Documentation AP4

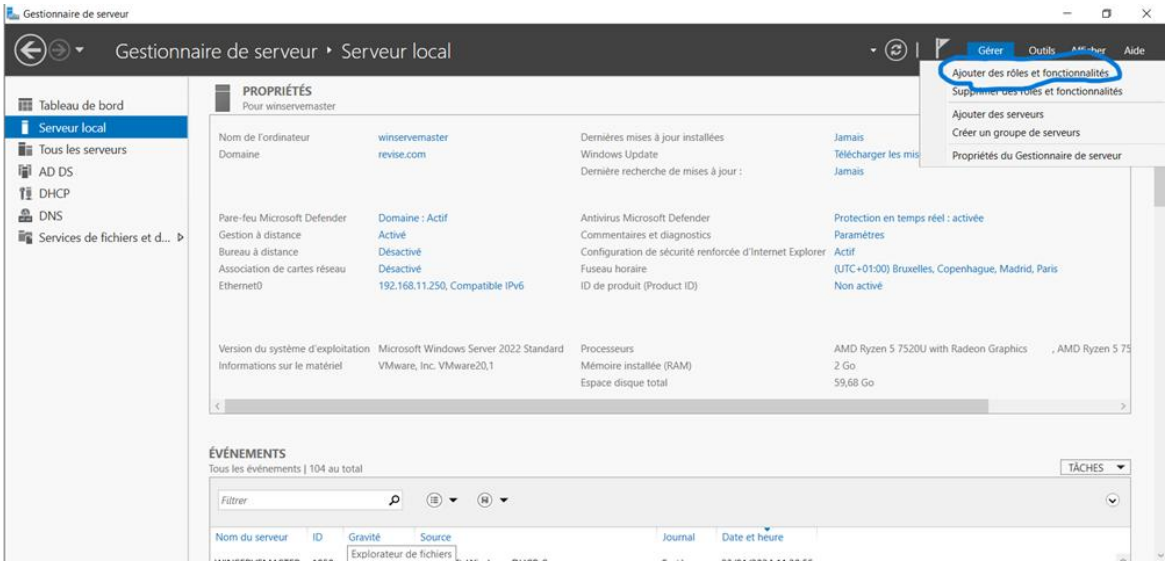
MEZZAROBBA Nathan
RICHTER Paul

Contrôleurs de domaines

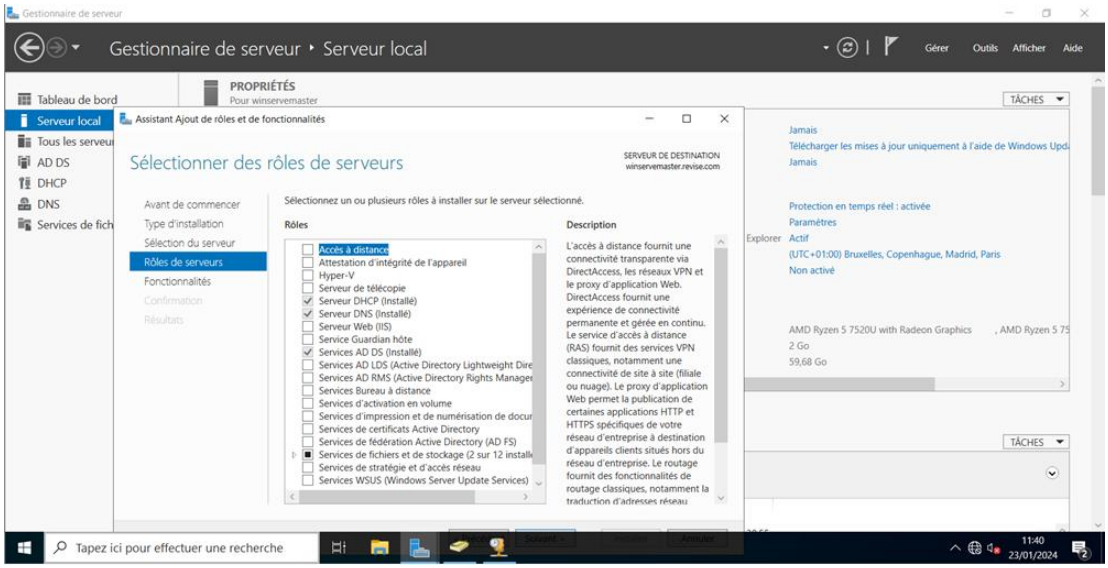
Les contrôleurs de domaine jouent un rôle clé dans la gestion des ressources réseau, en assurant l'authentification centralisée, la gestion des comptes utilisateurs et l'application des stratégies de groupe.

Installation de l'ADDS

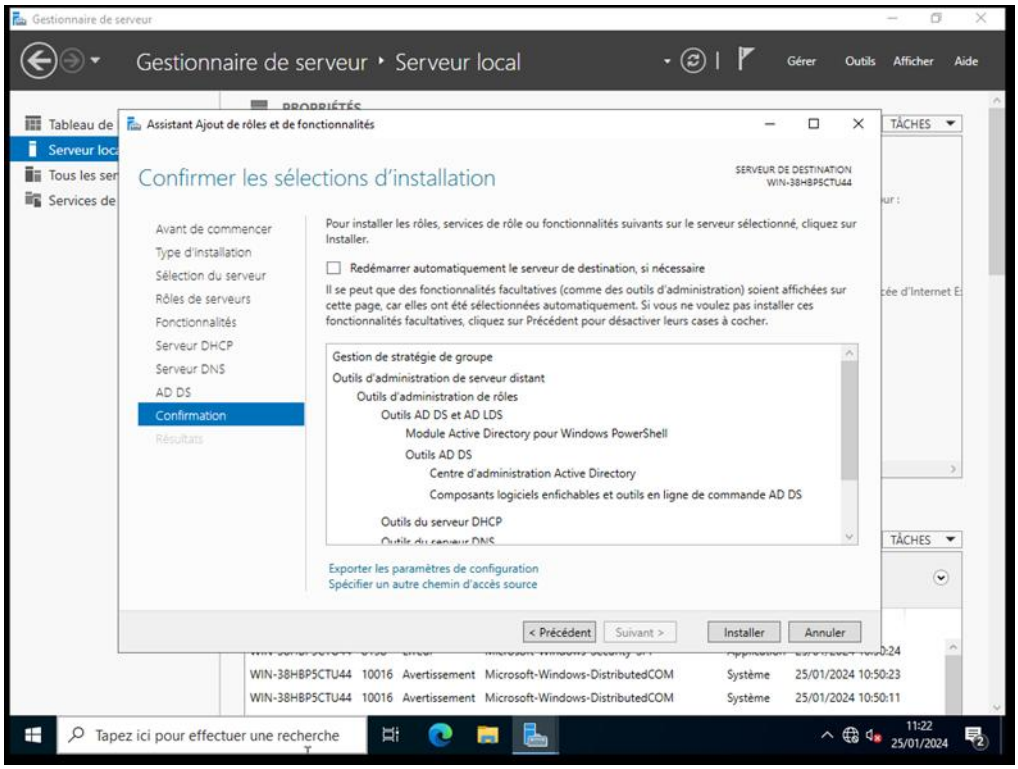
On va sur le gestionnaire de serveur et on clique « Gérer » et « ajouter rôles et fonctionnalités » :



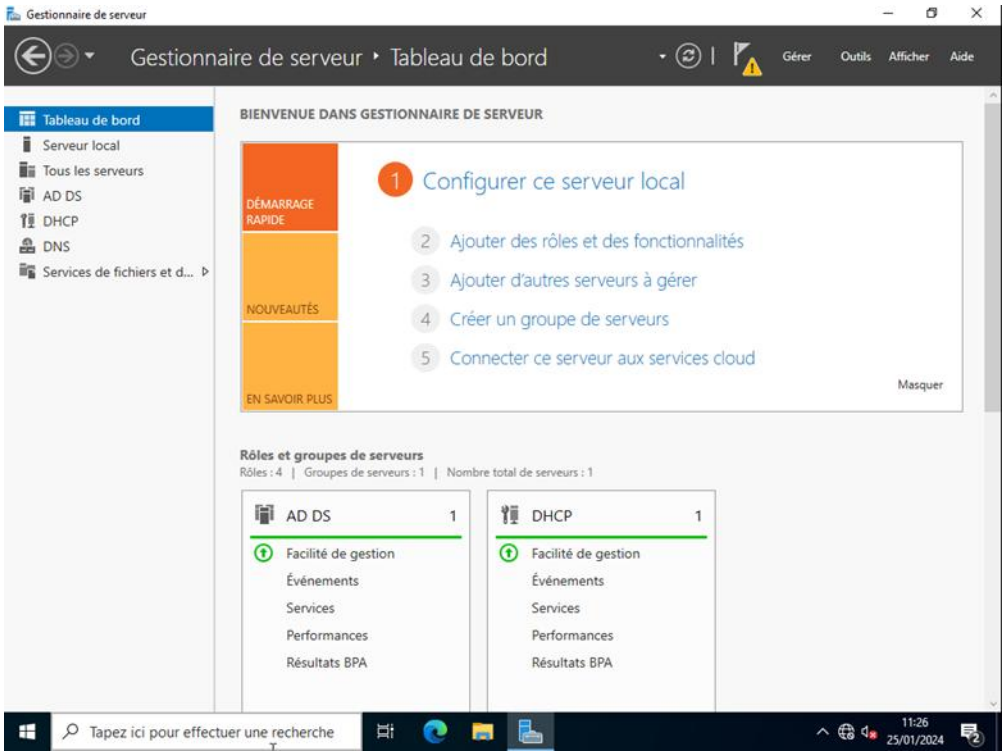
On fait suivant jusqu'à arriver sur cette fenêtre. On coche « Serveur AD DS » quand la fenêtre s'ouvre, cliquer sure « ajouter des fonctionnalités ». On ne décoche rien et suivant.



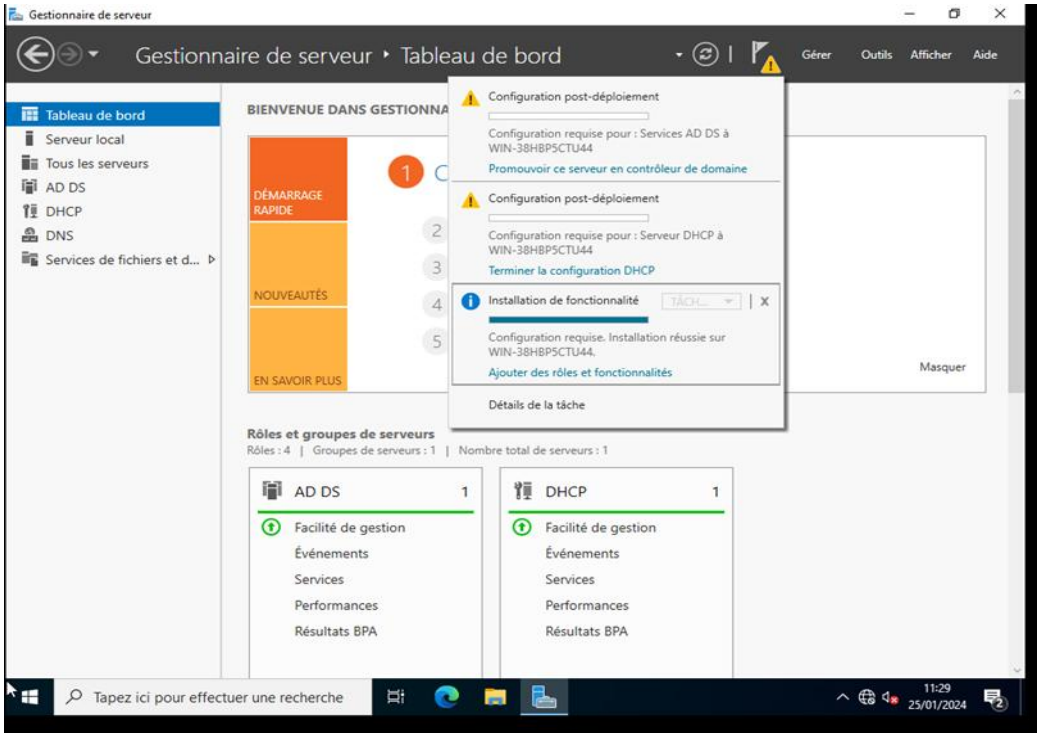
On clique sur Suivant jusqu'à arriver sure cette page. Là on clique sur installez et on attend :



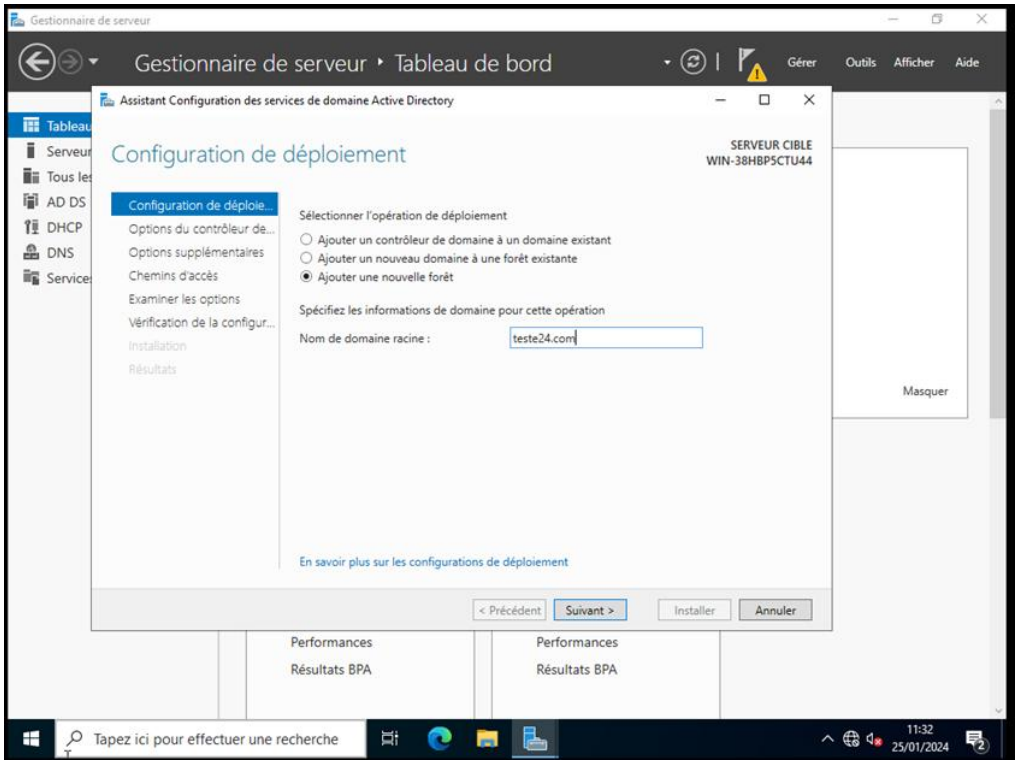
Une fois que tout est installé on clique sur « fermer » et un triangle jaune aura apparu sous le drapeau en haut à droite :



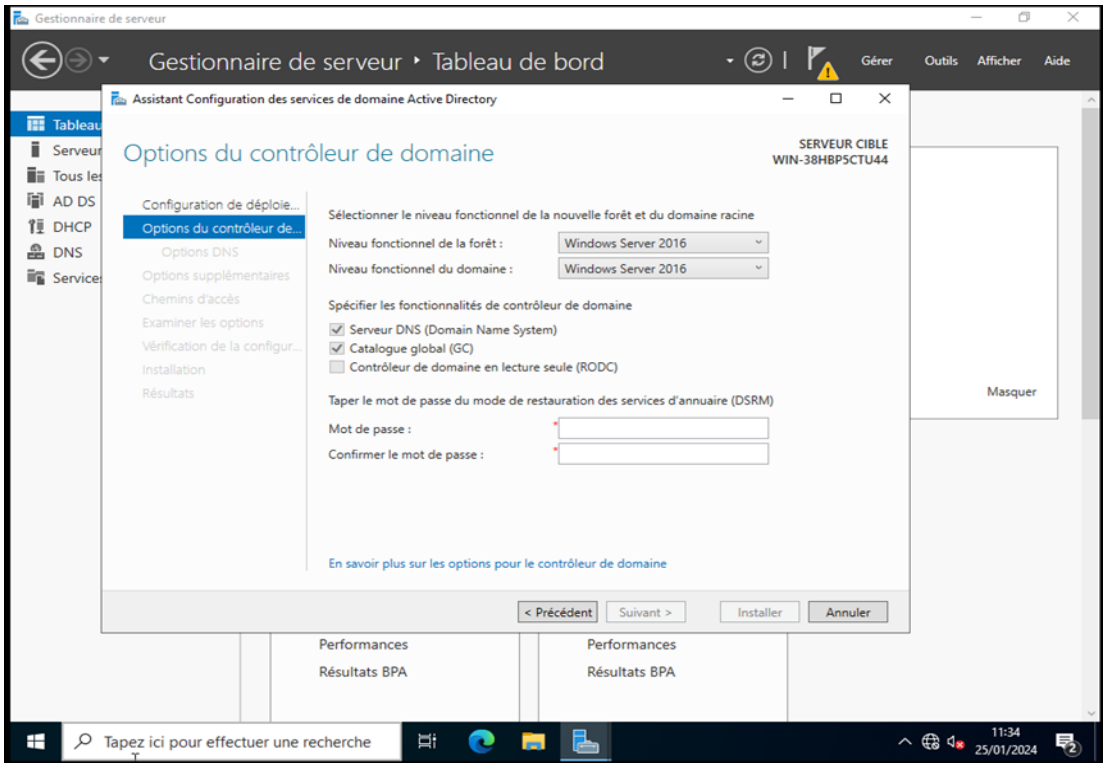
On clique dessus pour commencer à configurer l'ADDS. Une fois le menu ouvert on clique sur les promouvoir ce serveur en contrôleur de domaine :



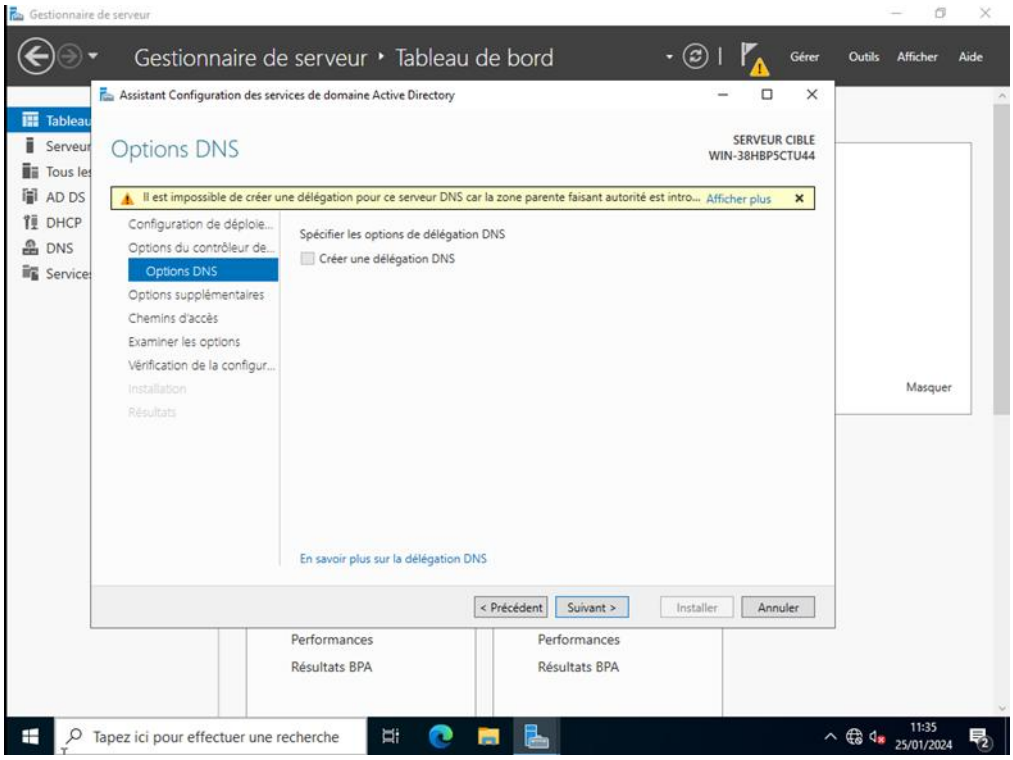
On commence par l'ADDS. On coche « crée une nouvelle forêt » et on lui donne un nom en point. Ici j'ai choisi « test24.com » pour l'exemple puis suivant :



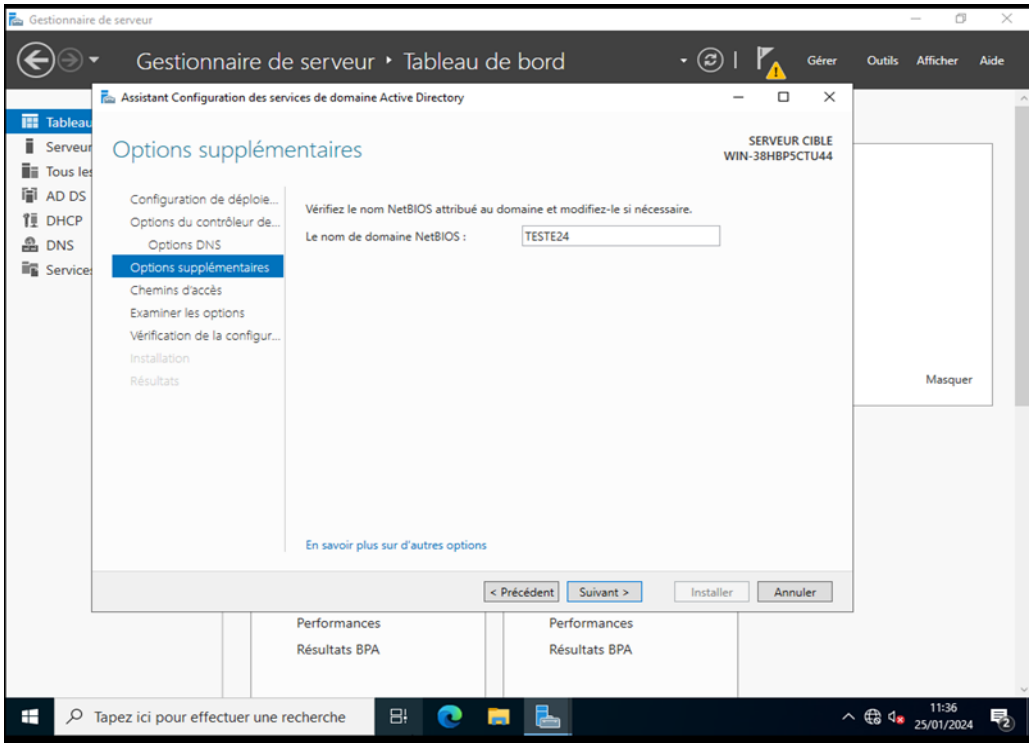
Ici on ne touche uniquement le mot de passe. Une fois renseigné on clique sur suivant :



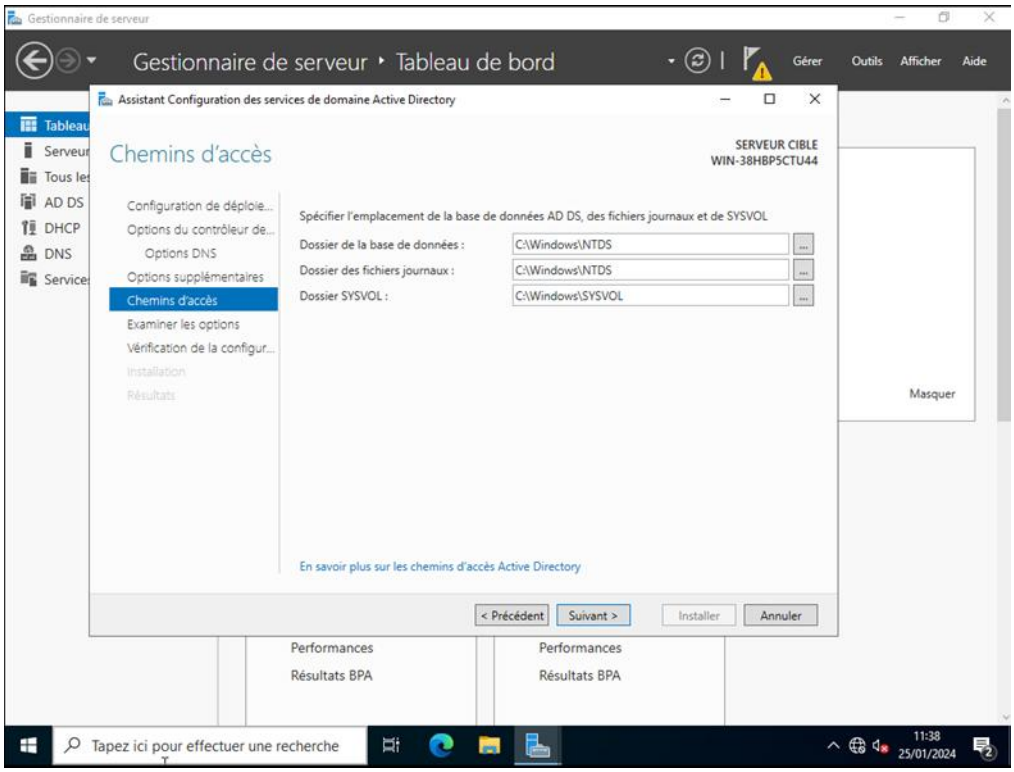
Rien à toucher ici, suivant :



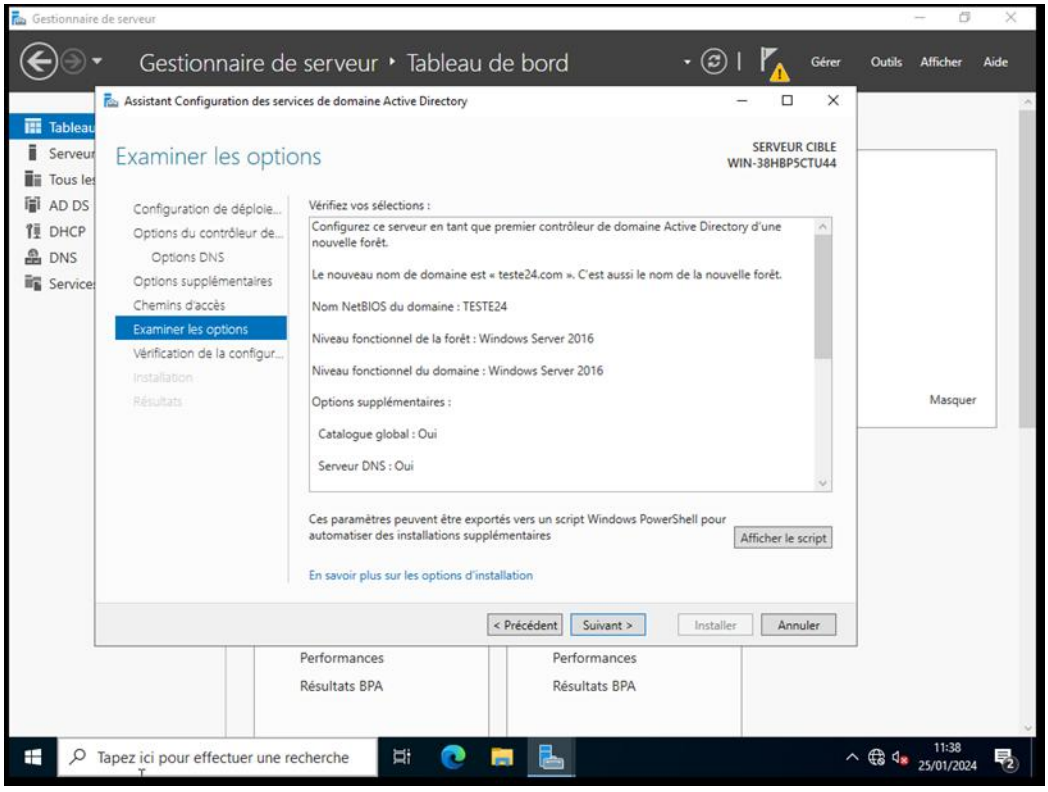
Important, ici Windows va nous « générer » notre nom de domaine, ne pas l'oublier. On fait Suivant :



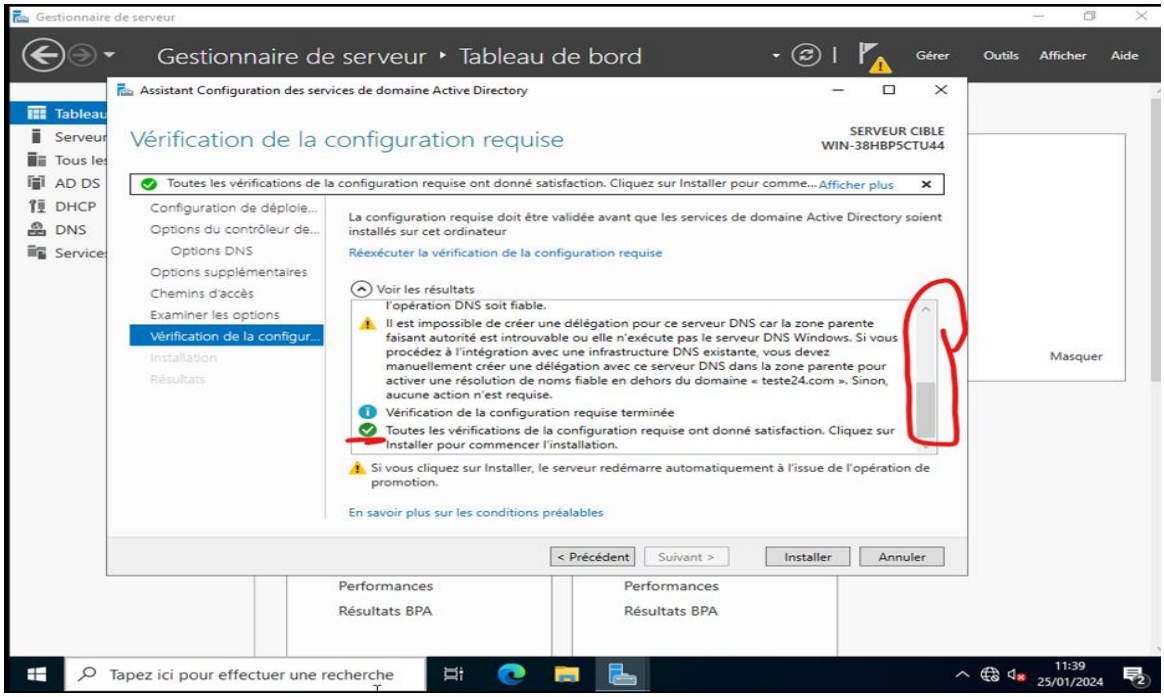
Rien à toucher, suivant :



Rien à toucher, suivant :



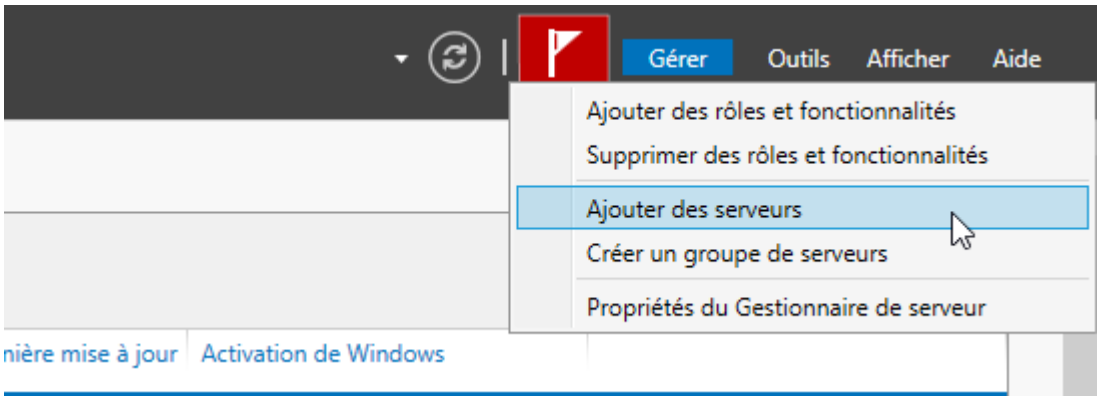
Ici on descend pour vérifier que tout est correcte, c'est vert donc on peut installer ADDS. On clique sure Installer :



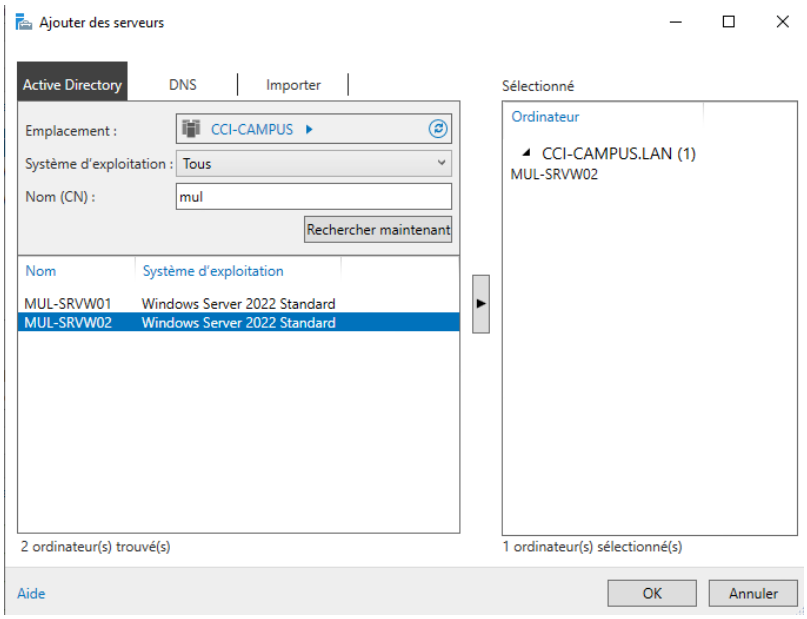
Une fois installé une fenêtre bleue apparait et vous dit de redémarre votre serveur, cliquez sur fermer. Votre serveur va redémarrer et sera contrôleur de domaine.

Redondance de l'AD

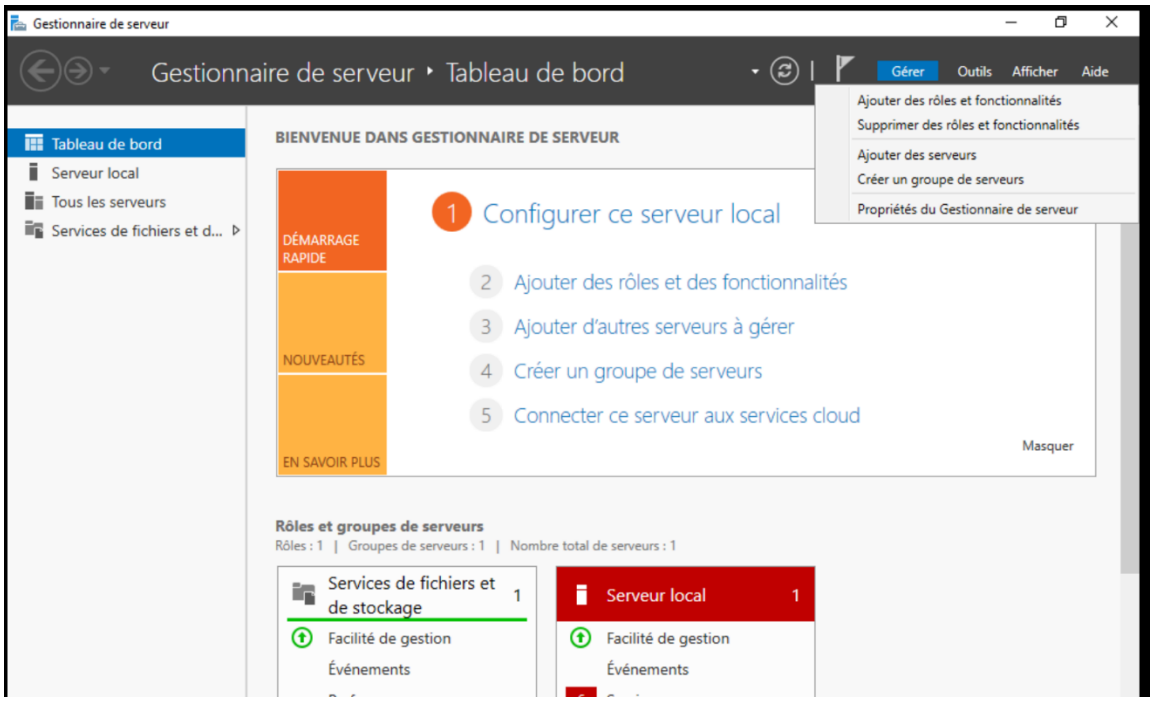
Vous pouvez ajouter votre serveur en version core au serveur que vous gérer depuis une version avec UI.
Pour cela allez dans gérer et ajouter des serveurs.



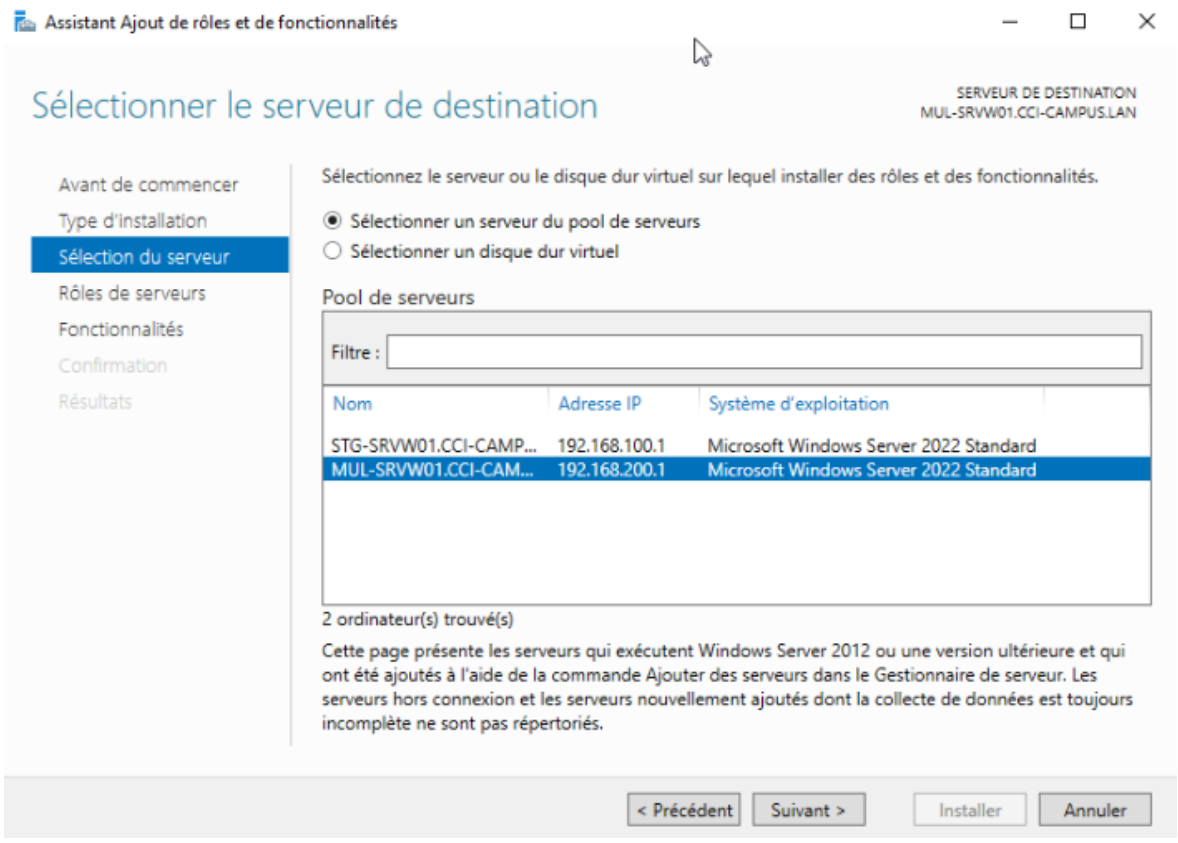
Sélectionner ensuite le serveur que vous voulez gérer



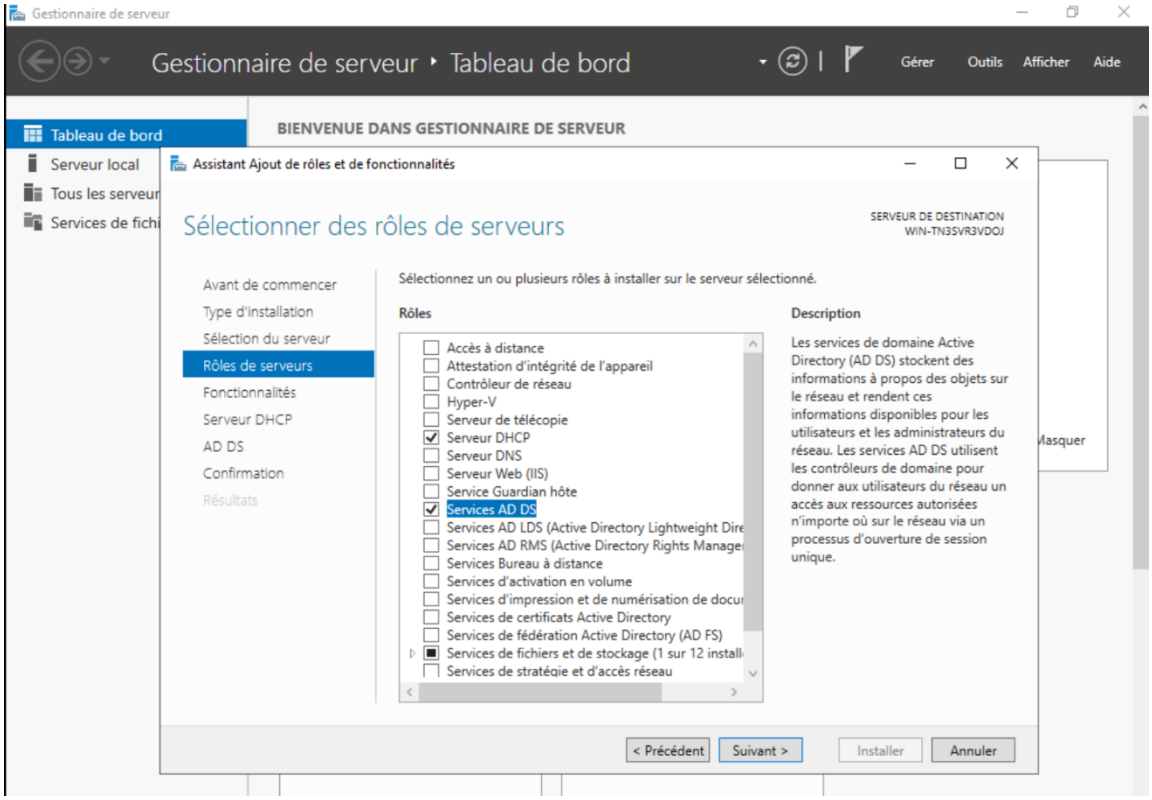
Allez dans Gérer, Ajouter des rôles et fonctionnalités.



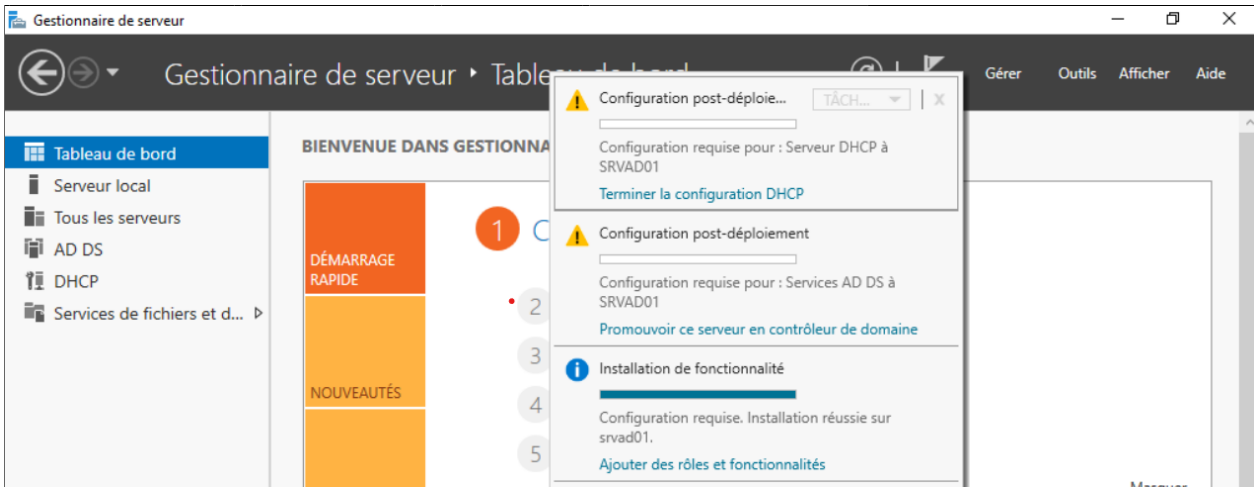
Faites Suivant jusqu'à cette page ou vous choisissez sur quel serveur ajouter le rôle.



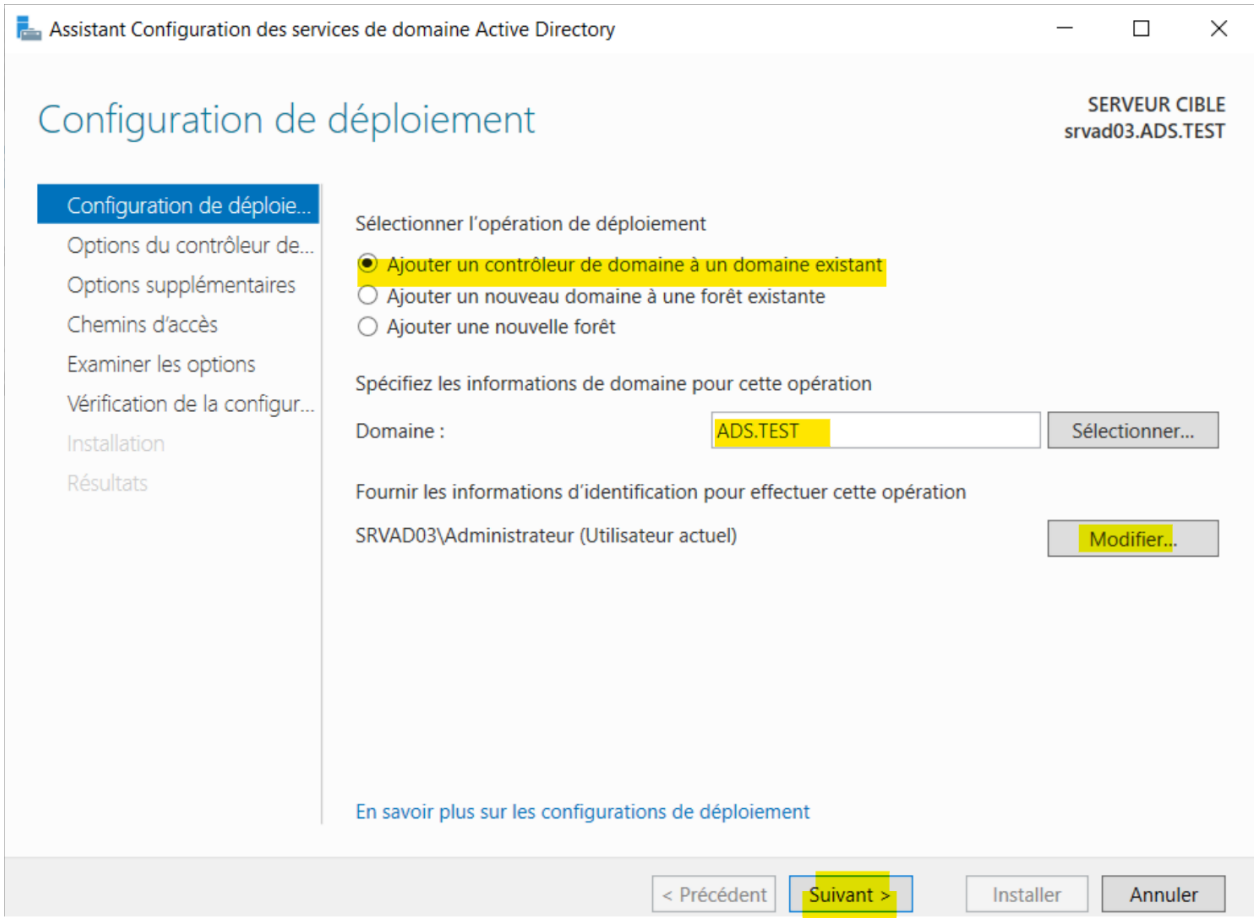
Sélectionnez AD DS.
Refaites Suivant puis Installer



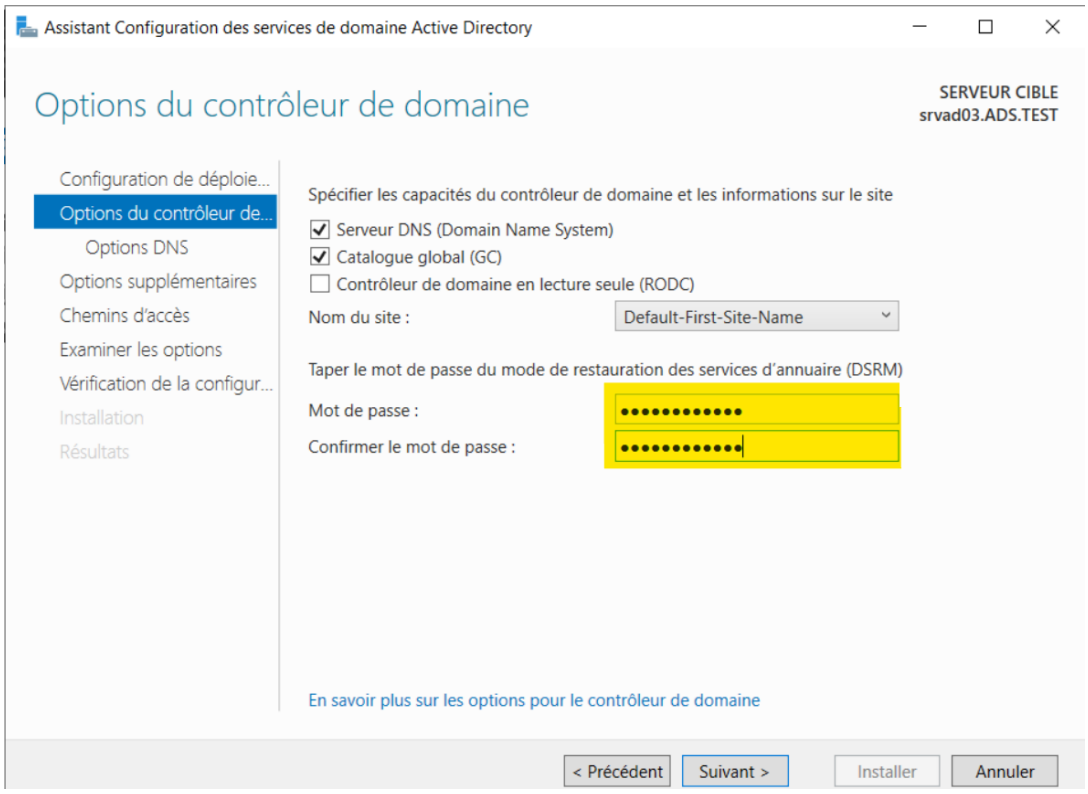
Cliquez sur le drapeau
Cliquez sur Promouvoir ce serveur en contrôleur de domaine



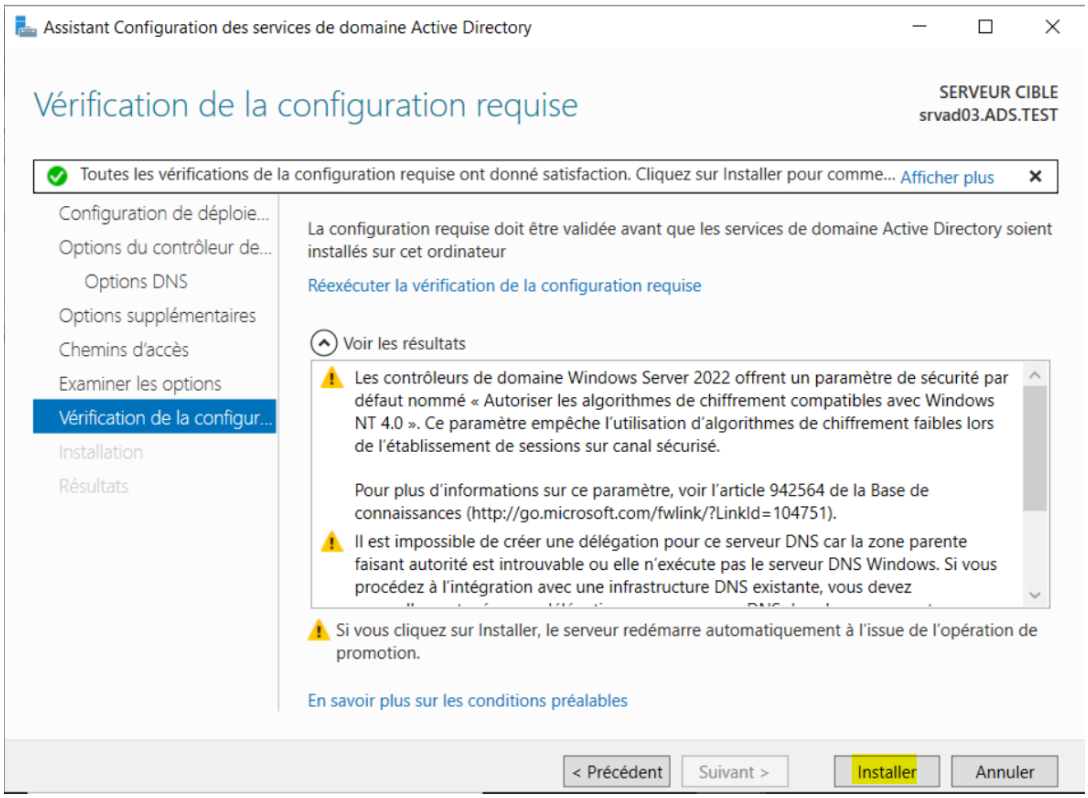
Ajoutez un contrôleur au domaine et rentrer un compte administrateur



Rentrez un mot de passe



Cliquez sur suivant jusqu'à arriver sur cette page

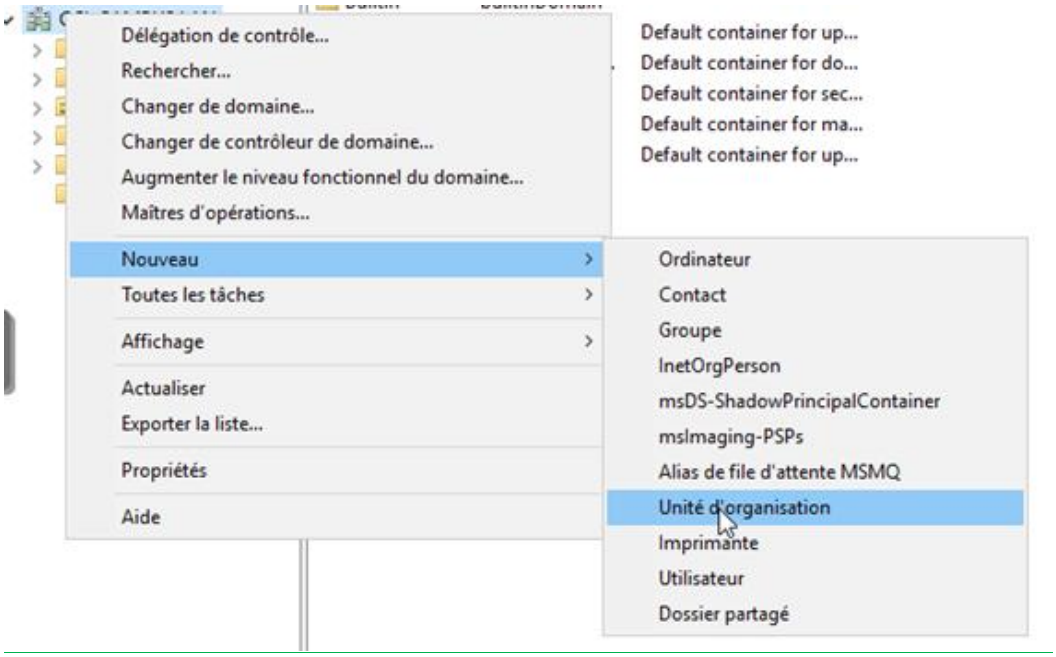


Si vous avez tout bien fait vous n'aurez pas d'erreur ici cliquez sur installer. Après le redémarrage votre AD est redondant.

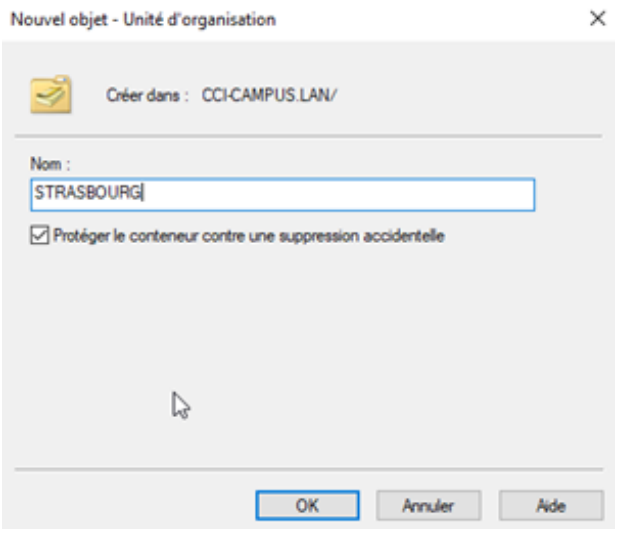
Création d'unités organisationnelles

Allez dans outils puis dans utilisateurs et ordinateurs Active Directory

Cliquez sur nom de domaine puis :

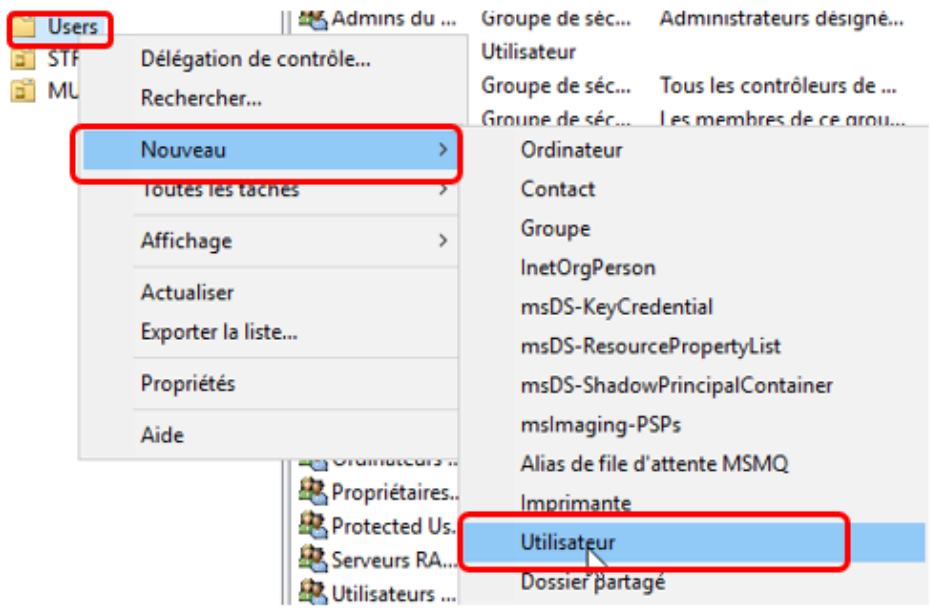


Nommez votre unité

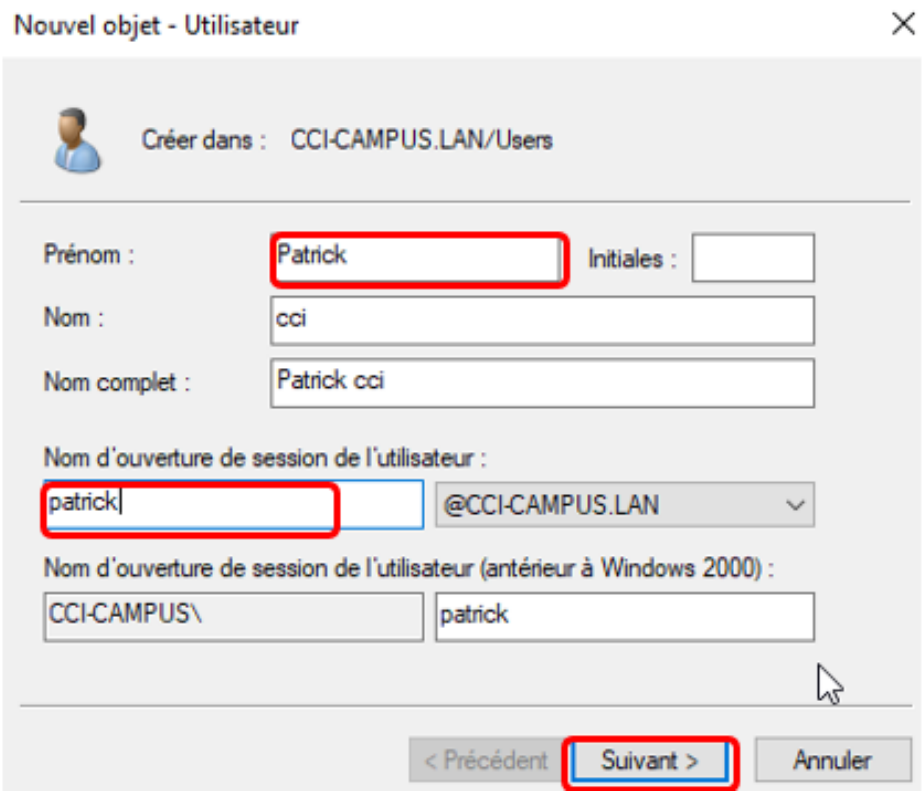


Création d'un utilisateur

Toujours dans la gestion active directory sélectionner l'UI ou vous voulez créer votre utilisateur puis :

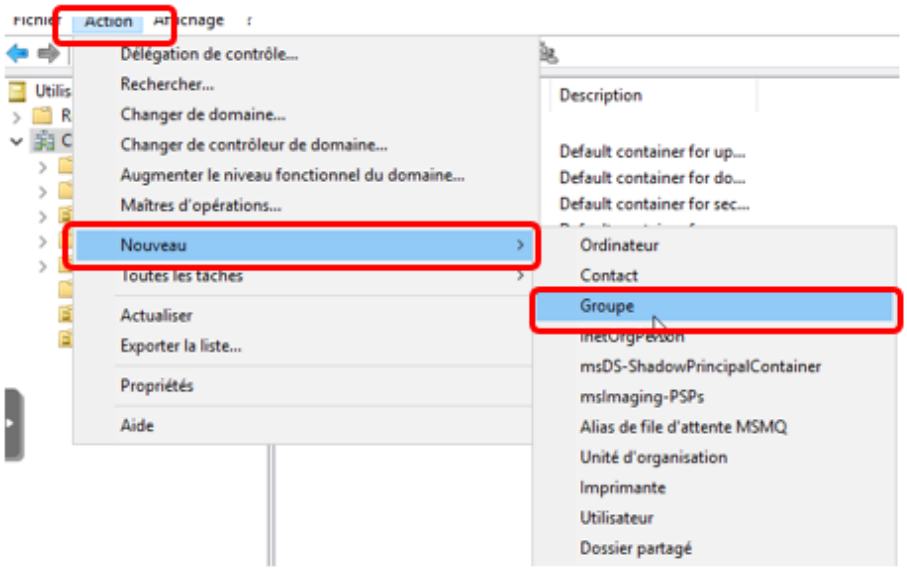


Nommez votre utilisateur et donnez-lui son identifiant

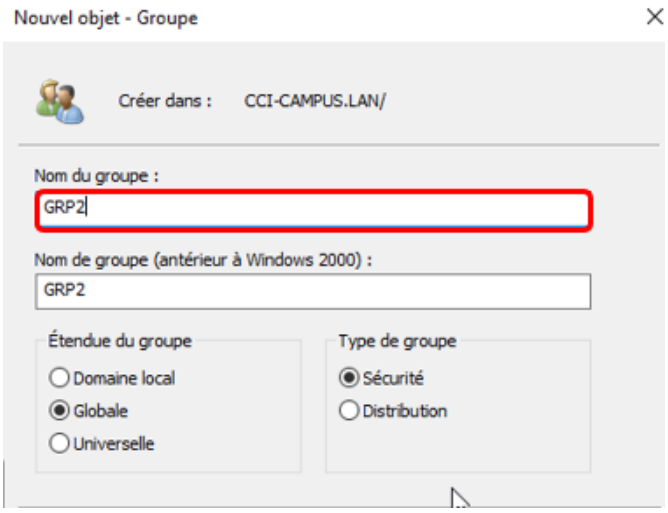


Création de groupe de sécurité

Dans la console de gestion faites :

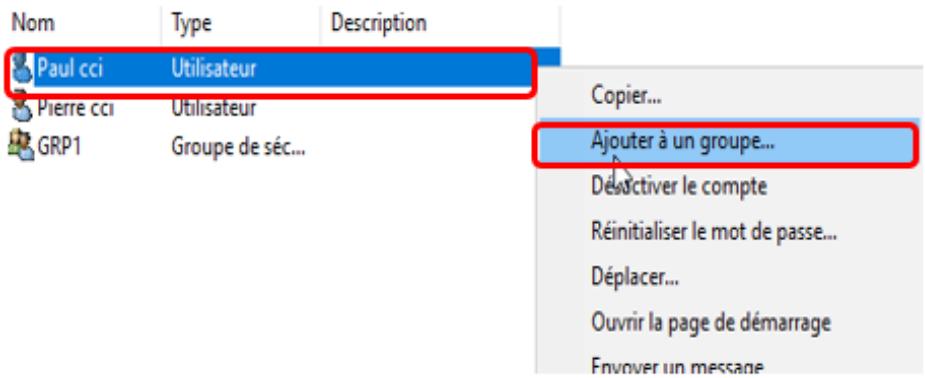


Nommez le groupe

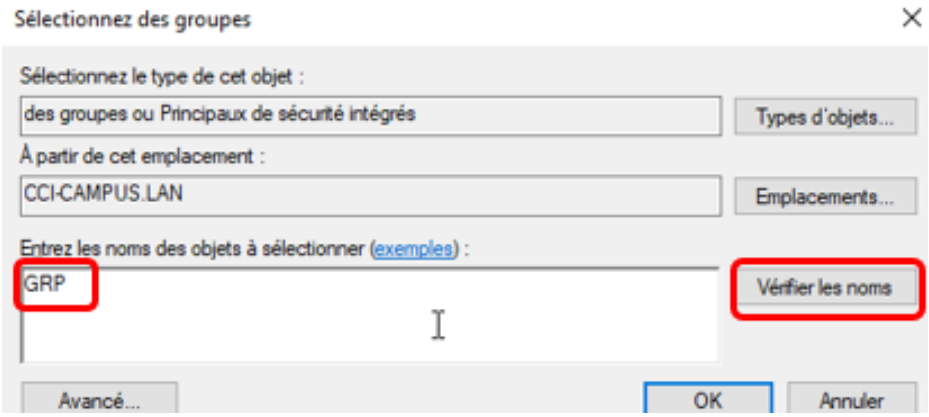


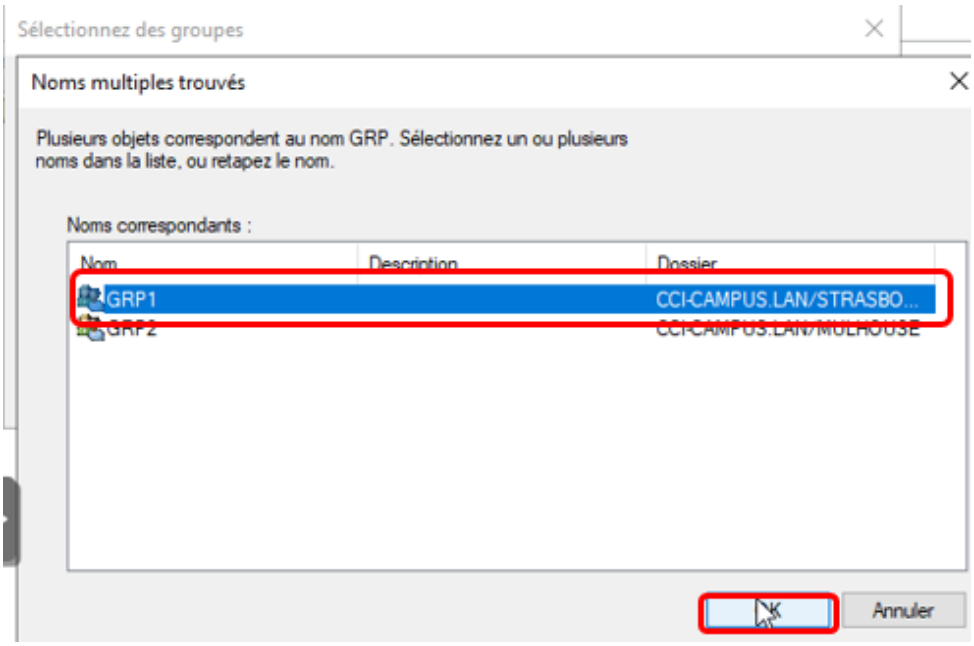
Intégration de l'utilisateur dans un groupe

Sélectionner un utilisateur et :



Choisissez le groupe de sécurité auquel il doit appartenir.





DHCP

Le service DHCP (Dynamic Host Configuration Protocol) permet l'attribution automatique des adresses IP et des configurations réseau aux dispositifs connectés.

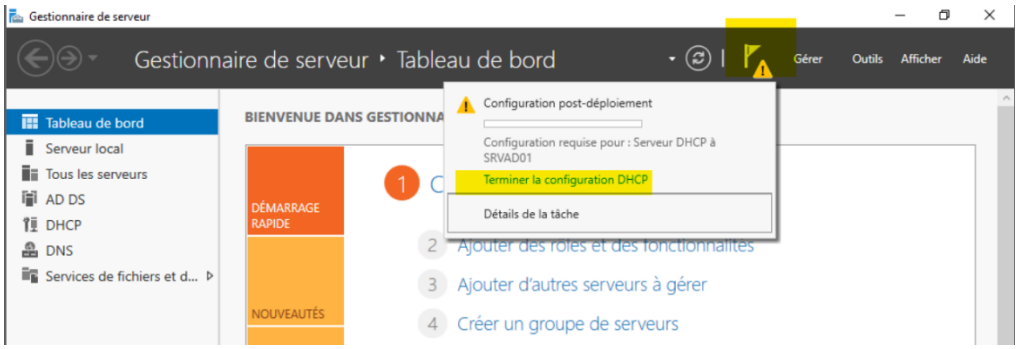
Prérequis

Infrastructure :

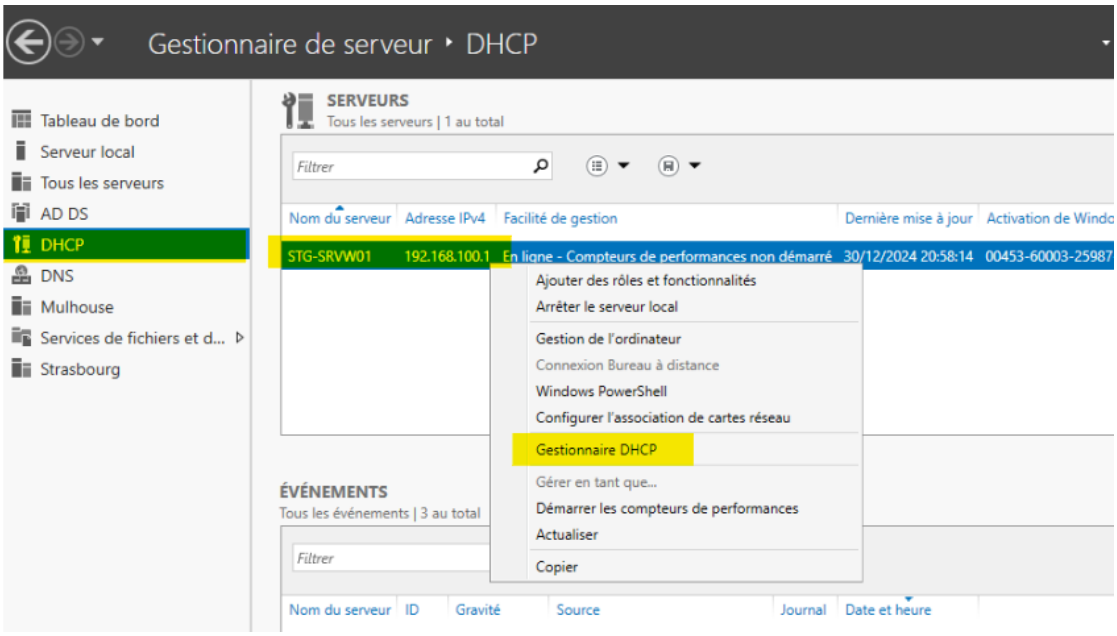
- Deux serveurs ADDS (Active Directory Domain Services) avec le rôle DHCP installé.

Configuration du DHCP

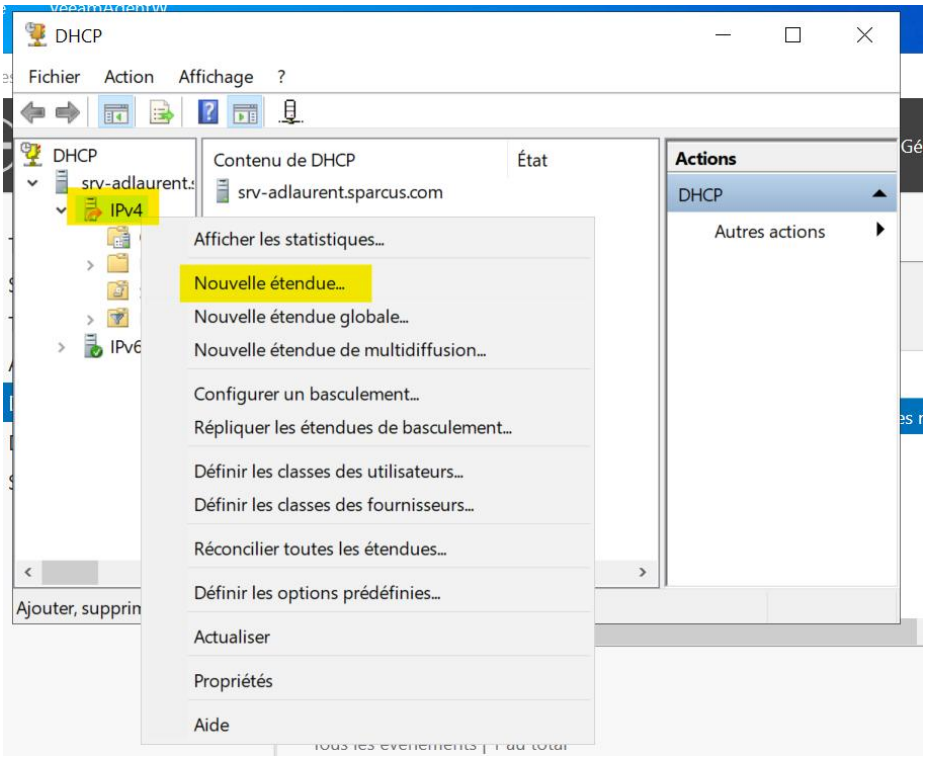
Cliquez sur le drapeau et terminez la configuration DHCP



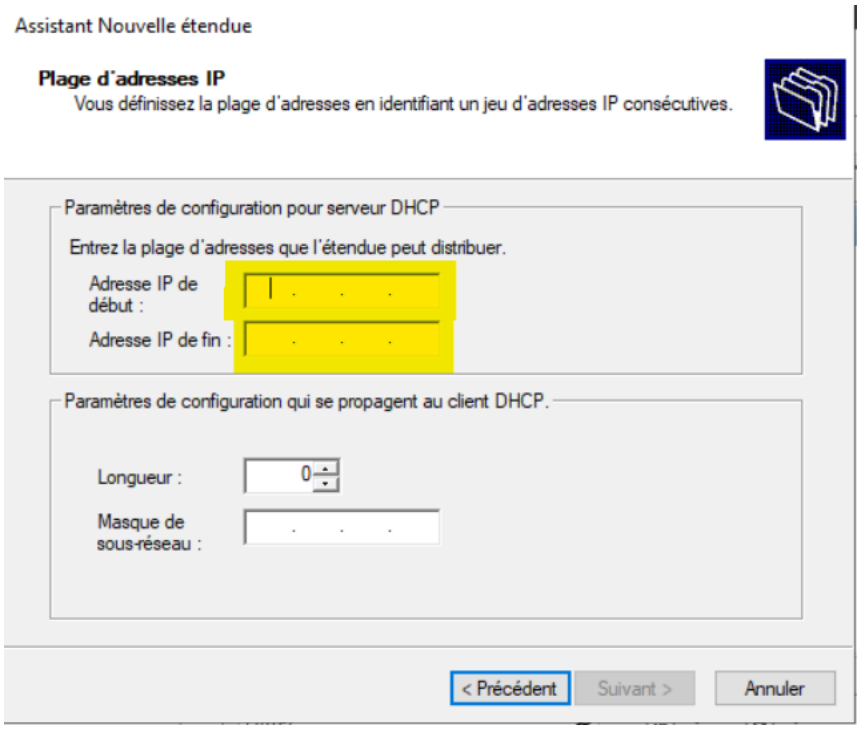
Cliquez sur suivant puis continuez.
Allez ensuite sur DHCP Faites clic droit sur votre serveur puis Gestionnaire DHCP.



Dans votre serveur faites clic droit sur IPv4 puis nouvelle étendue.



Donnez un nom à votre étendu puis suivant.
Ici rentrez l'a première IP puis la dernière.

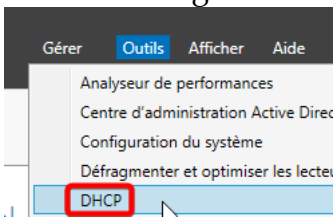


Vous pouvez cliquer sur suivant et terminer.

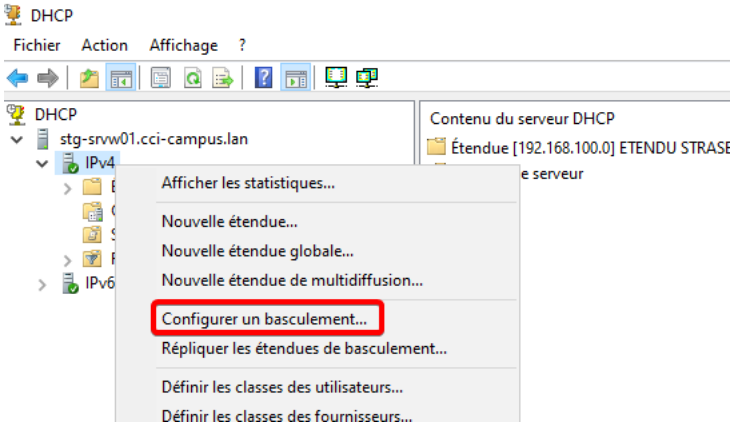
Vous avez maintenant votre DHCP fonctionnel.

Mise en place de la redondance du DHCP

Pour réaliser la redondance du serveur DHCP, il est nécessaire de créer un basculement DHCP entre les serveurs concernés. Pour se faire, aller dans Outils > DHCP sur le gestionnaire de serveur :

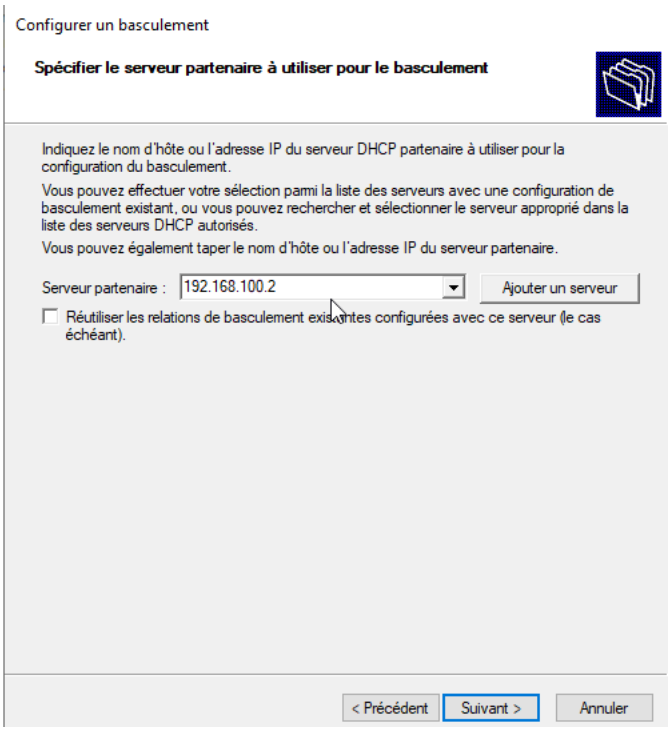


Puis développer le nœud qui correspond à votre serveur, et faite clic droit sur IPv4, puis "Configurer un basculement..." :



On sélectionne nos étendues :

Puis on choisit le serveur partenaire :



Enfin, on choisit le mode "Serveur de secours" pour de la redondance efficace, on attribue 10% d'adresses de secours et on rentre un secret partagé :

Pour finir, on peut cliquer sur Terminer
Le basculement est maintenant opérationnel.

Firewall

Un pare-feu est un élément clé de la sécurité réseau, chargé de filtrer et de contrôler les flux entrants et sortants il protège les systèmes des menaces extérieures. Quand au VPN il permet de créer un tunnel sécurisé entre les deux sites distants, garantissant la sécurité des données.

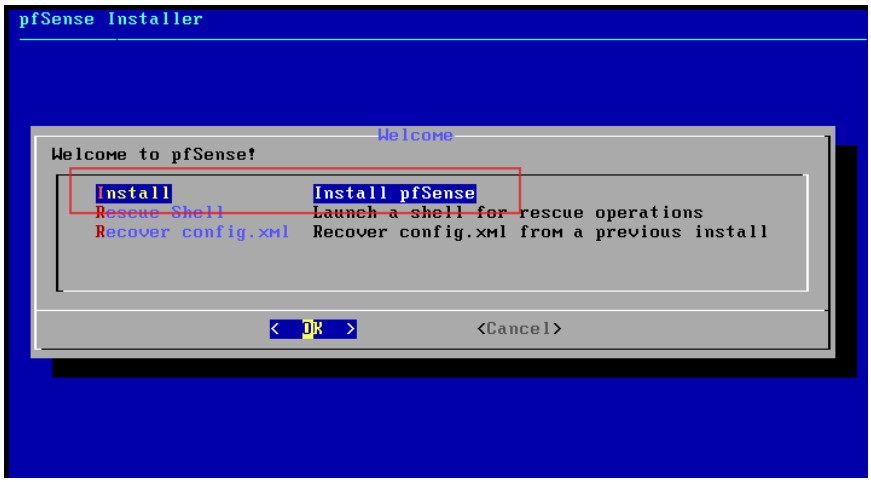
Prérequis

Ressources matériels minimum :

- Processeur : Minimum 1 GHz
- RAM : 512 Mo
- Stockage : 1 disque de 8 Go
- Interface réseau. : 2 interfaces Ethernet (WAN/LAN)

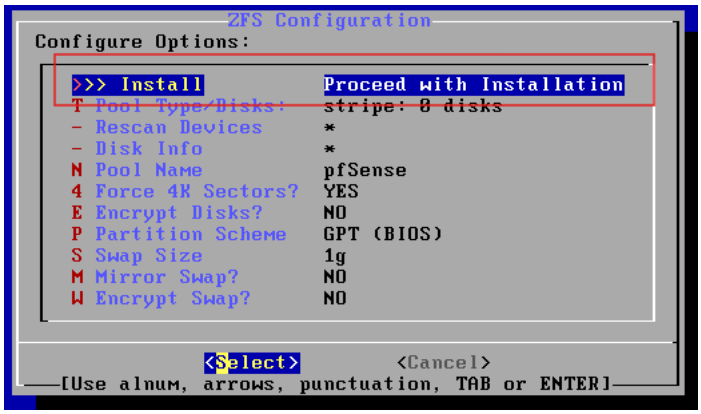
Installation Pfsense

Lancez l'installation de Pfsense.



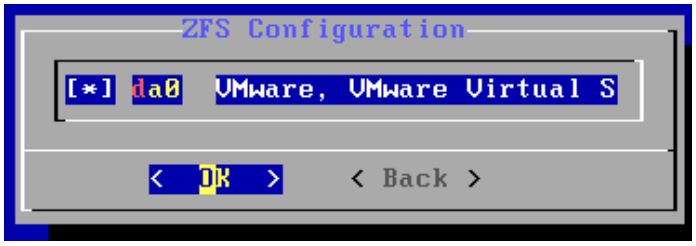
Ici sélectionnez la première option.

Lancez l'installation

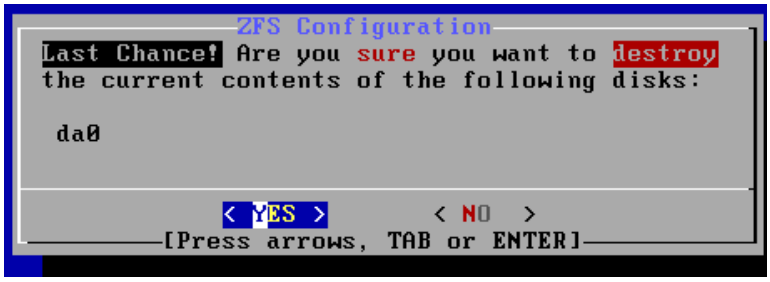


Ici nous ne voulons pas faire de redondance donc nous allons sélectionner la première option.

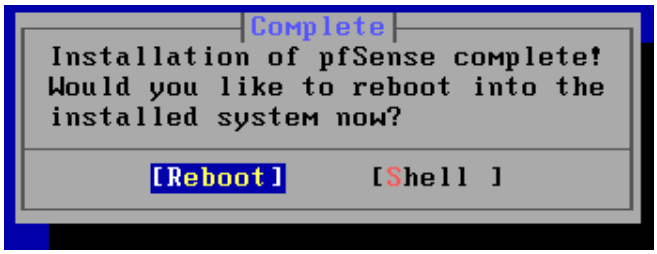
On choisit le disque sur le quelle on va installer le système.



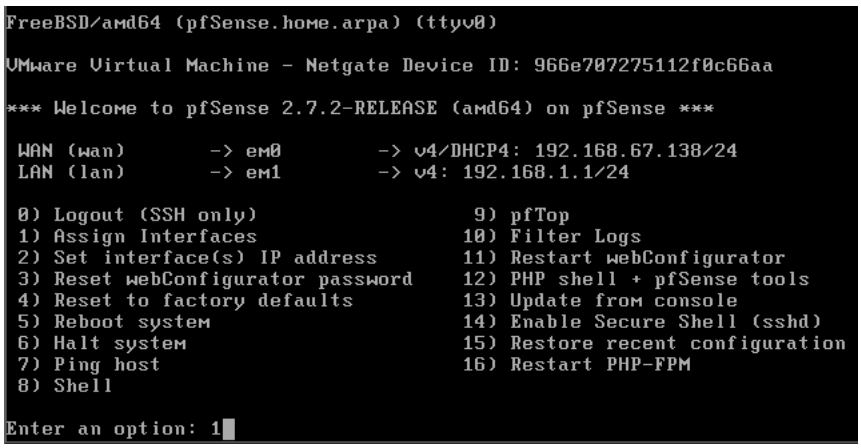
On nous dit que le disque va être effacer et on accepte.



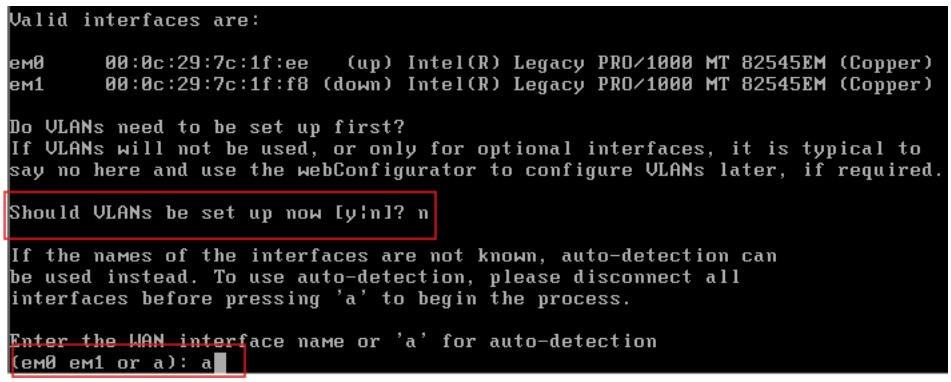
L'installation à réussit on redémarre la machine.



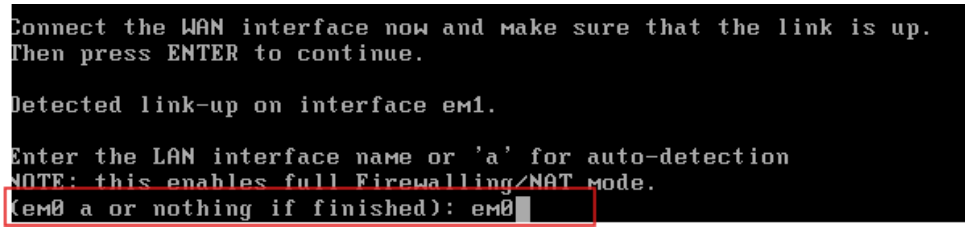
Au redémarrage nous allons configurer nos carte réseaux et pour cela nous allons rentrer dans l'option 1.



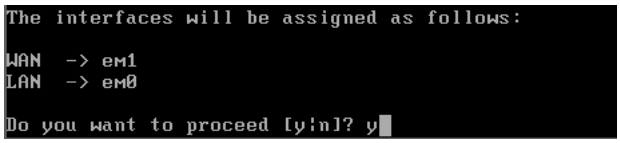
Nous n'allons pas configurer de VLANs donc on commence par rentrer « N ». Ensuite nous devons déterminer quelle interface sera le WAN. PFSENSE le fait automatiquement si on rentre « A ».



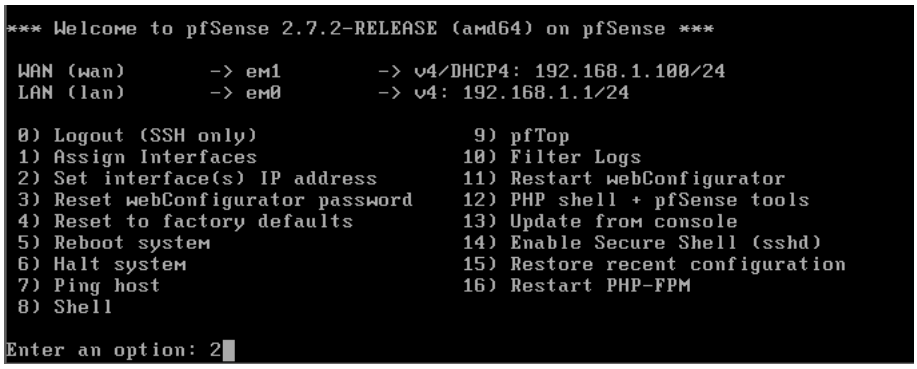
Notre interface vers le WAN à bien été détecté on peut maintenant sélectionner l'autre interface pour notre LAN.



On répond « Y » à la vérification

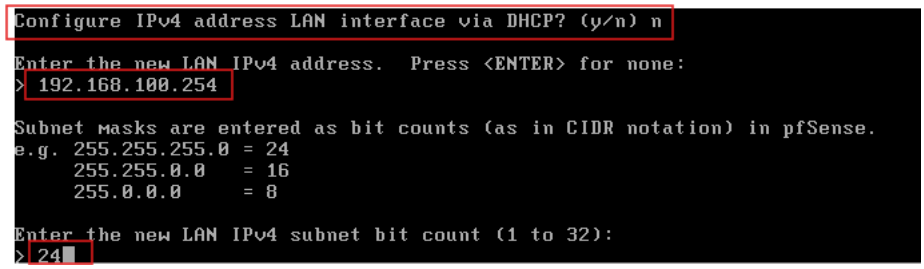


Notre interface WAN prend son IP par DHCP il nous faut donc configurer l'IP de notre interface LAN. Pour ceci on entre l'option 2

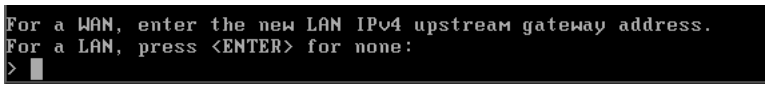


On choisit notre interface LAN

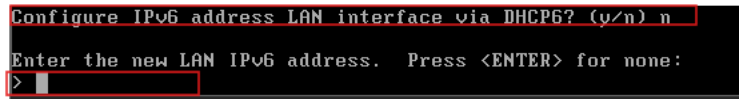
On dit non au DHCP puis on rentre notre IP et notre masque.



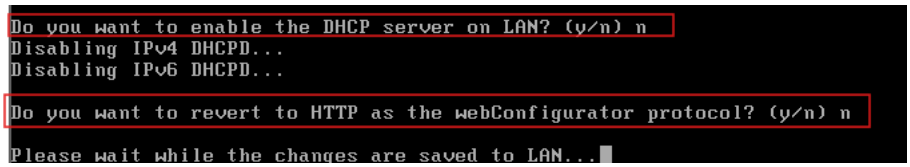
On nous demande une gateway. Comme nous somme sur une interface LAN on ne rentre rien.



On ne configure pas notre IPV6 donc on dit non au DHCP et on ne rentre pas d'adresse.

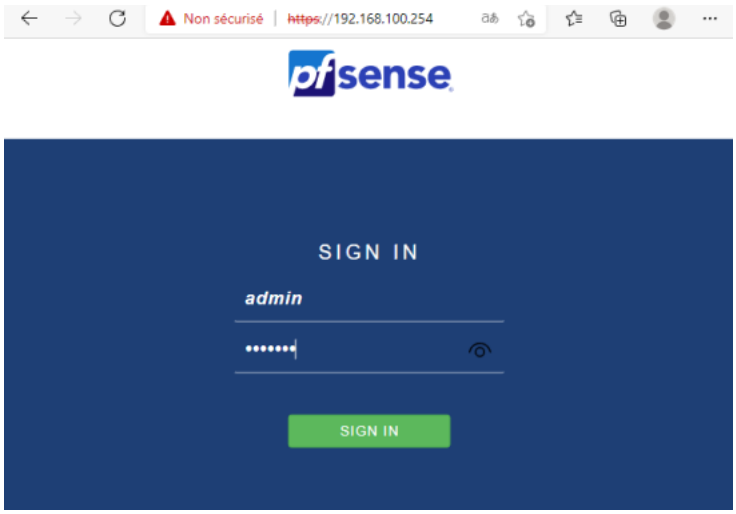


On répond « n » à toutes les prochaines questions et notre interface et maintenant prête.

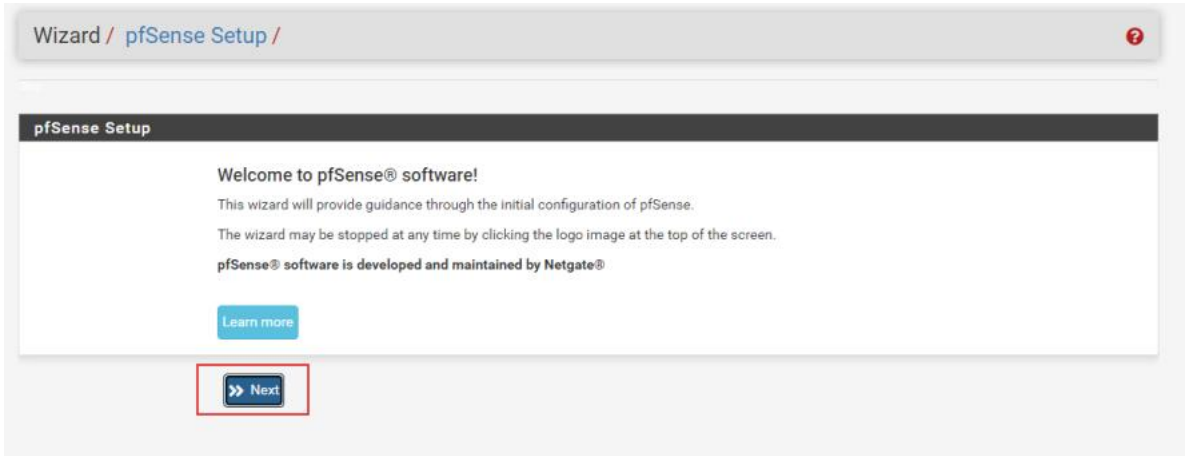


On refait la même chose pour la DMZ

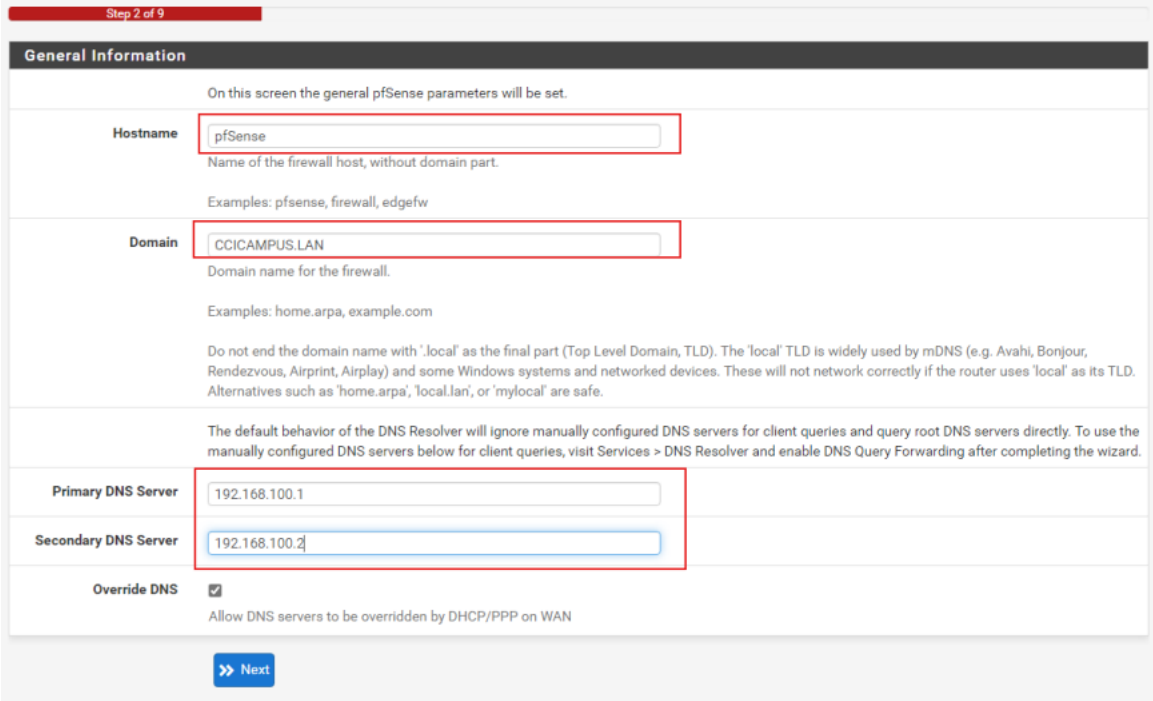
On peut maintenant se connecter à l'UI via une machine client sur le LAN pour ceci rentrez l'adresse IP de votre PFSENSE dans un navigateur. On arrive sur une page de connexion. Les identifiants par défaut son admin pour le nom d'utilisateur et Pfsense pour le mot de passe.



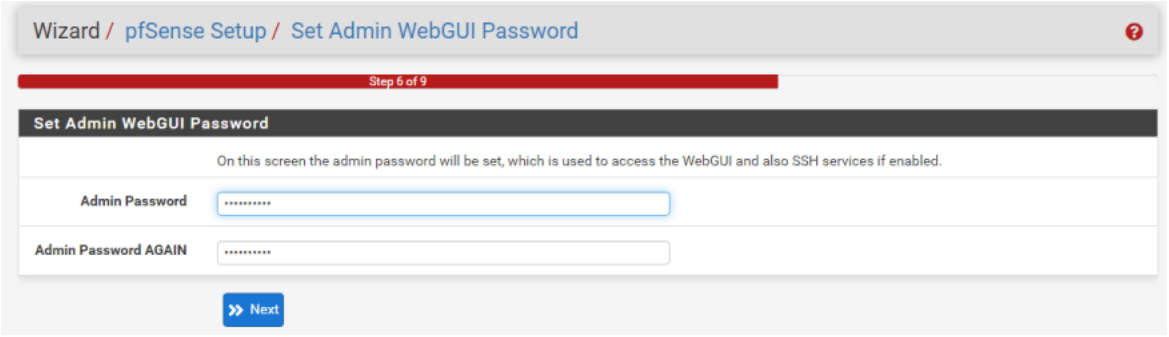
On rentre dans la configuration de PFSENSE on clique sur next



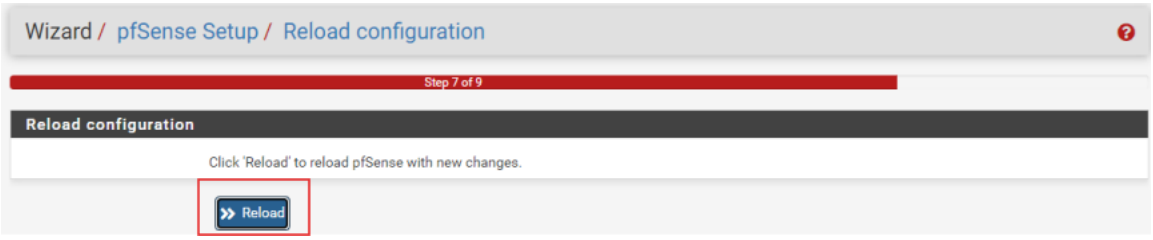
On reclique sur next et on rentre le nom que l'on veut donner à notre DNS son domaine et ces DNS



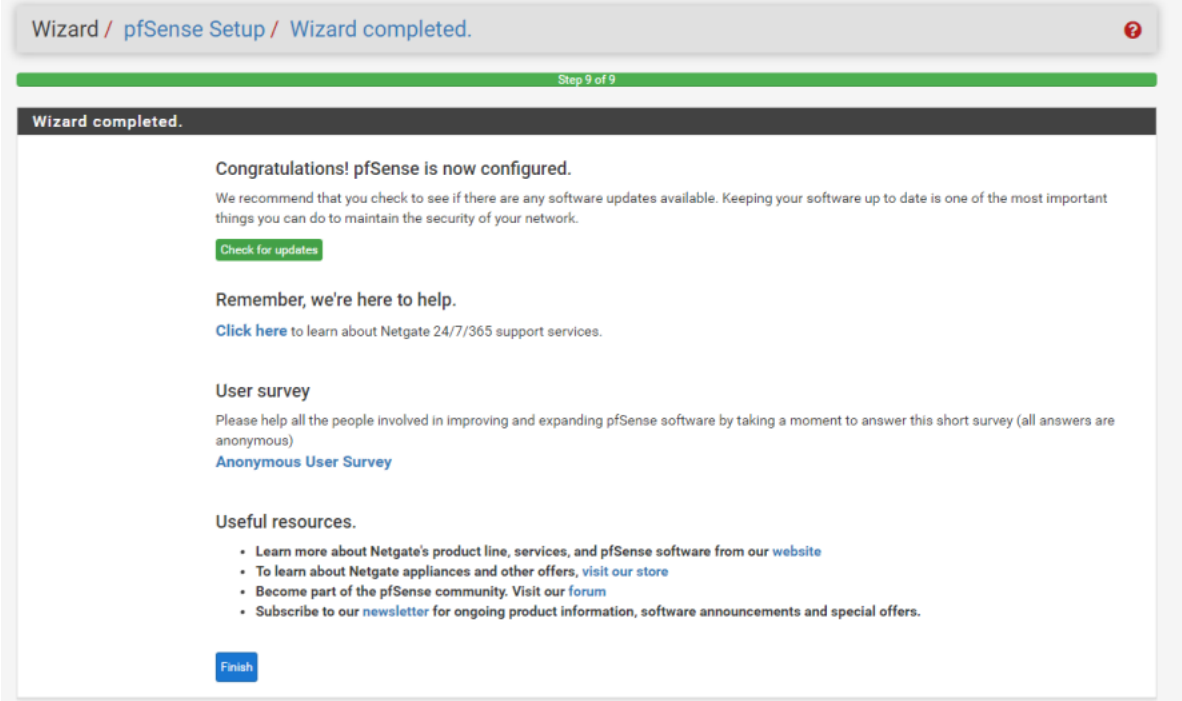
On clique sur next jusqu'à ce que l'on rentre le mot de passe Admin



On clique sur reload

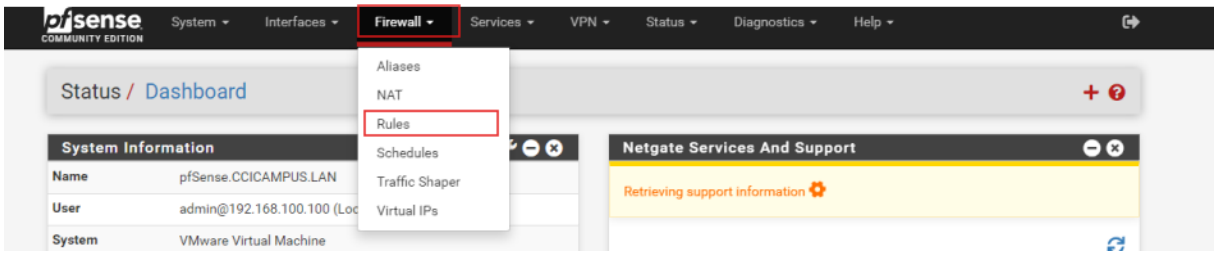


Après le chargement notre PFSENSE est configurer et prêt à être utilisé.

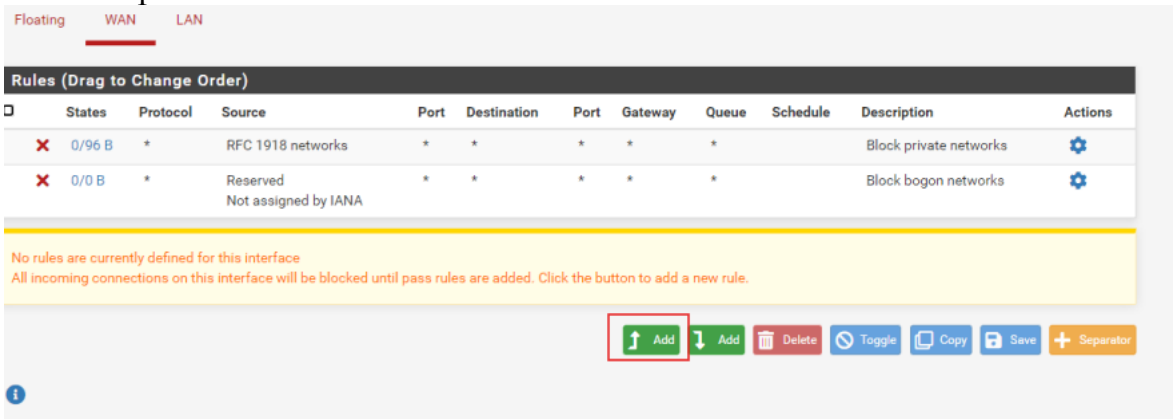


Création des règles du Pare-Feu

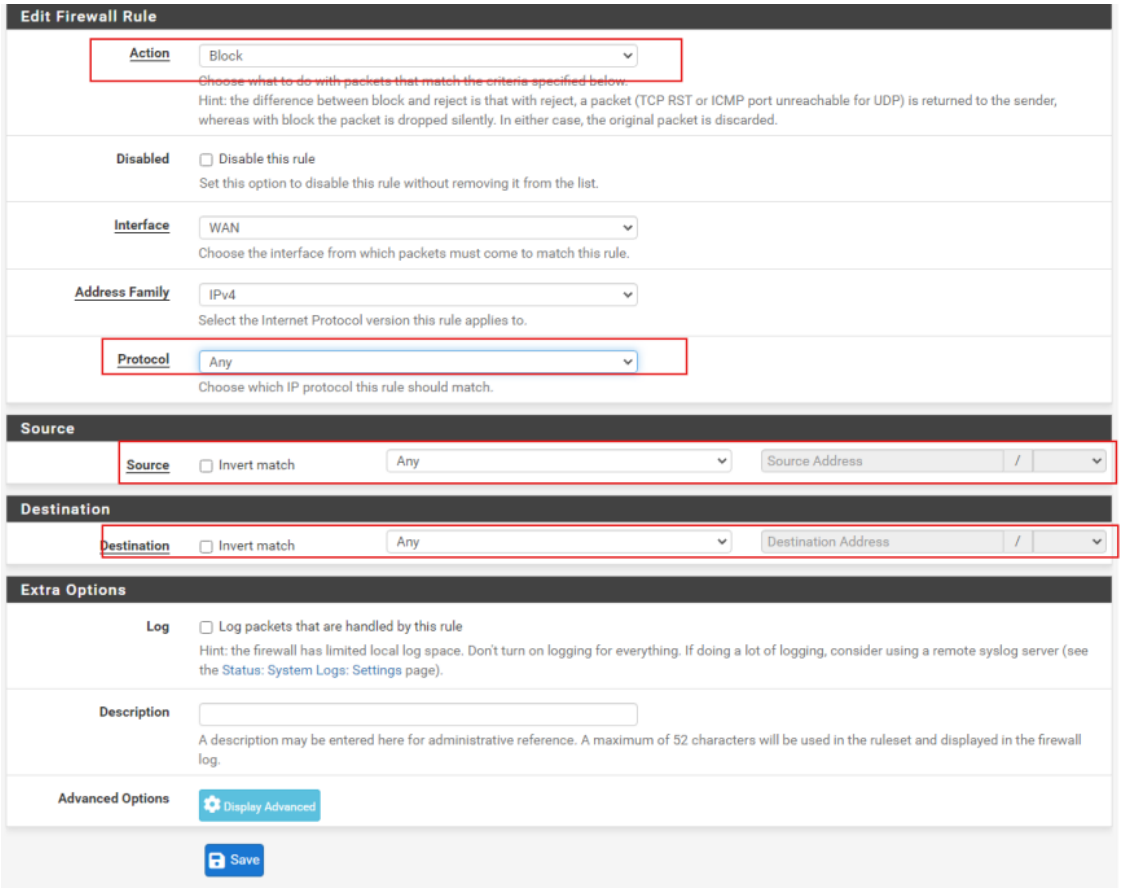
Nous allons créer des règles de Pare-Feu. Pour ceci nous allons allez dans Firewall puis Rules



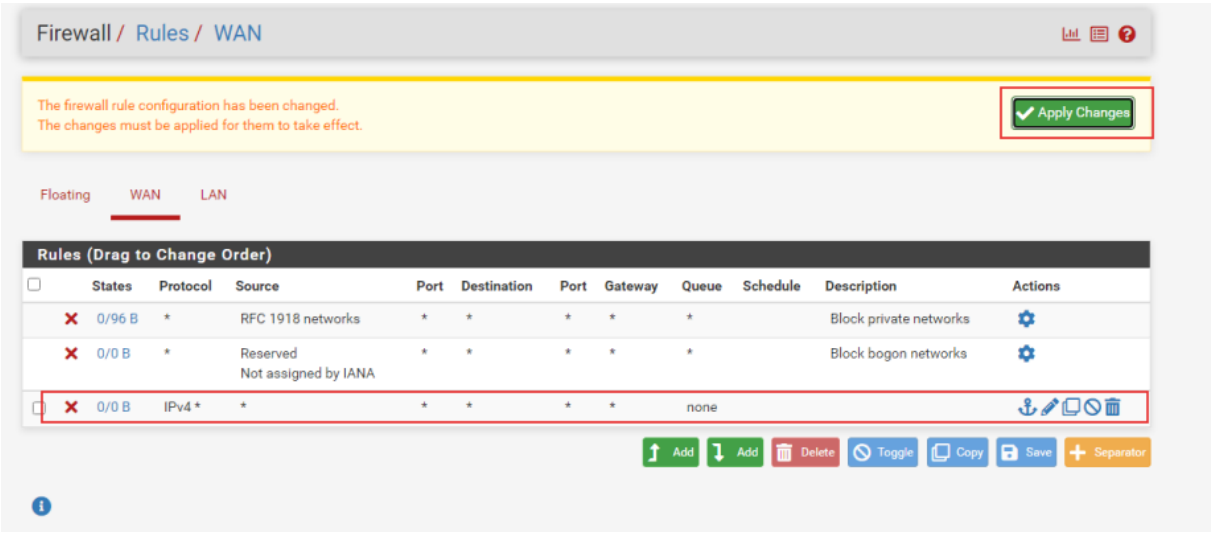
La première chose à faire est de bloquer toutes les communications pour cela nous allons cliquez sur ADD



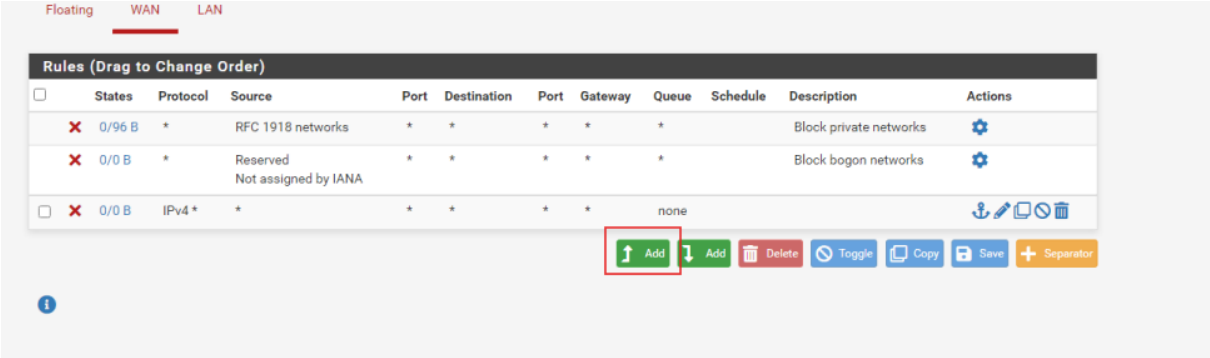
En action nous allons mettre block en protocole any. Également any en source et en destination.



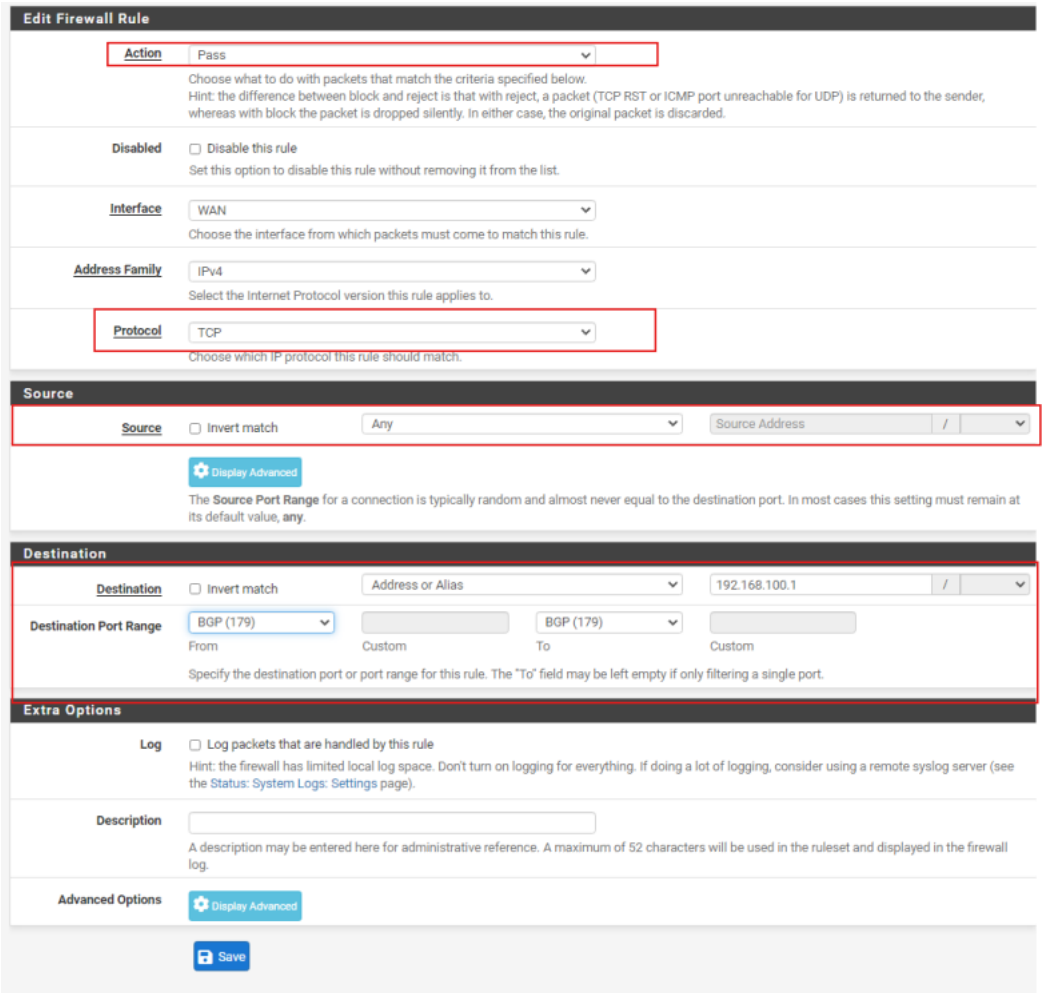
Notre règle est bien apparue on clique sur apply changes



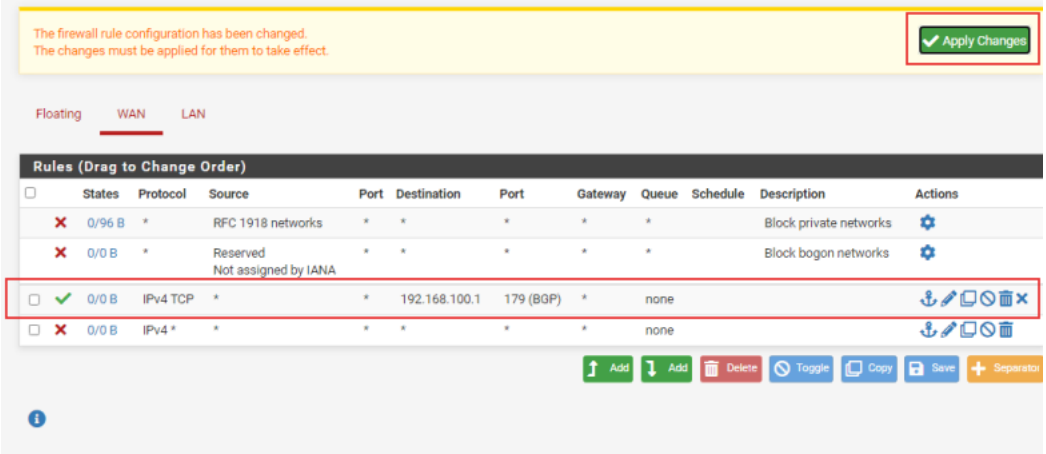
Maintenant nous pouvons n'importe quelle règle pour gérer les autorisations. Pour cela on va cliquez sur ADD



On commence par indiquer Pass dans action, on peut ensuite choisir le protocole puis la source, la destination ainsi que son port.



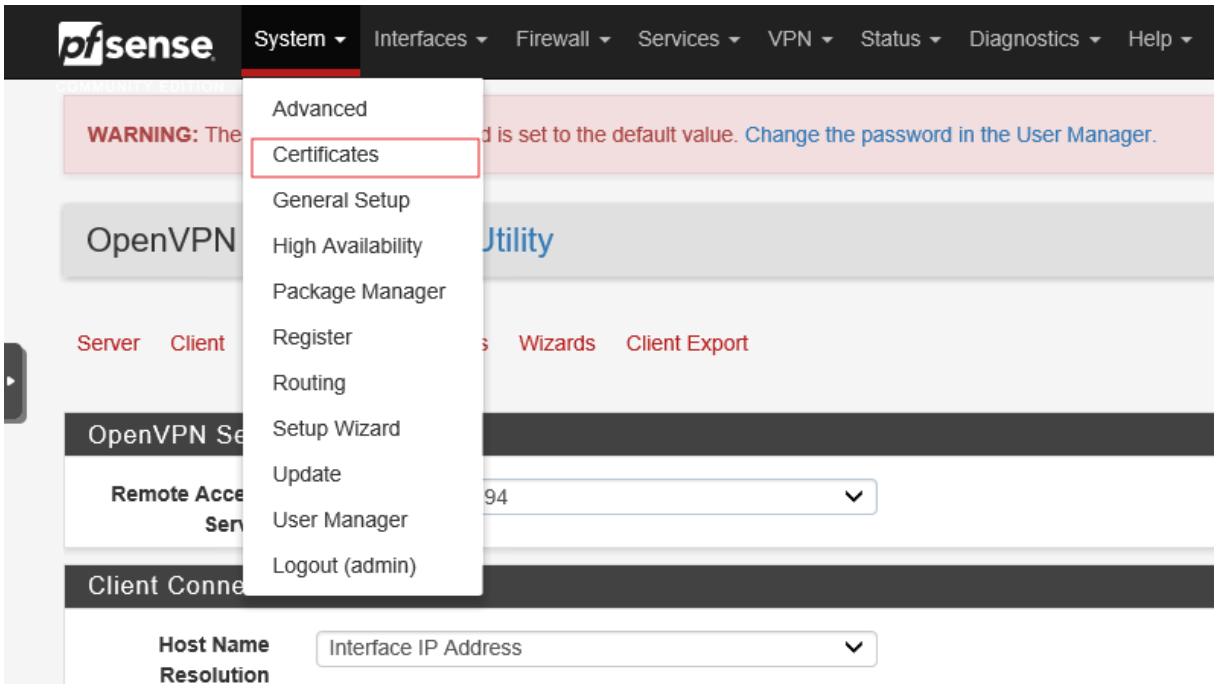
On clique sur Save on vérifie que notre règle est bien apparue et on clique sur Apply Changes.



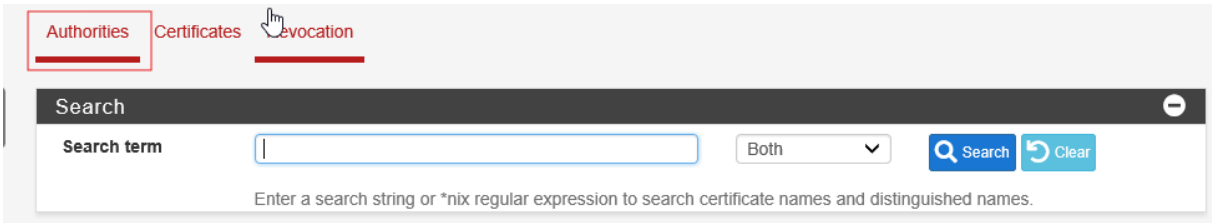
Création VPN Road Warior

Créer les certificats

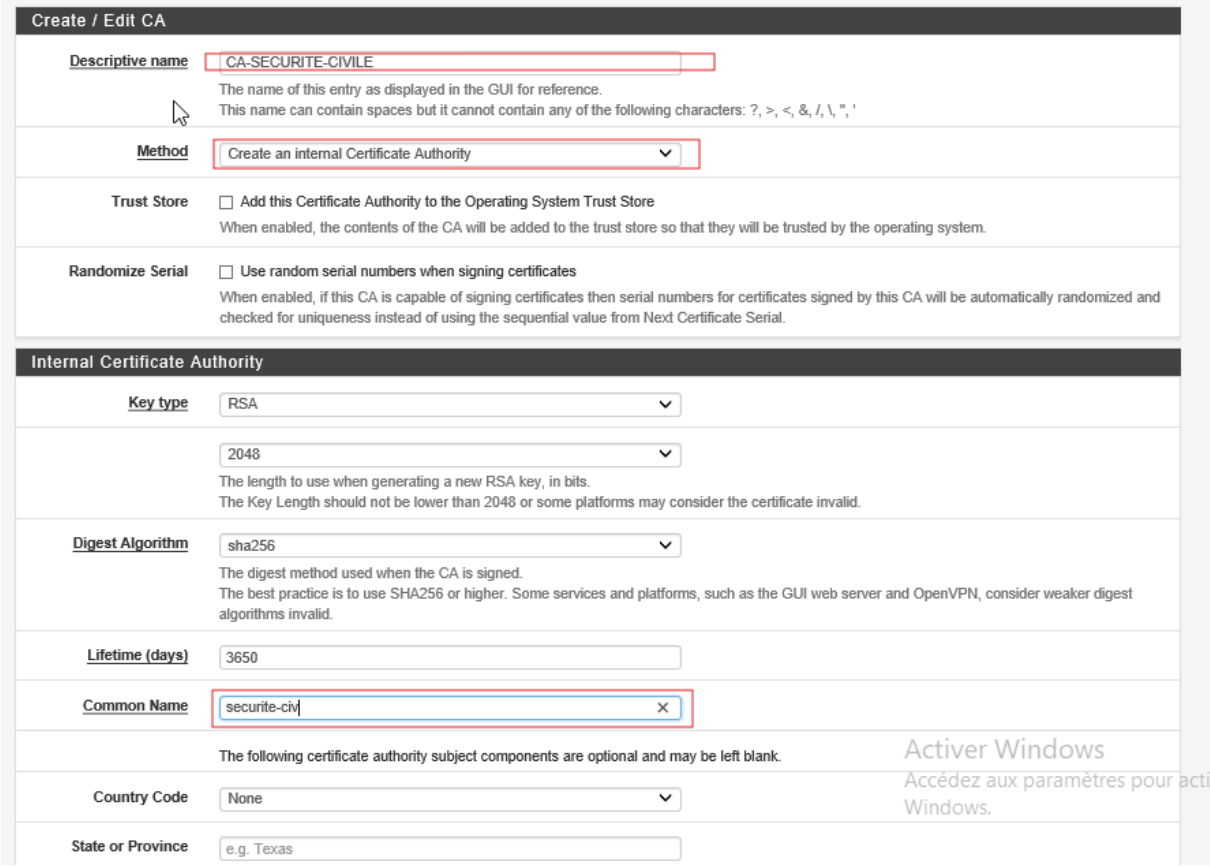
Allez dans **System > Cert. Manager**



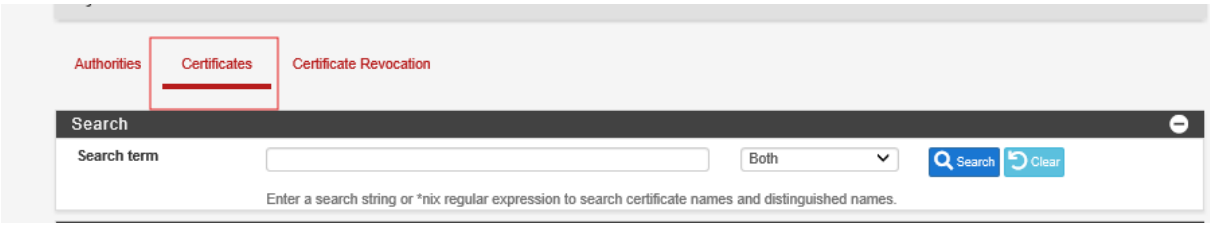
Dans Authorities cliquez sur **ADD**



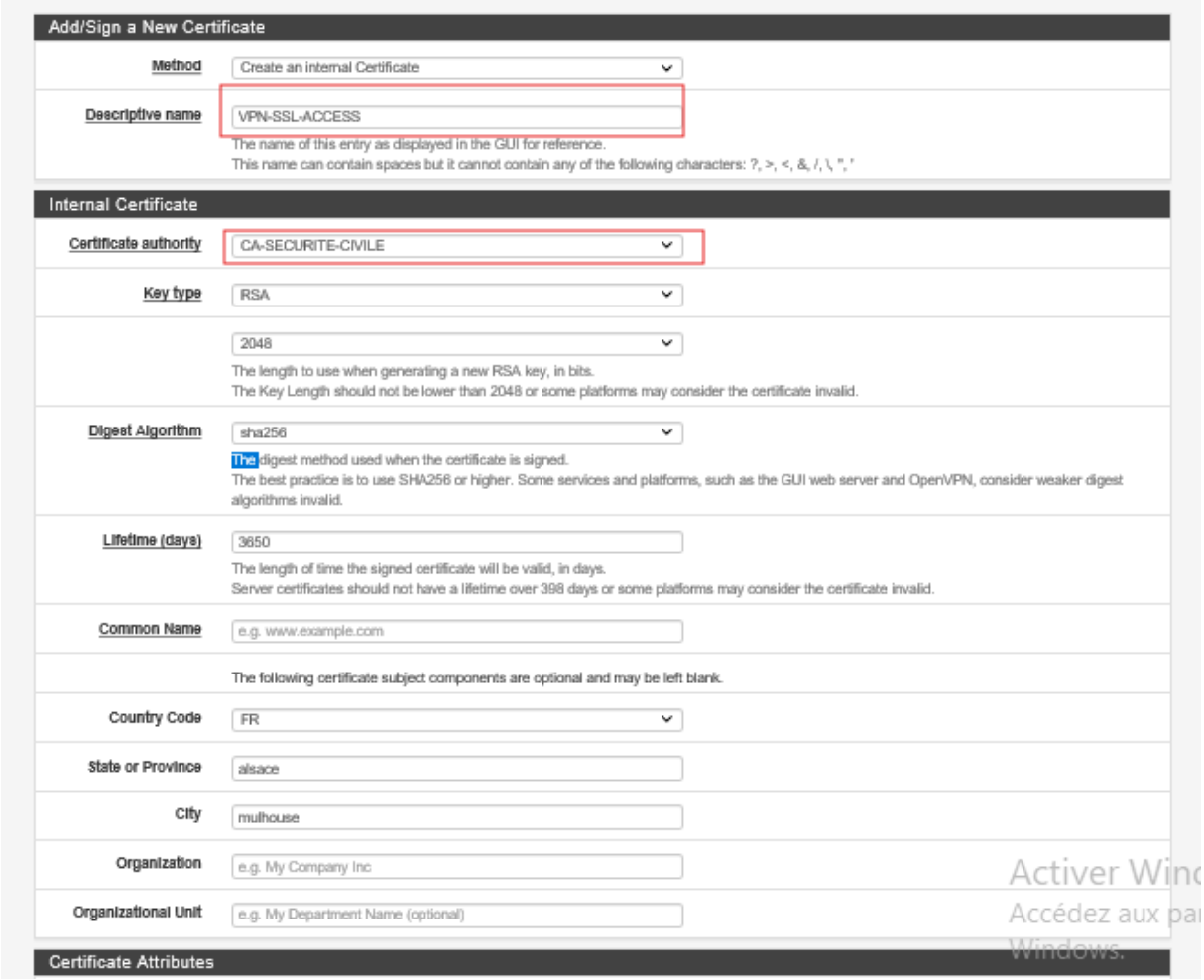
Nommer votre règle et choisissez **Create an internal Certificate Authority** mettez un nom et sauvegardez



Allez dans **Certificates** et faites **ADD**

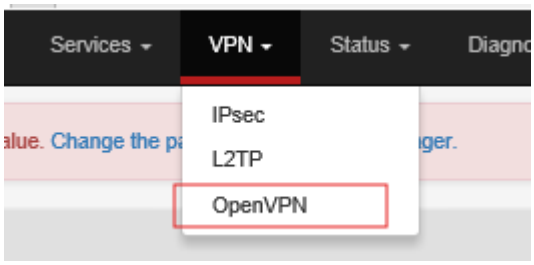


Nommer le certificat et choisissez l'autorité

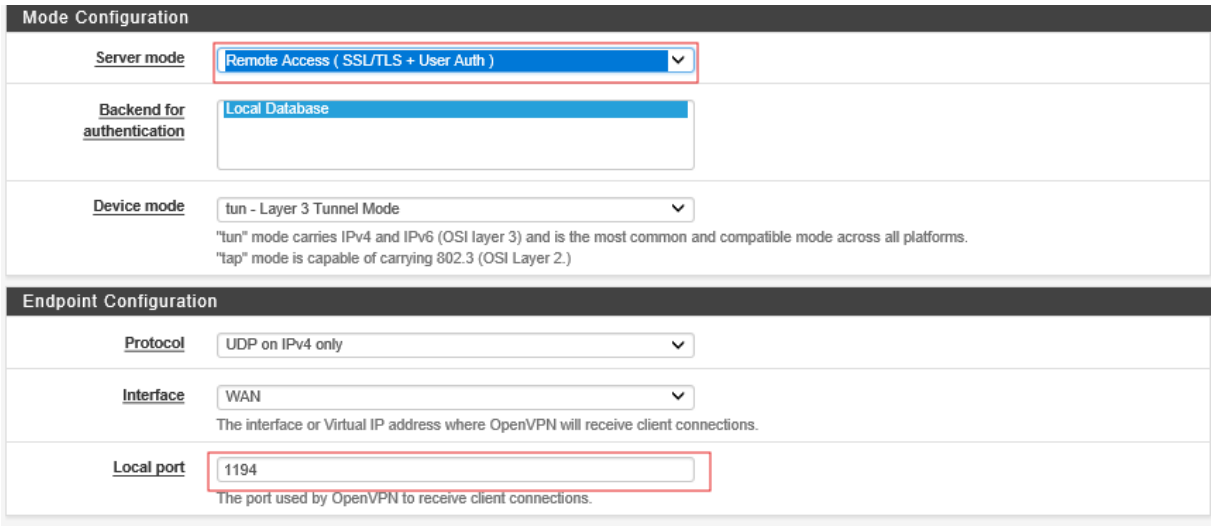


Configuration OpenVPN

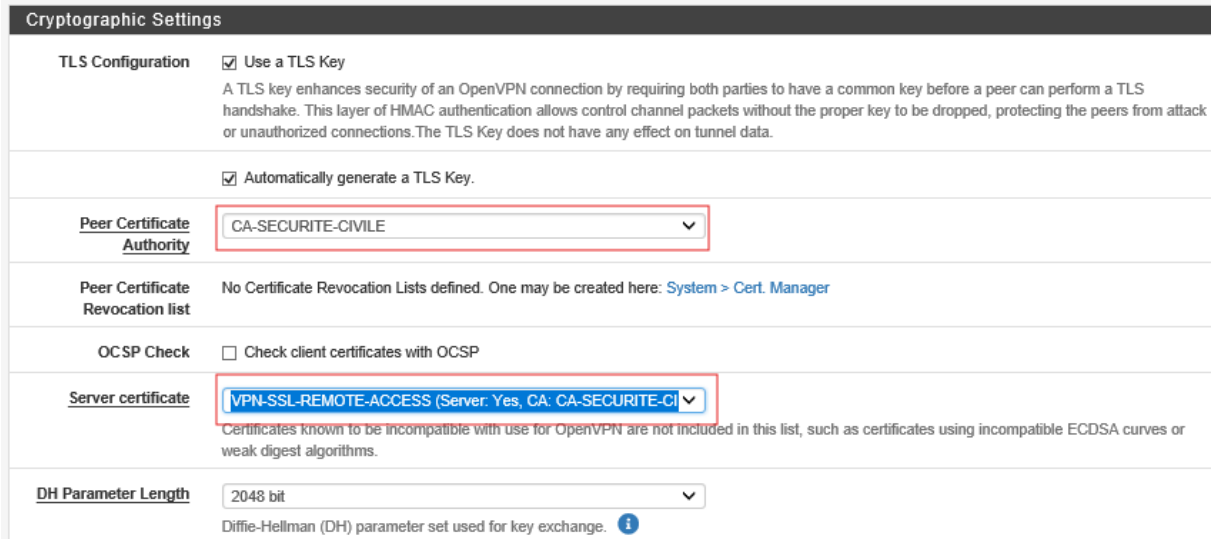
Cliquez sur le menu "**VPN**" puis "**OpenVPN**"



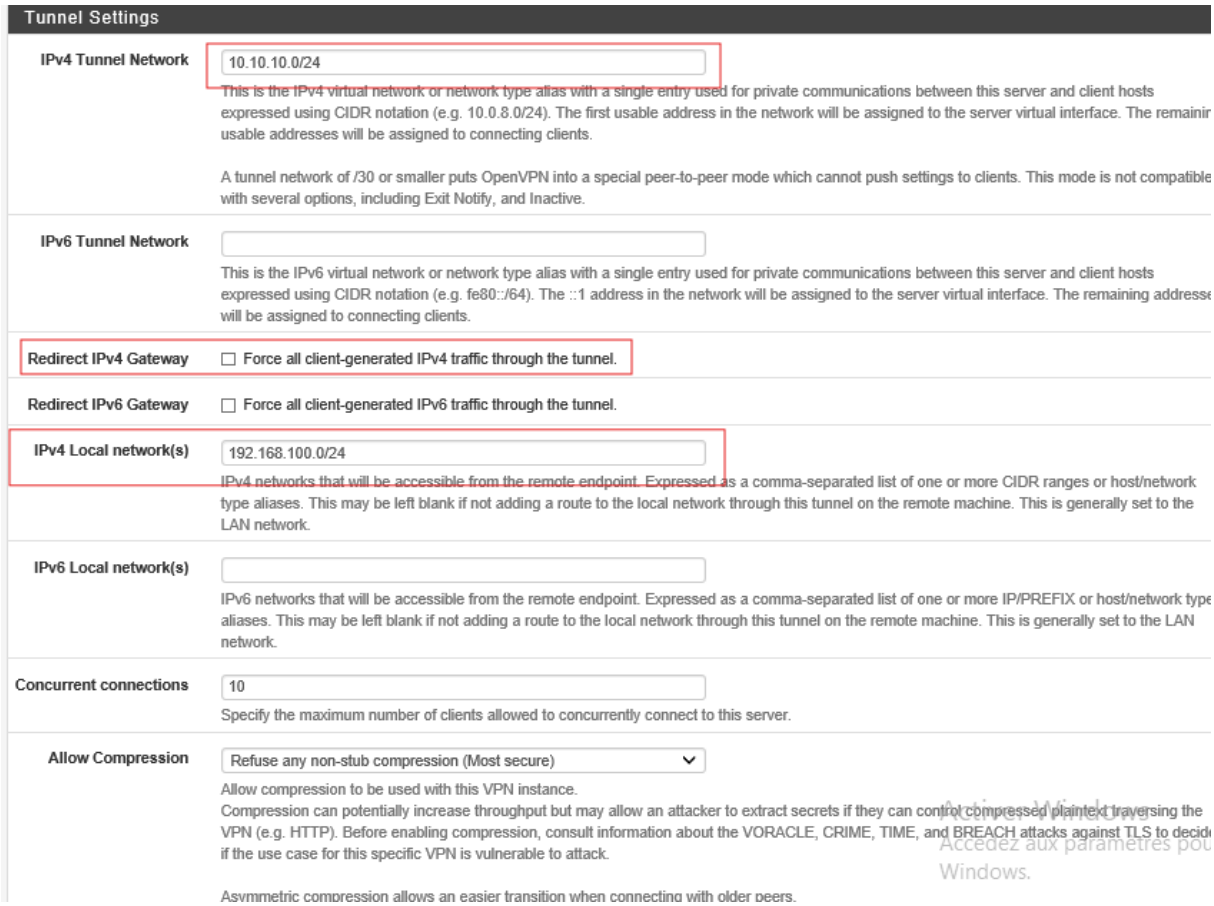
Dans serveur cliquez sur **add**
Choisissez le serveur mode ainsi que le port que vous souhaiter



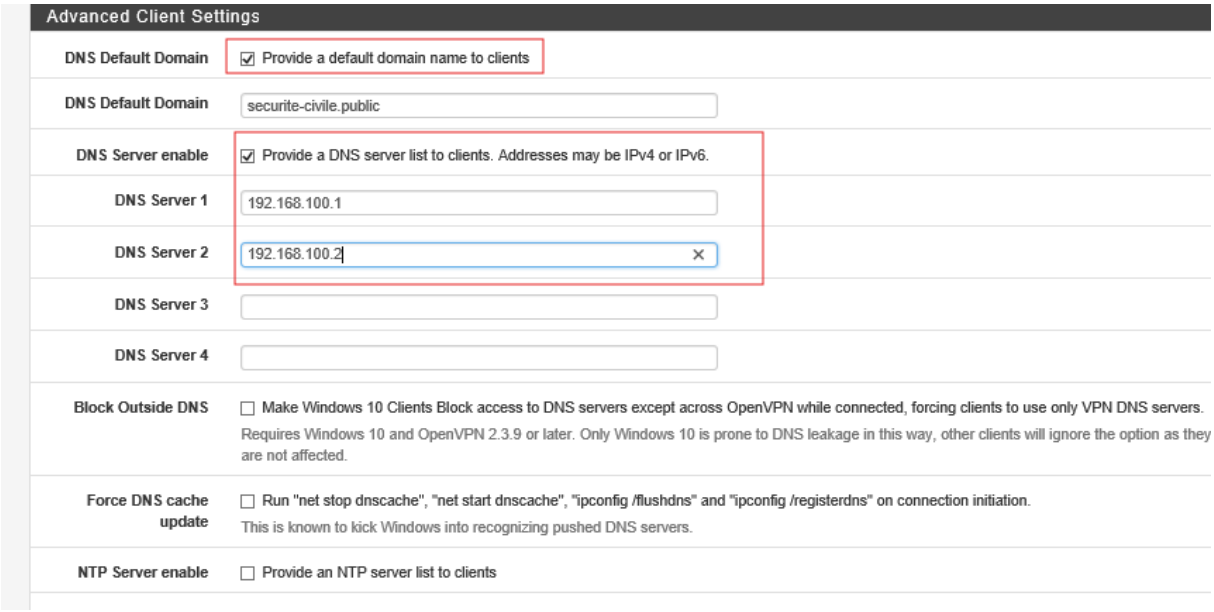
Choisissez vos certificats



Vous pouvez maintenant rentrer les paramètres de votre tunnel
IPv4 Tunnel Network : réseau attribué aux clients VPN, utilisé comme IP locale à la connexion.
Redirect IPv4 Gateway : active le full tunnel (tout le trafic passe par le VPN) ; sinon, split-tunnel.
IPv4 Local Network : réseaux LAN accessibles via le VPN (ex. : 192.168.1.0/24), séparés par des virgules si plusieurs.

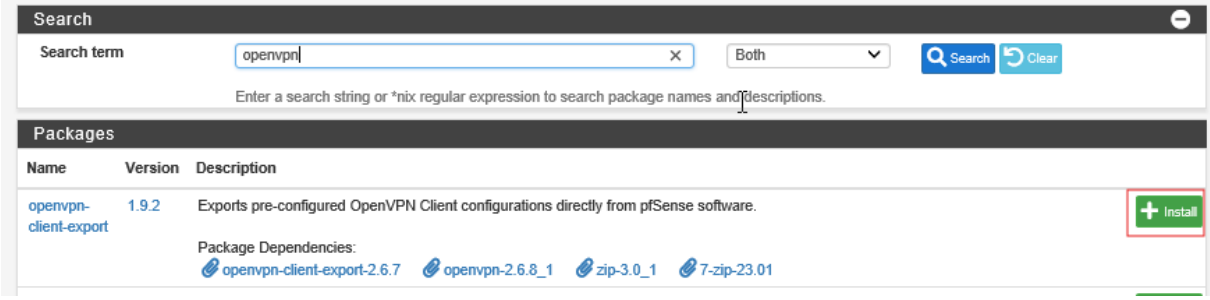


Rentrez l'informations de votre DNS



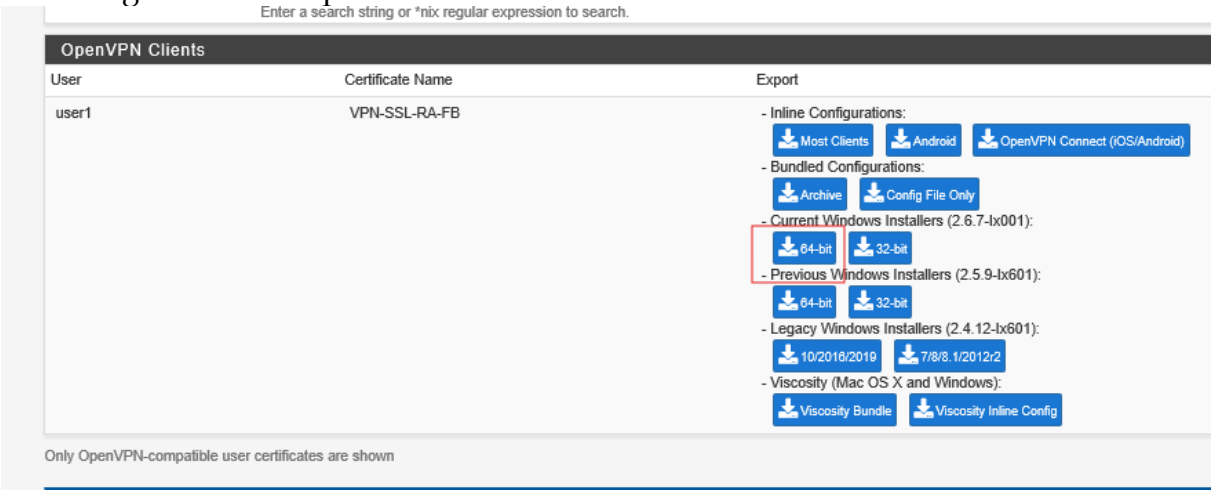
Exporter la configuration OpenVPN

Dans **System > Package Manager > Available Packages**. Installer le package **openvpn-client-exporter**



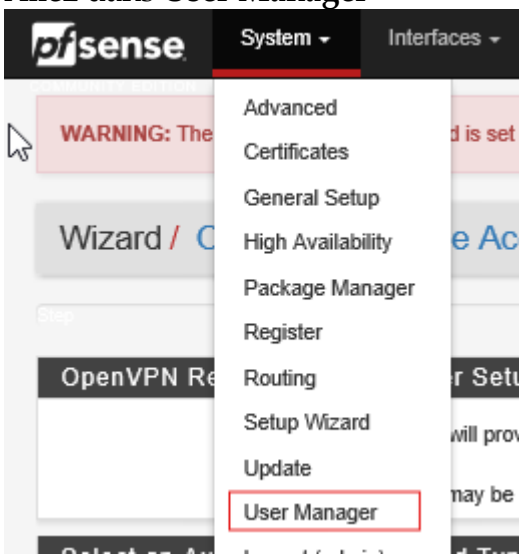
Lorsque c'est fait, retournez dans le menu "**OpenVPN**" puis dans l'onglet "**Client Export**".

Télécharger la version pour votre machine

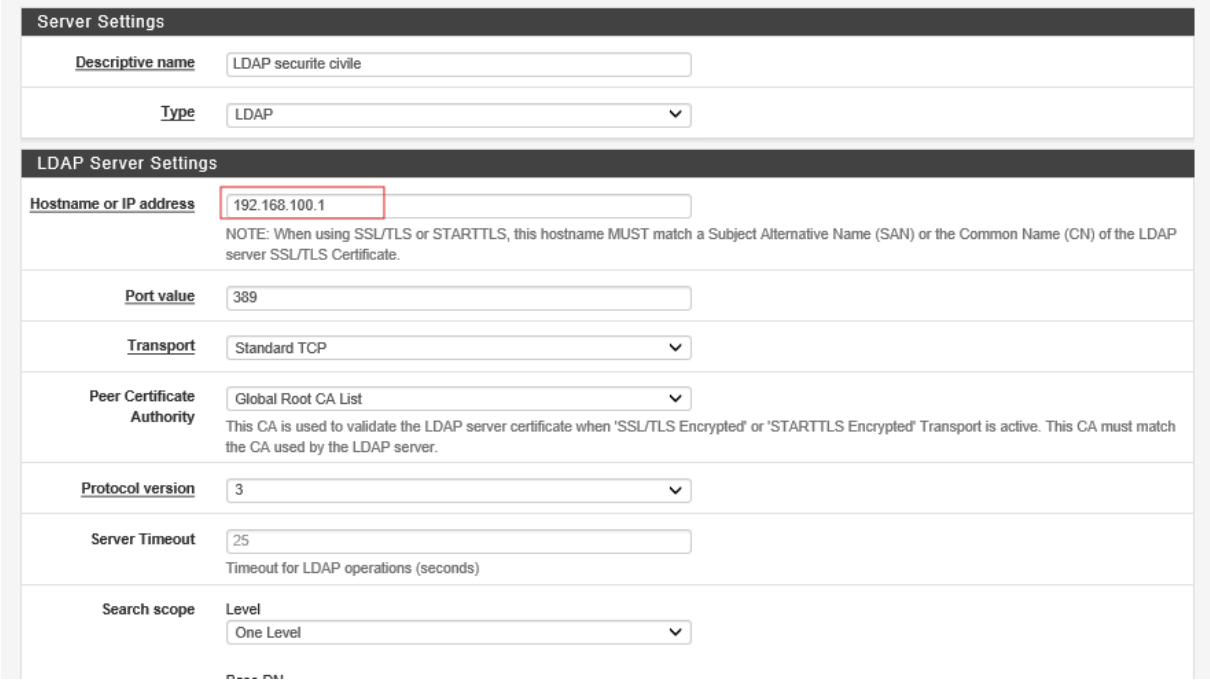


Lier LDAP à OpenVPN

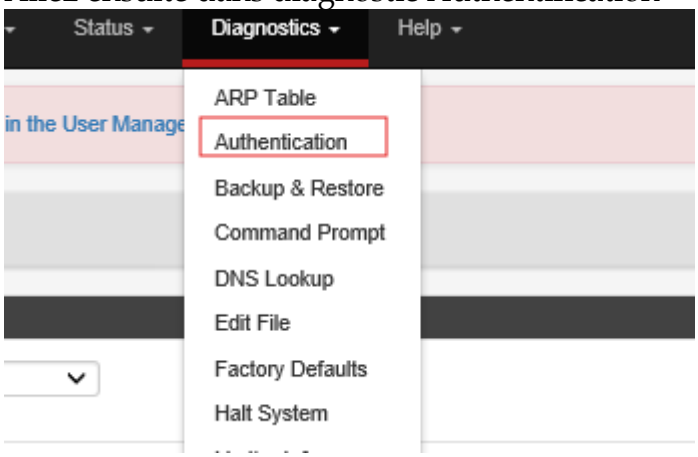
Allez dans **User Manager**



Cliquez ensuite sur "*Authentication Servers*".
Ajouter une nouvelle base.
Nommez le Serveur et mettez l'IP de votre LDAP



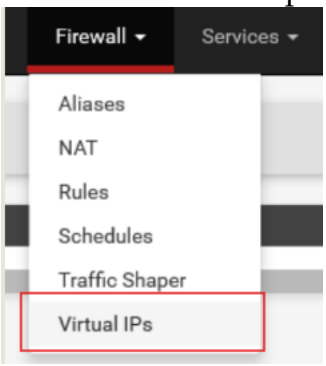
Allez ensuite dans diagnostic Authentification



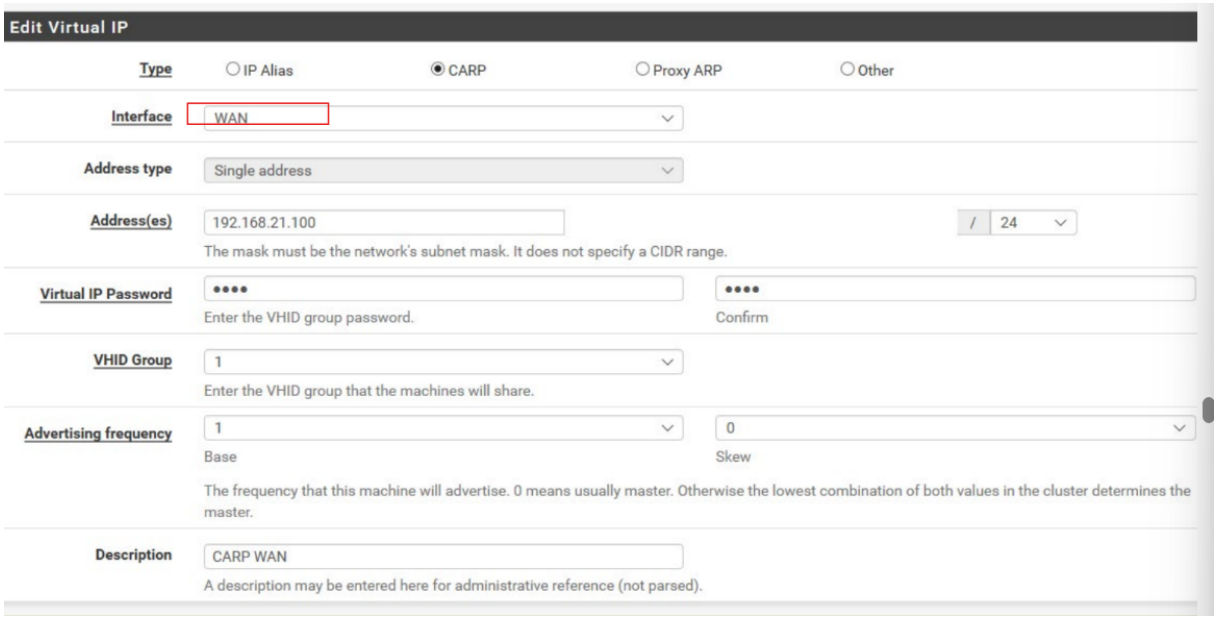
Configurer Redondance

Configurer CARP

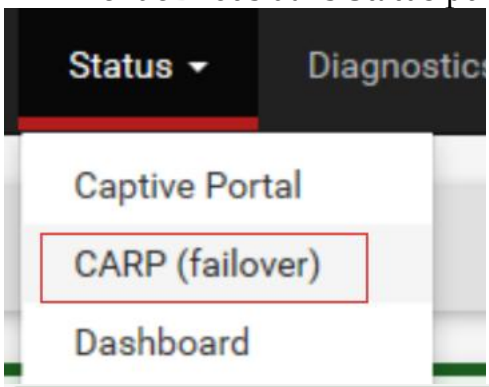
Aller dans **Firewall** puis **Virtual Ips**

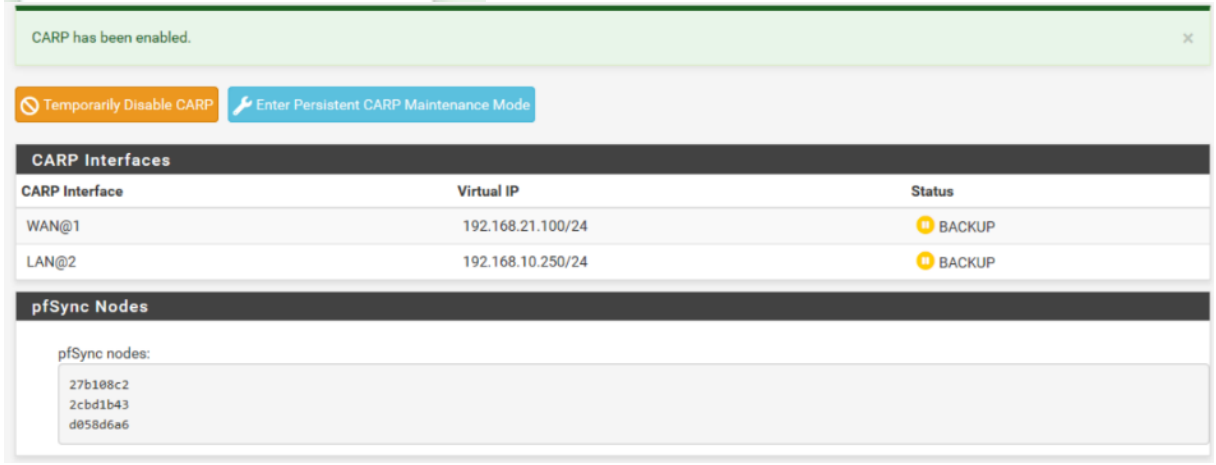


Sélectionner Carp et l'interface que vous souhaitez.



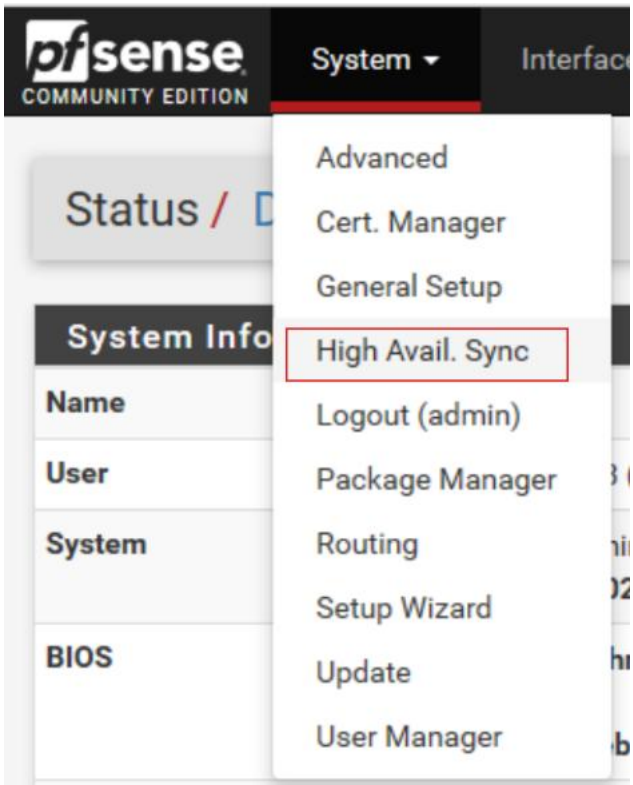
Répéter sur toute les interfaces et sur le second serveur
Enfin rendez vous dans **Status** puis dans **CARP(failover)**



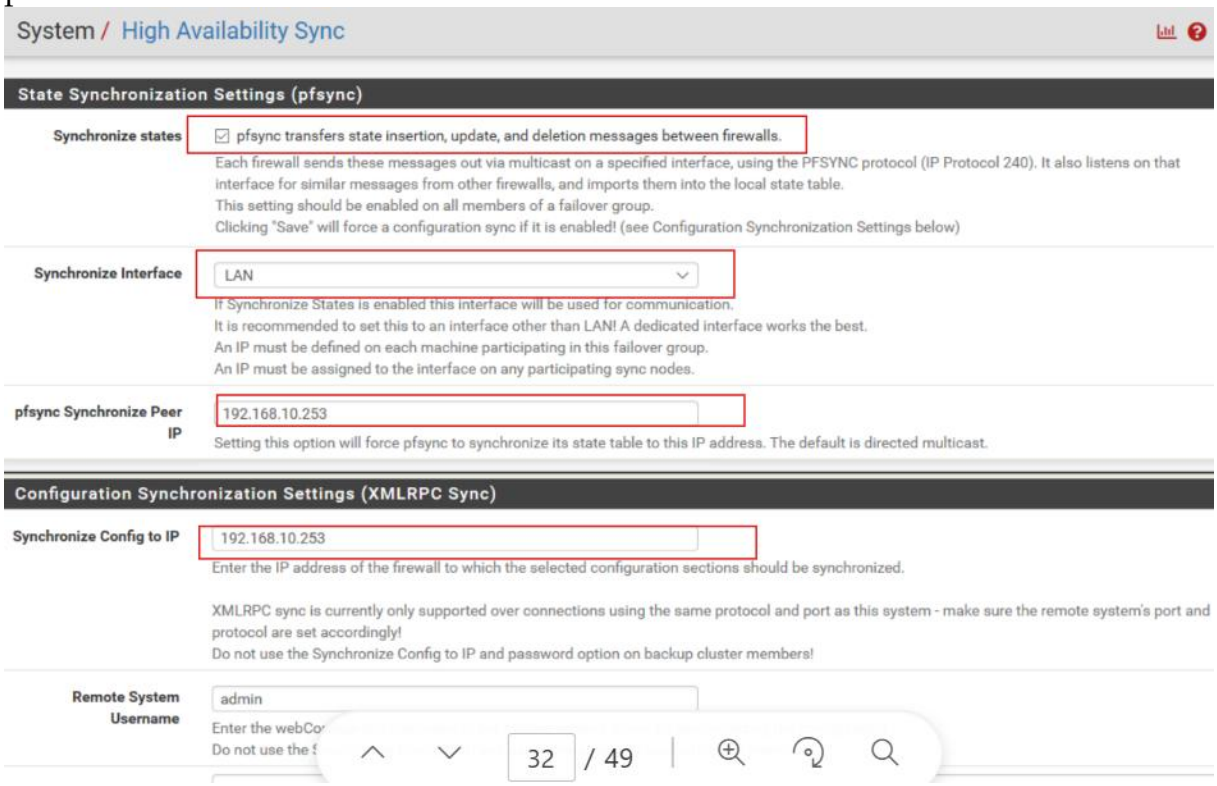


Mise en place de la Haute disponibilité

Sur le serveur maitre aller dans



Cochez la case de la synchronisation, sélectionner l'interface ou va se faire le réplicat puis mettez l'adresse du serveur slave



Vous n'avez plus qu'a mettre les informations de connexion du serveur esclave.

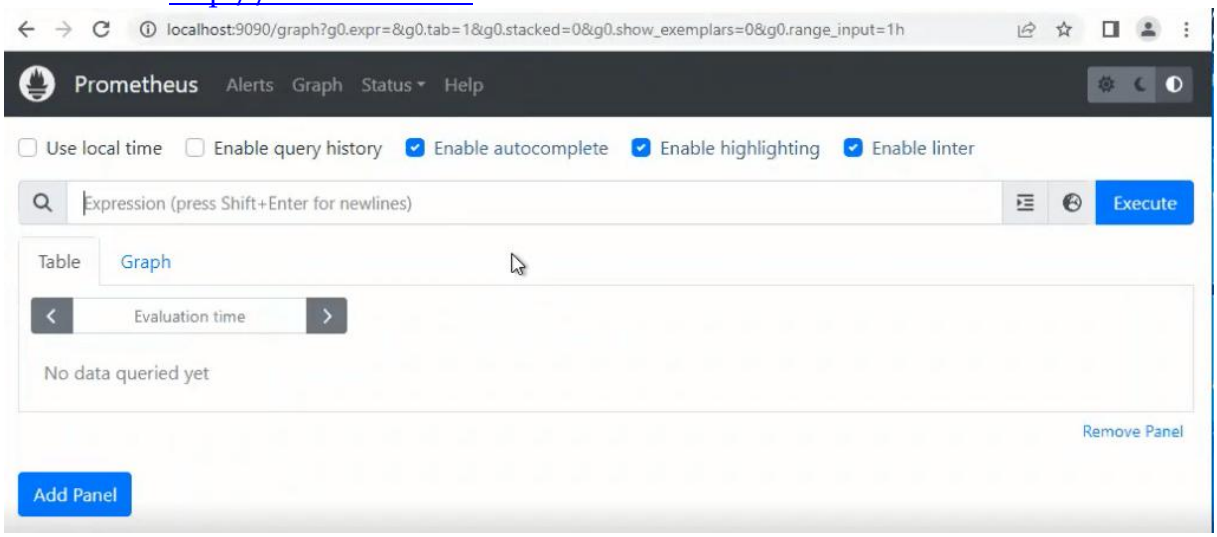
Instalation de la supervision

Notre supervision va être constitué de trois éléments
Windows exporter qui va mettre en place les informations

Prometheus qui va regrouper les informations des différents Windows exporter
Grafana qui va permetre de mettre en forme et visualiser ces informations.

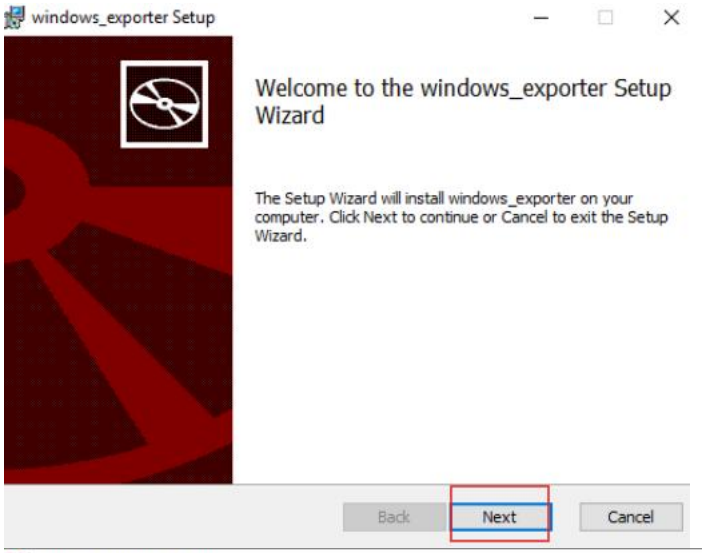
Instalation de prometheus

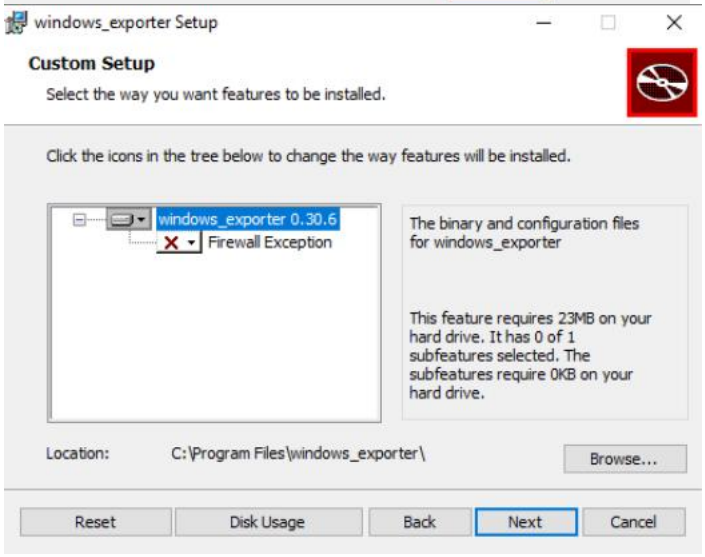
Télécharger prometeus et ouvrez un CMD dans le dossier et rentrer cette commande
prometheus.exe --config.file prometheus.yml --web.listen-address ":9090" --storage.tsdb.path "data"
Maintenant prometeus est correctement installer sur votre machine. Vous pouvez le vérifier sur http://localhost:9090

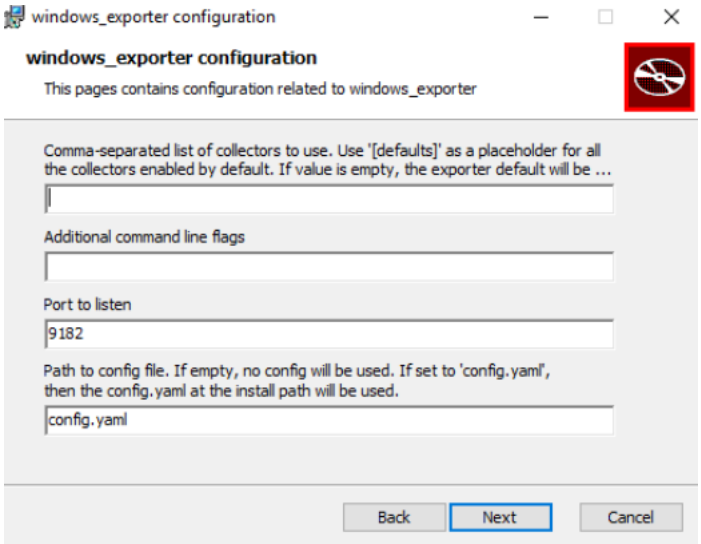


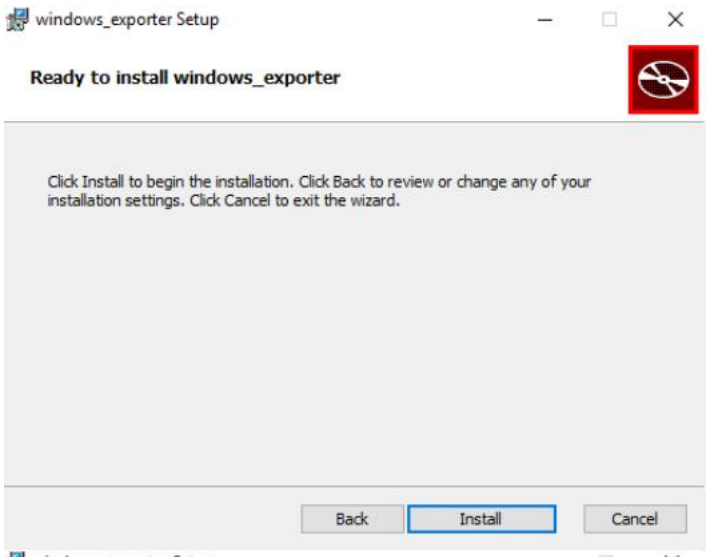
Installation Windows Exporter

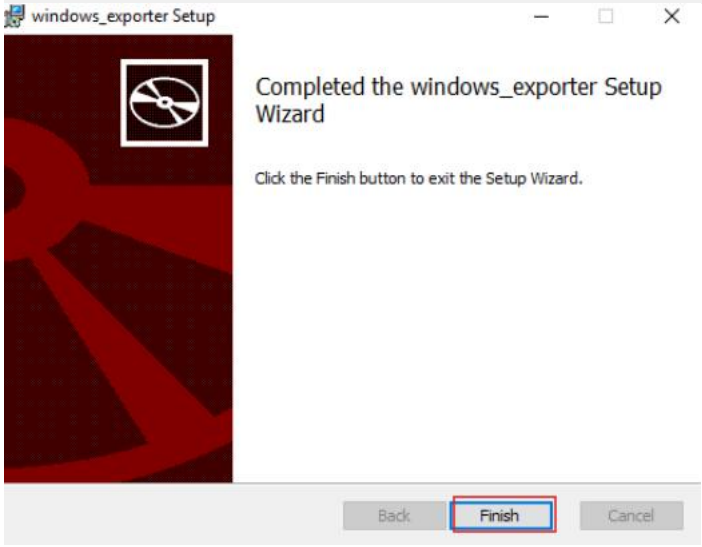
Cette étape est à faire sur tout les serveurs que vous voulez superviser.
Télécharger windows exporter ici :
https://github.com/prometheus-community/windows_exporter/releases
Ouvrer le msi puis vous pouvez garder la config de base


windows_exporter Setup
Welcome to the windows_exporter Setup Wizard
The Setup Wizard will install windows_exporter on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

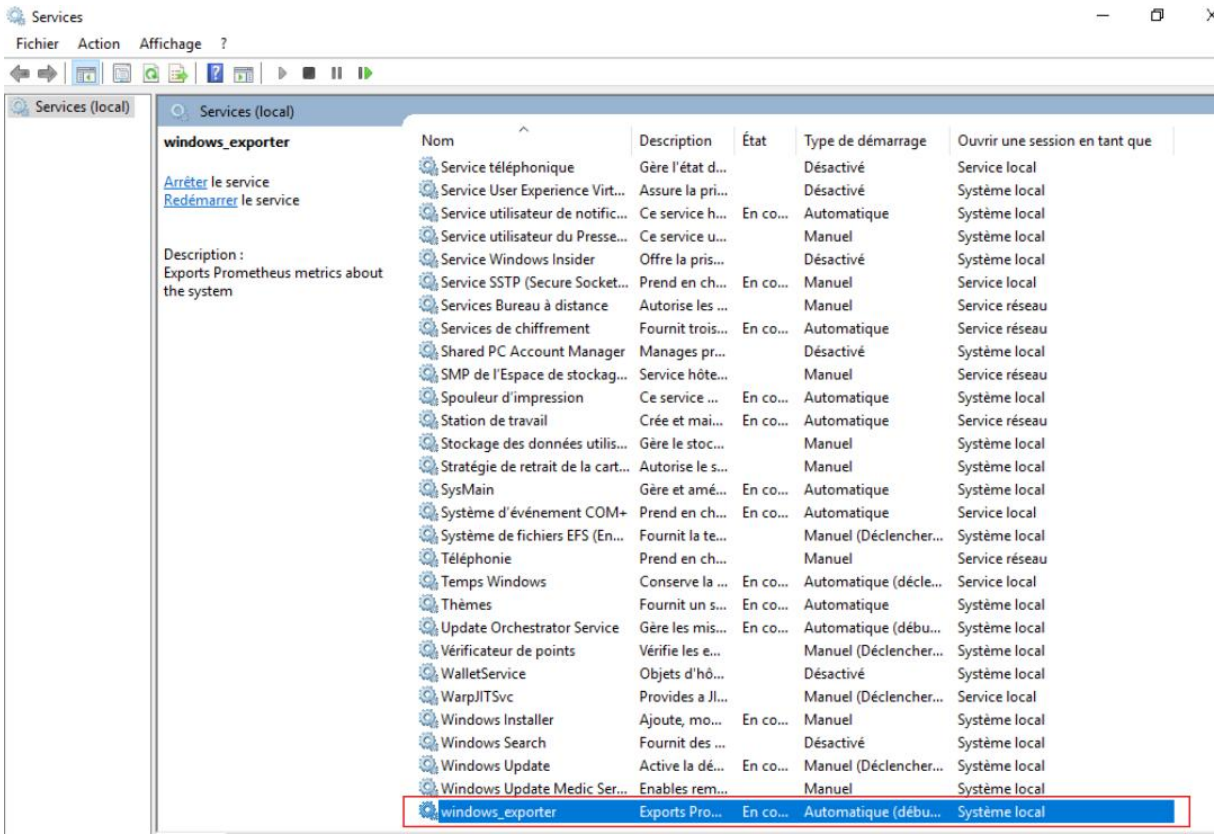

windows_exporter Setup
Custom Setup
Select the way you want features to be installed.
Click the icons in the tree below to change the way features will be installed.
windows_exporter 0.30.6
Firewall Exception
The binary and configuration files for windows_exporter
This feature requires 23MB on your hard drive. It has 0 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.
Location:
C:\Program Files\windows_exporter\
Browse...
Reset
Disk Usage
Back
Next
Cancel


windows_exporter configuration
windows_exporter configuration
This pages contains configuration related to windows_exporter
Comma-separated list of collectors to use. Use '[defaults]' as a placeholder for all the collectors enabled by default. If value is empty, the exporter default will be ...
Additional command line flags
Port to listen
9182
Path to config file. If empty, no config will be used. If set to 'config.yaml', then the config.yaml at the install path will be used.
config.yaml
Back
Next
Cancel

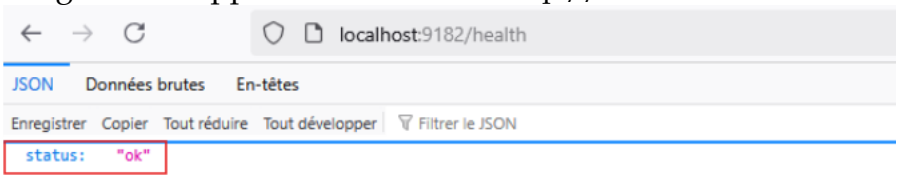




Windows exporter devrait apparaitre dans vos services :



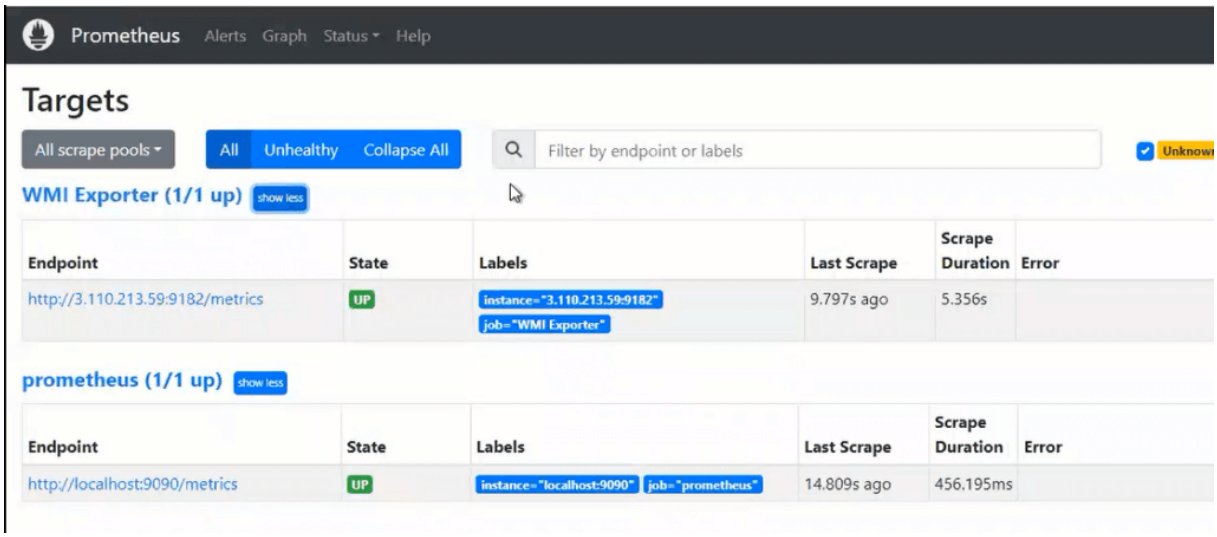
Et également apparaitre à l'adresse http://localhost:9182



Il suffit enfin d'ajouter ceci dans le fichier Prometheus.yml qui se trouve dans les fichier de votre prometheus

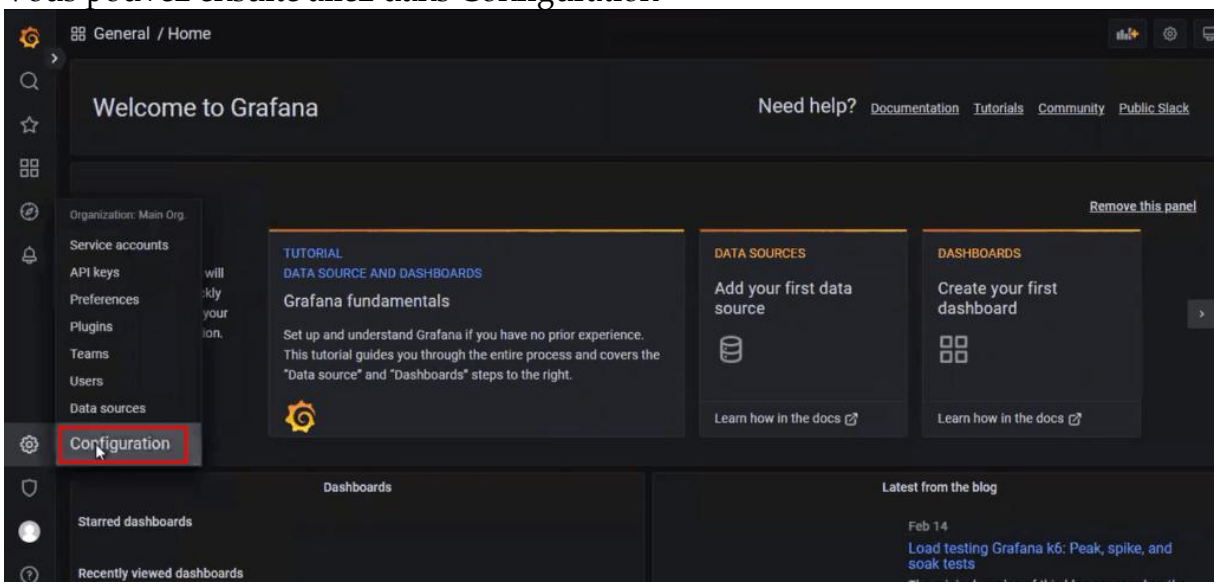
```
- job_name: "WMI Exporter"

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.

    static_configs:
      - targets: ["IP_Client:9182"]
```

Relancer le service prometeus sur votre serveur puis vous pouvez vérifier si le nouveau serveur apparait bien à l'adresse
https://localhost:9090/targets

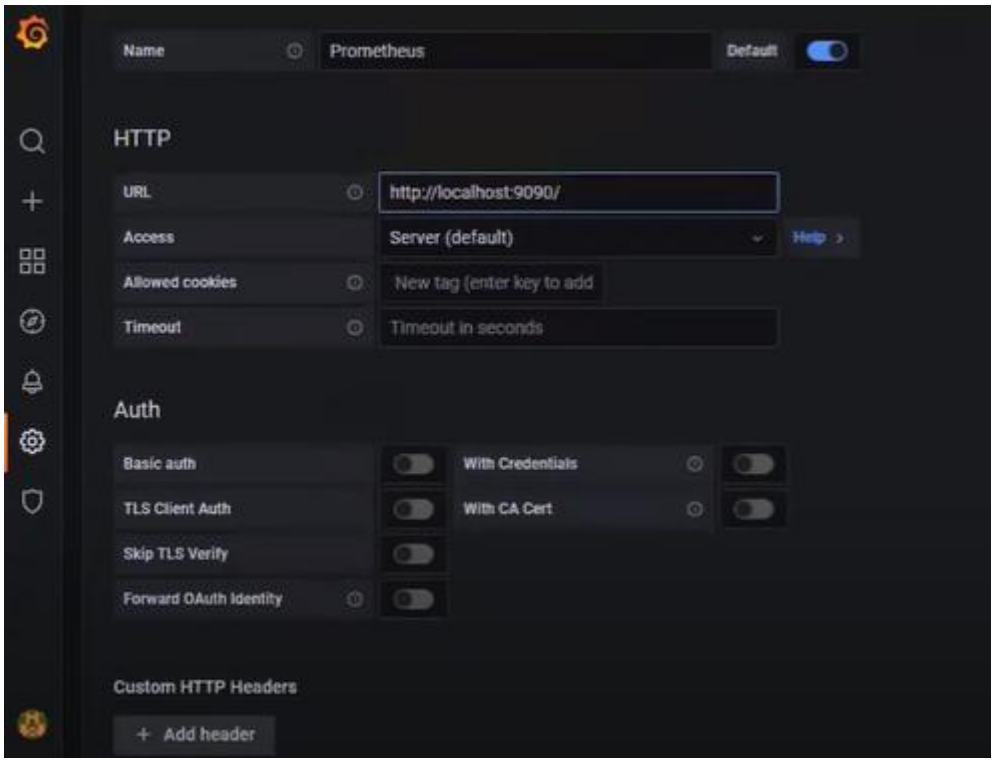


Installation Grafana

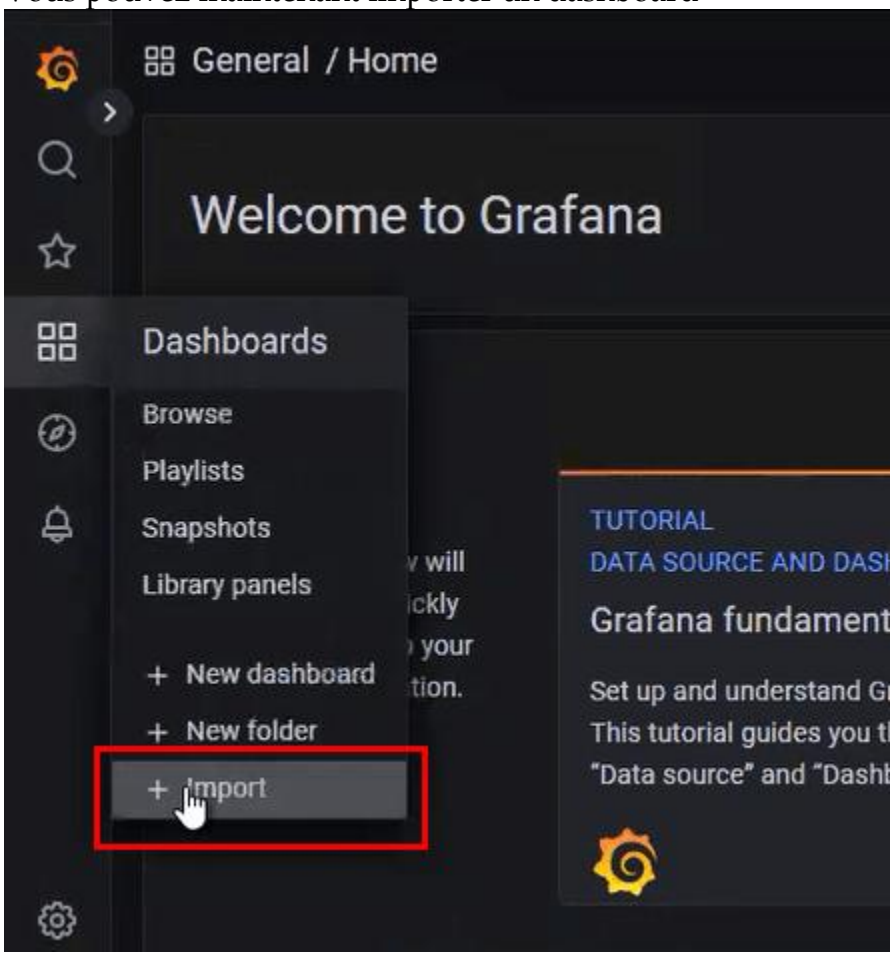
Allez chercher la version la plus récente de Grafana puis installer là en laissant tout par défaut.
Vous pouvez ensuite vous connecter à l'adresse
http://localhost:3000
Avec le nom admin et mot de passe admin
Vous pouvez ensuite allez dans Configuration



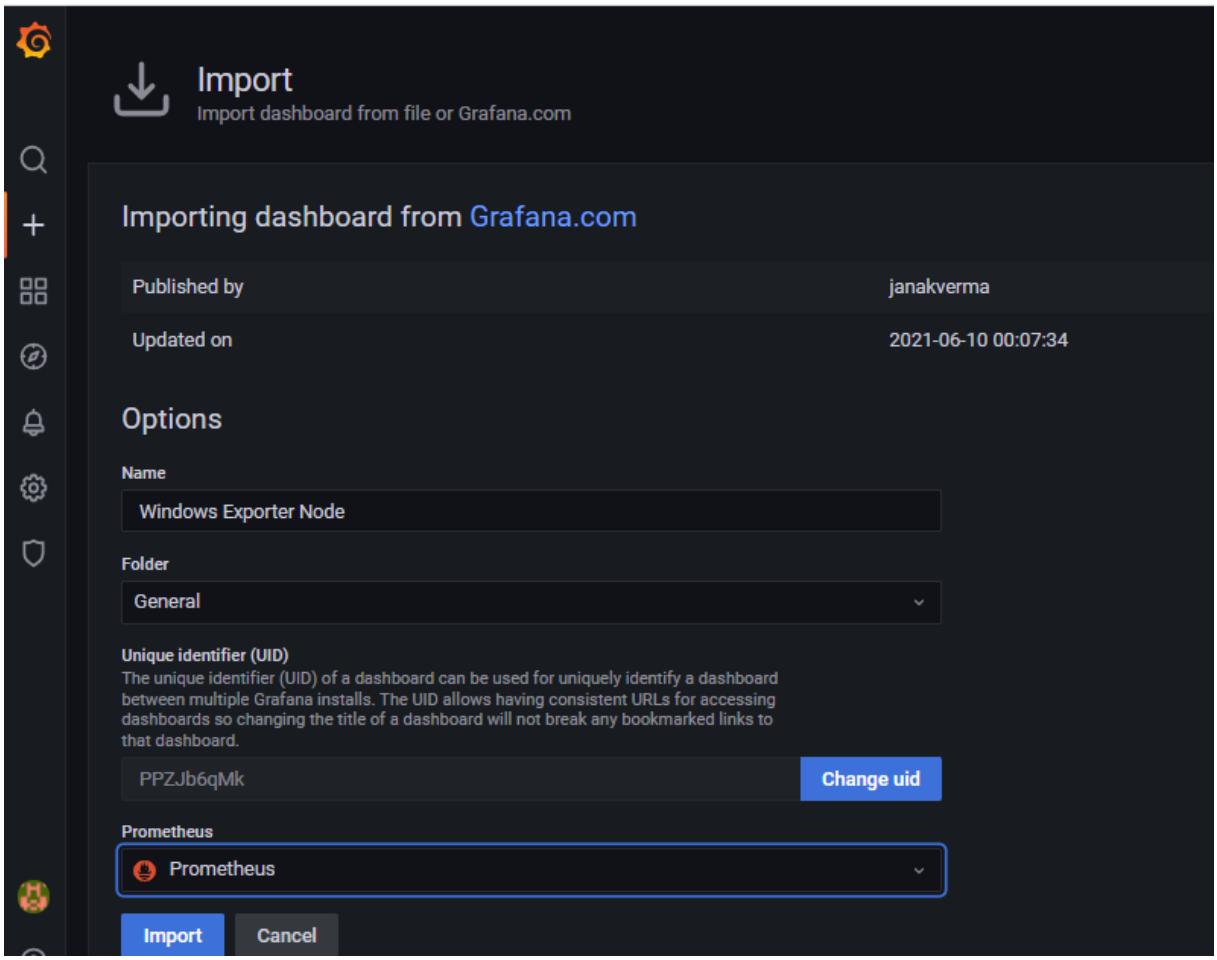
Puis dans **App Data sources** sélectionner **Prometheus**
Rentrer l'URL de votre Prometheus et sauvegarder.



Vous pouvez maintenant importer un dashboard



Donner un nom et cliquez sur **Import**



Vous aurez un template personnalisé.

Installation HMAIL Serveur

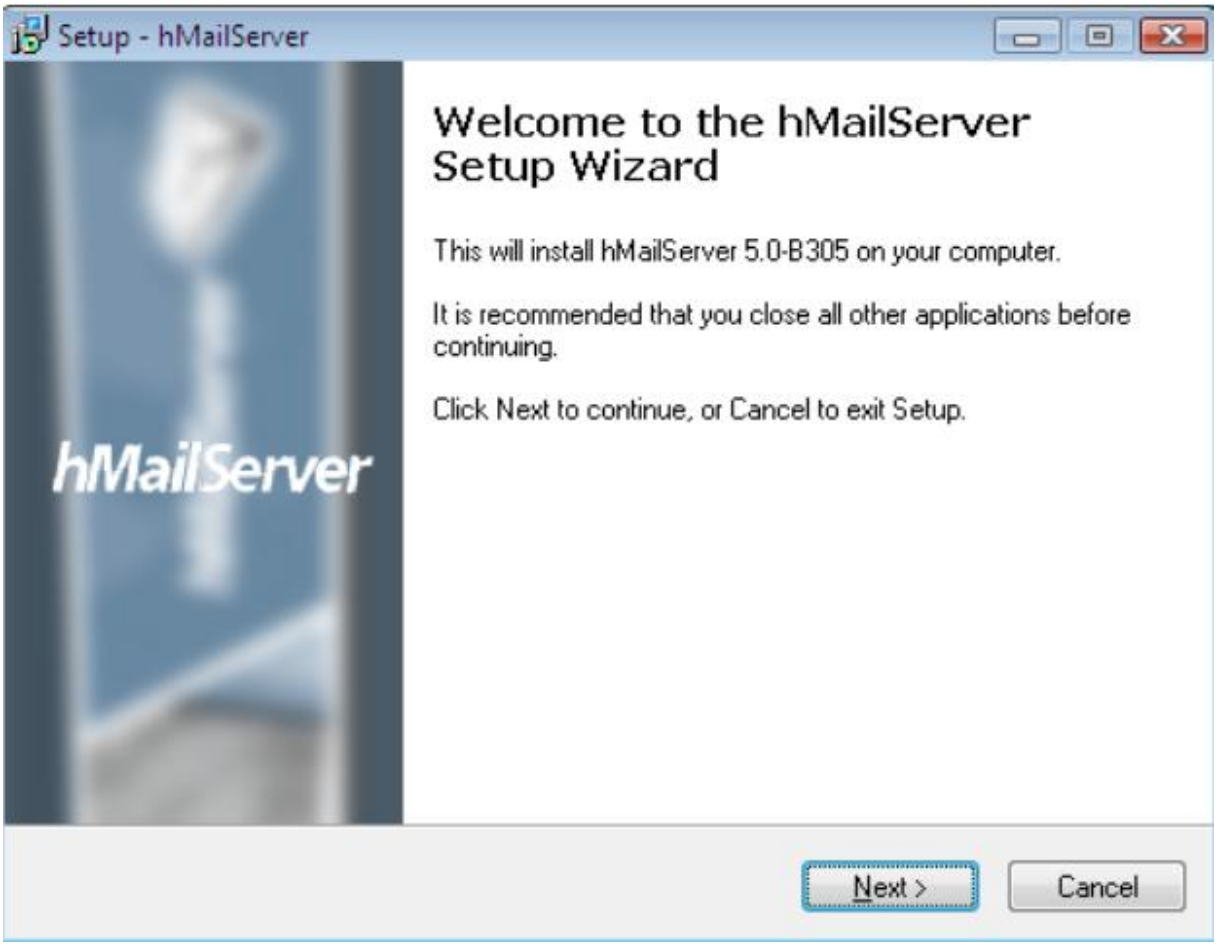
Étape 1 : Télécharger

La première étape consiste à télécharger hMailServer. Le programme d'installation est disponible sur la page de téléchargement. Il est recommandé de prendre la **dernière version stable**.

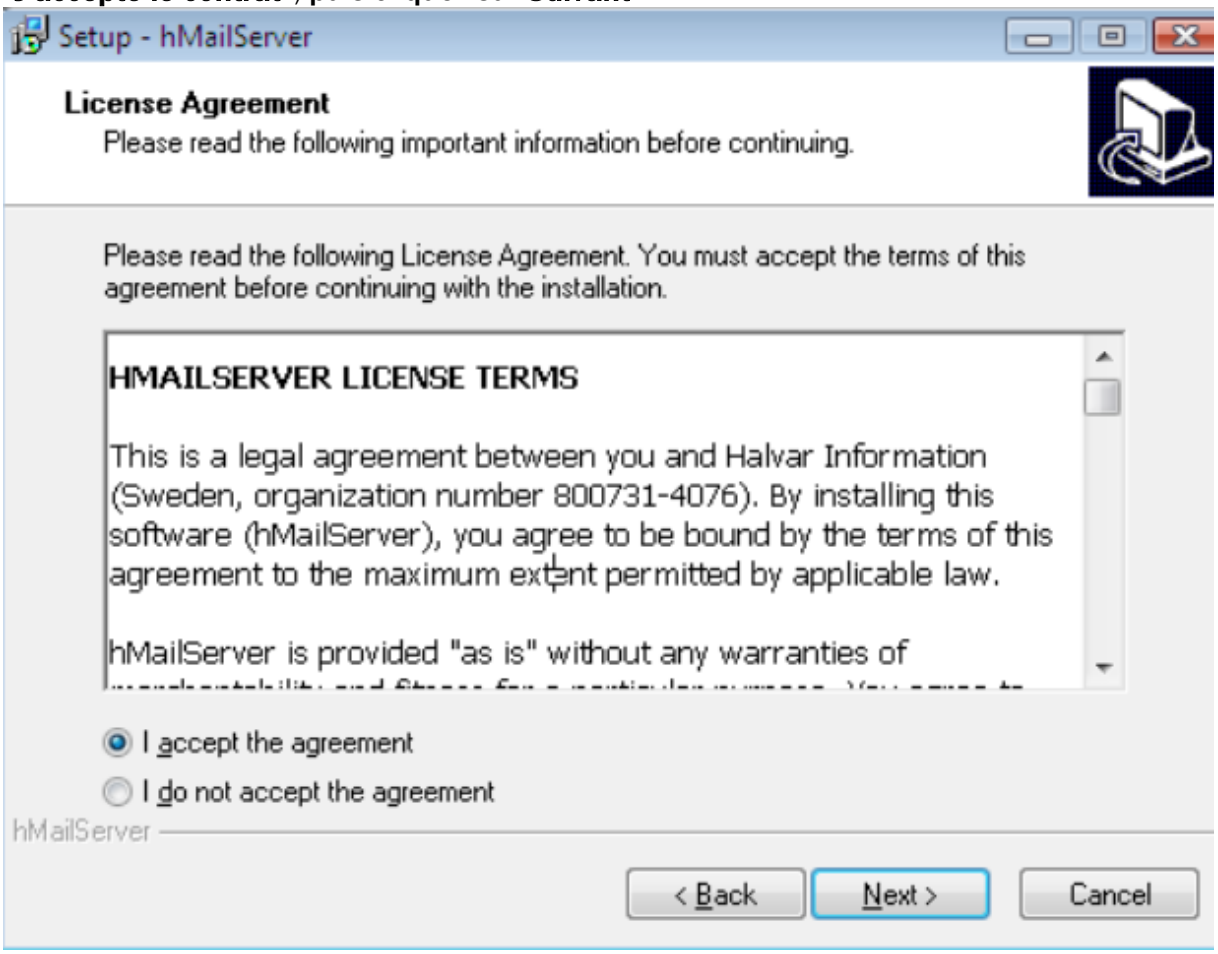
Étape 2 : Installer

Double-cliquez sur le fichier téléchargé pour lancer l'installation.

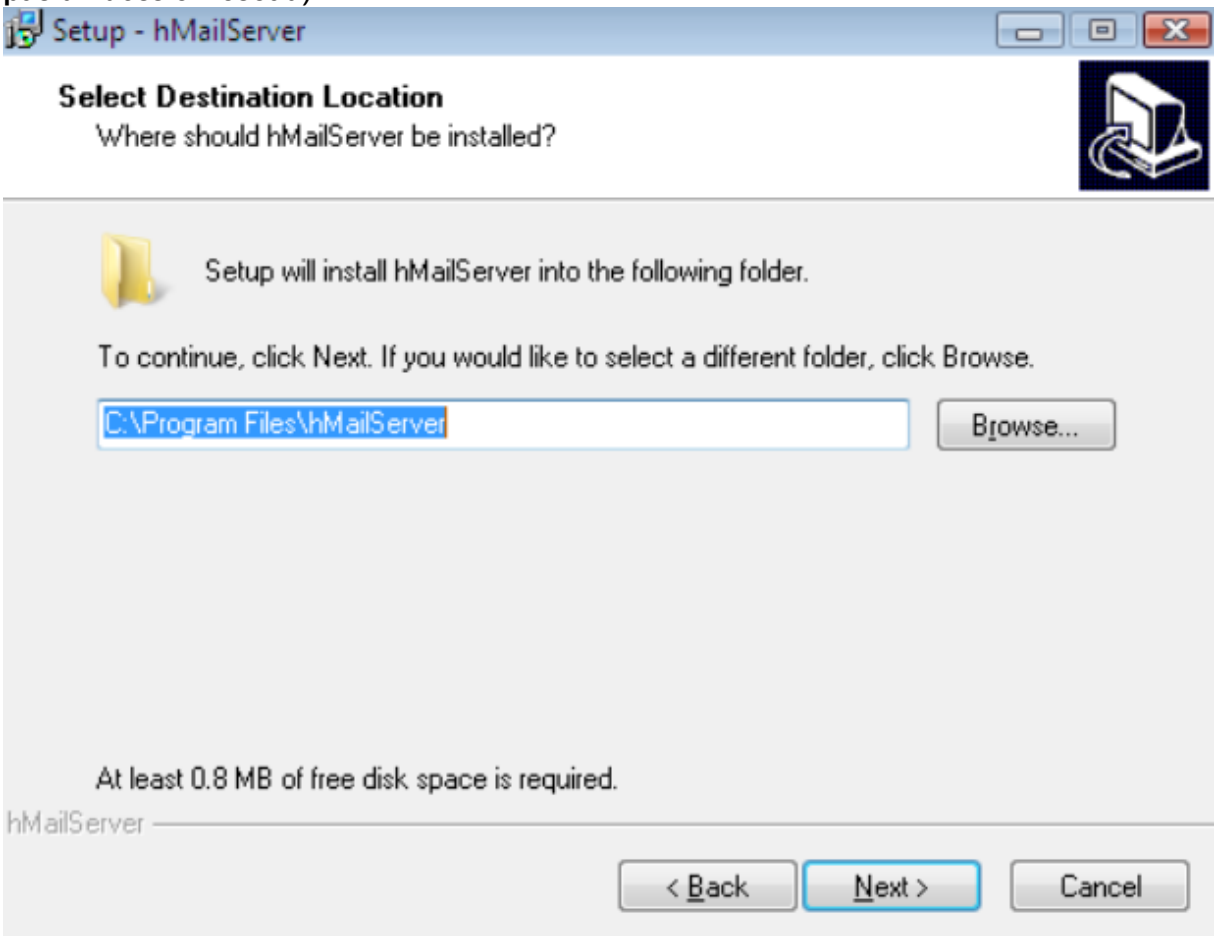
Une première fenêtre **"Bienvenue"** s'affiche. Cliquez sur **Suivant**.



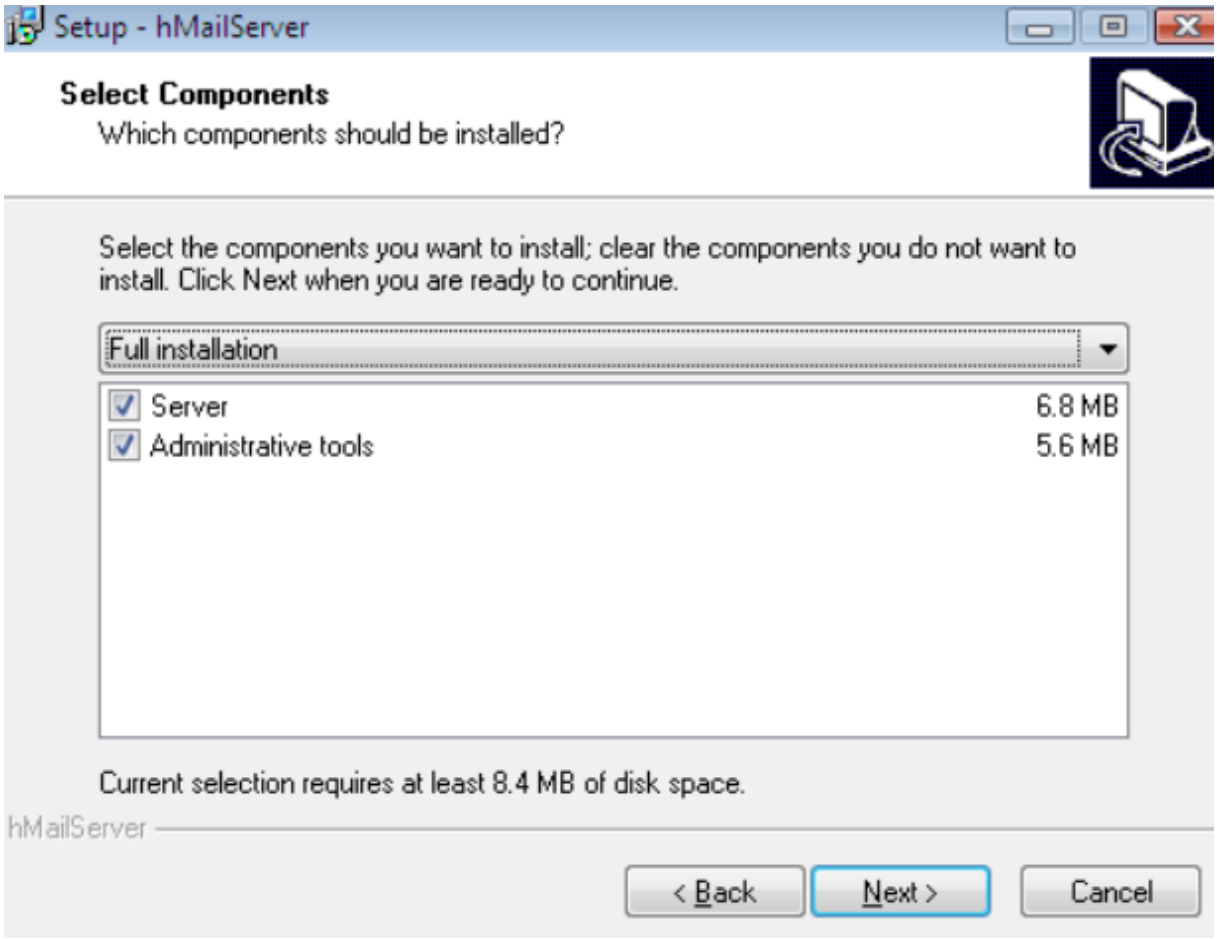
Ensuite, lisez le contrat de licence. Si vous acceptez les conditions, cochez **"J'accepte le contrat"**, puis cliquez sur **Suivant.**



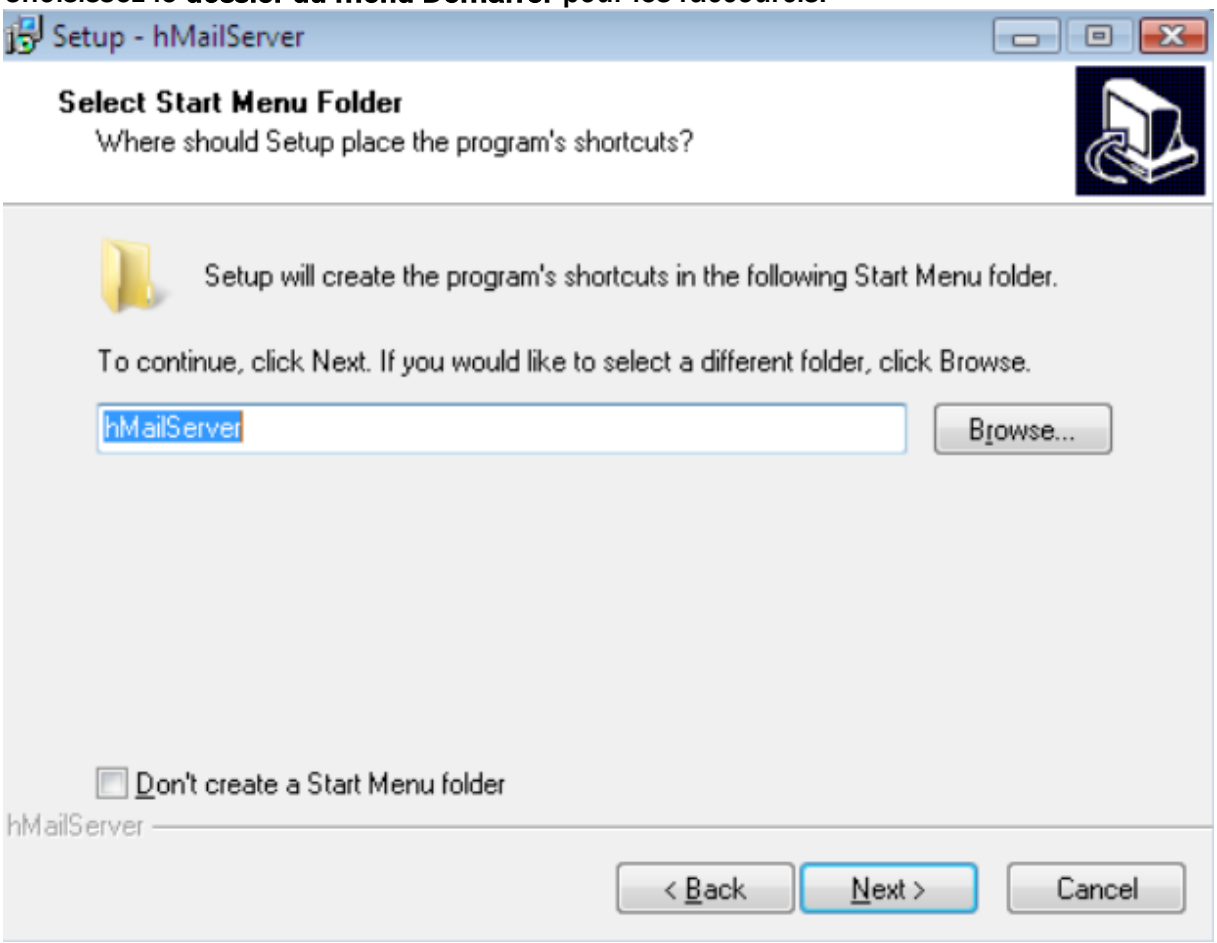
Choisissez le **dossier de destination** (il est recommandé d'utiliser un disque local, pas un dossier réseau).



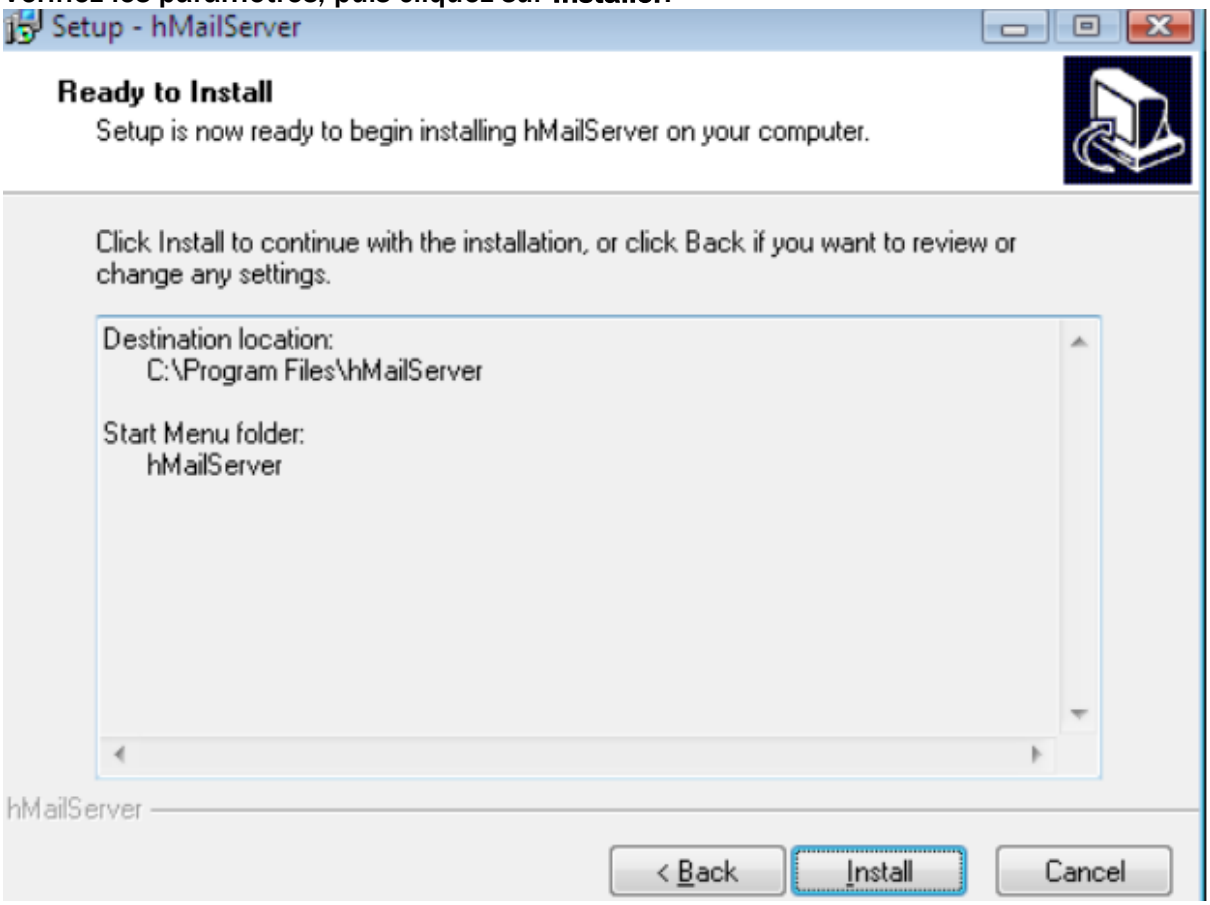
Choisissez les **composants à installer**. Sur le serveur principal, installez tout. Si vous administrez un serveur distant, vous pouvez ne cocher que les outils d'administration.


Setup - hMailServer
Select Components
Which components should be installed?
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.
Full installation
Server
6.8 MB
Administrative tools
5.6 MB
Current selection requires at least 8.4 MB of disk space.
hMailServer
< Back
Next >
Cancel

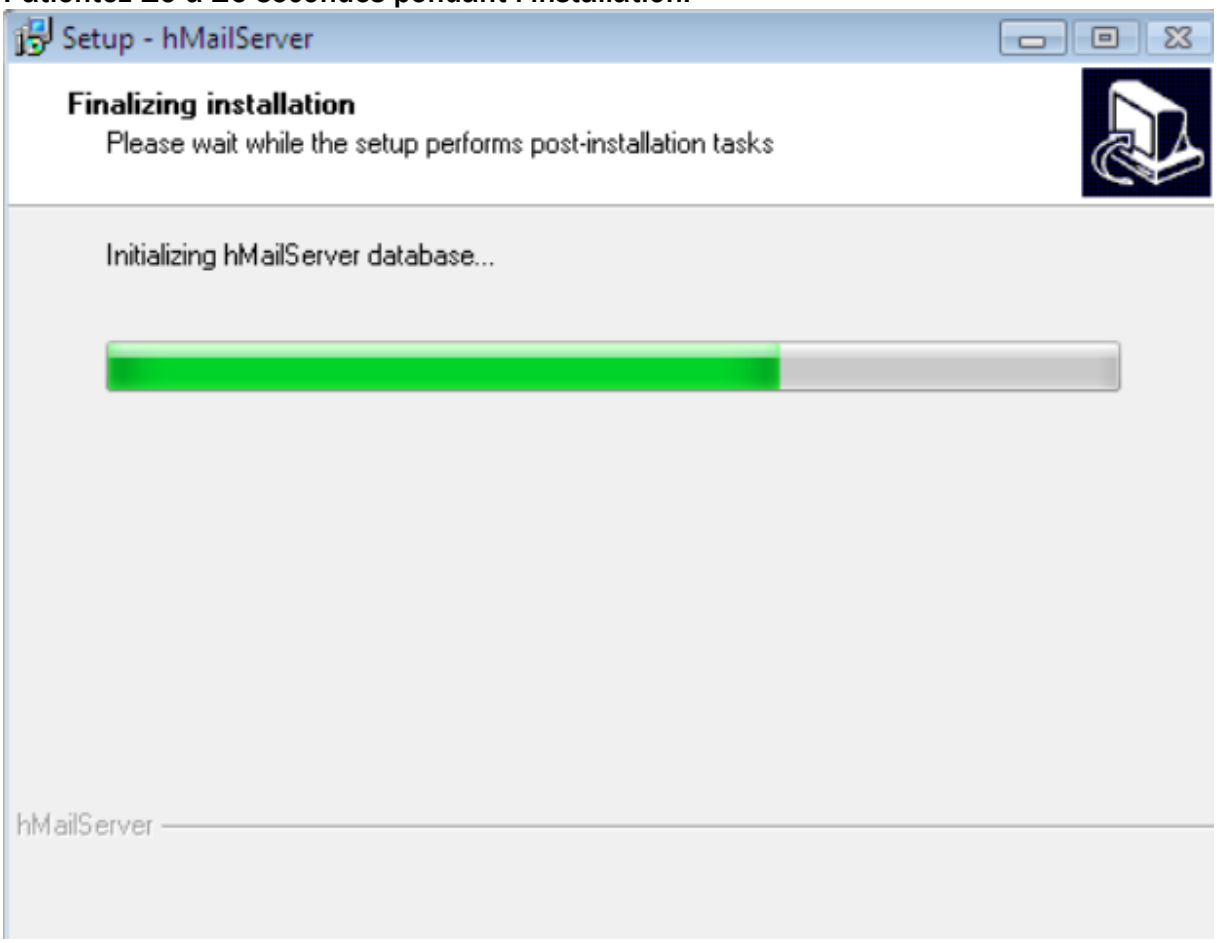
Choisissez le **dossier du menu Démarrer** pour les raccourcis.



Vérifiez les paramètres, puis cliquez sur **Installer**.



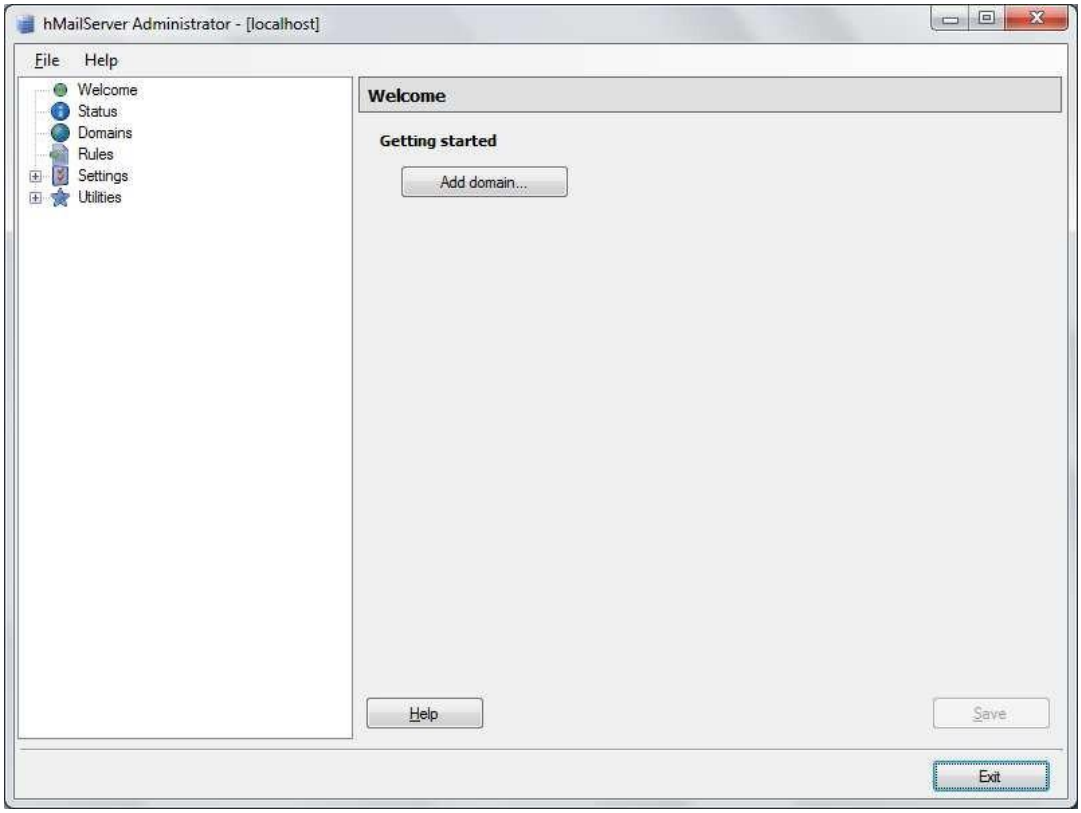
Patientez 10 à 20 secondes pendant l'installation.



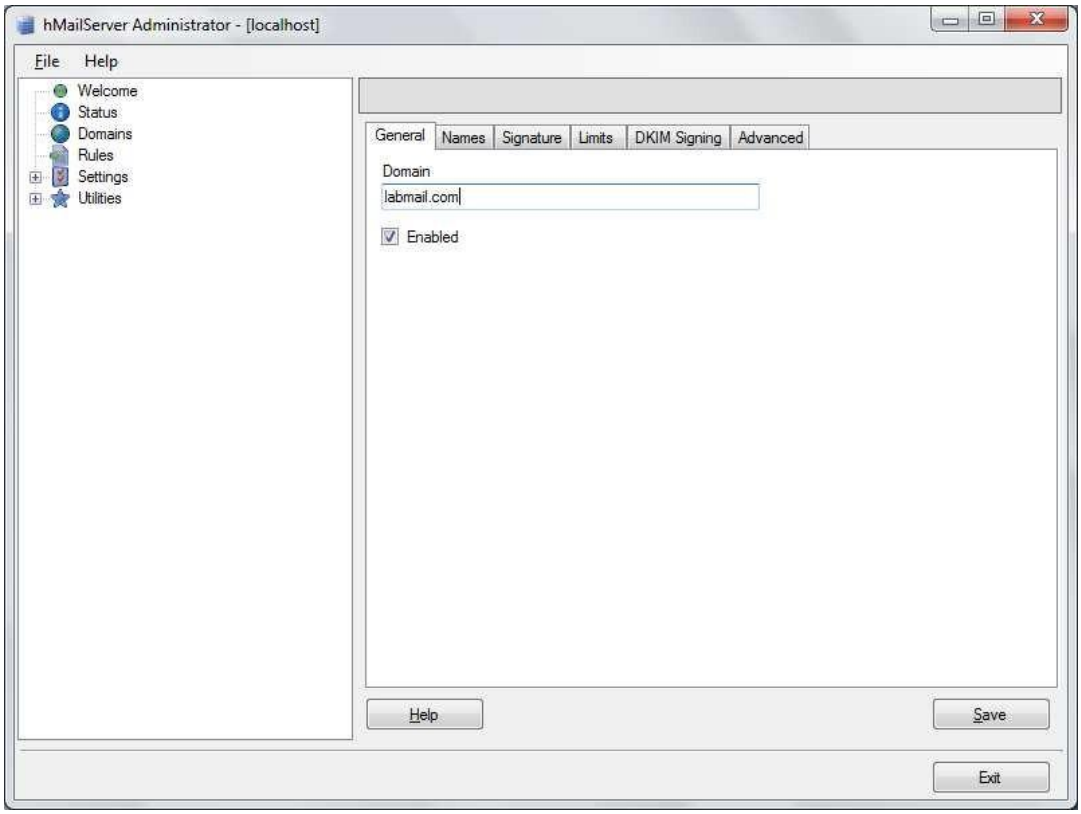
Définir le mot de passe principal

Après l'installation, vous devez définir un **mot de passe principal** pour sécuriser l'administration de hMailServer (minimum 6 caractères).
Ce mot de passe sera demandé à chaque fois que vous ouvrirez la console

Configuration de base de hMailServer :

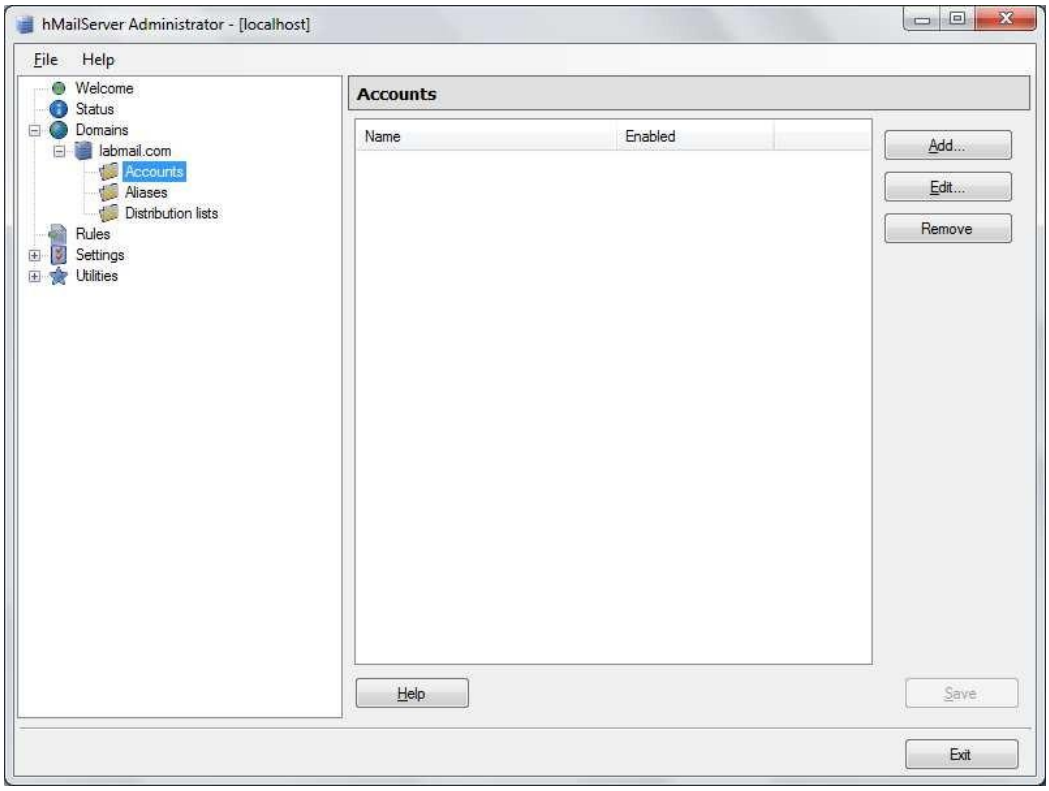


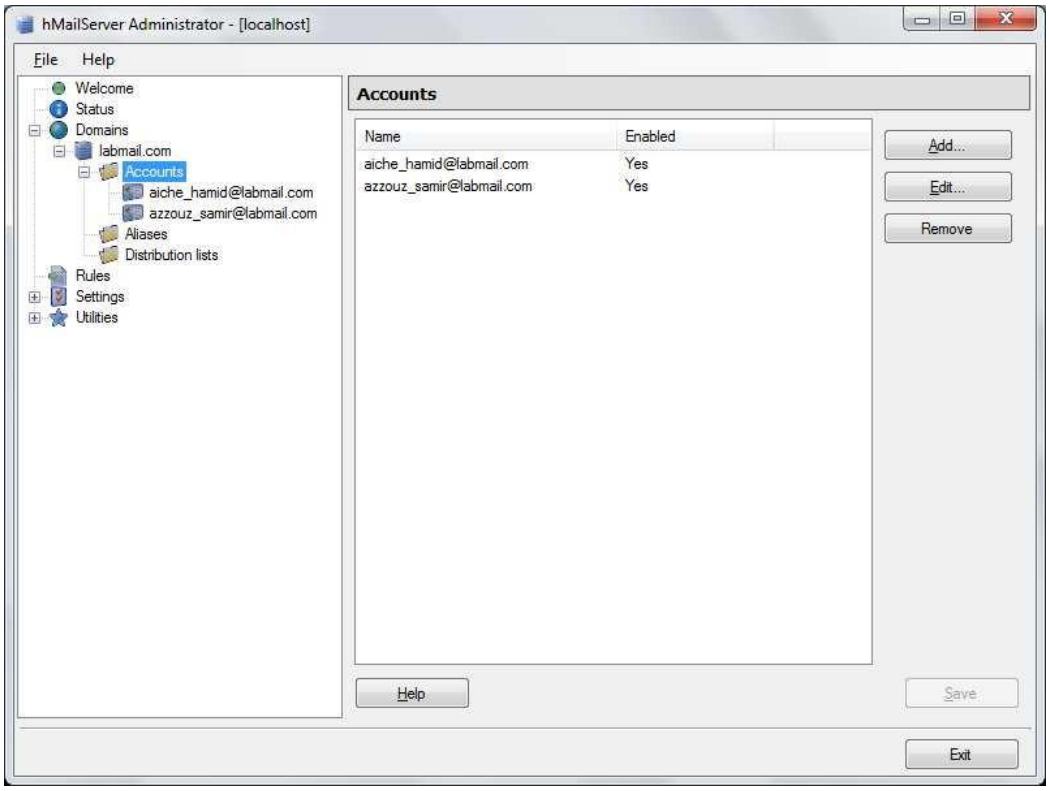
Voici la console d'administration de hMailServer.
Cliquez sur le bouton « Add Domain » pour ajouter votre domaine de messagerie.



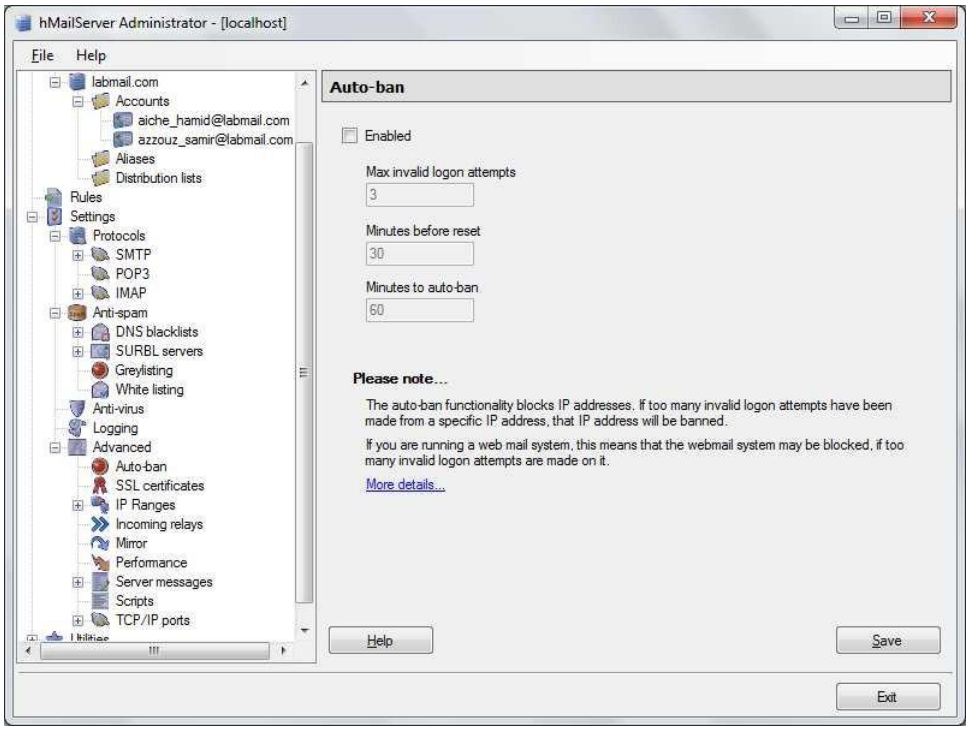
Cliquer sur le bouton « Save ».

Nous allons à présent pouvoir créer un ou plusieurs comptes utilisateurs pour effectuer nos tests.

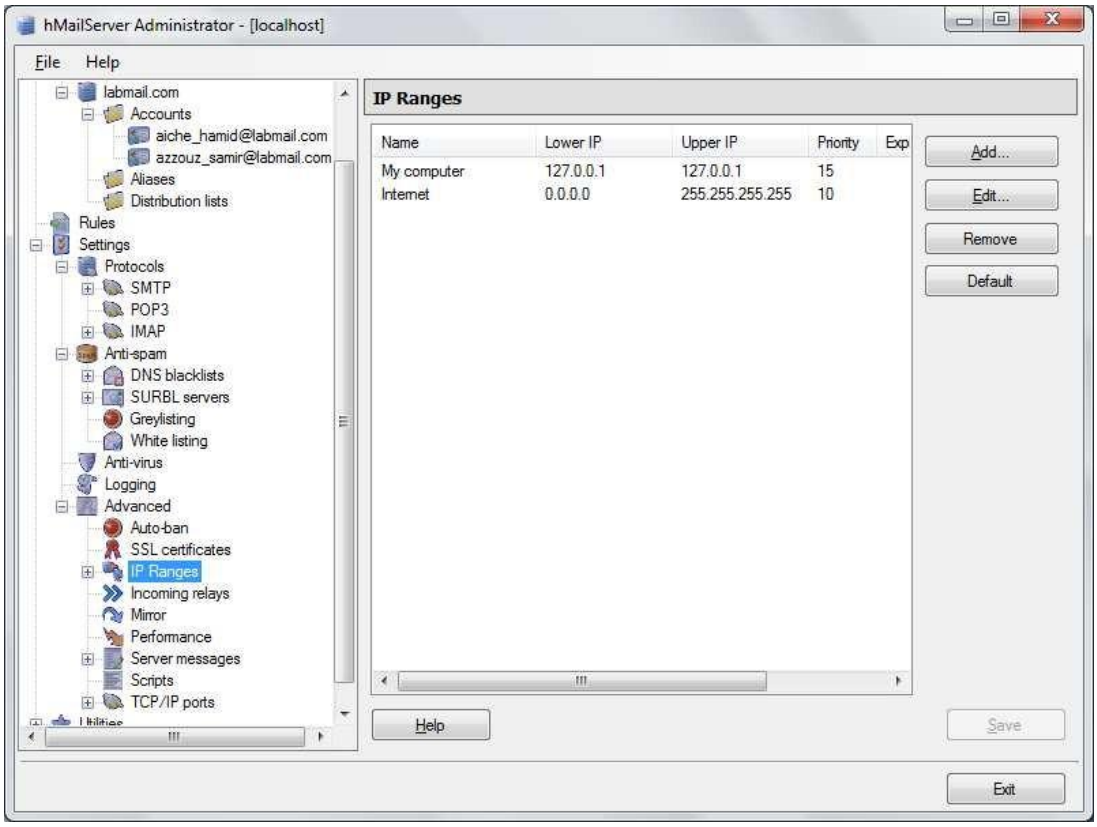




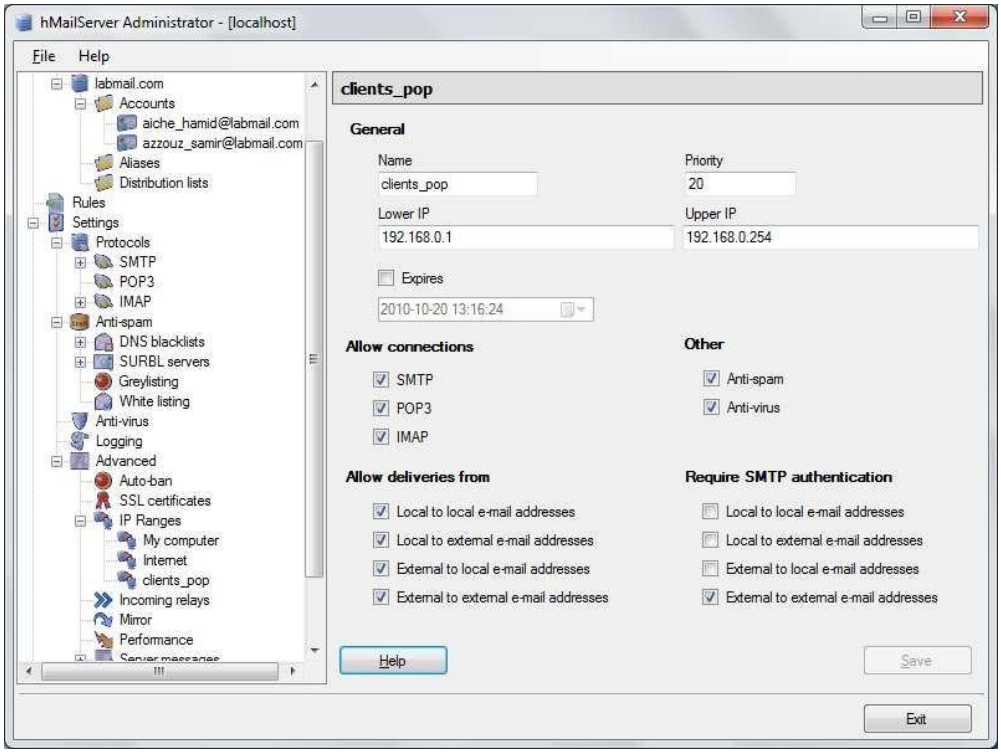
À présent, passons à la phase de configuration.
Tout d'abord nous allons désactiver la fonctionnalité AUTO-BAN : Settings\Advanced\Auto-ban



Configurez le serveur pour qu'il accepte les adresses IP de votre réseau en allant dans Settings > Advanced > IP Ranges.



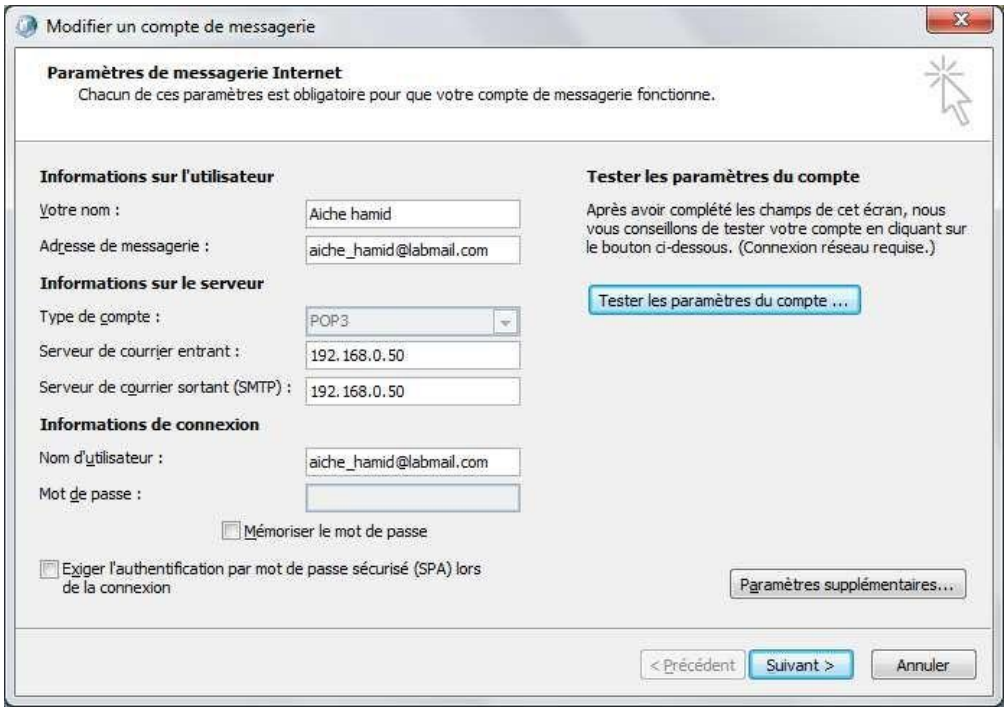
Cliquez sur le bouton « Add » pour ajouter une plage d'adresse :



Le champ « Priority » doit avoir une valeur supérieure à celle définie dans la plage par defaut « Internet »

A présent, votre serveur de messagerie SMTP/POP3/IMAP4 est fonctionnelle. Vous pouvez le tester en utilisant le client POP3 de votre choix : Outlook, OutlookExpress, ThunderBird, …

Exemple de configuration : un client Outlook 2007 configuré en POP



Faites des tests d'envoi/réception pour vous assurer que tout fonctionne correctement.

Installation du Webmail

Installation d'Apache :

Commencez par installer le service Apache sur le serveur.
Lancez le fichier d'installation pour démarrer l'installation d'Apache.

Installation de PHP :

Lancez le fichier d'installation de PHP pour l'installer sur le serveur.

Installation de AfterLogic Webmail Lite :

Décompressez l'archive .zip
Ensuite, arrêtez le service Apache et ouvrez le fichier de configuration httpd.conf avec un éditeur de texte.
La directive DocumentRoot indique le dossier utilisé par défaut par Apache. Par défaut, elle est définie ainsi :

```
DocumentRoot "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs"
```

Remplacez cette ligne par :

```
DocumentRoot "C:/webmail/webmail"
```

De même, modifiez cette ligne :

```
<Directory "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs">
```

par :

```
<Directory "C:/webmail/webmail">
```

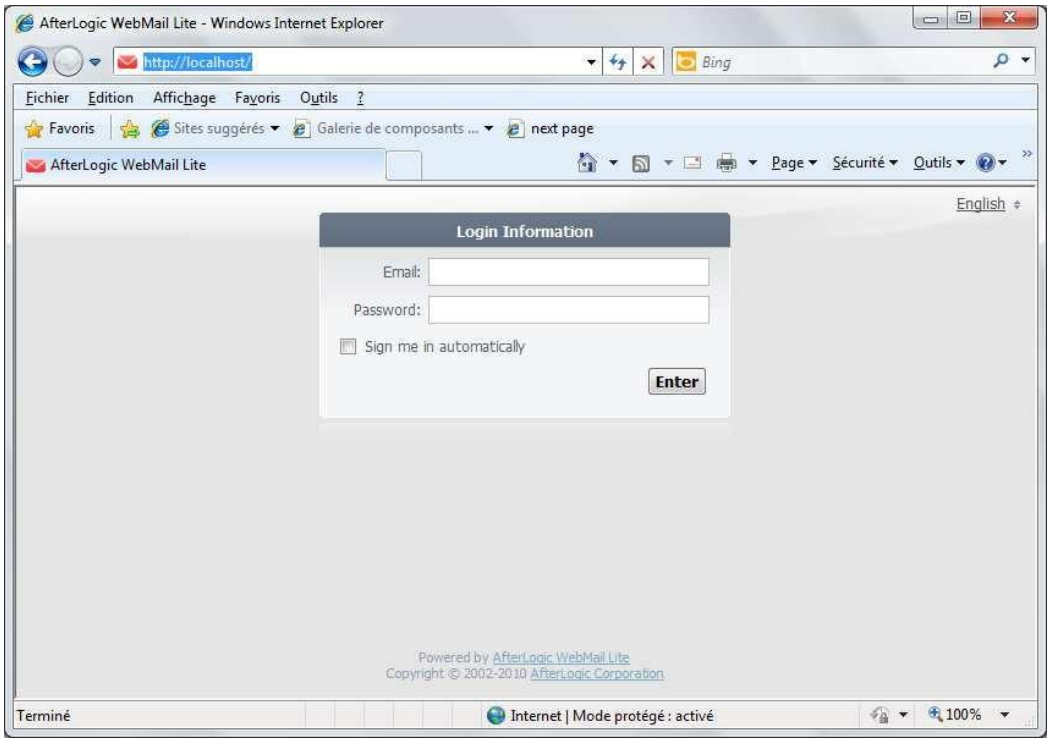
Et enfin, remplacez ce bloc :

```
php-template
CopierModifier
<IfModule dir_module>
  DirectoryIndex index.html
</IfModule>
```

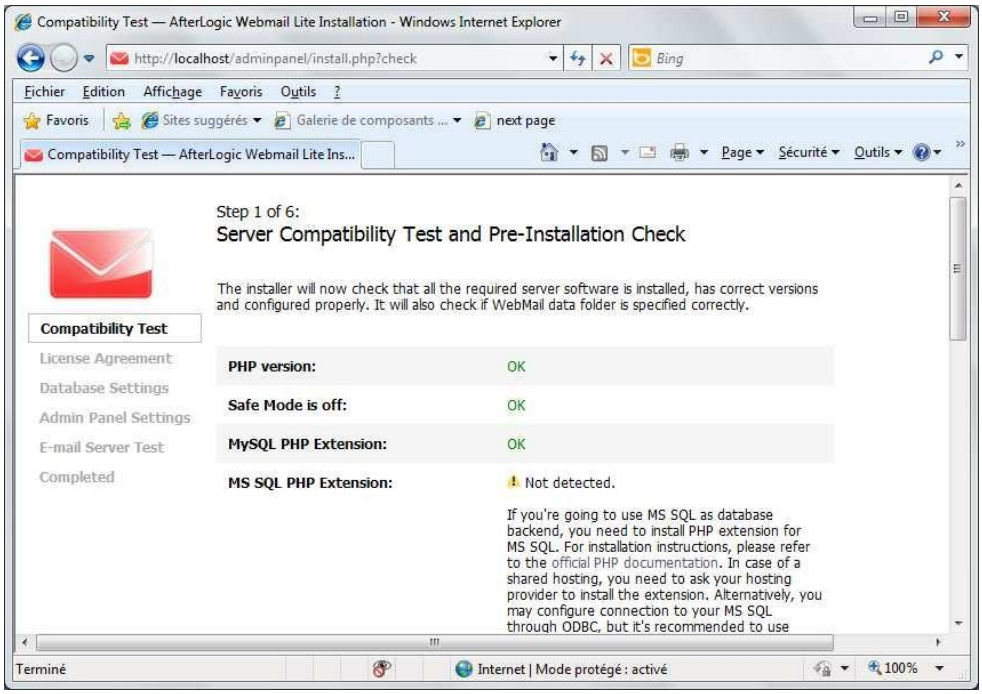
par :

```
php-template
CopierModifier
<IfModule dir_module>
  DirectoryIndex index.php index.html
</IfModule>
```

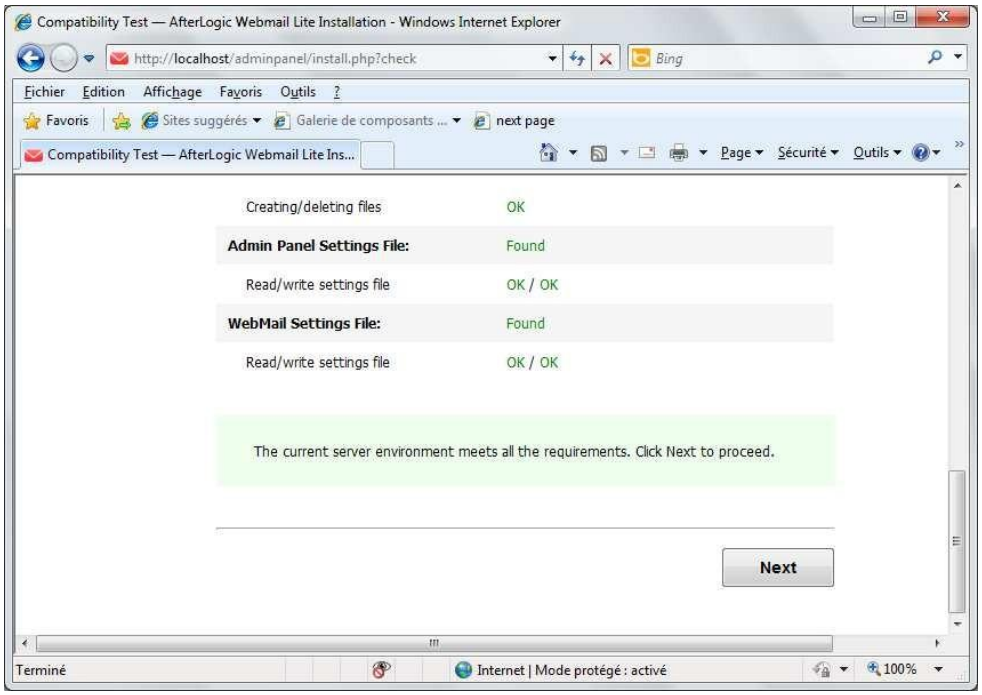
À présent, redémarrez le service Apache puis ouvrez l'adresse http://localhost dans votre navigateur.
Vous devriez voir une page similaire à celle-ci :



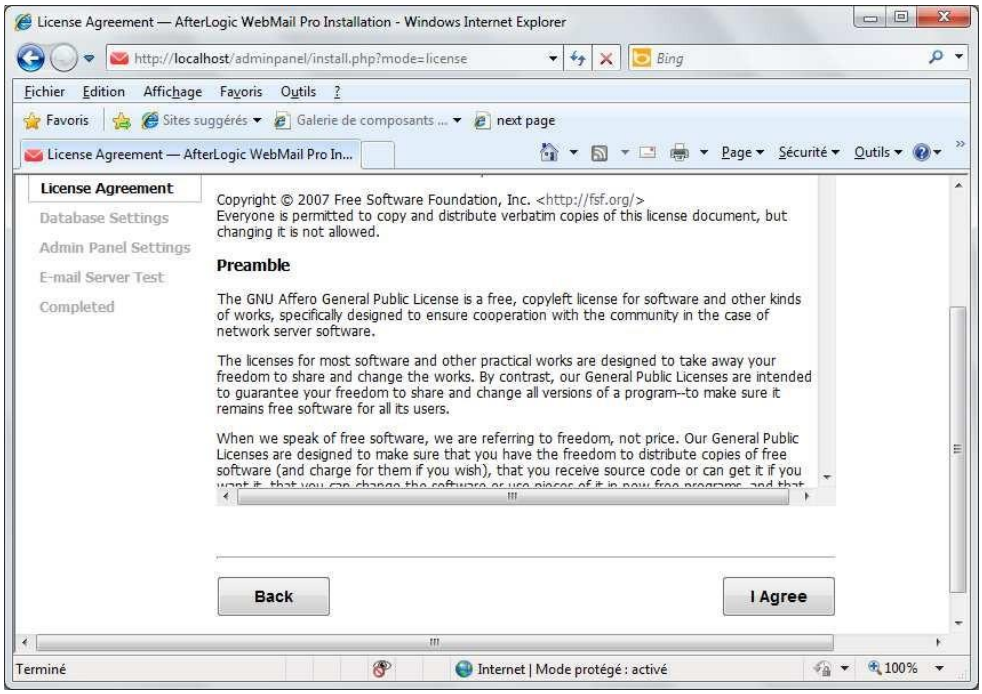
Connectez vous à présent à l'adresse http://localhost/adminpanel/install.htm et cliquez sur le lien
« Run the Installer ».



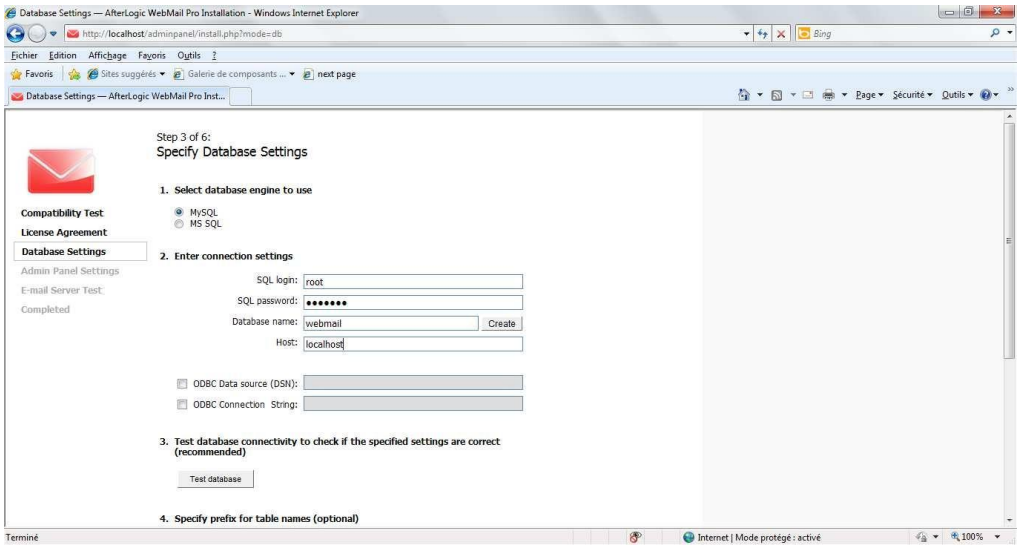
Le service effectue une série de test afin de s'assurer que les prérequis sont installés et fonctionnels.



Cliquez sur « Next ».



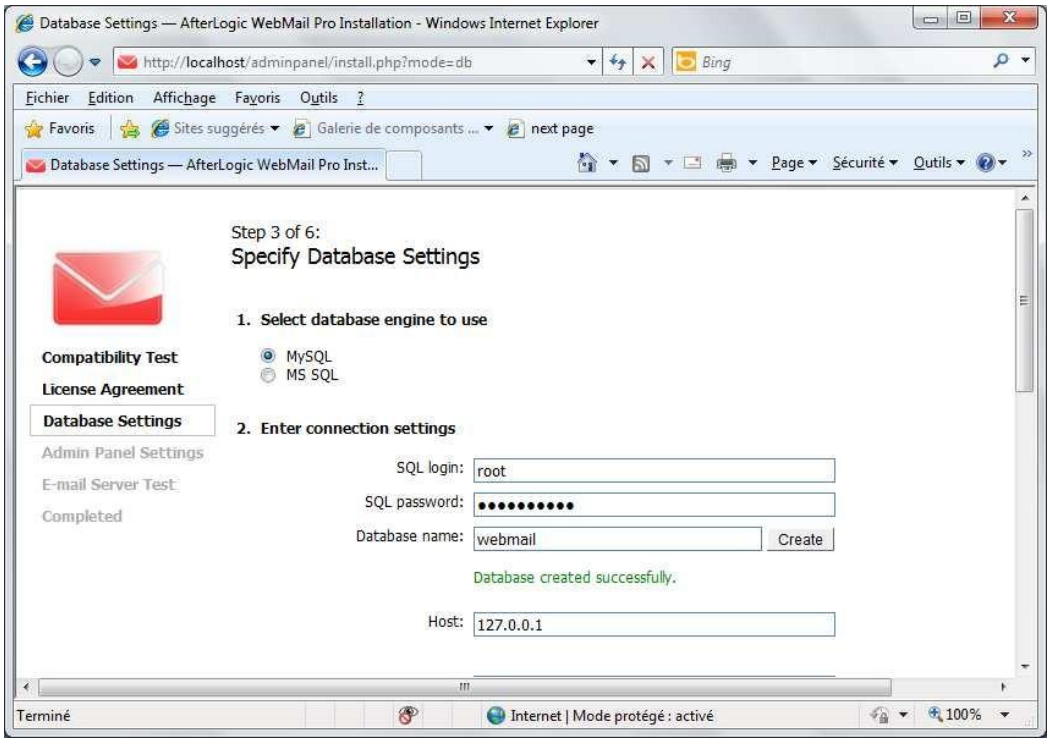
Acceptez les termes d'utilisation du produit en cliquant sur le bouton « I Agree »



Nous allons à présent paramétrer l'accés à la base de données (MySQL) utilisée par le webmail pour y stocker ses données.

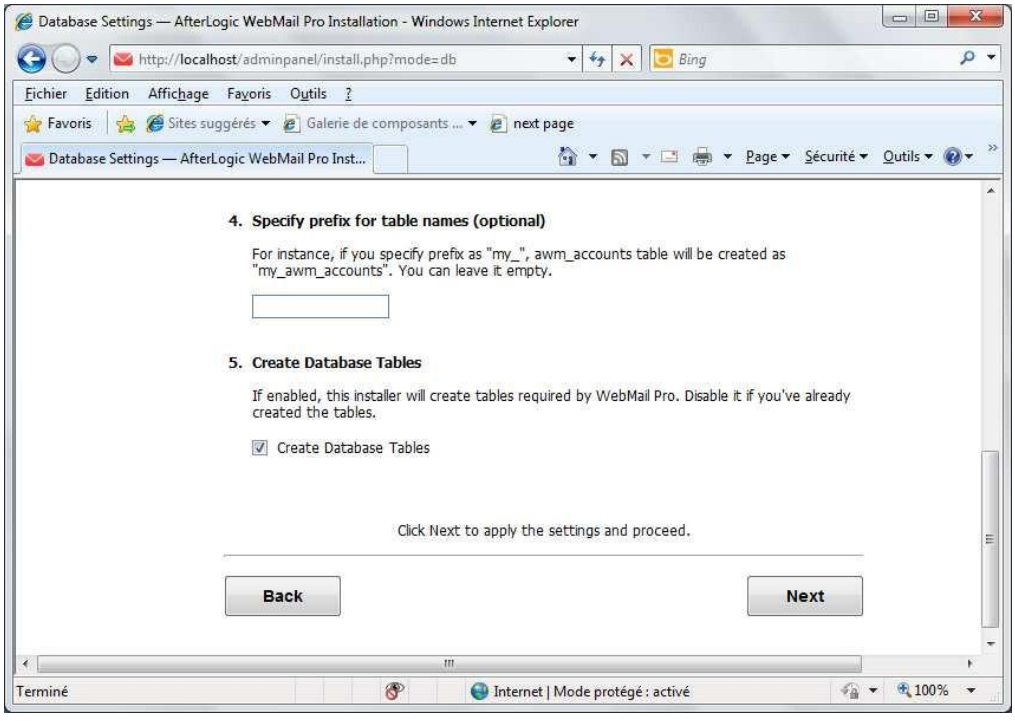
Type de base de données	MySQL
SQL Login	Root
SQL Password	*******
Database name	Webmail
Host	127.0.0.1

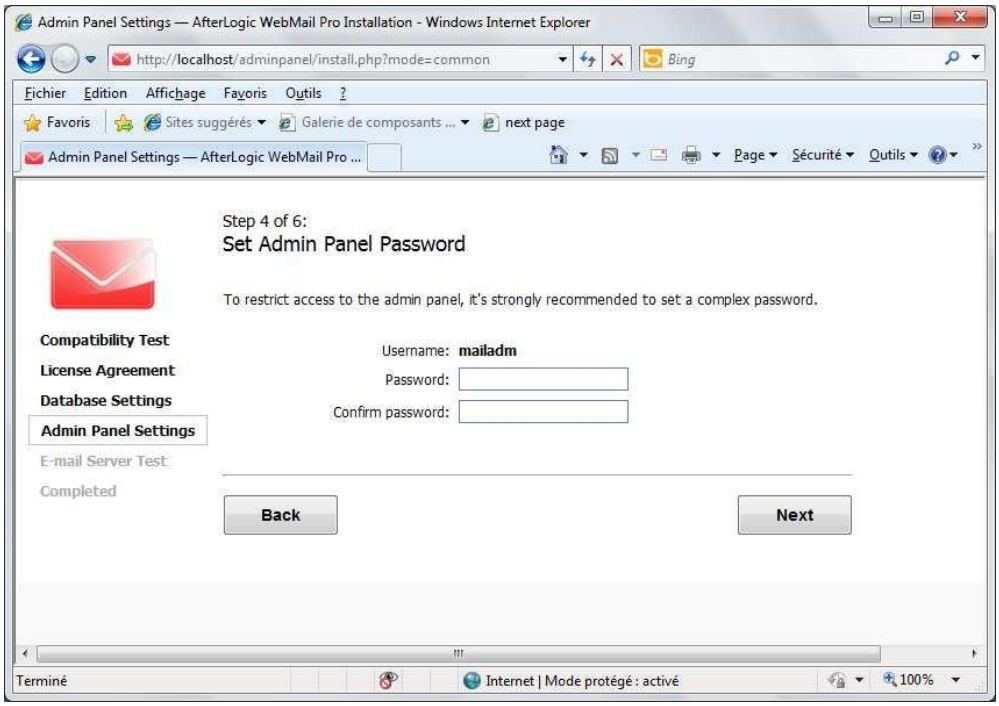
Cliquez à présent sur le bouton « Create »



Si la création se passe correctement, le message « Database created successfully »

Assurez vous que la case « Create Database tables » est cochée et cliquez sur le bouton « Next »

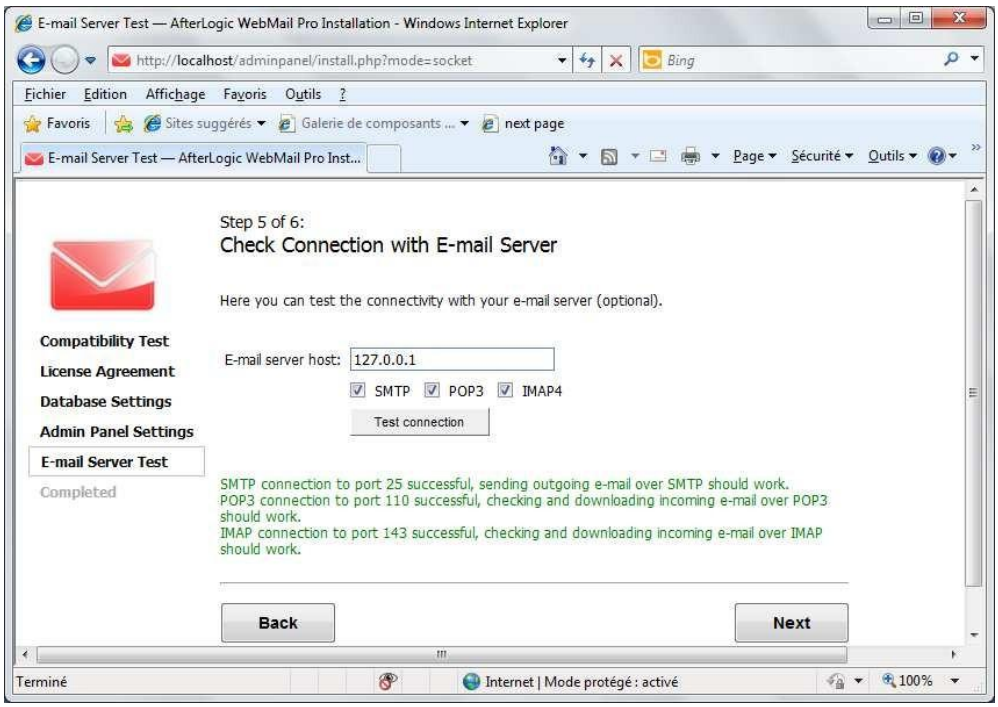




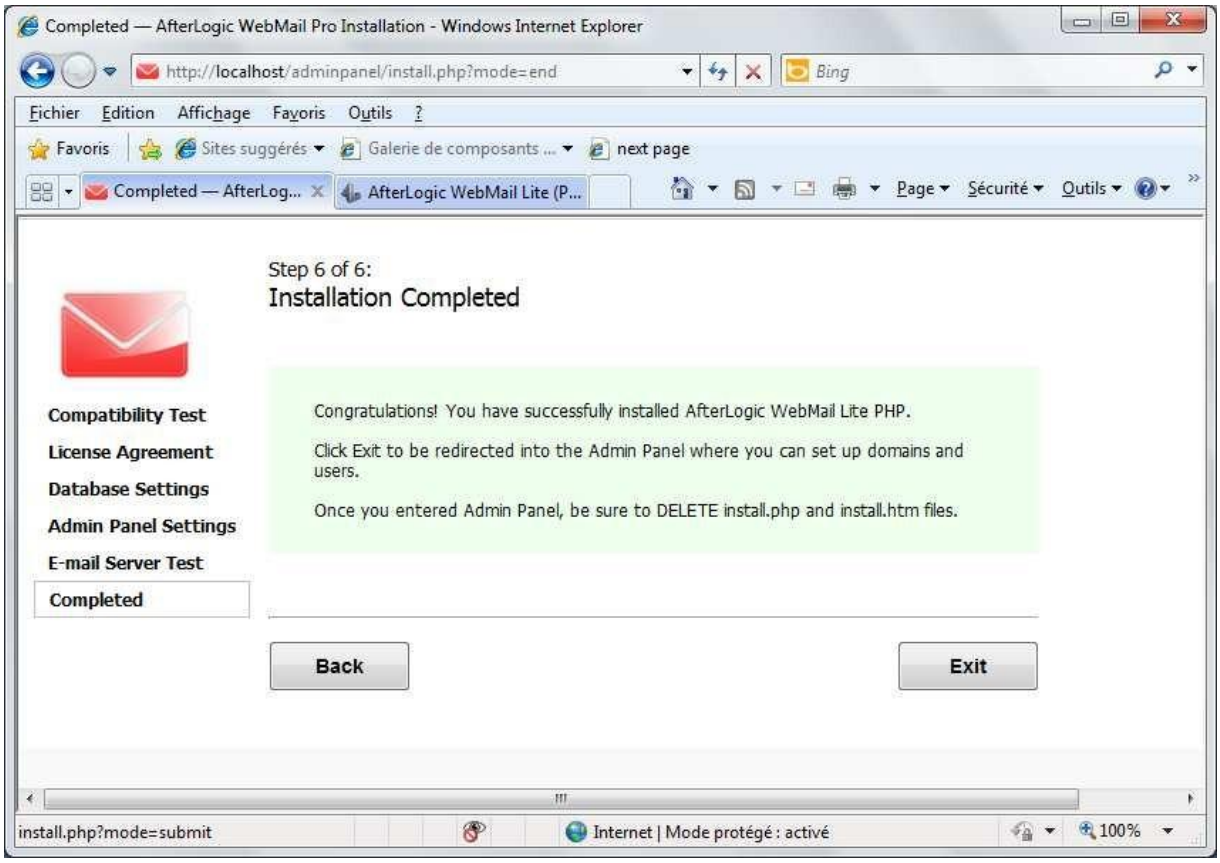
La création des tables s'est déroulée normalement, à présent vous devez définir le mot de passe de l'administrateur Webmail :

Username : mailadm

Password : *******



Précisez le nom ou l'adresse IP de votre serveur (127.0.0.1) et effectuez un test pour vous assurer que la communication POP3, SMTP et IMAP4 est opérationnelle.



L'installation est à présent terminée. Supprimer ou renommer les fichiers install.* pour éviter de relancer accidentellement l'assistant de configuration.

Connectez-vous à http://localhost/adminpanel
Je vous laisse découvrir les options de configuration de l'interface webm

Installation Serveur eBrigade

Lancement de l'installation d'Alpine :

Une fois que vous avez démarré sur l'image ISO d'Alpine Linux, tapez la commande suivante pour démarrer l'installation : **setup-alpine**

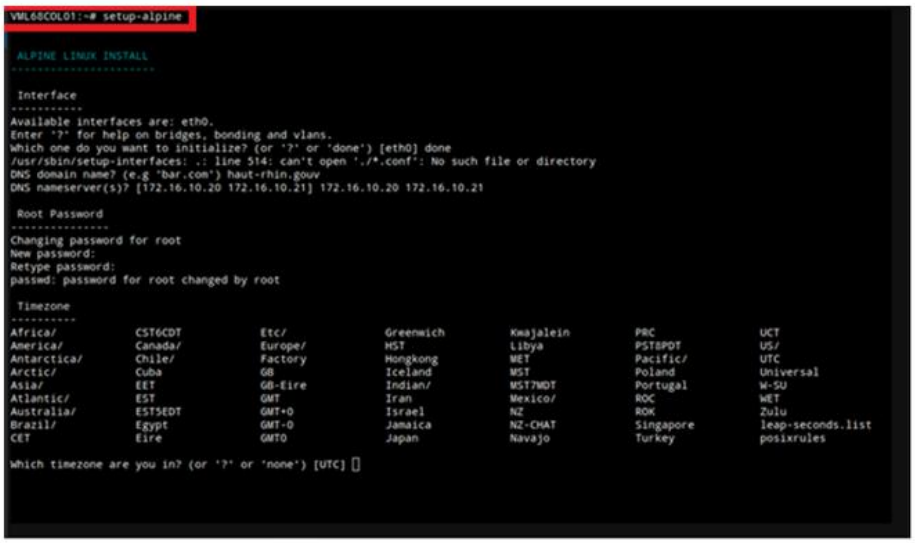
Cela lance le script interactif de configuration de base.

Choix de l'interface réseau :
Alpine vous demande de choisir l'interface réseau à configurer. Ici, eth0 est utilisée par défaut. Tapez simplement son nom si elle ne s'affiche pas automatiquement, ou appuyez sur Entrée.

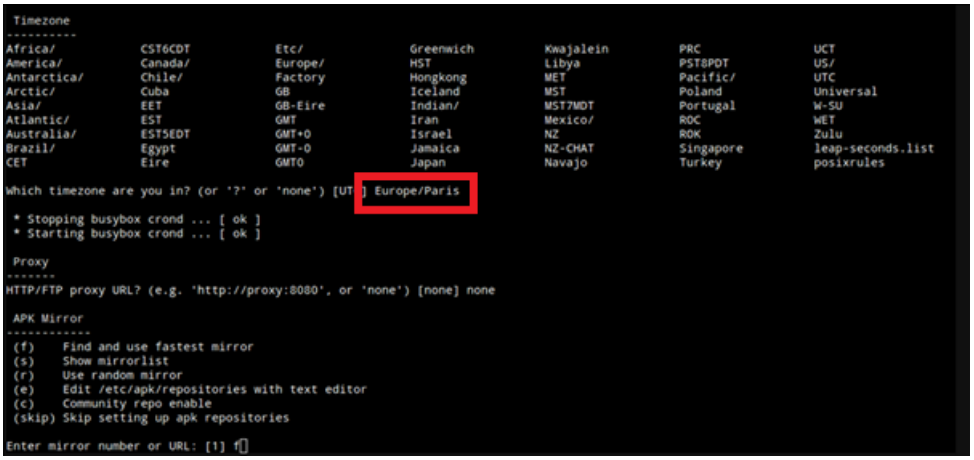
Nom d'hôte :
Vous pouvez définir un nom d'hôte pour votre machine. Dans cet exemple, le nom d'hôte VUL600CL001 a été utilisé.

Configuration DNS :
Entrez les adresses IP des serveurs DNS (séparées par des espaces si vous en mettez plusieurs). Ici, on a : 172.16.10.20 172.16.10.21.

Mot de passe root :
L'installateur vous demandera ensuite de définir un mot de passe pour l'utilisateur root. Tapez-le une première fois, puis une seconde fois pour confirmation.



Configuration du fuseau horaire (timezone) :
Enfin, vous devez spécifier votre fuseau horaire, ici **Europe/Paris**



Création de l'utilisateur ebrigade et configuration du SSH :

Après avoir mis à jour les index des dépôts, Alpine vous propose de configurer un utilisateur non-root.

Création de l'utilisateur ebrigade :
À la question « *Setup a user?* », entrez ebrigade pour créer un utilisateur avec ce nom.
Il vous sera ensuite demandé :

- Le nom complet (vous pouvez laisser la valeur par défaut : ebrigade).
- Un mot de passe pour cet utilisateur, à saisir deux fois.

Clé SSH ou URL :
Si vous avez une clé SSH publique à associer à l'utilisateur, vous pouvez la renseigner ici. Sinon, tapez none.
Choix du serveur SSH :
Alpine vous demande quel serveur SSH installer. Choisissez openssh (par défaut) en appuyant sur Entrée.
Cela va automatiquement :
-Ajouter le service sshd au démarrage,
-Générer les clés hôtes nécessaires (RSA, ECDSA, ED25519),
-Démarrer le service sshd.

Une fois terminé, vous revenez à l'invite de commande, prêt à continuer la configuration ou à vous connecter à distance en SSH avec l'utilisateur ebrigade

```
Updating repository indexes... done.

 User
------
Setup a user? (enter a lower-case loginname, or 'no') [no] ebrigade
Full name for user ebrigade [ebrigade]
Changing password for ebrigade
New password:
Retype password:
passwd: password for ebrigade changed by root
Enter ssh key or URL for ebrigade (or 'none') [none]
OK: 9 MiB in 29 packages
Which ssh server? ('openssh', 'dropbear' or 'none') [openssh]
 * service sshd added to runlevel default
 * Caching service dependencies ... [ ok ]
ssh-keygen: generating new host keys: RSA ECDSA ED25519
 * Starting sshd ... [ ok ]
VML68COL01:~#
```

Installation de sudo et configuration :

Une fois l'utilisateur créé et la configuration SSH terminée, vous pouvez installer le paquet sudo pour permettre à l'utilisateur non-root d'exécuter des commandes avec des privilèges élevés.

Installation de sudo :

Pour installer le paquet sudo, utilisez la commande suivante :

apk add sudo

Cela va télécharger et installer sudo sur votre machine.

Configuration de sudo :

Après l'installation, vous devez configurer sudo pour l'utilisateur ebrigade. Pour ce faire, ouvrez le fichier de configuration sudoers en utilisant visudo :

visudo

Cela ouvrira l'éditeur de texte visudo en mode sécurisé, où vous pourrez ajouter des règles spécifiques pour l'utilisateur.

```
~ # apk add sudo
OK: 16 MiB in 41 packages
~ # visudo
```

Modification du fichier sudoers pour autoriser l'utilisateur ebrigade :

Dans le fichier ouvert avec visudo, vous allez accorder les droits sudo à votre utilisateur.

Ce que vous voyez dans le fichier :

La ligne : root ALL=(ALL:ALL) ALL indique que l'utilisateur root a tous les droits.

Plus bas, on trouve plusieurs lignes commentées (avec #) qui permettent d'accorder les droits sudo à d'autres groupes comme wheel ou sudo.

Ce que vous devez faire :

Pour accorder les privilèges sudo à l'utilisateur ebrigade, ajoutez la ligne suivante à la fin du fichier ou juste en dessous de la ligne root :

ebrigade ALL=(ALL) ALL

Cela signifie que l'utilisateur ebrigade pourra exécuter toutes les commandes en tant que superutilisateur via sudo.

Appuyez sur Ctrl+X, puis Y, puis Entrée pour enregistrer et fermer si vous utilisez l'éditeur nano, ou suivez les instructions en bas de l'éditeur si c'est vi.

```
##
## User privilege specification
##
root ALL=(ALL:ALL) ALL

## Uncomment to allow members of group wheel to execute any command
# %wheel ALL=(ALL:ALL) ALL

## Same thing without a password
# %wheel ALL=(ALL:ALL) NOPASSWD: ALL

## Uncomment to allow members of group sudo to execute any command
# %sudo ALL=(ALL:ALL) ALL

## Uncomment to allow any user to run sudo if they know the password
## of the user they are running the command as (root by default).
Defaults targetpw  # Ask for the password of the target user
ALL ALL=(ALL:ALL) ALL  # WARNING: only use this together with 'Defaults targetpw'

## Read drop-in files from /etc/sudoers.d
@includedir /etc/sudoers.d
```

Passage à l'utilisateur ebrigade et installation de sshfs :

Maintenant que l'utilisateur ebrigade est prêt et que sudo fonctionne, on peut passer à l'étape suivante : préparer l'environnement de travail.

Se connecter en tant qu'utilisateur ebrigade :

su ebrigade

Cela vous connecte à l'utilisateur ebrigade depuis le compte root.

Créer un dossier de travail : Par convention, on crée un dossier source dans le home directory pour y mettre les futurs fichiers montés ou clonés :

mkdir source

Installer sshfs : sshfs permet de monter un système de fichiers distant via SSH, pratique pour accéder à des fichiers sur un autre serveur. Utilisez la commande suivante :

sudo apk add sshfs

Cela installera également les dépendances nécessaires comme fuse3, glib, libmount, etc.

Entrée du mot de passe sudo : Comme sudo est utilisé, vous serez invité à entrer le mot de passe de l'utilisateur ebrigade.

```
~ # su ebrigade
/root $ cd ~
~ $ mkdir source
~ $ sudo apk add sshfs
[sudo] password for root:
(1/12) Installing fuse-common (3.16.2-r1)
(2/12) Installing fuse-openrc (3.16.2-r1)
(3/12) Installing fuse3-libs (3.16.2-r1)
(4/12) Installing fuse3 (3.16.2-r1)
(5/12) Installing libffi (3.4.7-r0)
(6/12) Installing libintl (0.22.5-r0)
(7/12) Installing libeconf (0.6.3-r0)
(8/12) Installing libblkid (2.40.4-r0)
(9/12) Installing libmount (2.40.4-r0)
(10/12) Installing pcre2 (10.43-r0)
(11/12) Installing glib (2.82.5-r0)
(12/12) Installing sshfs (3.7.3-r1)
Executing busybox-1.37.0-r9.trigger
Executing glib-2.82.5-r0.trigger
OK: 23 MiB in 53 packages
~ $
```

Connexion à la machine Alpine via SSHFS-Win Manager :

Pour accéder facilement au système de fichiers de la machine Alpine depuis un poste Windows, on peut utiliser **SSHFS-Win Manager**, une interface graphique pour monter des répertoires distants via SSH.

Configuration de la connexion :

Nom de la connexion (NAME) :
Donnez un nom à votre connexion pour l'identifier facilement, par exemple VML68C0L01.

Adresse IP / Hôte (IP/HOST) :
Entrez l'adresse IP de votre machine Alpine (dans cet exemple, 172.16.15.20).

Port :
Par défaut, le port SSH est 22. Ne changez rien sauf si vous utilisez un port personnalisé.

Utilisateur (USER) :
Saisissez ebrigade, l'utilisateur créé précédemment.

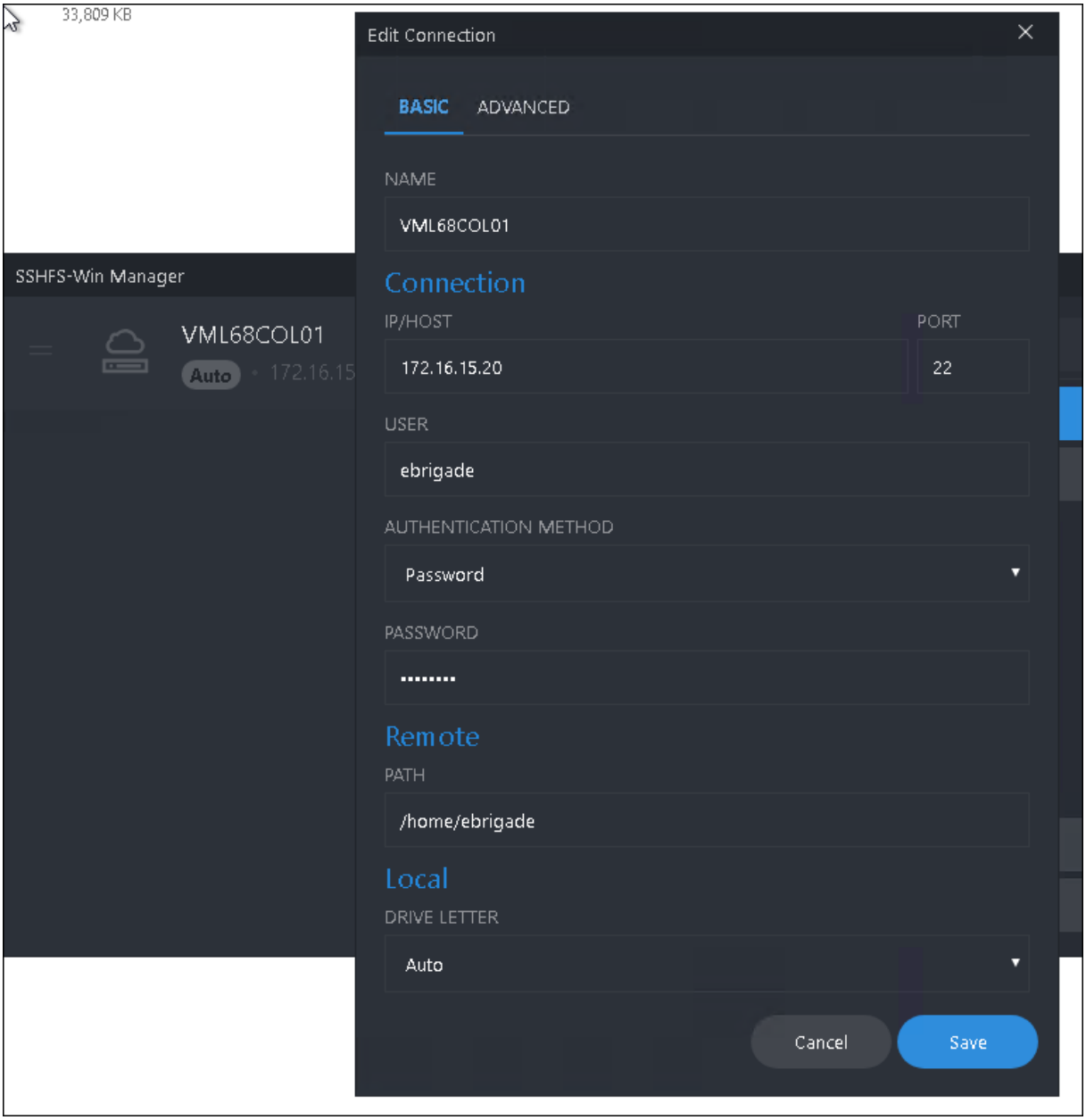
Méthode d'authentification :
Choisissez Password pour une connexion simple avec mot de passe.

Mot de passe :
Entrez le mot de passe associé à l'utilisateur ebrigade.

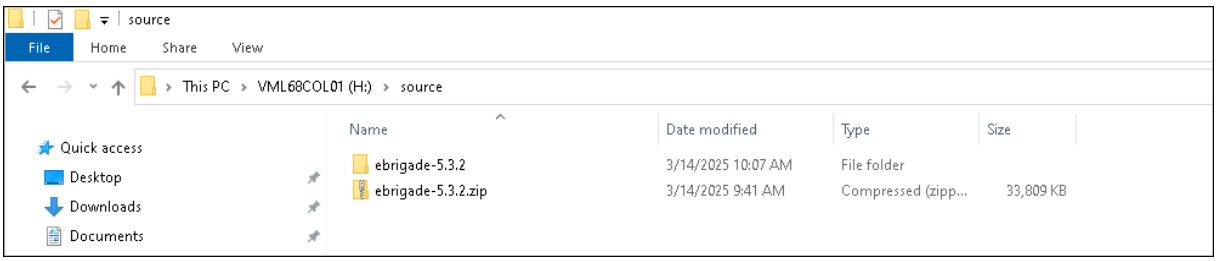
Chemin distant (Remote PATH) :
Spécifiez le chemin à monter, ici : /home/ebrigade.

Lettre du lecteur (Drive Letter) :
Laissez sur Auto ou choisissez une lettre de lecteur disponible si vous voulez accéder au montage comme à une clé USB.

Cliquez ensuite sur **Save** pour enregistrer la configuration.



Il va falloir ensuite sélectionner le dossier .zip



Copie des fichiers eBrigade vers le répertoire web :

On copie dans le dossier utilisé par le serveur web local pour les rendre accessibles via un navigateur. Pour cela, on utilise la commande suivante :
sudo cp source/ebrigade-5.3.2/* /var/www/localhost/htdocs -r
Cette commande copie tout le contenu du dossier ebrigade-5.3.2 vers /var/www/localhost/htdocs, qui est le répertoire par défaut pour les fichiers web. L'option -r permet de copier récursivement tous les sous-dossiers.
Après cette étape, les fichiers de l'application eBrigade sont en place pour être servis par le serveur web.

```
$ sudo cp source/ebrigade-5.3.2/* /var/www/localhost/htdocs -r
```

Installation du serveur web Apache2 :

Pour que les fichiers de l'application eBrigade soient accessibles via un navigateur, il faut installer un serveur web. Ici, on utilise **Apache2**, un serveur HTTP léger et compatible avec Alpine Linux.
Exécutez la commande suivante :
sudo apk add apache2

```
/var/www/localhost $ sudo apk add apache2
OK: 256 MiB in 89 packages
/var/www/localhost $
```

Ajout des dépôts main et community pour Alpine v3.14 :

Pour s'assurer que tous les paquets nécessaires (y compris certains comme PHP, modules Apache, etc.) soient disponibles, il est important que les dépôts **main** et **community** soient bien configurés.
La commande suivante vérifie si les lignes sont présentes dans /etc/apk/repositories, et les ajoute si ce n'est pas le cas :
sudo sh -c 'grep -q "v3.14/main" /etc/apk/repositories || echo "http://dl-cdn.alpinelinux.org/alpine/v3.14/main" >> /etc/apk/repositories && grep -q "v3.14/community" /etc/apk/repositories || echo "http://dl-cdn.alpinelinux.org/alpine/v3.14/community" >> /etc/apk/repositories'

Lancement du serveur Apache2 et gestion des permissions :

Une fois Apache installé, il faut :
Donner les bons droits au répertoire de configuration (si nécessaire)
Avant de démarrer Apache2, il est parfois nécessaire de corriger les droits d'accès pour éviter des erreurs de permission, notamment sur certains fichiers de configuration de l'application eBrigade.
sudo chown -R apache:apache /var/www/localhost/htdocs/conf/
sudo chmod -R 775 /var/www/localhost/htdocs/conf/
Démarrer Apache2
sudo rc-service apache2 start

Cela lance immédiatement le serveur Apache. Le message [ok] confirme que le service a démarré sans erreur.

Activer Apache2 au démarrage

sudo rc-update add apache2

Cette commande ajoute Apache2 au niveau de run par défaut, ce qui signifie qu'il sera automatiquement lancé à chaque démarrage de la machine.

À partir de maintenant, l'application eBrigade est servie par Apache2 et accessible via un navigateur à l'adresse :

http://[IP_de_la_machine]

```
/var/www/localhost $ sudo sh -c 'grep -q "v3.14/main" /etc/apk/repositories || echo "http://dl-cdn.alpinelinux.org/alpine/v3.14/main"
>> /etc/apk/repositories && grep -q "v3.14/community" /etc/apk/repositories || echo "http://dl-cdn.alpinelinux.org/alpine/v3.14/commun
ity" >> /etc/apk/repositories'
```

```
/var/www/localhost/htdocs $ sudo chown -R apache:apache /var/www/localhost/htdocs/conf/
/var/www/localhost/htdocs $ sudo chmod -R 775 /var/www/localhost/htdocs/conf/
```

```
/var/www/localhost/htdocs $ sudo rc-service apache2 start
[sudo] password for root:
 * Caching service dependencies ... [ ok ]
 * Starting apache2 ... [ ok ]
/var/www/localhost/htdocs $ sudo rc-update add apache2
 * service apache2 added to runlevel default
/var/www/localhost/htdocs $
```

Installation du serveur de base de données MariaDB :

L'application eBrigade nécessite une base de données pour fonctionner. Alpine Linux propose MariaDB, une alternative libre à MySQL, totalement compatible.

Pour l'installer, utilisez la commande suivante :

sudo apk add mariadb mariadb-client

```
/var/www/localhost/htdocs $ sudo apk add mariadb mariadb-client
[sudo] password for root:
(1/18) Installing mariadb-common (11.4.5-r0)
(2/18) Installing libaio (0.3.113-r2)
(3/18) Installing brotli-libs (1.1.0-r2)
(4/18) Installing c-ares (1.34.3-r0)
(5/18) Installing libunistring (1.2-r0)
(6/18) Installing libidn2 (2.3.7-r0)
(7/18) Installing nghttp2-libs (1.64.0-r0)
(8/18) Installing libpsl (0.21.5-r3)
(9/18) Installing zstd-libs (1.5.6-r2)
(10/18) Installing libcurl (8.12.1-r0)
(11/18) Installing libgcc (14.2.0-r4)
(12/18) Installing skalibs-libs (2.14.3.0-r0)
(13/18) Installing utmps-libs (0.1.2.3-r2)
(14/18) Installing linux-pam (1.6.1-r1)
(15/18) Installing libstdc++ (14.2.0-r4)
(16/18) Installing mariadb (11.4.5-r0)
Executing mariadb-11.4.5-r0.pre-install
(17/18) Installing mariadb-openrc (11.4.5-r0)
(18/18) Installing mariadb-client (11.4.5-r0)
Executing busybox-1.37.0-r9.trigger
OK: 248 MiB in 82 packages
/var/www/localhost/htdocs $
```

Initialisation de MariaDB :

Une fois MariaDB installé, il faut l'initialiser pour créer les fichiers de base et préparer le système à accueillir les bases de données.

Utilisez la commande suivante :

sudo /etc/init.d/mariadb setup

```
/var/www/localhost/htdocs $ sudo /etc/init.d/mariadb setup
 * Creating a new MySQL database .../usr/bin/mysql_install_db: Deprecated program name. It will be removed in a future release, use 'm
ariadb-install-db' instead
Installing MariaDB/MySQL system tables in '/var/lib/mysql' ...
OK

To start mariadbd at boot time you have to copy
support-files/mariadb.service to the right place for your system


Two all-privilege accounts were created.
One is root@localhost, it has no password, but you need to
be system 'root' user to connect. Use, for example, sudo mysql
The second is mysql@localhost, it has no password either, but
you need to be the system 'mysql' user to connect.
After connecting you can set the password, if you would need to be
able to connect as any of these users with a password and without sudo

See the MariaDB Knowledgebase at https://mariadb.com/kb

You can start the MariaDB daemon with:
cd '/usr' ; /usr/bin/mariadbd-safe --datadir='/var/lib/mysql'

You can test the MariaDB daemon with mariadb-test-run.pl
cd '/usr/mariadb-test' ; perl mariadb-test-run.pl

Please report any problems at https://mariadb.org/jira

The latest information about MariaDB is available at https://mariadb.org/.

Consider joining MariaDB's strong and vibrant community:
https://mariadb.org/get-involved/

 [ ok ]
/var/www/localhost/htdocs $
```

Maintenant que MariaDB est initialisé, on peut démarrer le service avec la commande suivante :
sudo rc-service mariadb start

```
/var/www/localhost/htdocs $ sudo rc-service mariadb start
 * Starting mariadb .../usr/bin/mysqld_safe: Deprecated program name. It will be removed in a future release, use 'mariadbd-safe' inst
ead
250314 11:52:13 mysqld_safe Logging to syslog.
250314 11:52:13 mysqld_safe Starting mariadbd daemon with databases from /var/lib/mysql
 [ ok ]
/var/www/localhost/htdocs $
```

Après avoir démarré MariaDB, il est fortement recommandé d'exécuter le script de sécurisation intégré pour protéger l'accès à la base de données.
Lancez :
sudo mysql_secure_installation

```
/var/www/localhost/htdocs $ sudo mysql_secure_installation
/usr/bin/mysql_secure_installation: Deprecated program name. It will be removed in a future release, use 'mariadb-secure-installation'
 instead

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
 ... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n]
```

```
By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n]
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] n
 ... skipping.

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n]
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
/var/www/localhost/htdocs $
```

Activer MariaDB au démarrage

Afin que le service MariaDB se lance automatiquement à chaque démarrage de la machine, il faut l'ajouter au niveau de run par défaut avec la commande suivante :

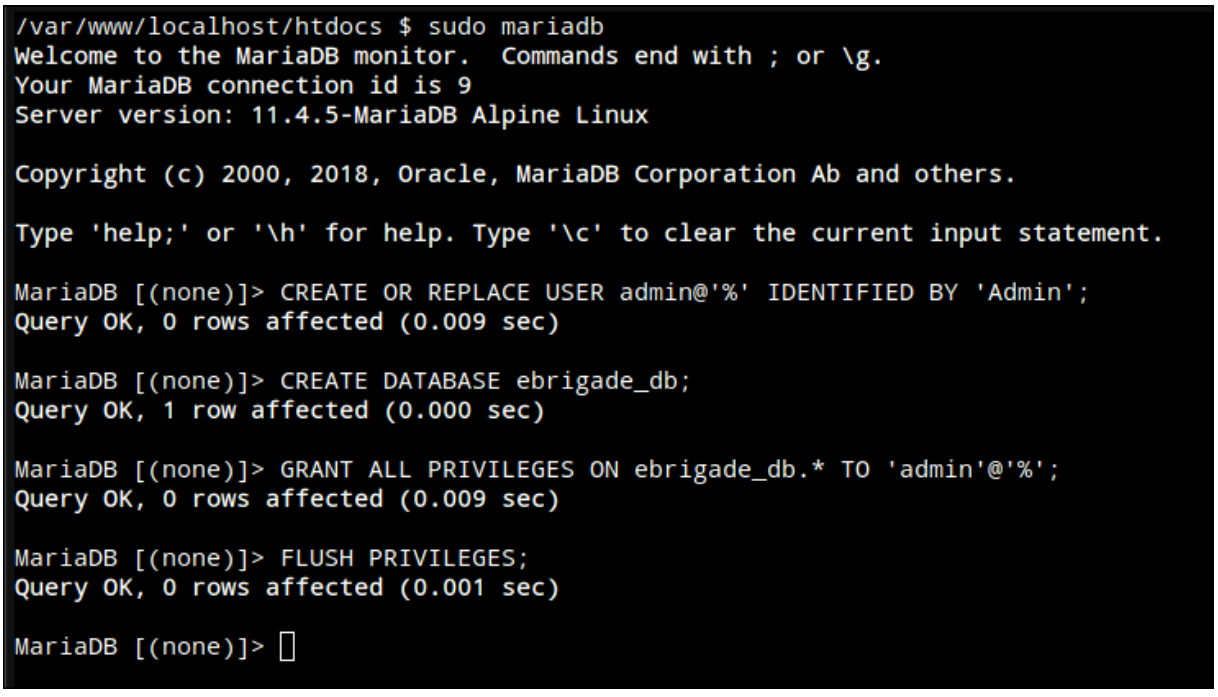
sudo rc-update add mariadb default

Une fois cette commande exécutée, MariaDB sera lancé automatiquement à chaque démarrage du système.

```
/var/www/localhost/htdocs $ sudo rc-update add mariadb default
 * service mariadb added to runlevel default
/var/www/localhost/htdocs $
```

Création de la base de données et d'un utilisateur pour eBrigade

Lancez le client MariaDB en mode administrateur :
sudo mariadb
Une fois connecté, exécutez les commandes suivantes dans l'ordre :
Créer un utilisateur nommé admin accessible depuis n'importe quelle IP (%) avec le mot de passe Admin :
CREATE OR REPLACE USER admin@'%' IDENTIFIED BY 'Admin';
Créer la base de données ebrigade_db :
CREATE DATABASE ebrigade_db;
Donner tous les droits à l'utilisateur admin sur la base ebrigade_db :
sql
CopierModifier
GRANT ALL PRIVILEGES ON ebrigade_db.* TO 'admin'@'%';
Recharger les privilèges pour appliquer les changements immédiatement :
FLUSH PRIVILEGES;

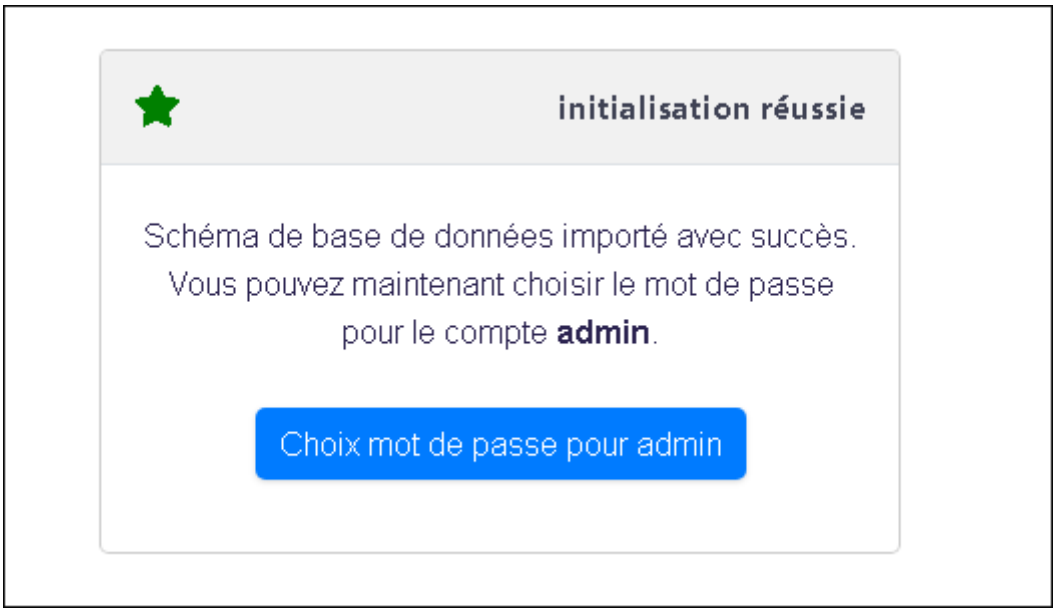


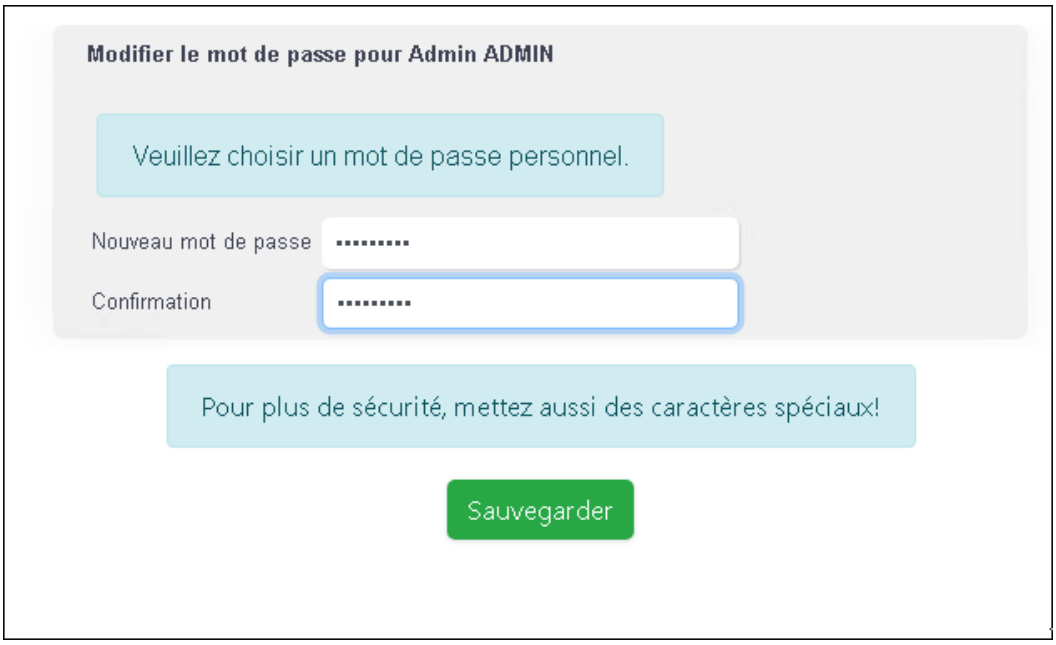
Configuration de la base de données via l'interface web

Une fois le serveur web démarré et les fichiers de l'application en place, accédez à eBrigade via un navigateur web en entrant l'adresse IP de votre machine Alpine

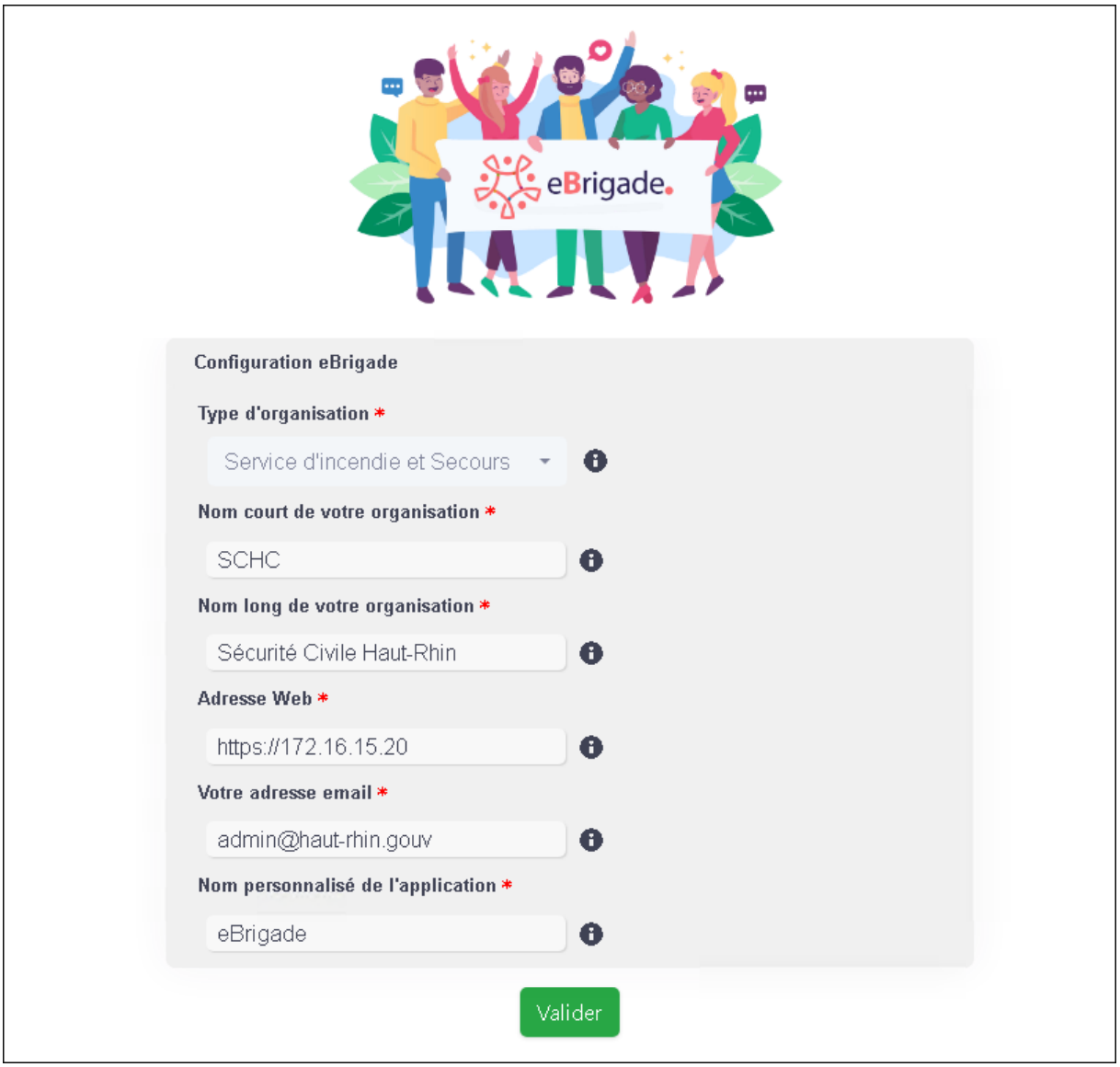
Choix du mot de passe administrateur

Une fois la base de données initialisée avec succès, eBrigade vous propose de définir un mot de passe pour le compte **admin**.
Saisissez un mot de passe sécurisé dans les deux champs puis cliquez sur **Sauvegarder**.
Ce mot de passe vous servira pour vous connecter à l'interface d'administration de l'application.

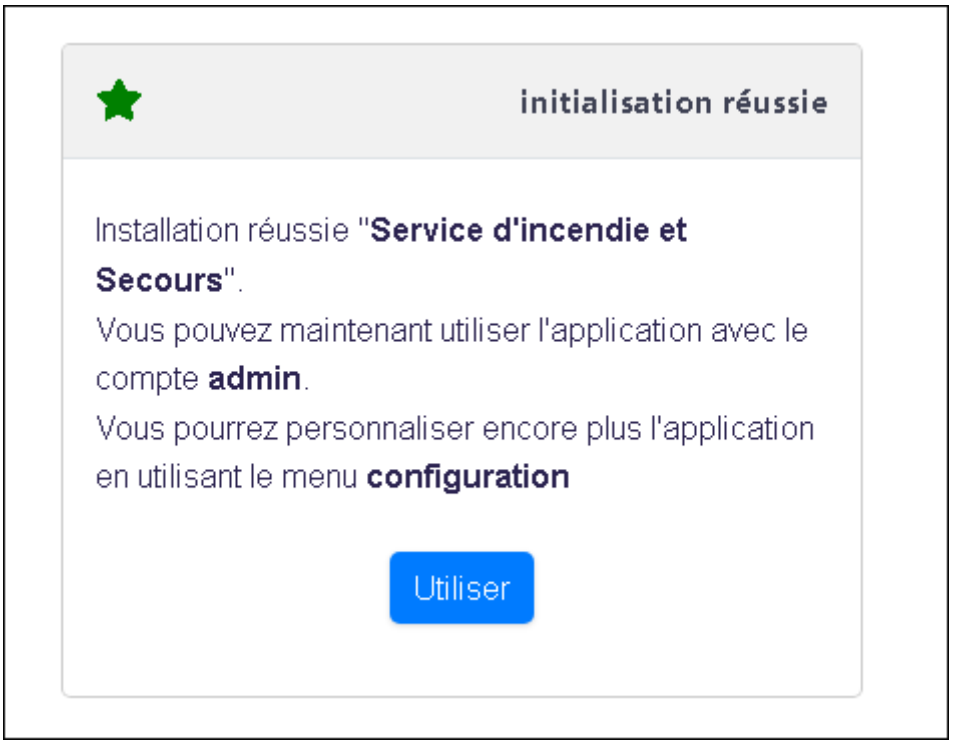




Remplissez les informations de votre organisation :



Cliquez sur **Valider** pour finaliser la configuration.
L'application eBrigade est maintenant prête à être utilisée.


initialisation réussie
Installation réussie "Service d'incendie et Secours".
Vous pouvez maintenant utiliser l'application avec le compte admin.
Vous pourrez personnaliser encore plus l'application en utilisant le menu configuration
Utiliser