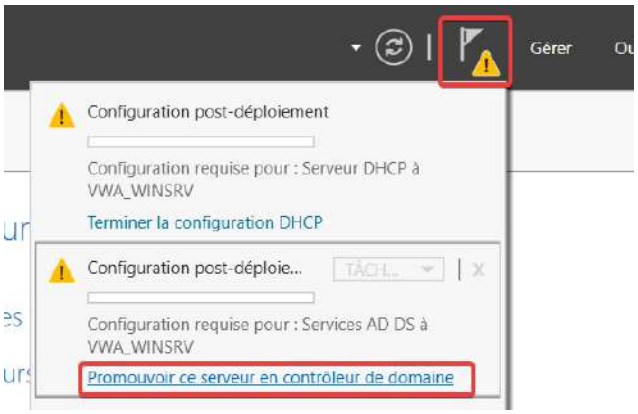
Pour le reste des onglets on peut laisser les paramètres par défaut et cliquer sur suivant et pour finir confirmer l'installation.

Redémarrer le serveur.

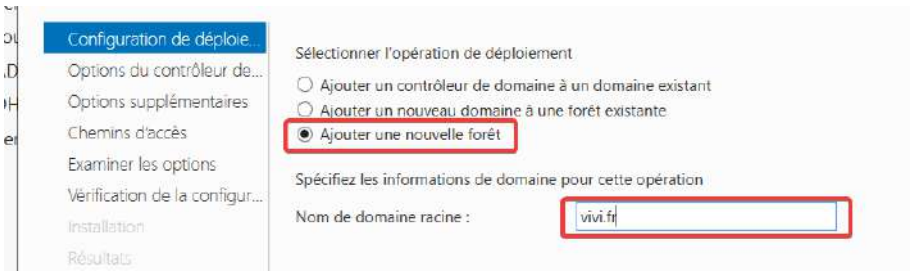
1.3.2) Configuration de l'AD DS

Afin d'utiliser l'AD DS il faudra encore réaliser quelques configurations. On peut notamment voir l'évolution de la configuration en cliquant sur le drapeau en haut a droite du gestionnaire de serveur.

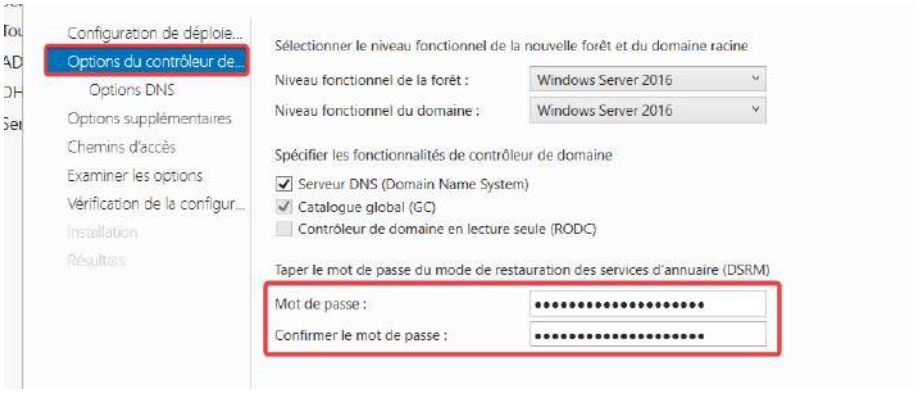
Pour commencer il faut cliquer sur le drapeau puis « Promouvoir ce serveur en contrôleur de domaine »



Dans la nouvelle fenêtre qui s'ouvre Il faut ensuite cliquer sur ajouter une nouvelle forêt (ne pas oublier l'extension dans notre cas « .fr »)

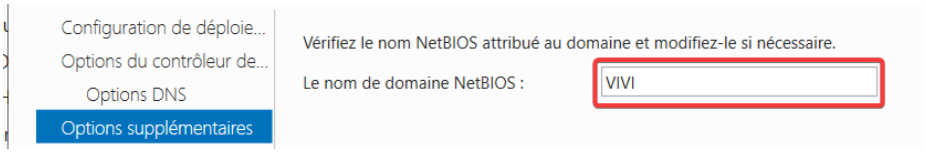


Puis on peut laisser les paramètres par défaut et mettre un mot de passe (Dans notre cas ce sera le même que celui de l'administrateur question de simplicité)



Ensuite, on ne souhaite pas ici créer de délégation DNS, on laisse donc la case décochée.

Dans l'onglet suivant, il faut mettre en nom de domaine NetBIOS le même nom que la nouvelle forêt (sans l'extension)



Pour les autres onglets on peut laisser les paramètres par défaut et confirmer l'installation.

Redémarrer le serveur.

1.3.3) Configuration du DHCP

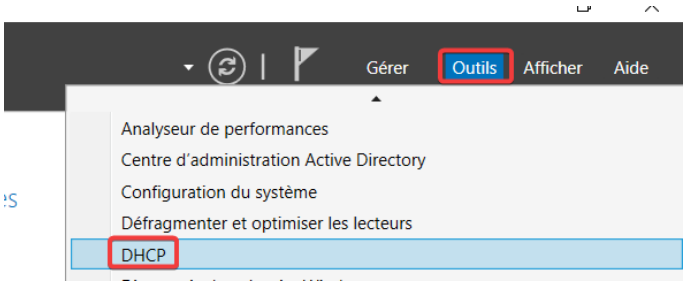
Pour mettre en place le serveur DHCP il faut finir la configuration.

Pour se faire, cliquer sur le drapeau puis sur « Terminer la configuration DHCP » depuis le gestionnaire de serveur.

Dans notre cas on peut laisser tous les paramètres de configuration par défaut.

Redémarrer le serveur.

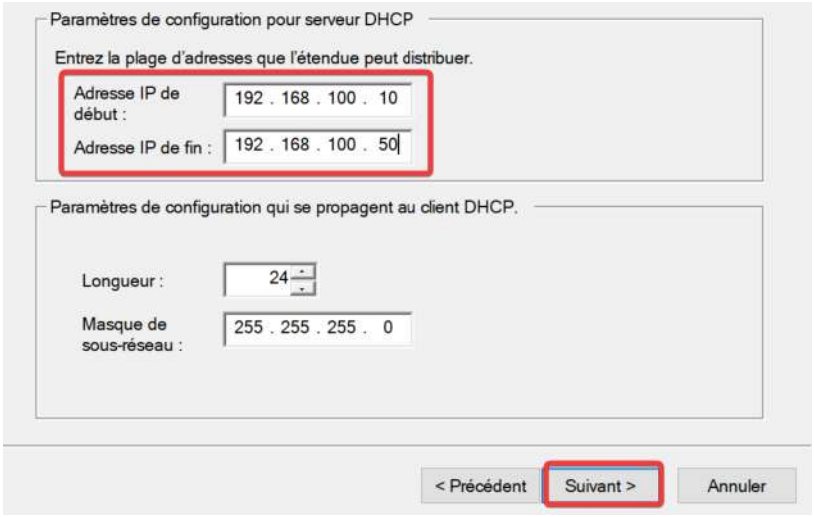
Après avoir redémarrer le serveur il faut maintenant donner dire au DHCP la configuration que l'on souhaite lui donner, pour faire cela il faut aller dans « Outils » puis « DHCP ».



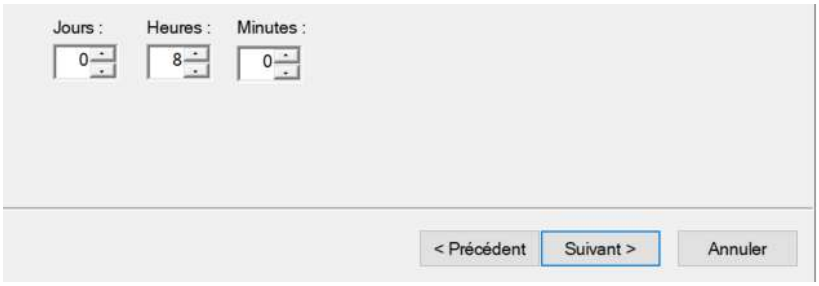
Dans la nouvelle fenêtre qui vient de s'ouvrir on peut développer notre serveur (composé de son nom suivi de notre nom de forêt avec l'extension). Puis il faut faire un clic droit sur « IPv4 » et sélectionner « Nouvelle étendue »

Ensuite, on peut donner un nom (sans importance) à cette étendue, puis, il faut définir la plage d'adresses que le DHCP va attribuer.

NB: Il faut que la plage d'adresse IP soit dans le même réseau que notre serveur.



Ensuite, il faut définir la durée du bail. Par principe on donne un bail de 8 heures.



Dans notre cas on peut laisser les autres paramètres par défaut, puis activer l'étendu.

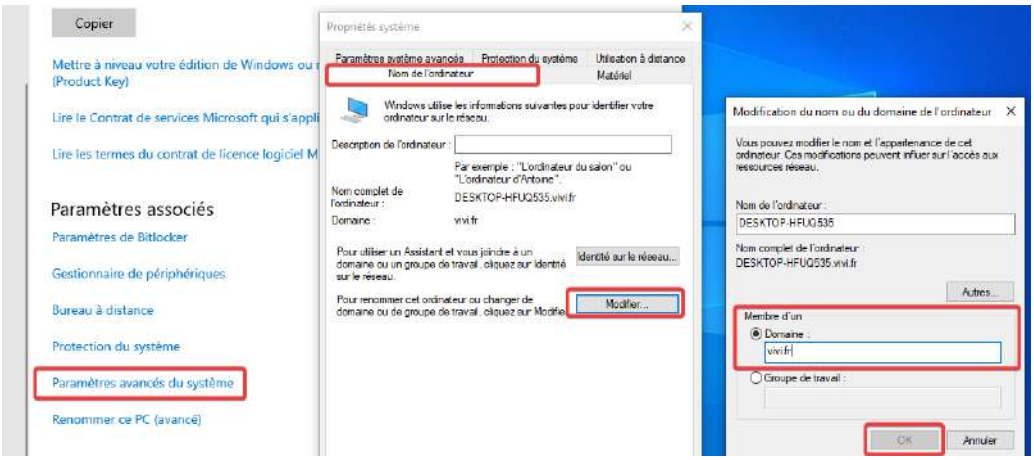
1.4) Exploiter le domaine

Après avoir créé notre domaine on peut maintenant l'utiliser, dans notre exemple pour des clients Windows.

1.4.1) Joindre le domaine

Pour joindre le domaine il faut avoir un client (ici un Windows 10) connecté sur la même interface réseau VMware et au même réseau que le Windows server.

Pour joindre le domaine il faut aller dans les paramètres, puis dans « système », « à propos », ensuite il faut cliquer sur « paramètres avancés du système ». Dans la nouvelle fenêtre qui s'ouvre il faut aller dans la catégorie « nom de l'ordinateur » puis sur « Modifier ». Enfin, « membre d'un » il faut sélectionner « Domaine » et renseigner le domaine avec son extension créé à l'étape 4.2.



Paramètre > Système > A Propos > Paramètres avancés du système > Nom de l'ordinateur > Modifier

On sera ensuite invité à renseigner les informations d'un compte administrateur de l'AD.

Redémarrer le PC

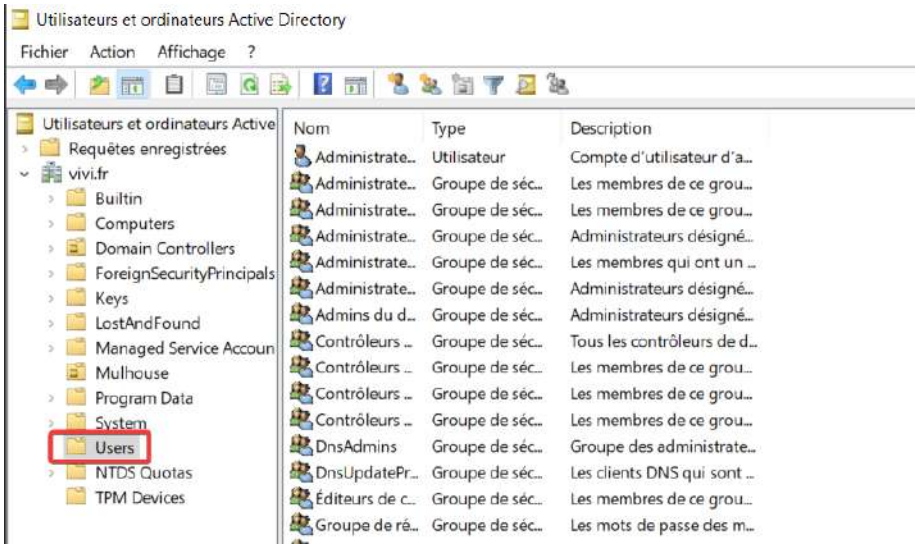
1.4.2) Créer un utilisateur/groupe

La mise en place d'utilisateurs et de groupes au sein de l'Active Directory est essentiel et renforce la gestion efficace des accès et des autorisations au sein de votre environnement informatique.

Pour créer un utilisateur ou un groupe il faut suivre la même procédure de départ.

Pour commencer rendez-vous dans « Outils » puis « Utilisateurs et ordinateurs Active Directory » sur le gestionnaire de serveur.

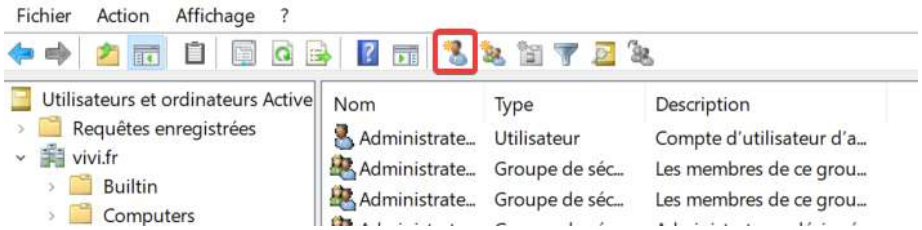
Dans la nouvelle fenêtre qui s'ouvre, vous pouvez développer votre domaine, dans notre cas « vivi.fr », puis on se positionner dans le dossier « Users ».



On peut voir que le dossier contient déjà des utilisateurs génériques générés au moment de la création de l'AD.

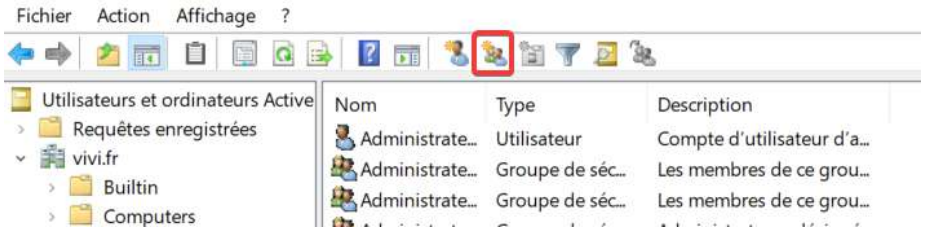
1.4.2 bis) Créer un utilisateur

Pour ajouter un utilisateur il suffit de cliquer sur bouton « Créer un nouvel utilisateur dans le conteneur actuel » puis il suffit de renseigner les informations que vous souhaitez.



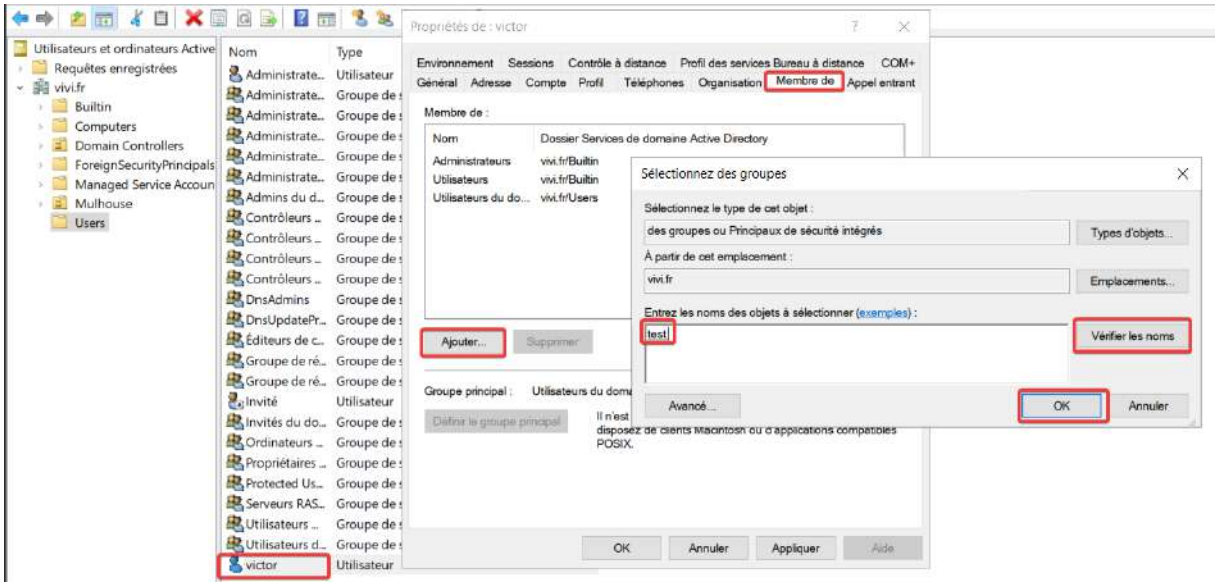
1.4.2 bis) Créer un groupe

Pour créer un groupe il faut cliquer sur le bouton « Créer un nouveau groupe dans le conteneur actuel » puis renseigner les informations que l'on souhaite.



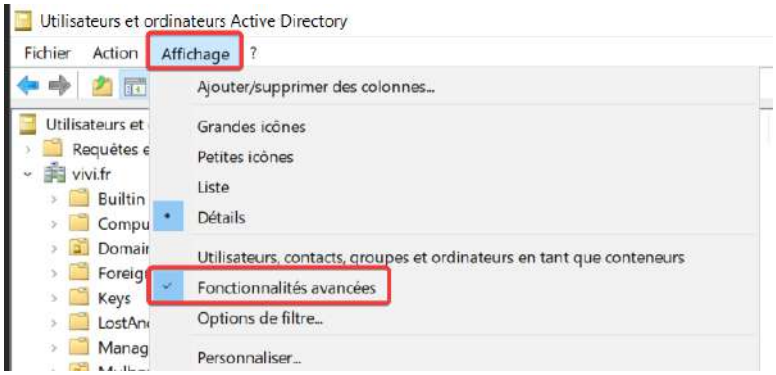
1.4.2 bis) Attribuer un groupe

Pour attribuer un groupe à un utilisateur, il faut double cliquer sur un utilsiateur, ensuite aller dans l'onglet « Membre de » puis cliquer sur « Ajouter ». Il suffit de donner le nom des groupes que l'on souhaite attribuer (il est possible d'en attribuer plusieurs en même temps), pour être certain d'attribuer le bon groupe on peut cliquer sur « vérifier les noms », si le nom du groupe se souligne alors le groupe a été trouvé, dans le cas ou le nom du groupe n'est pas trouvé ou incomplet, une nouvelle fenêtre de sélection s'ouvre.

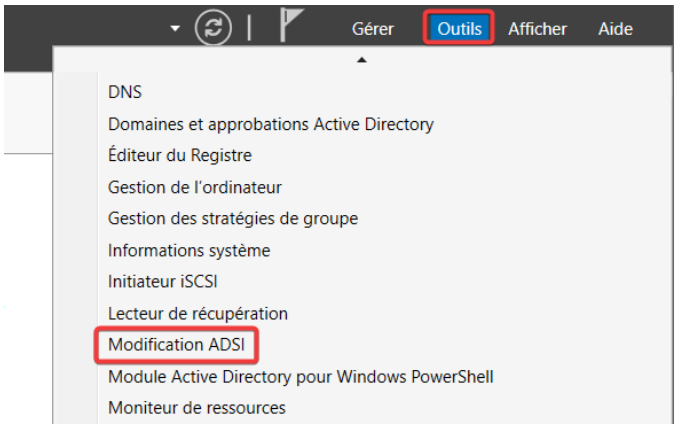


1.4.2 bis) Créer un conteneur

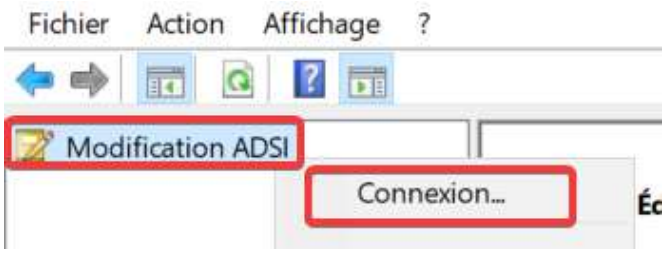
NB: Les conteneurs que nous nous apprêtons à créer sont seulement visible si l'option d'affichage des fonctionnalités avancées est activée.



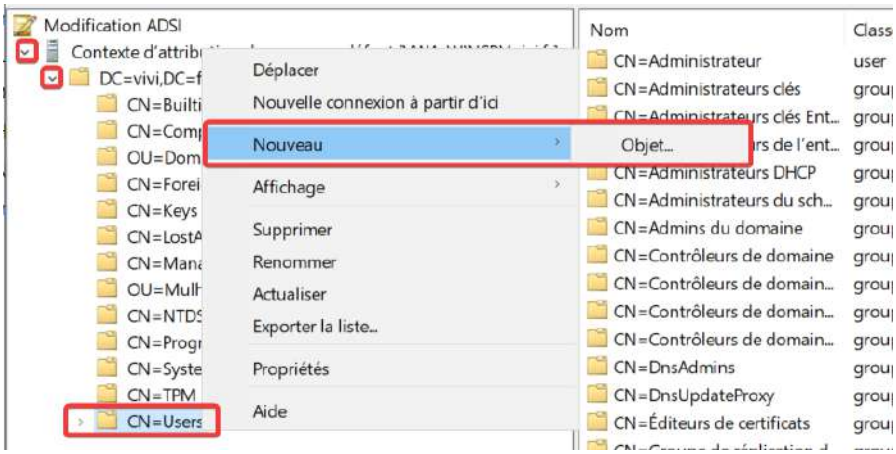
Pour créer un conteneur, il faut se rendre dans « Outils » puis « Modification ADSI »



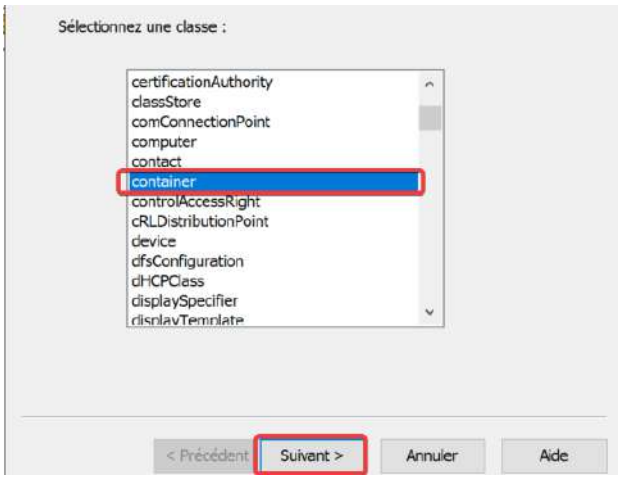
Dans la nouvelle fenêtre qui s'ouvre il faut faire clic droit sur « Modification ADSI » puis « Connexion », ensuite on laisse les paramètres par défaut et on clique sur « Ok »



Par la suite, il faut développer votre nouvelle connexion puis le domaine, puis faire clic droit sur le dossier de votre choix, dans notre cas « Users », puis « Nouveau », « Objet ».



Il faut ensuite cherche l'objet « Container », puis il ne vous reste plus qu'a appuyer sur suivant et le créer.



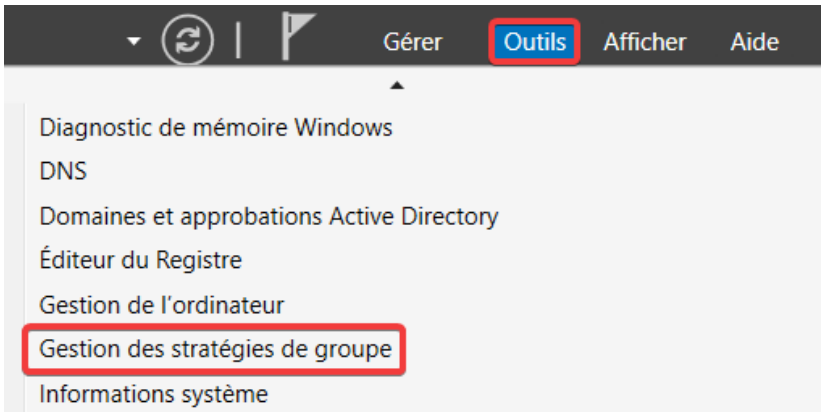
1.4.3) Modifier une GPO

Une GPO (Group Policy Object) est un ensemble de règles de configuration dans un domaine Windows, permettant aux administrateurs de définir des paramètres pour les ordinateurs et utilisateurs, assurant ainsi une gestion centralisée et cohérente des configurations.

Dans notre cas nous allons changer la politique de mot de passe afin de simplifier les accès au serveur.

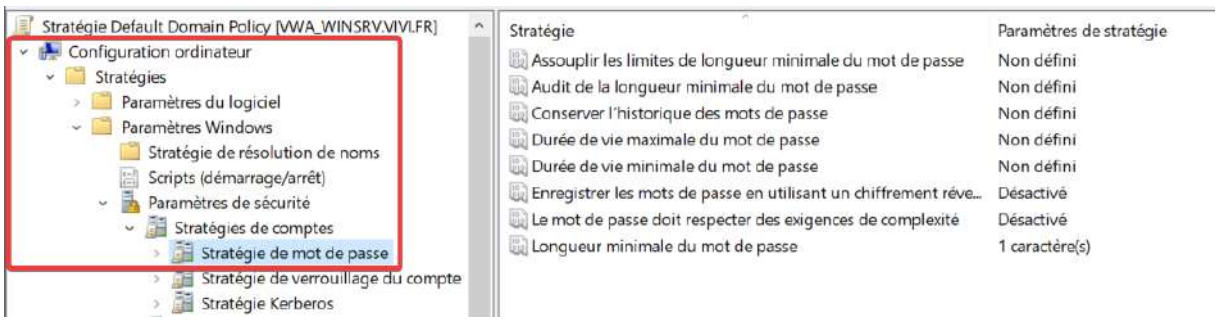
NB: Pour des raisons de sécurité évidentes, il n'est pas recommandé de baisser les exigences au minimum de la politique de mot de passe comme nous allons le faire.

Pour accéder aux GPO, il faut cliquer sur « Outils » puis dans « Gestion des stratégies de groupe » depuis le gestionnaire de serveur.

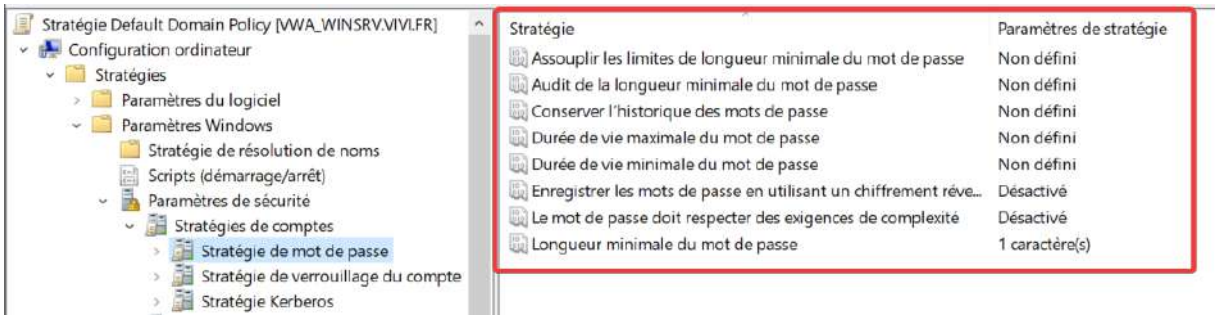


Puis dans la nouvelle fenêtre qui s'ouvre il faut développer la forêt puis « Domaines » puis votre domaine, dans notre cas « vivi.fr ». Ensuite, vous pouvez faire un clic droit sur « Default Domain Policy » enfin cliquer sur « Modifier ».

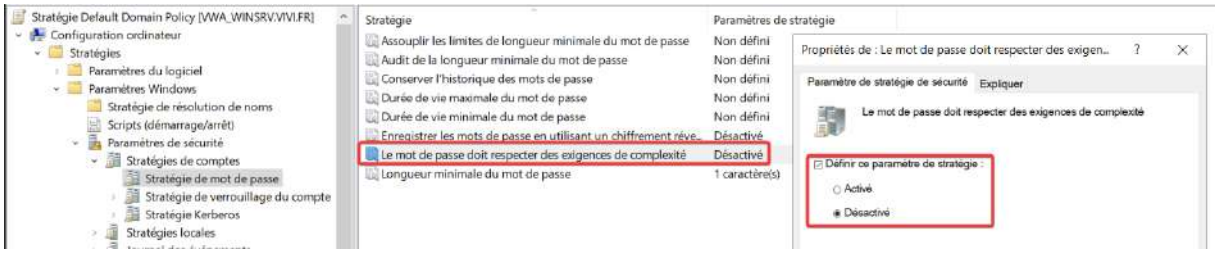
Dans la nouvelle fenêtre il faut développer « Configuration ordinateur », ensuite « Stratégies », puis « Paramètres Windows » et enfin « Paramètres de sécurité ». La stratégie qui nous intéresse dans notre cas est « Stratégie de mot de passe ».



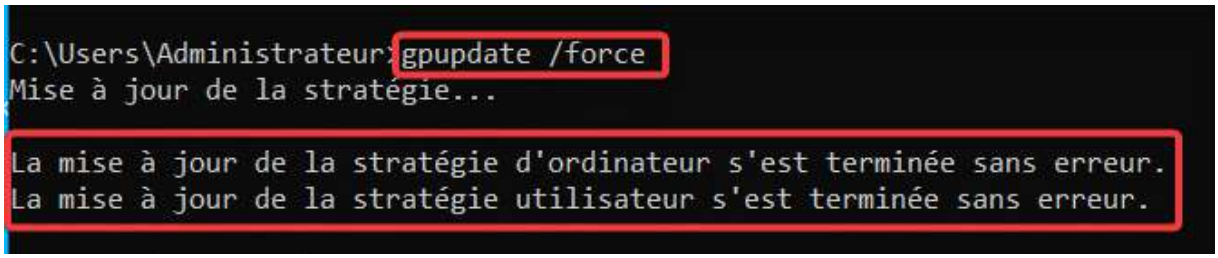
Après avoir cliqué sur « Stratégie de mot de passe » on peut voir dans la partie droite de la fenêtre l'ensemble des stratégies de mot de passe.



A l'aide d'un double clic sur une stratégie il est possible de modifier sa valeur. Dans notre cas, j'ai désactivé la stratégie qui impose une certaine complexité des mots de passe. N'oubliez pas de cliquer sur « Appliquer ».



Si la stratégie n'a pas été prise en compte directement il est possible de forcer son renouvellement en exécutant la commande « gpupdate /force » dans une invite de commande exécuté en administrateur sur le serveur.



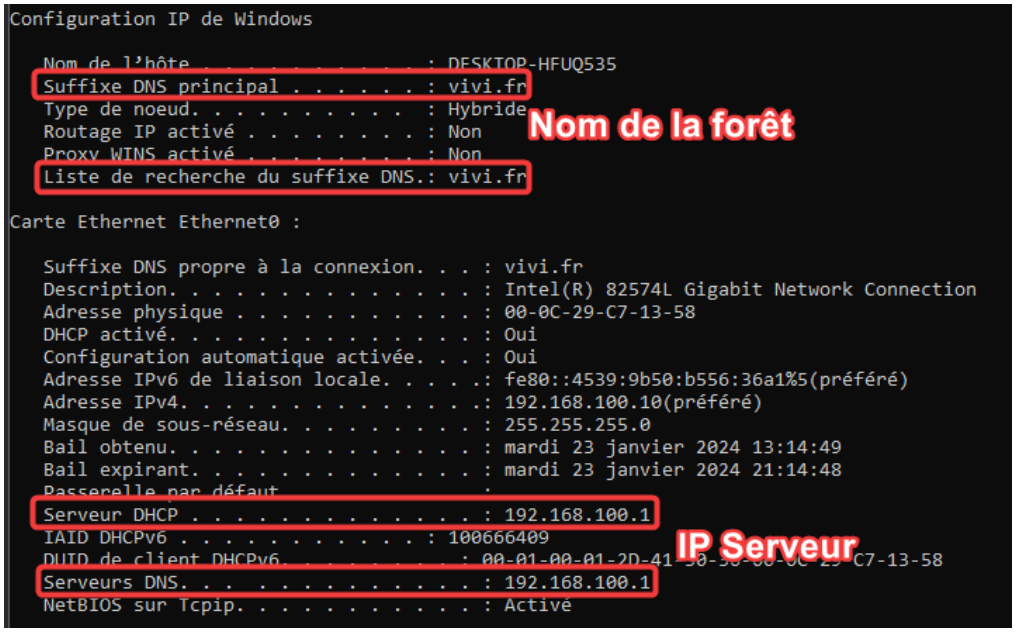
1.4.4) Vérification du domaine sur le PC

1.4.4 bis) Par ligne de commande

Avec la commande « ipconfig /all » il est possible de vérifier le suffixe DNS ainsi que l'adresse du serveur DHCP et du serveur DNS.

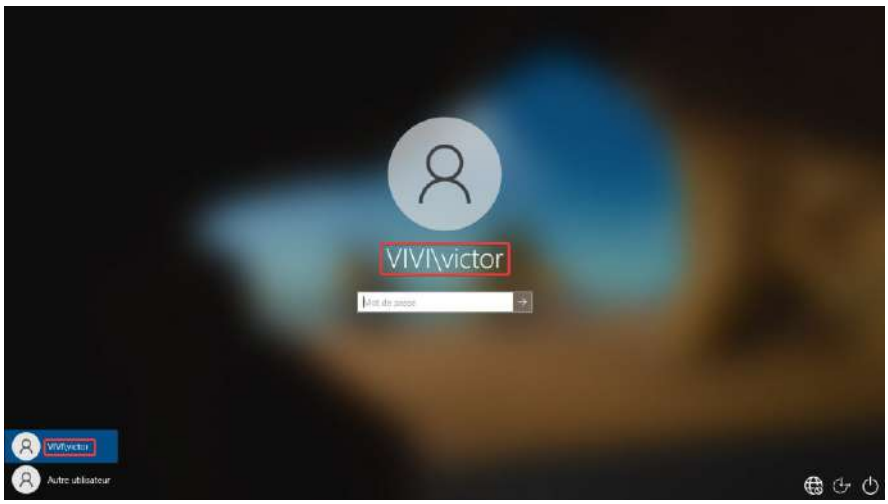
Le suffixe DNS doit correspondre au nom de la forêt donnée dans le contrôleur de domaine.

Les serveurs DHCP et DNS doivent bien être ceux configurer dans le DHCP du serveur (dans notre cas l'IP de ce même serveur).



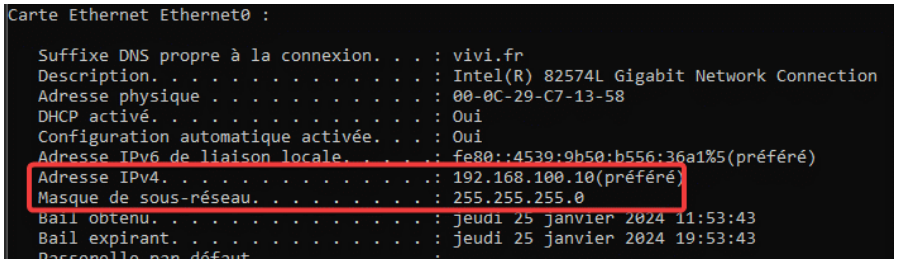
1.4.4 bis) Par interface graphique

Au moment de la connexion a un utilisateur il est possible de se connecter à un compte de l'Active Directory si vous avez bien joint le domaine. Cela se traduit par le nom NetBios du domaine dans notre cas « VIVI »



1.4.5) Vérification du DHCP sur le PC

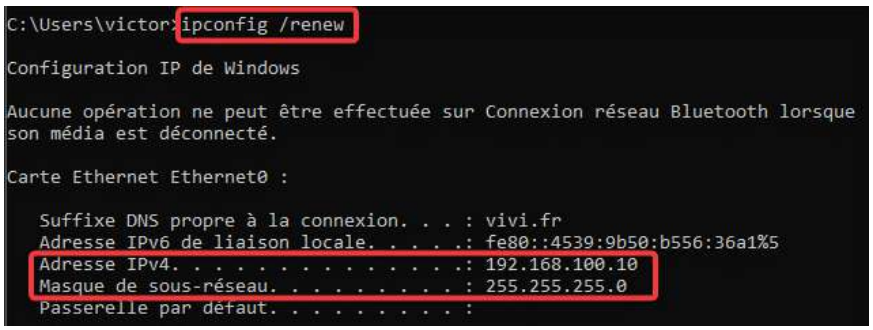
Il est possible de vérifier le bon fonctionnement du serveur DHCP sur un poste client. Tout d'abord on peut regarder la configuration de l'IPv4 actuelle avec la commande « ipconfig /all »



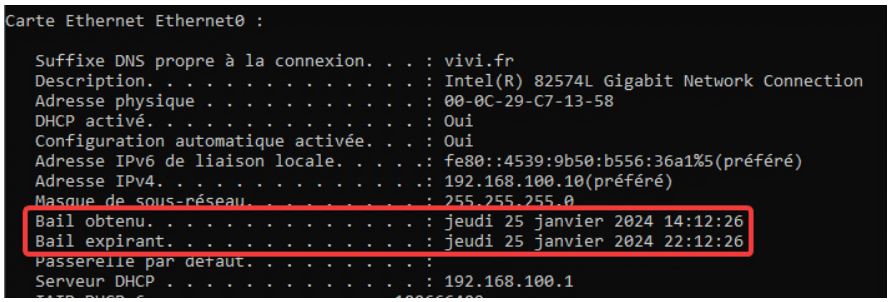
On retrouve bien dans notre cas une adresse contenu dans la plage que l'on a paramétrer dans notre serveur DHCP.

On peut ensuite utiliser les commandes « ipconfig /release » et « ipconfig /renew » qui permettent de résilier et renouveler le bail DHCP. On commence par faire « ipconfig /release » afin de résilier le bail dans un premier temps. On note bien qu'il n'y a plus d'adresse IPv4 ni de masque de sous-réseau attribués à notre machine.

Ensuite on renouvelle le bail avec « ipconfig /renew ». On peut observer qu'une nouvelle adresse IPv4 nous a été attribuée (dans notre cas la même que précédemment) qui est toujours contenu dans la plage de notre serveur DHCP.



On peut voir que le bail a bien été renouvelé avec à la commande « ipconfig /all ».



1.5) Redondance

Afin d'assurer la continuité des services et renforcer la fiabilité de notre infrastructure informatique il est possible de mettre en place des solutions de redondance pour nos serveurs Windows.

1.5.1) Pré configuration

Sur un nouveau Windows serveur ayant la même version que l'autre (ce n'est pas une obligation, tout dépend du niveau fonctionnel du domaine et de la forêt), il faut suivre les étapes du chapitre 3. Pré configuration.

Lors de l'étape 3.2 Configurer une adresse IP statique il est nécessaire de modifier les DNS de la façon suivante :

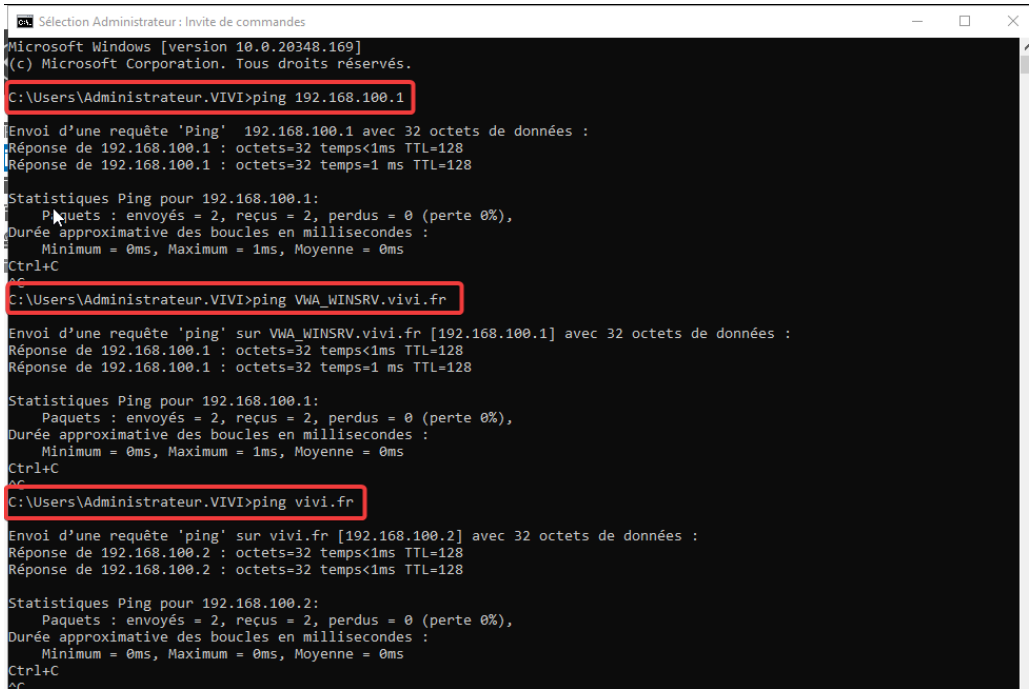
Il faut mettre en Serveur DNS préféré l'adresse IP du premier serveur que l'on a configuré. Et dans DNS auxiliaire il est nécessaire de mettre l'adresse de boucle (127.0.0.1) donc lui-même.

1.5.2) Connection au domaine

1.5.2 bis) Vérification des flux réseau

Il faut vérifier que notre nouveau serveur puisse joindre le premier.

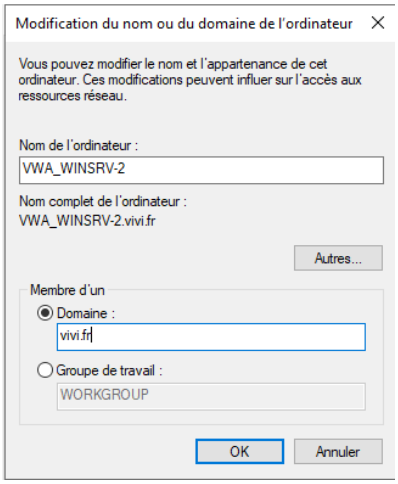
Dans un terminal sur le nouveau windows serveur, tenter de ping l'IP du premier serveur (ici 192.168.100.1) puis son nom complet FQDN (ici VWA_WINSRV.vivi.fr) et enfin le domaine (ici vivi.fr)



Si vous arrivez à ping toutes ces instances alors vous pouvez passer à la suite. Sinon, il faudra vérifier les différentes configurations réalisées précédemment.

1.5.2 bis) Joindre le serveur au domaine

On va ensuite joindre le serveur au domaine comme à l'étape 5.1 Joindre le domaine. La configuration donnera cela dans notre cas :



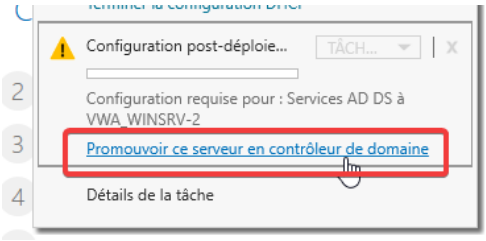
Puis redémarrer le serveur.

Au redémarrage, il est nécessaire de se connecter avec un compte d'administrateur du domaine pour la suite de la configuration.

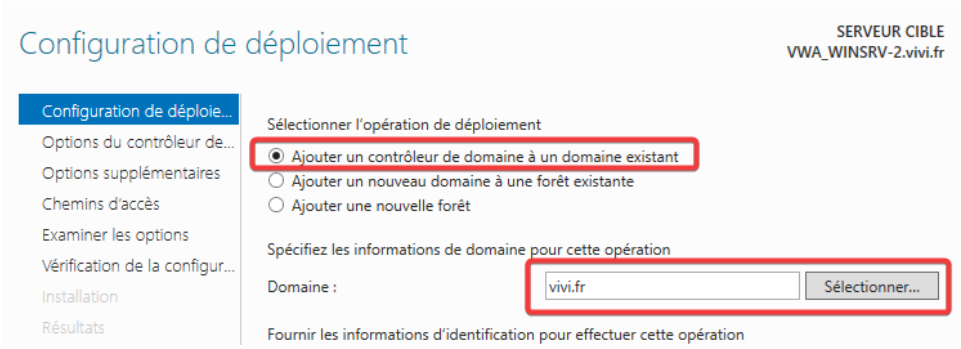
Enfin, il faut ajouter le rôle AD DS et DHCP sur le nouveau serveur.

1.5.3) Configuration des rôles

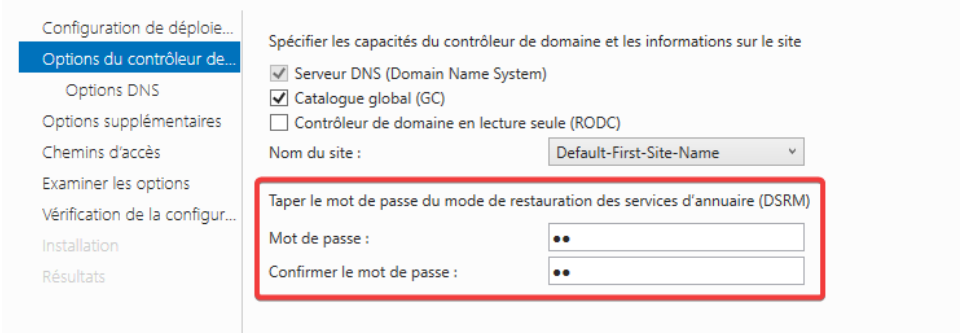
Tout d'abord depuis le gestionnaire de serveur, il faut cliquer sur le petit drapeau, puis sur promouvoir ce serveur en contrôleur de domaine.



Ensuite, on va ajouter le contrôleur de domaine à un domaine existant, il est nécessaire de renseigner le domaine, comme ci-dessous :



Puis il va falloir rentrer le mot de passe DSRM



Puis on peut cliquer sur suivant pour le reste des paramètres et installer.

Enfin, le serveur va redémarrer.

L'actualisation de l'AD peut prendre plusieurs minutes à se faire.

Pour le serveur DHCP, il suffit de cliquer sur le petit drapeau depuis le gestionnaire de serveur et de suivre les étapes pour terminer la configuration (tout laisser par défaut).

Redémarrer le serveur.

1.5.4) Vérification de la redondance

Afin d'être sûr que la redondance fonctionne correctement, il est possible de faire la vérification suivante :

Tout d'abord, depuis un client Windows 10 du domaine, il faut ping le domaine, dans notre cas « vivi.fr ».

```
C:\Users\vivi>ping vivi.fr

Envoi d'une requête 'ping' sur vivi.fr [192.168.100.1] avec 32 octets de données :
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.100.1 : octets=32 temps=2 ms TTL=128
Réponse de 192.168.100.1 : octets=32 temps<1ms TTL=128
```

La commande nous retourne l'adresse IP du premier serveur Windows.

Ensuite, il faut éteindre ce serveur Windows (192.168.100.1 dans notre cas) et recommencer la commande ping sur notre domaine.

```
C:\Users\vivi>ping vivi.fr

Envoi d'une requête 'ping' sur vivi.fr [192.168.100.2] avec 32 octets de données :
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=128
Réponse de 192.168.100.2 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.100.2 : octets=32 temps<1ms TTL=128
Réponse de 192.168.100.2 : octets=32 temps=1 ms TTL=128
```

Cette fois-ci la commande retourne l'adresse IP du deuxième serveur Windows.

On constate donc que le deuxième serveur a bien le relais, la redondance est donc fonctionnelle.

2) INSTALLATION ET CONFIGURATION D'UN HOMELAB PROXMOX

2.1) Prérequis

Pour monter un hyperviseur Proxmox, il est nécessaire d'avoir une machine suffisamment puissante. Dans notre cas, voici les spécifications techniques de la machine utilisée :

- CPU : Intel Core i7-10700F (8c/16t)
- RAM : 32 Go RAM DDR4 3600 MHz
- STOCKAGE : 1 To M.2 PCIe 3.0 NVMe

> ⓘ INFO
>
> Si vous souhaitez joindre l'hyperviseur depuis Internet, il sera nécessaire d'avoir une connexion Internet.

2.2) Installation de l'OS

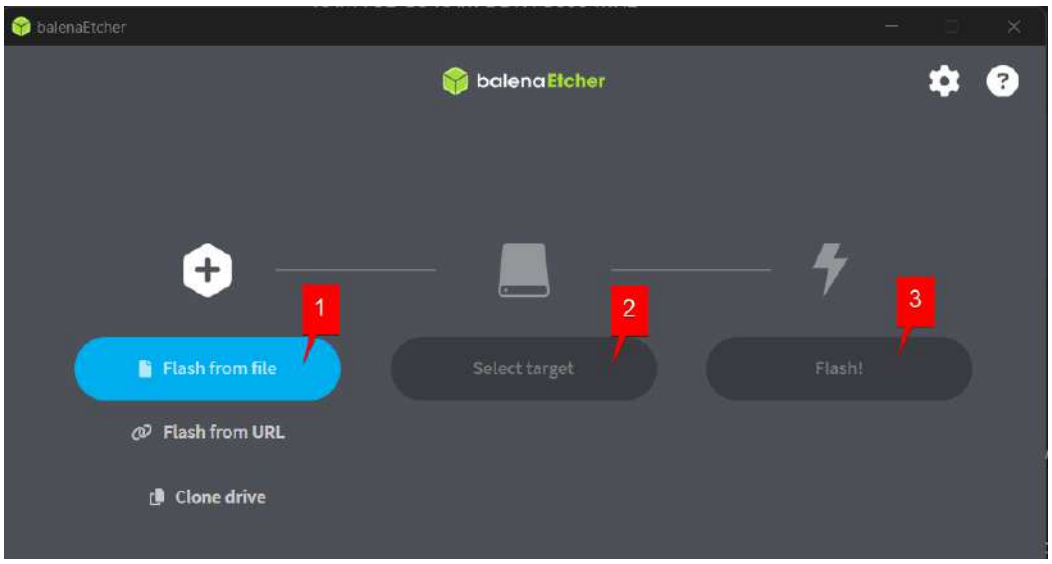
2.2.1) Préparation du support d'installation

Pour commencer, il sera nécessaire de télécharger la dernière version de Proxmox VE (8.2 dans notre cas) : https://www.proxmox.com/en/downloads

Ensuite, il va falloir préparer le support d'installation, dans notre cas, une clé USB bootable.

Pour rendre la clé USB bootable, il est possible d'utiliser un logiciel gratuit comme BalenaEtcher par exemple : https://etcher.balena.io/ :

1. On choisit notre ISO Proxmox VE
2. On sélectionne notre clé USB à rendre bootable
3. On Flash !

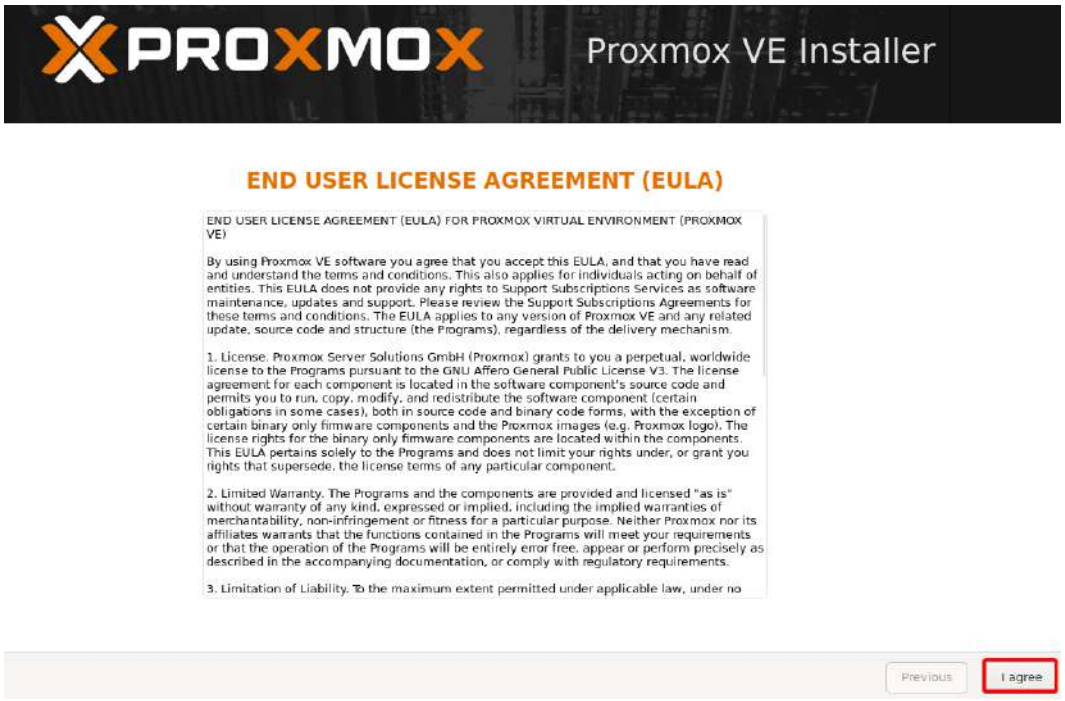


Puis, il ne reste plus qu'à vérifier que la virtualisation est activée dans le BIOS de notre machine et lancer la machine sur l'UEFI de la clé USB bootable.

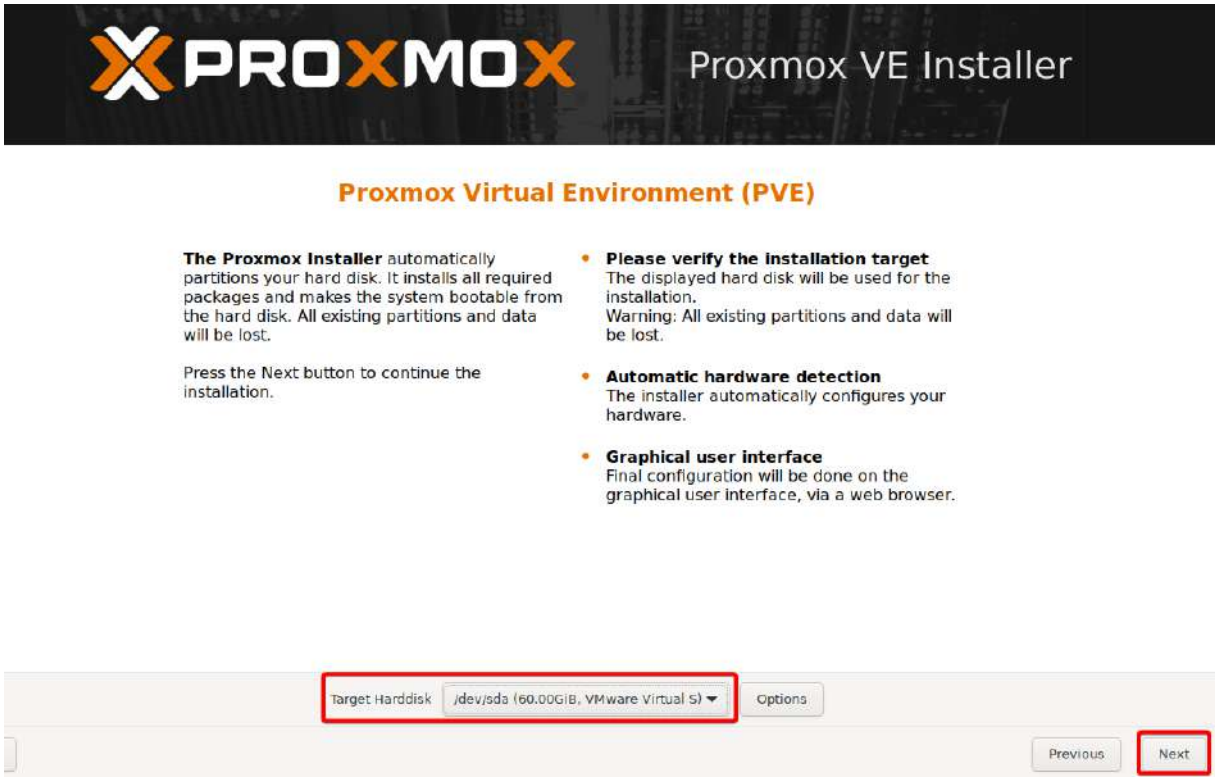
2.2.2) Installation

Dans notre cas, nous allons faire une installation classique :

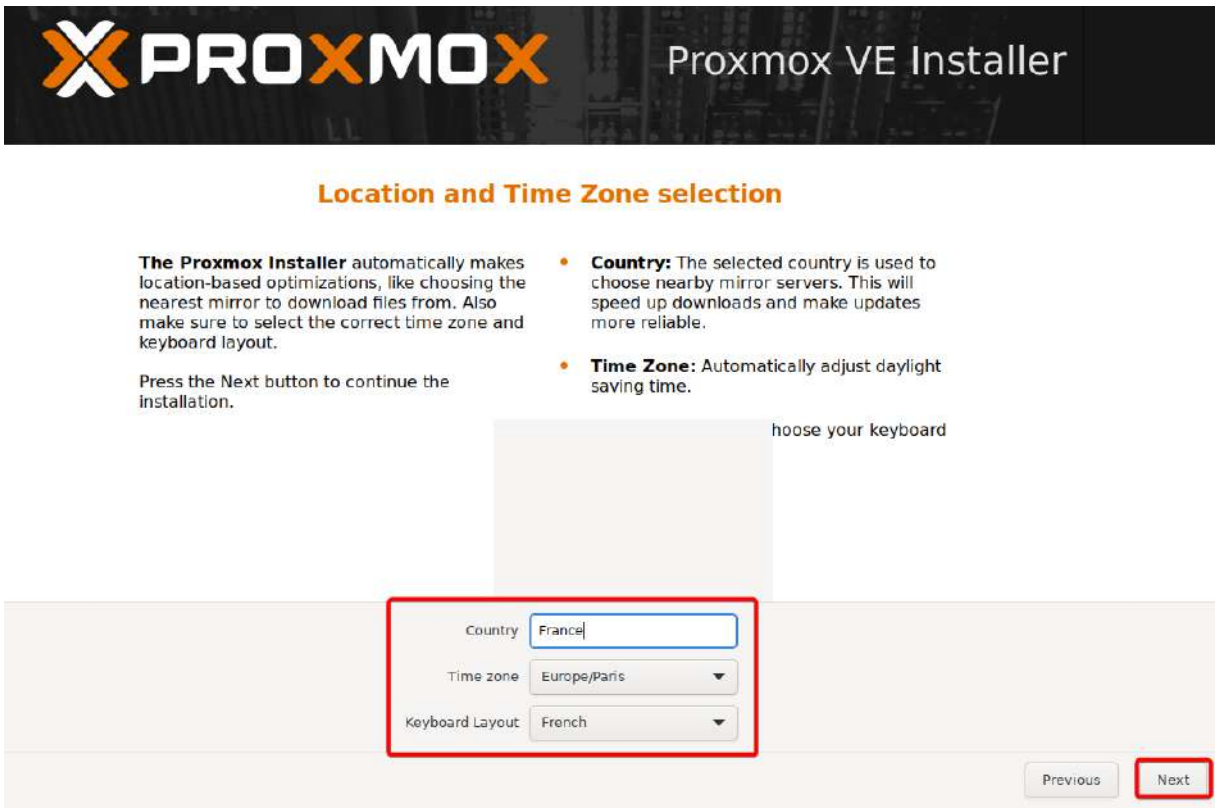
On accepte ensuite l'EULA :



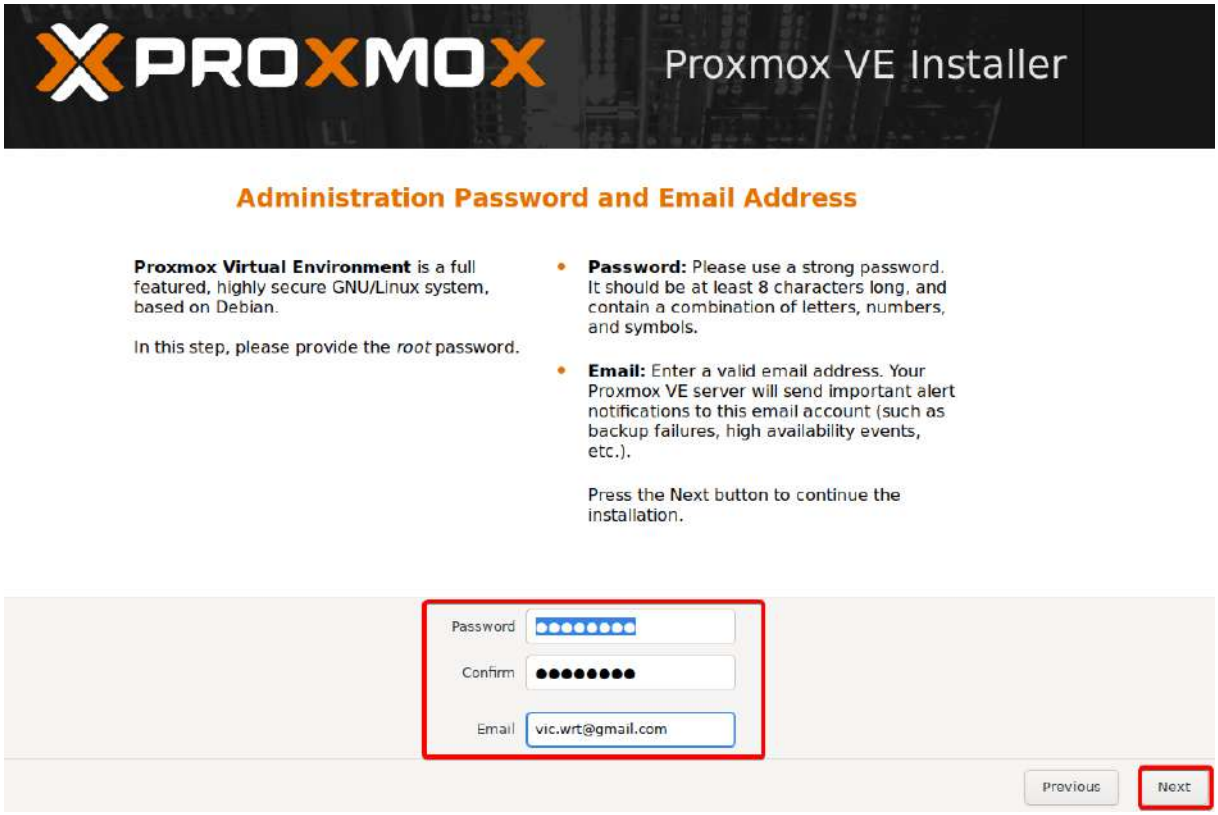
On choisit le disque d'installation :



Puis, la région ainsi que la disposition du clavier :



Ensuite, il faut renseigner le mot de passe root et un email au cas où :



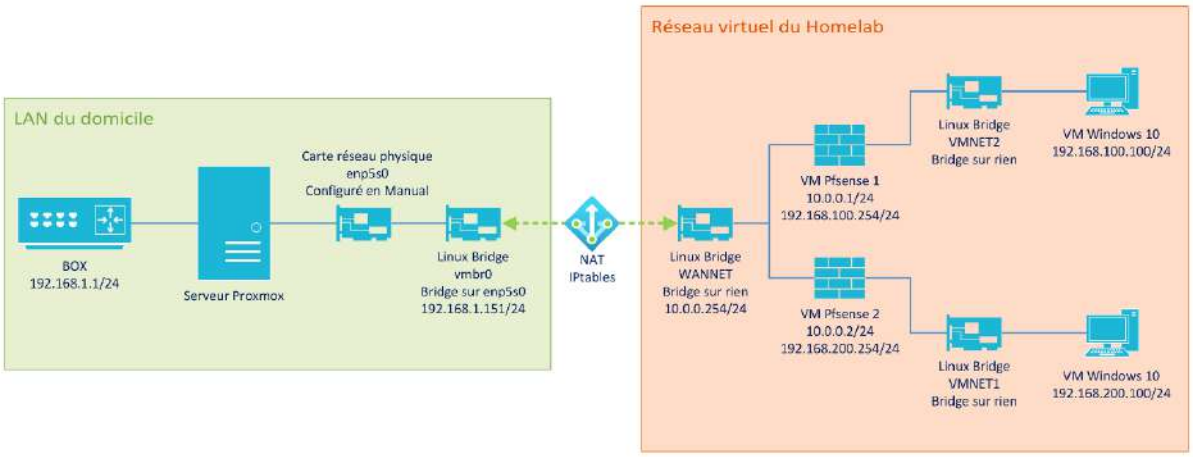
Enfin, on peut renseigner le nom FQDN et les différentes IP (Passerelle, DNS, etc...) :

Il est temps de cliquer sur installer :

2.3) Configuration réseau

2.3.1) Théorie

Dans le cadre d'un home lab, il peut être judicieux de ne pas bridge les VM directement sur notre réseau. Nous allons donc mettre en place une interface réseau virtuelle (Linux bridge) qui ne sera bridge sur aucune interface réseau physique, et pour que le trafic vers Internet passe, nous allons faire du forward (NAT) avec IPtables. Voici un schéma reprenant le fonctionnement :



Cela permet d'isoler notre réseau virtuel et de simuler un "WAN" entre le Linux Bridge WANNET et les VMNET1 et VMNET2 sans pour autant provoquer des conflits sur notre LAN.

2.3.2) Configuration interfaces réseau

Pour commencer, nous allons nous connecter en SSH sur notre serveur proxmox :

```
# Dans un cmd.exe se connecter en root en ssh
ssh root@IP_PROXMOX
```

Supprimer les source.list enterprise et ajouter le dépôt community :

```
# Modifier le premier dépôt enterprise
nano /etc/apt/sources.list.d/pve-enterprise.list

# Commenter la ligne suivante
deb https://enterprise.proxmox.com/debian/pve bookworm pve-enterprise

# Modifier le second dépôt
nano /etc/apt/sources.list.d/ceph.list

# Commenter la ligne suivante
deb https://enterprise.proxmox.com/debian/ceph-quincy bookworm enterprise

# Modifier les dépôts
nano /etc/apt/sources.list

# Ajouter la ligne suivante dans le sources.list
deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription

# Mettre à jour les dépôts
apt update
```

Puis modifier nos interfaces réseau :

```
# modifier les interfaces réseau
nano /etc/network/interfaces
```

Notre fichier de configuration devrait ressembler à cela :

```
auto lo
iface lo inet loopback
iface enp5s0 inet manual

auto vmbr0
iface vmbr0 inet static
        address 192.168.1.151/24
        gateway 192.168.1.1
        bridge-ports enp5s0
        bridge-stp off
        bridge-fd 0
```

```
source /etc/network/interfaces.d/*
```

Nous allons donc rajouter les interfaces virtuelles souhaitées :

```
auto WANNET
iface WANNET inet static
      address 10.0.0.254/24
      bridge-ports none
      bridge-stp off
      bridge-fd 0

auto VMNET1
iface VMNET1 inet static
      bridge-ports none
      bridge-stp off
      bridge-fd 0

auto VMNET2
iface VMNET2 inet static
      bridge-ports none
      bridge-stp off
      bridge-fd 0
```

Ce qui devrait nous donner :

```
auto lo
iface lo inet loopback

iface enp5s0 inet manual

auto vmbr0
iface vmbr0 inet static
      address 192.168.1.151/24
      gateway 192.168.1.1
      bridge-ports enp5s0
      bridge-stp off
      bridge-fd 0

auto WANNET
iface WANNET inet static
      address 10.0.0.254/24 #cette IP sera utilisé comme "passerelle" pour le NAT
      bridge-ports none
      bridge-stp off
      bridge-fd 0

auto VMNET1
iface VMNET1 inet static
```

```
        bridge-ports none
        bridge-stp off
        bridge-fd 0

auto VMNET2
iface VMNET2 inet static
        bridge-ports none
        bridge-stp off
        bridge-fd 0

source /etc/network/interfaces.d/*
```

Ensuite, nous pouvons redémarrer le service networking et désactiver/réactiver chaque interface virtuelle créée :

```
# redémarrer le service networking
 systemctl restart networking

# redémarrer chaque interface
ifdown WANNET && ifup WANNET
ifdown VMNET1 && ifup VMNET1
ifdown VMNET2 && ifup VMNET2
```

2.3.3) Configuration du NAT IPtables

Il faut ensuite configurer le NAT entre les interfaces vmbr0 et WANNET.

Tout d'abord, il faut autoriser le forwarding IPv4 :

```
# editer le fichier sysctl.conf
nano /etc/sysctl.conf

# Puis décommenter la ligne suivante :
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Après avoir enregistré le fichier, il est nécessaire d'appliquer les changements avec la commande suivante :

```
sysctl -p
```

Maintenant, nous allons appliquer les règles IPtables :

```
# Appliquer du nat (masquerade) pour le réseau source 10.0.0.0/24 qui sortira par l'interface vmbr0
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o vmbr0 -j MASQUERADE
```

```
# Autoriser le flux à transiter entre l'interface WANNET et vmbr0 pour les connections déjà établies et existantes
iptables -A FORWARD -i WANNET -o vmbr0 -j ACCEPT
iptables -A FORWARD -i vmbr0 -o WANNET -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Une fois cela fait, il se nous reste plus qu'à rendre persistante ces règles même après un reboot :

```
# Mettre à jour les paquets
apt update

# Installation de iptables-persistent
apt install iptables-persistent
```

Lors de l'installation, sauvegarder les règles IPv4. Il est aussi possible de les sauvegarder avec la commande suivante :

```
# sauvegarder les reègles en place
netfilter-persistent save

# reload le service pour prise en compte
netfilter-persistent reload
```

Après avoir installé le service, nous allons le restart puis tout sera en place !

```
systemctl restart netfilter-persistent
```

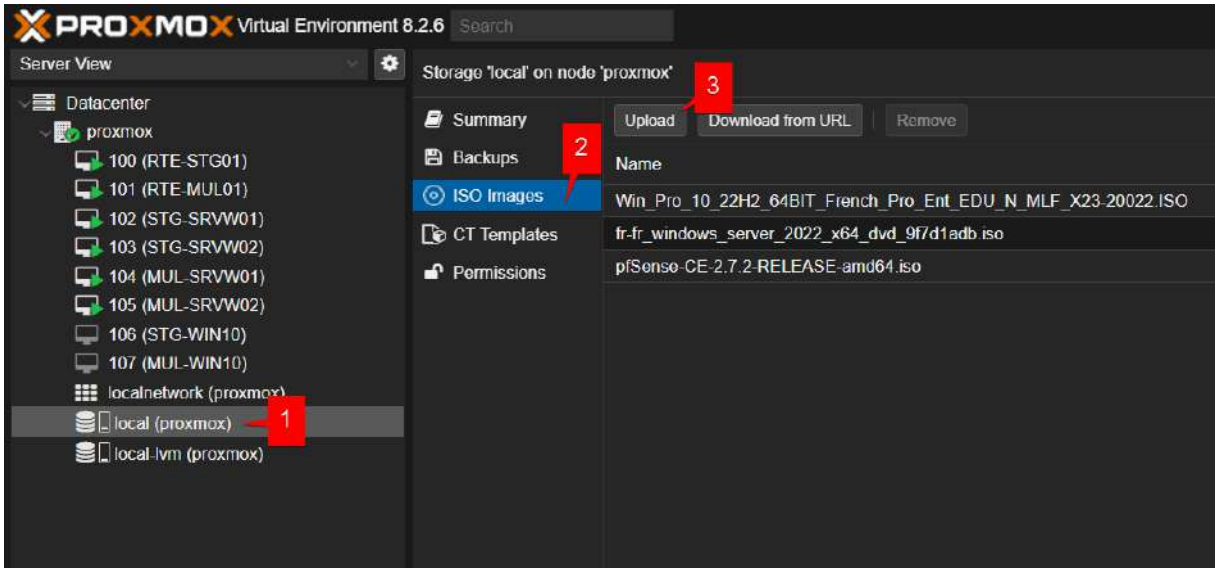
Nos VM connectées à l'interface virtuelle WANNET ont accès à Internet en passant par la passerelle 10.0.0.254/24 et possèdent une plage d'adresse pour elles (10.0.0.0/24), cela pourrait permettre de simuler un "WAN" par exemple.

2.4) Ajouter des ISO et créer sa première VM

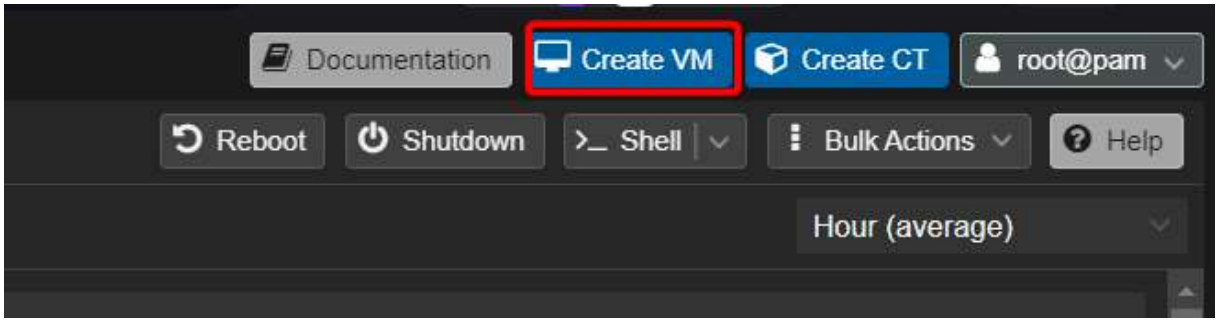
Proxmox prévoit un emplacement spécifique pour les ISO (dans le /var/lib/vz/template/iso) afin de les centraliser.

Pour en ajouter une, il faut se connecter à l'interface promox (https://IP_PROXMOX:8006). Les identifiants sont "root" et le mot de passe mis lors de l'installation.

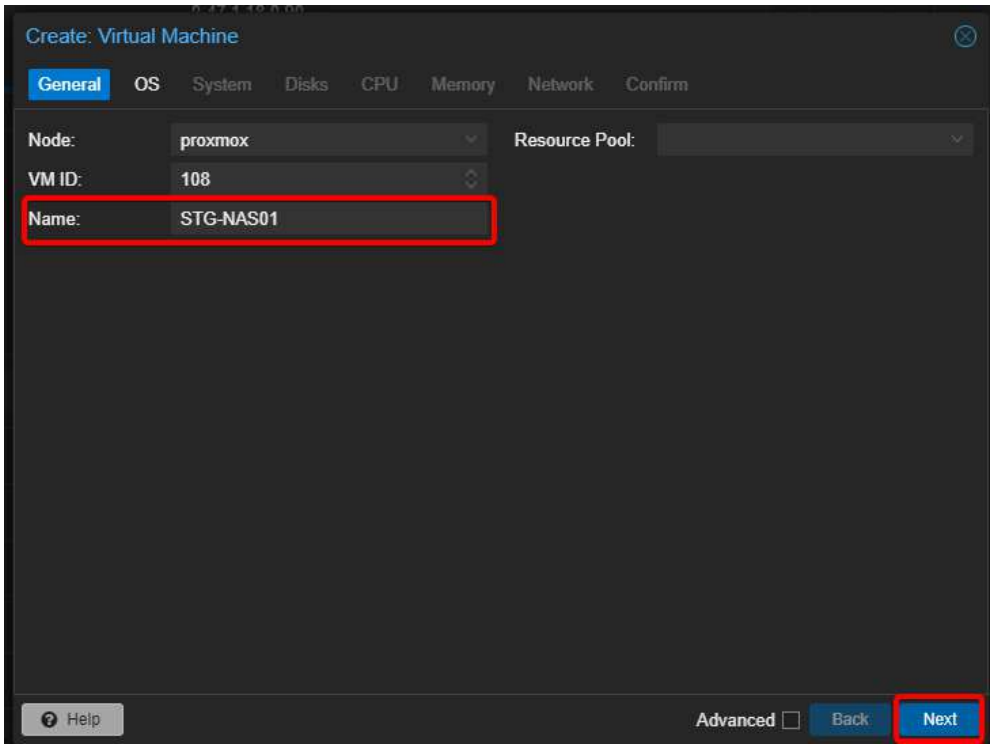
Puis développer le Datacenter et le noeud proxmox, cliquer sur votre stockage local (1), puis ISO Images (2) et enfin Upload (3) :



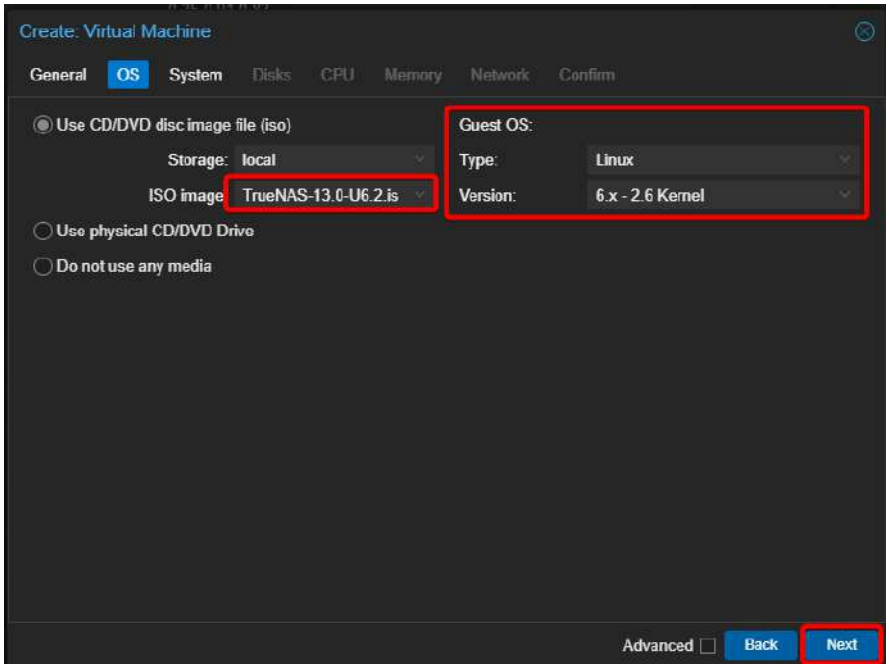
Pour créer votre première VM, nous allons cliquer sur "Create VM" en haut à droite :



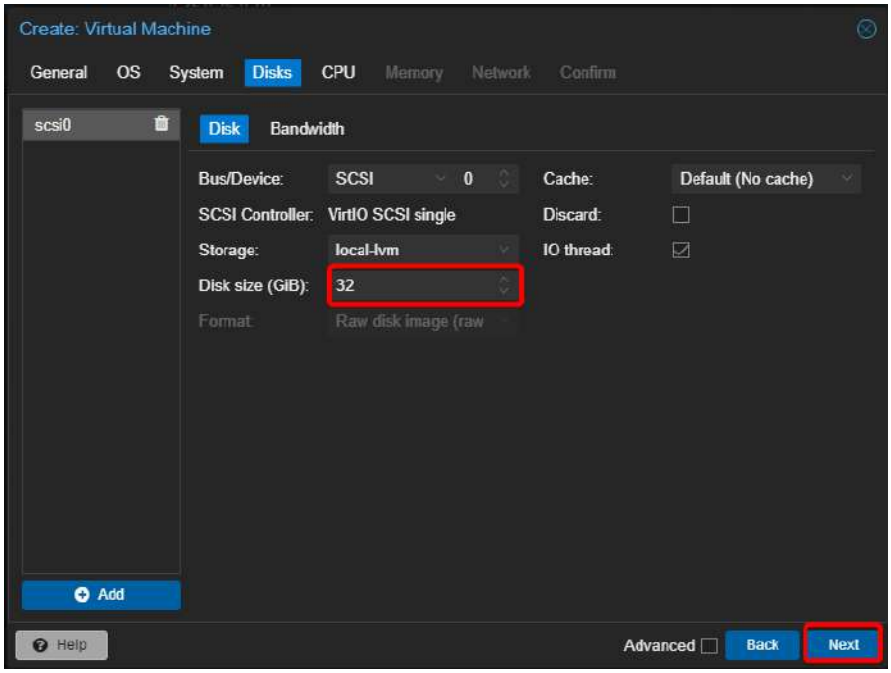
Ensuite, nous allons lui donner un nom, je laisse l'ID par défaut et vérifie qu'elle soit bien dans le nœud proxmox :



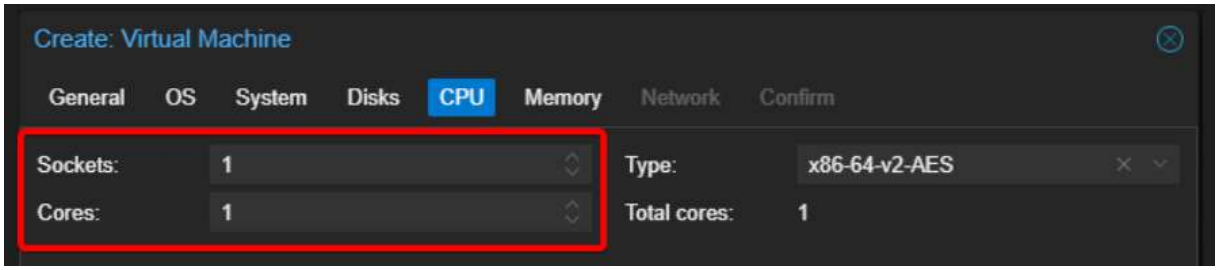
Après je sélectionne l'ISO et l'OS souhaitée :



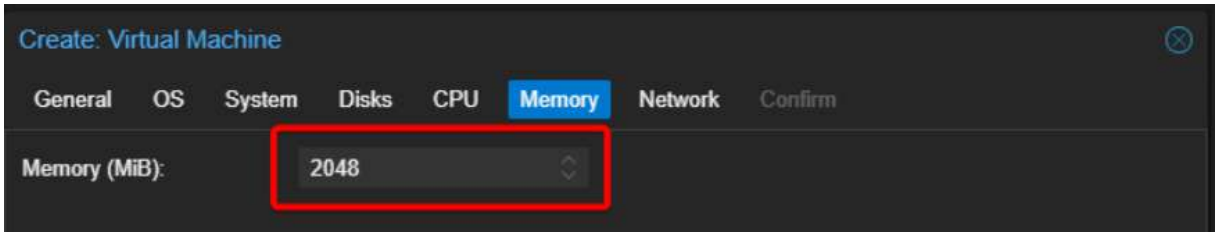
Ensuite, on peut laisser par défaut la partie System, puis on créé un disque virtuel :



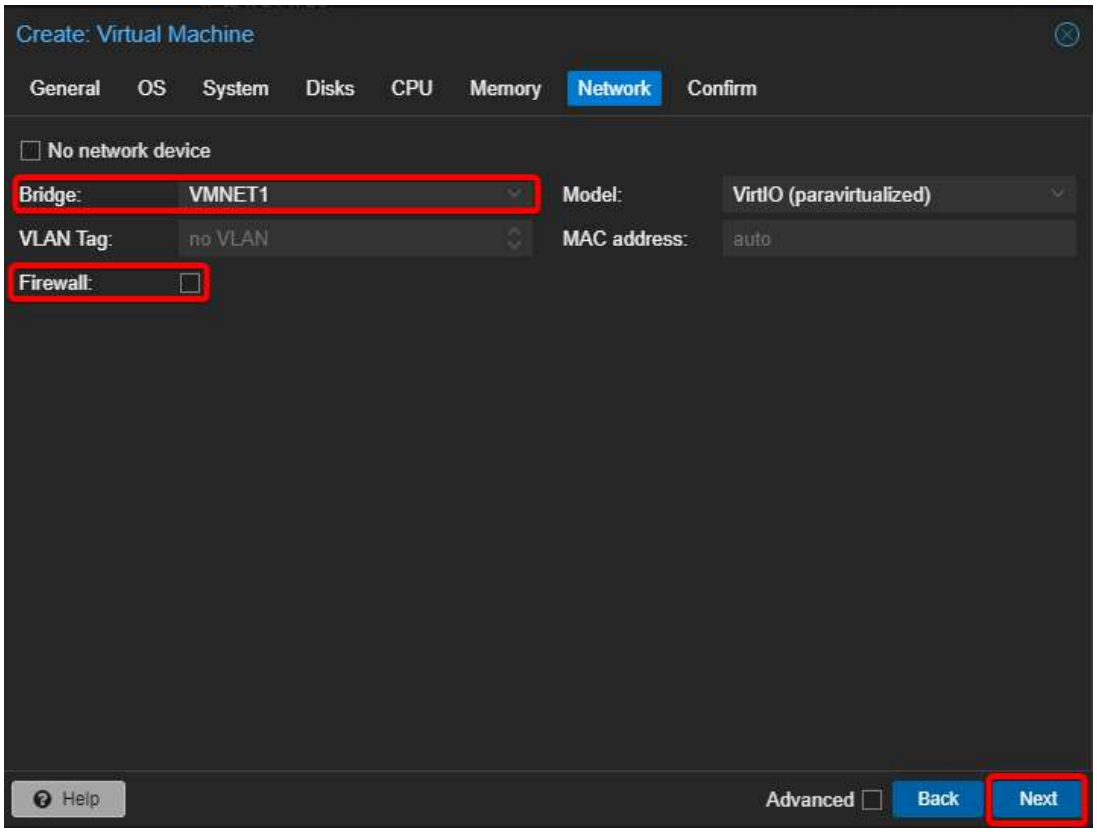
J'attribue le nombre de CPU :



La RAM :



Et enfin, l'interface réseau sur laquelle ma VM sera et je n'oublie pas de décocher le firewall :



On peut ensuite cliquer sur Finish, et voilà, la VM est maintenant créé.

2.5) Joindre l'hyperviseur depuis Internet

Il peut être pratique de joindre son hyperviseur depuis l'extérieur. Certains opérateurs ne permettent plus une ouverture de port correcte en IPv4. Ainsi, nous allons utiliser Tailscale pour rendre notre hyperviseur accessible depuis Internet.

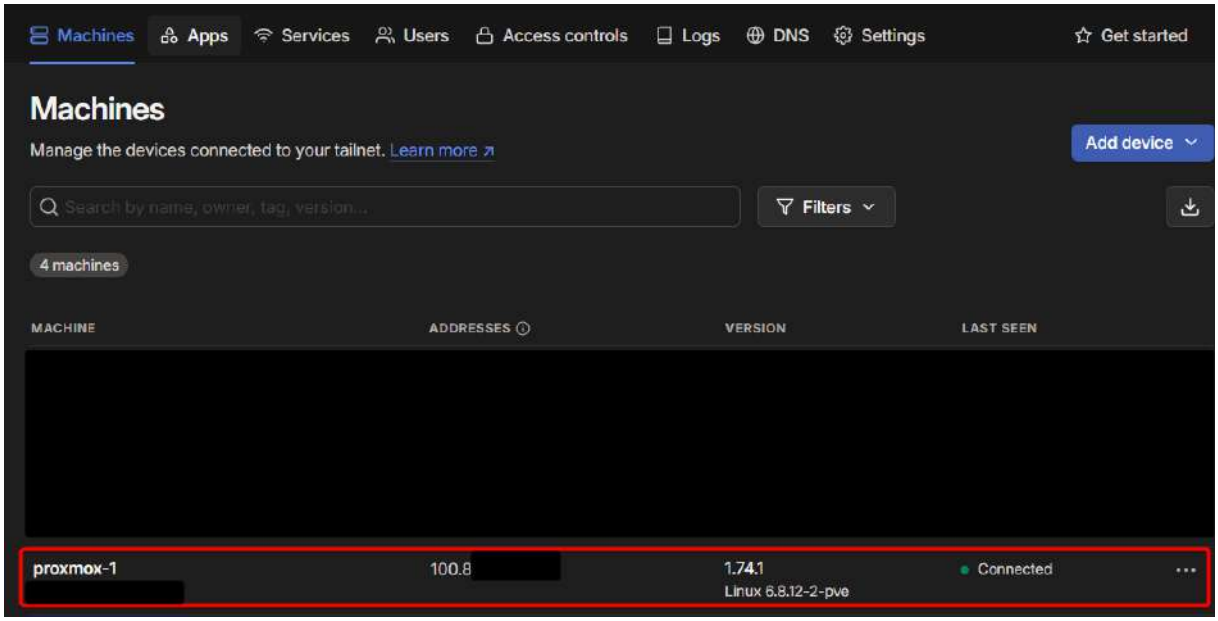
Pour cela, il suffit d'installer tailscale sur notre proxmox :

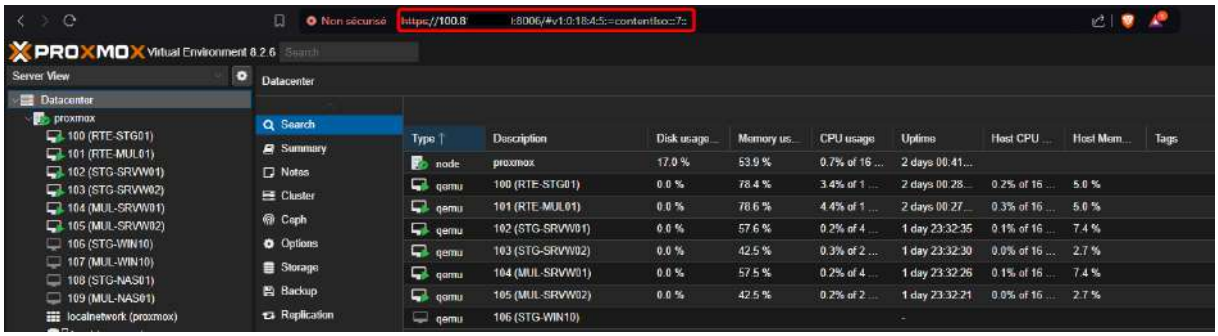
```
# se connecter en SSH
ssh root@IP_PROXMOX

# installer tailscale (nécessite une connexion Internet)
curl -fsSL https://tailscale.com/install.sh | sh
# lancer le login
```

tailscale up

Ensuite il faudra juste vous connecter sur un autre appareil à votre compte Tailscale avec le lien qui sera renvoyé à la suite du tailscale up.

Pour se connecter dessus avec un autre appareil, il faudra que vous ayez installé et configuré Tailscale sur l'appareil souhaité (https://tailscale.com/download/windows) puis sur l'Admin console, vous pourrez retrouver l'IP Tailnet de votre Hyperviseur et vous y connecter :

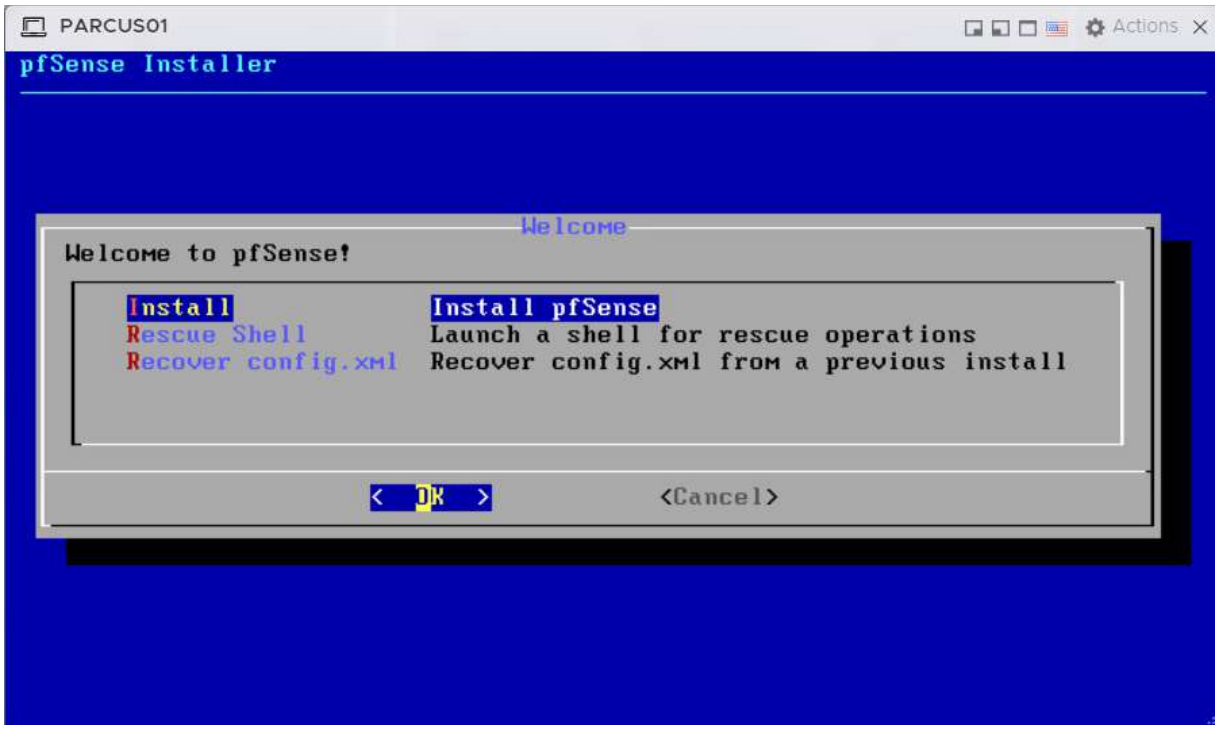


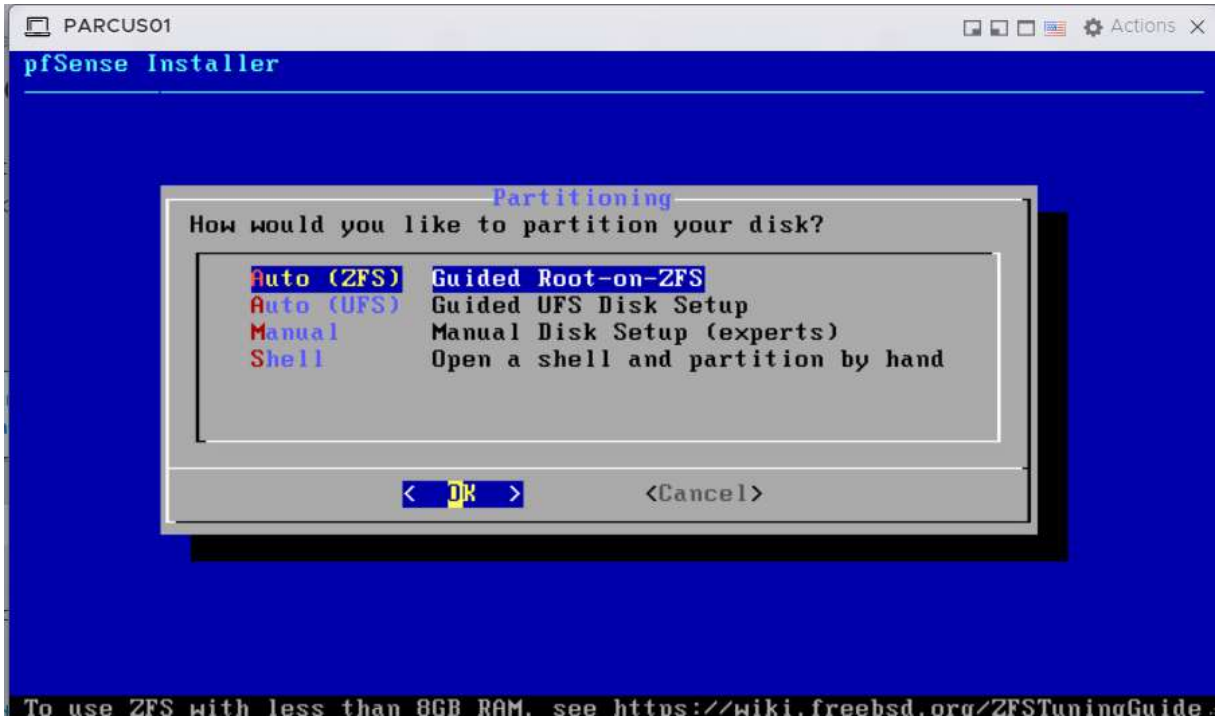


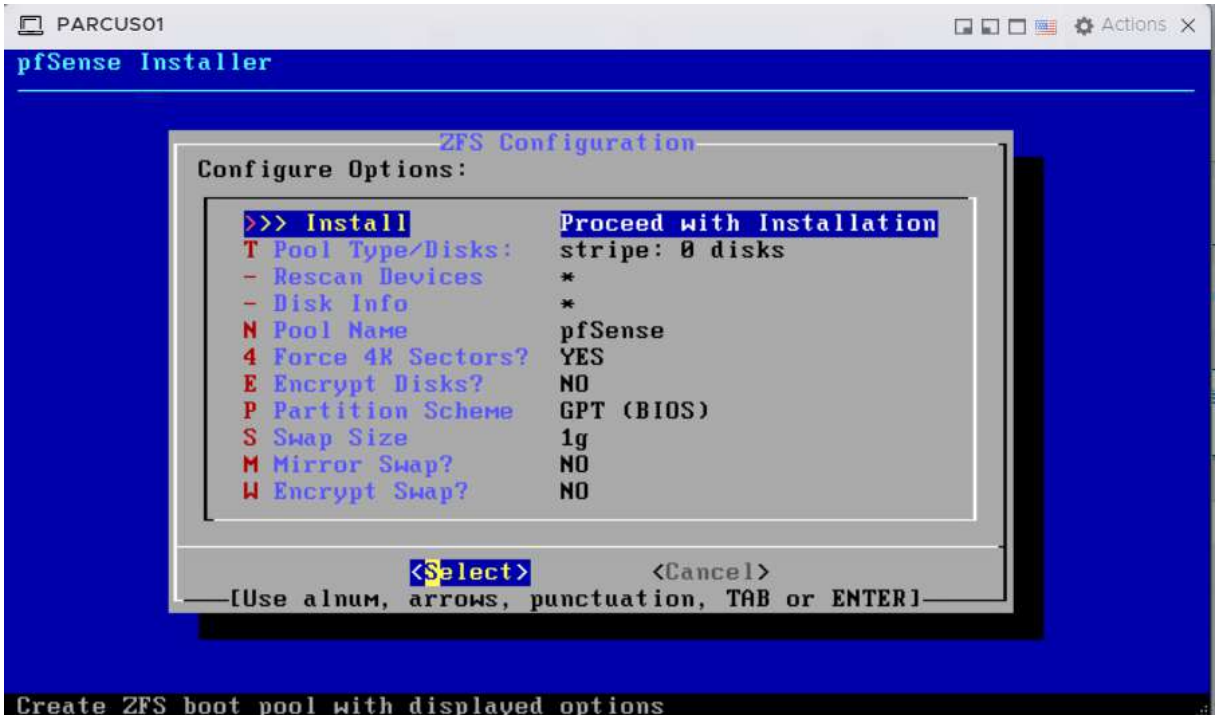
3) INSTALLATION ET CONFIGURATION DE PFSENSE

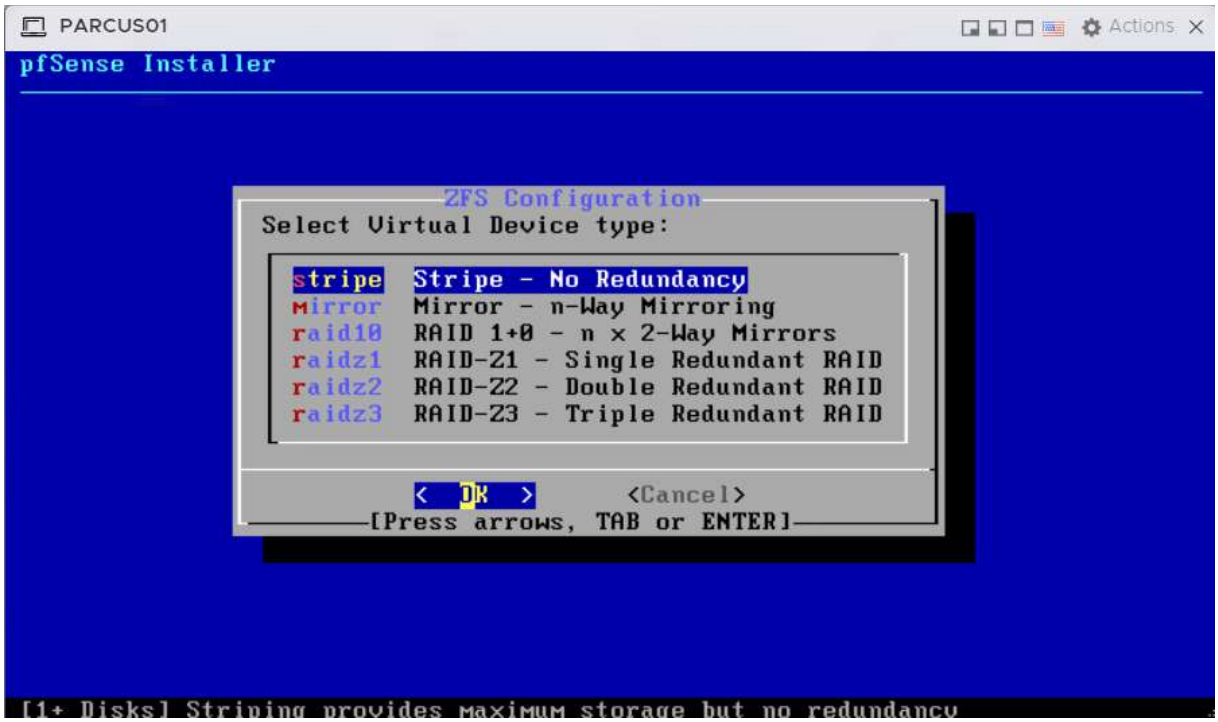
3.1) Installation de Pfsense

Mettre sous tension la machine, puis au lancement, lancer l'installation de pfsense :

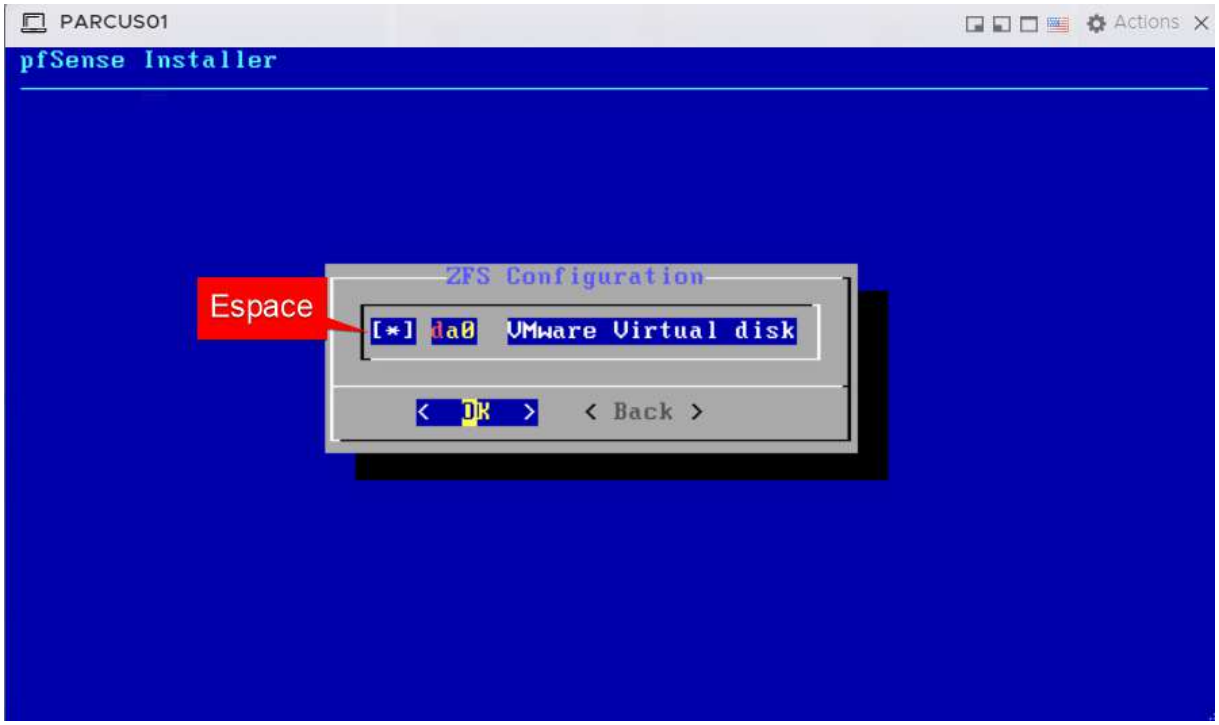


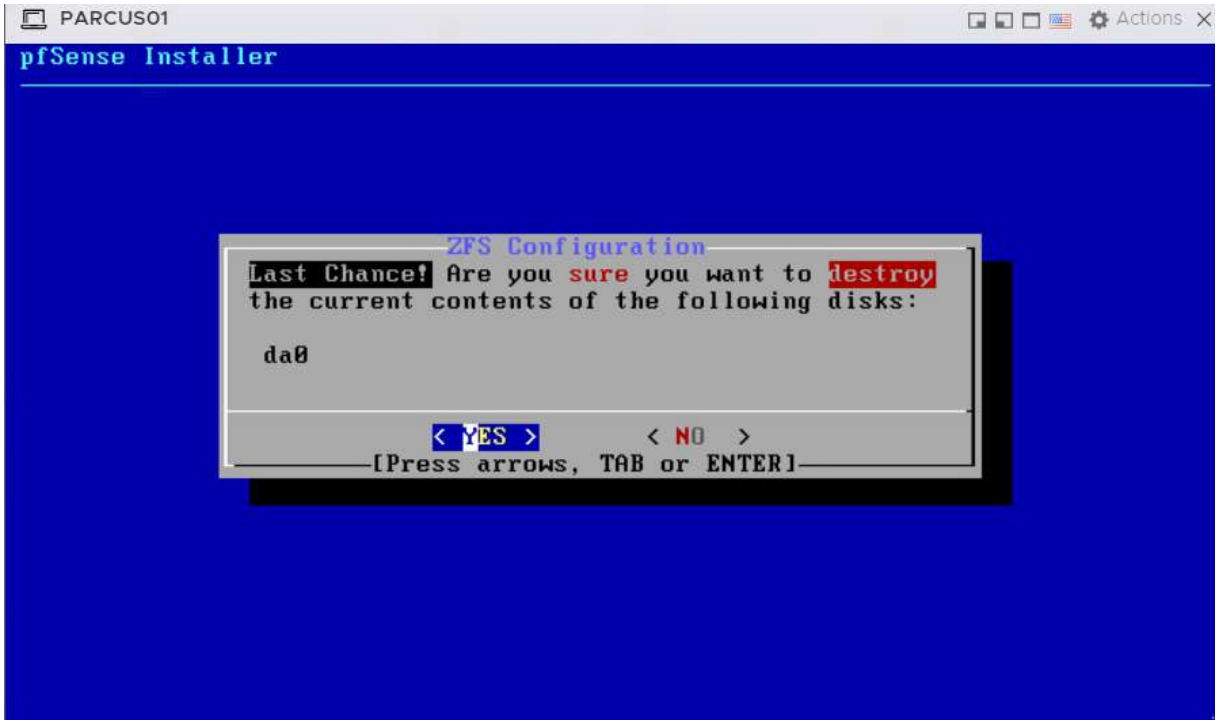



PARCUS01
Actions
pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap? NO
<Select> <Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]
Create ZFS boot pool with displayed options


PARCUS01
Actions
pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK > <Cancel>
[Press arrows, TAB or ENTER]
[1+ Disks] Striping provides maximum storage but no redundancy

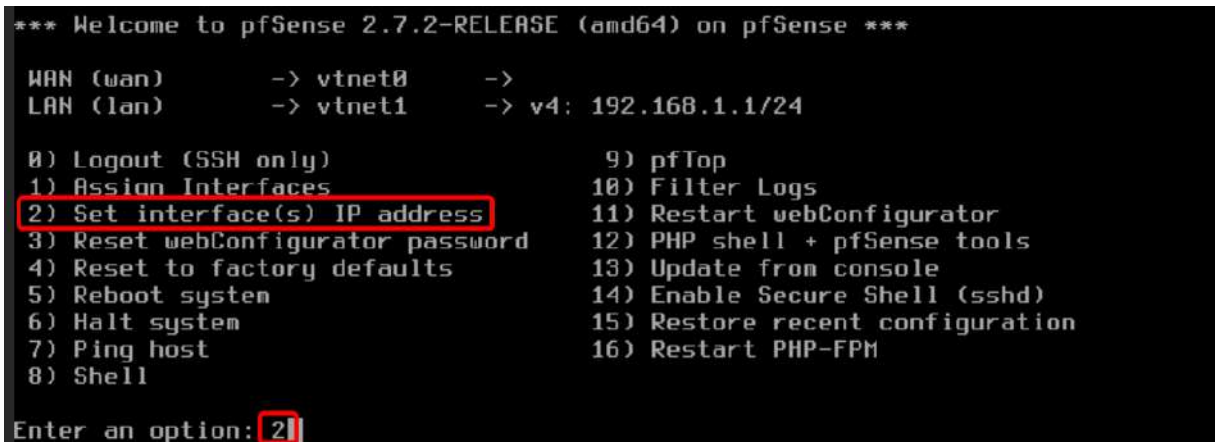
Sélectionner le disque avec la touche espace puis continuer :



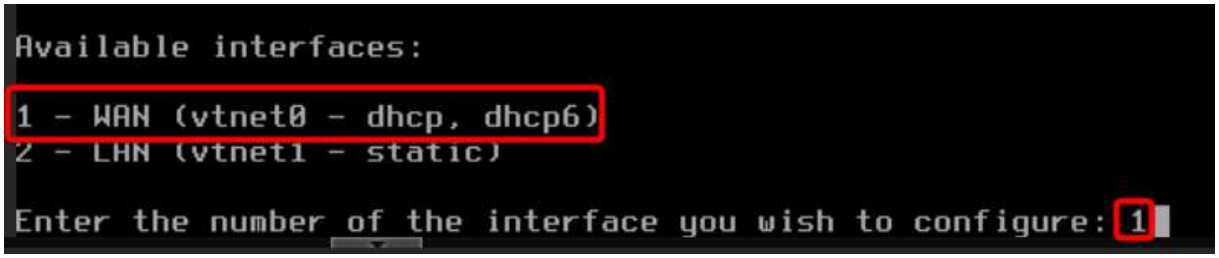


Ensuite, on va nous proposer de reboot la machine, on accepte donc de reboot la machine.

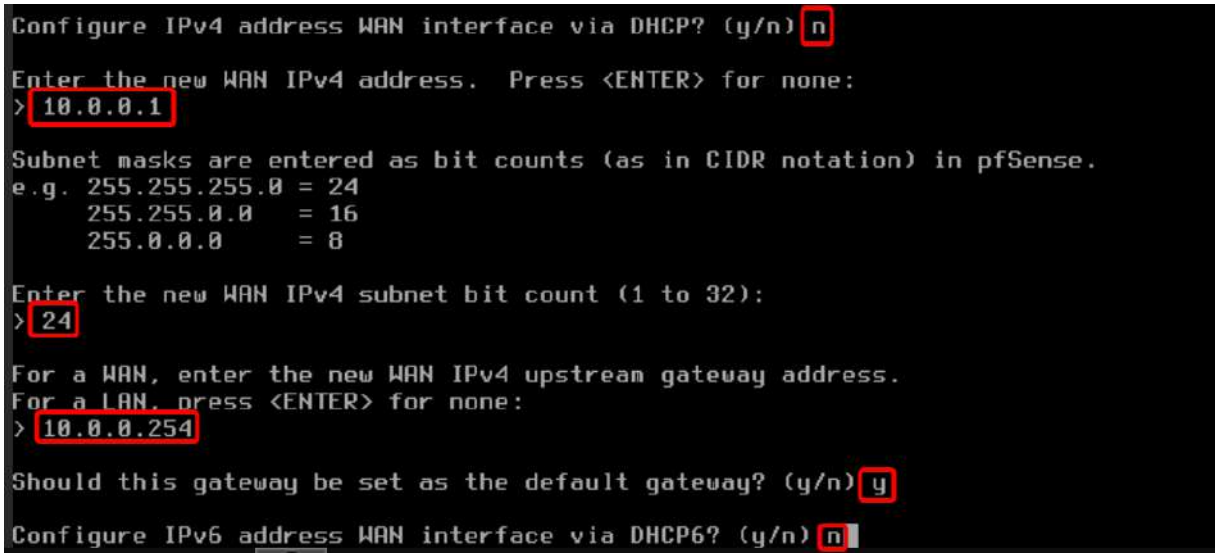
On sélectionne l'option 2 afin de set les adresses IP des interafces réseaux :



Puis, on sélectionne l'interface WAN :



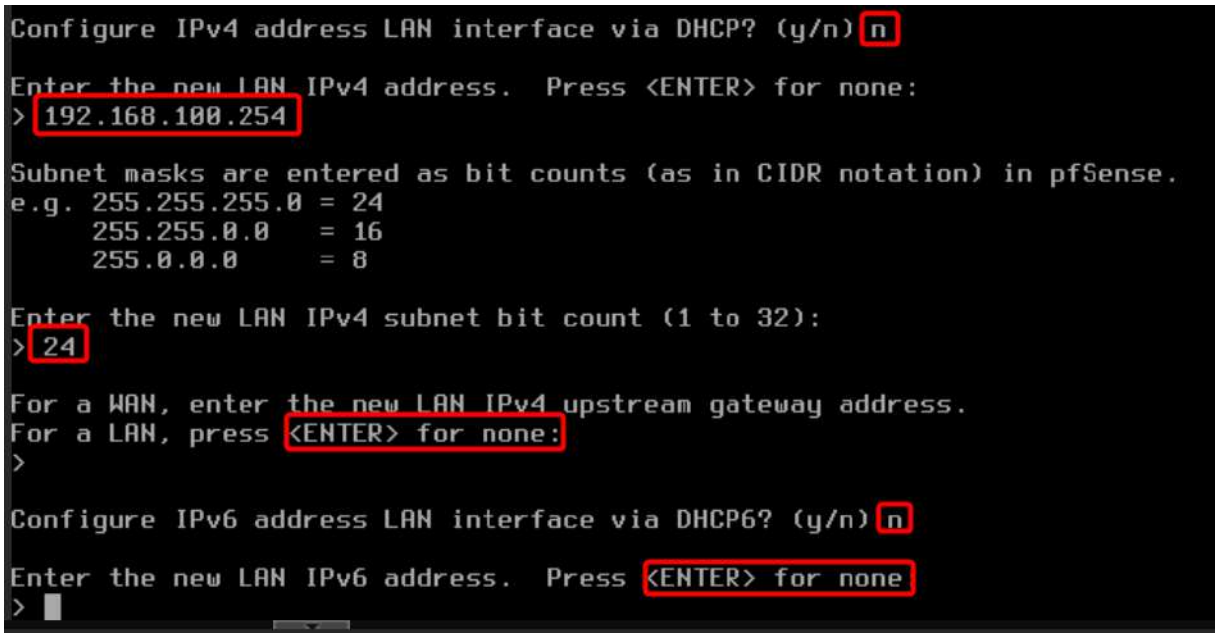
Ensuite, on configure l'adresse IPv4 WAN et la passerelle WAN :



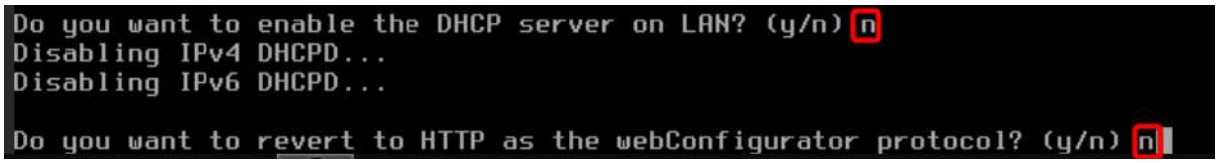
On ne configurera pas d'IPv6 dans notre cas et on laisse le protocole HTTPS :

On configure ensuite l'interface LAN :

On rentre notre IPv4, nous ne configureront pas d'IPv6 :



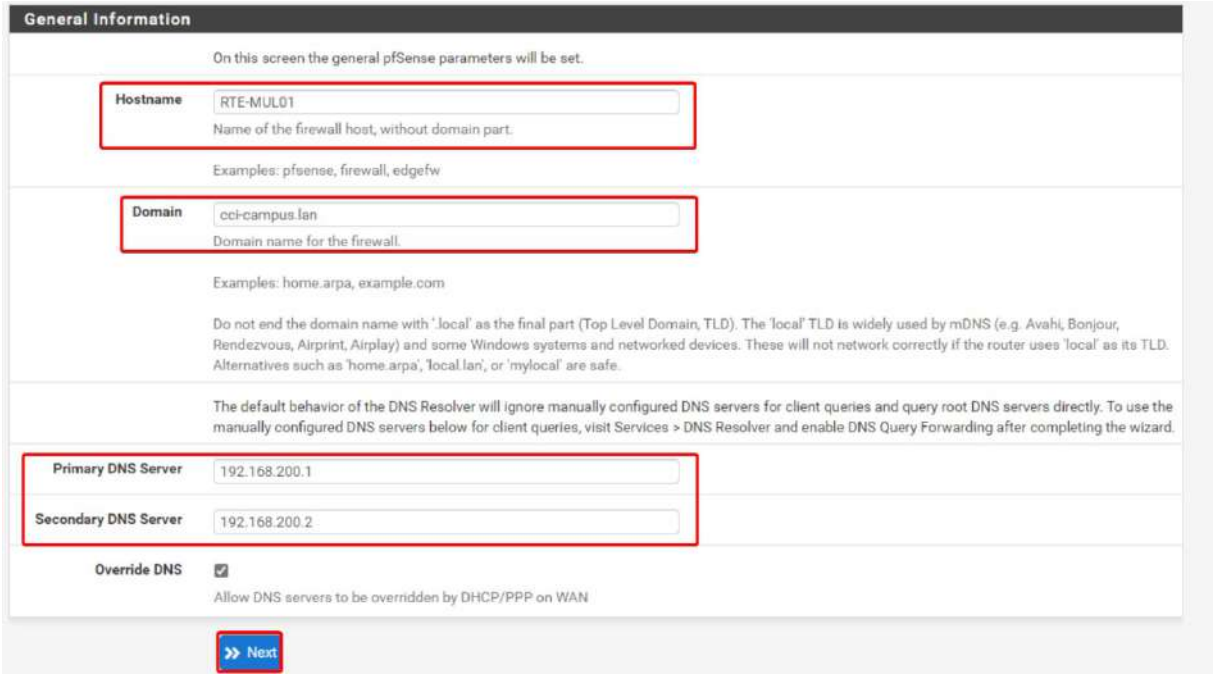
On n'activera pas le serveur DHCP sur le LAN et on laisse le protocole HTTPS :



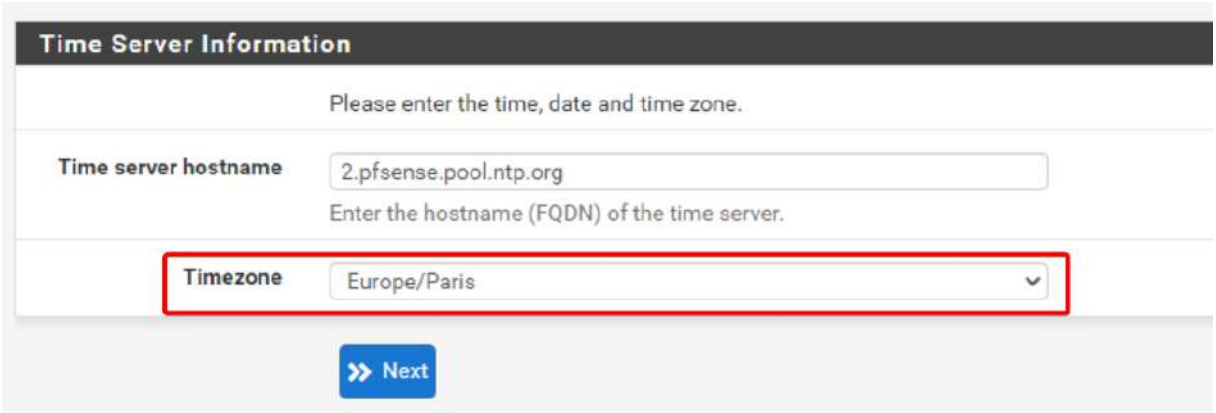
3.2) Configuration de Pfsense

Pour cette partie, il faudra accéder à l'interface web de notre pfsense : https://IP_PFSENSE

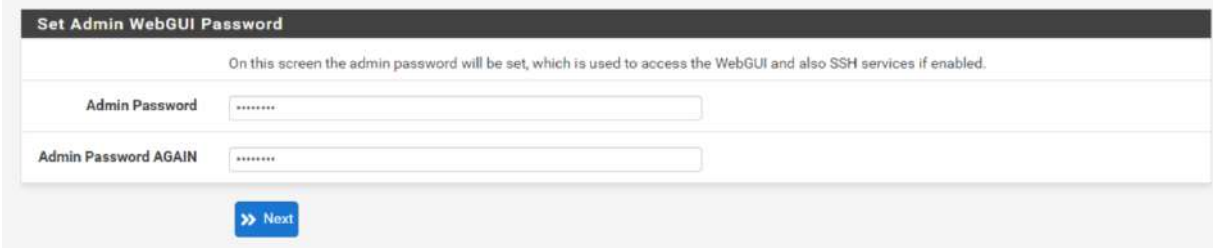
Le wizard va se lancer, il faut donc configurer le hostname, le domaine et les DNS :



On sélectionne notre timezone, puis Next :



On peut cliquer 2 fois sur suivant, et ensuite saisir notre mot de passe Admin :



3.3) Mise en place de la haute disponibilité Pfsense

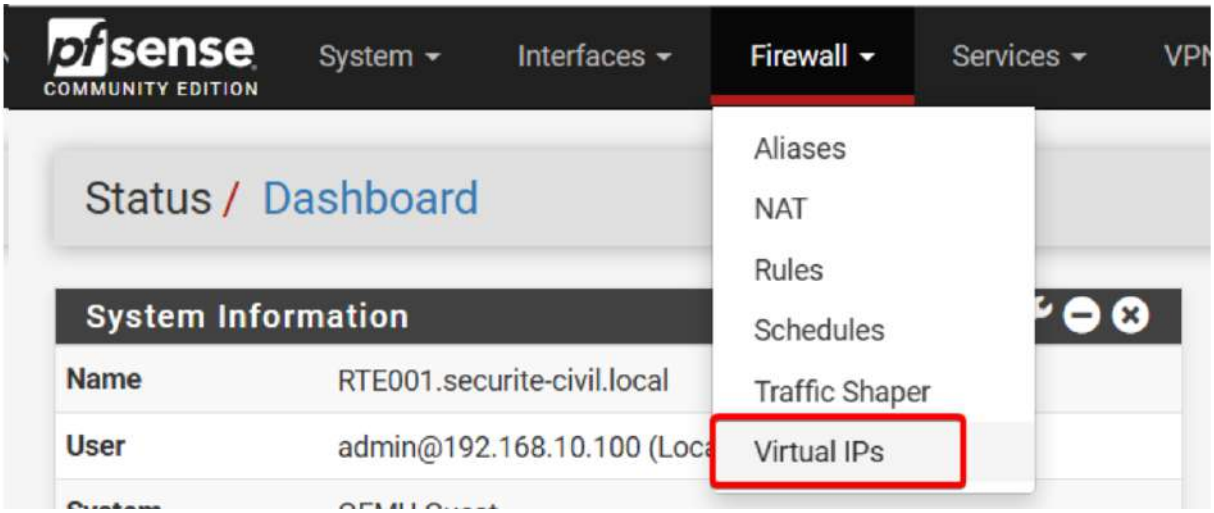
3.3.1) Mise en place d'une VIP

Le protocole **CARP** (Common Address Redundancy Protocol) sur pfSense permet de configurer une adresse IP virtuelle partagée entre plusieurs pare-feux pour assurer une **haute disponibilité** (HA).

Il est utilisé pour créer des **Virtual IPs (VIPs)**, qui permettent à plusieurs pare-feux pfSense de répondre comme s'ils étaient une seule machine. Cela garantit qu'en cas de panne du pare-feu principal, un autre prend le relais sans interruption de service, assurant ainsi la **continuité réseau**.

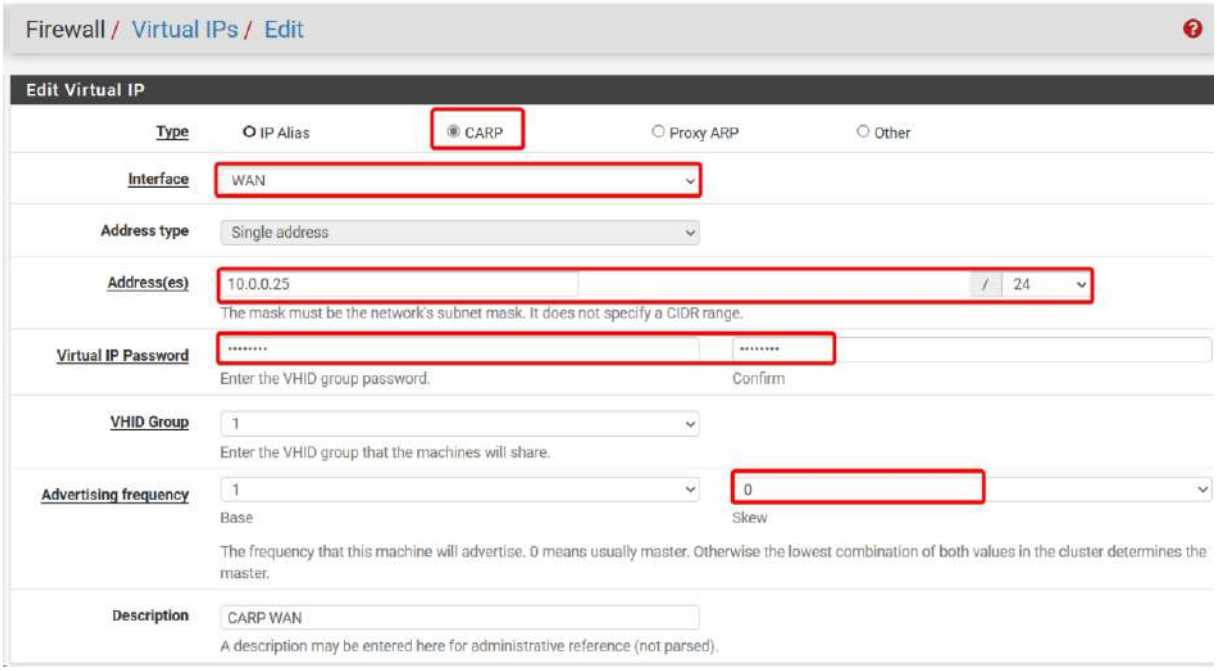
Pour mettre en place cette IP virtuelle, il faut donc avoir 2 pfsense sur le même réseau. Nous allons commencer par la configuration du serveur pfsense **primaire**.

Pour commencer, sur le serveur **primaire** il faut aller sous Firewall > Virtual IPs :

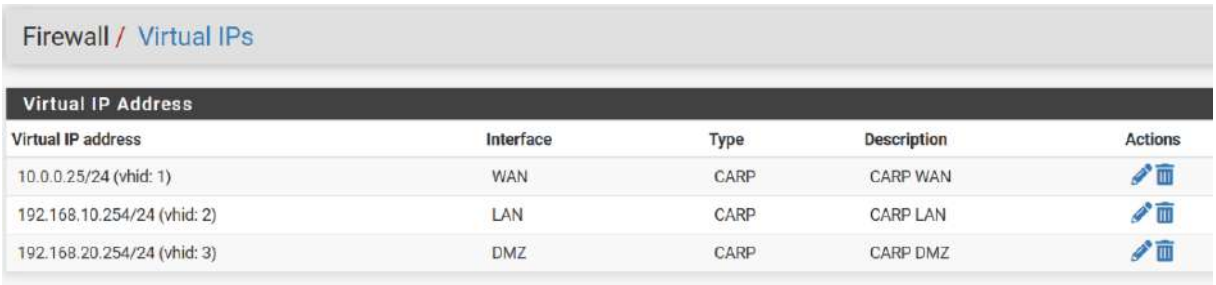


Ensuite, on clique sur "+" pour en ajouter une nouvelle et on met les paramètres suivants :

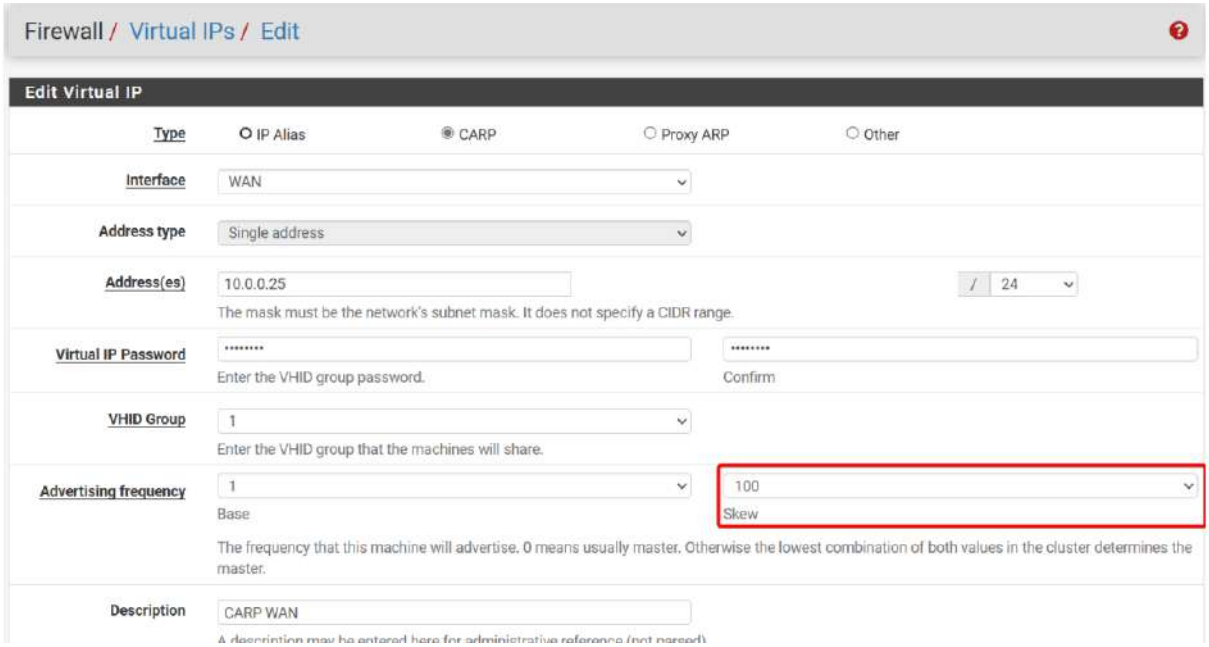
- **Type :** CARP
- **Interface :** Correspond à l'interface sur laquelle on aura une IP virtuelle, dans notre cas nous ferons ceci pour la WAN, LAN et DMZ
- **Address(es) :** Correspond à l'adresse IP virtuelle que l'on souhaite et son masque de son réseau
- **Virtual IP Password :** Ce mot de passe sera nécessaire pour rejoindre le VHID Group, c'est donc le même mot de passe que l'on rentrera sur le Pfsense secondaire.
- **Advertising frequency :** On peut laisse le paramètre Base à 1. Le paramètre Skew lui permet de définir le MASTER (0) ou le SLAVE (100) de l'IP virtuelle. Ici étant donné qu'il s'agit de notre Pfsense primaire, ce sera le master donc 0.



On peut sauvegarder et réitérer l'opération pour nos interfaces LAN et DMZ :



Il sera ensuite nécessaire de refaire les mêmes configurations sur le pfsense **secondaire** en ajustant correctement le champ "Skew" :

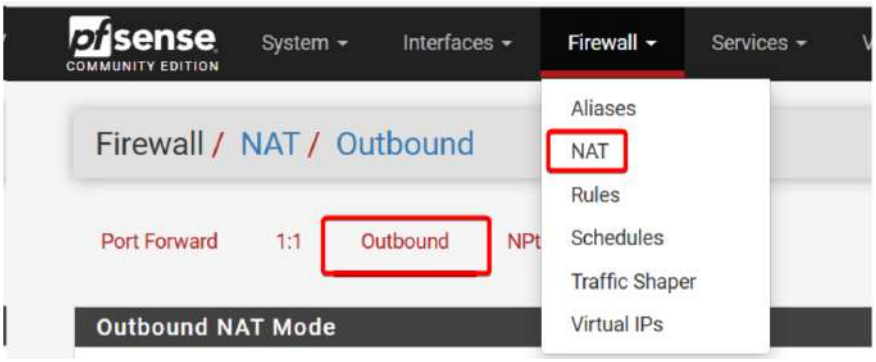


L'IP virtuelle est maintenant en place, cependant il faut encore forcer les sorties sur Internet avec l'IP virtuelle.

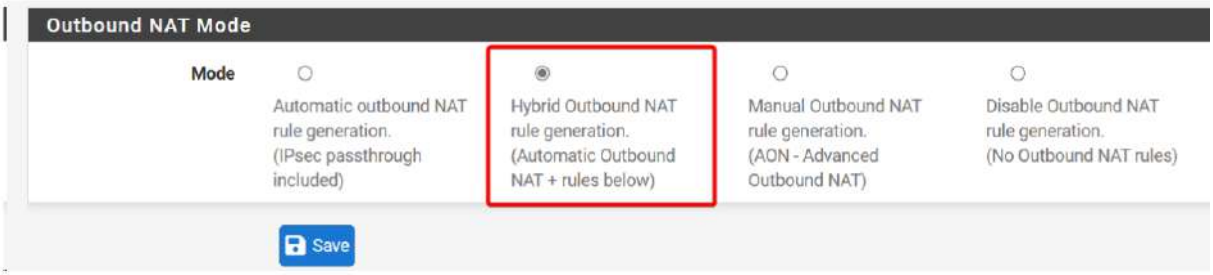
3.3.2) Forcer l'utilisation de la VIP

Les règles de firewall ci-dessous sont à reproduire sur le pfsense secondaire si PFSYNC n'est pas configuré par la suite.

Pour se faire, il est nécessaire d'aller dans Firewall > NAT > Outbound :

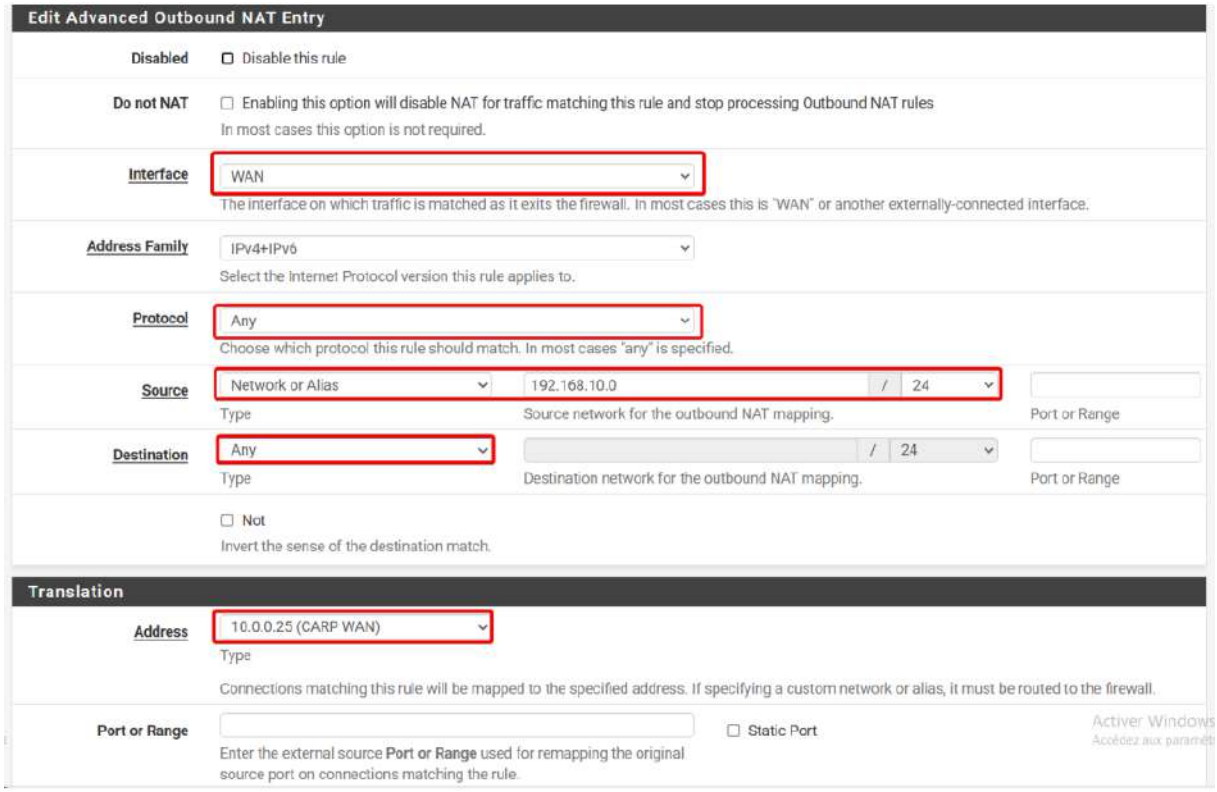


Il faut ensuite cocher "Hybrid Outbound" :



Et créer une nouvelle règle avec les paramètres suivant :

- **Interface :** WAN
- **Protocol :** Any
- **Source :** On indiquera ici l'adresse du sous-réseau de notre LAN (la même règle sera donc à reproduire si vous avez une DMZ).
- **Destination :** Any
- **Address :** On vient sélectionner ici notre VIP WAN créée précédemment

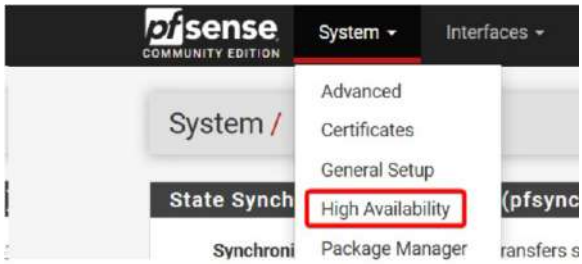


3.3.3) Mise en place de PFSYNC et XMLRPC Sync

Le module **High Availability** de pfSense est conçu pour assurer la **redondance et la continuité de service** en cas de panne. Il repose sur des fonctionnalités comme **CARP** (pour les VIPs), la synchronisation des configurations, et le partage des états (State Synchronization) entre deux ou plusieurs pare-feux.

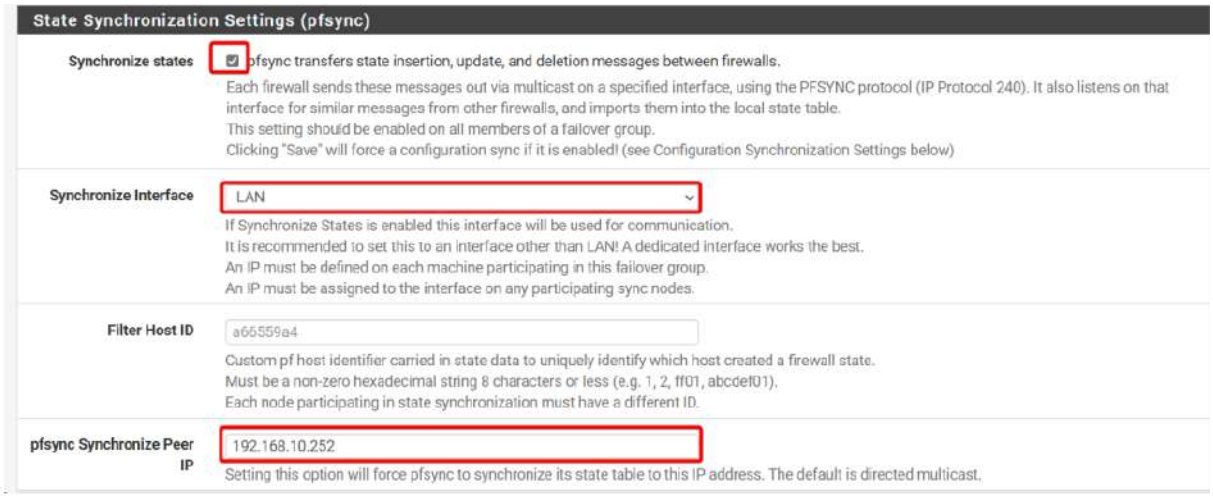
Ce module permet à plusieurs pare-feux de fonctionner comme un seul, assurant qu'en cas de défaillance d'un appareil, un autre prend immédiatement le relais, minimisant ainsi les interruptions réseau.

Pour configurer PFSYNC et XMLRPC Sync, il faut se rendre sous System > High Availability sur notre Pfsense primaire et secondaire :



Sur le pfsense **primaire et secondaire** il sera nécessaire de renseigner les paramètres suivants :

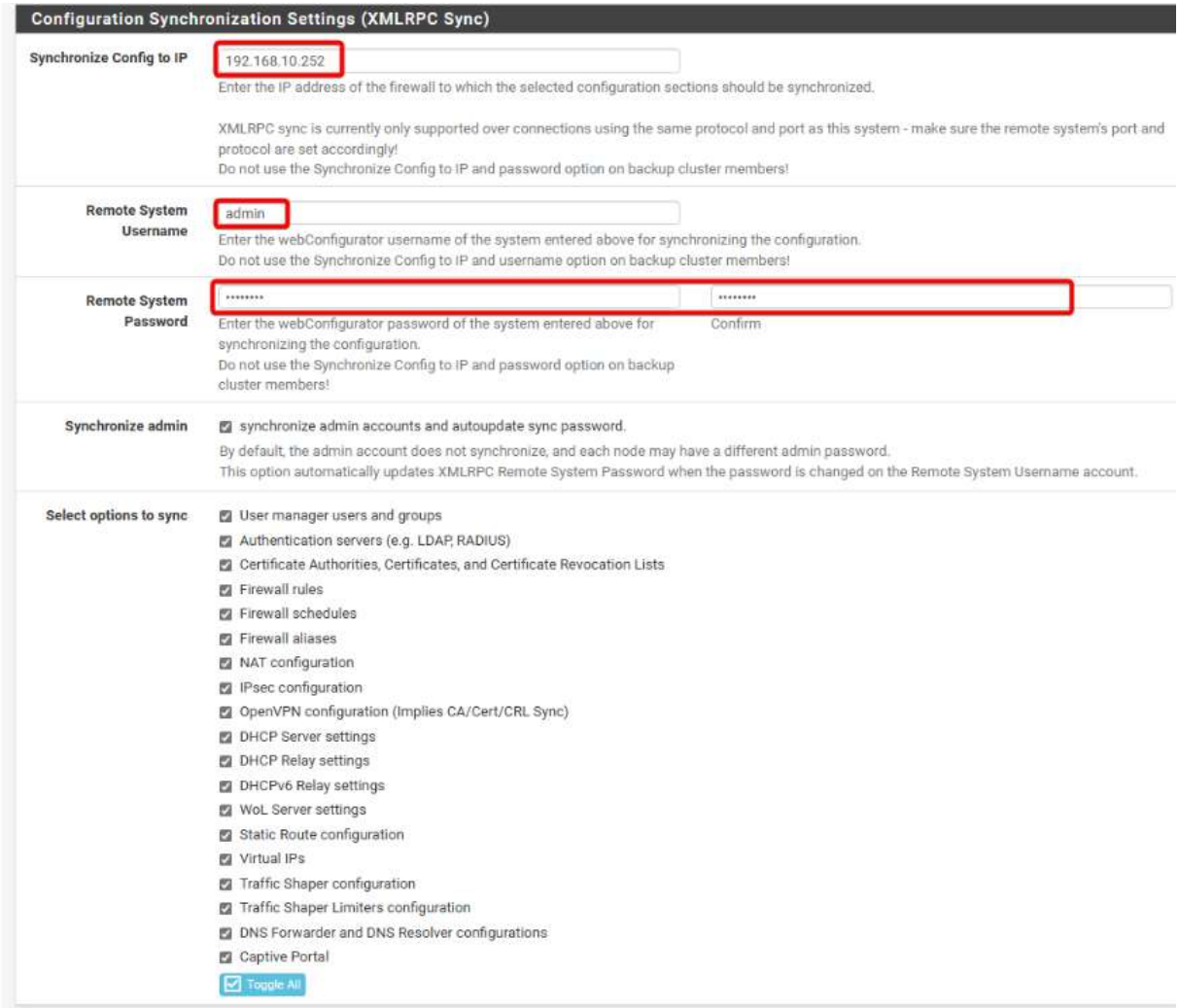
- **Synchronize states :** Il faut cocher la case
- **Synchronize interface :** Il s'agit de l'interface réseau qui sera utilisée pour réaliser la synchronisation des Pfsense. Il est recommandé d'en dédiée une à la synchronisation, mais dans notre cas nous utiliserons celle de notre LAN.
- **pfsync Synchronize Peer IP :** Il s'agit de l'IP du pfsense partenaire (donc le secondaire si on est sur le primaire, et le primaire si on est sur le secondaire). Attention, cette IP doit être celle attribué sur le réseau ou est connecté l'interface physique.



Ensuite, sur le pfsense **primaire** uniquement, il faudra renseigner les paramètres suivants :

- **Synchronize Config to IP :** Il s'agit de la même IP que celle utilisée pour "pfsync Synchronize Peer IP". C'est l'IP du pfsense **secondaire**
- **Remote System Username :** Ce champ doit correspondre au nom d'utilisateur utilisé pour se connecter à l'interface web du pfsense **secondaire**
- **Remote System Password :** Il s'agit du mot de passe utilisé pour se connecter à l'interface web du pfsense **secondaire**

On peut ensuite cocher les options que l'on souhaite répliquer (à faire sur le pfsense **primaire et secondaire**) :



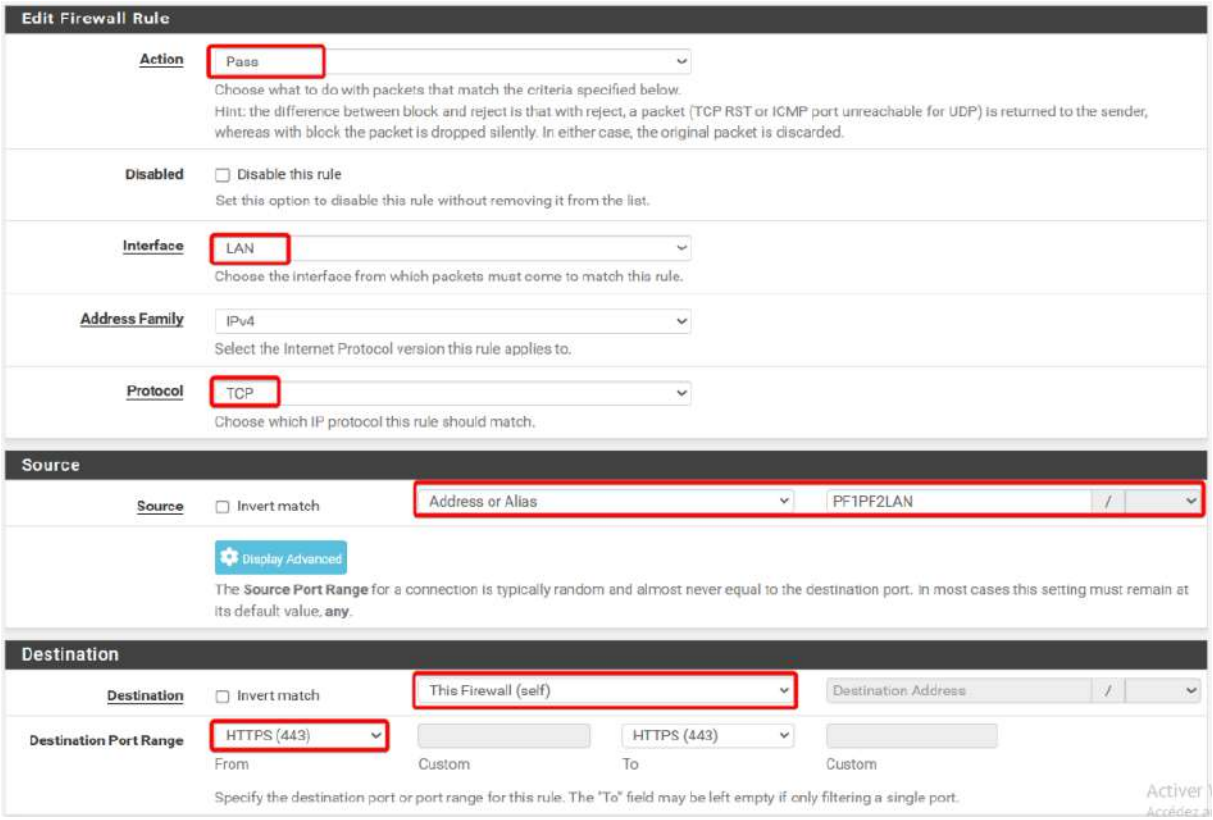
Enfin, on peut valider sur le pfsense primaire et sur le secondaire.

3.3.4) Règles de pare feu nécessaire pour la synchronisation

Il est nécessaire d'ouvrir certains flux pour synchroniser les pfsense.

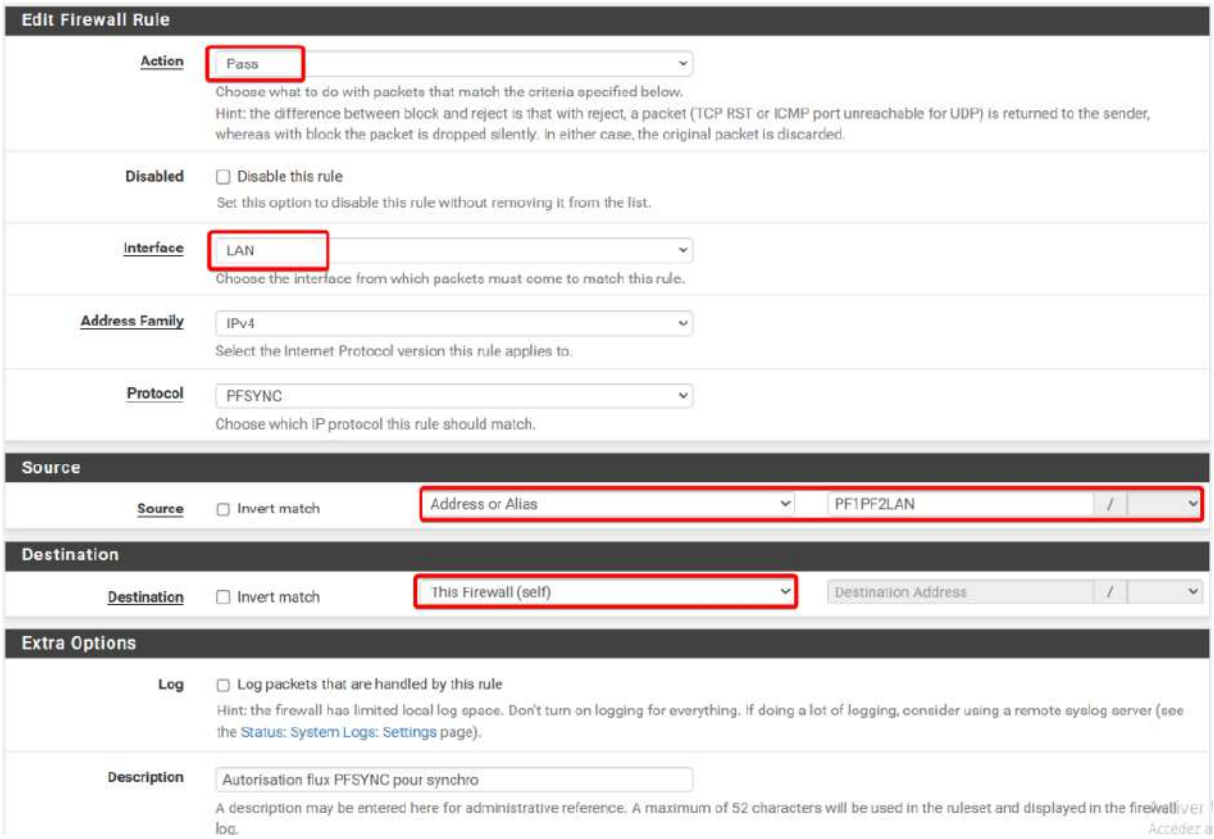
Il faut donc se rendre sous Firewall > Rules, puis créer une règle sur l'interface utilisée par nos pfsense pour se synchroniser (dans notre cas LAN) :

- Action : Pass
- Interface : LAN
- Protocol : TCP
- Source : L'IP ou le sous réseau de vos pfsense. L'alias PF1PF2LAN, représente ici les IP LAN de nos deux PfSense
- Destination : This Firewall (self)
- Destination Port Range : HTTPS (443)



Puis il faudra créer une dernière règle pour permettre la synchronisation avec le protocole PFSYNC:

- Action : Pass
- Interface : LAN
- Protocol : PFSYNC
- Source : L'alias qui pointe vers nos deux pfsense sur le LAN
- - Destination : This Firewall (self)



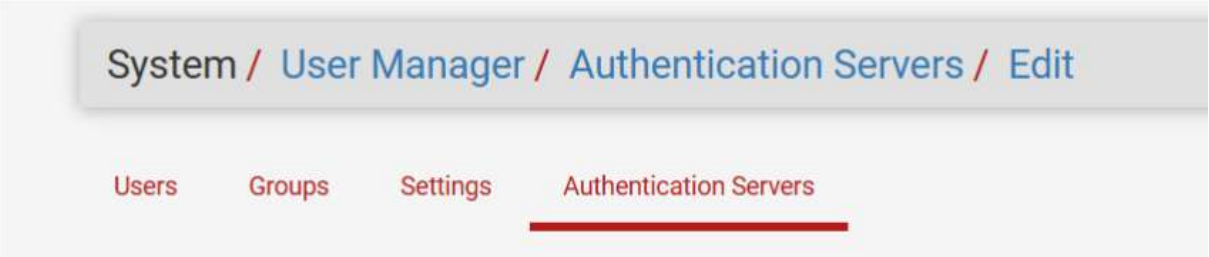
Notre configuration est maintenant terminée, il est possible de vérifier si la réplication fonctionne correctement en regarder si les règles sont répliquées sur le deuxième firewall.

3.4) Mise en place d'un serveur OpenVPN (Road Warrior)

Pfsense inclus nativement un serveur OpenVPN.

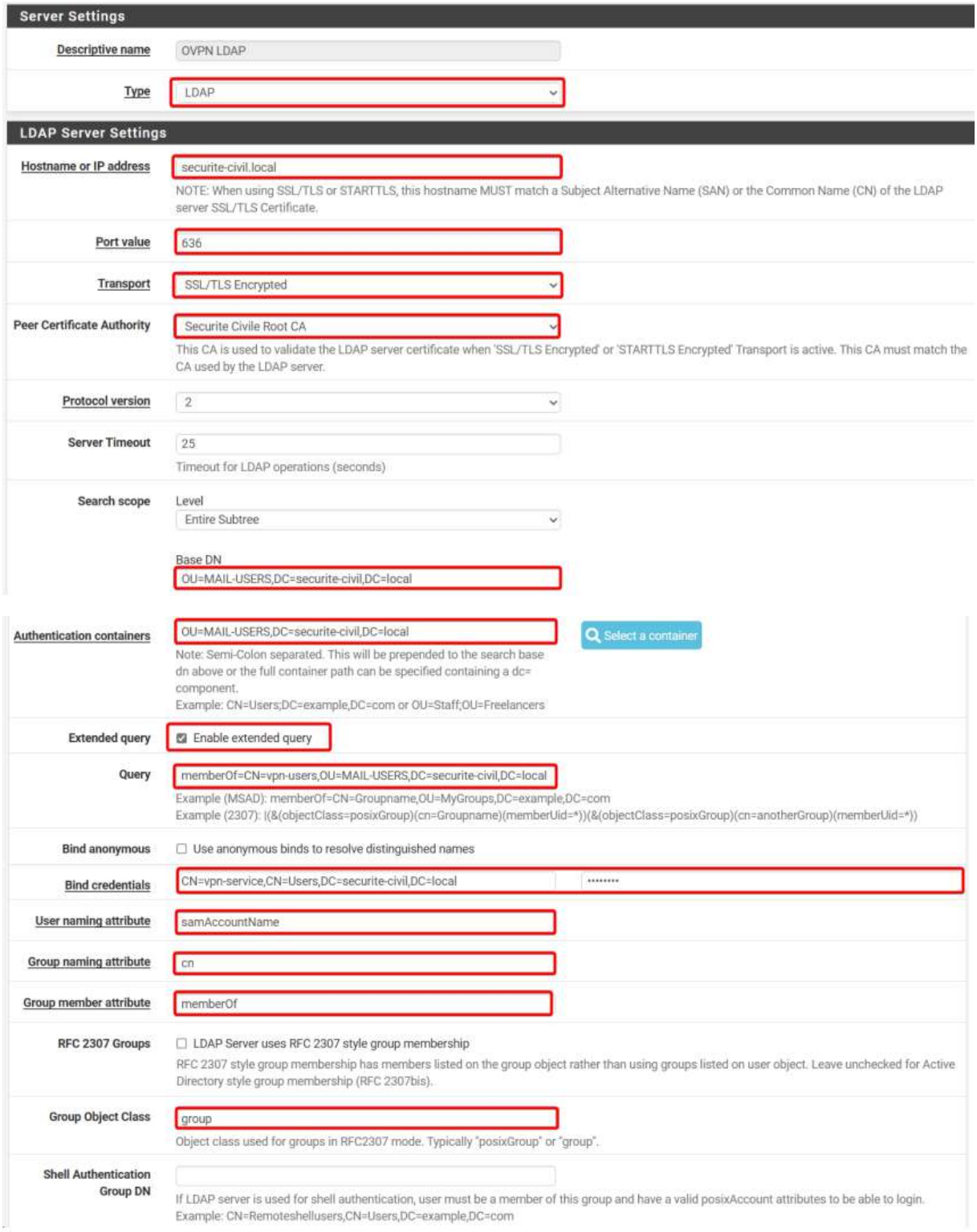
3.4.1) Liaison avec l'Active Directory

Tout d'abord, il faut se rendre dans Sytem > User Manager > Authentication Servers, et on clique sur ajouter afin de configurer la liaison LDAP avec notre AD :



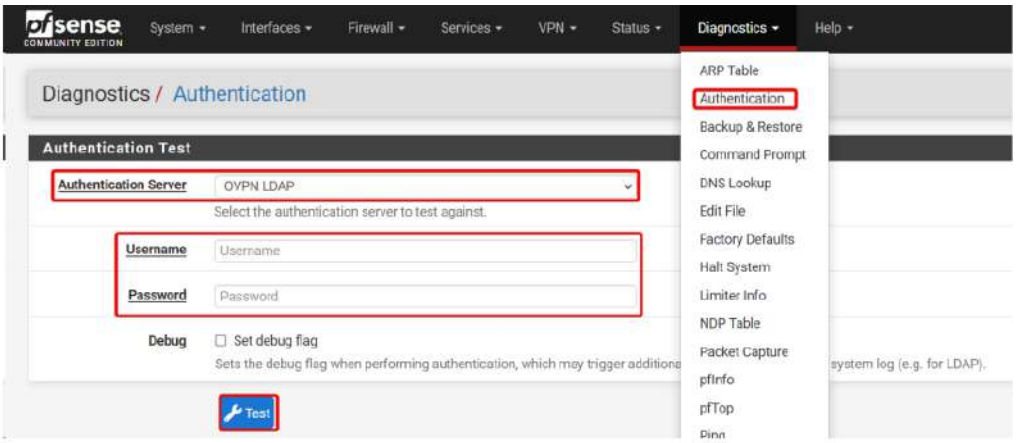
Ensuite, on remplit les différentes informations concernant l'annuaire LDAP, avec une connexion en LDAPS :

- Hostname or IP address : IP ou nom DNS de l'annuaire LDAP
- Port value : Ici on rentre le port LDAPS (636)
- Transport : On sélectionne SSL/TLS Encrypted pour du LDAPS
- Peer CA : On renseigne l'authorité racine de notre LDAPS
- Base DN : Il s'agit de l'endroit ou nos utilisateurs et groupes vont être récupérés dans notre AD
- Authentification containers : Il s'agit de l'endroit ou nos utilisateurs et groupes vont être récupérés dans notre AD pour s'authentifier
- Extended query : On peut activer cette option et renseigner la Query afin d'autoriser uniquement des utilisateurs appartenant à un certain groupe à s'authentifier sur notre serveur VPN
- Bind credentials : Il s'agit du compte de service qui va être utilisé pour récupérer les utilisateurs dans l'AD
- User naming attribute : On renseigne l'attribut qui matchera avec le nom pour s'authentifier
- Group naming attribute : On renseigne ici "cn"
- Group member attribute : il s'agit de l'attribut qui va contenir les groupes
- Group Object Class : On peut laisser "group" pour un AD windows



Puis, on peut sauvegarder la configuration.

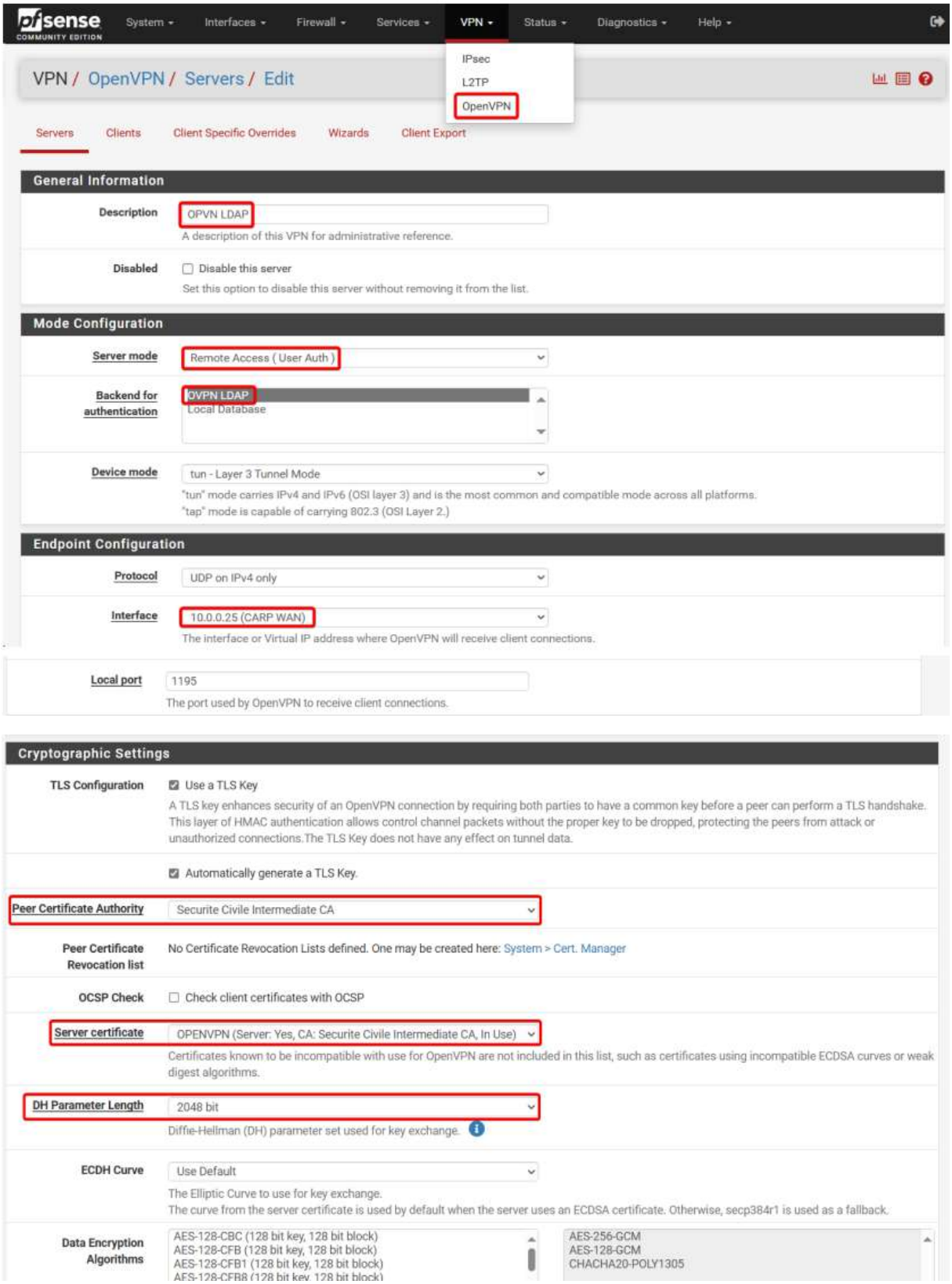
Il est ensuite possible de tester si la configuration mise en place est fonctionnelle en allant sous Diagnostics > Authentication. On renseigne ensuite le serveur d'authentification à tester et des credentials pour tester :

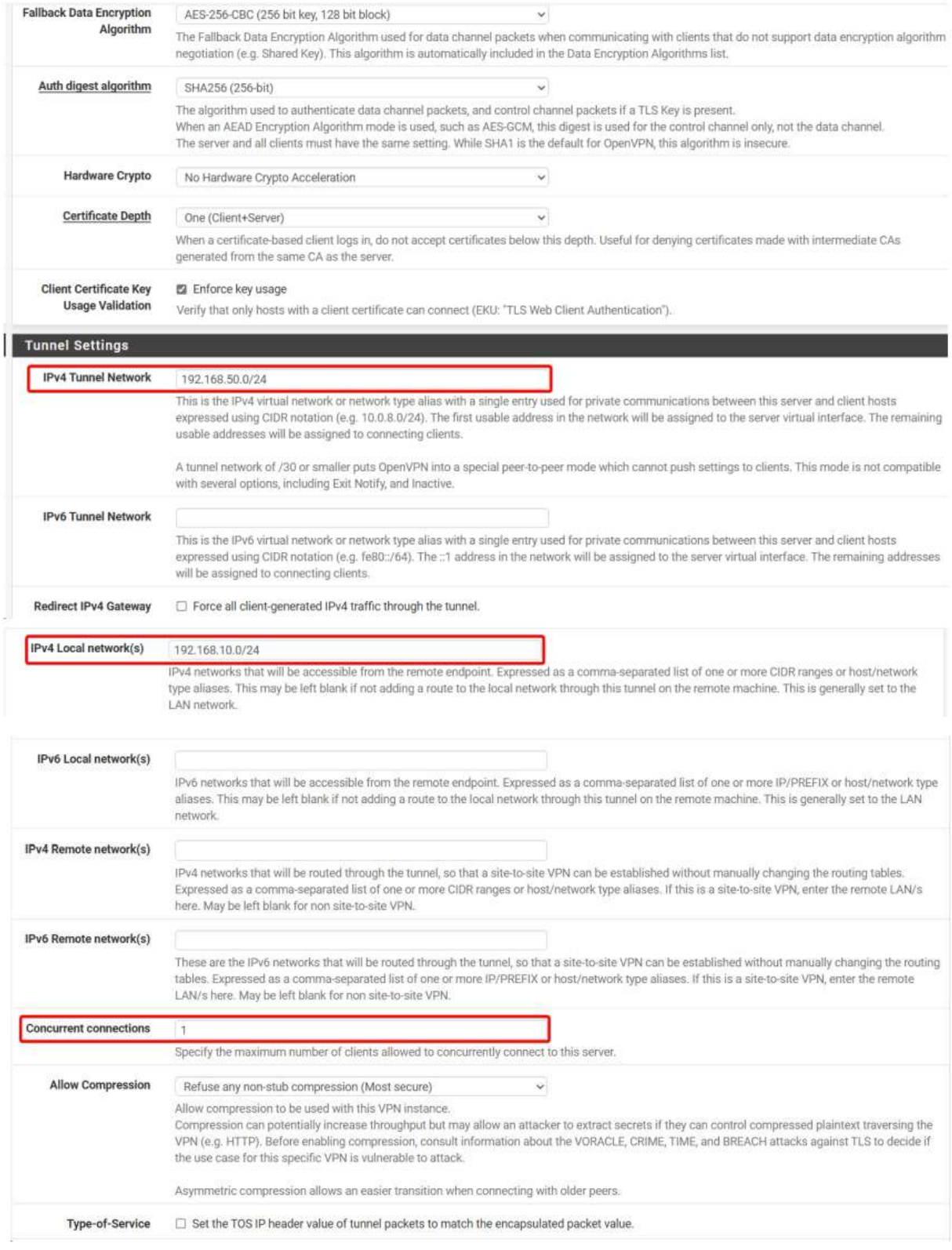


3.4.2) Configuration du serveur OpenVPN

Puis, pour configurer le serveur OpenVPN, il faut aller sous VPN > OpenVPN. Puis on ajoute un serveur et on renseigne les champs suivants :

- Description : On renseigne une description pour notre serveur OpenVPN
- Server mode : Remote Access (User Auth)
- Backend for authentification : On renseigne l'annuaire d'authentification configuré précédement
- Interface : On sélectionne ici notre IP WAN CARP
- Peer Certificate Authority : On reseigne l'authorité de certification qui sera nécessaire au client pour se connecter
- Server certificate : On reseigne notre certificat prévu pour le serveur OpenVPN et la longueur de la clé utilisée
- IPv4 Tunnel Network : Il s'agit des IP utilisés par OpenVPN pour la communication entre le client et le serveur
- IPv4 Local Network : On renseigne les routes qui seront poussées au travers du VPN
- Conccurent connections : Il s'agit du nombre de connexion simultanées

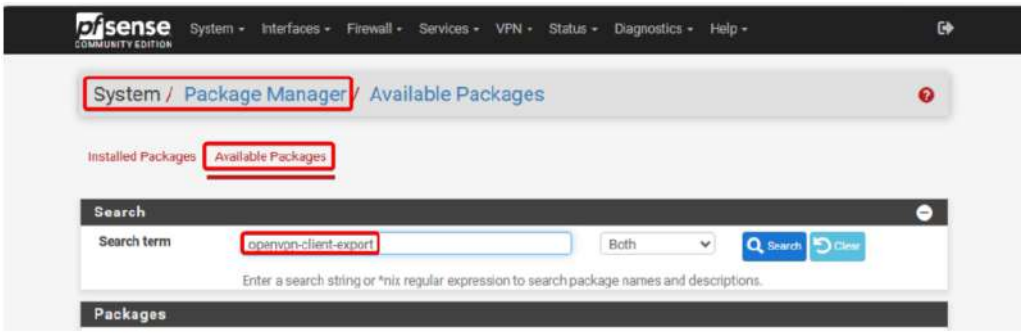

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
IPsec
L2TP
OpenVPN
VPN / OpenVPN / Servers / Edit
Servers
Clients
Client Specific Overrides
Wizards
Client Export
General Information
Description
OPVN LDAP
A description of this VPN for administrative reference.
Disabled
Disable this server
Set this option to disable this server without removing it from the list.
Mode Configuration
Server mode
Remote Access (User Auth)
Backend for authentication
OVPN LDAP
Local Database
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration
Protocol
UDP on IPv4 only
Interface
10.0.0.25 (CARP WAN)
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port
1195
The port used by OpenVPN to receive client connections.
Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.
Automatically generate a TLS Key.
Peer Certificate Authority
Securite Civile Intermediate CA
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check
Check client certificates with OCSP
Server certificate
OPENVPN (Server: Yes, CA: Securite Civile Intermediate CA, In Use)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.
ECDH Curve
Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Algorithms
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305



On peut ensuite cliquer sur "Save".

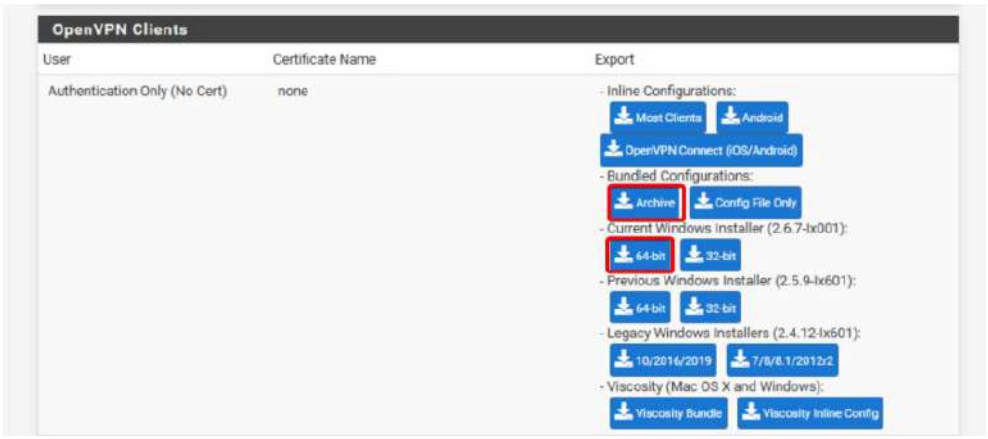
3.4.3) Exporter la configuration client pour le VPN

Pour exporter facilement la configuration client, on peut installer le package "openvpn-clientexport" depuis le Package Manager de Pfsense :



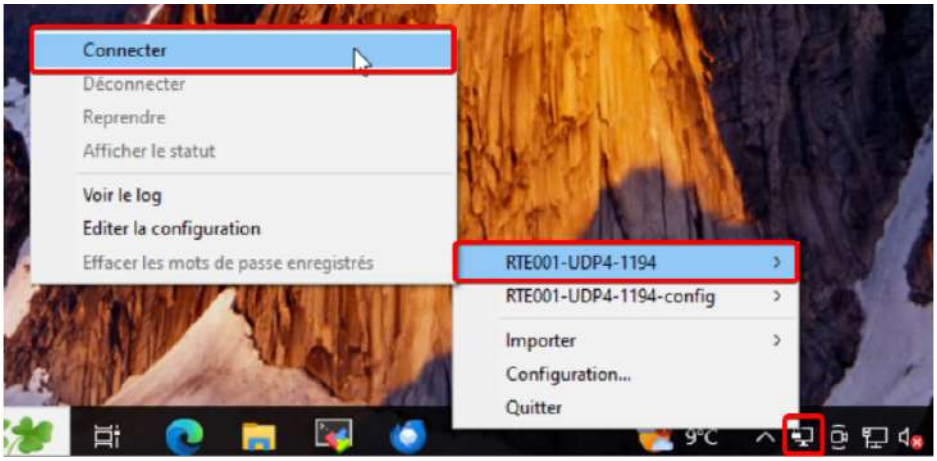
Ensuite, on peut aller sous VPN > OpenVPN puis on sélectionne notre configuration OpenVPN :

Enfin, on peut cliquer sur le Bundled Configuration ou directement installer le OpenVPN avec le fichier de configuration :

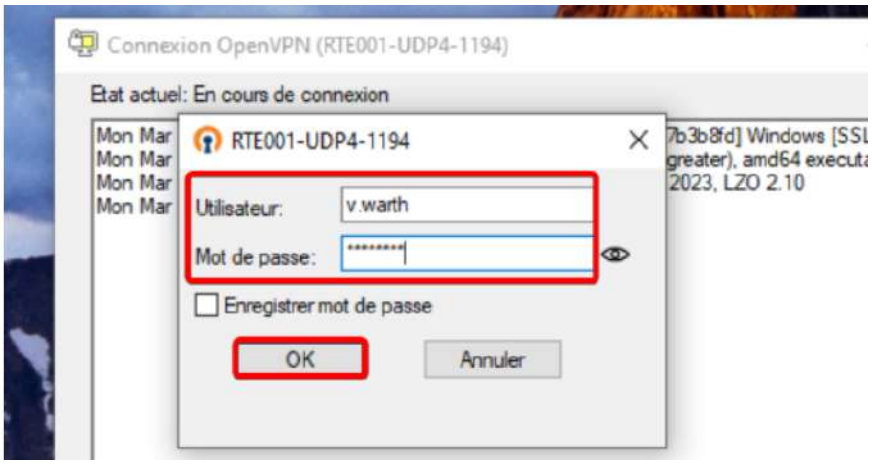


3.4.4) Se connecter avec un client OpenVPN

Une fois le client installé, il faut faire clic droit sur le logo OpenVPN, puis sélectionner la configuration adéquate et enfin cliquer sur "Connecter" :



Ensuite, on renseigne les mots de passe Active DIrectory et on peut cliquer sur OK, on est ensuite connecté :



4) INSTALLATION ET CONFIGURATION DE CHECKMK

CheckMK est une solution de monitoring, simple, ergonomique qui permet de faire des remontées d'informations et de logs principalement via un Agent ou le protocole SNMP.

4.1) Prérequis système

Pour installer CheckMK nous utiliserons une machine sous Debian 12.

Les prérequis annoncés par CheckMK qui seront nécessaire pour notre installation sont les suivants :

- Avoir un système à l'heure qui se synchronise sur un serveur NTP
- Disposer d'un serveur SMTP

Il est possible de retrouver les autres recommandations/prérequis système sur la documentation de CheckMK : https://docs.checkmk.com/latest/fr/install_packages.html

4.2) Mise à jour du système

Nous allons tout d'abord vérifier que les sources apt sont correcte :

```
vi /etc/apt/source.list

deb http://deb.debian.org/debian/ bookworm main
deb https://security.debian.org/debian-security bookworm-security main
# deb http://deb.debian.org/debian bookworm-updates main
```

Ensuite, avant de commencer l'installation, il faut mettre à jour le système et installer wget :

```
apt update && apt upgrade -y
apt install wget -y
```

4.3) Installation de CheckMK

Pour l'installation, il faut télécharger les packages checkmk et les installer :

```
cd /tmp/ && wget https://download.checkmk.com/checkmk/2.3.0p30/check-mk-raw2.3.0p30_0.bookworm_amd64.deb && apt install /tmp/check-mk-raw2.3.0p30_0.bookworm_amd64.deb
```

Ensuite on peut vérifier que la commande s'est exécutée correctement :

```
root@SRVMK002:/tmp# omd version

OMD - Open Monitoring Distribution Version 2.3.0p30.cre
```

Ensuite, on supprime les packages d'installation du /tmp :

```
rm /tmp/check-mk-raw-2.3.0p30_0.bookworm_amd64.deb
```

Enfin on créé un un site de monitoring CheckMk :

```
omd create monitoring
```

Cela devrait créer une sortie comme ceci :

```
Adding /opt/omd/sites/monitoring/tmp to /etc/fstab.
Creating temporary filesystem /omd/sites/monitoring/tmp...OK
Updating core configuration...
Generating configuration for core (type nagios)...
Precompiling host checks...OK
Executing post-create script "01_create-sample-config.py"...OK
Executing post-create script "02_cmk-compute-api-spec"...OK
Restarting Apache...OK
Created new site monitoring with version 2.3.0p30.cre.
The site can be started with omd start monitoring.
The default web UI is available at http://SRVMK002/monitoring/
The admin user for the web applications is cmkadmin with password: ZE4hpl0Vha6X
For command line administration of the site, log in with 'omd su
monitoring'.
After logging in, you can change the password for cmkadmin with 'cmk-passwd
cmkadmin'.
```

On peut ensuite lancer le site de monitoring que l'on a créé :

```
omd start monitoring
```

On devrait avoir un retour comme ceci :

```
Temporary filesystem already mounted
Starting agent-receiver...OK
Starting mkeventd...OK
Starting rrdcached...OK
Starting npcd...OK
Starting nagios...OK
Starting apache...OK
Starting redis...OK
Initializing Crontab...OK
```

CheckMk est maintenant installé néanmoins, il est nécessaire d'installer un MTA sur la machine afin d'utiliser les notifications par mail.

Pour se faire :

```
apt install msmtp msmtp-mta mailutils
```

Ensuite, il faut switch sur le user de notre site de monitoring. Dans notre cas l'utilisateur s'appelle monitoring :

```
su – monitoring

cat > .msmtprc << EOF
# ~/.msmtprc
defaults
auth on
tls on
tls_trust_file /etc/ssl/certs/ca-inter-certificates.pem
logfile ~/.msmtp.log
account securite-civil
host smtp.securite-civil.local
port 587
from checkmk@securite-civil.local
user checkmk
password 01_Admin

account default : securite-civil
EOF
```

On peut enfin modifier les droits :

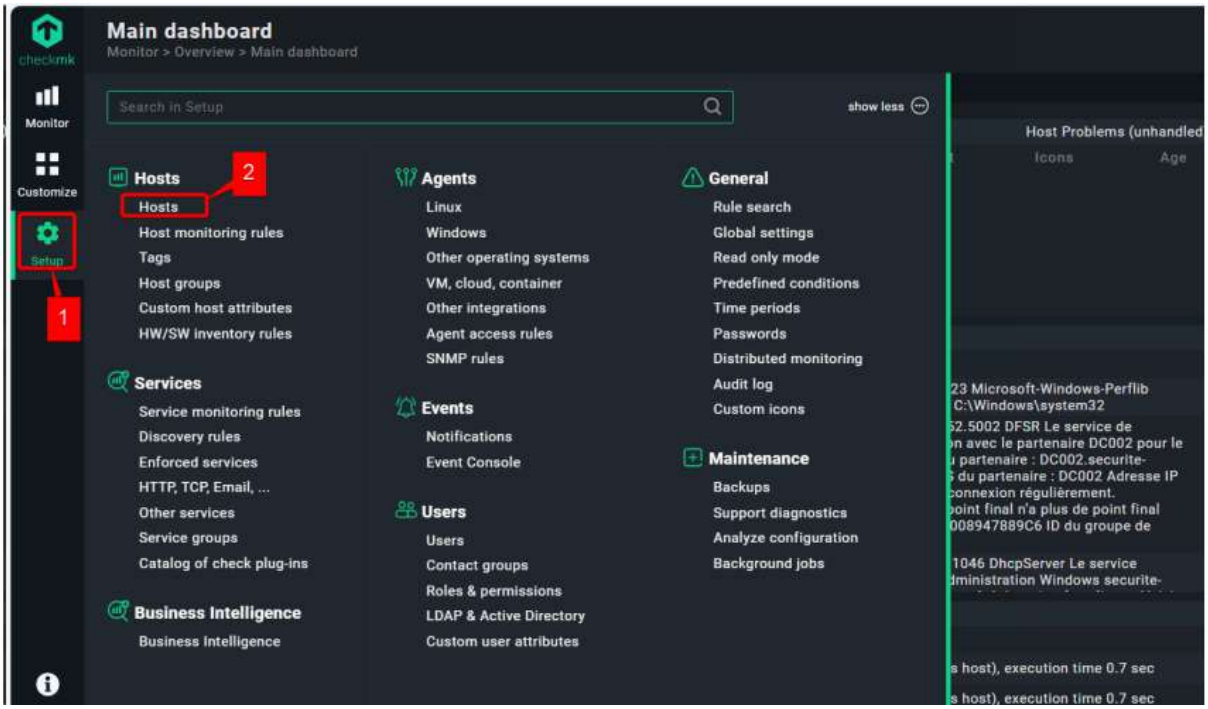
```
chmod 600 ~/.msmtprc
```

Ensuite, on peut tester d'envoyer un mail avec la commande suivante :

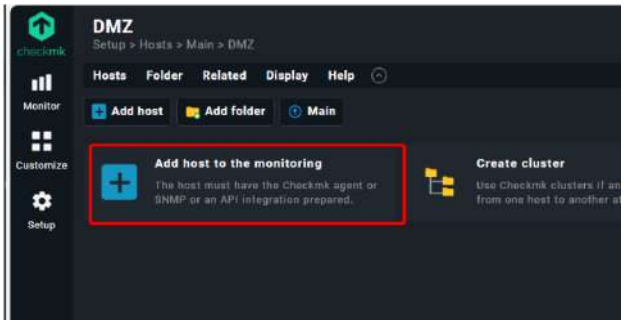
```
echo "Hello from msmtp!" | mail -s "Test SMTP" destinataire@example.com
```

4.4) Configuration de CheckMK

Pour ajouter un hôte à monitorer depuis l'interface web, il faut aller dans Setting > Hosts :

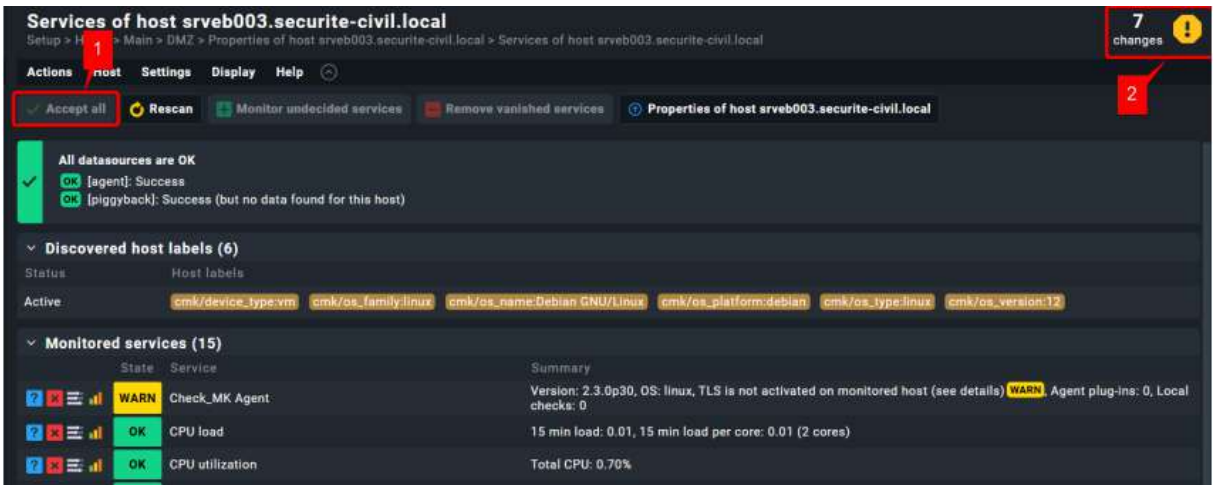


Puis, on clique sur "Add host to the monitoring" :

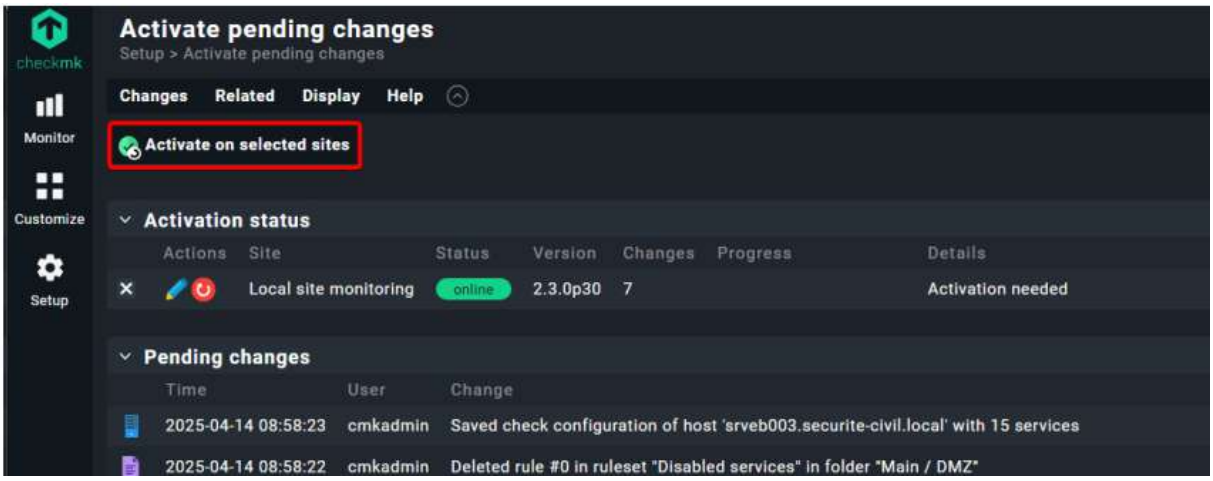


Ensuite, on ajoute les différentes informations comme l'alias DNS du serveur, son adresse IPv4, et pour finir on va cliquer sur "Save & run service discovery" :

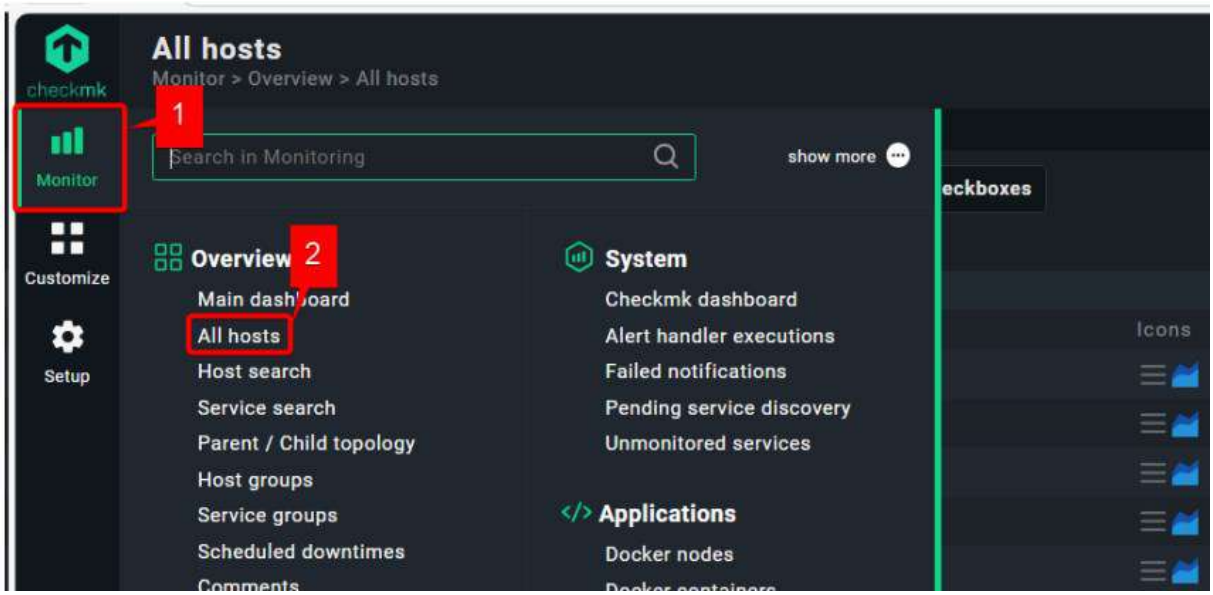
On peut ensuite sélectionner manuellement chaque service à monitorer ou les sélectionner tous avec "Accept all" et enfin, on clique sur "? changes" pour appliquer les changements :



Et enfin, on peut cliquer sur "Activate on selected sites" :



On peut vérifier la précense de l'hôte dans Monitor > All hosts :



5) MISE EN PLACE DE STALWART MAIL

Stalwart Mail est un serveur de messagerie moderne, rapide et sécurisé, conçu pour offrir une gestion fine des flux SMTP et IMAP à travers une configuration flexible et déclarative.

5.1) Installation de Stalwart

L'installation de Stalwart est assez simple et rapide, il faut tout d'abord télécharger le script d'installation :

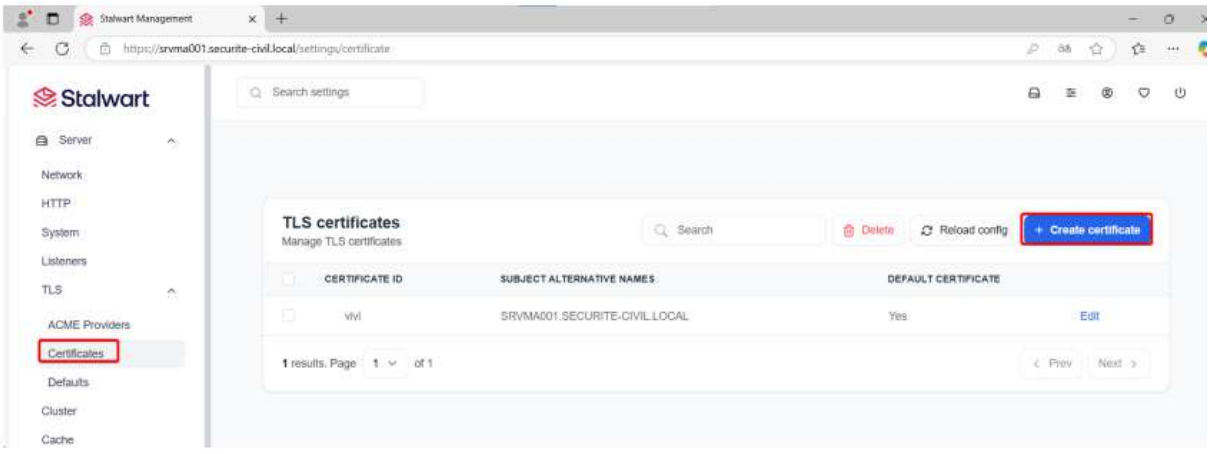
```
curl --proto '=https' --tlsv1.2 -sSf https://get.stalw.art/install.sh -o install.sh
```

Ensuite, il suffit de l'exécuter :

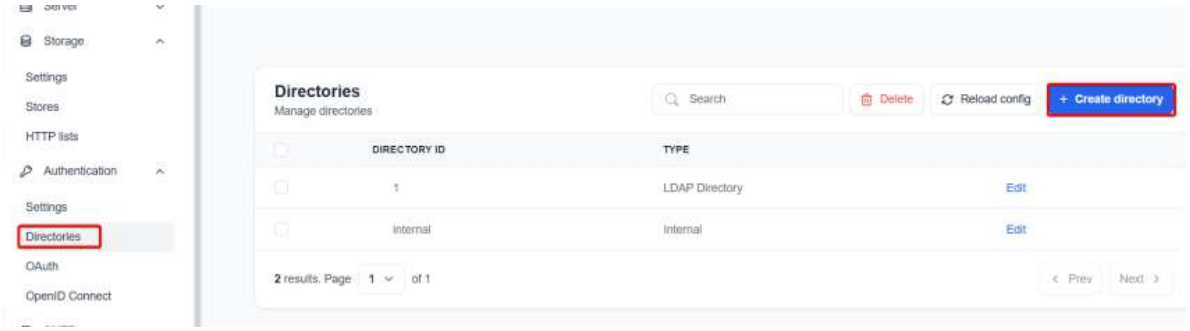
```
sh install.sh /path/to/install

✅ Configuration file written to /opt/stalwart-mail/etc/config.toml
🔑 Your administrator account is 'admin' with password 'w95Yuiu36E'.
🎉 Installation complete! Continue the setup at http://yourserver.org:8080/login
```

5.2) Configuration de Stalwart

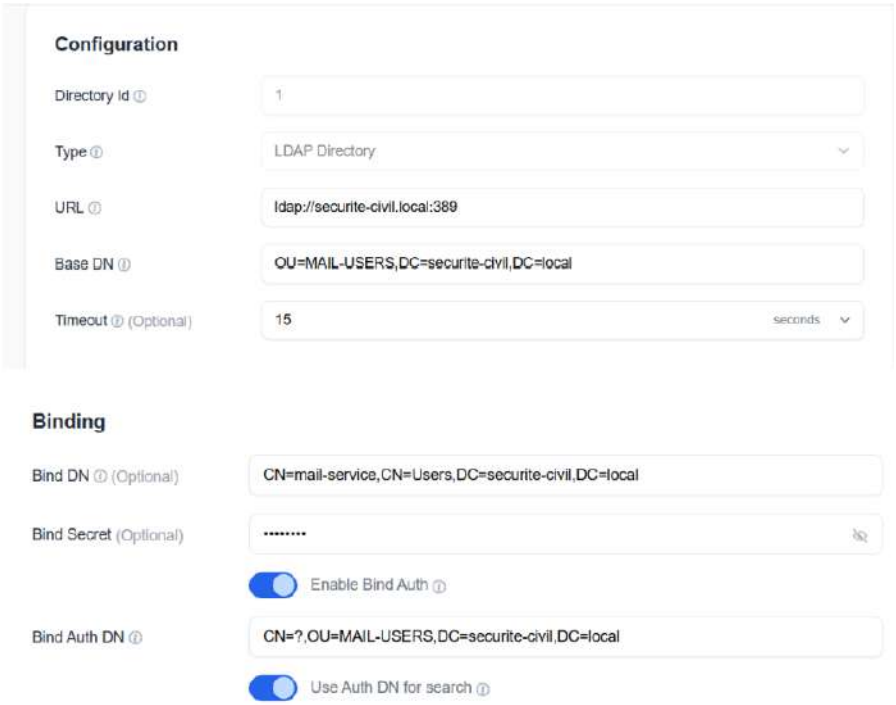
Tout d'abord, on peut configurer un certificat pour notre serveur en cliquant sur "Create certificate" :

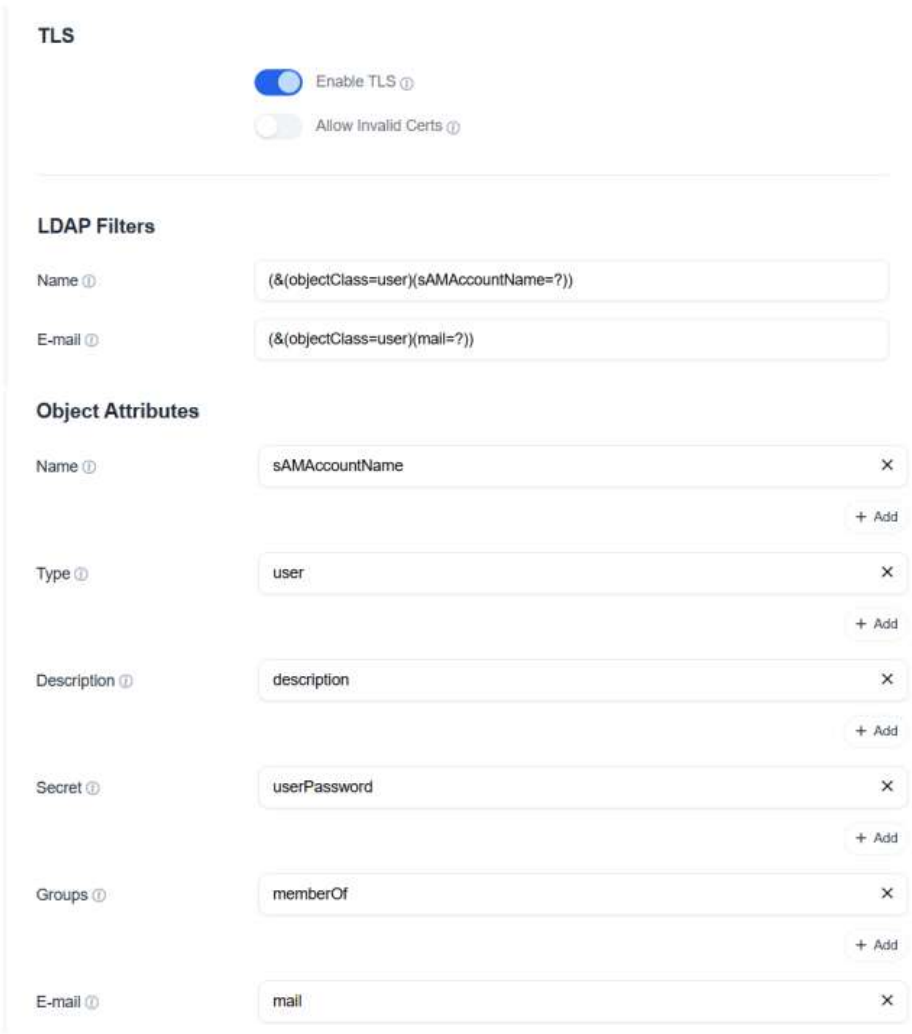


Ensuite, il faut configurer un "Directorie" pour réaliser une connexion avec l'AD et permettre l'authentification avec des comptes de l'AD :



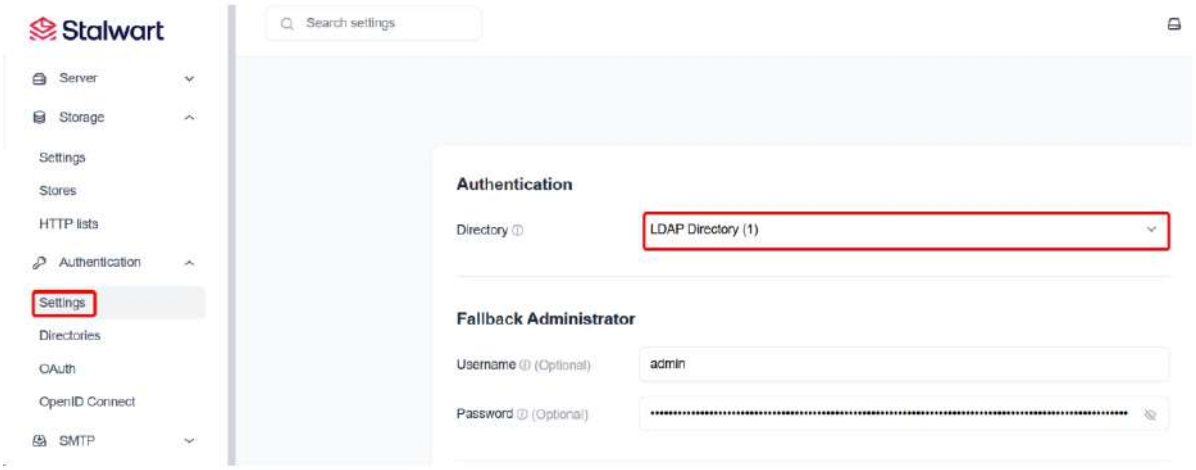
Ensuite, on configure le Directorie :





Après avoir configuré notre Directorie, il suffit de cliquer sur "Save & reload" :

Il ne reste plus qu'à le déclarer comme Directorie à utiliser, pour se faire il faut aller sous Authentication > Settings et sélectionner celui que l'on vient de créer :



Il faut ensuite créer les alias DNS sur notre serveur DNS. Stalwart indique les suivants en exemple dans sa documentation d'installation :

```
MX example.org. 10 mail.example.org.

TXT 202404e._domainkey.example.org. v=DKIM1; k=ed25519; h=sha256;
p=MCowBQYDK2VwAyEAOT2JN9F8SLTVFNEODDu22SD9RJDC282mugCAeXkzjH0=


TXT 202404r._domainkey.example.org. v=DKIM1; k=rsa; h=sha256;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAykeYJjv5N0AlnJ8gKF+/8qjbStiMFW
vPg+p3JPh96GPXEN6l9W/Ee6Lag6i3vLyTVH5dnRVRBhfWhc+Dc0nKreZe4f5i4L5M4RI31+RpEg
u4bCmncUIk2WzJgGBW5XbiOwXjge6OKWtJQN9d8Lc1AuryL5xeged9iS6xd/+EJz4WxAf18U+j3
8xmAm8fJUTBnQVeb/AZup+voSKAS59jyumsb0jQtXfX5xnwTFXdiX2OF8LRrmmNs/ObHozgHft
xAv+YCiSU4bqSlKNPQIrN5kk1YnZDnLlc1Gr66AWlmdUVE7PWtZPTy4f8+uHO93EW3WUxLmy
nZm+Syn9FTJC2uwID  AQAB TXT mail.example.org. v=spf1 a -all ra=postmaster


TXT example.org. v=spf1 mx -all ra=postmaster


TXT _dmarc.example.org. v=DMARC1; p=reject; rua=mailto:postmaster@example.org;
ruf=mailto:postmaster@example.org
```

Il ne reste plus qu'à utiliser un client mail comme Thinderbird pour se connecter via les identifiants LDAP.

6) MISE EN PLACE DE EBRIGADE

eBrigade est une solution open source de gestion opérationnelle permettant de centraliser et de suivre en temps réel les interventions, le personnel, et les ressources d'une organisation de sécurité civile.

6.1) Installation de eBrigade

Tout d'abord, il faut installer apache2 et le module php de apache2 :

```
apt update && apt install apache2 7zip apt-transport-https lsb-release ca-certificates wget
curl gnupg -y
```

Ensuite, nous allons ajouter les repository pour installer PHP 7.4 sur Debian 12 (par défaut il n'est plus disponible)

```
wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg

echo "deb https://packages.sury.org/php/ $(lsb_release -sc) main" | tee
/etc/apt/sources.list.d/php.list

apt update && apt install php7.4 libapache2-mod-php7.4 php7.4-mysql php7.4-cli php7.4-
curl php7.4-xml php7.4-mbstring php7.4-zip php7.4-gd
```

Ensuite, il faut décompresser l'archive qui contient le site php de ebrigade dans le dossier par défaut d'apache /var/www/html :

```
7zz x /tmp/ebrigade-5.3.2.zip -o/var/www/html/
```

Puis, il faut mettre les bons droits pour que le serveur apache2 puisse gérer les fichier :

```
chown -R root:www-data /var/www/html/* && chmod -R 775 /var/www/html/ebrigade-5.3.2/
```

Ensuite, il faut installer une BDD

```
curl -LsS https://r.mariadb.com/downloads/mariadb_repo_setup | sudo bash -s -- --mariadb-server-version=11.4
apt update && apt install mariadb-server
```

On se connecte ensuite à mysql et on créé une BDD :

```
mysql -u root -p
```

On envoie donc les requêtes SQL ci-dessous :

```
CREATE DATABASE ebrigade_db CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'ebrigade_user'@'localhost' IDENTIFIED BY '01_Admin';
GRANT ALL PRIVILEGES ON ebrigade_db.* TO 'ebrigade_user'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

6.2) Configuration de apache2

```
a2enmod ssl
systemctl restart apache2
```

Si l'on a un certificat, on peut modifier le site apache default-ssl pour indiquer le chemin vers le certificat :

```
nano /etc/apache2/sites-available/default-ssl.conf

<SNIP...>
DocumentRoot /var/www/html/ebrigade-5.3.2
<SNIP...>
SSLCertificateFile /etc/ssl/certs/srveb003.pem
SSLCertificateKeyFile /etc/ssl/private/srveb003.key
<SNIP...>
```

On active ensuite la redirection HTTP vers HTTPS :

```
nano /etc/apache2/sites-available/000-default.conf


<SNIP...>
Redirect permanent / https://srveb003.securite-civil.local/
<SNIP...>
```

Enfin, on peut enable le site default-ssl et reload apache2 :

```
a2ensite default-ssl.conf
systemctl reload apache2
```

6.3) Configuration de eBrigade

Pour terminer, il faut lancer la configuration de eBrigade, pour se faire, on se connecte sur l'URL de notre eBrigade : https://srveb003.securite-civil.local/

Et on renseigne l'ensemble des informations concernant notre BDD créé plus tôt :

Puis on choisit un mot de passe pour l'Admin :

Ensuite eBrigade nous demandera des informations sur l'organisation.

eBrigade est maintenant opérationnel.

FIN