BTS SIO 2025 Option SISR
Projet : DATATEL
DOCUMENTATION TECHNIQUE

Epreuve E6
-
Situation professionnelle 2

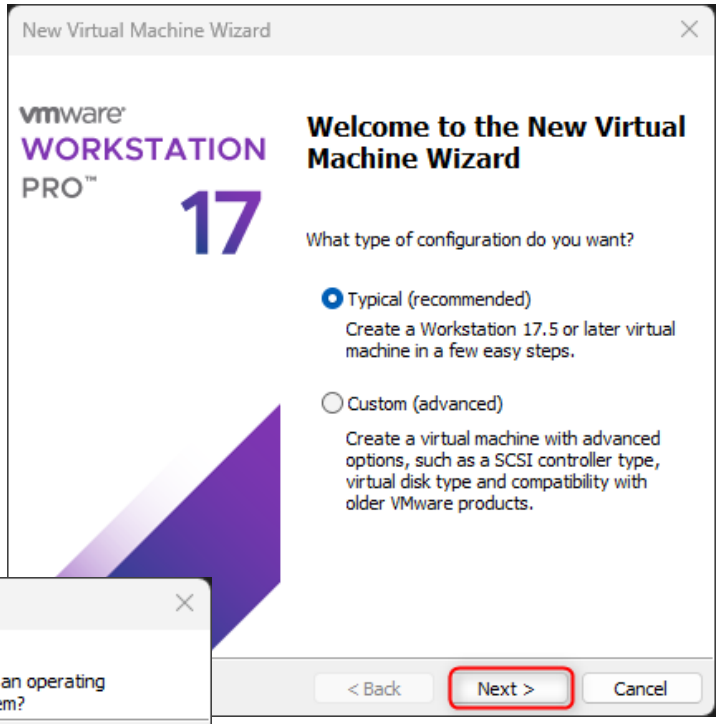
Table des matières

Création, d'une VM sur VM WARE

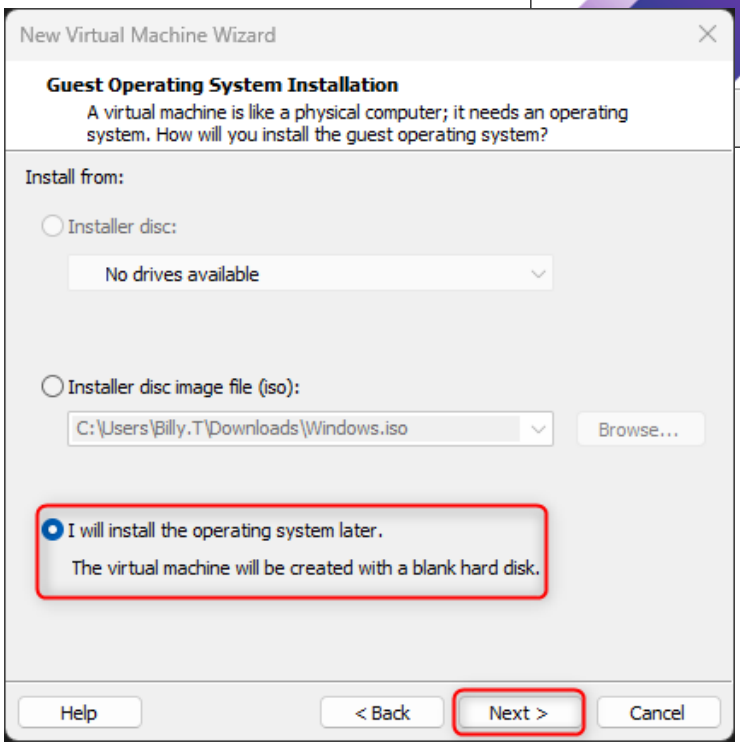
Lorsque vous créer une machine virtuelle l'option « Typical (recommended) est cocher de base.

Cliquer sur « Next » pour passer à la prochaine étape.

Cliquer sur « Next »



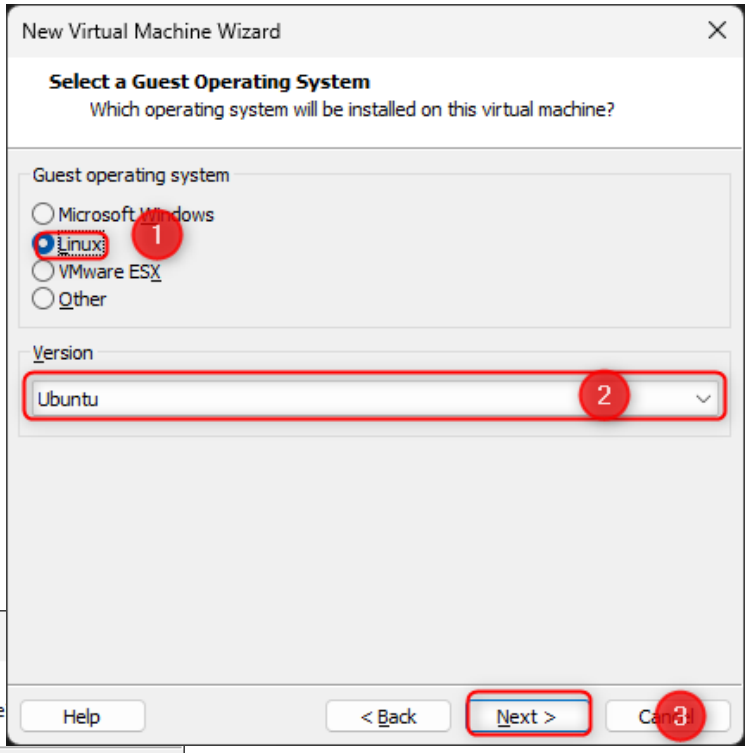
Cliquer sur « Next » pour passer à la prochaine étape



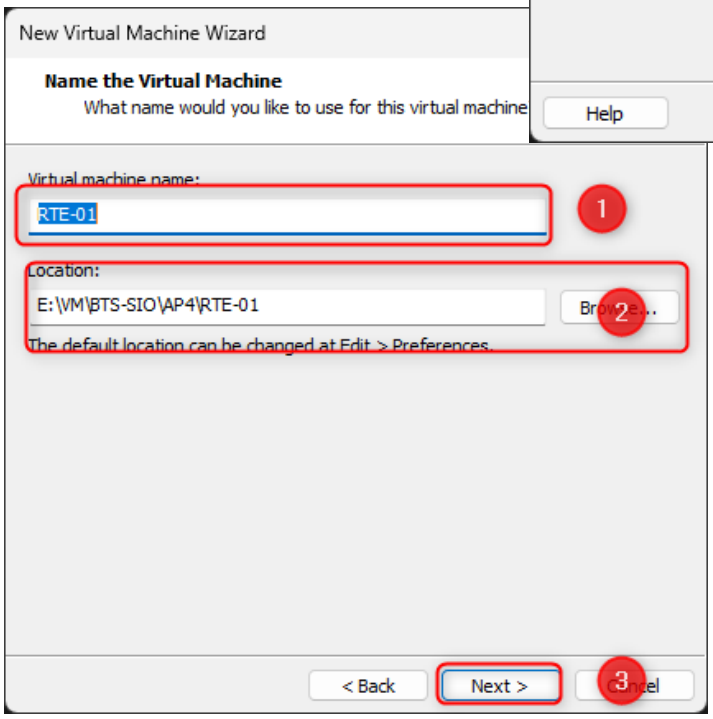
Dans notre cas à nous allons choisir « Linux » car nous auront besoin d'installer d'un pare-feu sur le serveur

Cliquer dans le menu déroulant puis sélectionner « Linux»

Cliquer sur « Next » pour passer à la prochaine étape



Dans cette étape nous allons devoir nommer le serveur ainsi que choisir l'emplacement de la VM



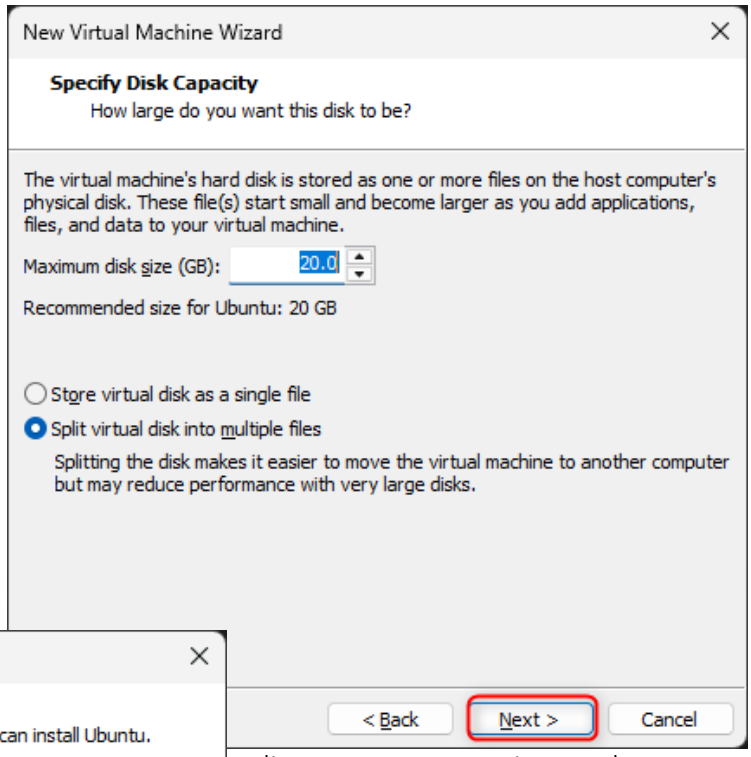
(1) Ensuite nous allons nommer le server

(2) Choisir l'emplacement ou sera situé la VM

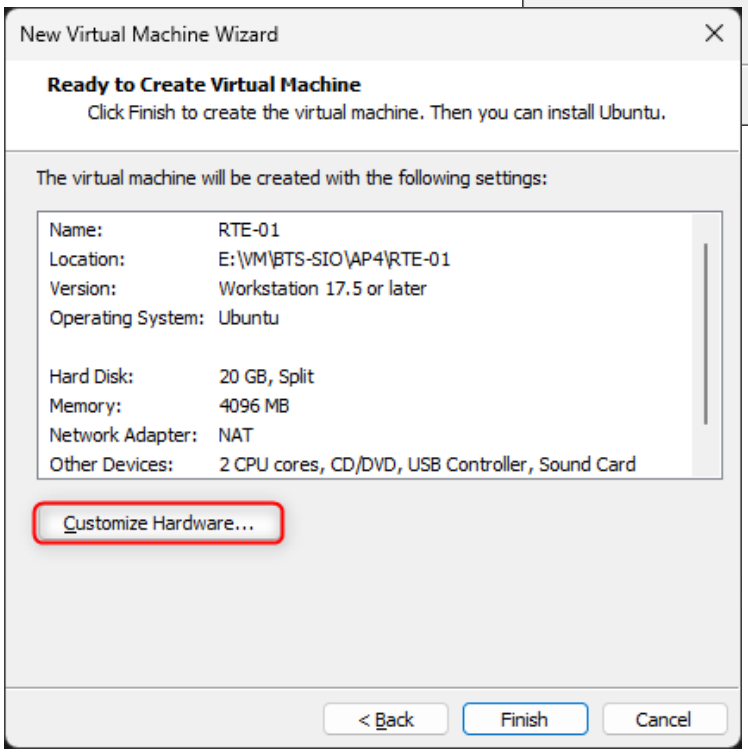
(3) Cliquer sur « Next » pour passer à la prochaine étape

Ensuite sur cette étape nous allons allouer l'espace du disque pour notre serveur. Dans notre cas il n'est pas nécessaire d'avoir un gros espace de stockage sur notre serveur.

Cliquer sur « Next » pour passer à la prochaine étape



Ensuite dans cette partie-là nous allons configurer les options suivantes :

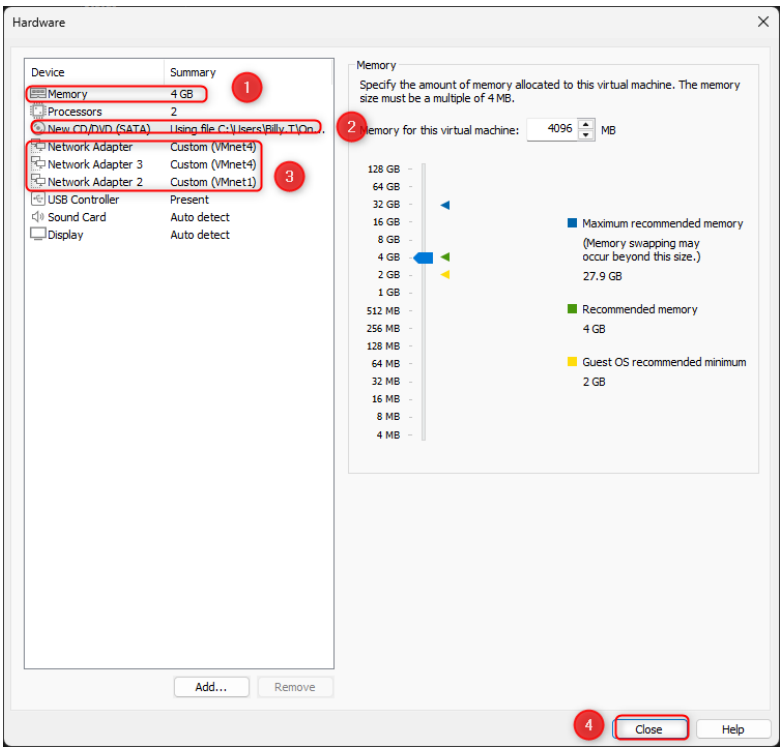


Cliquer sur « Customize Hardware »

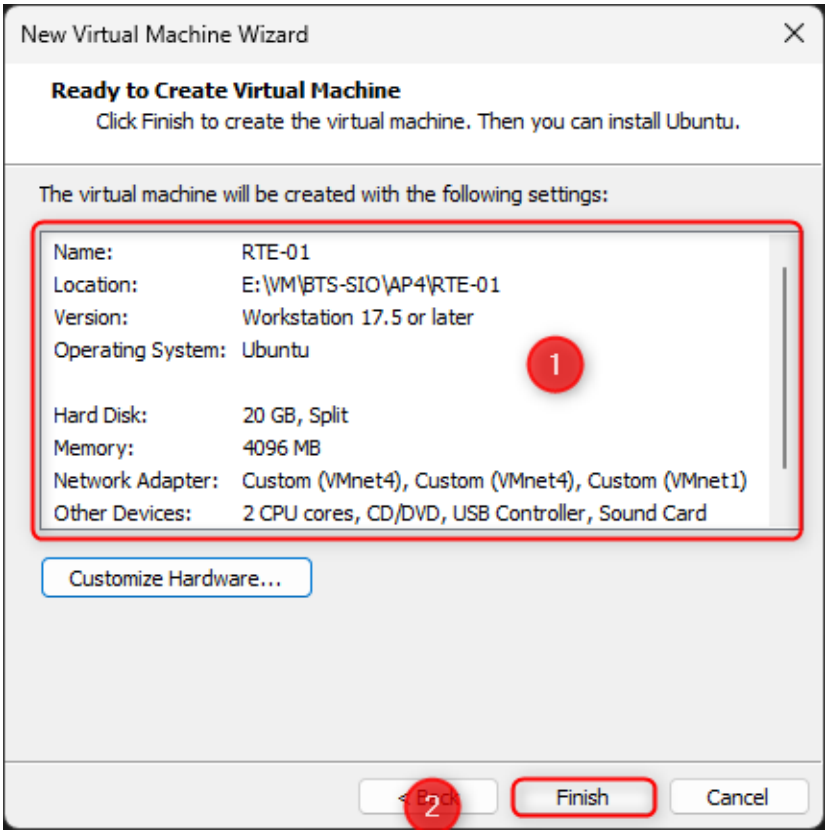
Dans cette partis nous allons paramétrer selon nos besoins :

(1) Memory = 4 GB
(2) CD/ DVD = Pfsens
(3) Network Adapter = Vmnet 4 (bridge)
Network Adapter = Vmnet 4 (bridge)

Network adapter = Vmnet 1
(4) Cliquer sur « Close » pour fermer la fenêtre

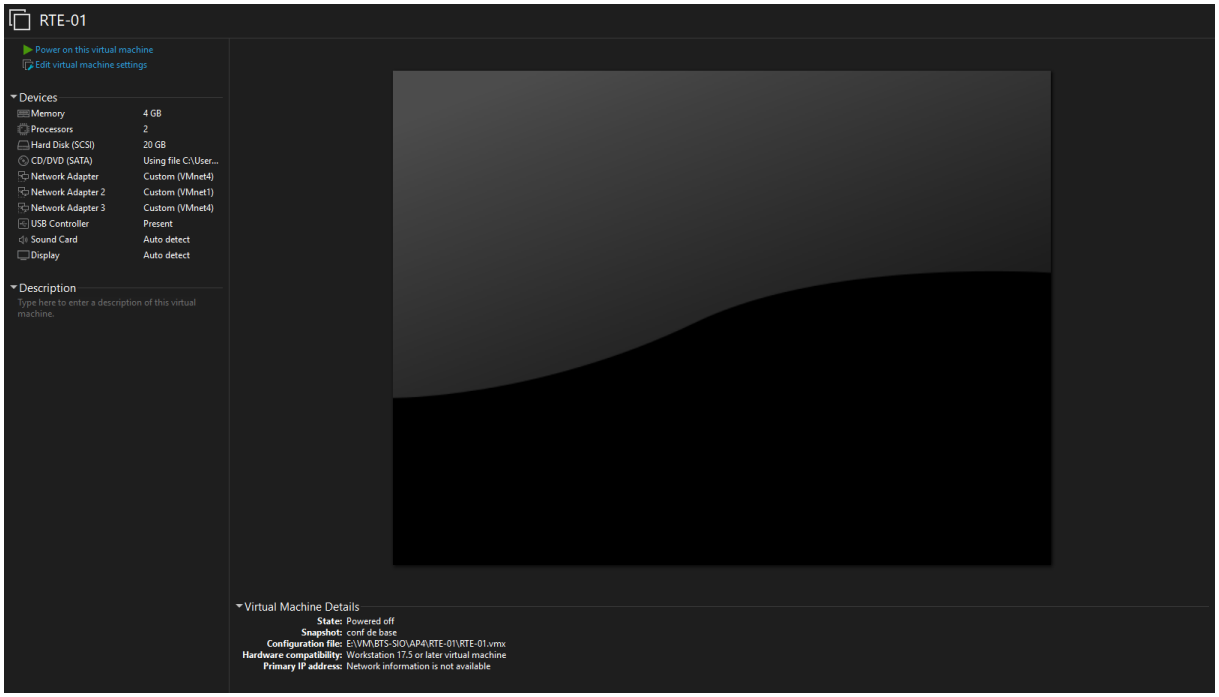


Une fois que la configuration est finit vous aller avoir ce menu-là :



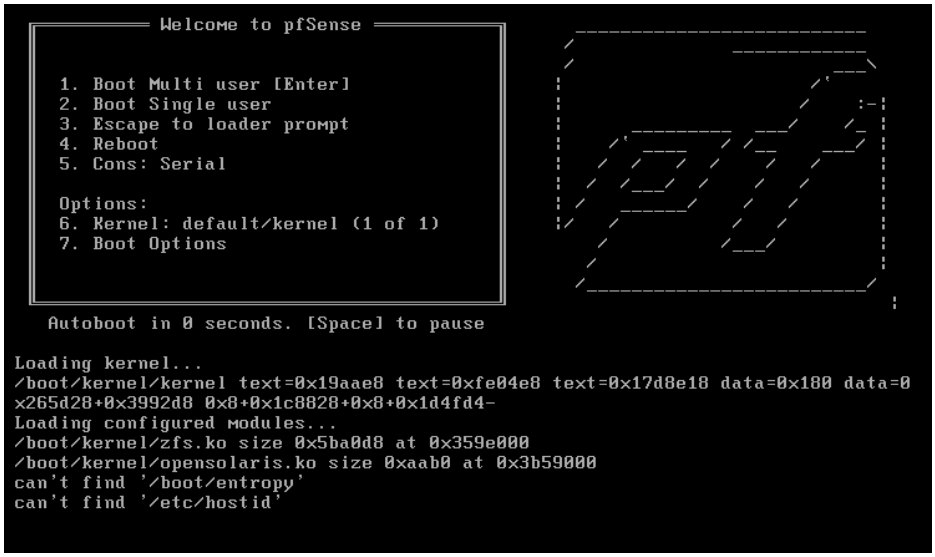
(1) Récapitulatif de la configuration du serveur.
(2) Cliquer sur « Finish » pour passer à la prochaine étape

Une fois avoir fini de vérifier les information du serveur, la VM (Virtual Machine) va se créer ainsi vous pouvez le lancer.

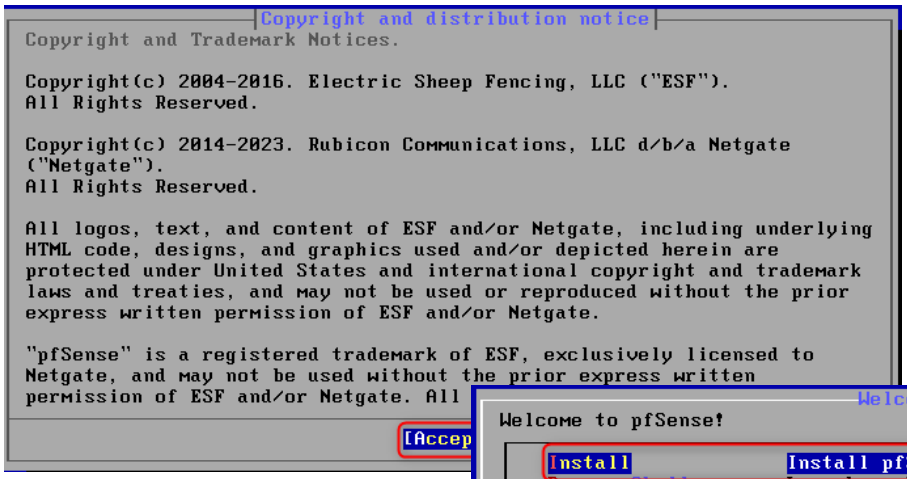

RTE-01
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 4 GB
Processors 2
Hard Disk (SCSI) 20 GB
CD/DVD (SATA) Using file C:\User...
Network Adapter Custom (VMnet4)
Network Adapter 2 Custom (VMnet1)
Network Adapter 3 Custom (VMnet4)
USB Controller Present
Sound Card Auto detect
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Snapshot: conf de base
Configuration file: E:\VM\BTS-SIO\AP4\RTE-01\RTE-01.vmx
Hardware compatibility: Workstation 17.5 or later virtual machine
Primary IP address: Network information is not available

Installation Pfsense

Lorsque la machine à démarrer vous allez avoir cette interface et donc il faudra patienter quelque seconde afin que pfsense lance l'installation.

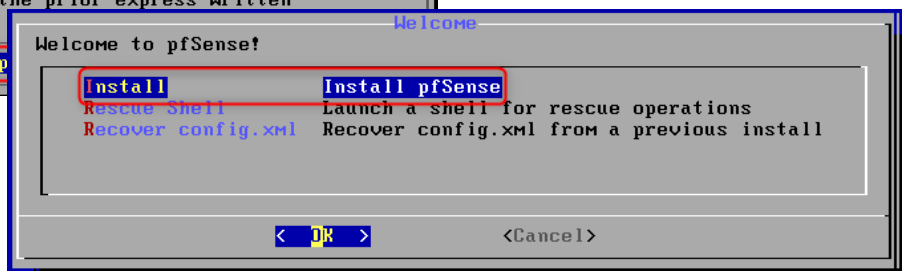


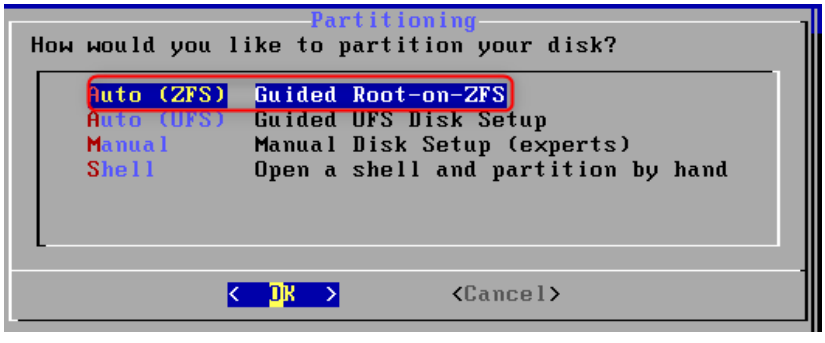
Une fois que cela est fait vous allez atterrie sur cette page avec les conditions à accepter



Sélectionner « Accept »

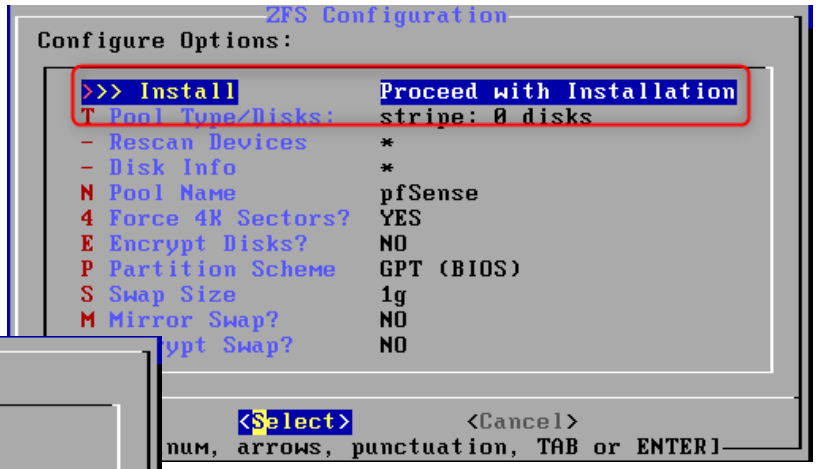
Sélectionner « Install »





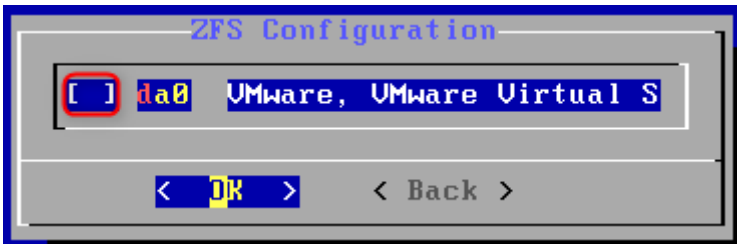
Sélectionner « Auto (ZFS)

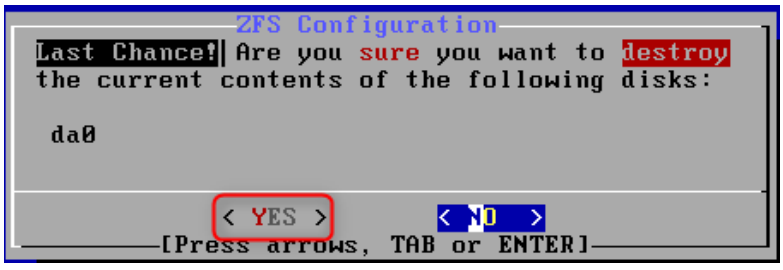
Sélectionner « Install »



Sélectionner « Stripe »

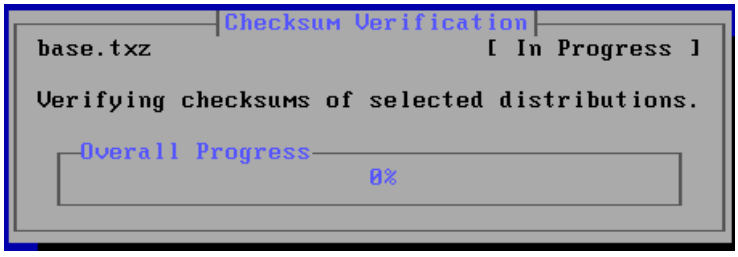
Cocher la case « da0 » pour installer l'os sur se disque

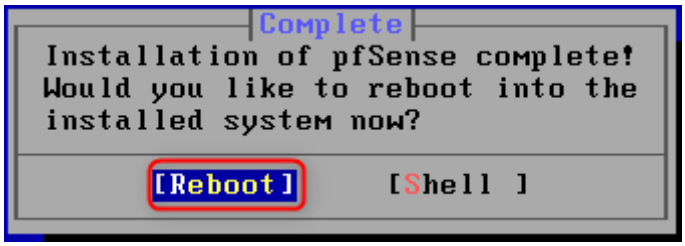




Sélectionner « Yes »

Une fois avoir répondu à Yes patienter quelque minutes afin que l'installation se finit.

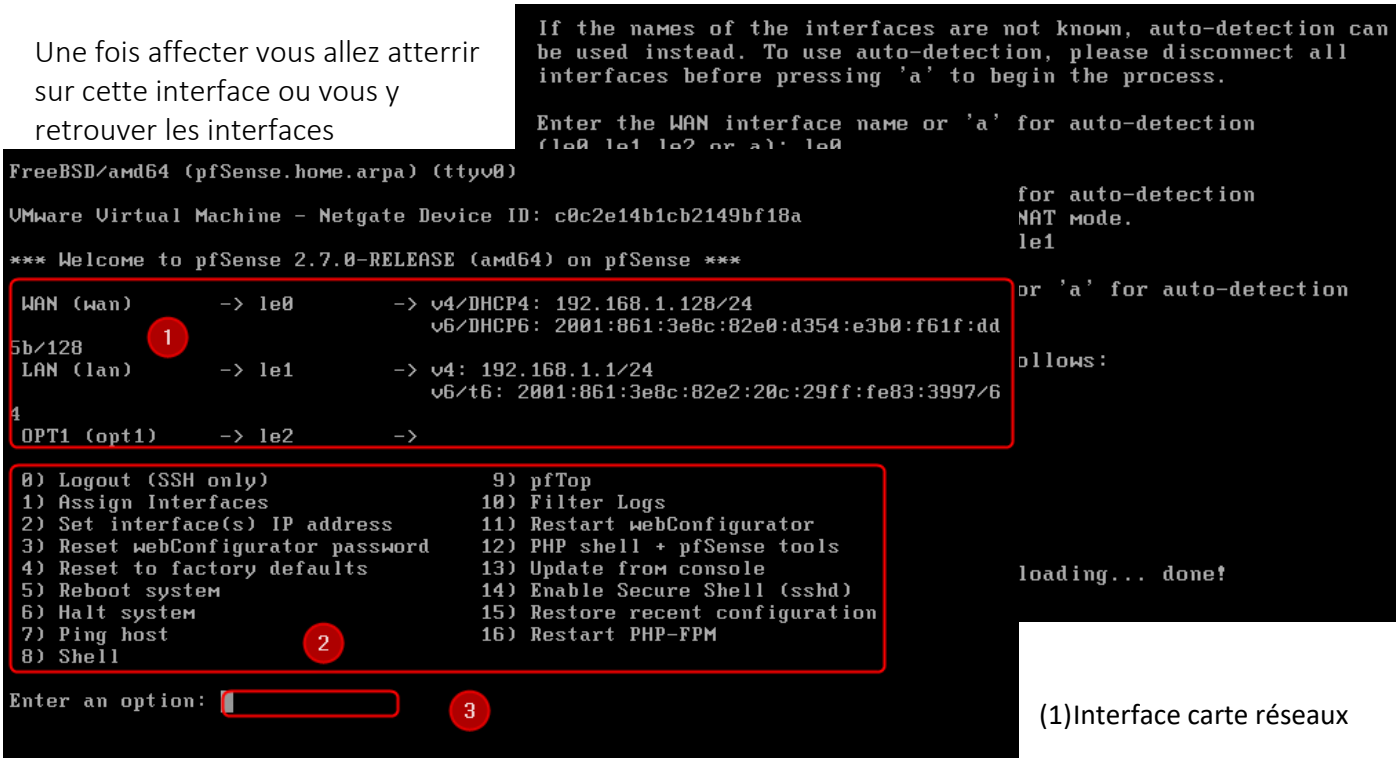




Sélectionner « Reboot »

Une fois que cela a fini de redémarrer Pfsense va detecter 3 carte réseaux et donc nous allons devoir les affecter.

Une fois affecter vous allez atterrir sur cette interface ou vous y retrouver les interfaces



(1)Interface carte réseaux

(2) Choix option

(3) Zone de choix à entrer

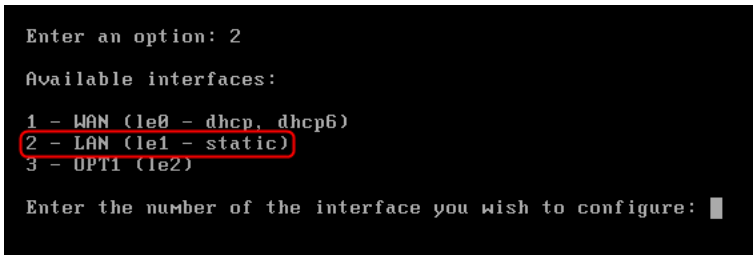
Assignation des interfaces sur pFsense

Une fois après avoir vu le menu nous allons assigner les interfaces

(1) Choisir set interface IP
(2) Renter le numéro 2 accéder à cette option

pour

Une fois sélectionner le bon choix merci vous allez devoir choisir entre le WAN,LAN ou OPT1. Pour nous cela être le choix 2 LAN



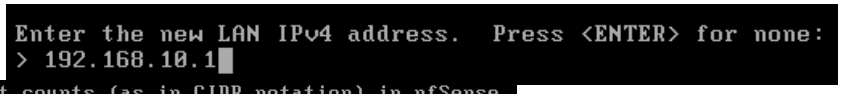
Taper le numéro 2 pour configurer le LAN

Une fois cela fait nous allons devoir répondre à plusieurs questions :

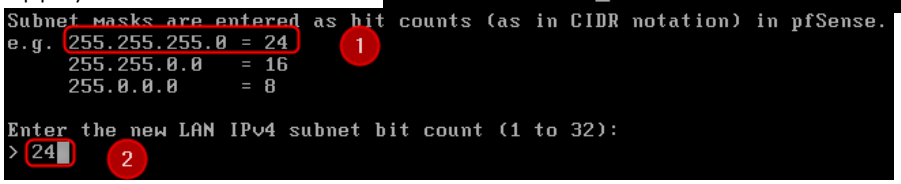
Taper n pour refuser de le configurer en DHCP

Taper l'adresse ip

Une fois après avoir taper Appuyer sur ENTRER

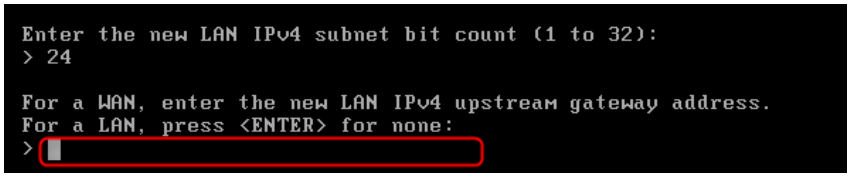


l'IP



(1) Choisir le bon mask sous réseaux
(2) Dans notre cas à nous c'est le /24

Taper juste entrer



Une fois cela pfsense demande à configurer IPV6 du LAN , dans notre cas il n'est pas nécessaire d'avoir une IPV6

Taper la lettre n

Laisser la case vite et taper entrer

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
```

```
Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
```

Taper la lettre n

Taper la lettre N

```
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Une fois après avoir finaliser la configuration du LAN Pfsense va nous donne l'IP pour se connecter à l'interface

```
The IPv4 LAN address has been set to 192.168.10.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.10.1/

Press <ENTER> to continue.
```

Ip pour se connecter à l'interface

Lorsque vous taper sur Entrer nous allons retourner sur l'interface de pfsense et donc comme vous pouvez le constaté l'IP de LAN est configurer

Comme vous pouvez le voir le LAN a bien pris son IP

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> le0        -> v4/DHCP4: 192.168.1.128/24
                                  v6/DHCP6: 2001:861:3e8c:82e0:d354:e3b0:f61f:dd
5b/128
 LAN (lan)       -> le1        -> v4: 192.168.10.1/24
 OPT1 (opt1)     -> le2        ->

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

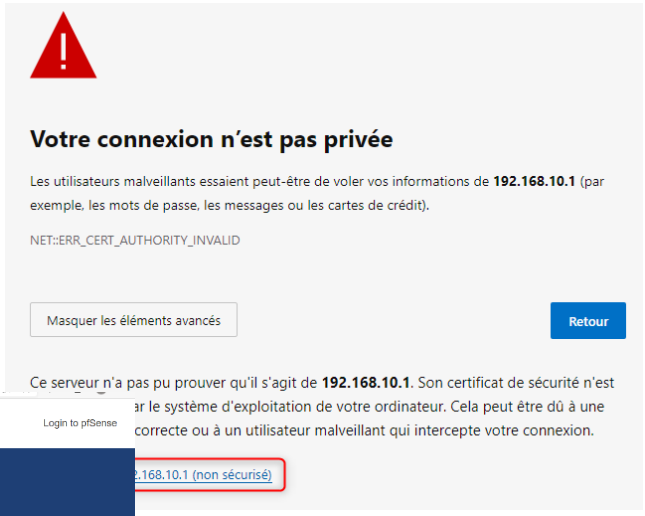
Connexion interface pfsense

Une fois après avoir bien fixer les ip nous allons nous connecter sur l'interface Pfsense en tapant l'adresse ip indiquer sur le serveur.

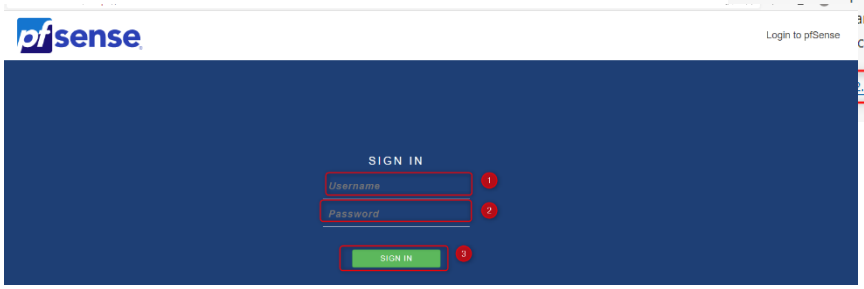
(1) Rentrer l'IP du lan qui est 192.168.10.1

(2) Cliquer sur avancer

Cliquer sur Continuer vers 192.168.10.1 (non sécurisé)



Après voir cliquer nous allons arriver sur le page de connexion de Pfsense.

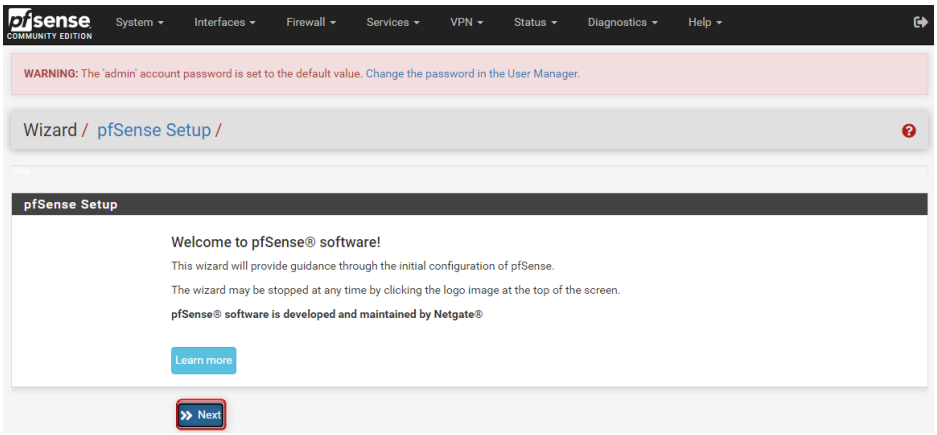


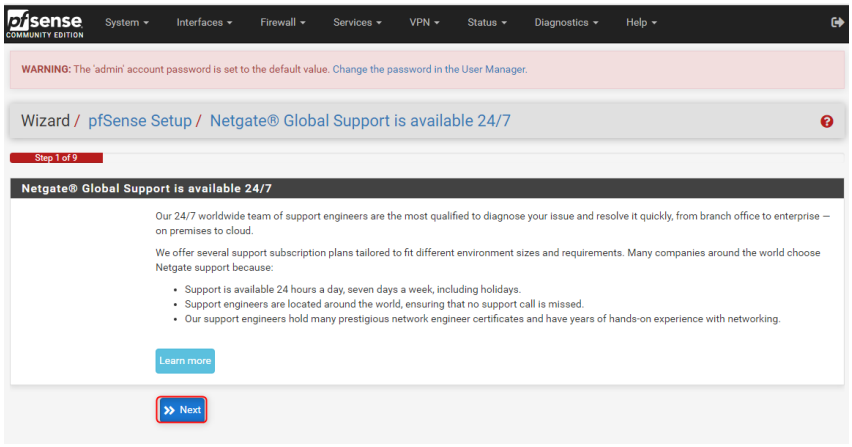
(1) Admin
(2) Pfsense
(3) Cliquer sur Signe IN pour se connecter

Configuration depuis l'interface Web pfsense

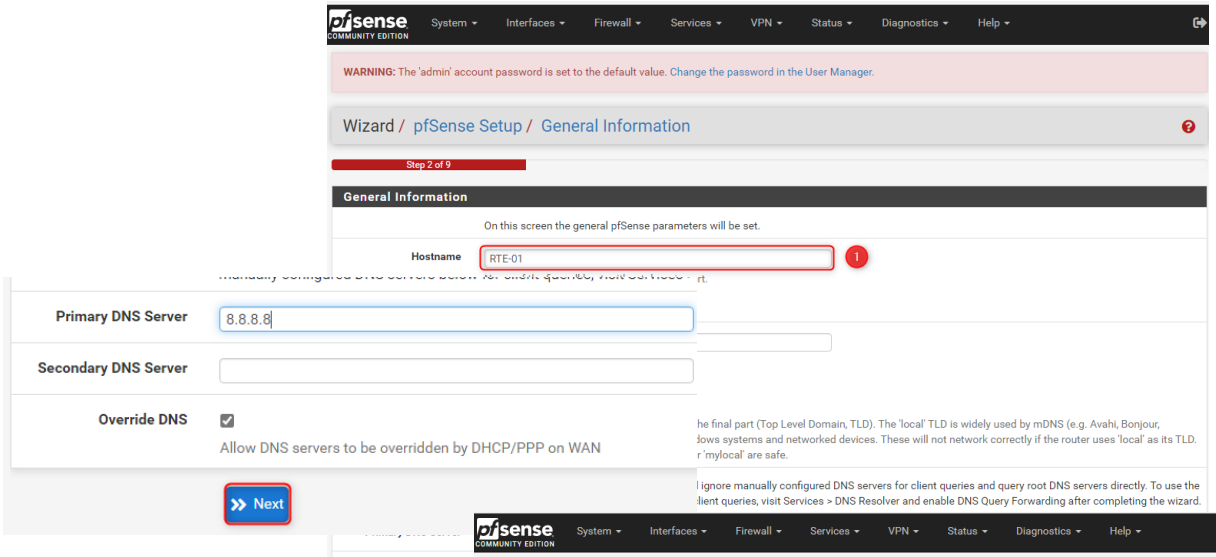
Une fois après être connecter sur l'interface de Pfsense vous allez être sur cette page.

Cliquer sur Next



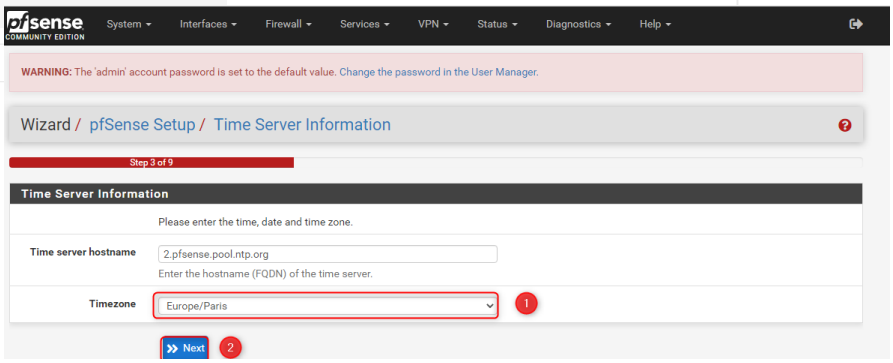


(1) Mettre le nom du routeur RTE-01
(2) Mettre le DNS de google

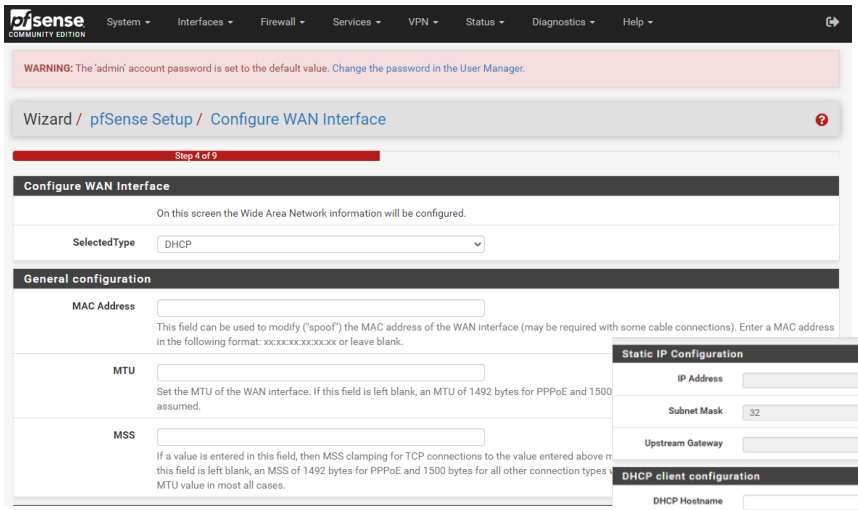


Cliquer sur Next

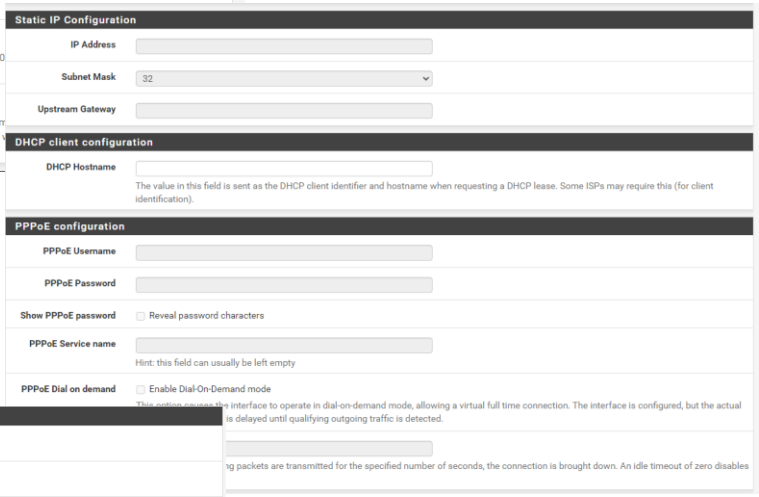
(1) Cliquer sur menu déroulant et sélectionner Europe/Paris
(2) Cliquer sur Next



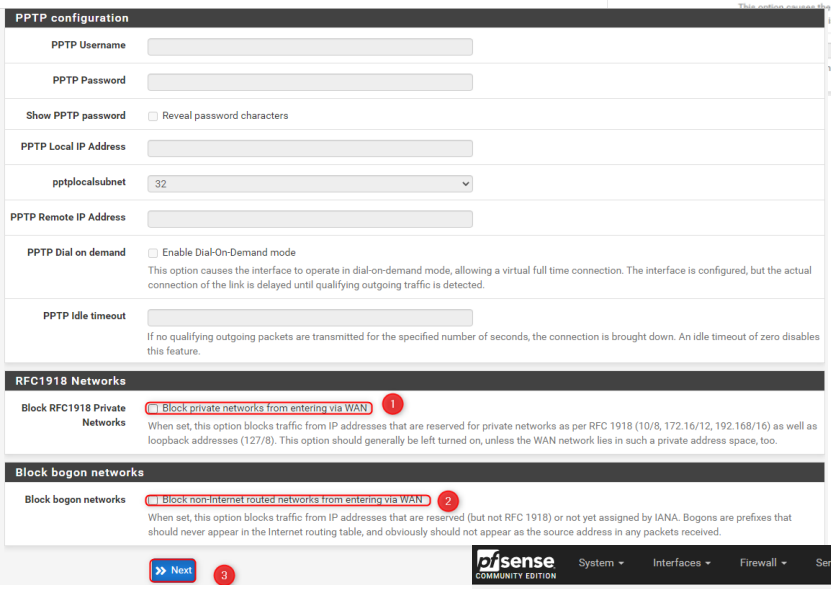
Dans cette partie il n'y pas grand-chose à modifier



Pas d'élément à modifier

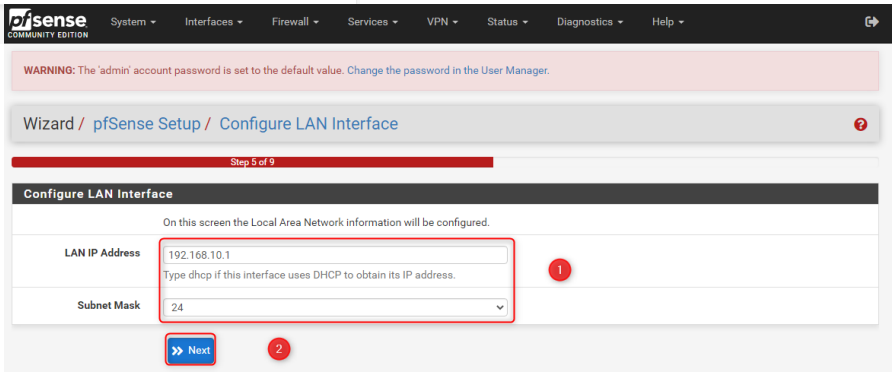


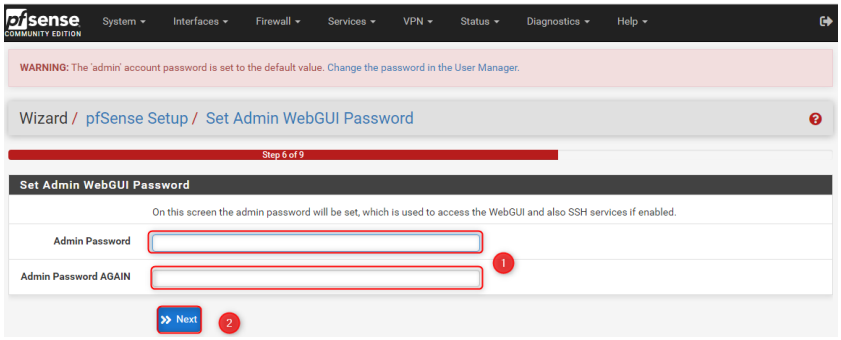
Pas d'élément à modifier



(1) Décocher la case Block private networks from entering via WAN
(2) Décocher la case Block non-Internet routed netdwork from entering via WAN
(3) Cliquer sur Next

(1) Vérifier bien que les information soit bon
(2) Cliquer sur Next

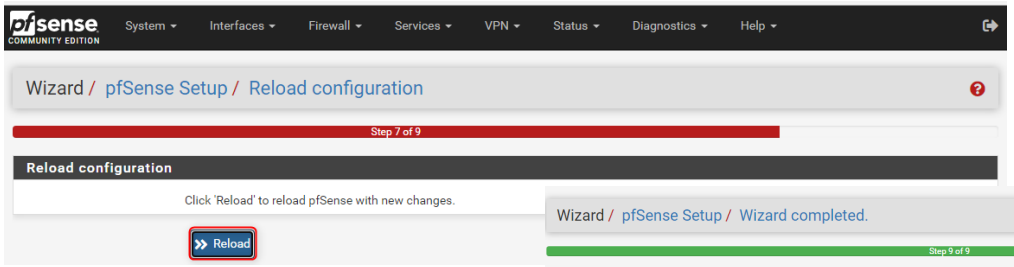




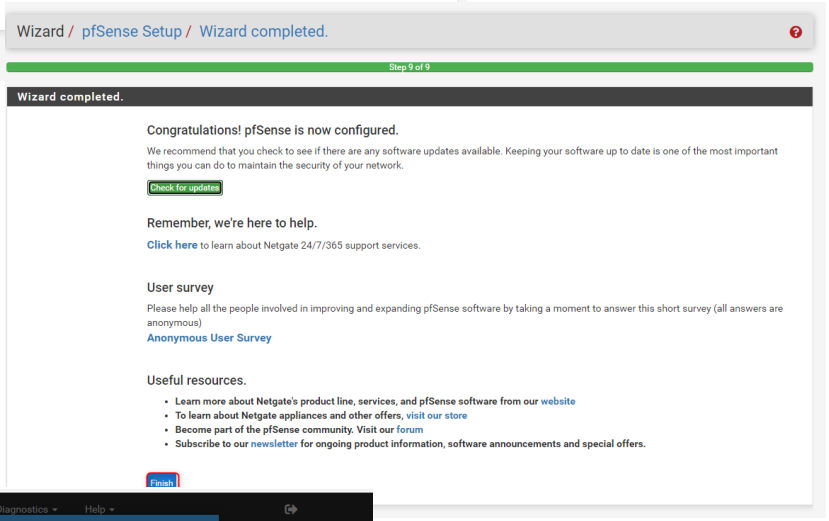
(1) Mettre en place le mot de passe Testap04@

(2) Cliquer sur Next

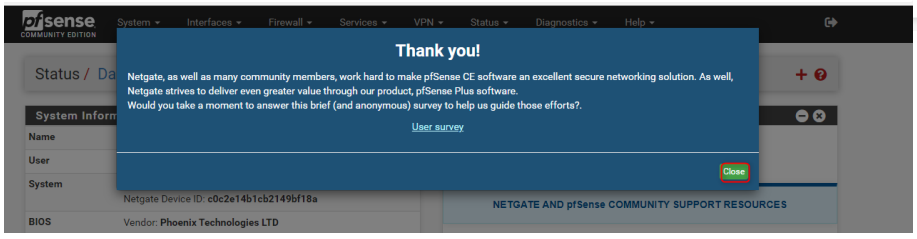
Une fois après modifier le mot de passe nous allons redémarrer la configuration



Cliquer sur Reload

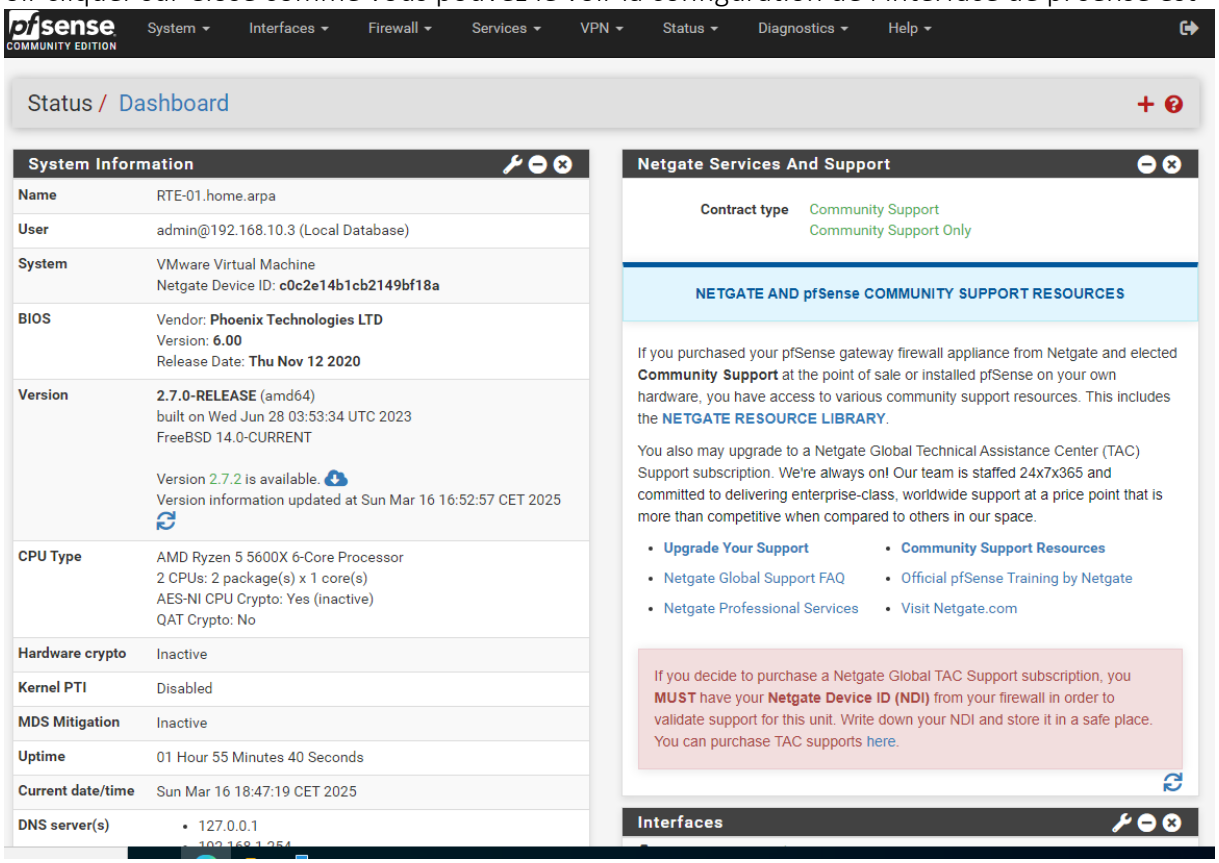


Cliquer sur Finish



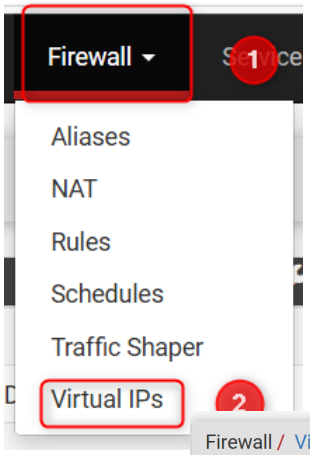
Cliquer sur Close

Après avoir cliquer sur Close comme vous pouvez le voir la configuration de l'interface de pFsense est bien fini

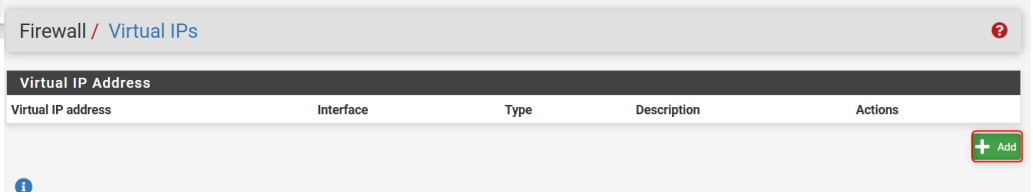


Création du CARP dans Pfsense

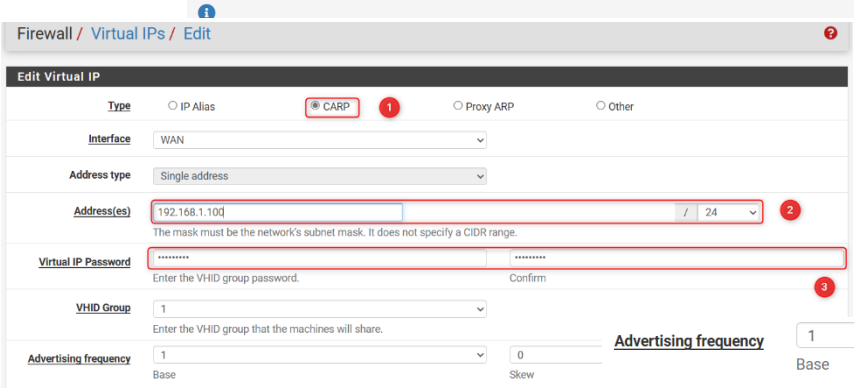
Nous allons créer un carp sur le routeur pour cela nous allons cliquer dans le menu de la barre de pfsense



(1) Cliquer sur Firewall
(2) Cliquer sur Virtual IPs

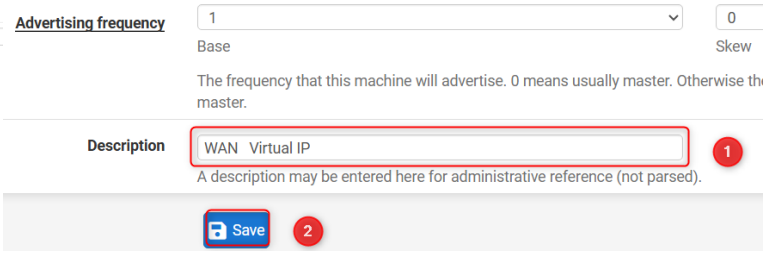


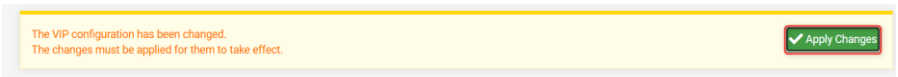
Cliquer sur Add



(1) Cliquer sur CARP
(2) Rentrer l'ip qui est 192.168.1.100

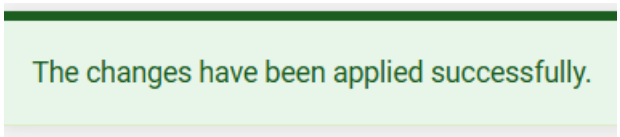
(1) Mettre un descriptif
(2) Cliquer sur Save



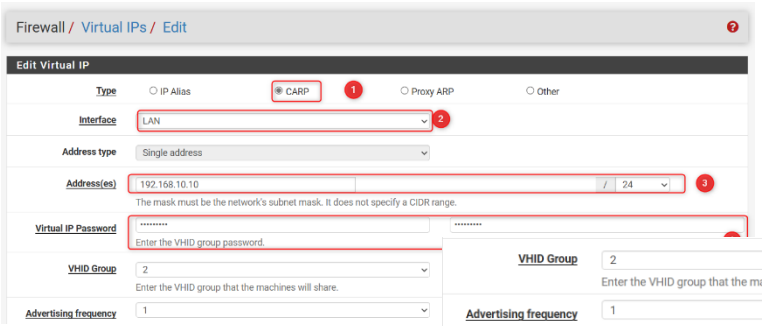


Cliquer sur Apply Change
Une fois avoir cliquer sur apply

vous aurez un message
Message de confirmation

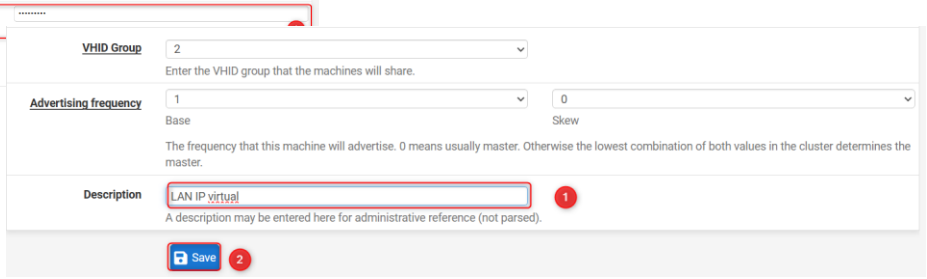


Puis ensuite refaire la même métode avec le LAN

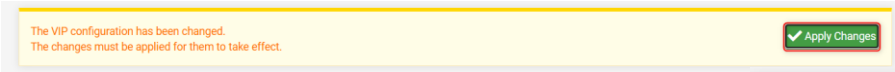


(1) Cocher la case CARP
(2) Rentrer l'ip 192.168.10.10
(3) Rentrer un mot de mot de passe

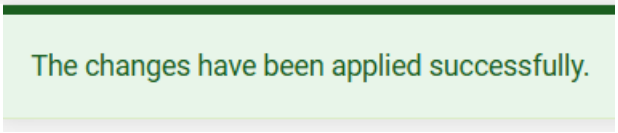
(1) Rentrer une description
(2) Cliquer sur Save

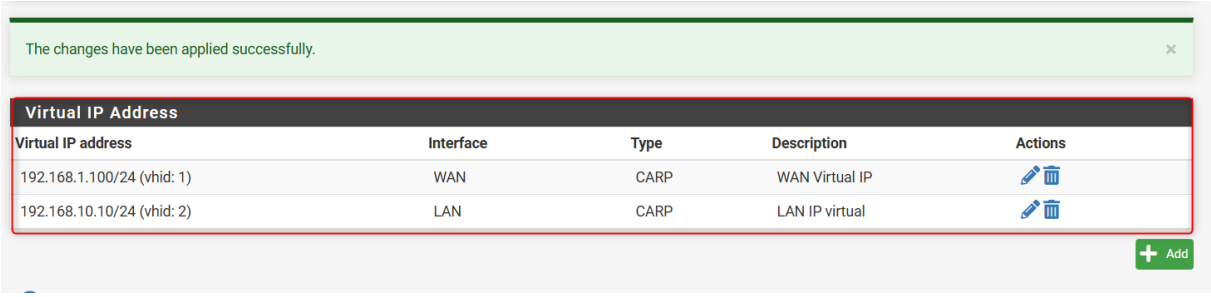


Cliquer sur Apply Change



Message de confirmation

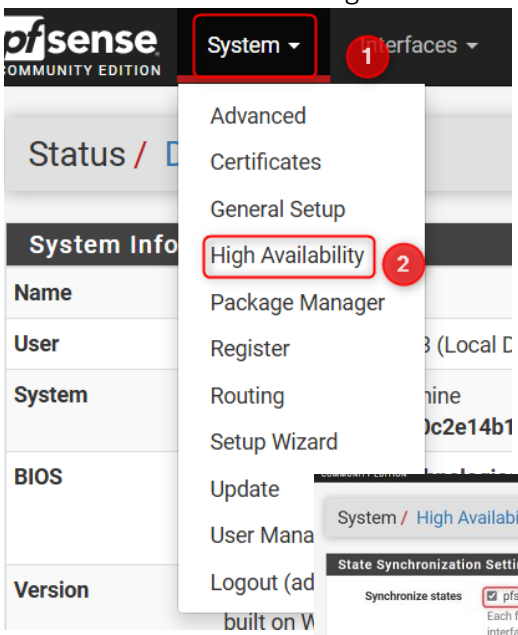




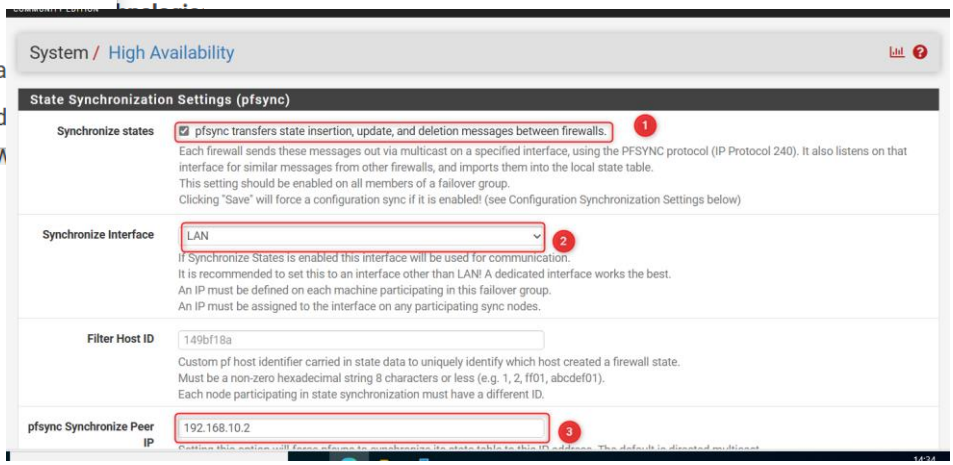
Une fois voici le résultat

Activation du Pfsync sur pfsense

Donc dans la barre de navigation nous allons cliquer sur l'option suivant :



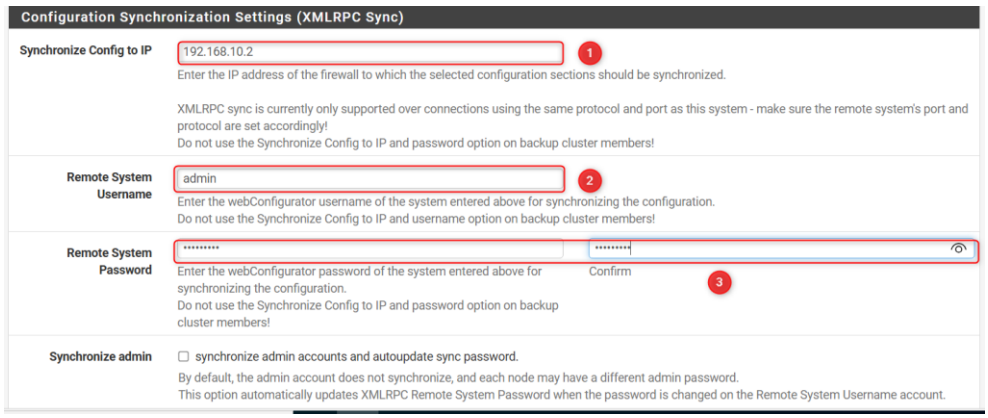
(1)cliquer sur System
(2)Cliquer sur High Availability



(1) Cocher la case pour activer pfsync cette option

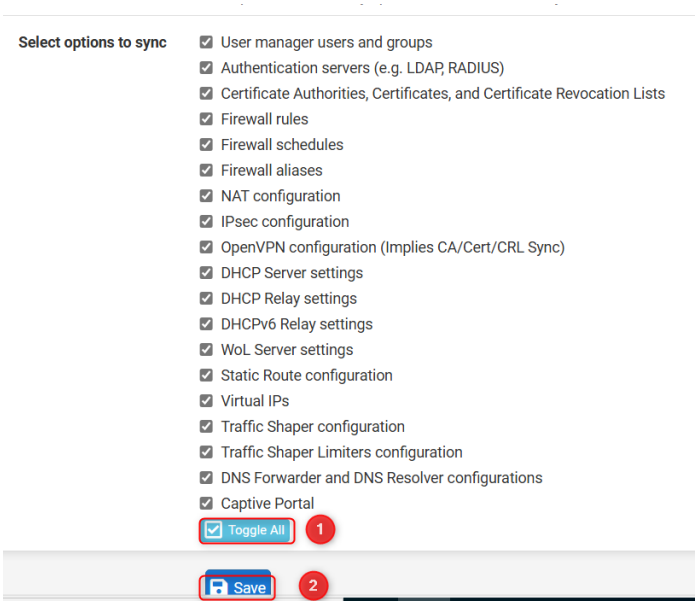
(2) Cliquer dans le déroulant puis selectionner la menu lan

(3) Rentrer l'ip du routeur 2 su LAN : 192.168.10.2



(1)Rentrer l'ip du routeur
(2)Rrentrer le nom utilisateur
(3)Rentrer le mot de passe
pour se connecter au pfsense

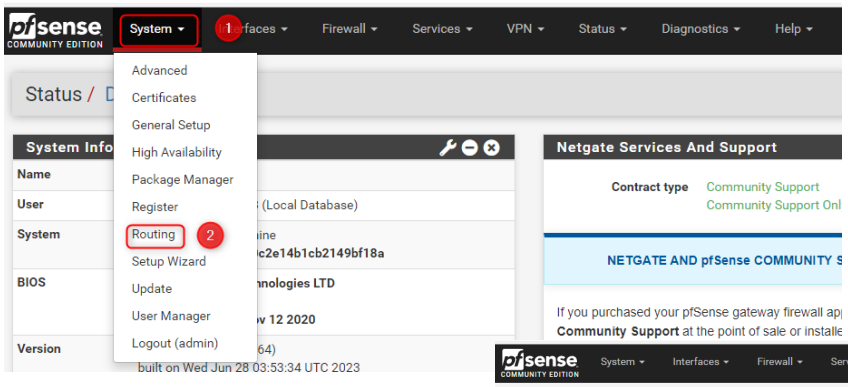
(1) Cliquer sur Toogle all pour tout selectionner les option
(2) Cliquer sur Save



Règle pare-feu Pfsyncs

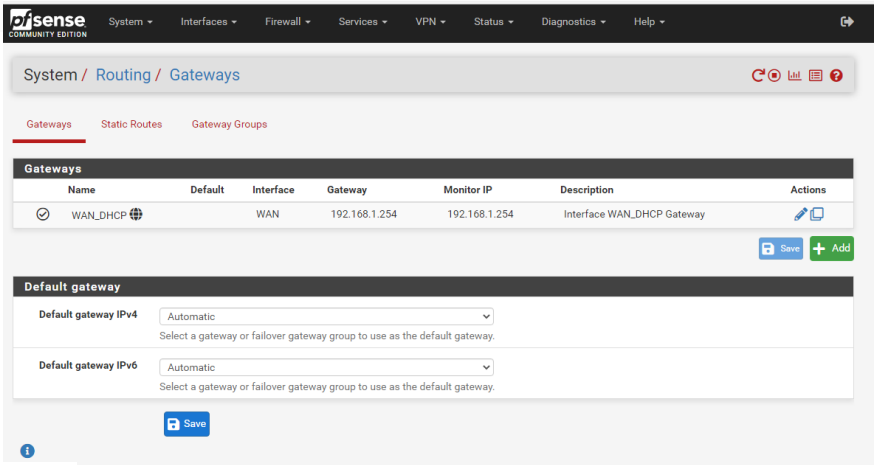
Configuration double WAN

Pour configurer le double WAN depuis l'interface web nous allons devoir cliquer dans une catégorie

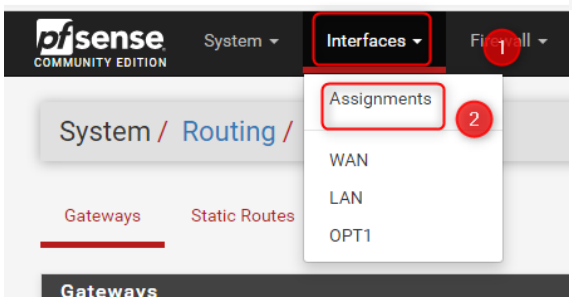


(1) Cliquer sur System
(2) Cliquer sur Routing

Et comme vous pouvez le voir nous avons que un WAN

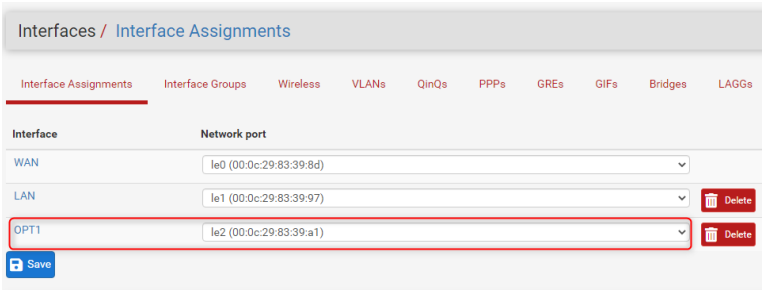


Dans notre cas nous allons configurer une deuxième interface



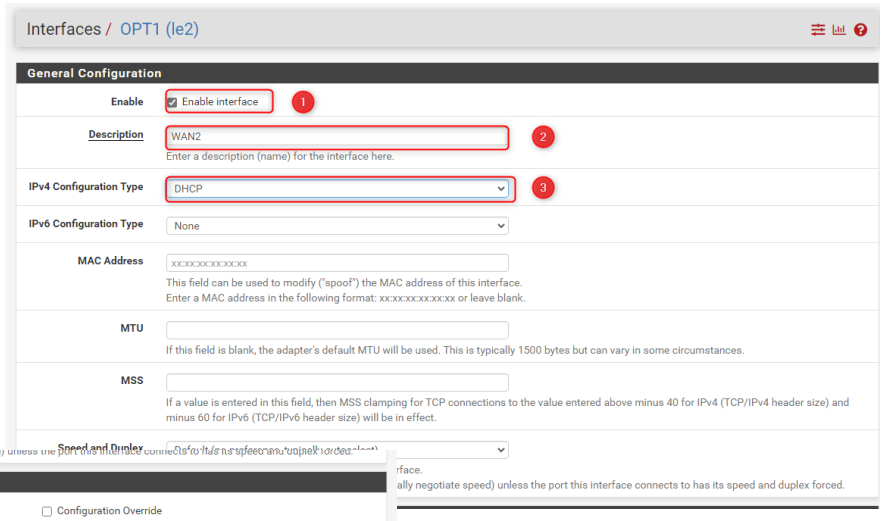
(1) Cliquer sur Interface
(2) Cliquer sur Assignements

Une fois sur l'interface vous allez voir plusieurs carte réseaux

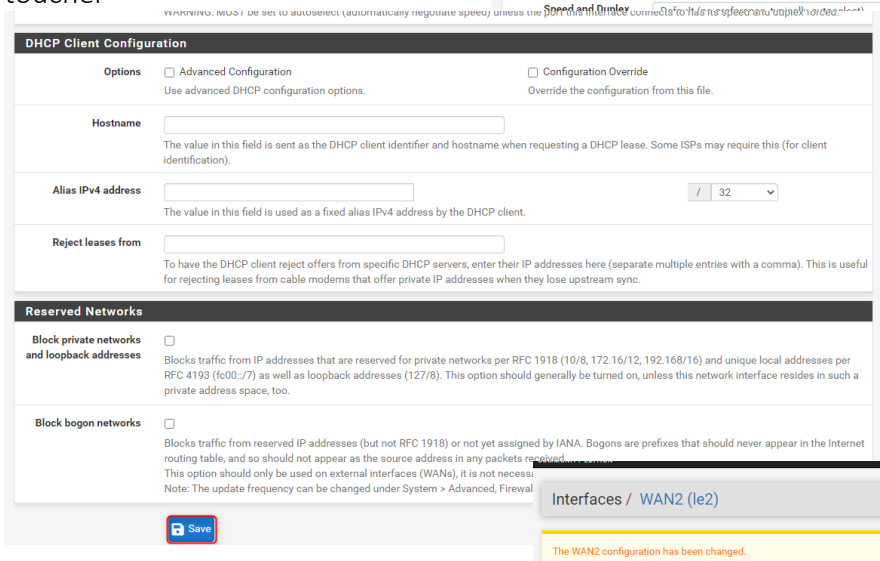


Cliquer sur OPT1

(1) Cocher la case enable interface
(2) Modfiier la description par WAN 2
(3) Cliquer sur le menu déroulant et choisir DHCP

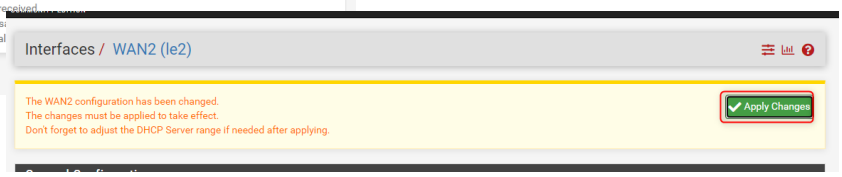


dans cette partis là rien est à toucher

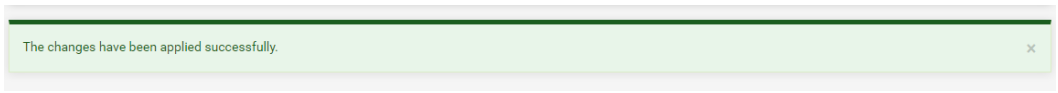


Cliquer sur save

Cliquer sur Apply Changes

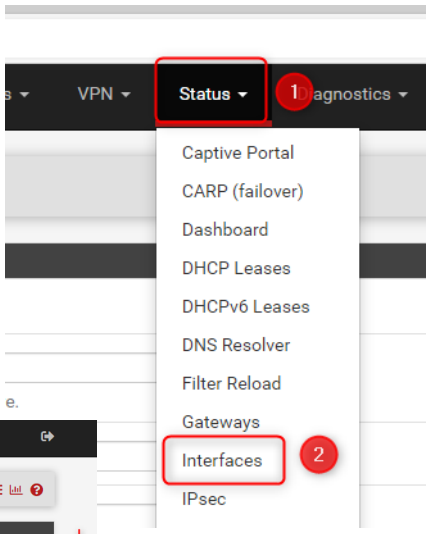


Ensuite un message s'affiche pour vous dire que la configuration à bien était prise en compte

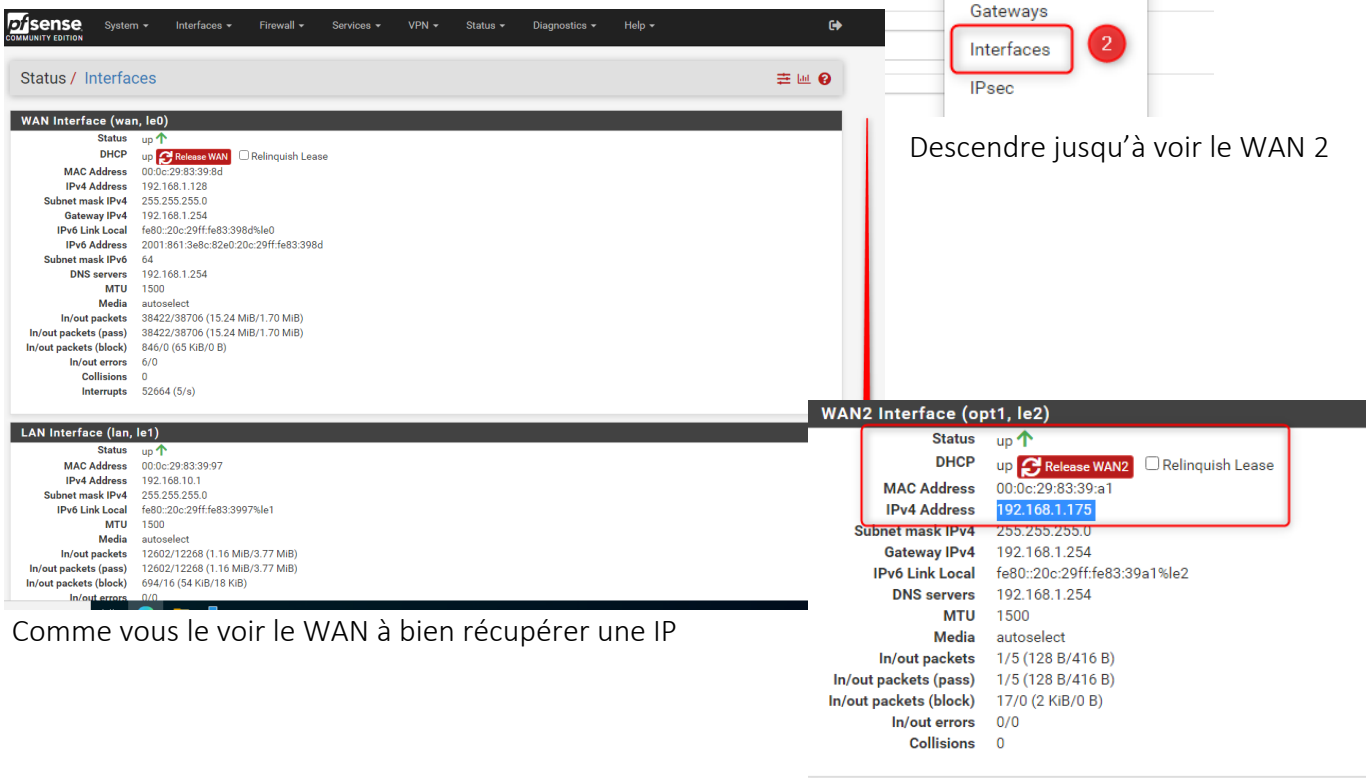


Puis pour bien voir si le WAN 2 est bien actif nous allons allez dans le menu suivant :

(1) cliquer sur Status
(2) Cliquer sur Interfaces

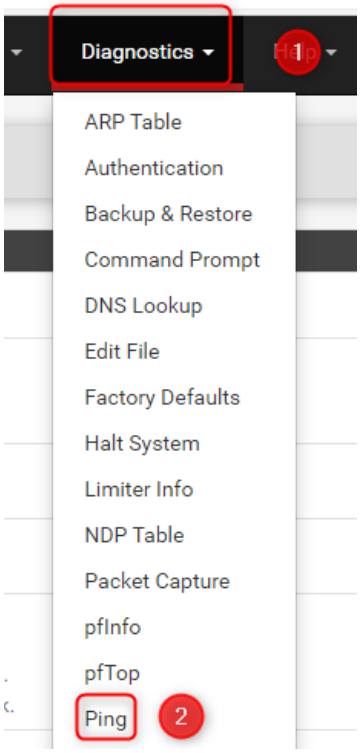


Descendre jusqu'à voir le WAN 2



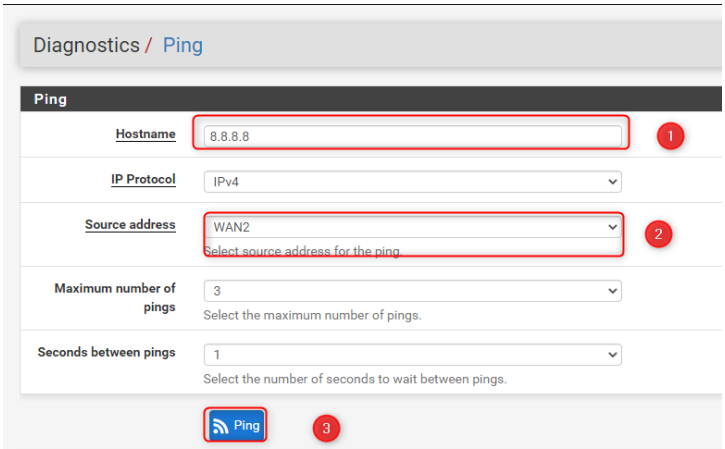
Comme vous le voir le WAN à bien récupérer une IP

ET donc pour vérifier que le WAN 2 fonctionne bien nous allons aller dans le menu suivant :



(1) Cliquer sur Diagnostics
(2) Ping

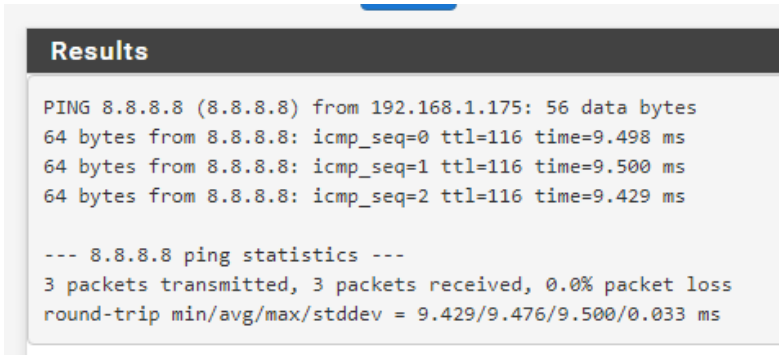
(1) Rentrer le serveur google
(2) Mettre la sources c'est-à-dire



le WAN 2

(3) Cliquer sur PING

comme vous pouvez le voir le WAN 2 fonctionne bien

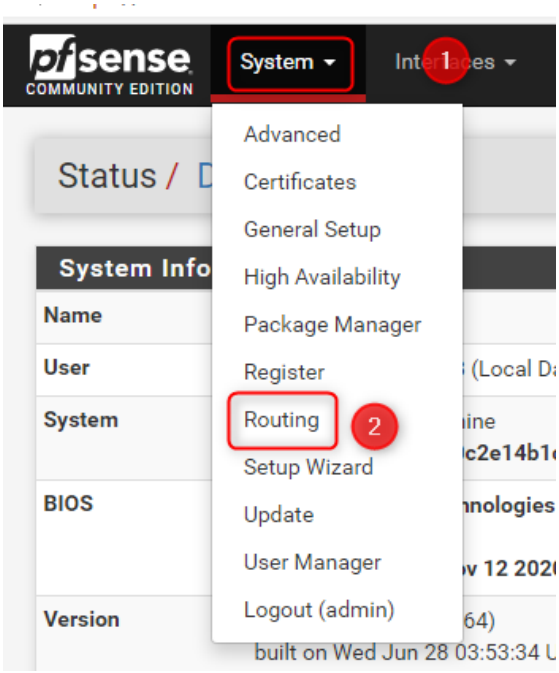


Résultat du ping 8.8.8.8 vers le WAN2

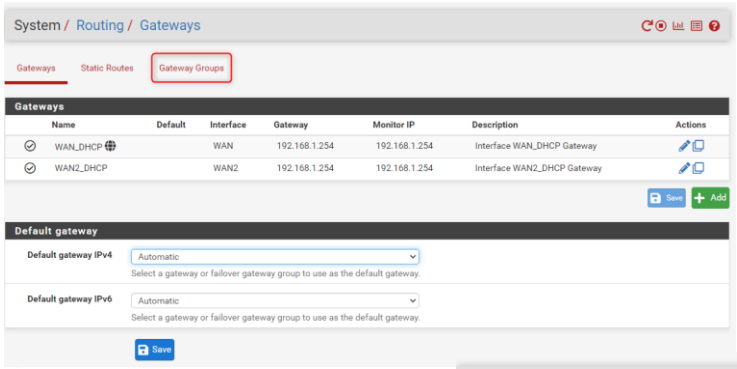
Configuration un groupe de passerelle

Donc pour cela nous allons retourner dans menu système puis routing

(1) Cliquer sur System
(2) Cliquer sur Routing

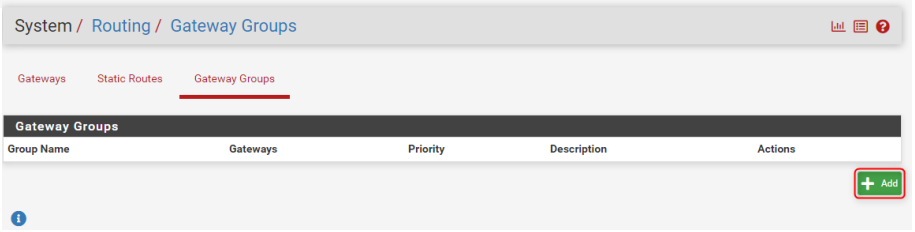


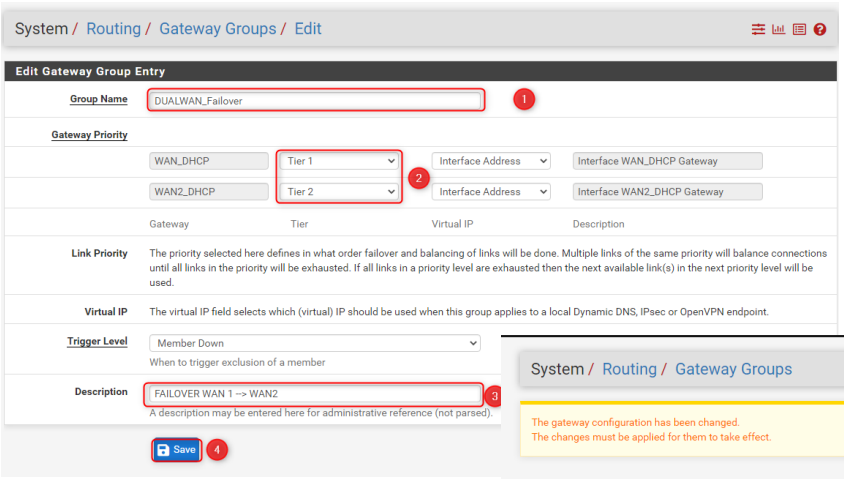
Une fois sur cette interface nous allons cliquer sur un paramètre bien précis



Cliquer Gateway Groups

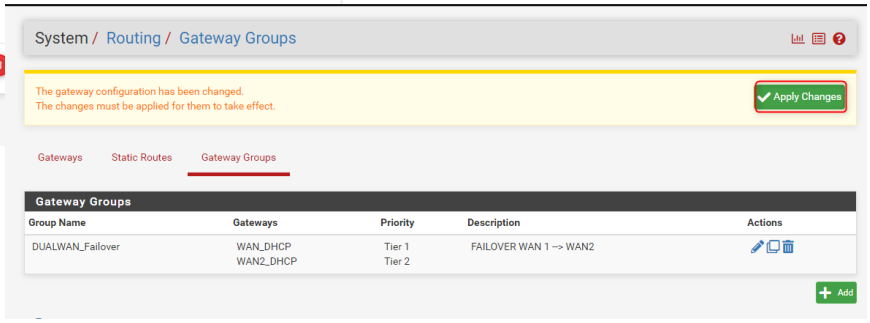
Cliquer sur Add



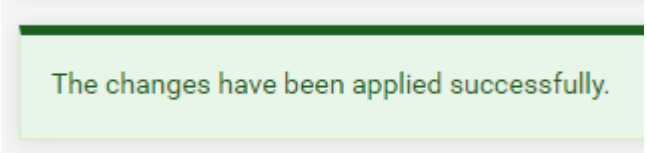


(1) Donner un nom pour le groupe
(2) Mettre en priorité le type de carte qu'on souhaite utiliser
(3) Réaliser une description
(4) Cliquer sur Save

Cliquer sur Apply Change pour sauvegarder.



Une fois que vous avez appliqué les paramètre un message va apparaitre

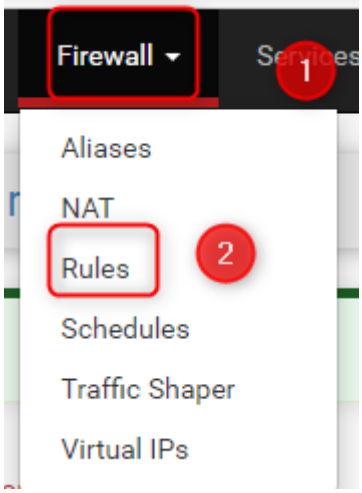


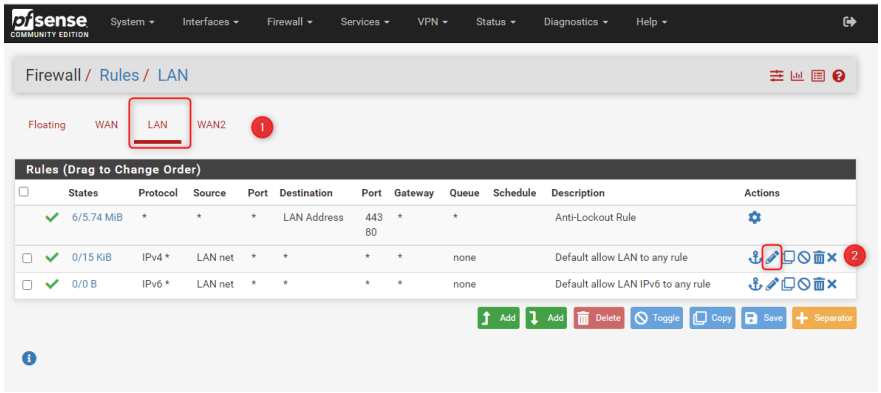
Ceci est un message comme quoi la configuration à bien pris en compte

Appliquer le groupe aux règles par Pare-feu

Pour cela nous allons cliquer dans le menu de la barre puis cliquer dans l'onglet suivant :

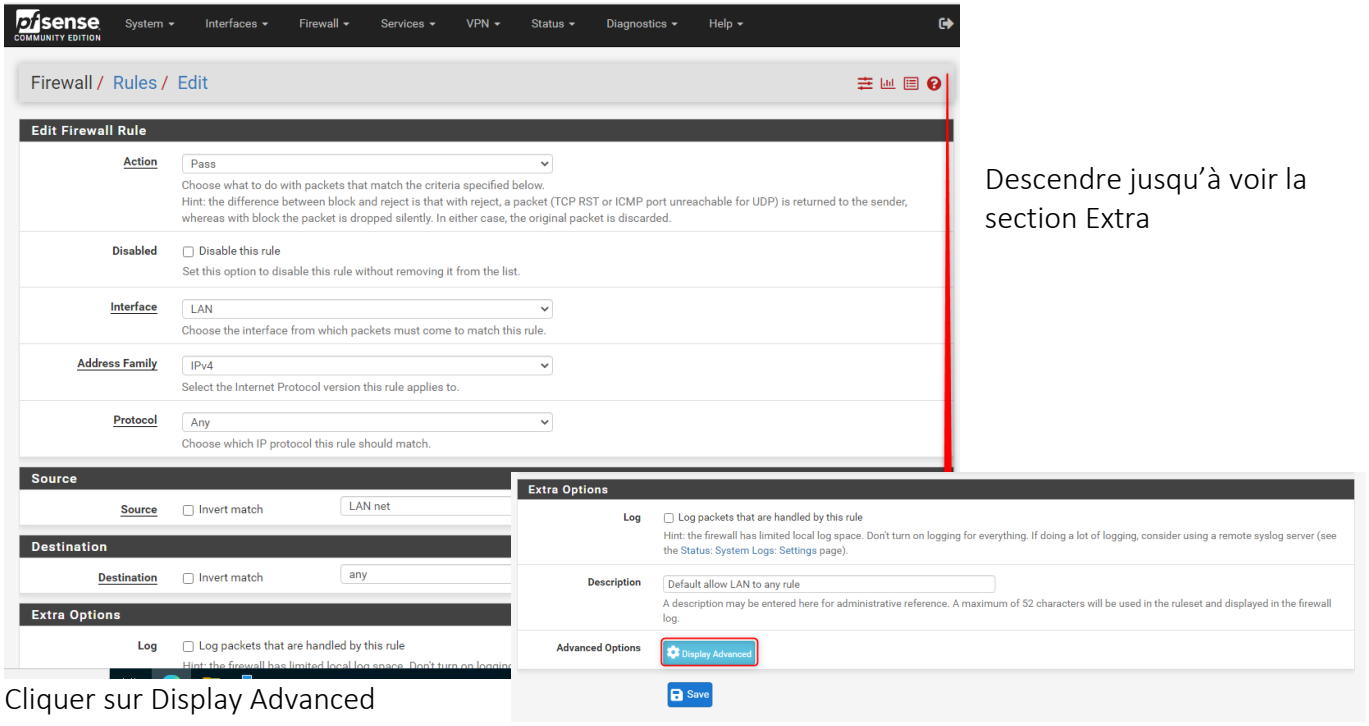
(1) Cliquer sur Firewall
(2) Cliquer Rules





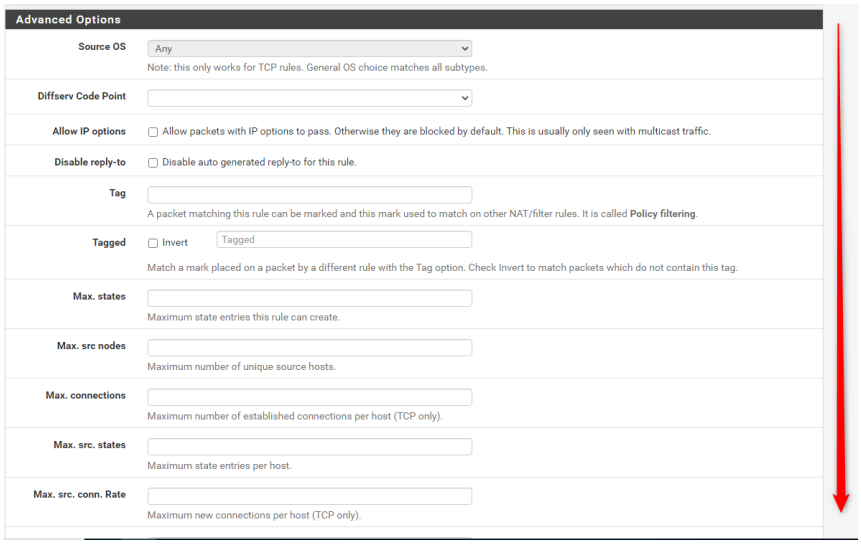
(1) Cliquer sur LAN
(2) Ensuite cliquer sur le crayon sur la ligne LAN.NET IPV4

Après avoir cliqué sur le crayon vous aurez cette page



Descendre jusqu'à voir la section Extra

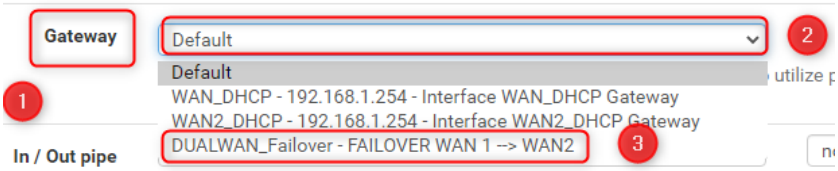
Cliquer sur Display Advanced



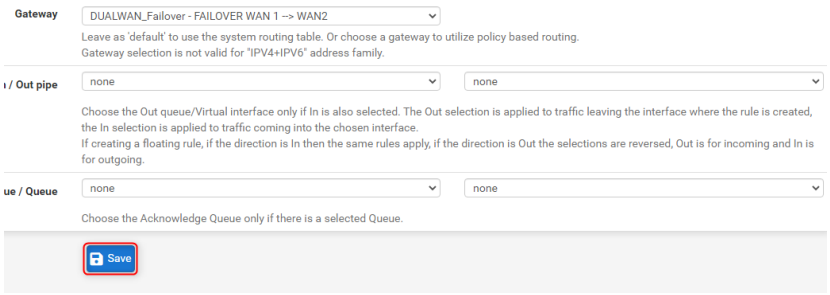
Descendre jusqu'à voir l'option Gateway

Après avoir trouver l'option en question

(1) repérer Gatway
(2) Cliquer sur le menu déroulant
(3) Sélectionner DUAL WAN FAILOVER

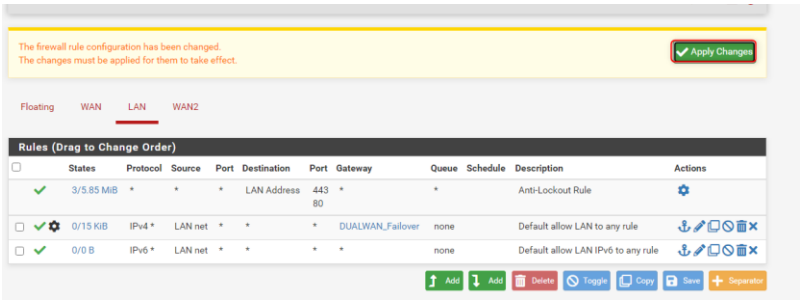


Après avoir fait ceci nous allons enregistrer la configuration que nous avons effectué

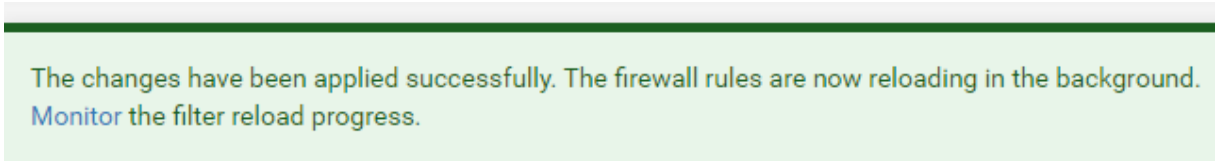


Cliquer sur Save

Cliquer sur Apply Change



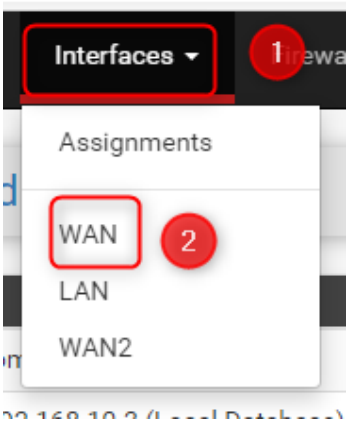
Une fois avoir cliquer un message confirme la configuration réaliser

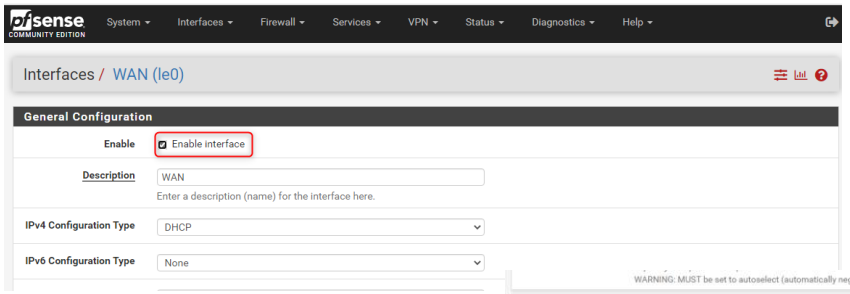


Test du Dual-WAN

Pour voir si tout fonctionne correctement nous allons cliquer dans le menu suivant :

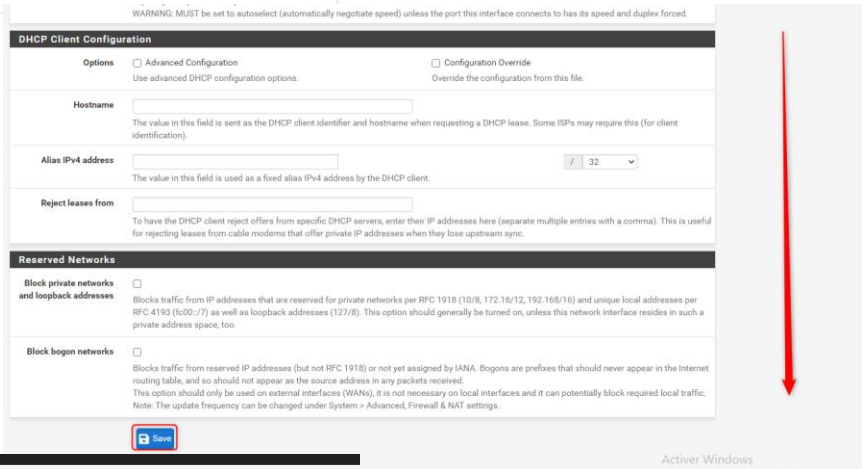
(1) Cliquer sur Interfaces
(2) WAN

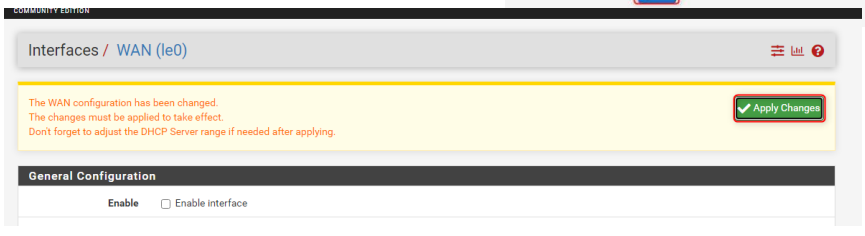




Cocher la case Enable Interface pour la désactiver

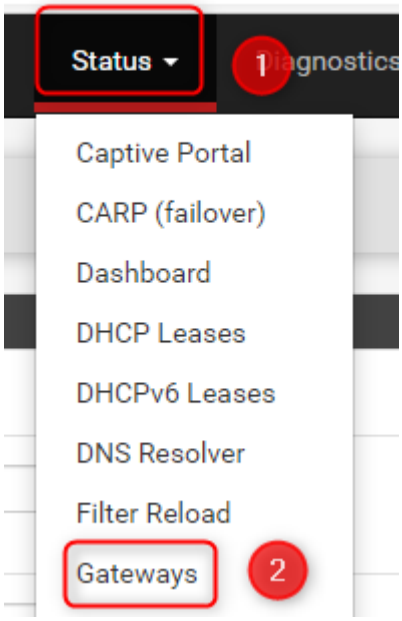
Descendre jusqu'à trouver le bouton Save
Cliquer sur Save





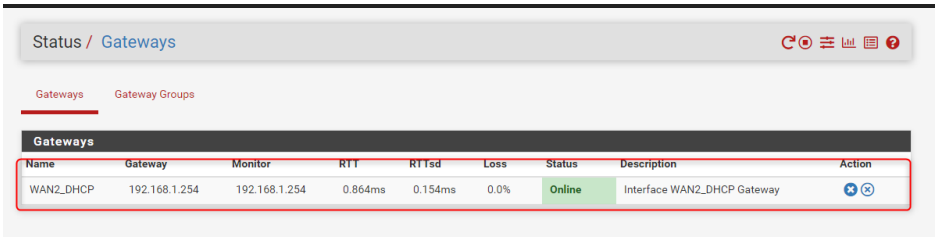
Cliquer sur Apply Change

Ensuite lorsque vous aurez juste appliquer vous allez devoir allez dans la barre de menu de pfsense



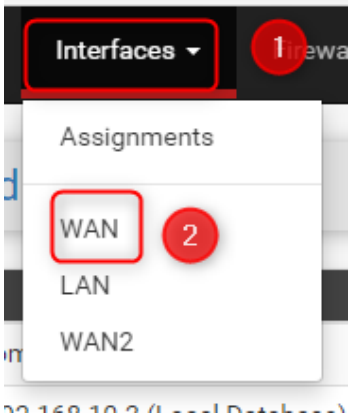
(1) Cliquer sur Status
(2) Cliquer sur Gateway

Lorsqu'on désactive l'interface WAN voici le résultat.



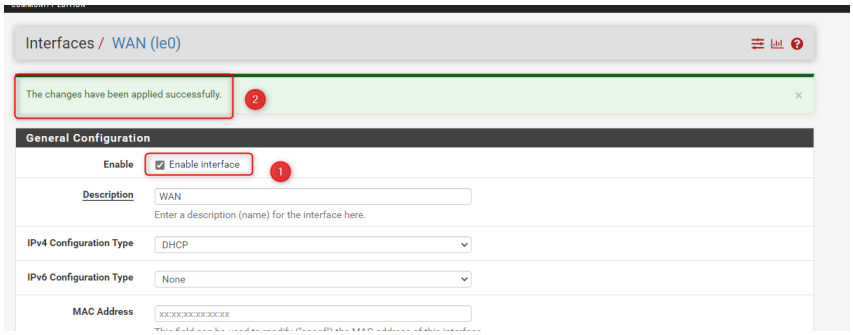
Comme vous pouvez le voir le WAN à est plus disponible donc c'est le WAN 2 qui à repris le relève

Donc lorsqu'on reconnecte le WAN donc pour cela nous allons retourner sur l'interface

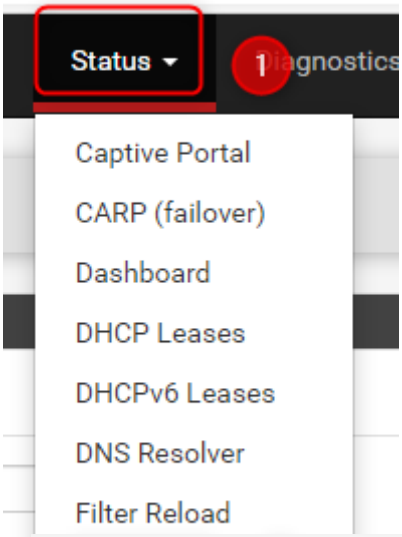


(1) Cliquer sur Interfaces
(2) WAN

(1) Cliquer sur la case pour réactiver l'interface WAN
(2) Message de prise en compte

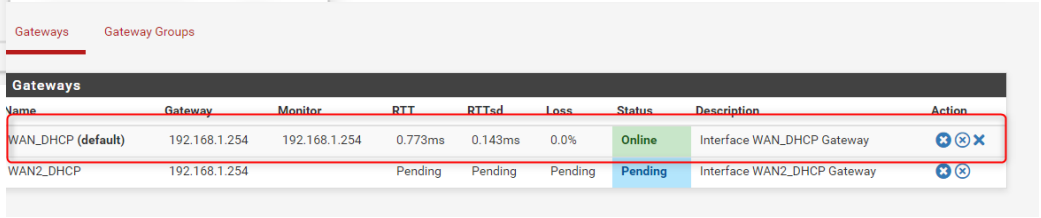


Ensuite pour vérifier que cela fonction nous allons retourner dans la barre du menu de pfsense



(1) Cliquer sur Status
(2) Cliquer sur Gateway

ET donc comme vous pouvez le constater le WAN est bien réapparu.



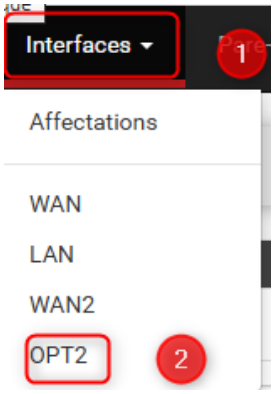
Pour dire que cela fonctionne bien

Configuration DMZ

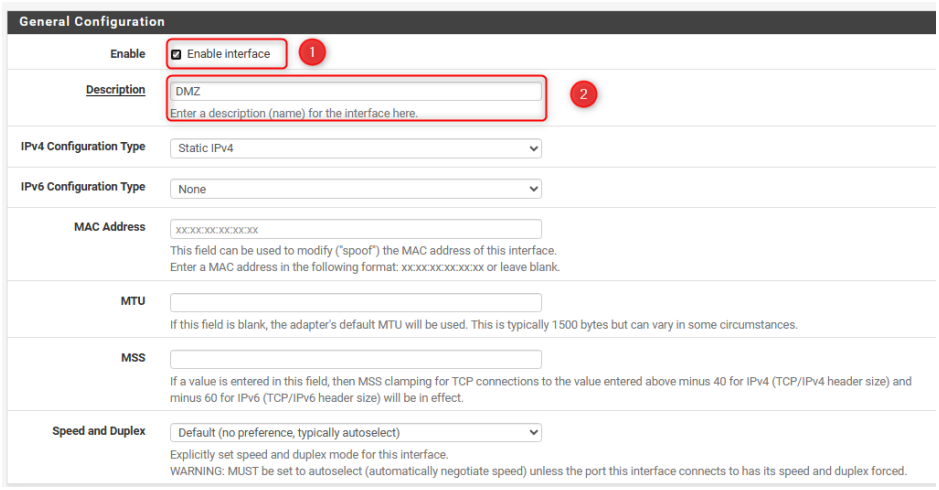
Avant de configurer la DMZ, vérifier bien que vous avez une carte réseau qui est dédier. Une fois fait

(1) Cliquer sur Interface

(2) Cliquer sur OPT2



1.



Activation de l'interface

L'option **"Enable interface"** est cochée afin d'activer l'interface réseau.

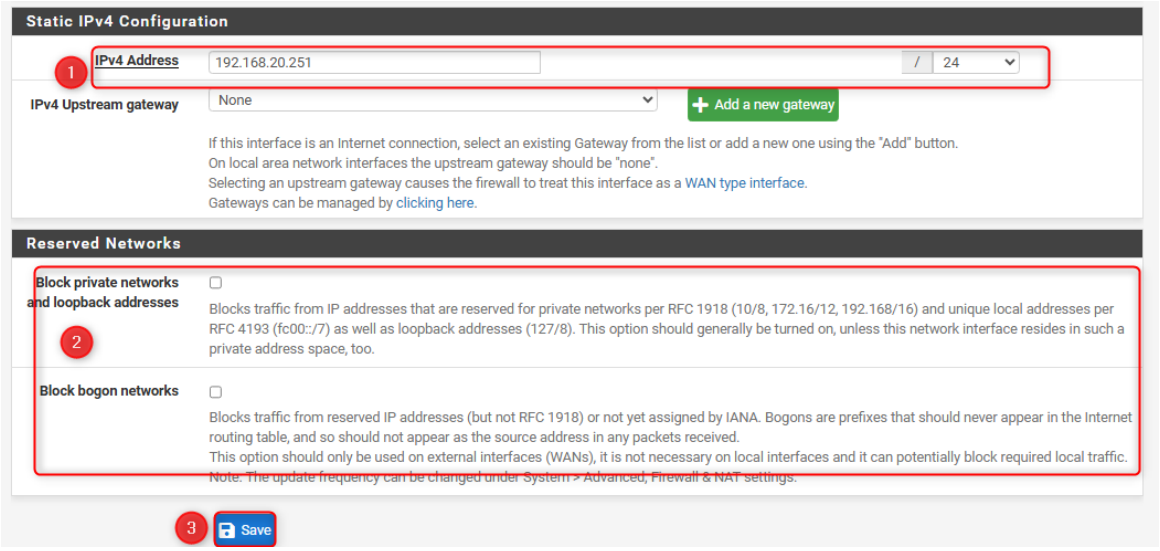
Cette étape est obligatoire pour que l'interface soit prise en compte par le pare-feu pfSense.

2. **Nom de l'interface**

Le champ **"Description"** est renseigné avec le nom **"DMZ"**.

Ce nom permet une identification rapide de l'interface dans les différents menus de configuration et de gestion (interfaces, règles firewall, routage, etc.).

Définir manuellement une adresse IP pour l'interface DMZ afin de l'intégrer dans un sous-réseau spécifique, ici dédié aux services placés en zone démilitarisée.



1. Adresse IPv4 statique
   - Le champ "IPv4 Address" est renseigné avec 192.168.20.251/24.
   - Cette adresse correspond à la passerelle (gateway) du sous-réseau DMZ. Elle sera utilisée comme point d'accès pour les machines situées dans la zone DMZ (exemple : un serveur web en 192.168.20.10).
2. Options des réseaux réservés (à laisser décochées dans ce cas)
   - "Block private networks and loopback addresses" : cette option est décochée car cette interface est destinée à une DMZ, donc un réseau privé. Activer cette option bloquerait potentiellement tout le trafic utile.
   - "Block bogon networks" : décochée également, pour éviter de bloquer des plages d'adresses utilisées localement qui ne sont pas encore officiellement allouées. Cette option est surtout utile sur une interface WAN.
3. Sauvegarde de la configuration
   - Cliquer sur "Save" pour valider les paramètres appliqués à cette interface.

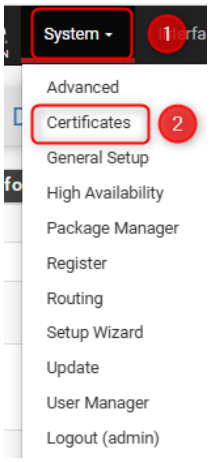
Importance de cette configuration :

- L'attribution manuelle d'une IP sur l'interface DMZ permet un **meilleur contrôle du routage** et de la **sécurité réseau**.
- En DMZ, il est essentiel d'avoir une configuration réseau **maîtrisée, stable et isolée** du reste du réseau interne.

Configuration OPNVPN ROAD WARRIOR

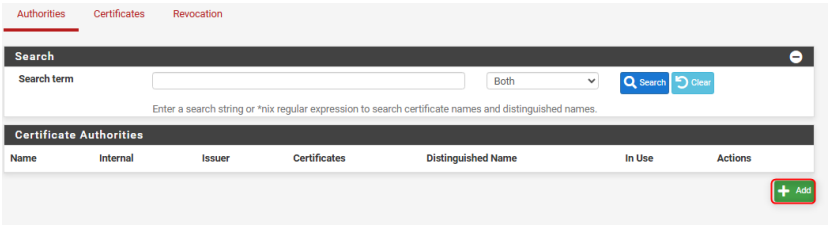
Création du Certifcat

Dans cette partie nous allons configurer open VPN donc pour cela nous nous diriger vers la barre de navigation de pfsense



(1) Cliquer sur System
(2) Cliquer sur Certificates

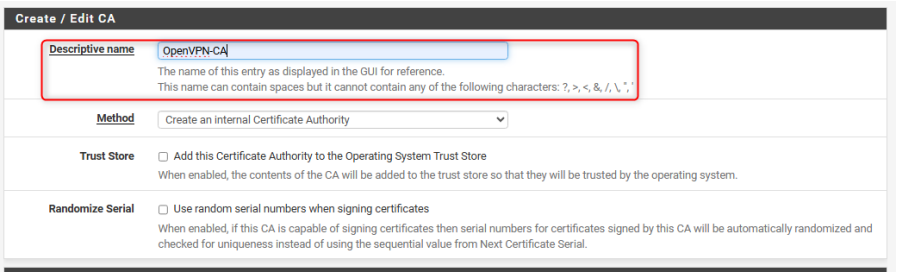
Cette page permet de consulter les autorités de certification déjà créées dans pfSense. Pour démarrer la configuration VPN, il faut d'abord créer une CA qui servira à signer les certificats.



Cliquer sur **Add** pour commencer la création d'une nouvelle CA.

Dans cette vue, on configure les **premiers paramètres** de la nouvelle autorité de certification.

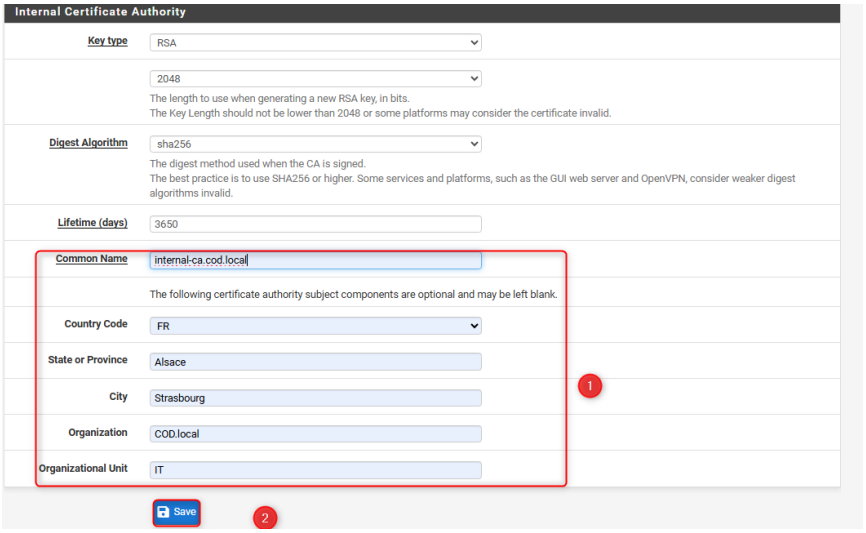
- **Descriptive name** : nom lisible de la CA dans l'interface pfSense. Il doit être clair pour identifier l'usage prévu (ex : OpenVPN-CA).
- **Method** : permet de définir si la CA est :
  - générée localement (*Create an internal Certificate Authority*),
  - importée depuis une autre instance (externe),
  - ou une CA intermédiaire.
- **Trust Store (optionnel)** : permet d'ajouter la CA au magasin de certificats du système pour qu'elle soit reconnue comme de confiance.
- **Randomize Serial** : génère des numéros de série aléatoires pour les certificats signés, ce qui améliore la sécurité contre les collisions ou les attaques ciblées.



Rentrer le nom souhaiter dans le Descriptive name dans notre cas ç nous c'est OpenVPN-CA

Dans cette section, on définit les détails techniques et d'identification de la CA :

- **Key Type / Length** : RSA 2048 bits (standard recommandé).
- **Digest Algorithm** : SHA256.
- **Lifetime** : durée de validité de la CA (ex : 3650 jours = 10 ans).
- **Common Name, Organization, etc.** : ces champs identifient la CA dans les certificats.

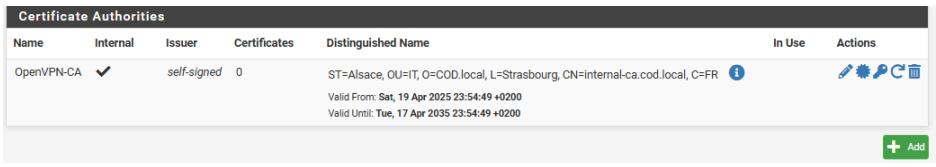


(1) Rentrer les champs demander c'est-à-dire : Common Name : internal-ca local , Country Code FR, City Strasbourg , Organization : COD.local , Organizationnal Unit : IT
(2) Cliquer sur Save

Une fois la CA enregistrée, elle apparaît dans la liste.

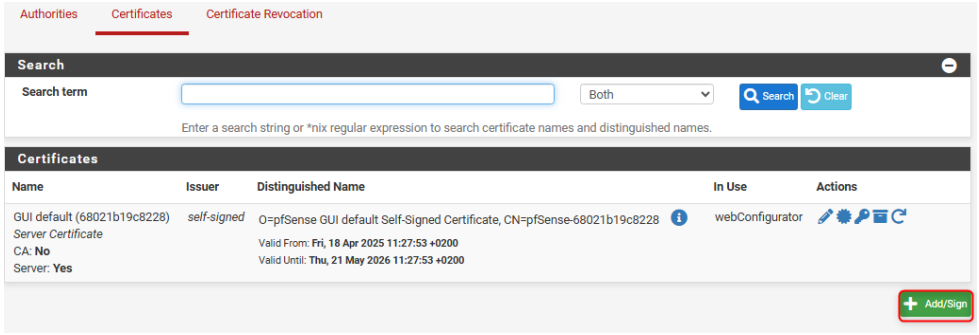
- **Issuer : self-signed** → c'est une CA racine locale.
- **Certificates : 0** → aucun certificat encore généré avec cette CA.
- **Valid From / Until** : dates de validité.
- On pourra l'utiliser pour signer des certificats (VPN ou autre)

Certificat créer



Cette section permet de consulter les certificats disponibles dans pfSense.
On y voit ici un certificat **auto-signé par défaut** utilisé pour l'accès HTTPS à l'interface d'administration (webConfigurator).
Ce qu'il faut savoir :

- Un **certificat serveur signé par une CA** est obligatoire pour sécuriser les connexions OpenVPN.
- Le certificat **doit être de type "Server Certificate"**, afin d'être accepté par les clients OpenVPN.



Cliquer sur **Add/Sign** (bouton vert) pour **créer un nouveau certificat** signé Cette page permet de **générer un certificat interne**, signé par la CA créée précédemment.

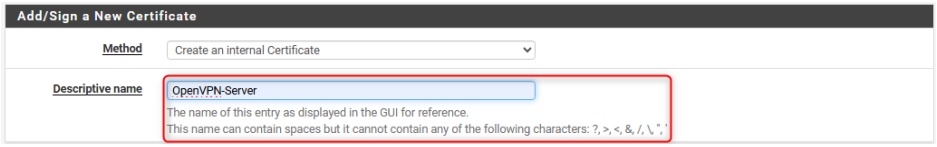
Ce certificat est indispensable pour que le serveur OpenVPN puisse établir une connexion chiffrée avec les clients.

⚙️ **Champs à renseigner :**

- **Method** :
  Laisser sur Create an internal Certificate → on veut un certificat local, pas un certificat externe ou une demande de signature.

- **Descriptive name** :
  Nom du certificat, visible uniquement dans pfSense (ex : OpenVPN-Server).
  Important pour différencier les certificats si plusieurs sont créés pour différents services.

Dans notre cas OpenVPN-Server



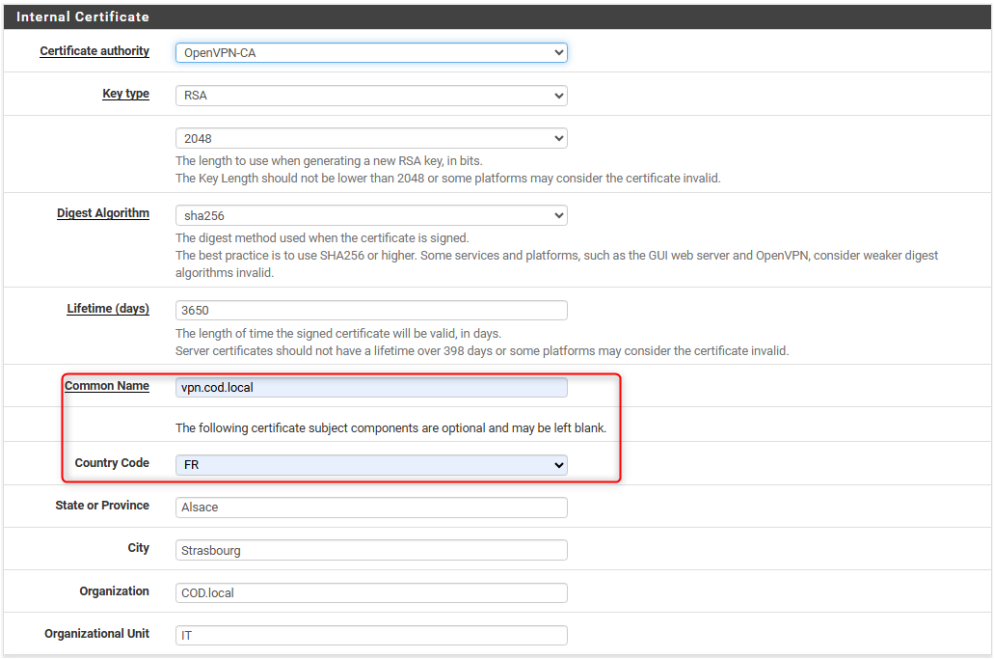
c'est

Ces informations sont intégrées dans le certificat et servent à identifier le serveur :

Champ	Description
Common Name	Nom du serveur (ex : vpn.cod.local) utilisé par OpenVPN. Doit correspondre à l'adresse utilisée par les clients.
Country Code	Code du pays (ex : FR).
State / City	Localisation (ex : Alsace / Strasbourg).
Organization / Unit	Nom du domaine ou de l'entreprise (ex : COD.local) et service (ex : IT).

🔐 **Remarque importante** : Le **Common Name** doit idéalement **correspondre au FQDN ou IP** utilisé par les clients VPN pour se connecter au serveur, afin d'éviter des erreurs de validation de certificat côté client.

➡️ Une fois ce formulaire rempli, il suffit de cliquer sur **Save** pour générer et signer le certificat. Il sera ensuite utilisable dans la configuration du serveur OpenVPN.



Dans notre cas nous renseigner Common Name : vpn.cod.local
Country code DR

Cette section permet d'**ajouter des contraintes ou des informations supplémentaires** au certificat.

Détails des champs :

- **Certificate Type** :
  Type d'utilisation du certificat.
  - Ici, il faut sélectionner **Server Certificate** (et non "User Certificate") si le certificat est destiné à un **serveur OpenVPN**.
  - Un mauvais type peut empêcher le certificat d'être accepté pendant la connexion VPN.
- **Alternative Names** (SAN – Subject Alternative Names) :
  Permet d'ajouter d'autres **noms ou adresses** que le Common Name.
  Par exemple : un FQDN, un nom DNS ou une IP utilisée par les clients pour joindre le serveur.

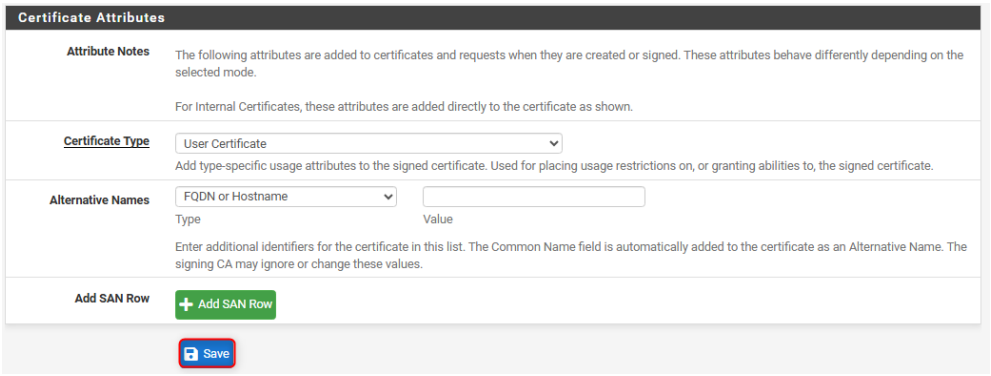
Ce champ est **optionnel** mais recommandé si plusieurs noms sont utilisés pour accéder au serveur (ex : vpn.cod.local, vpn.cod.lan, IP publique, etc.).

- **Add SAN Row** :
  Bouton pour ajouter une ligne SAN.

Finalisation :

- Une fois tous les champs correctement remplis, cliquer sur **Save** pour générer et signer le certificat.

Cliquer sur Save



Problème détecté :
Dans la liste des certificats, le champ **Certificate Type** affiche :

- **User Certificate**
- **Server : No**

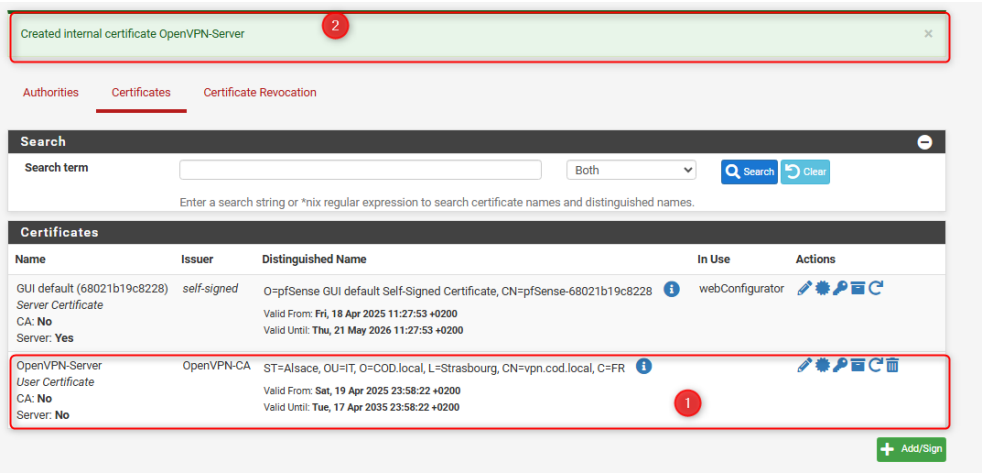
Cela signifie que le certificat a été généré en tant que **certificat utilisateur**, et **non serveur**.
Explication du problème :
Lors de l'étape précédente (capture 8), la **valeur "Certificate Type" n'a pas été changée** : elle est restée sur "User Certificate" au lieu de "Server Certificate".
Résultat : le certificat ne pourra **pas être utilisé pour un serveur OpenVPN**, car il n'est pas reconnu comme tel.
🛠️ **Solution :**
Tu dois **recréer un nouveau certificat**, en prenant bien soin de :

- Choisir le type **Server Certificate**,
- Conserver les mêmes paramètres (nom, Common Name, CA, etc.).

Une fois le bon certificat créé, tu verras dans la liste :

- **Certificate Type** : Server Certificate
- **Server : Yes**

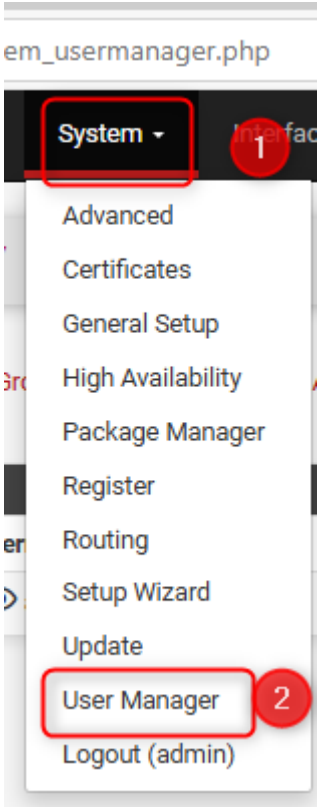
Remarque :
Même si le certificat apparaît comme "User Certificate", il peut tout de même fonctionner pour OpenVPN.
Il est cependant recommandé de spécifier "Server Certificate" pour respecter les bonnes pratiques et garantir une compatibilité maximale avec tous les clients.



En haut, on voit le message : **“Created internal certificate OpenVPN-Server”**
Cela confirme que la création du certificat s’est bien déroulée.

Création d’un utilisateur pour l’exportation du certificat

Cette capture montre le chemin pour accéder au **User Manager** de pfSense.



(1) Cliquer sur System
(2) Cliquer sur User Manager

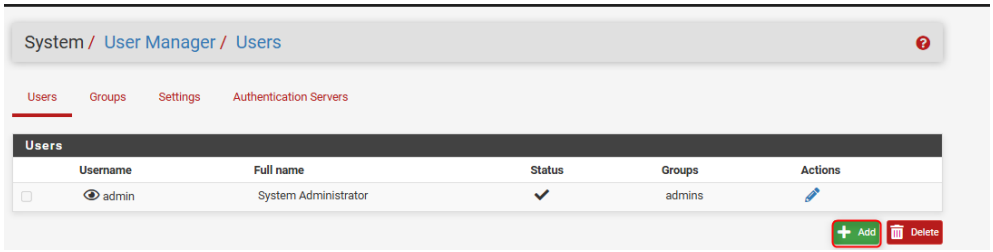
Cela permet de créer des comptes qui pourront ensuite être utilisés pour :

- L’**authentification VPN**,
- L’accès à l’interface d’administration (avec droits),
- D’autres services liés à l’utilisateur (certificat, portail captif, etc.).

Cas d'usage dans le cadre OpenVPN Road Warrior :

- Si tu ne relies pas encore pfSense à un annuaire (LDAP/Active Directory), tu peux :
    - créer des **utilisateurs locaux**,
    - et les utiliser pour s'authentifier au VPN.
- Ces utilisateurs peuvent également être associés à des **certificats** s'ils doivent utiliser une double authentification : **login + mot de passe + certificat**.

Cliquer sur Add

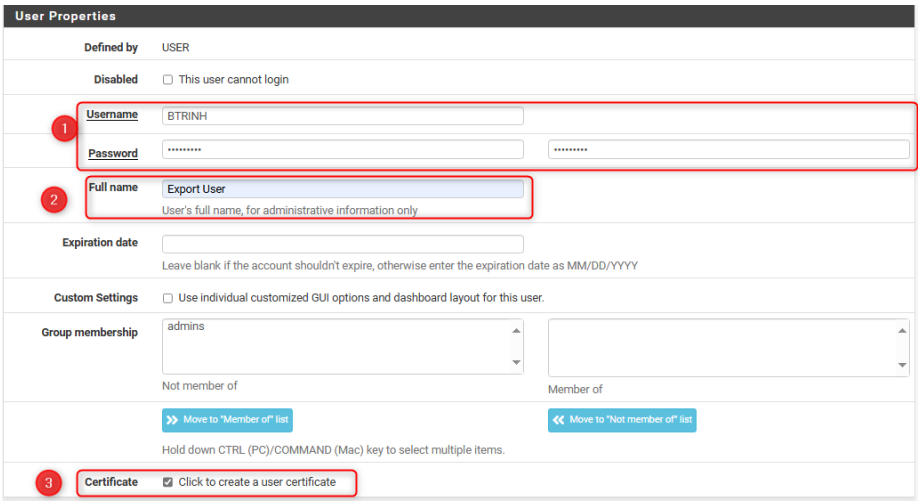


Créer un **utilisateur local** dans pfSense, avec un **certificat associé**.
Ce type de compte est utilisé pour :

- Authentification VPN (mode *user auth + cert*)
- Tests internes sans dépendre d'un annuaire externe (Active Directory)

Détail des champs importants :

1. **Username / Password** :
   Identifiants que l'utilisateur saisira pour se connecter au VPN.
2. **Full name** *(facultatif)* :
   Sert uniquement à des fins administratives (nom descriptif dans l'interface).
3. **Certificate (✓)** :
   Cette case permet de générer **automatiquement un certificat utilisateur** lié à ce compte.
   Ce certificat sera nécessaire si l'authentification OpenVPN nécessite un **certificat client**, en plus du mot de passe.



Créer un **certificat numérique** associé à un compte utilisateur local. Ce certificat est utilisé pour établir une connexion VPN **authentifiée et chiffrée**, notamment dans un scénario OpenVPN avec authentification **par certificat client + mot de passe**.

Champ Description

Descriptive name Nom du certificat, visible dans l'interface pfSense (ex : vpn-user-export-cert).

Certificate Authority CA qui va signer le certificat (ici : OpenVPN-CA). Doit être valide et déjà créée.

Key Type / Length RSA 2048 bits – recommandé pour un bon équilibre sécurité/performance.

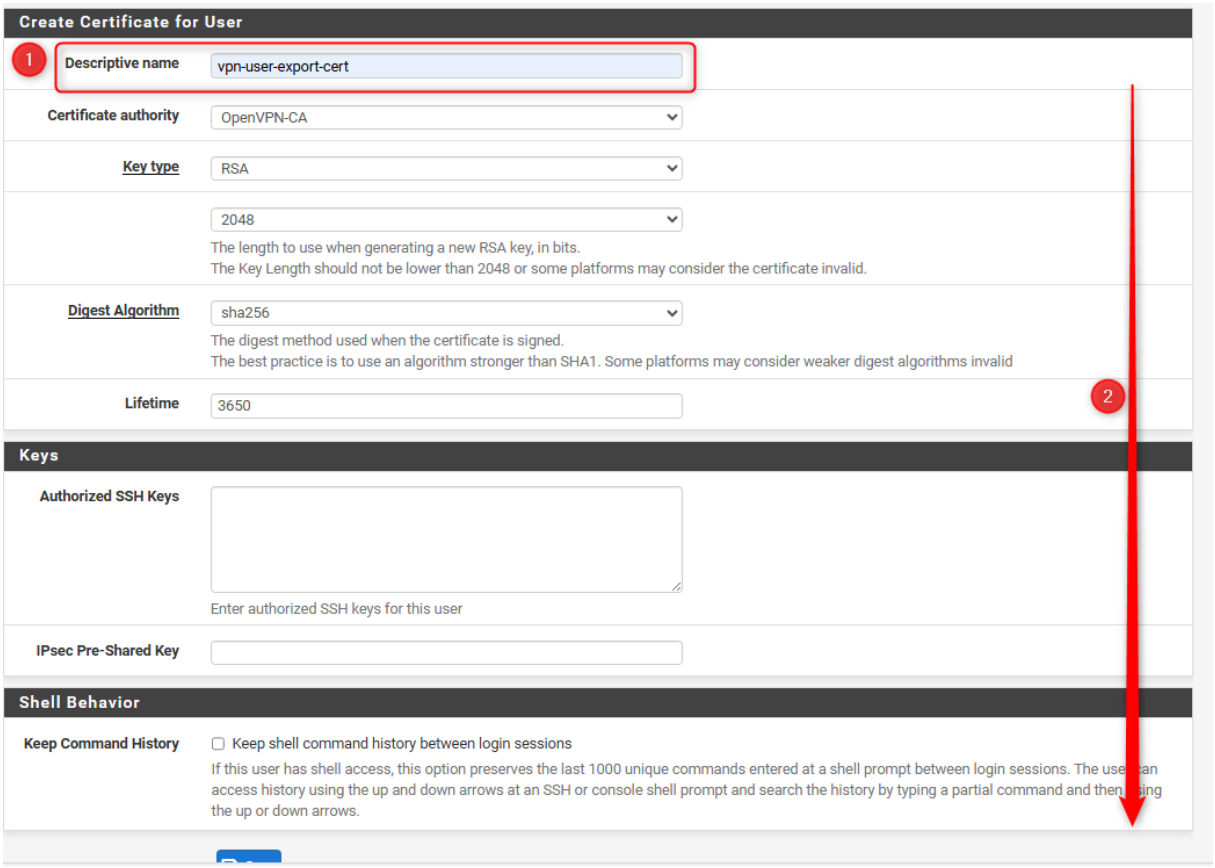
Digest Algorithm SHA256 – recommandé pour garantir l'intégrité de la signature.

Lifetime Durée de validité en jours (ex : 3650 = 10 ans).

Dans notre infrastructure, ce certificat est destiné à l'utilisateur BTRINH, afin qu'il puisse s'authentifier sur le serveur OpenVPN via :

- un **login/mot de passe**,

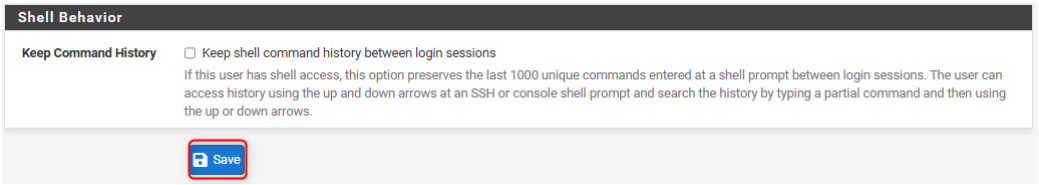
- et un **certificat client personnel**, qui sera exporté par la suite.



Valider l'ensemble des paramètres de l'utilisateur local et **enregistrer le compte**, avec ou sans historique de commandes shell.

Keep Command History :
Cette option est utile uniquement si l'utilisateur accède au shell (via SSH ou console).
Elle permet de **conserver un historique de 1000 commandes** entre les connexions.
Dans la plupart des cas (comme ici, pour un usage VPN), cette option **n'est pas nécessaire**.

Cliquer sur Save

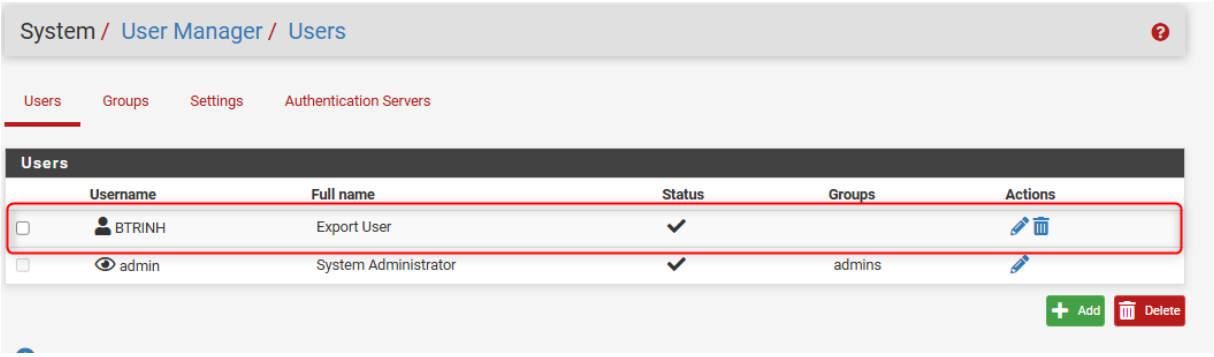


Vérifier que l'utilisateur a bien été ajouté à pfSense et qu'il est actif.

Colonne	Description
Username	Nom d'utilisateur, ici BTRINH
Full Name	Description administrative visible, ici Export User
Status	✓ indique que le compte est **actif** (non désactivé)
Groups	Groupe(s) auquel appartient l'utilisateur (vide ici, ou admins pour le compte admin)
Actions	✏️ Modifier le compte – 🗑️ Supprimer

Ce que cela confirme :

- Le compte est **valide et activé**.
- Le certificat (créé automatiquement) est associé.
- L'utilisateur est prêt pour l'**authentification VPN** si le serveur OpenVPN est configuré pour l'accepter.

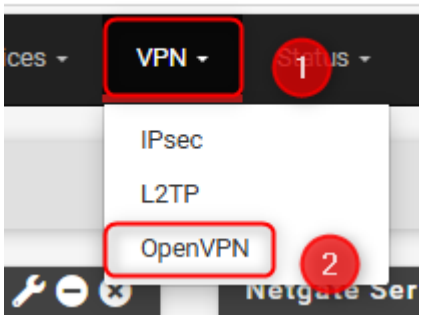


Configuration du VPN

Accéder au menu de gestion d'OpenVPN dans pfSense afin de :

- Créer un **serveur VPN** (mode Road Warrior),
- Gérer les **clients**, **exportations**, ou la **topologie du tunnel**,
- Suivre les connexions et journaux.

(1) Cliquer sur VPN
(2) Cliquer sur OpenVPN

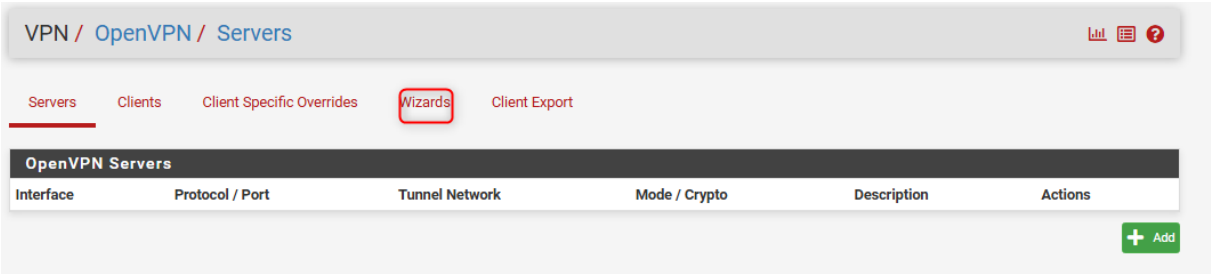


Ce menu donne accès aux différents éléments de configuration :

- **Servers** : pour créer et configurer un serveur OpenVPN (notre objectif ici),
- **Clients** : (si pfSense doit se connecter à un VPN tiers),
- **Client Export** : pour générer les fichiers de configuration .ovpn,
- **Wizard** : assistant de configuration pas-à-pas.

Démarrer l'assistant de création d'un **serveur OpenVPN**.
Cet assistant guide étape par étape la configuration :

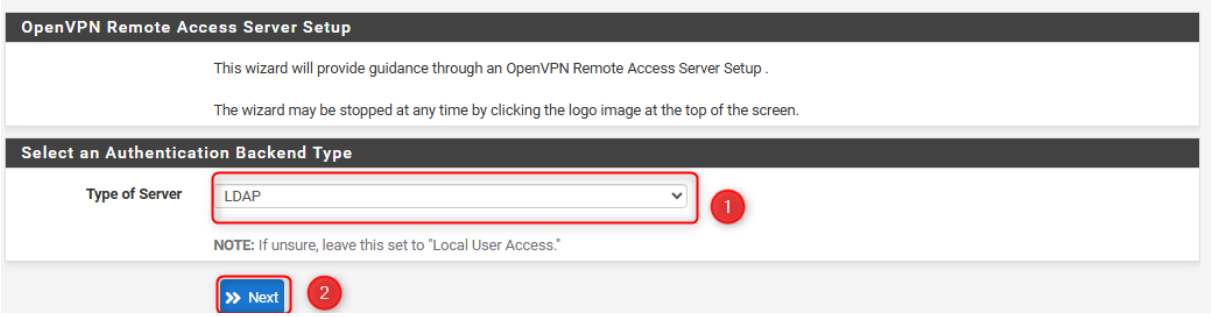
- du certificat serveur,
- de la méthode d'authentification (utilisateur, LDAP...),
- du réseau VPN (adresse, routage...),
- du chiffrement et des options de sécurité.



L'assistant OpenVPN commence par demander le **type de backend d'authentification** à utiliser pour les connexions VPN.
Cette option détermine comment les utilisateurs seront **authentifiés** lors de la tentative de connexion.

Type of Server :
Ce menu déroulant permet de sélectionner la méthode d'authentification parmi :

- Local User Access (comptes internes pfSense),
- LDAP (Active Directory ou autre annuaire compatible),
- RADIUS (serveur d'authentification réseau),
- etc.



Ici, le **type LDAP** est sélectionné, car l'authentification sera **déléguée à un Active Directory** configuré en amont dans pfSense.
Cela permet d'intégrer la solution VPN à l'environnement **de gestion centralisée des identités** de l'organisation.

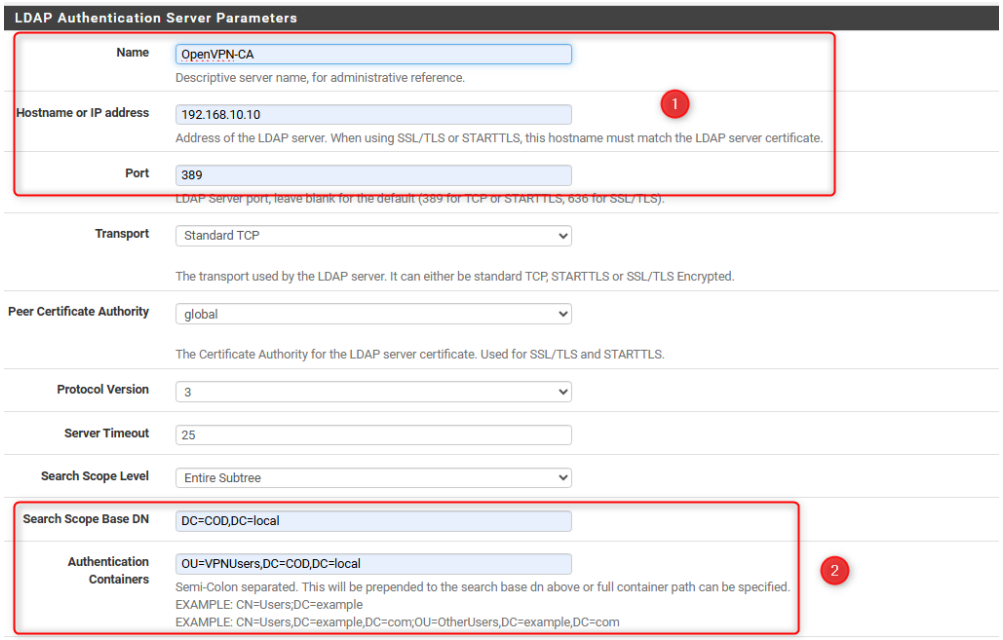
Intérêt d'une authentification LDAP :

- Permet l'utilisation des **comptes utilisateurs déjà existants** dans l'entreprise.
- Évite la duplication des identifiants.
- Renforce la sécurité en unifiant les règles de mot de passe et de politique d'accès.

Configurer la connexion entre pfSense et le **serveur LDAP (Active Directory)**, afin que ce dernier soit utilisé comme **backend d'authentification** pour les utilisateurs VPN.

Champ	Description
Name	Nom administratif de la connexion LDAP (ex. OpenVPN-CA). N'a aucun impact sur le fonctionnement, il sert uniquement à l'identification dans pfSense.
Hostname or IP address	Adresse du serveur Active Directory. Dans ce cas : 192.168.10.10. Ce champ peut contenir un FQDN si la résolution DNS est fonctionnelle.
Port	Port utilisé pour le protocole LDAP. Le port 389 est le port standard pour une connexion LDAP non chiffrée (TCP simple).

hamp	Description
Transport	Définit si la communication avec l'AD se fait en clair (Standard TCP) ou via une connexion sécurisée (STARTTLS, SSL/TLS).
Protocol Version	Version LDAP utilisée, généralement 3.
Search Scope Level	Détermine si la recherche s'effectue uniquement dans un conteneur spécifique ou dans tout l'annuaire (ici Entire Subtree).



Le bon fonctionnement de cette étape dépend :

- D'une **connectivité réseau fonctionnelle** entre pfSense et le serveur AD,
- D'une **configuration correcte du bind DN** (à venir dans l'étape suivante),
- D'un **horodatage synchronisé** entre les deux machines (important avec TLS).

Définir les paramètres d'identification utilisés par pfSense pour :

1. Se connecter au serveur LDAP (via un compte de service),
2. Rechercher et authentifier les utilisateurs.

Champ	Description
LDAP Bind User DN	Identifiant utilisé pour interroger l'annuaire. Ici : btrinh@COD.local, compte de service disposant des droits nécessaires à la lecture LDAP.
LDAP Bind Password	Mot de passe du compte ci-dessus. Il ne s'agit pas d'un compte utilisateur VPN, mais d'un compte technique servant uniquement aux requêtes LDAP.

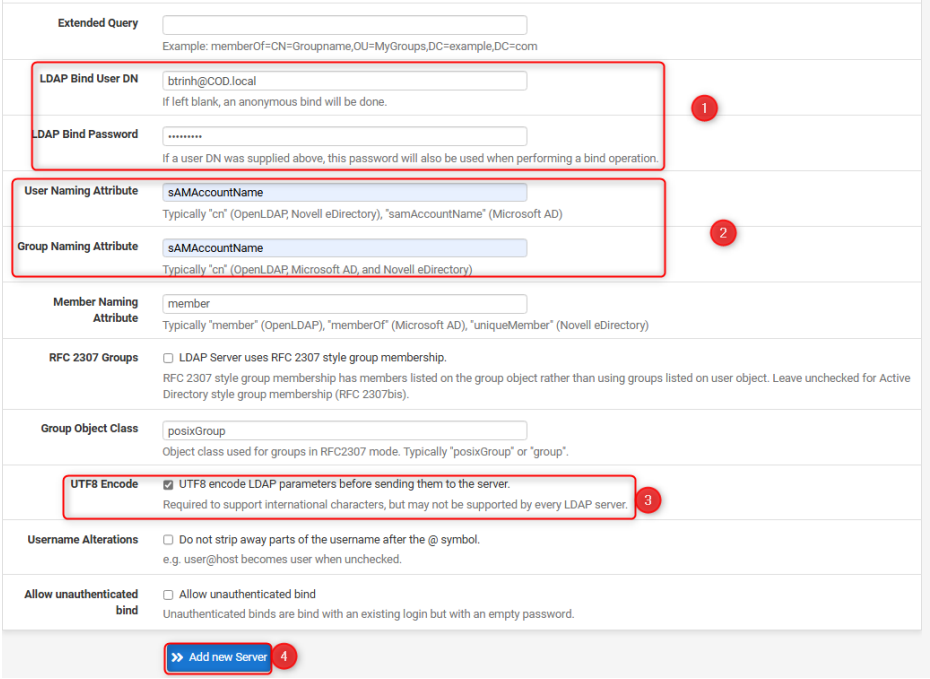
Champ	Description

Attributs d'identification

Champ	Valeur	Rôle
User Naming Attribute	sAMAccountName	C'est l'attribut LDAP correspondant au nom d'utilisateur Windows (ex. : btrinh).
Group Naming Attribute	sAMAccountName	Permet de retrouver les groupes via leur nom NetBIOS/Windows stand

Cliquer sur **Add new Server** permet d'enregistrer le connecteur LDAP dans pfSense. Il pourra ensuite être sélectionné comme **méthode d'authentification** lors de la configuration du serveur OpenVPN.

Ces attributs sont compatibles avec Microsoft Active Directory.



Option	Description
UTF8 Encode	Permet d'encoder les requêtes LDAP en UTF-8. À activer pour gérer correctement les caractères accentués ou spéciaux.

Associer un certificat SSL/TLS valide au service OpenVPN.
Ce certificat est utilisé pour authentifier le serveur auprès des clients et établir une connexion chiffrée.

Champ	Description
Certificate	Sélection du certificat précédemment généré dans pfSense. Ici, le certificat OpenVPN-Server est choisi. Il a été signé par la CA interne OpenVPN-CA.

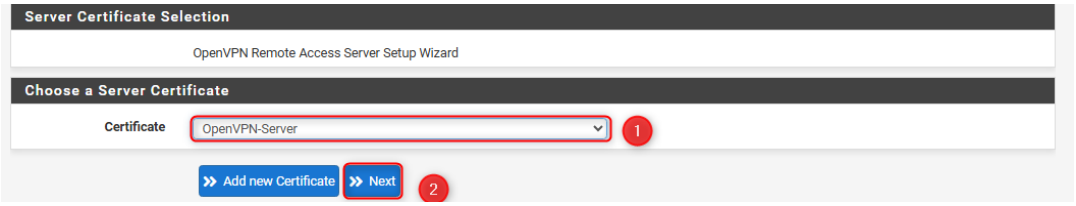
Le certificat permet :

- de garantir l'identité du serveur VPN (évite les attaques de type "man-in-the-middle"),
- d'initier une communication sécurisée avec les clients VPN via le protocole TLS.

Le certificat doit impérativement :

- être de type **Server Certificate**,

- être signé par une **CA de confiance** (en l'occurrence, la CA interne créée au début du projet).



Cliquer sur **Next** pour poursuivre l'assistant et passer à la configuration réseau du tunnel VPN.

Associer au serveur OpenVPN une **autorité de certification (CA)** de confiance, qui a servi ou servira à **signer les certificats client**.

Champ	Description
Certificate Authority	Sélection de la CA interne utilisée dans la configuration. Ici : OpenVPN-CA, créée au début du projet. Elle signe les certificats serveur et client utilisés dans la communication VPN.

Rôle de la CA :

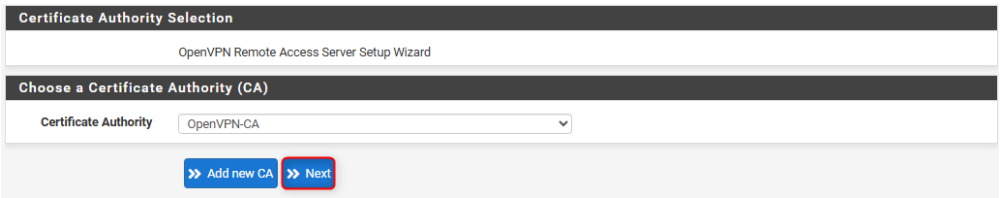
- Elle permet à pfSense (serveur VPN) de **vérifier que les certificats clients présentés sont valides**,
- Elle est **indispensable dans une architecture basée sur TLS** où l'authentification par certificat est active.

Pré-requis :

Avant d'arriver à cette étape, il est impératif d'avoir :

- Créé une **CA interne** (ou importé une CA externe),
- Utilisé cette CA pour signer le **certificat serveur** (et éventuellement les certificats utilisateurs).

Cliquer sur **Next** pour poursuivre l'assistant de configuration OpenVPN, qui enchaînera sur les **paramètres réseau du tunnel**.



Définir l'identifiant administratif du serveur VPN et les **paramètres d'écoute réseau** sur pfSense.
Cela permet de préciser comment le serveur va accepter les connexions des clients.

Détail des champs :

Description

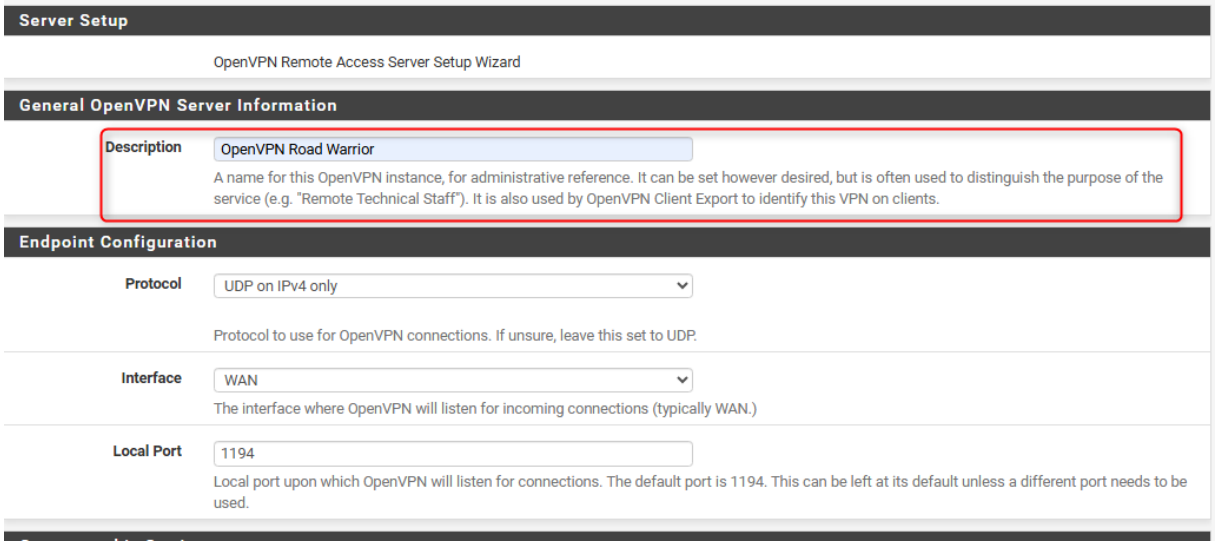
- Nom donné au serveur OpenVPN (ex. : OpenVPN Road Warrior).
- Utilisé à titre **administratif** pour identifier ce service dans pfSense.
- Il est également affiché dans les fichiers générés par le module **OpenVPN Client Export**, facilitant la reconnaissance du profil VPN côté client.

Protocol

- Choix entre **UDP** ou **TCP** pour les connexions VPN.
- Ici : UDP on IPv4 only, recommandé pour les performances (moins de surcharge que TCP).
- 🔹 **Interface**
- Interface réseau sur laquelle pfSense écoutera les connexions VPN entrantes.
- Généralement WAN, sauf dans des cas spécifiques (VPN interne, site à site, etc.).

Local Port

- Port d'écoute du serveur OpenVPN.
- Par défaut : 1194, le port standard du protocole OpenVPN.
- Peut être modifié si un autre service utilise déjà ce port, ou pour des raisons de sécurité (obscurcissement).



Définir les **algorithmes de chiffrement et d'authentification TLS** utilisés par le serveur OpenVPN afin de garantir :

- l'intégrité des communications,
- la confidentialité des données,
- la vérification mutuelle de l'identité des participants.

Paramètre	Description
Protocol	UDP on IPv4 only – recommandé pour ses performances.
Interface	WAN – interface réseau d'écoute pour les connexions VPN.
Local Port	1194 – port standard d'OpenVPN, personnalisable si nécessaire.

Cryptographic Settings :

Paramètre	Description
TLS Authentication	Coche activée → active une couche supplémentaire de sécurité en exigeant une **clé TLS pré-partagée** pour l'authentification du canal TLS. Cela empêche les connexions non autorisées (DoS, scans réseau, etc.).
Generate TLS Key	Permet à pfSense de **générer automatiquement** cette clé TLS.
DH Parameters Length	2048 bits – Longueur des paramètres Diffie-Hellman pour l'échange de clé sécurisé. Valeur recommandée en entreprise (équilibre entre sécurité et performance).

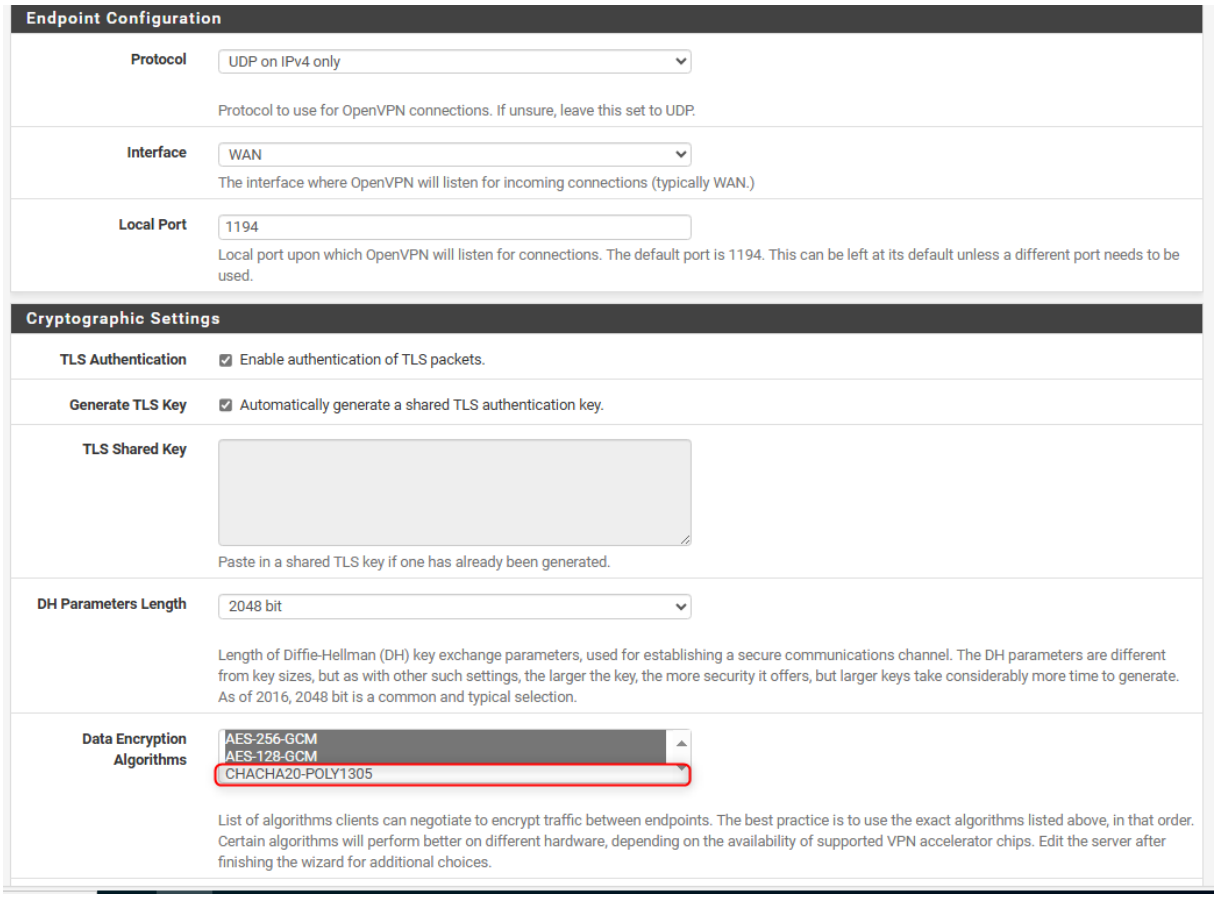
Data Encryption Algorithms :

Ce champ permet de sélectionner les **algorithmes de chiffrement symétrique** négociés avec les clients. Dans cette configuration, trois algorithmes sont proposés :

- **AES-256-GCM** : très sécurisé, recommandé par la plupart des standards actuels.
- **AES-128-GCM** : plus rapide, mais légèrement moins sécurisé.
- **CHACHA20-POLY1305** : performant sur CPU sans accélération matérielle AES.

Bonne pratique : Laisser les trois algorithmes listés dans cet ordre permet aux clients de négocier le plus fort qu'ils supportent.

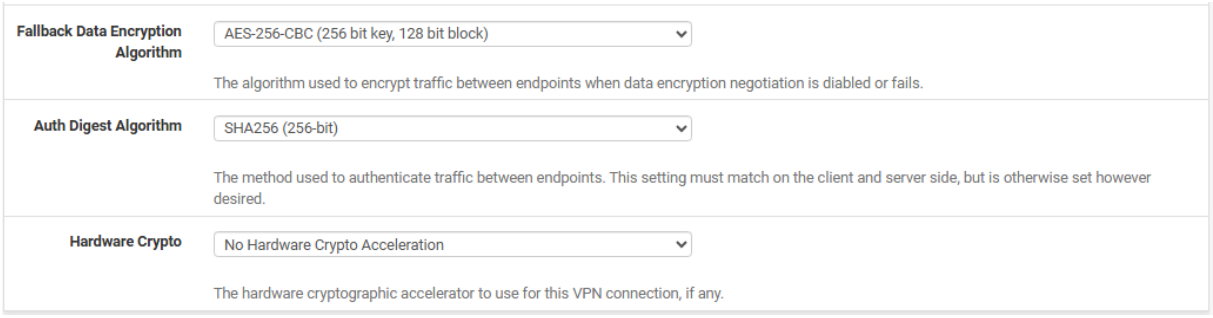
Activer **TLS Authentication** est **fortement recommandé** pour la sécurité.
AES-256-GCM est généralement préféré sauf contraintes matérielles.
La longueur de clé Diffie-Hellman doit être au minimum de 2048 bits pour respecter les politiques de sécurité d'entreprise.



Configurer les **algorithmes de secours**, le **hachage d'authentification** des paquets VPN, et les **ressources matérielles** utilisées pour accélérer le chiffrement.

Détail des paramètres :

Paramètre	Description
Fallback Data Encryption Algorithm	AES-256-CBC : algorithme utilisé **en secours** si la négociation principale échoue. Il offre un chiffrement fort basé sur un bloc de 128 bits avec une clé de 256 bits. Cela garantit que la communication reste chiffrée même dans des conditions de compatibilité dégradée.
Auth Digest Algorithm	SHA256 (256-bit) : algorithme de hachage utilisé pour l'**authentification des messages TLS**. Il permet de vérifier que les données transmises n'ont pas été altérées. Ce paramètre doit être le **même côté client et serveur**.
Hardware Crypto	No Hardware Crypto Acceleration : désactive l'utilisation d'un **accélérateur cryptographique matériel**. Ce choix est adapté si le matériel ne dispose pas d'un moteur de chiffrement compatible (comme AES-NI sur les processeurs Intel). Sur un serveur de production, l'activation peut améliorer les performances.



Définir la **topologie réseau du VPN**, c'est-à-dire :

- le réseau attribué aux clients VPN (Tunnel Network),
- le réseau local à atteindre via le tunnel (Local Network),
- les limitations de connexion et les options de sécurité complémentaires.

Pv4 Tunnel Network

Valeur : 10.8.0.0/24
Ce champ définit le **réseau IP virtuel utilisé pour les connexions VPN**.

- La première adresse (ex. 10.8.0.1) sera assignée au serveur VPN.
- Les adresses suivantes seront distribuées aux clients VPN.
- Ce réseau ne doit pas être en conflit avec le LAN ou d'autres sous-réseaux déjà en place.

IPv4 Local Network

Valeur : 192.168.10.0/24
Il s'agit du **réseau interne (LAN)** que les clients VPN pourront atteindre une fois connectés.

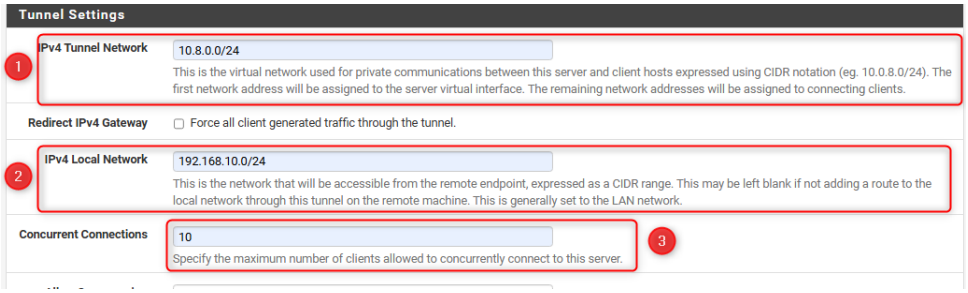
- Cela permet aux clients d'accéder aux **ressources internes de l'entreprise** (serveurs, imprimantes, NAS, etc.).
- Cette route est automatiquement poussée vers les clients lors de l'établissement du tunnel.

Concurrent Connections

Valeur : 10
Définit le **nombre maximum de clients** autorisés à se connecter simultanément à ce serveur OpenVPN.

- Cette limitation peut être adaptée en fonction des besoins et des capacités de l'infrastructure.

- Elle est utile pour contrôler l'accès ou prévenir la surcharge.



Une fois ces paramètres définis, l'assistant poursuivra avec la configuration des options DNS/DHCP poussées aux clients.

Définir les paramètres de **résolution de noms (DNS)**, **synchronisation horaire (NTP)** et éventuellement **NetBIOS**, transmis aux clients VPN lors de leur connexion.

Détail des champs principaux :

DNS Default Domain

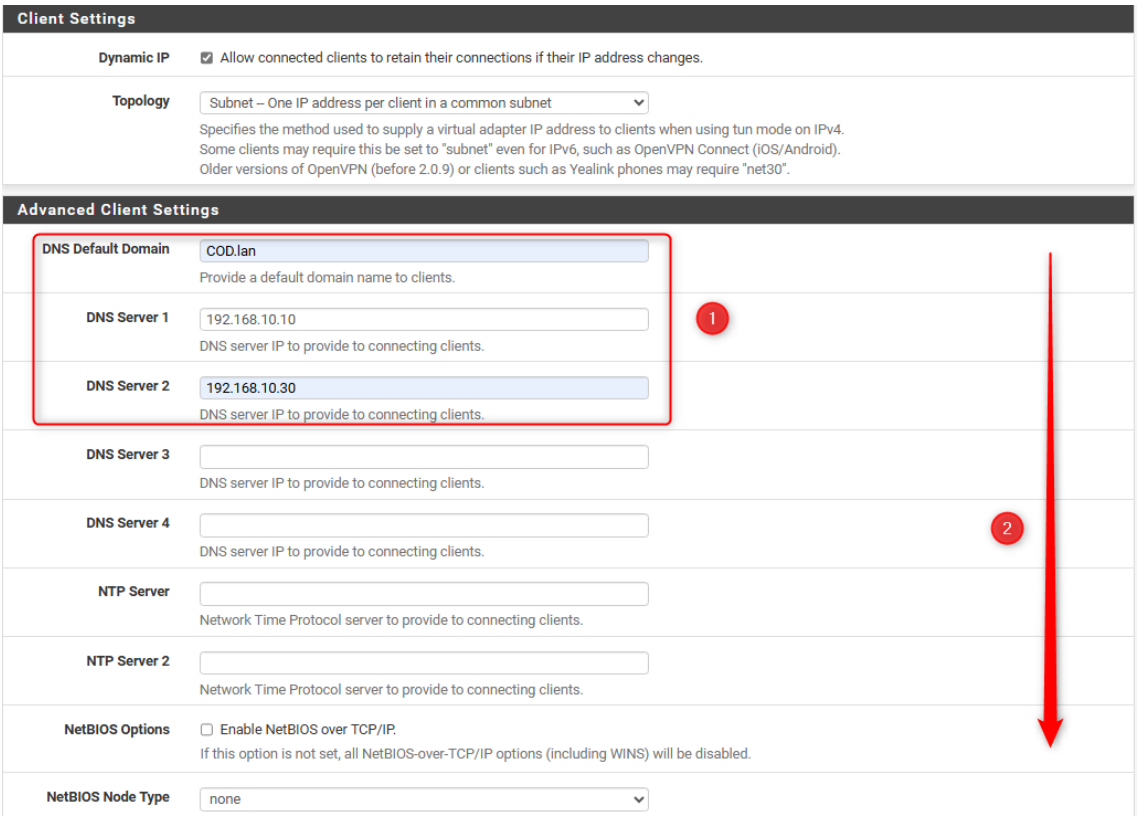
Valeur : COD.lan

- Ce champ permet d'attribuer un **suffixe DNS** par défaut aux clients.
- Cela facilite la résolution de noms internes : un client pourra par exemple pinguer serveur1 au lieu de serveur1.COD.lan.

NS Server 1 & DNS Server 2

Valeurs : 192.168.10.10 et 192.168.10.30

- Ces adresses pointent généralement vers les **contrôleurs de domaine Active Directory** disposant du rôle **DNS**.
- Elles permettent aux clients VPN de :
    - résoudre les noms internes (ordinateurs, serveurs, imprimantes),
    - joindre les ressources internes comme s'ils étaient physiquement présents sur le réseau local.



Ces paramètres assurent aux clients VPN une **expérience réseau équivalente à celle d'un poste local**, avec accès direct aux ressources internes grâce à la résolution DNS et au routage configuré précédemment.

Créer les **règles de pare-feu** indispensables pour :

- -Permettre l'établissement de la connexion VPN depuis Internet,
- Autoriser le trafic interne des clients à travers le tunnel VPN.
- **Firewall Rule – Traffic from clients to server**
- Coche activée
- Ajoute une règle sur l'interface **WAN** autorisant l'accès au **port du serveur OpenVPN** (par défaut : UDP 1194).
- Sans cette règle, **aucun client ne pourra initier de connexion VPN** depuis l'extérieur.

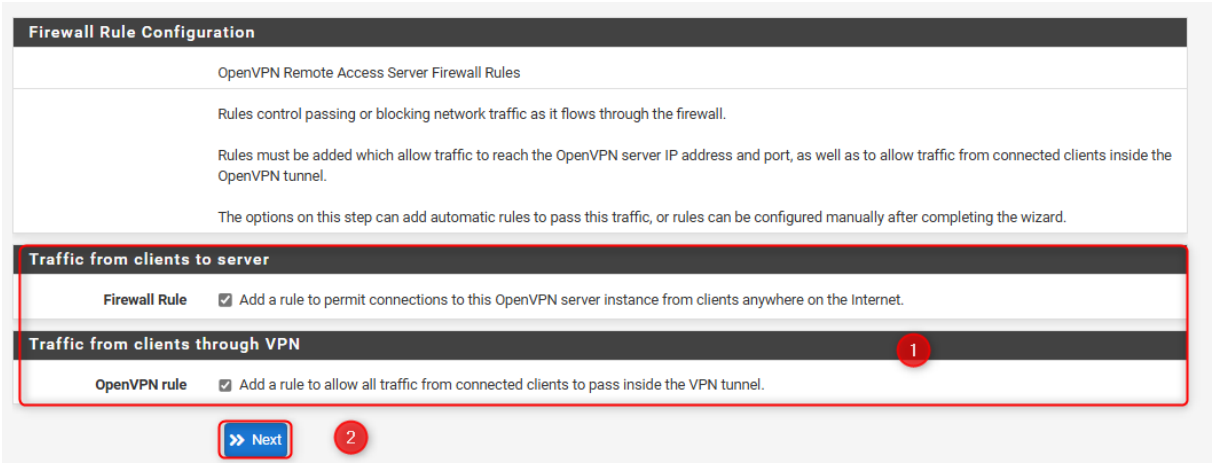
OpenVPN Rule – Traffic from clients through VPN

- Coche activée ✅
- Ajoute une règle sur l'interface **OpenVPN** autorisant **tout le trafic sortant** des clients VPN vers le réseau local.
- Sans cette règle, les clients VPN pourront se connecter au serveur, mais **ne pourront pas accéder aux ressources internes** (réseau, DNS, fichiers, etc.).

Remarques importantes :

- Ces règles peuvent être **modifiées manuellement** après l'assistant pour affiner la sécurité (ex. : filtrer certains protocoles ou IP).

- Il est essentiel de **limiter les accès** dans un environnement de production (principe du moindre privilège).

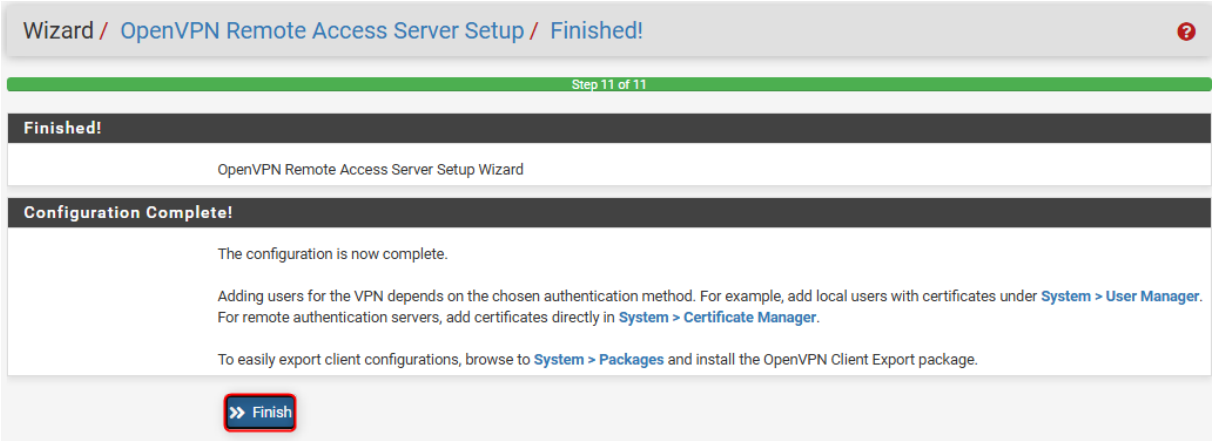


Cliquer sur **Next** permet de terminer la configuration du serveur VPN, avec les règles de pare-feu ajoutées automatiquement.

Afficher un message de confirmation indiquant que **le serveur OpenVPN est maintenant opérationnel**, et rappeler les prochaines actions possibles (ajout d'utilisateurs, export des clients, etc.).

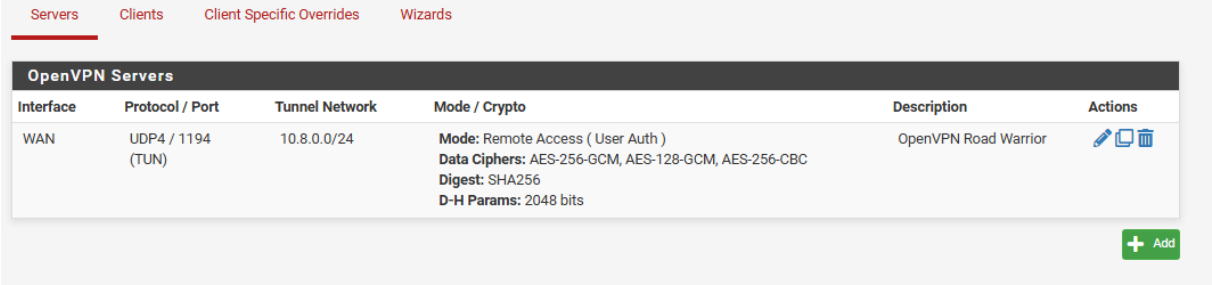
Résultat de la configuration :

- Le **serveur VPN est actif** sur l'interface WAN, prêt à recevoir des connexions.
- Les **règles de pare-feu** ont été générées automatiquement pour autoriser le trafic entrant et sortant.
- Les **certificats** (serveur et utilisateurs) sont correctement liés à la CA interne.
- La **méthode d'authentification LDAP** permet de sécuriser les accès en s'appuyant sur un **Active Directory** déjà en place.



Cliquer sur Finis pour passer à la prochaine étape

Afficher un **récapitulatif technique** de l'instance OpenVPN active. Cette vue permet de contrôler les paramètres essentiels du serveur VPN et d'accéder aux fonctions de gestion (édition, duplication, suppression).



Cette vue confirme que le **serveur OpenVPN est actif, sécurisé et prêt à être utilisé** par des utilisateurs distants. Il constitue désormais un **point d'entrée sécurisé** au réseau interne de l'organisation, tout en s'intégrant à l'infrastructure Active Directory existante via LDAP.

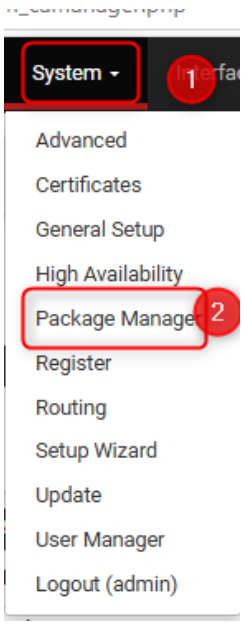
Installation module exportation du client VPN

Accéder au **Package Manager** de pfSense afin d'installer un **module tiers** : openvpn-client-export.
Ce package facilite considérablement la génération des profils. ovpn nécessaires à la connexion des clients VPN.

Fonction du Package Manager :

Le gestionnaire de paquets de pfSense permet :

- D'installer des **extensions officielles** pour étendre les fonctionnalités,
- De maintenir ces packages à jour,
- De désinstaller ceux devenus inutiles.



Accéder à l'onglet **Available Packages**, rechercher **openvpn-client-export**, puis procéder à son installation.
Tu peux m'envoyer cette prochaine capture, et je continuerai dans le même ton technique et structuré.

Rechercher et installer le **module d'exportation des clients OpenVPN** depuis le gestionnaire de paquets de pfSense. Ce module permet de :

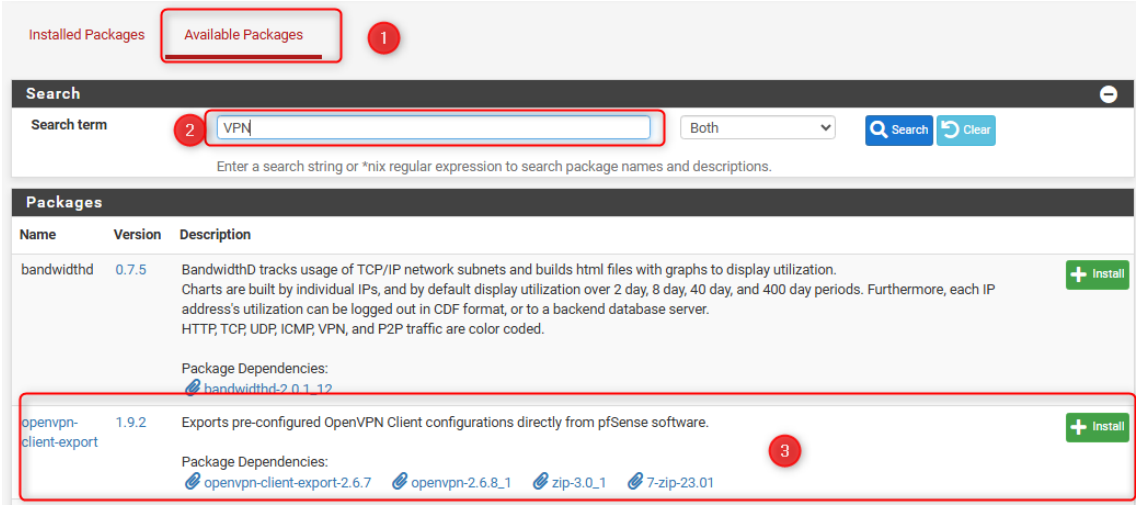
- Générer facilement les fichiers de configuration .ovpn,
- Créer des installeurs Windows auto-configurés,
- Exporter des profils adaptés aux systèmes Windows, macOS, Linux, Android et iOS.

Onglet : `Available Packages`
Accès à tous les packages installables depuis pfSense.

(1) **Onglet** : Available Packages
Accès à tous les packages installables depuis pfSense.
(2) **Recherche** : "VPN"
Permet de filtrer les paquets liés aux technologies VPN. Ici, on cible **openvpn-client-export**.
(3) **Package identifié** :

- **Nom** : openvpn-client-export
- **Version** : 1.9.2 (dans cet exemple)

- **Description** : "Exports pre-configured OpenVPN Client configurations directly from pfSense software."
- Cliquez sur **Install** pour lancer l'installation.



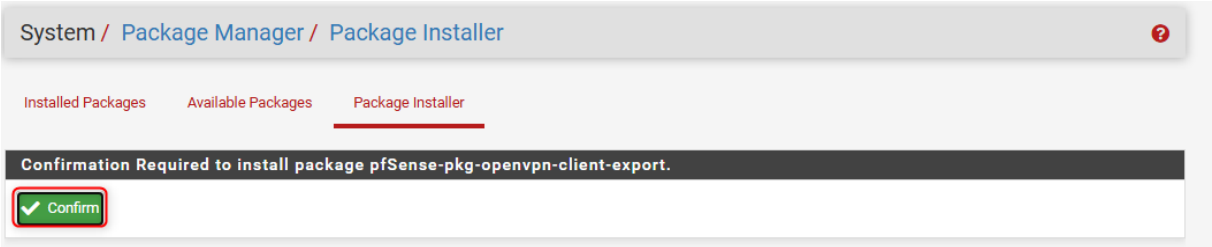
Fonctionnalités principales du module :

- Export de fichiers .ovpn prêts à l'emploi,
- Création d'exécutables pour installation rapide sur Windows (.exe),
- Inclusion des certificats, options de chiffrement et serveurs DNS,
- Options de personnalisation (authentification, interface, compression...).

Valider l'installation du package d'exportation de clients VPN. Cette confirmation déclenche le **téléchargement** et **l'installation automatique** du package et de ses dépendances.

Cliquer sur le bouton **Confirm** permet à pfSense de :

- télécharger le package depuis ses dépôts officiels,
- vérifier son intégrité,
- l'intégrer à l'interface Web.



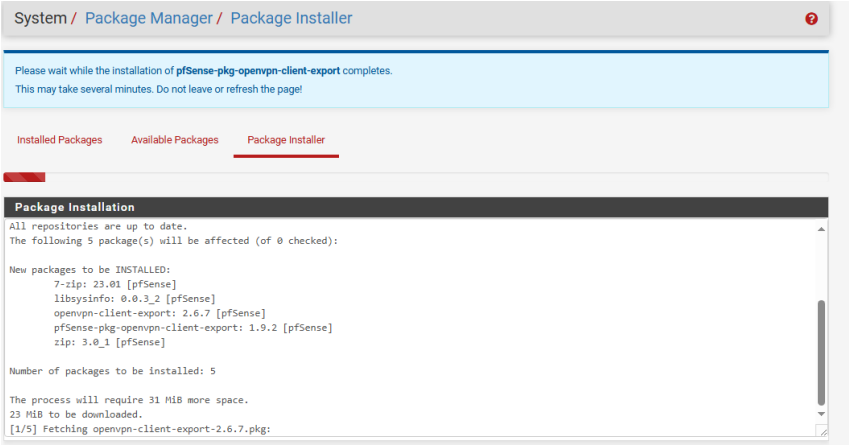
Afficher l'état d'avancement du **téléchargement et de l'installation** des composants nécessaires au bon fonctionnement du module d'export.
Les paquets suivants sont installés :

- **openvpn-client-export** (version 1.9.2) : cœur du module d'exportation.
- **7-zip** : utilisé pour compresser certains fichiers d'installation.

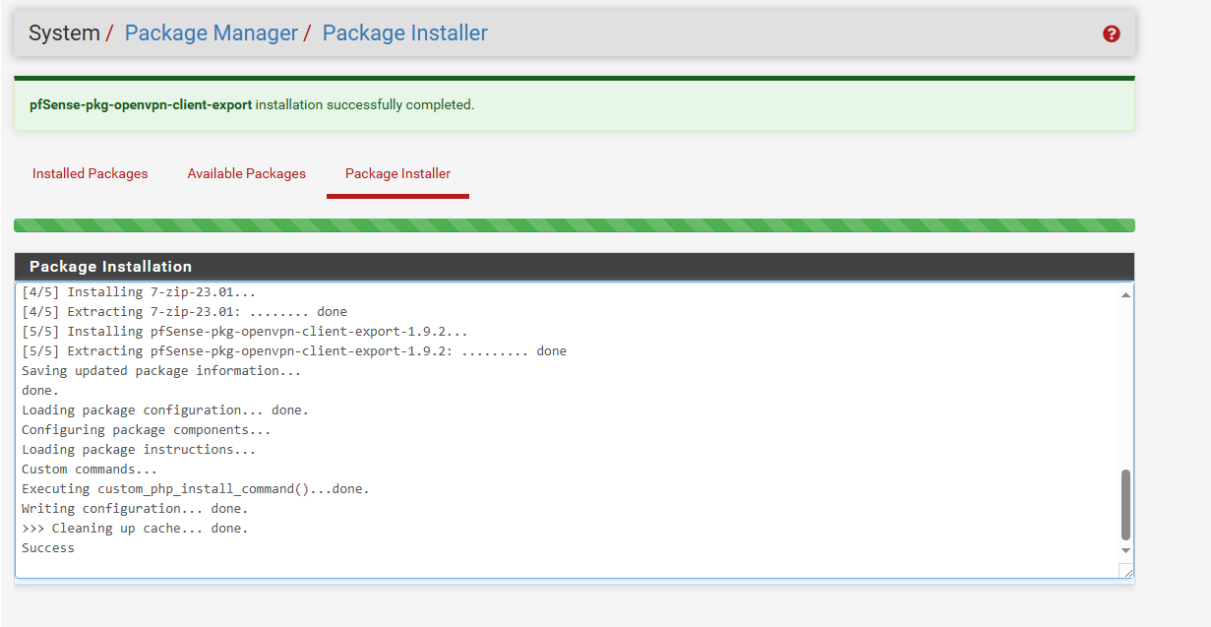
- zip, libsysinfo, openvpn-client-export-2.6.7 : dépendances internes.

Le message indique :

- 5 paquets à installer,
- 31 MiB d'espace requis,
- L'opération est en cours (étape 1 sur 5).



Le package est désormais opérationnel, comme l'indique le message :



Vérification règles Firewall

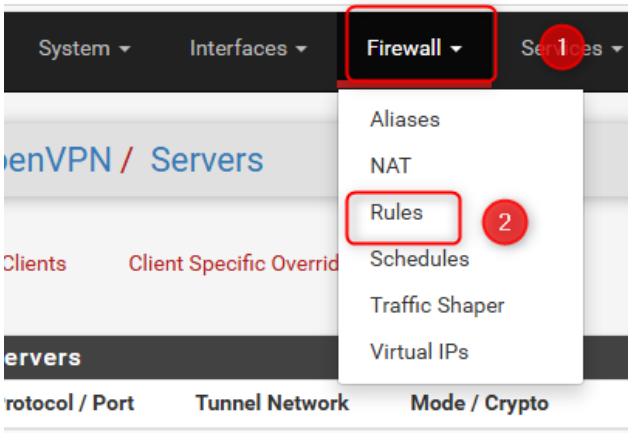
Afficher, modifier ou ajouter des règles de filtrage réseau dans pfSense, pour :

- Autoriser le trafic VPN entrant (depuis WAN),
- Contrôler le trafic entre les clients VPN et les ressources internes,

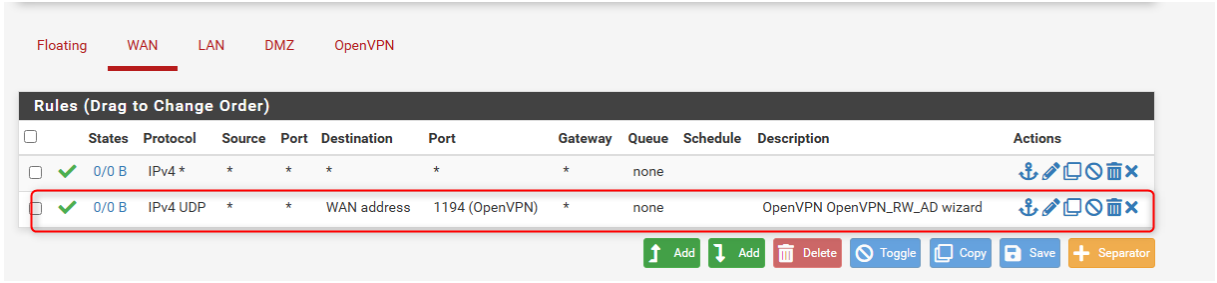
- Appliquer des **restrictions de sécurité supplémentaires** (ex. : bloquer certains ports, limiter à certaines IP...).

Même si l'assistant OpenVPN peut les créer automatiquement, une **revue manuelle** permet de :

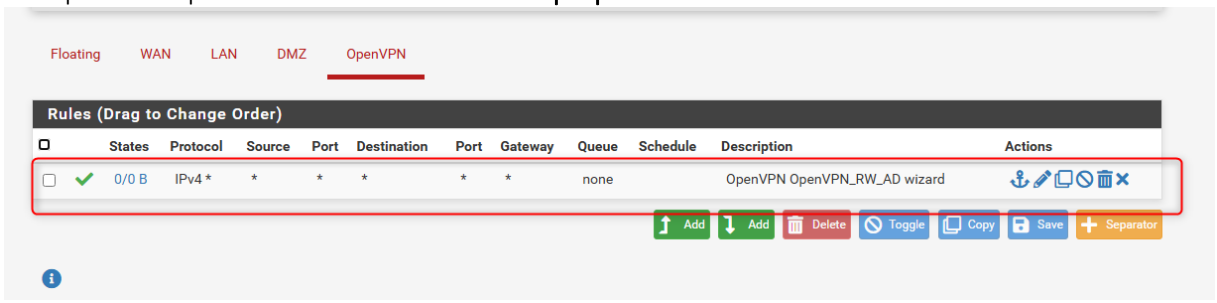
- Affiner les **droits d'accès** des utilisateurs VPN,
- Appliquer le **principe du moindre privilège**,
- Garantir une **conformité** avec la politique de sécurité de l'entreprise.



Sans cette autorisation, **aucun client externe** ne pourra initier de connexion VPN.
Le port 1194 en UDP est celui par défaut d'OpenVPN, mais peut être modifié en fonction de la configuration.



Permettre aux **utilisateurs connectés via le VPN** d'émettre du trafic vers le réseau interne. Cette règle est indispensable pour **autoriser le transit des paquets** à l'intérieur du tunnel VPN.

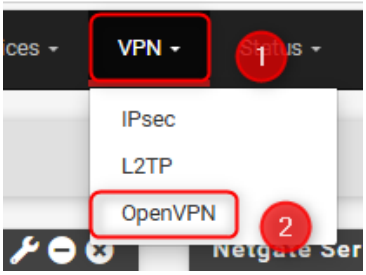


- Cette règle permet aux **clients VPN** d'accéder aux ressources du réseau local (ex. : serveurs AD, partages, messagerie...).
- Elle autorise **tout le trafic sortant**, ce qui est pratique en environnement de test ou lors d'une configuration initiale.

Configuration du client de l'exportation

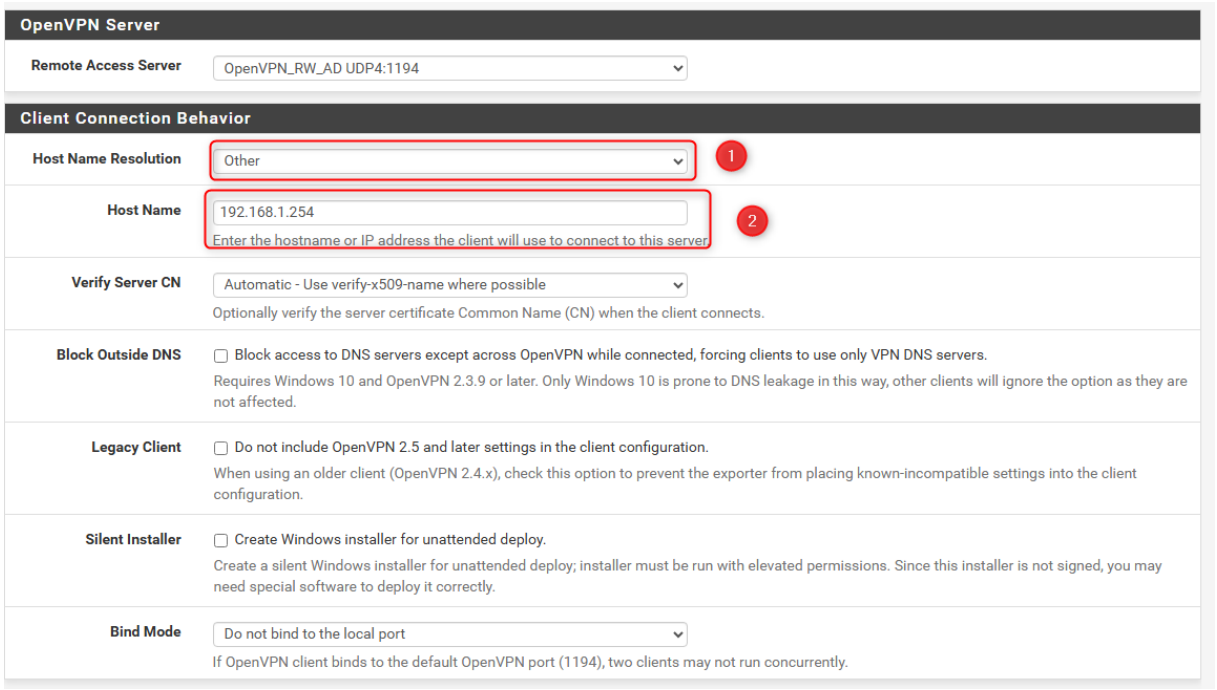
Accéder à toutes les fonctionnalités liées à OpenVPN dans pfSense, notamment :

- La gestion des **serveurs** VPN,
- La configuration des **clients** (client-to-site),
- Les exports via l'onglet **Client Export** (visible après installation du package).



Définir les options de connexion que le fichier .ovpn ou l'installeur OpenVPN utilisera lors du **déploiement sur les postes clients**.

Option	Description
Remote Access Server	Sélection du serveur OpenVPN à utiliser (ici OpenVPN_RW_AD UDP4:1194).
Host Name Resolution	Permet de spécifier l'adresse publique ou IP locale utilisée par les clients pour se connecter.
Host Name	Dans notre cas : 192.168.1.254 – c'est l'IP publique (ou IP NATée) du pare-feu **vue depuis l'extérieur**.
Verify Server CN	Vérifie le nom commun (CN) du certificat serveur – utile pour sécuriser la connexion.
Silent Installer	Génère un exécutable Windows prêt à installer sans intervention de l'utilisateur.
Block Outside DNS	Empêche les fuites DNS en forçant l'usage des DNS internes VPN.
Bind Mode	Contrôle si le client doit lier le port local (optionnel).



Définir les **paramètres de stockage, chiffrement et sécurité** des certificats et profils VPN à destination des utilisateurs finaux.

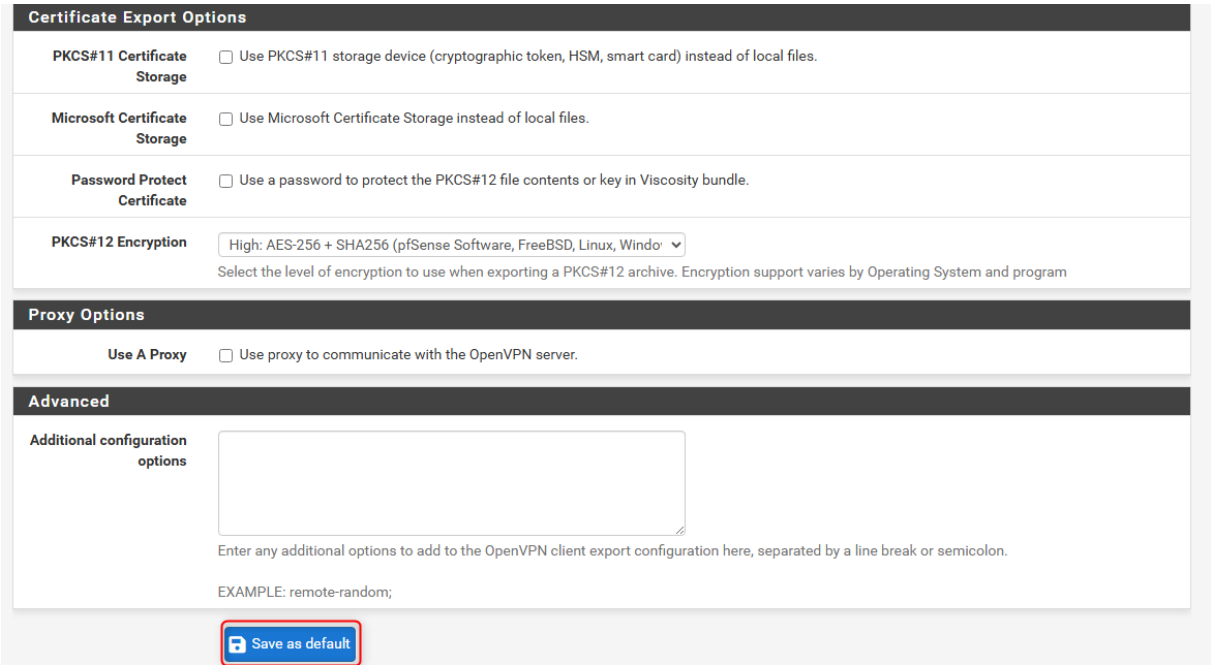
Option	Fonction
PKCS#11 Certificate Storage	Permet l'usage de **tokens matériels** (HSM, cartes à puce) pour sécuriser le certificat client.
Microsoft Certificate Storage	Stocke le certificat dans le **magasin de certificats Windows**, utile pour l'intégration système.
Password Protect Certificate	Protège le certificat PKCS#12 avec un mot de passe. Recommandé pour les profils sensibles.

PKCS#12 Encryption Niveau de chiffrement pour le bundle client (ex. : **AES-256 + SHA256**, recommandé).

Use a Proxy Active l'usage d'un **proxy réseau** pour les clients OpenVPN.

Additional configuration options	Ajoute des options personnalisées au fichier .ovpn (ex. : remote-random, route-delay, etc.).

Save as default Enregistre ces paramètres comme configuration par défaut pour tous les exports futurs.

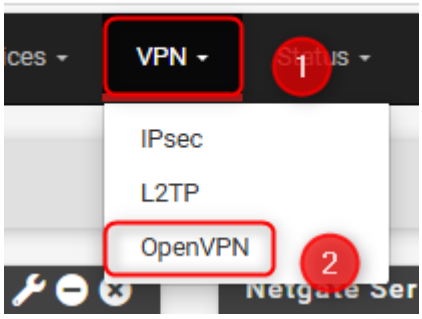


Cliquer sur Save as default

Exportation du client OPenVPN

Ouvrir le panneau de gestion OpenVPN dans pfSense pour :

- Vérifier l'état du serveur VPN,
- Accéder à l'onglet **Client Export**,
- Télécharger les profils VPN générés automatiquement pour chaque utilisateur ayant un certificat valide.

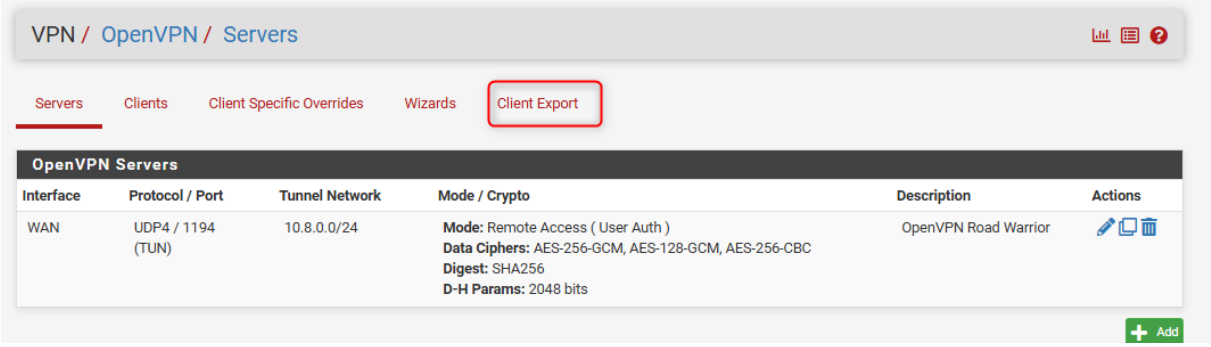


L'onglet **Client Export** est désormais visible grâce à l'installation du package openvpn-client-export.

Il permet de générer :

- Un fichier .ovpn (configuration brute),
- Un .exe (installeur Windows auto-configuré),
- Une archive .zip (certificat + clé + profil),

- Des profils compatibles **OpenVPN Connect**, **Viscosity**, **Tunnelblick** ou encore **Linux NetworkManager**.



Cliquer sur Client Export
Permettre aux utilisateurs de **télécharger leur configuration OpenVPN prête à l'emploi**, selon leur système d'exploitation et méthode de déploiement.

Inline Configurations

Ces formats embarquent tous les éléments (certificat, clé, paramètres) dans un seul fichier .ovpn.

- Most Clients : Fichier .ovpn standard pour Windows/Linux/Mac.
- Android : Adapté aux applications mobiles comme **OpenVPN for Android**.
- OpenVPN Connect (iOS/Android) : Compatible avec l'application officielle **OpenVPN Connect**.

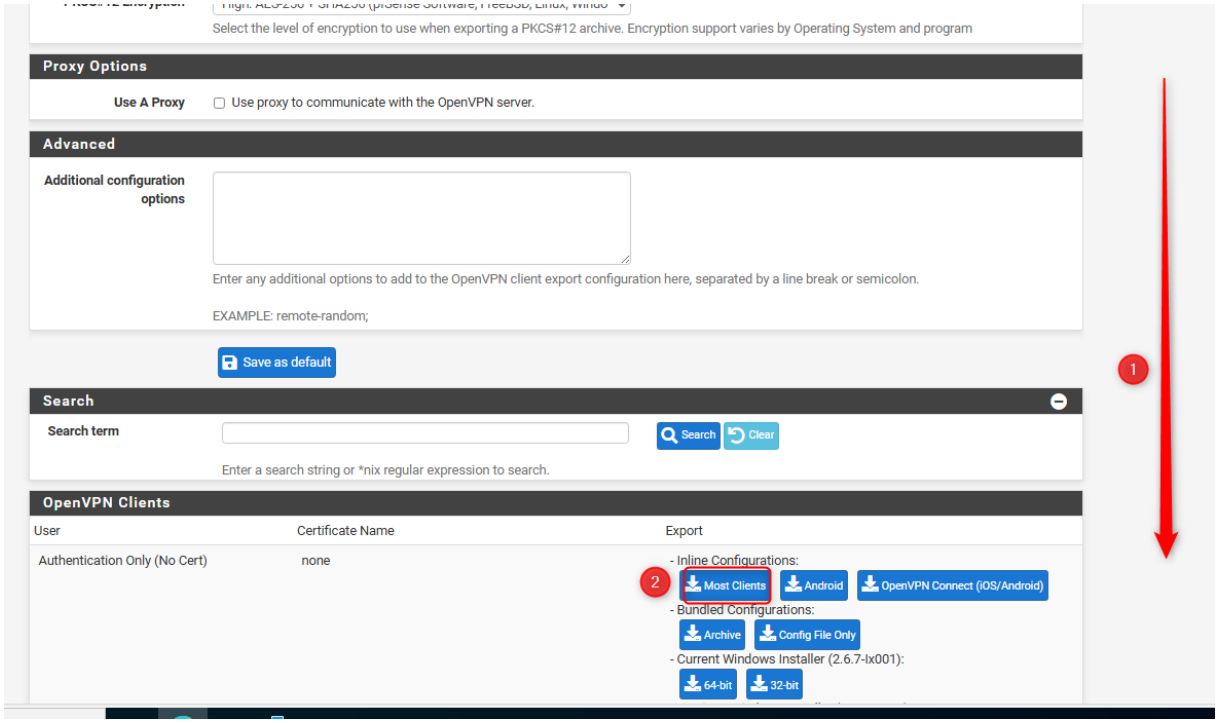
Bundled Configurations

Ces options séparent ou regroupent les fichiers nécessaires :

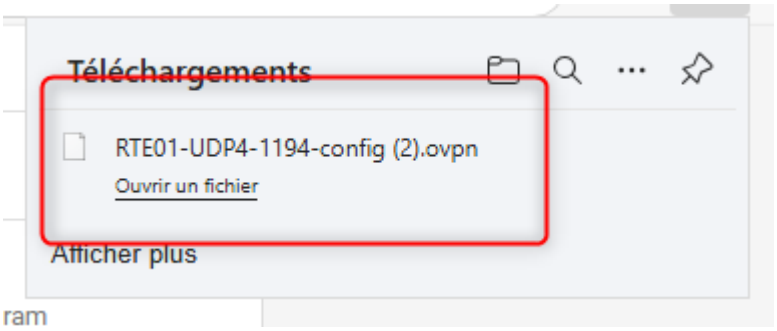
- Archive (.zip) : Contient le .ovpn, les certificats, les clés.
- Config File Only : Le fichier .ovpn seul, sans certificat séparé.

Windows Installer

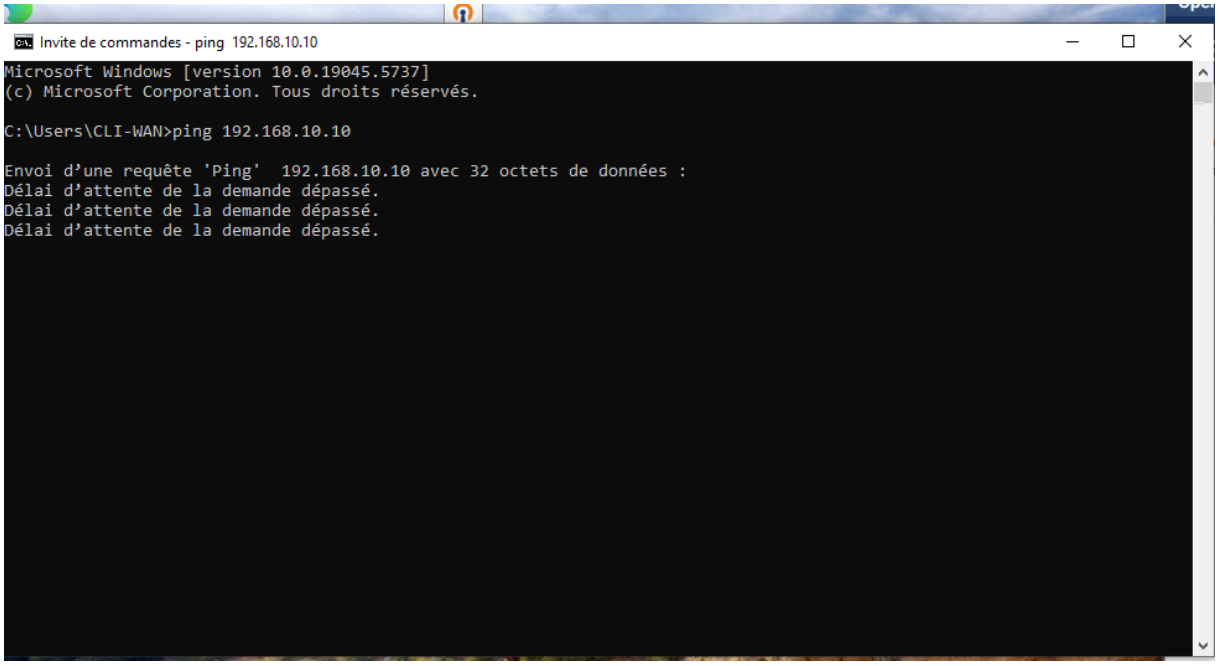
- 64-bit / 32-bit : Installeur Windows préconfiguré pour l'utilisateur (inclut tous les éléments dans un .exe autonome).
- L'utilisateur peut choisir le format de configuration le plus adapté.
- L'administrateur peut fournir un fichier sécurisé et immédiatement fonctionnel.



Cliquer sur Most client pour exporter la configuration
Ce fichier .ovpn contient **tous les paramètres nécessaires à la connexion** VPN via un client OpenVPN (Windows, Linux, macOS, Android, iOS...).



Dans ce contexte, le client tente de joindre un hôte du réseau interne via le tunnel VPN, mais la tentative échoue avec le message suivant :
Délai d'attente de la demande dépassé.
Cela s'explique de manière logique et attendue par le fait que **la configuration OpenVPN n'est pas encore finalisée** et que le **client distant n'est pas encore connecté au réseau VPN**, ni intégré au sous-réseau local géré par le routeur pfSense.
À ce stade de la mise en place, il est normal que le client distant ne puisse pas accéder aux ressources internes (comme le serveur Active Directory). La connectivité réseau ne sera possible **qu'une fois la configuration du serveur OpenVPN activée**, que le client se connecte correctement au service VPN, et que les **règles de pare-feu** ainsi que les **routes réseau** soient appliquées.



Étape préalable : téléchargement et installation du client

Avant d'accéder à cette interface, il est nécessaire de **télécharger et installer le client officiel OpenVPN Connect** sur le poste utilisateur. Ce logiciel permet d'importer un fichier de configuration et d'établir une connexion VPN vers un serveur distant.

Lien de téléchargement officiel :
https://openvpn.net/client-connect-vpn-for-windows/

Procédure d'installation :

1. Accéder au lien ci-dessus à l'aide d'un navigateur Internet.
2. Télécharger la version du client correspondant au système d'exploitation utilisé.
3. Lancer le fichier exécutable (.exe) téléchargé.
4. Suivre l'assistant d'installation par défaut jusqu'à la fin.

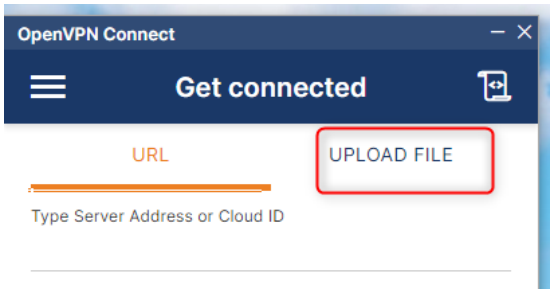
Interface de connexion – Premier lancement

Une fois le client OpenVPN Connect installé et lancé, l'interface ci-dessus s'affiche. Elle propose deux méthodes de connexion :

- **URL** : saisie manuelle de l'adresse d'un serveur ou d'un ID cloud (non utilisée dans notre cas),
- **UPLOAD FILE** : **importation d'un fichier de configuration .ovpn**, fourni par l'administrateur réseau.

Dans notre cas, cliquer sur l'onglet **"UPLOAD FILE"**, afin de procéder à l'importation du fichier généré depuis pfSense. Ce fichier contient l'ensemble des informations nécessaires à la connexion sécurisée au serveur VPN (certificats, IP, port, mode d'authentification, etc.).

Cliquer sur Upload File



Étape : ajout du profil VPN dans OpenVPN Connect

Une fois le client OpenVPN Connect lancé et l'onglet **"UPLOAD FILE"** sélectionné, il est possible d'importer le profil de connexion au serveur VPN.

Pour cela, effectuer un **glisser-déposer** du fichier .ovpn précédemment généré sur le bureau (dans notre cas : RTE01-UDP4-1194-config.ovpn) vers la zone centrale de l'interface, comme illustré ci-dessus.

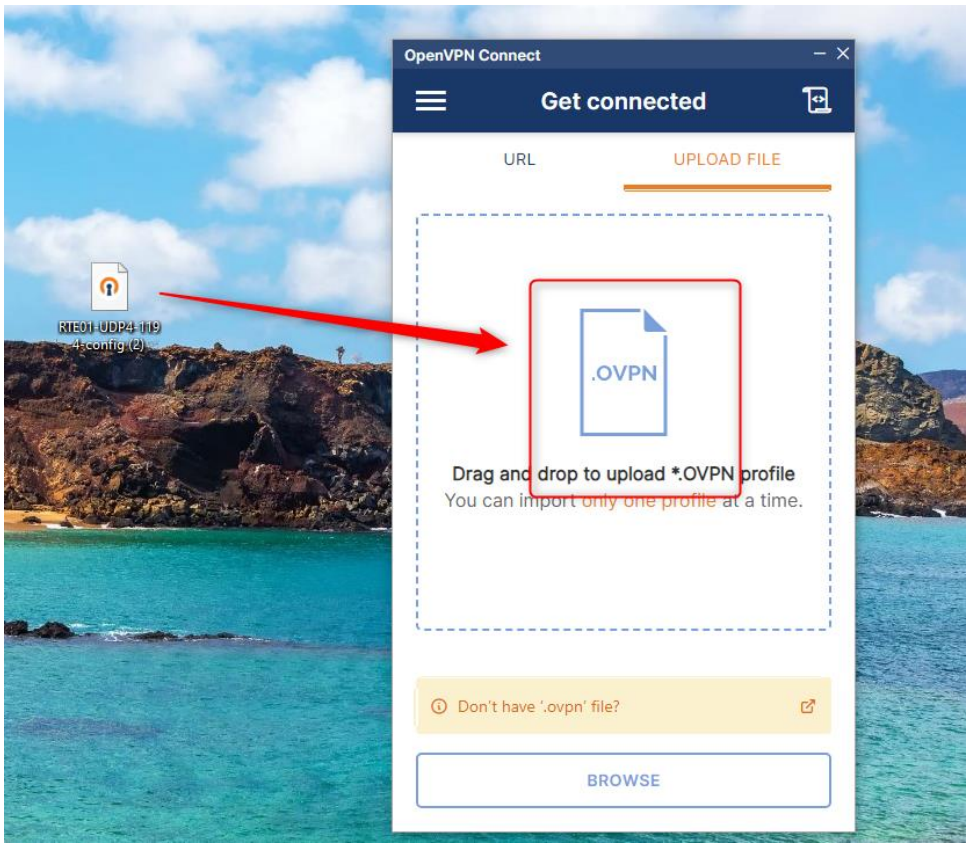
🔎 Le fichier .ovpn contient l'ensemble des paramètres nécessaires pour établir une session VPN :

- L'adresse IP et le port du serveur distant,
- Les certificats d'authentification,
- Le mode de chiffrement et d'encapsulation,
- Les routes à appliquer une fois la connexion établie.

Remarque : un seul fichier .ovpn peut être importé à la fois.

Une fois le fichier déposé, le client OpenVPN Connect propose automatiquement de passer à l'étape de connexion en affichant un bouton **"Connect"**. Cette opération permet de tester la liaison avec le serveur VPN configuré sur pfSense.

Étape :



authentification de l'utilisateur

Une fois le fichier de configuration .ovpn importé dans le client **OpenVPN Connect**, la fenêtre **"Imported Profile"** s'affiche automatiquement. Celle-ci contient deux champs essentiels pour la phase d'authentification :

- **Server Hostname** : affiche l'adresse IP ou le nom DNS du serveur VPN (ici, 192.168.1.251). Cette valeur est verrouillée car elle provient du fichier de configuration.
- **Username** : ce champ doit être complété avec les **identifiants d'un utilisateur du domaine Active Directory**.

Dans notre cas :

Le nom d'utilisateur sera par exemple BTRINH, comme défini précédemment dans le gestionnaire d'utilisateurs de pfSense.

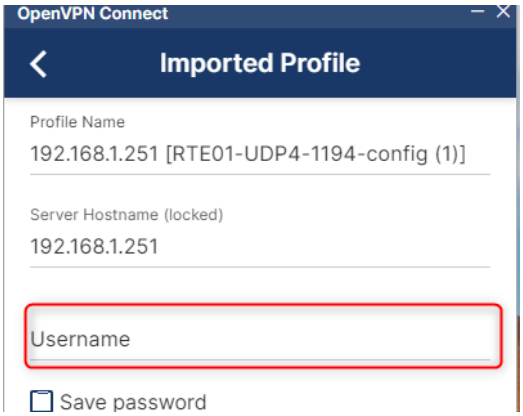
Il est également possible de cocher la case **"Save password"** si l'on souhaite que le mot de passe soit mémorisé pour les connexions futures (non recommandé sur des postes partagés ou sensibles).

Finaliser la connexion

Une fois les informations saisies, cliquer sur le bouton **"CONNECT"** afin d'établir la connexion VPN.

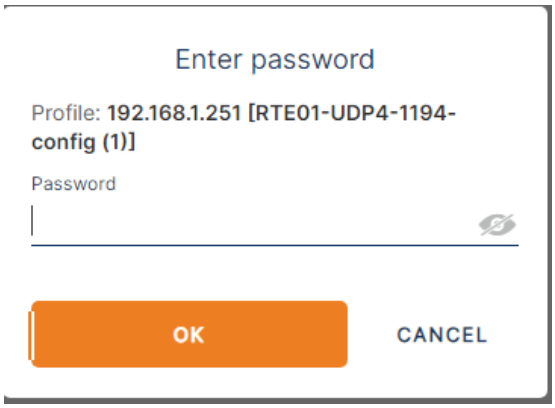
Le client initiera alors une demande TLS vers le serveur OpenVPN, s'authentifiera à l'aide du certificat et des identifiants Active Directory, et établira un tunnel chiffré sécurisé.

Rentrer l'utrilisateur BTRINH créer auparavant via l'active directory



Après avoir cliqué sur **"CONNECT"**, une fenêtre s'affiche automatiquement demandant la **saisie du mot de passe** associé au **nom d'utilisateur précédemment renseigné**.

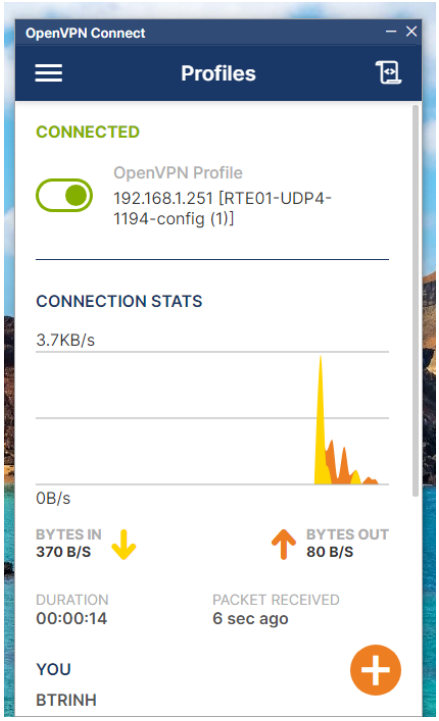
- **Profile** : identifie le profil de connexion utilisé (ici RTE01-UDP4-1194-config (1) pointant vers 192.168.1.251).
- **Password** : ce champ doit contenir le **mot de passe Active Directory** correspondant à l'utilisateur.



Dans notre cas :
Le mot de passe à saisir est celui associé à l'utilisateur **BTRINH**, tel que défini dans l'annuaire Active Directory.
Une fois le mot de passe entré, cliquer sur **"OK"** pour procéder à l'authentification.

L'image ci-dessus confirme que **la connexion VPN a bien été établie** à l'aide du client **OpenVPN Connect** :

- **Statut : CONNECTED** → L'utilisateur est désormais relié de façon sécurisée au réseau distant via le tunnel VPN.
- **Profil utilisé** : 192.168.1.251 [RTE01-UDP4-1194-config (1)] (ce fichier de configuration .ovpn contient les informations nécessaires pour initier la session VPN).
- **Données en transit** :
  - **Bytes In** : données reçues depuis le serveur VPN (ici 370 B/s)
  - **Bytes Out** : données envoyées vers le serveur (ici 80 B/s)
- **Identité utilisateur** : BTRINH (authentifié via l'annuaire Active Directory).



La session VPN est **active** et **fonctionnelle**. Le poste client est désormais en mesure d'accéder aux ressources internes du réseau de l'entreprise (serveurs, partages, etc.), **comme s'il était physiquement connecté au LAN**.

Suite à la connexion réussie via le client **OpenVPN Connect**, des tests de connectivité ont été réalisés afin de s'assurer que la machine cliente peut bien accéder aux ressources du réseau distant via le tunnel VPN :

Test Ping réussi

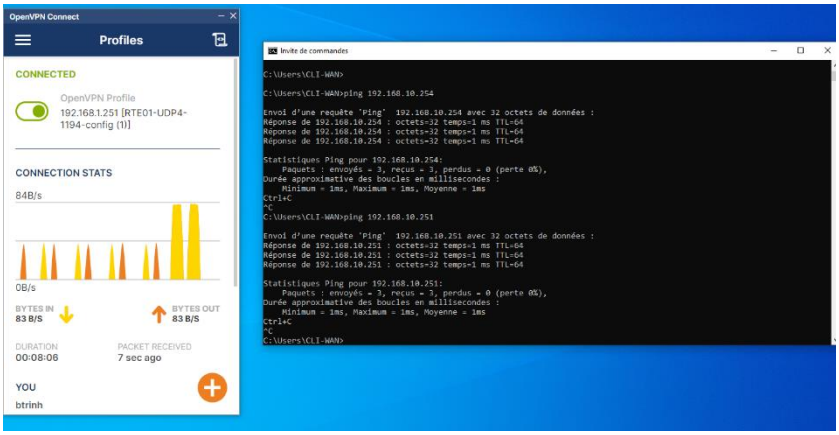
Deux adresses IP ont été pingées avec succès depuis le client :

- **192.168.10.254** → Interface LAN du routeur distant (PfSense)
- **192.168.10.251** → Adresse d'un équipement ou serveur situé dans le réseau local distant

Dans les deux cas :

- **Temps de réponse** : 1 ms
- **Paquets reçus** : 100 %
- **Aucune perte de paquets**

La configuration du VPN Road Warrior avec authentification LDAP/Active Directory est **opérationnelle**, et la connectivité réseau est **confirmée** par ces tests. L'utilisateur distant peut désormais utiliser les services internes (AD, fichiers, imprimantes réseau, etc.).



Procédure d'utilisation VPN

Pour établir une connexion VPN avec le serveur OpenVPN, l'utilisateur doit suivre les étapes ci-dessous :

1. Lancer l'application OpenVPN Connect

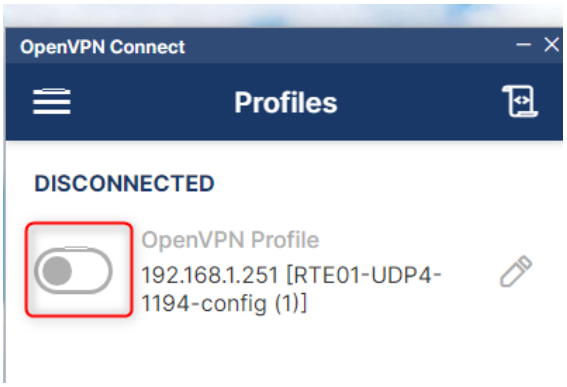
- Dans la barre des tâches de Windows (en bas à droite de l'écran), cliquer sur la **flèche vers le haut** (📌 étape **1** sur la capture) pour afficher les icônes cachées.
- Rechercher et **cliquer sur l'icône d'OpenVPN Connect** (📌 étape **2** sur la capture). Cette icône symbolise un casque avec un petit point rouge.

Cela permet d'ouvrir l'interface du client OpenVPN et de gérer les profils de connexion.

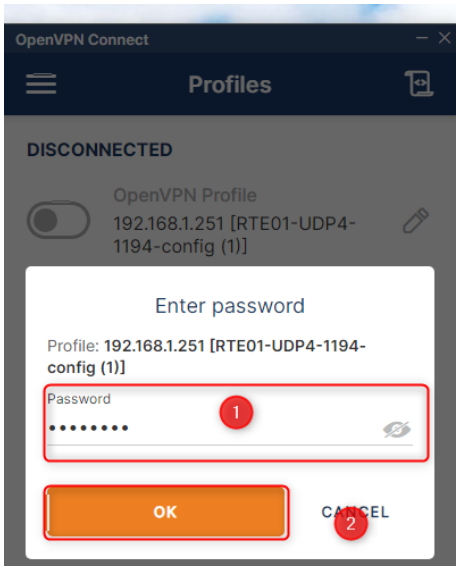
Une fois l'application **OpenVPN Connect** ouverte, l'utilisateur accède à l'interface de gestion des **profils VPN**.

2. Activer la connexion VPN

- L'utilisateur voit son profil VPN affiché dans la liste (dans cet exemple : 192.168.1.251 [RTE01-UDP4-1194-config (1)]).
- Le statut affiché est **DISCONNECTED** (déconnecté).
- Pour se connecter, il suffit de **cliquer sur l'interrupteur gris** (encadré en rouge sur la capture) pour lancer la connexion.



Une fois l'interrupteur activé pour établir la connexion VPN, une **fenêtre de saisie du mot de passe** apparaît.



1. **Entrer le mot de passe associé au compte utilisateur** (dans cet exemple, le compte est BTRINH).

Ce mot de passe correspond à celui de l'annuaire Active Directory si l'authentification LDAP a été configurée.

2. **Cliquer sur OK** pour valider l'identification et établir la connexion VPN.

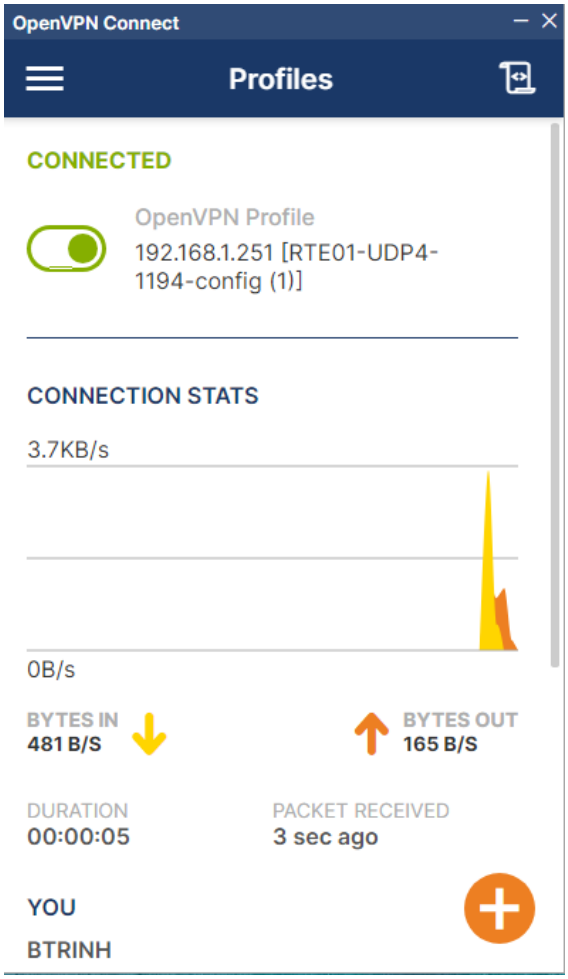
Si les identifiants sont corrects et que le serveur OpenVPN est fonctionnel, la connexion sera établie et le statut passera à **CONNECTED**.

Connexion réussie

Une fois le mot de passe validé, la fenêtre suivante s'affiche indiquant que la **connexion VPN est établie avec succès**.

Informations visibles :

- **Statut : CONNECTED** (en vert) confirme que le tunnel VPN est actif.



Nom du profil : ici, 192.168.1.251 [RTE01-UDP4-1194-config (1)], qui correspond au fichier .ovpn importé.
Statistiques de connexion :
Débit entrant/sortant (BYTES IN / OUT) : données échangées en temps réel entre le client et le serveur.
Durée : temps écoulé depuis l'établissement de la connexion.
Nom d'utilisateur : l'utilisateur authentifié (ex. BTRINH dans cet exemple).

Vous êtes désormais connecté au réseau interne via le tunnel VPN. Vous pouvez accéder aux ressources du réseau distant (serveurs, partages, services internes) comme si vous étiez physiquement sur site.

Annexe : Glossaire des termes techniques

VM (Virtual Machine)

Une machine virtuelle est un système d'exploitation simulé dans un environnement logiciel comme VMware. Elle permet d'exécuter plusieurs OS sur un même ordinateur physique.

VMware

VMware est un logiciel d'hypervision qui permet de créer et gérer des machines virtuelles pour virtualiser des serveurs ou postes de travail.

pfSense

pfSense est une distribution open source basée sur FreeBSD utilisée comme pare-feu, routeur, serveur VPN, etc.

LAN / WAN / DMZ

- LAN (Local Area Network) : réseau interne de l'entreprise.
- WAN (Wide Area Network) : connexion vers Internet.
- DMZ (Demilitarized Zone) : zone tampon entre le LAN et Internet pour héberger des services publics (web, mail...).

Interface réseau

Une interface réseau est une carte réseau virtuelle ou physique à laquelle est attribuée une adresse IP pour permettre la communication réseau.

ZFS

ZFS est un système de fichiers moderne et fiable, utilisé par pfSense pour garantir l'intégrité des données.

DHCP

Le DHCP est un protocole permettant d'attribuer automatiquement une adresse IP aux équipements connectés à un réseau.

CARP (Common Address Redundancy Protocol)

CARP permet à deux routeurs pfSense de partager une adresse IP virtuelle et d'assurer une haute disponibilité.

pfsync

pfsync permet de synchroniser les connexions actives entre deux pare-feux pour éviter les coupures lors d'un basculement.

Failover

Le failover permet de basculer automatiquement vers une autre connexion ou un autre équipement en cas de panne.

Load balancing

Le load balancing (répartition de charge) répartit le trafic réseau entre plusieurs connexions pour améliorer les performances et la redondance.

Gateway Group

Un Gateway Group permet de regrouper plusieurs passerelles avec des priorités pour gérer le failover ou le load balancing dans pfSense.

Pare-feu (Firewall)

Un pare-feu filtre les connexions réseau entrantes ou sortantes selon des règles. Il protège le réseau contre les attaques ou accès non autorisés.

OpenVPN
OpenVPN est un protocole VPN open source qui crée un tunnel sécurisé entre un client et un réseau distant.

Road Warrior
Road Warrior est une configuration VPN OpenVPN pour utilisateurs nomades, leur permettant de se connecter à distance au réseau d'entreprise.

CA (Certificate Authority)
Une autorité de certification (CA) est une entité qui signe des certificats numériques, utilisés pour sécuriser et authentifier les connexions.

Certificat serveur / utilisateur
Un certificat numérique contient des clés cryptographiques utilisées pour chiffrer les connexions (VPN, HTTPS...) et identifier les serveurs ou utilisateurs.

LDAP (Lightweight Directory Access Protocol)
LDAP est un protocole permettant d'interroger un annuaire comme Active Directory pour authentifier des utilisateurs.

Active Directory (AD)
Active Directory est un service d'annuaire Microsoft qui centralise la gestion des utilisateurs, groupes et ressources réseau.

Tunnel VPN
Un tunnel VPN est une connexion sécurisée entre un utilisateur et un réseau distant, chiffrée pour garantir la confidentialité.

TLS (Transport Layer Security)
TLS est un protocole de sécurité qui chiffre les communications entre deux systèmes (ex : VPN, HTTPS...).

Port 1194
Le port 1194 UDP est le port par défaut utilisé par OpenVPN pour accepter les connexions entrantes.

.ovpn
Un fichier .ovpn est un fichier de configuration OpenVPN contenant les paramètres nécessaires à la connexion VPN.

OpenVPN Client Export
OpenVPN Client Export est un module pfSense qui permet d'exporter facilement des fichiers .ovpn pour les utilisateurs.

Bind DN / Password
Le Bind DN est un identifiant utilisé par pfSense pour se connecter à un annuaire LDAP afin de vérifier les identifiants des utilisateurs.

UDP / TCP
- UDP : protocole rapide sans vérification (utilisé pour VPN, jeux en ligne...).
- TCP : protocole fiable avec vérification (utilisé pour HTTP, FTP...).

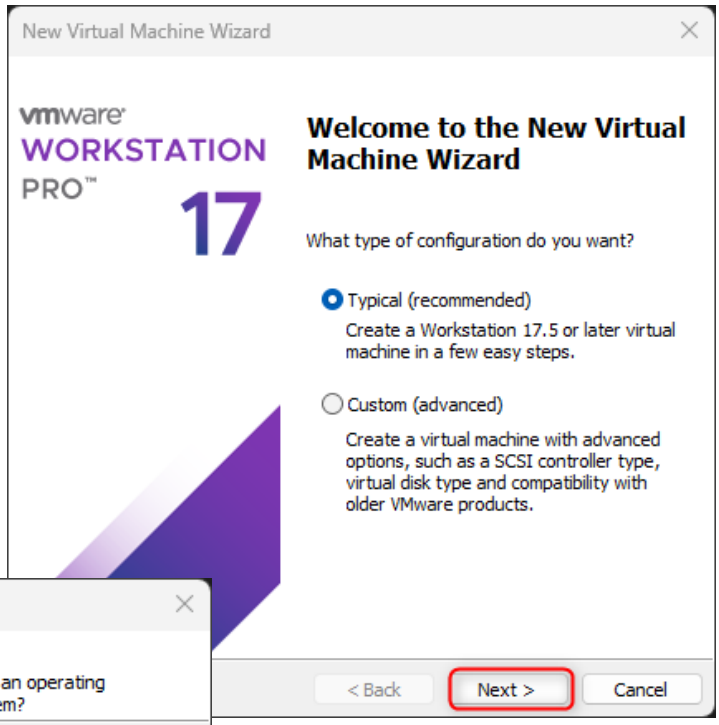
AES / SHA256 / CHACHA20
- AES : algorithme de chiffrement très sécurisé utilisé dans OpenVPN.
- SHA256 : algorithme de hachage pour vérifier l'intégrité des données.
- CHACHA20 : alternative performante à AES, notamment sur les processeurs sans accélération matérielle.

Création, d'une VM sur VM WARE

Lorsque vous créer une machine virtuelle l'option « Typical (recommended) est cocher de base.

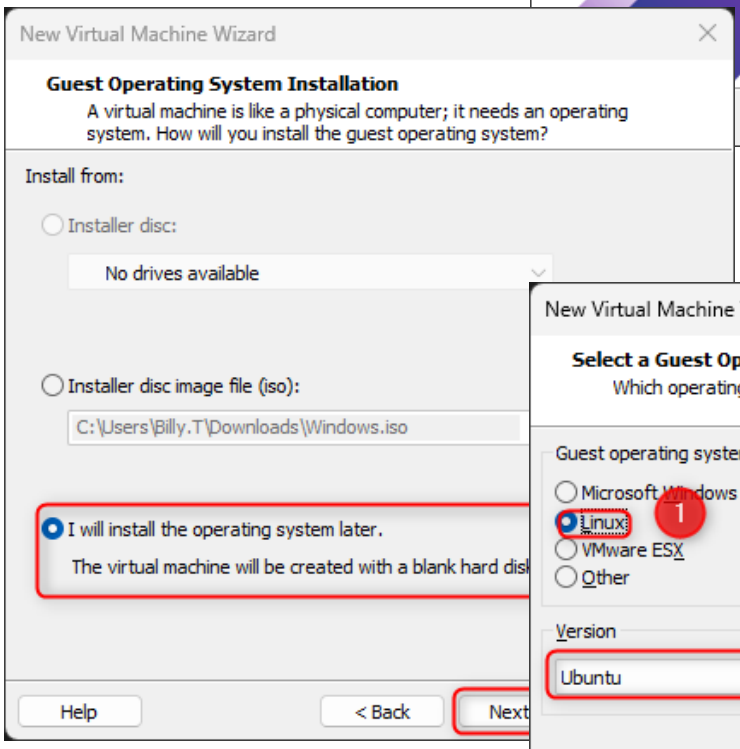
Cliquer sur « Next » pour passer à la prochaine étape.

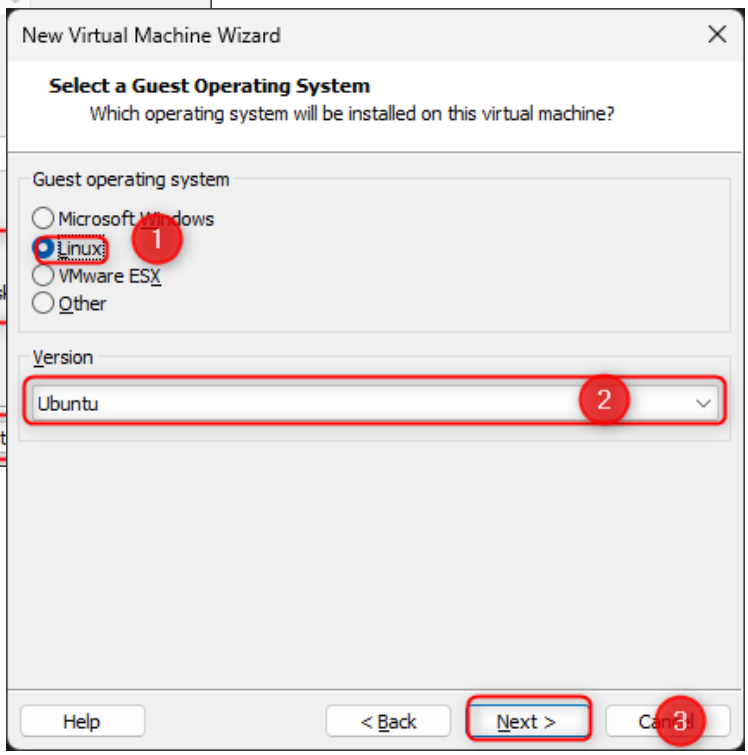
Cliquer sur « Next »



Cliquer sur « Next » pour passer à la prochaine étape

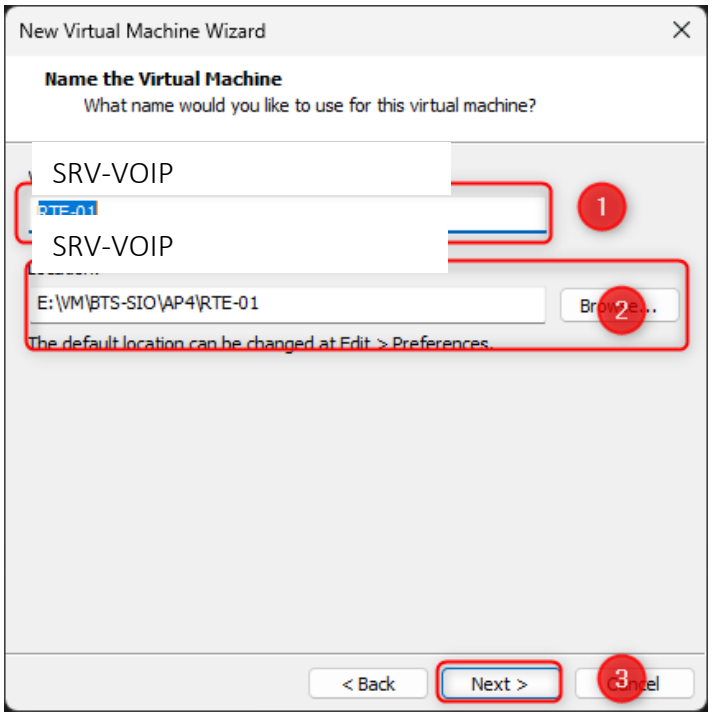
Dans notre cas à nous allons choisir « Linux » car nous auront besoin d'installer d'un pare-feu sur le serveur





Cliquer dans le menu déroulant puis sélectionner « Linux»

Cliquer sur « Next » pour passer à la prochaine étape



Dans cette étape nous allons devoir nommer le serveur ainsi que choisir l'emplacement de la VM

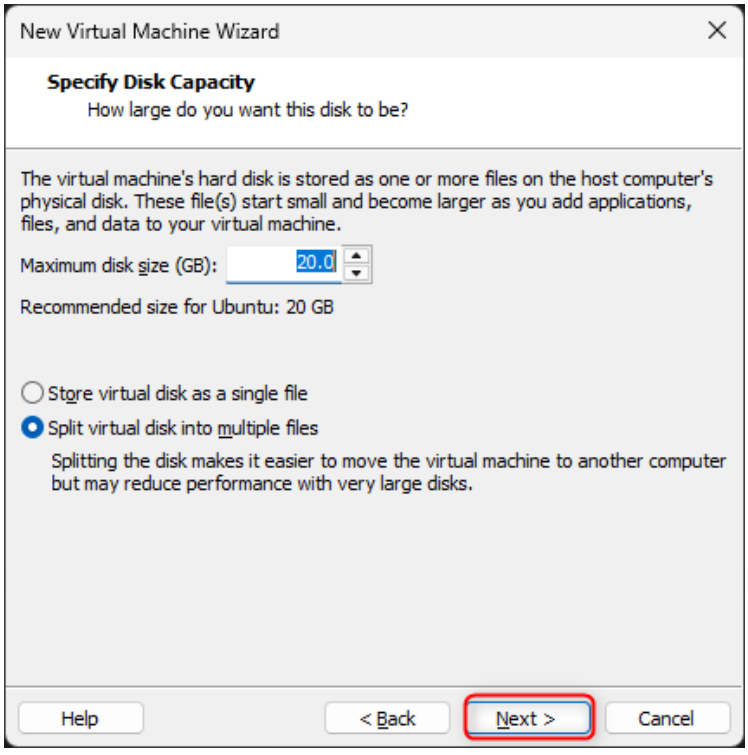
(1) Ensuite nous allons nommer le server

(2) Choisir l'emplacement ou sera situé la VM

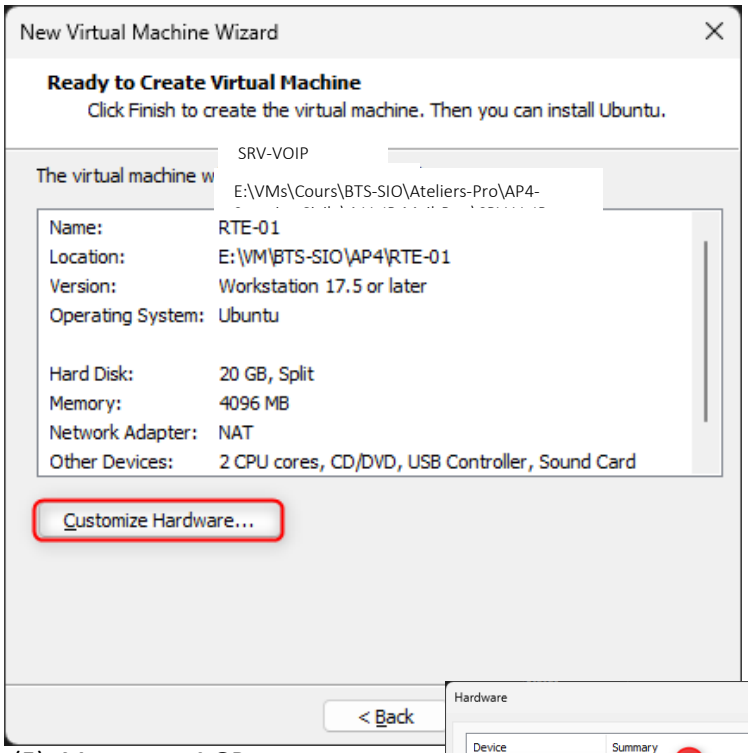
(3) Cliquer sur « Next » pour passer à la prochaine étape

Ensuite sur cette étape nous allons allouer l'espace du disque pour notre serveur. Dans notre cas il n'est pas nécessaire d'avoir un gros espace de stockage sur notre serveur.

Cliquer sur « Next » pour passer à la prochaine étape

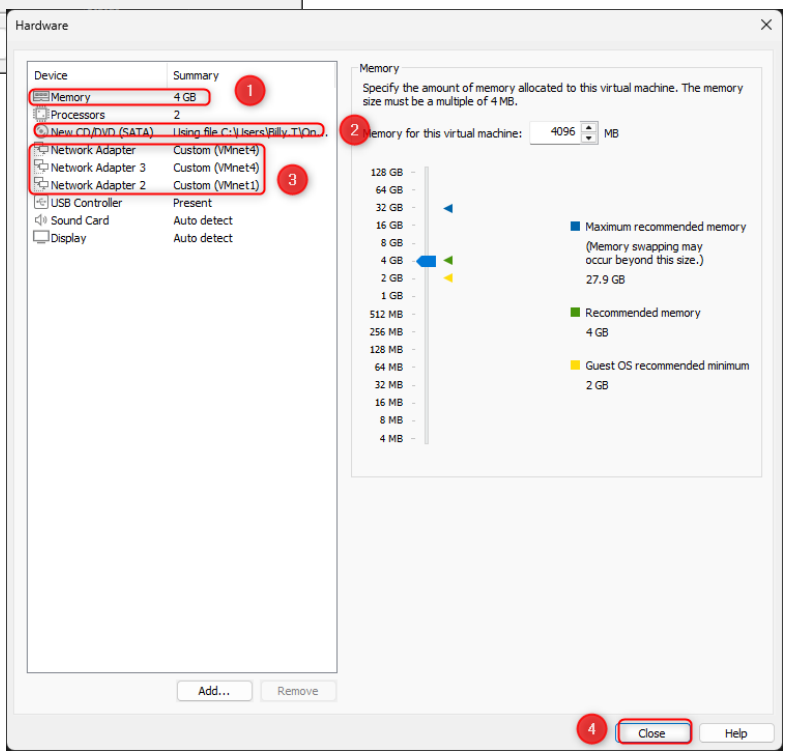


Ensuite dans cette partie-là nous allons configurer les options suivantes :



Cliquer sur « Customize Hardware »

Dans cette partis nous allons paramétrer selon nos besoins :

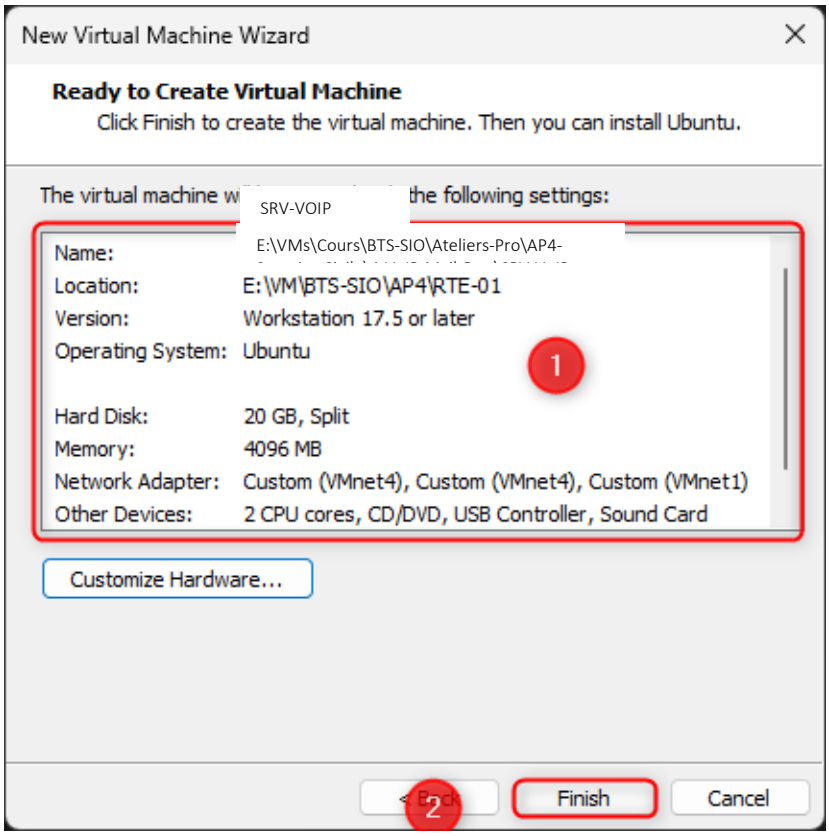


(5) Memory = 4 GB
(6) CD/ DVD = Pfsens
(7) Network Adapter = Vmnet 4 (bridge)
Network Adapter = Vmnet 4 (bridge)

Network adapter = Vmnet 1

(8) Cliquer sur « Close » pour fermer la fenêtre

Une fois que la configuration est finit vous aller avoir ce menu-là :

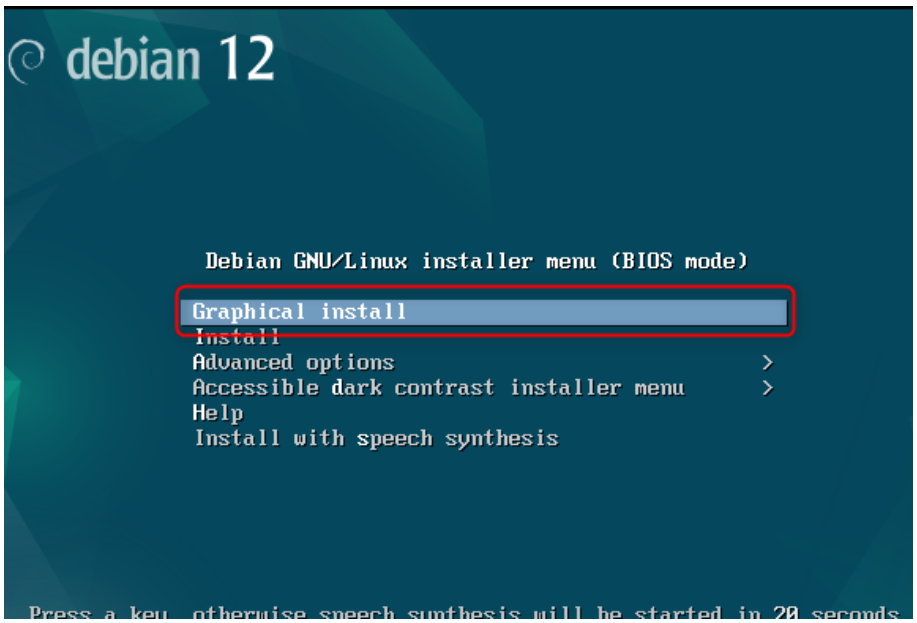


(3) Récapitulatif de la configuration du serveur.
(4) Cliquer sur « Finish » pour passer à la prochaine étape

Une fois avoir fini de vérifier les information du serveur, la VM (Virtual Machine) va se créer ainsi vous pouvez le lancer.

Installation Débian 12.0

L'écran affiché correspond au **menu principal du programme d'installation de Debian 12**, exécuté en mode BIOS. À cette étape, plusieurs options sont proposées à l'utilisateur pour initier l'installation du système d'exploitation.
L'option actuellement sélectionnée est :
Graphical install : cette méthode propose une installation assistée via une interface graphique conviviale, facilitant la configuration pour les utilisateurs non familiers avec l'environnement en ligne de commande.

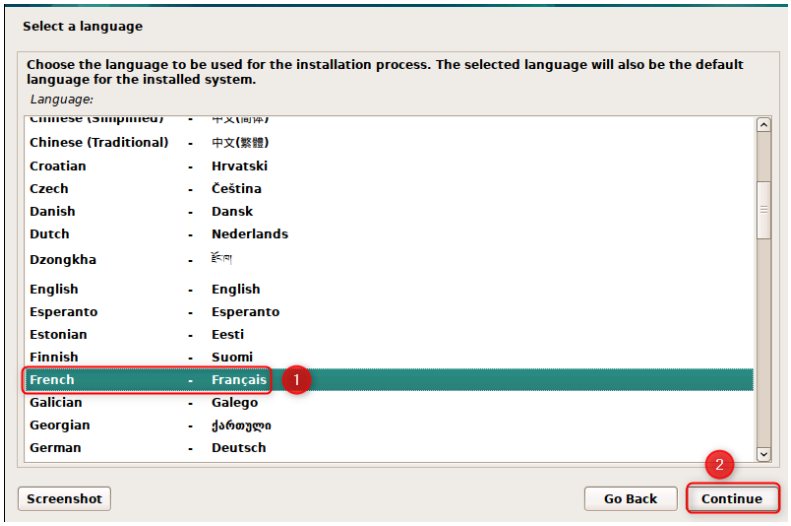


Sélectionner Graphical install

Autres options disponibles :

- **Install** : installation en mode texte, adaptée aux environnements serveur ou aux systèmes nécessitant une configuration légère sans interface graphique.
- **Advanced options** : permet d'accéder à des paramètres spécifiques (ex. : expert install, mode rescue...).
- **Accessible dark contrast installer menu** : mode d'installation graphique avec un thème à contraste élevé, destiné à améliorer l'accessibilité visuelle.
- **Help** : documentation succincte sur les options d'installation.
- **Install with speech synthesis** : installation adaptée aux personnes malvoyantes, avec synthèse vocale activée.

Sélection de la langue – Étape détaillée
L'image ci-dessus correspond à l'écran de sélection de la langue dans le programme d'installation de Debian 12.



Sélectionner la langue souhaitée :
Cliquer sur l'entrée « **French – Français** » afin de définir le français comme langue principale pour l'installation ainsi que pour le système une fois celui-ci installé.

1. **Valider le choix** :
Cliquer sur le bouton **Continue** (en bas à droite) pour passer à l'étape suivante.

Remarque : La langue sélectionnée influencera également la disposition du clavier proposée, les formats de date/heure, et certaines préférences régionales par défaut.
Cette étape permet d'adapter l'ensemble du processus d'installation à la langue de l'utilisateur, garantissant ainsi une meilleure lisibilité et une configuration personnalisée.

Choix de la situation géographique

Cette étape consiste à sélectionner le **pays de résidence** ou la **zone géographique** dans laquelle le système sera utilisé.

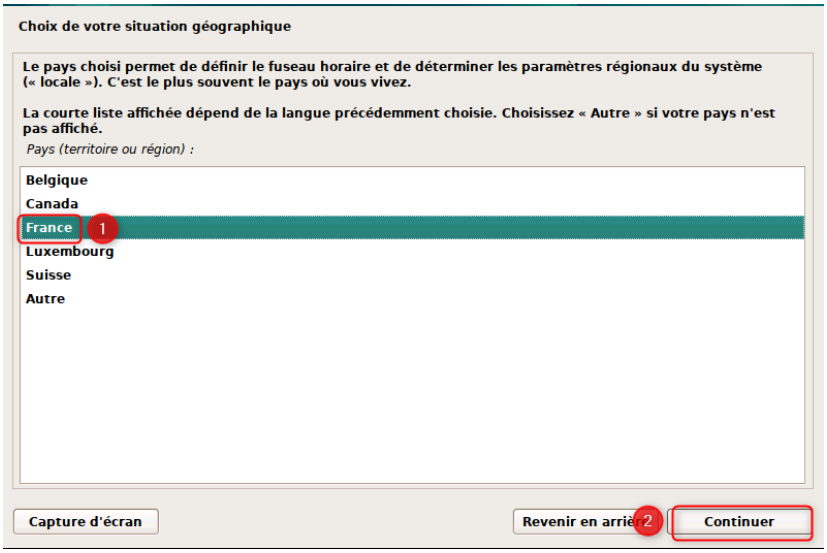
Objectif :

Le pays sélectionné permet à l'installeur de :

- Définir automatiquement le **fuseau horaire**,
- Appliquer les **paramètres régionaux** appropriés (format de date, heure, devise, etc.),
- Adapter certaines **préférences linguistiques** si nécessaire.

1. **Sélection de la région** :
   L'utilisateur a ici sélectionné **France** comme situation géographique (étape ① sur la capture).

2. **Validation de l'étape** :
   Cliquer sur le bouton **Continuer** (étape ②) pour valider la sélection et poursuivre l'installation.



Cette étape est essentielle pour assurer le bon fonctionnement des paramètres régionaux du système Debian une fois installé.

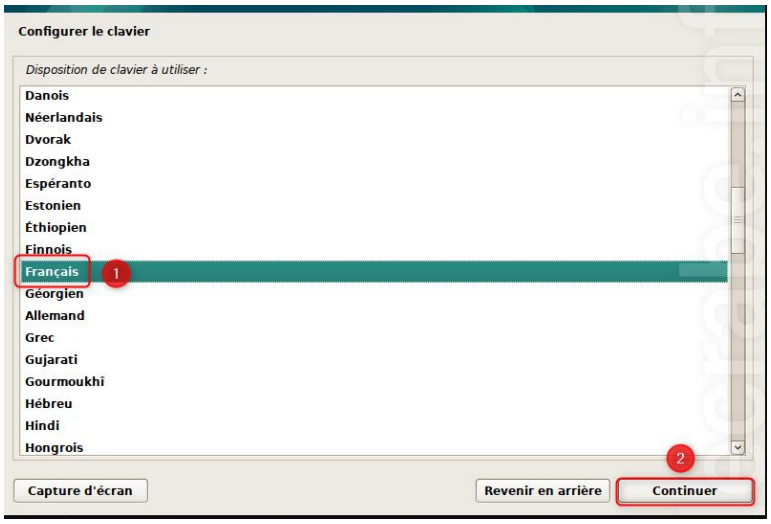
Configuration du clavier

Cette étape permet de définir la **disposition du clavier** utilisée pendant l'installation et après l'installation du système Debian.

Le choix de la disposition clavier permet :

- D'assurer la correspondance entre les touches physiques et les caractères affichés,
- D'éviter les erreurs de saisie lors de la configuration (notamment pour les mots de passe),
- D'adapter l'environnement de travail à la langue et au matériel utilisés par l'utilisateur.

Détail des actions visibles à l'écran :



1. **Sélection de la disposition** :
L'utilisateur a sélectionné **Français** comme disposition clavier (étape ① sur la capture). Cette option correspond à une disposition **AZERTY**, standard sur les claviers utilisés en France.

2. **Validation de l'étape** :
Cliquer sur le bouton **Continuer** (étape ②) pour confirmer la sélection et passer à l'étape suivante de l'installation.

Configuration du réseau – Attribution d'une adresse de lien local (link-local)

Suite à l'échec de la détection d'une configuration via DHCP, l'installeur tente de configurer automatiquement une **adresse IP de lien local** pour permettre une connectivité minimale.

L'adresse de lien local (appelée aussi **link-local**) permet à un équipement réseau de s'auto-attribuer une adresse IP dans la plage **169.254.0.0/16** lorsqu'aucun serveur DHCP n'est disponible. Cela peut temporairement permettre des communications locales (entre machines connectées directement).

- Le système affiche le message :
  « Attente de l'adresse du lien local ("link-local")... »
  Cela signifie que Debian tente d'attribuer une adresse IP automatique sans dépendre d'un serveur.
- **Cliquer sur le bouton « Annuler »** permet d'interrompre ce processus si vous souhaitez configurer l'adresse réseau manuellement.

Configuration du réseau – Échec de l'attribution automatique (DHCP)

À cette étape, le programme d'installation tente de configurer automatiquement l'interface réseau via le protocole **DHCP (Dynamic Host Configuration Protocol)**. Toutefois, une erreur s'est produite.

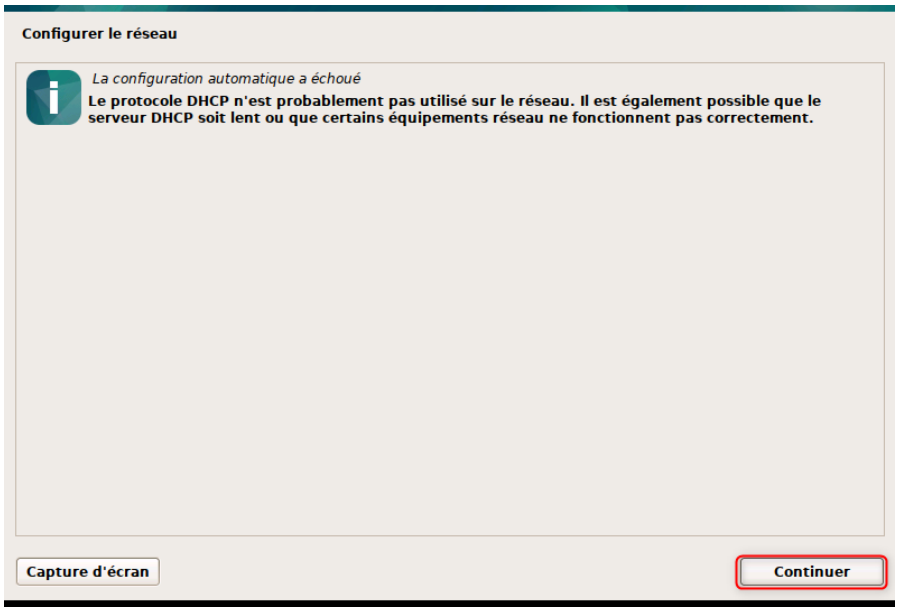
Cette phase a pour but d'obtenir automatiquement une adresse IP ainsi que les informations réseau nécessaires (passerelle, DNS) depuis un serveur DHCP, généralement présent sur le réseau local.

Informations affichées à l'écran :

Le message indique que la configuration automatique a échoué. Les causes possibles incluent :

- L'absence de serveur DHCP sur le réseau,

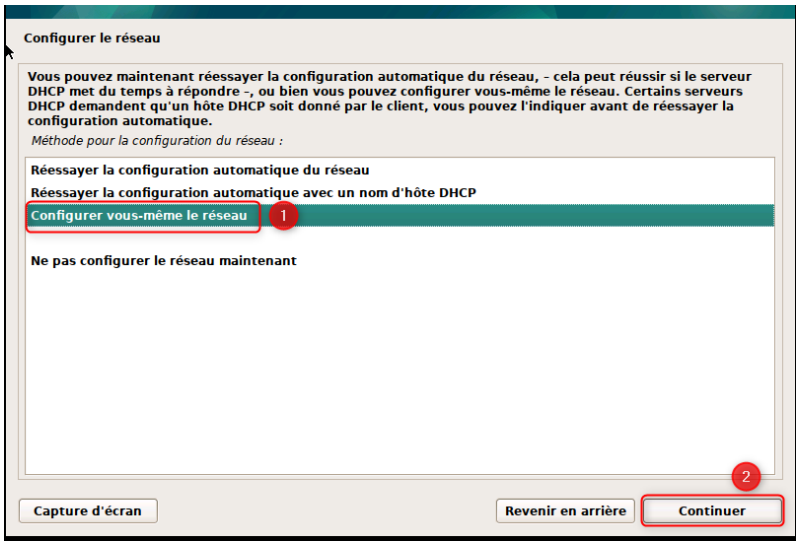
- Un délai de réponse anormalement long du serveur DHCP,
- Une mauvaise détection ou défaillance matérielle de l'interface réseau.



- **Cliquer sur le bouton "Continuer"** pour poursuivre l'installation et configurer manuellement les paramètres réseau lors de l'étape suivante.

Configuration du réseau – Choix de la méthode
Cette étape permet à l'utilisateur de définir **comment le réseau sera configuré**, suite à l'échec des tentatives automatiques via DHCP.

Déterminer manuellement ou automatiquement les paramètres réseau pour permettre au système de communiquer avec l'extérieur ou le réseau local.



1. **Sélection de la méthode de configuration** – repère ① :
L'utilisateur a sélectionné l'option **« Configurer vous-même le réseau »**, ce qui permet de définir manuellement les paramètres réseau tels que :

- l'adresse IP,
- le masque de sous-réseau,
- la passerelle,
- et les serveurs DNS.

2. **Validation de l'étape** – repère ② :
   Cliquer sur **« Continuer »** permet d'accéder à l'assistant de configuration manuelle.

Autres options proposées :

- **Réessayer la configuration automatique** : utile si le serveur DHCP était temporairement inaccessible.
- **Réessayer avec un nom d'hôte DHCP** : certains serveurs DHCP nécessitent un nom d'hôte pour attribuer une adresse.
- **Ne pas configurer le réseau maintenant** : à éviter dans la majorité des cas, sauf si l'accès réseau est volontairement désactivé (par exemple en environnement isolé ou test local).

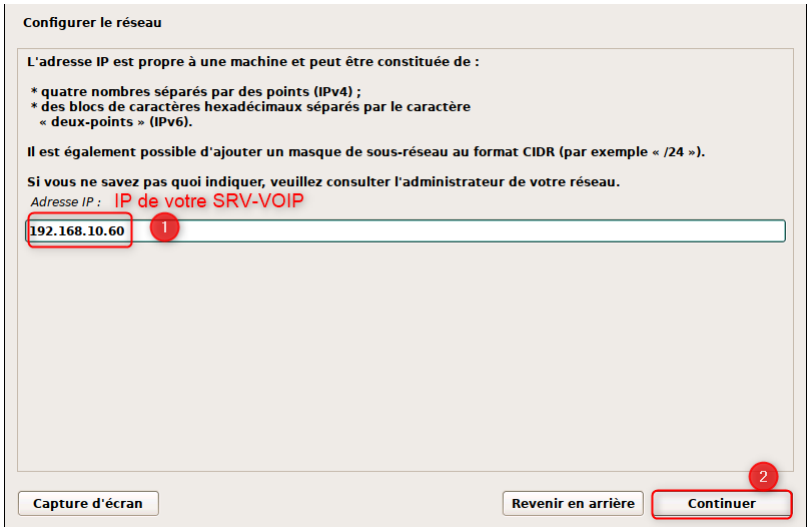
onfiguration du réseau – Définition manuelle de l'adresse IP

Dans cette phase, l'utilisateur est invité à **saisir manuellement l'adresse IP** qui sera attribuée à l'interface réseau principale de la machine.

L'adresse IP permet à la machine Debian d'être identifiée sur le réseau local. Cette étape est essentielle dans une configuration réseau statique (absence de DHCP).

Détail des actions visibles à l'écran :

1. **Saisie de l'adresse IP** – repère ① :
   L'utilisateur a saisi l'adresse IP **192.168.10.60**, qui correspond à l'IP statique prévue pour le serveur nommé **SRV-VOIP** dans l'infrastructure cible.



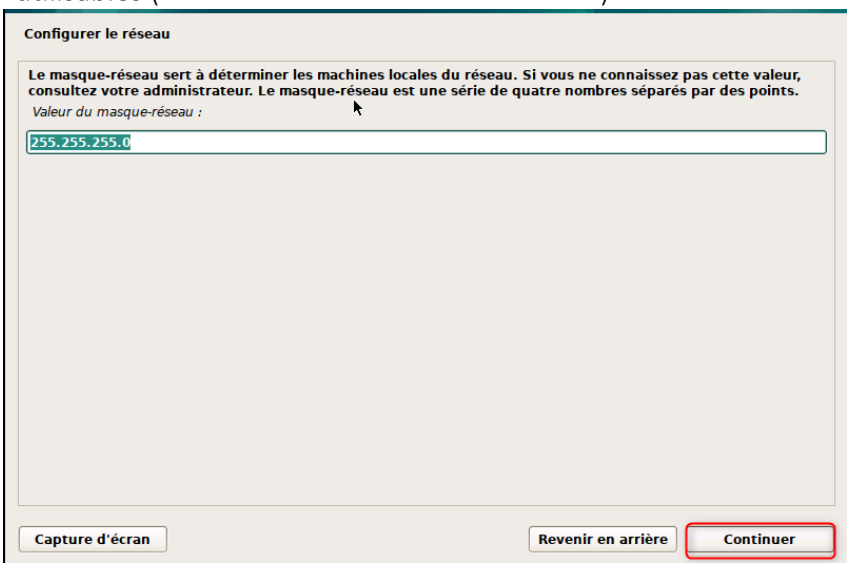
2. **Validation de l'adresse** – repère ② :
   Cliquer sur **« Continuer »** permet de confirmer cette adresse IP et de passer à l'étape suivante (masque de sous-réseau).

Cette adresse doit impérativement appartenir au même sous-réseau que les autres équipements du réseau local, et être **unique** pour éviter les conflits IP.

Configuration du réseau – Définition du masque de sous-réseau
Après la saisie de l'adresse IP, cette étape permet de renseigner le **masque de sous-réseau**, paramètre indispensable pour déterminer l'étendue du réseau local.
Objectif :
Le masque de sous-réseau permet de :

- Identifier quelles adresses IP sont considérées comme locales (dans le même réseau),
- Définir la taille du réseau (nombre d'hôtes disponibles),
- Assurer une communication efficace entre les machines du même sous-réseau.

Exemple utilisé :
Dans la capture, l'utilisateur a saisi :
255.255.255.0, ce qui correspond au préfixe **/24**, soit un réseau contenant jusqu'à **254 hôtes utilisables** (de 192.168.10.1 à 192.168.10.254).



Cliquer sur **« Continuer »** pour valider le masque et poursuivre la configuration réseau (passerelle par défaut).

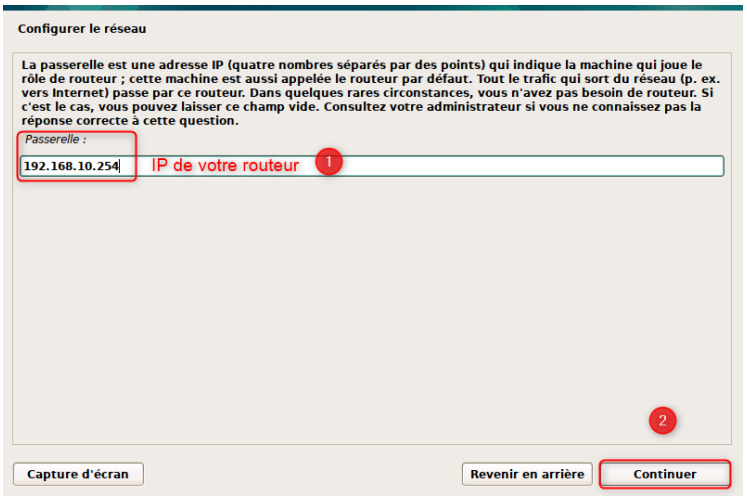
Configuration du réseau – Définition de la passerelle (routeur par défaut)
Une fois l'adresse IP et le masque de sous-réseau définis, cette étape permet d'indiquer la **passerelle par défaut**, c'est-à-dire l'adresse IP du routeur par lequel transite tout le trafic sortant du réseau local.

La passerelle est utilisée pour :

- Accéder à d'autres réseaux, y compris Internet,
- Acheminer les paquets destinés à des adresses extérieures au sous-réseau local,
- Garantir la connectivité complète d'un serveur ou d'un poste de travail.

Détail des actions visibles à l'écran :

1. **Saisie de l'adresse IP du routeur** – repère ① : L'utilisateur a saisi **192.168.10.254**, adresse IP typiquement utilisée pour représenter l'interface LAN d'un routeur (dans cet exemple, probablement l'adresse LAN d'un pare-feu pfSense).



2. **Validation de l'étape** – repère ② : Cliquer sur **« Continuer »** permet de confirmer la passerelle et de passer à la configuration des serveurs DNS.

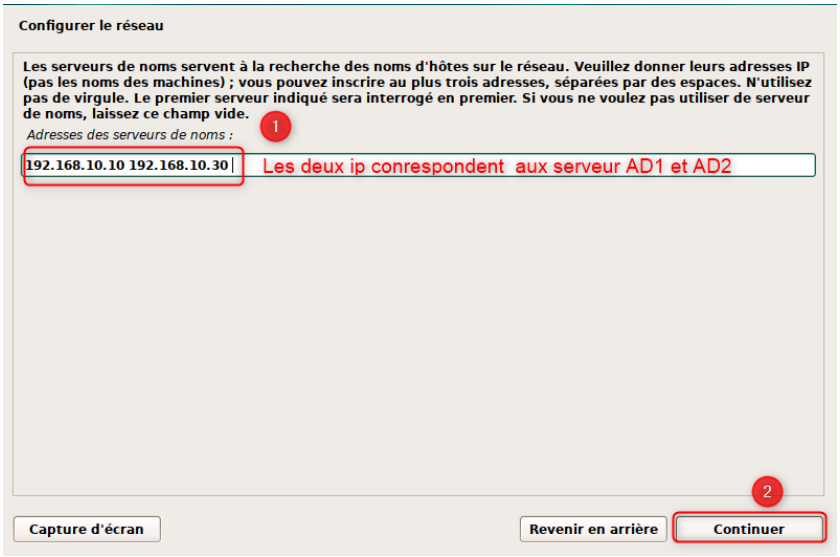
Configuration du réseau – Définition des serveurs DNS

Lors de cette étape, l'installateur Debian demande à l'utilisateur de renseigner les adresses IP des serveurs DNS qui seront utilisés pour la résolution de noms de domaine (traduction d'un nom comme srv-voip.cod.lan en adresse IP).

Les serveurs DNS permettent :

- La résolution des noms d'hôtes en adresses IP sur le réseau local ou Internet,
- Le bon fonctionnement des services réseau nécessitant une communication par nom (Active Directory, messagerie, accès web, etc.),

- Une gestion centralisée des ressources via les FQDN (noms complets de machines).



1. **Saisie des adresses IP des serveurs DNS** – repère ① :
L'utilisateur a renseigné deux adresses :

192.168.10.10 : correspond au serveur AD1 (Active Directory principal),
192.168.10.30 : correspond au serveur AD2 (ou un serveur secondaire gérant également le rôle DNS).
Ces deux serveurs doivent être configurés pour répondre aux requêtes DNS internes à l'organisation (et potentiellement faire du "forwarding" vers Internet).

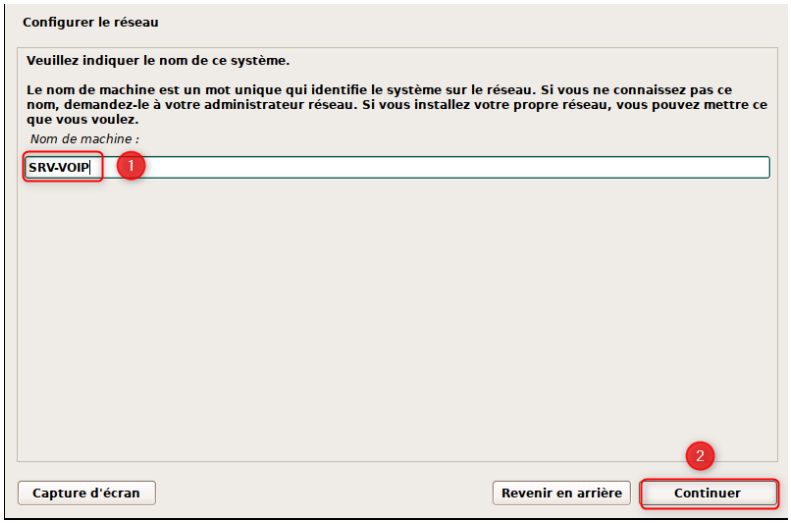
2. **Validation de l'étape** – repère ② :
Cliquer sur **« Continuer »** permet de valider les serveurs DNS et d'enregistrer la configuration réseau complète.

Configuration du réseau – Nom de machine (hostname)

Dans cette étape, l'installateur Debian demande à l'utilisateur de définir un **nom d'hôte**. Il s'agit d'un identifiant unique utilisé pour nommer la machine sur le réseau.

Le nom d'hôte permet :

- D'identifier facilement le serveur dans l'infrastructure réseau,
- De faciliter la résolution DNS et l'intégration dans un domaine Active Directory,
- D'assurer la lisibilité dans les journaux systèmes, les services réseau, et les interfaces de supervision.



1. **Saisie du nom d'hôte** – repère ① : L'utilisateur a défini le nom de la machine comme **SRV-VOIP**. Ce nom est explicite : il indique qu'il s'agit d'un **serveur de téléphonie IP** (Voice Over IP).

Il est recommandé d'utiliser une convention de nommage claire (ex. SRV-ROLE-SITE, comme SRV-AD-STG01 ou SRV-WEB-DMZ).

2. **Validation de l'étape** – repère ② : Cliquer sur **« Continuer »** permet de confirmer le nom et de passer à la configuration du domaine.

Configuration du réseau – Domaine

Lors de cette étape, l'installeur Debian propose généralement de définir un **nom de domaine** afin de compléter le nom d'hôte du serveur (FQDN). Cependant, **dans le cadre de cette installation, aucun nom de domaine n'a été spécifié**, et le champ a volontairement été laissé vide.

Le nom de domaine est habituellement utilisé pour :

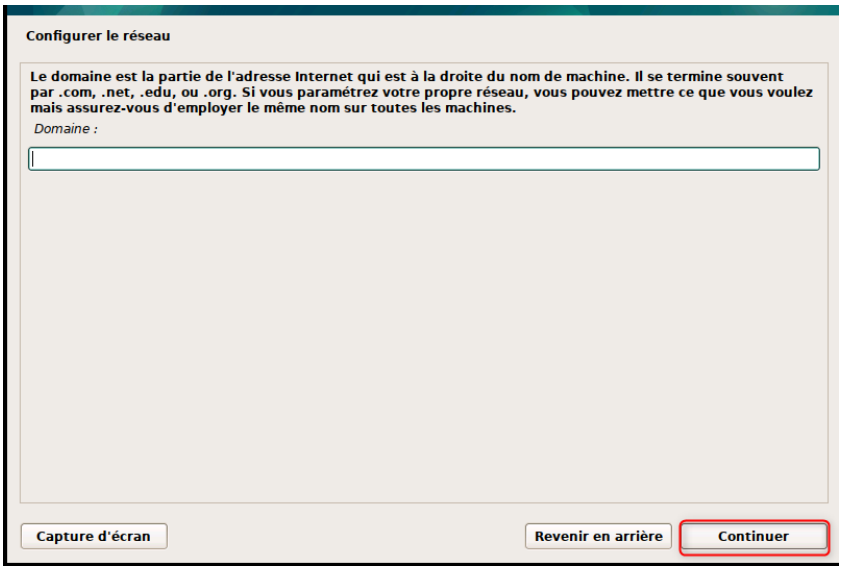
- Intégrer le système dans un réseau d'entreprise structuré,

- Permettre une résolution DNS cohérente entre les hôtes,
- Créer un FQDN du type nom-machine.domaine.local.

Justification :
Dans ce cas précis, le domaine n'a **pas été renseigné** car :

- Le serveur n'est pas encore intégré à un domaine Active Directory,
- L'utilisation de FQDN n'est pas requise pour les services prévus,
- Le réseau local repose actuellement sur une résolution d'hôtes manuelle ou par DNS local préconfiguré.

- le champ "Domaine" a été laissé **vide**.
- L'utilisateur a cliqué sur **« Continuer »** pour valider cette étape et poursuivre l'installation.



Création du mot de passe superutilisateur (root)

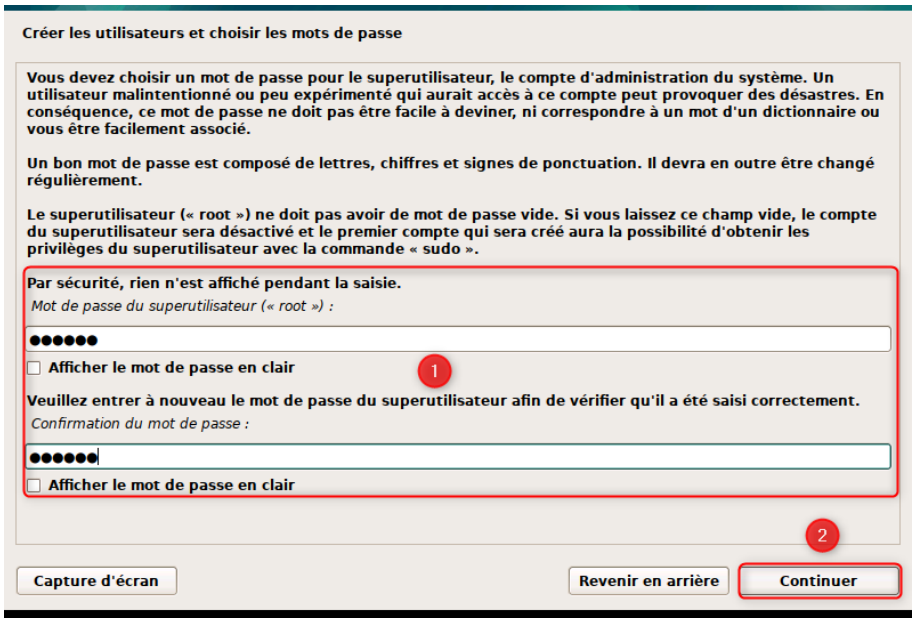
Cette étape permet de définir un mot de passe sécurisé pour le **compte superutilisateur** (également appelé **root**), qui possède tous les droits d'administration sur le système Debian.

Le mot de passe root est essentiel pour :

- Administrer le système,
- Installer ou supprimer des paquets,
- Modifier des fichiers sensibles (comme ceux de configuration réseau ou système),
- Intervenir en cas de panne ou de défaillance d'un utilisateur.

Recommandations de sécurité :

- Le mot de passe doit **contenir au minimum huit caractères**.
- Il est recommandé d'inclure **des majuscules, des minuscules, des chiffres et des caractères spéciaux**.
- Il ne doit **pas être trop simple ou prévisible**, ni réutilisé sur d'autres comptes ou systèmes.



1. Saisie du mot de passe root dans le champ prévu (étape ① sur la capture).
2. Confirmation du mot de passe en le saisissant une seconde fois.
3. Validation en cliquant sur **« Continuer »** (étape ②).

Création d'un utilisateur standard

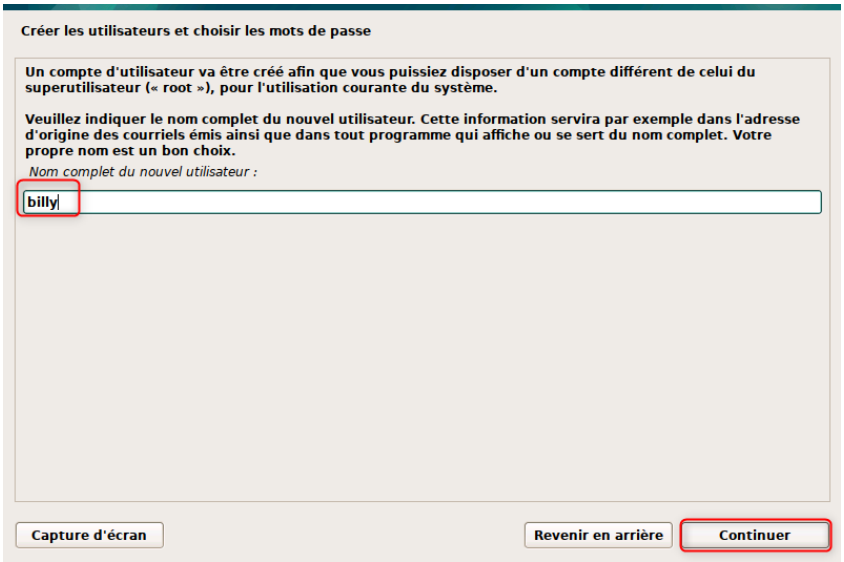
Cette étape permet la création d'un **compte utilisateur non privilégié**, destiné à un usage courant du système. Il s'agit d'une **bonne pratique de sécurité**, qui vise à séparer les actions administratives (réalisées avec le compte root ou via sudo) des usages classiques (navigation, bureautique, développement, etc.).

Créer un utilisateur personnel afin de :

- Travailler sans utiliser le compte root,
- Protéger le système contre les erreurs involontaires d'administration,

- Permettre l'identification claire de chaque utilisateur du système.

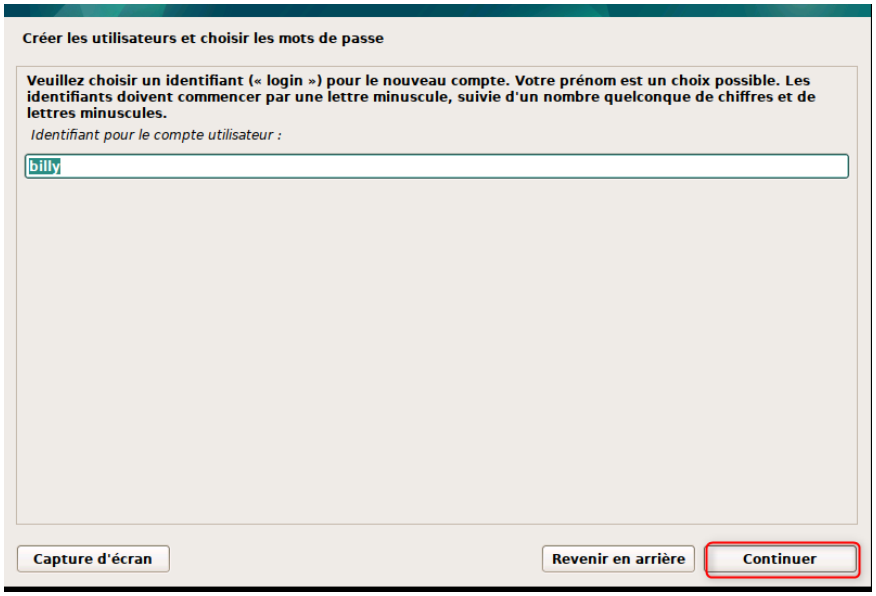
1. **Saisie du nom complet** de l'utilisateur (dans notre exemple, « **billy** ») dans le champ prévu à cet effet.
2. **Validation de l'étape** en cliquant sur le bouton **« Continuer »**.



Définition de l'identifiant système (login)

Cette étape consiste à **attribuer un identifiant unique** au nouvel utilisateur. Cet identifiant, également appelé **login**, permet à l'utilisateur de se connecter à son compte sous Debian.

- Définir un identifiant conforme aux règles de nommage des utilisateurs sous Linux,
- Associer cet identifiant à un environnement utilisateur personnel,
- Permettre l'authentification lors des connexions locales ou distantes.



1. **Saisie de l'identifiant** souhaité (dans cet exemple : billy) dans le champ dédié.
2. **Validation de l'étape** en cliquant sur le bouton **« Continuer »**.

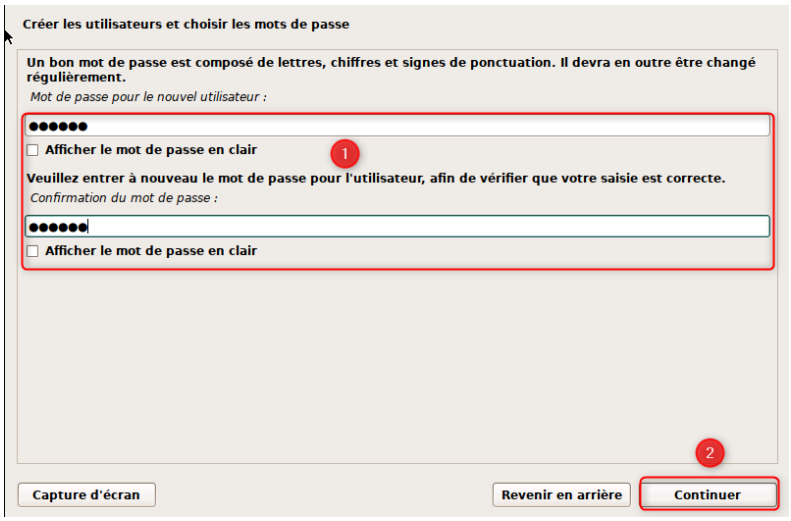
Définir le mot de passe du nouvel utilisateur

Une fois le nom complet et l'identifiant utilisateur renseignés, cette étape permet de définir un **mot de passe sécurisé** pour le compte utilisateur nouvellement créé.

Objectif :

- Assurer la protection du compte utilisateur par un mot de passe fort,
- Vérifier que le mot de passe est correctement saisi via une double confirmation.

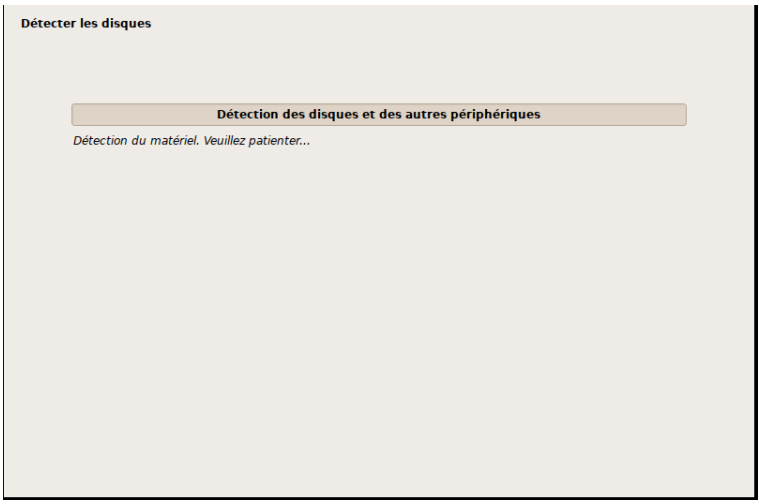
Détail des actions visibles à l'écran :



1. **Saisie du mot de passe** dans le champ prévu à cet effet, puis **confirmation** dans le second champ (étape ①).
2. **Validation** de l'étape en cliquant sur le bouton **« Continuer »** (étape ②).

Détection des disques et du matériel
Lors de cette étape, l'installateur Debian procède automatiquement à la **détection des périphériques de stockage** présents sur la machine. Cela inclut les disques durs, SSD, clés USB ou tout autre média de stockage.

- Identifier les disques disponibles afin de proposer les options de partitionnement adaptées,
- Déterminer la configuration matérielle nécessaire pour l'installation du système.

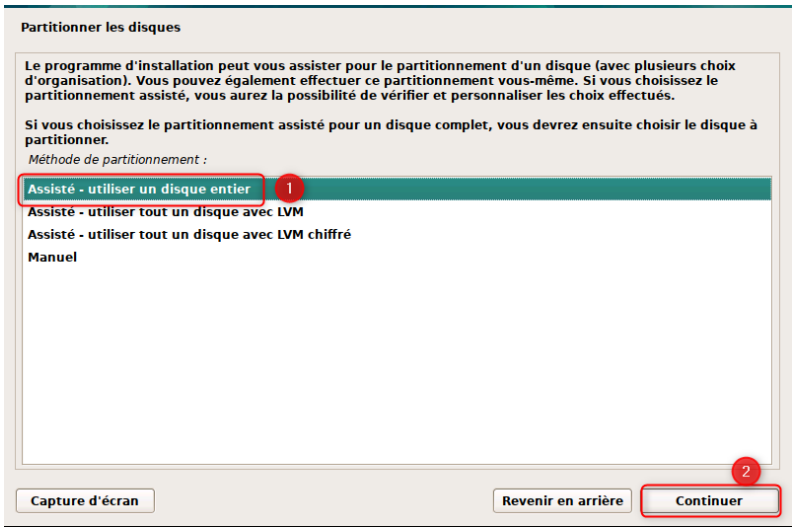


- Une barre de progression intitulée **« Détection des disques et des autres périphériques »** s'affiche, accompagnée du message **« Détection du matériel. Veuillez patienter... »**, signalant que le système analyse le matériel présent.

Partitionnement des disques
Cette étape permet de définir la manière dont les données seront réparties sur le disque dur. Le programme d'installation Debian propose plusieurs méthodes de partitionnement, allant de l'automatique à la configuration manuelle avancée.

- Créer les partitions nécessaires à l'installation du système d'exploitation.
- Choisir une méthode adaptée selon le niveau de personnalisation souhaité.

Détail des actions visibles à l'écran :



1. **Méthode sélectionnée** :
L'utilisateur a choisi l'option **« Assisté – utiliser un disque entier »** (étape ① sur la capture), ce qui permet à l'installateur de gérer automatiquement la création des partitions standards.

2. **Validation de l'étape** :
Cliquer sur le bouton **Continuer** (étape ②) pour confirmer la méthode de partitionnement sélectionnée.

Cette méthode est recommandée pour une installation simple, notamment lorsque :

- Le disque est entièrement dédié à Debian,
- Aucune donnée importante ne doit être conservée sur ce disque (car il sera formaté).

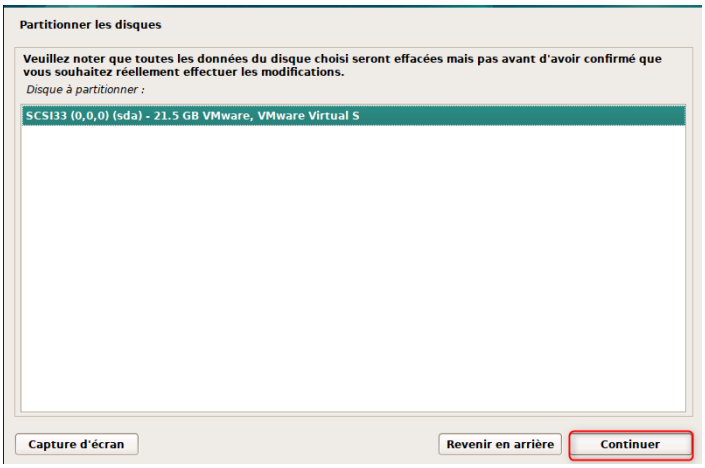
Sélection du disque à partitionner

Après avoir choisi la méthode de partitionnement, l'installateur propose de sélectionner le disque physique sur lequel les partitions seront créées.

- Déterminer le support de stockage principal destiné à recevoir le système Debian.
- S'assurer que l'espace disque sélectionné est disponible et que son utilisation ne compromettra pas d'autres systèmes existants.

Détail des actions visibles à l'écran :

1. **Disque sélectionné** :
   Dans cet exemple, l'utilisateur a sélectionné le disque virtuel **SCSI3 (0,0,0) (sda) – 21.5 GB VMware Virtual S**, correspondant à un disque alloué dans un environnement VMware.
2. **Validation de l'étape** :
   Cliquer sur le bouton **Continuer** pour confirmer la sélection du disque et poursuivre le processus de partitionnement.

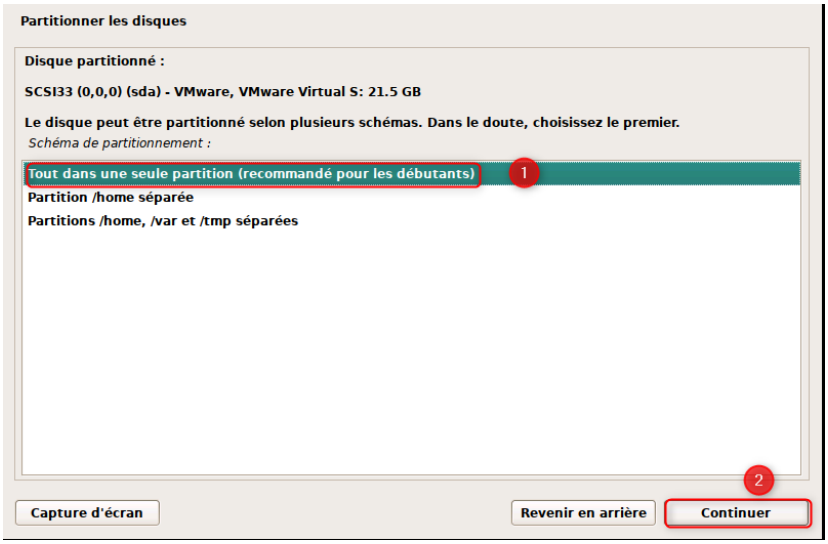


Attention : Toutes les données présentes sur ce disque seront supprimées. Cette opération est irréversible une fois validée.

Choix du schéma de partitionnement

Une fois le disque sélectionné, l'assistant d'installation propose plusieurs méthodes de partitionnement en fonction de l'usage du système.

- Déterminer la manière dont les données seront organisées sur le disque dur.
- Adapter la structure du système de fichiers selon le niveau de compétence ou les besoins spécifiques de l'utilisateur.



1. **Méthode sélectionnée** :
L'option **Tout dans une seule partition (recommandé pour les débutants)** est ici choisie (étape ①).

2. **Validation de l'étape** :
Cliquer sur le bouton **Continuer** (étape ②) pour confirmer le choix et passer à l'étape suivante.

Ce mode de partitionnement place l'ensemble des fichiers système, des données utilisateur et des journaux dans une seule partition (généralement /).

Avantages : simple à gérer, adapté aux environnements de test ou aux utilisateurs novices.
Inconvénients : en cas de saturation du disque, cela peut impacter l'ensemble du système (pas d'isolation entre /home, /var, etc.).

Validation du schéma de partitionnement

Cette étape permet de vérifier et de valider le plan de partitionnement du disque sélectionné avant de procéder à son application.

- Confirmer la structure des partitions définies précédemment.
- Écrire les modifications sur le disque pour permettre l'installation du système.

Présentation de la table de partitions

Le système affiche les partitions créées :

- Une partition principale de type ext4, point de montage /, avec une taille de 20.4 Go.
- Une partition logique de type swap de 1.0 Go, utilisée comme mémoire d'échange.

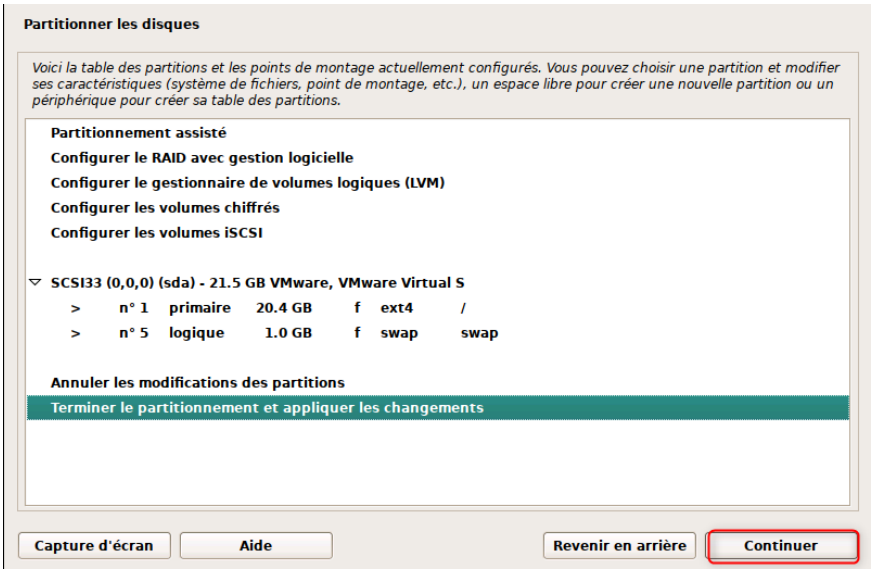
Ces partitions sont listées sous le périphérique sélectionné :
SCSI3 (0,0,0) (sda) – 21.5 GB VMware, VMware Virtual S.

Action sélectionnée

L'utilisateur choisit l'option **Terminer le partitionnement et appliquer les changements**. Cette action est requise pour finaliser cette étape et initier la phase de formatage des partitions.

Validation

Cliquer sur le bouton **Continuer** pour confirmer ce choix et passer à l'étape suivante de l'installation.

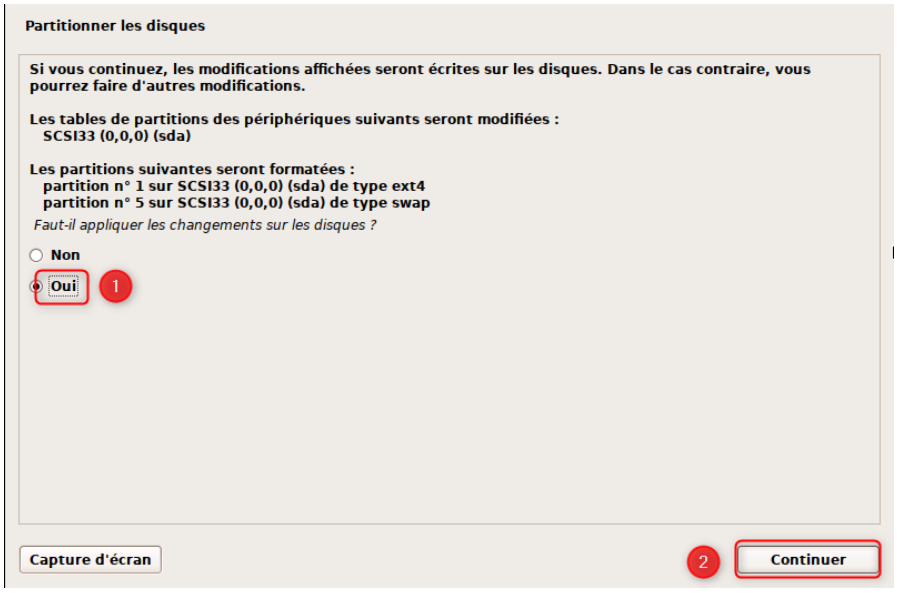


Confirmation de l'écriture des modifications sur le disque

À cette étape, le système demande une confirmation avant d'écrire définitivement les modifications sur le disque dur. Il s'agit d'une étape critique, car elle entraîne l'effacement complet des données précédemment présentes sur le disque sélectionné.

Objectif :

- Autoriser le programme d'installation à formater les partitions et écrire la nouvelle table des partitions sur le disque.



1. **Choix de confirmation**

L'utilisateur a sélectionné l'option **Oui** (étape ①) pour autoriser l'application des changements.

2. **Validation**

Cliquer sur le bouton **Continuer** (étape ②) permet de lancer effectivement le formatage et l'écriture sur le disque.

Installation du système de base

Cette étape marque le début de l'installation effective du système Debian. Elle consiste à copier et configurer les fichiers essentiels au bon fonctionnement du système d'exploitation.

Objectif :

- Installer les composants de base nécessaires à l'exécution du système (bibliothèques, noyau, utilitaires de gestion, etc.).

Détail des actions visibles à l'écran :

- Le système procède à l'**installation du système de base**, comme indiqué par la barre de progression.
- La mention *« Validation de libhogweed6… »* indique qu'un paquet spécifique est en cours de traitement.

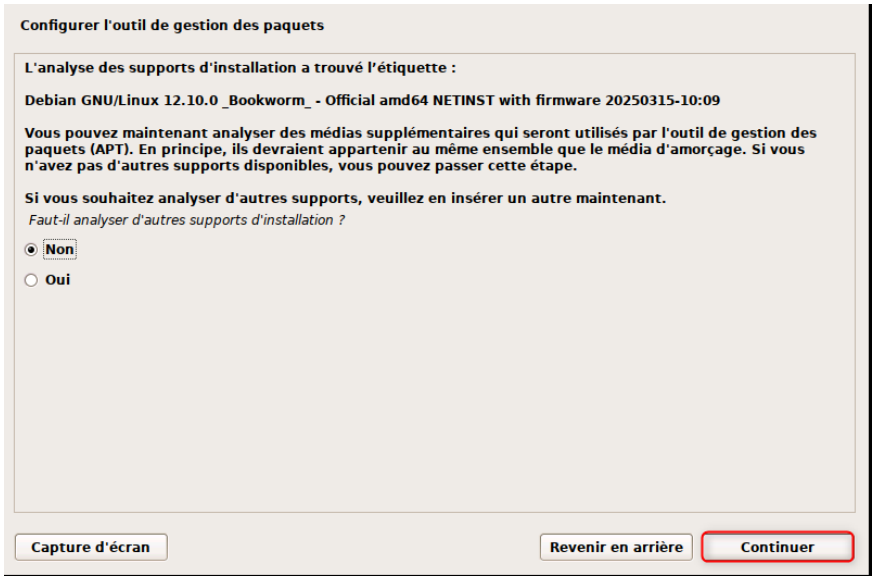
Configuration de l'outil de gestion des paquets

Lors de cette phase, l'installeur identifie le support d'installation utilisé et propose éventuellement d'ajouter d'autres sources pour la récupération des paquets logiciels.

- Valider le support d'installation principal contenant les paquets.
- Proposer à l'utilisateur d'ajouter des sources supplémentaires si nécessaire (ex : autre CD/DVD ou clé USB).

  Le système détecte automatiquement le média d'installation en cours :
  Debian GNU/Linux 12.10.0 *Bookworm* – Official amd64 NETINST with firmware 20250315-10:09.
  Le message indique que ce média sera utilisé pour l'installation des paquets via l'outil APT.

L'utilisateur sélectionne **Non** (étape ①) car aucun support supplémentaire n'est requis dans ce contexte.



Cliquer sur le bouton **Continuer** (étape ②) permet de passer à l'étape suivante.

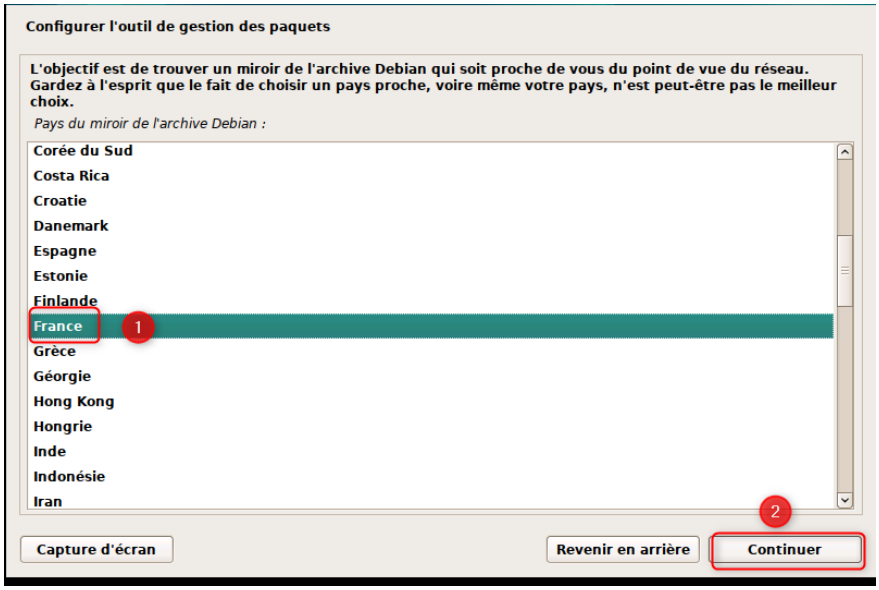
Cette étape est utile uniquement si vous disposez de plusieurs sources de paquets physiques. Dans la majorité des cas (comme ici), elle peut être ignorée en toute sécurité.

Sélection du pays pour le miroir Debian

Cette étape permet de configurer le téléchargement des paquets via un **miroir réseau**. Un miroir Debian est un serveur contenant les fichiers nécessaires à l'installation et à la mise à jour du système.

- Choisir un pays géographiquement proche afin d'optimiser la rapidité des téléchargements.
- Faciliter la connexion à un miroir fiable et à jour.

1. Sélection du pays **France** dans la liste des miroirs disponibles (étape ①).
2. Valider la sélection en cliquant sur le bouton **Continuer** (étape ②).



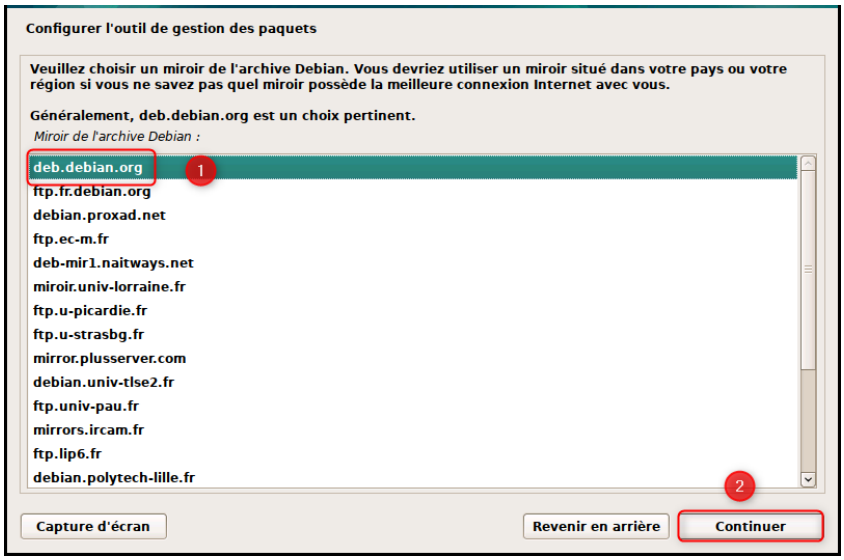
Sélection du miroir Debian

Une fois le pays sélectionné, l'installeur propose une liste de **miroirs** disponibles dans la région. Ces miroirs sont des serveurs hébergeant les fichiers nécessaires à l'installation et à la mise à jour du système Debian.

Objectif :

- Choisir un miroir fiable et performant pour télécharger les paquets via le gestionnaire APT.
- Optimiser la vitesse d'installation et de mise à jour.

Détail des actions visibles à l'écran :



1. Sélection du miroir **deb.debian.org**, recommandé par défaut pour sa stabilité et sa répartition mondiale (étape ①).
2. Cliquer sur **Continuer** pour valider le choix et passer à l'étape suivante (étape ②).

Configuration d'un mandataire HTTP (proxy)

Dans cette étape, le programme d'installation propose d'indiquer un mandataire HTTP (également appelé proxy) si l'accès à Internet est restreint dans l'environnement réseau.

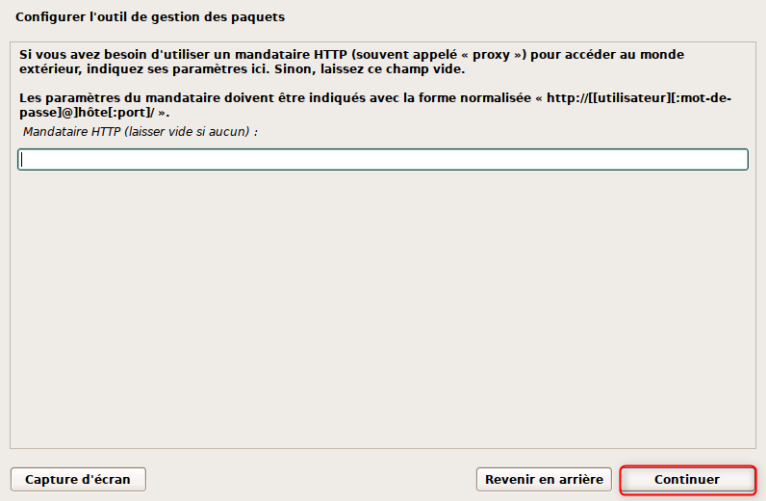
Objectif :

- Permettre à l'outil APT de télécharger les paquets via un serveur mandataire, si nécessaire.

Situation spécifique :

Dans le cadre de cette installation, **aucun proxy n'est requis**. Le champ « Mandataire HTTP » est donc **laissé vide**.

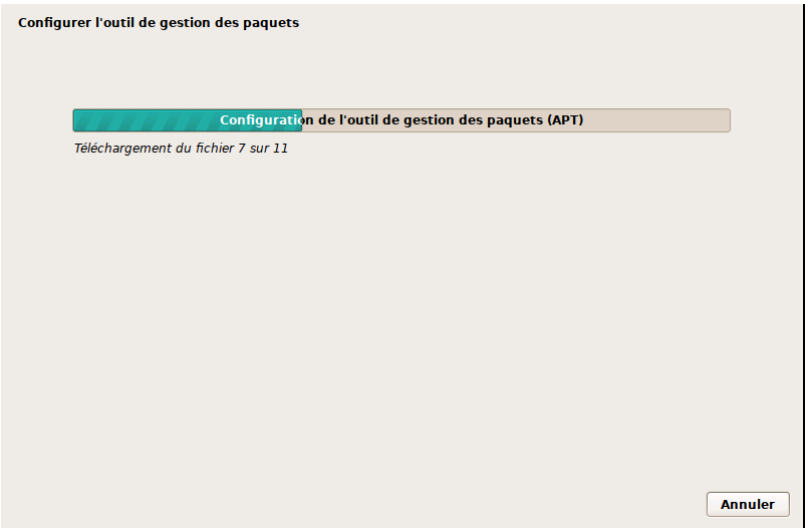
Laisser le champ de saisie vide, car aucune configuration proxy n'est nécessaire.
Cliquer sur **Continuer** pour valider et passer à l'étape suivante.
Remarque : Cette étape est optionnelle et ne bloque pas l'installation si elle est ignorée.



Téléchargement des fichiers de configuration APT

Une fois le miroir Debian sélectionné et, le cas échéant, le mandataire HTTP configuré (ou laissé vide si inutile), l'installateur procède automatiquement à la configuration de l'outil de gestion des paquets APT.

- Télécharger les fichiers nécessaires à la gestion des paquets Debian.
- Préparer l'environnement pour l'installation des paquets supplémentaires.



- Une barre de progression indique l'état d'avancement du téléchargement (ici, **fichier 7 sur 11**).
- Aucun paramètre n'est requis de la part de l'utilisateur à cette étape.

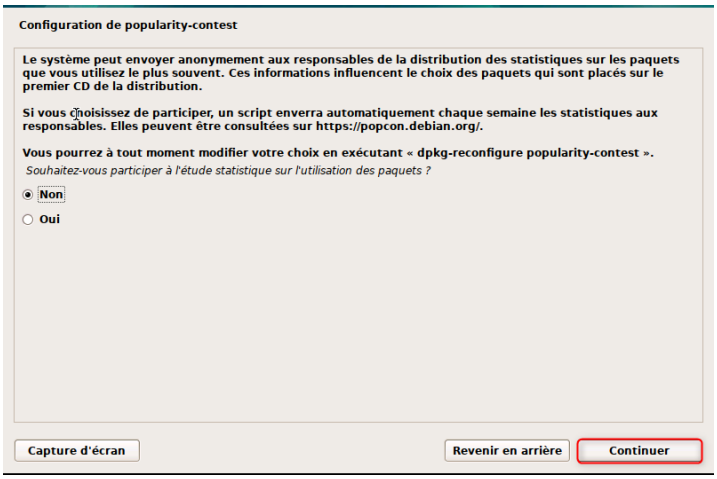
Remarque : Cette opération peut prendre plusieurs minutes selon la vitesse de connexion Internet et la réactivité du miroir sélectionné.

Configuration de popularity-contest

Cette étape propose à l'utilisateur de participer à une étude statistique anonyme sur l'utilisation des paquets Debian installés.

Permettre à la communauté Debian de recueillir des données d'usage réelles afin de :

- Mieux prioriser les paquets les plus utilisés sur les supports d'installation,
- Améliorer l'optimisation de la distribution.
- Dans ce cas précis, l'option **"Non"** est sélectionnée (voir capture d'écran).
- Le système n'enverra donc aucune donnée statistique aux serveurs Debian.



Informations complémentaires :

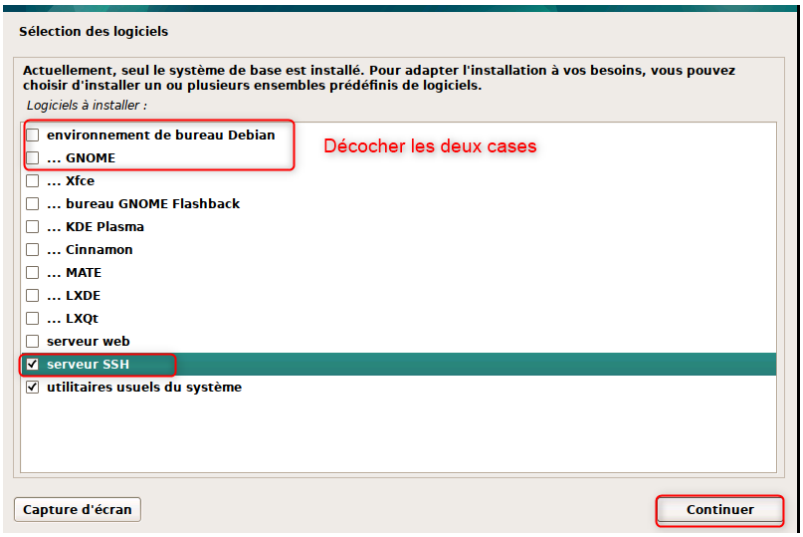
- En cas de changement d'avis, il est possible de reconfigurer cette option ultérieurement à l'aide de la commande :

Sélection des logiciels à installer

À ce stade, seul le système de base est installé. L'installeur propose d'ajouter des ensembles de logiciels prédéfinis en fonction de l'usage prévu du système.

Objectif :

Permettre à l'utilisateur de choisir les composants à installer selon le rôle futur de la machine.



1. **Désélection de l'environnement graphique** :
Les cases « **environnement de bureau Debian** » et ses variantes (GNOME, KDE, etc.) sont **décochées** afin d'obtenir une installation **minimaliste en mode texte**, adaptée à un usage serveur ou à une configuration personnalisée.

2. **Activation du serveur SSH** :
La case « **serveur SSH** » est cochée, ce qui permet l'accès distant sécurisé à la machine via le protocole SSH.

3. **Utilitaires usuels du système** :
Cette option est cochée par défaut et **conservée** pour garantir l'installation d'outils de base nécessaires au bon fonctionnement du système Debian.

Résultat attendu :

À la fin de cette étape, le système sera installé sans interface graphique, mais avec les utilitaires essentiels et un accès distant possible via SSH.

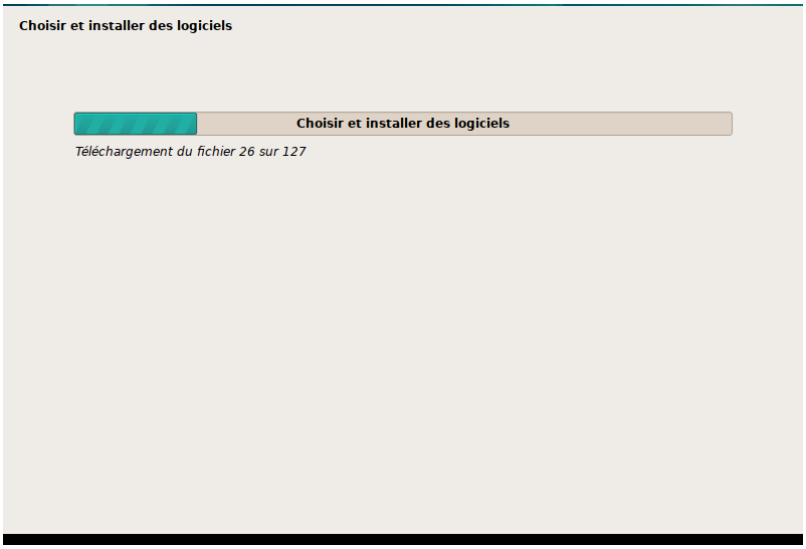
Téléchargement et installation des logiciels sélectionnés

Une fois les options de logiciels validées (serveur SSH + utilitaires système), l'installeur Debian procède automatiquement à leur **téléchargement** et à leur **installation**.

Objectif :

Installer les paquets nécessaires au bon fonctionnement du système, en fonction des choix faits à l'étape précédente.

- Une **barre de progression** permet de suivre l'état d'avancement.
- L'indicateur « Téléchargement du fichier X sur Y » informe du nombre de paquets en cours de traitement.



À savoir :

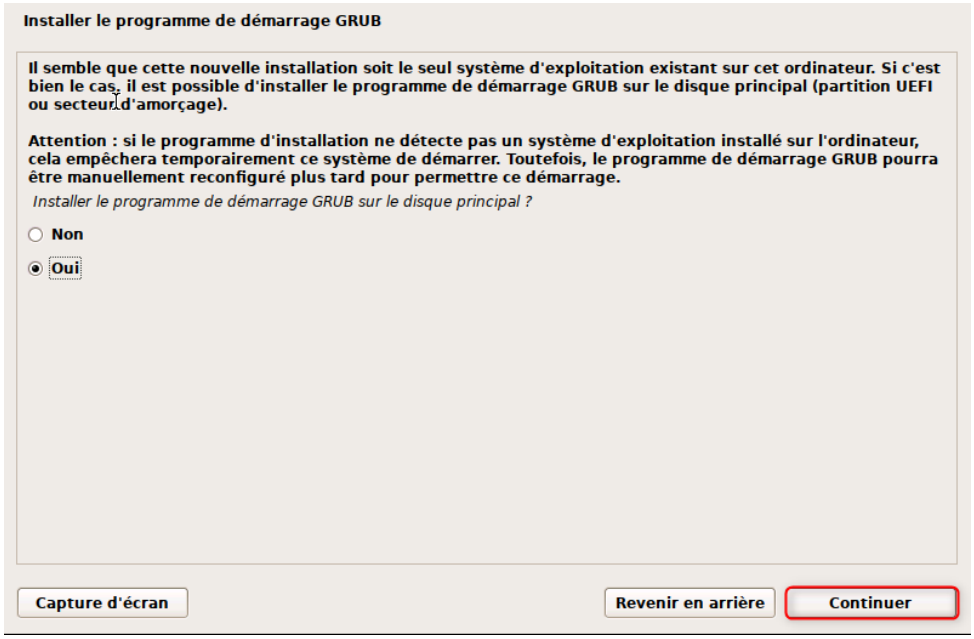
- Cette étape peut durer plusieurs minutes selon la **vitesse de connexion Internet**.
- Aucune intervention manuelle n'est nécessaire à ce stade.

Installation du programme de démarrage GRUB

Cette étape permet d'installer le chargeur d'amorçage GRUB, nécessaire pour démarrer le système Debian installé.

Objectif :

Installer **GRUB** sur le disque principal, afin que l'ordinateur puisse démarrer automatiquement sur le nouveau système Debian.



1. L'option **Oui** est sélectionnée (par défaut), car il s'agit de la seule installation présente sur l'ordinateur.
2. Cliquer sur **Continuer** pour valider et poursuivre l'installation.

À savoir :

- GRUB est indispensable pour que le système soit amorçable.
- Si aucun système n'est détecté, Debian considère que GRUB doit être installé.
- En cas de multi-boot, une configuration plus avancée pourrait être requise.

Choix du périphérique d'installation de GRUB

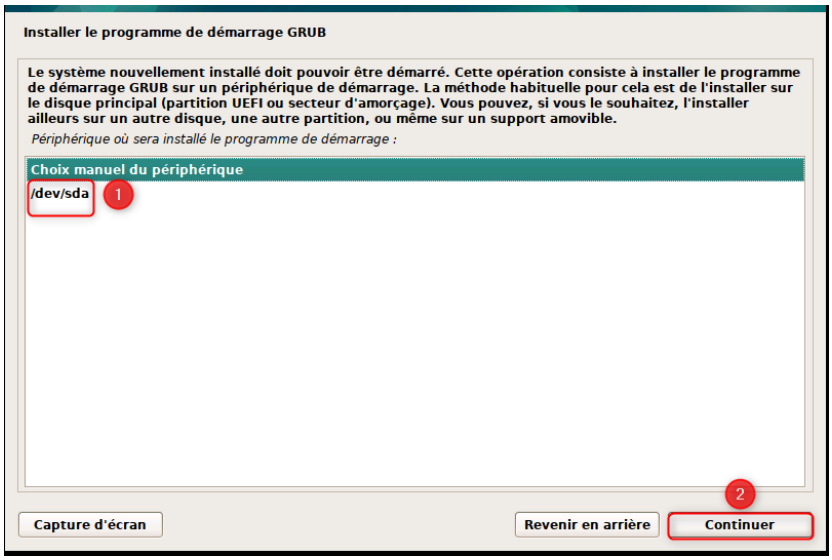
Cette étape consiste à spécifier **sur quel disque** sera installé le chargeur d'amorçage GRUB, afin de rendre le système bootable.

Objectif :

Installer **GRUB** sur le disque principal (/dev/sda) pour garantir que Debian se lance automatiquement au démarrage de la machine.

Détail de l'écran :

1. L'utilisateur sélectionne **/dev/sda**, correspondant au disque principal (étape ①).
2. Cliquer sur **Continuer** pour valider ce choix et finaliser l'installation de GRUB (étape ②).



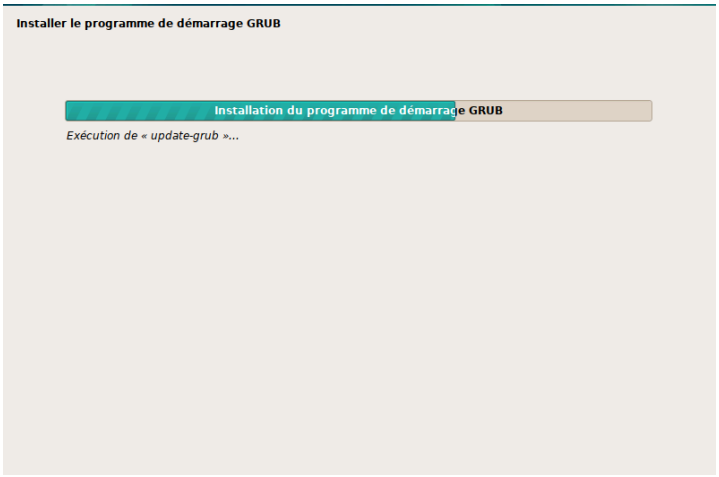
Remarques :

- /dev/sda est généralement le premier disque détecté, utilisé pour l'amorçage.
- Il est essentiel de ne pas confondre avec une partition spécifique comme /dev/sda1.
- Ce choix assure un démarrage automatique sans intervention manuelle après redémarrage.

Installation de GRUB

Objectif :

Finaliser l'installation du gestionnaire de démarrage **GRUB** afin de permettre le lancement de Debian automatiquement au démarrage du PC.



- Une **barre de progression** indique l'installation en cours du programme de démarrage.
- Le message « Exécution de update-grub… » confirme que GRUB est mis à jour pour reconnaître les systèmes installés.

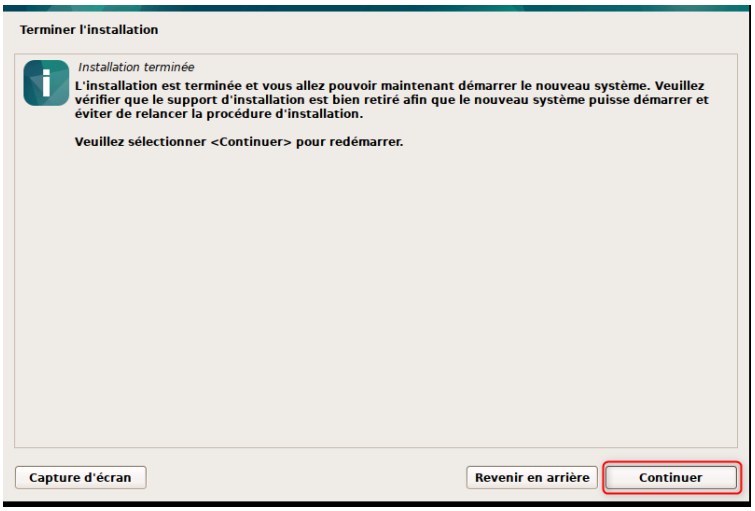
Remarques :

- Cette opération est automatique et ne nécessite pas d'intervention.
- À la fin de cette étape, le système est prêt à démarrer normalement depuis le disque principal.

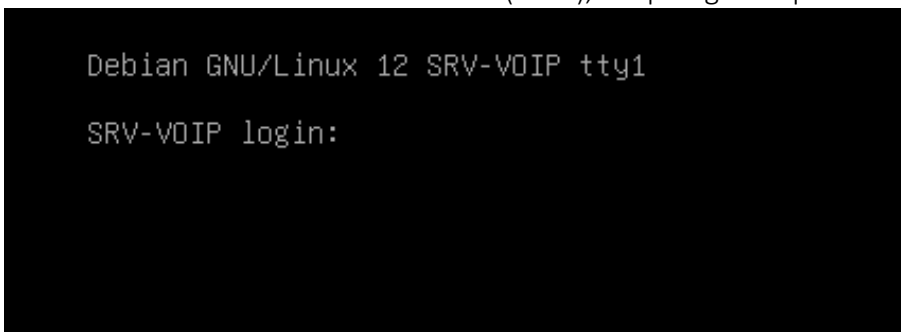
Terminer l'installation

Finaliser le processus d'installation de Debian et redémarrer sur le nouveau système.

- Le message confirme que **l'installation est complète**.
- Il est demandé de **retirer le support d'installation** (clé USB, CD, etc.) avant de continuer, pour éviter de relancer l'installation au redémarrage.
- Cliquer sur le bouton **Continuer** déclenchera le **redémarrage de la machine**.



Parfait ! Ce dernier écran indique que le système **Debian 12 a démarré correctement**. Tu arrives sur l'invite de connexion en mode console (TTY1), ce qui signifie que :



- L'installation s'est bien déroulée
- Le nom de la machine est bien SRV-VOIP (comme défini pendant l'installation)

Connexion à la machine

La machine **SRV-VOIP**, fraîchement installée sous **Debian GNU/Linux 12**, est désormais opérationnelle. Voici les points clés vérifiés :

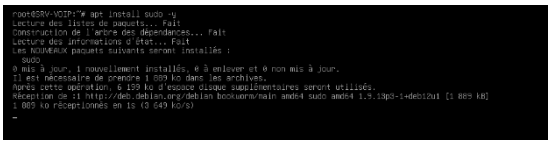
- **Adresse IP** attribuée : 192.168.10.60/24
- **Passerelle par défaut** : 192.168.10.254
- **Résolution DNS** : assurée via les serveurs internes 192.168.10.10 et 192.168.10.30
- **Connexion Internet** : testée avec succès par un ping vers 8.8.8.8 (0 % de perte de paquets)

La connectivité réseau est donc fonctionnelle et stable.

```
root@SRV-VOIP:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:25:09:72 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.60/24 brd 192.168.10.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe25:972/64 scope link
       valid_lft forever preferred_lft forever
root@SRV-VOIP:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=10.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=12.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=11.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=127 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=127 time=12.8 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=127 time=11.0 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=127 time=10.6 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=127 time=12.3 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=127 time=11.0 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=127 time=10.2 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=127 time=10.2 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=127 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=127 time=10.7 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=127 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=127 time=10.4 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=127 time=10.3 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=127 time=10.6 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=127 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=127 time=18.2 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=127 time=12.3 ms
^C
--- 8.8.8.8 ping statistics ---
25 packets transmitted, 25 received, 0% packet loss, time 24052ms
rtt min/avg/max/mdev = 10.232/11.302/18.206/1.563 ms
root@SRV-VOIP:~# _
```

Installation du paquet sudo

- Commande exécutée : apt install sudo -y
- Version installée : 1.9.13p3-1+deb12u1 (issue des dépôts Debian Bookworm)
- Espace disque utilisé : ~6,2 Mo



Ajout user dans le groupe sudo dans Debian 12

Comme on le voit dans ton terminal, l'utilisateur billy a bien été ajouté au groupe sudo
usermod -aG sudo billy

```
root@SRV-VOIP:~# usermod -aG sudo billy
root@SRV-VOIP:~# groups billy
billy : billy cdrom floppy sudo audio dip video plugdev users netdev
root@SRV-VOIP:~#
```

Mise à jour du système et installation des dépendances sudo apt update && sudo apt upgrade -y

Cette commande est composée de deux instructions distinctes reliées par les symboles &&, ce qui indique que la seconde instruction (sudo apt upgrade -y) ne sera exécutée que si la première (sudo apt update) s'exécute correctement et sans erreur.

```
billy@SRV-VOIP:~$ sudo apt update && sudo apt upgrade -y
[sudo] Mot de passe de billy :
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Réception de :2 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Réception de :3 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Réception de :4 http://security.debian.org/debian-security bookworm-security/main Sources [153 kB]
Réception de :5 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [260 kB]
Réception de :6 http://security.debian.org/debian-security bookworm-security/main Translation-en [156 kB]
672 ko réceptionnés en 9s (71,9 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
billy@SRV-VOIP:~$
```

- sudo :
  - Permet d'exécuter la commande avec des privilèges administratifs (root). Cela est nécessaire car ces opérations touchent au système lui-même et nécessitent des droits spécifiques.
- apt update :
  - Met à jour la liste des paquets disponibles à partir des sources configurées dans le fichier /etc/apt/sources.list et du répertoire /etc/apt/sources.list.d/.
  - Télécharge uniquement les informations sur les dernières versions disponibles des paquets, sans modifier ni installer aucun paquet.
- apt upgrade -y :
  - Met à jour tous les paquets installés sur le système vers leur version la plus récente disponible dans les dépôts.
  - L'argument -y (yes) permet de répondre automatiquement « oui » à toutes les questions posées par le gestionnaire de paquets durant le processus d'installation, évitant ainsi une interaction manuelle.

Cela signifie que votre système est déjà totalement à jour à l'instant de l'exécution de cette commande, et aucune action supplémentaire n'était nécessaire.

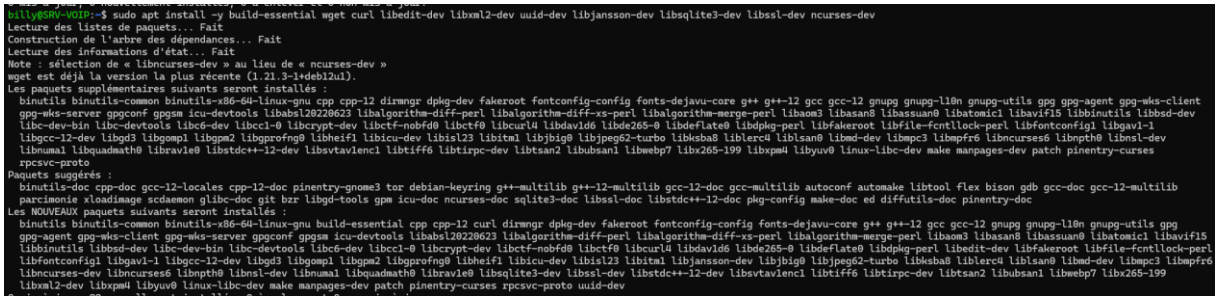
Cette commande exécute une installation groupée de plusieurs paquets essentiels et de bibliothèques nécessaires au développement logiciel, notamment pour compiler et exécuter certaines applications sur Debian 12.

- sudo :

- Utilisé pour exécuter les commandes avec les droits administrateurs nécessaires à l'installation de paquets système.

- apt install -y :
  - Installe les paquets spécifiés en argument.
  - Le paramètre -y automatise la réponse affirmative à toutes les questions posées lors de l'installation.

- Description des paquets installés :
  - build-essential : Méta-paquet regroupant les outils de base nécessaires à la compilation de logiciels (gcc, make, etc.).
  - wget : Outil permettant le téléchargement de fichiers depuis Internet via la ligne de commande.
  - curl : Outil en ligne de commande permettant d'effectuer des transferts de données avec des URL, notamment utile pour récupérer des fichiers ou interagir avec des API.
  - libedit-dev : Bibliothèque d'édition de lignes en mode interactif utilisée principalement pour gérer les interactions utilisateur en terminal.
  - libxml2-dev : Bibliothèque permettant le traitement des documents XML.
  - uuid-dev : Bibliothèque permettant la création et gestion d'identifiants uniques universels (UUID).
  - libjansson-dev : Bibliothèque légère permettant l'encodage, le décodage et la manipulation de données JSON.
  - libsqlite3-dev : Bibliothèque de développement pour SQLite, une base de données embarquée légère.
  - libssl-dev : Bibliothèque de développement pour le chiffrement SSL/TLS, nécessaire à la sécurisation des communications réseau.
  - ncurses-dev : Bibliothèque permettant le développement d'interfaces utilisateur interactives en mode texte (TUI).

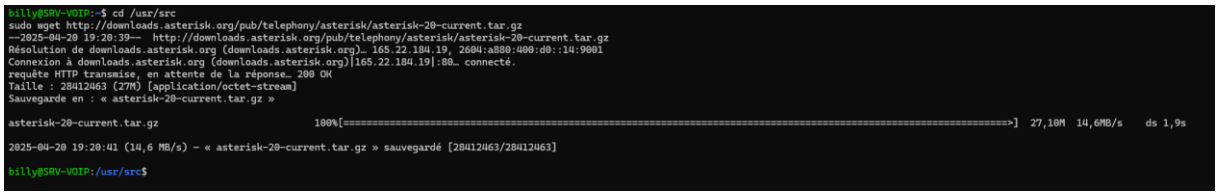


Téléchargement et extraction des sources d'Asterisk :

Téléchargement des sources :

cd /usr/src
sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20-current.tar.gz

- cd /usr/src :
  - La commande cd signifie Change Directory (« changer de répertoire »).
  - Le chemin /usr/src est traditionnellement utilisé sur les systèmes Linux pour stocker le code source des applications ou modules destinés à être compilés depuis les sources.
- sudo wget :
  - Exécute le téléchargement avec des droits administrateurs (privilège root), nécessaire pour écrire dans le répertoire /usr/src.
  - wget est une commande permettant de récupérer du contenu depuis un serveur web via le protocole HTTP ou HTTPS.
- URL :
  http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20-current.tar.gz
  - Ceci est l'adresse complète menant vers le serveur officiel d'Asterisk pour télécharger la dernière version stable actuelle (version 20) sous forme d'archive compressée au format .tar.gz.
- Archive .tar.gz :
  - Format combinant TAR (archive) et GZip (compression), largement utilisé sous Unix/Linux.
  - Elle contient les fichiers sources nécessaires pour compiler et installer l'application (ici : Asterisk).



Extraction des fichiers sources :

sudo tar xvf asterisk-20-current.tar.gz

```
billy@SRV-VOIP:/usr/src$ sudo tar xvf asterisk-20-current.tar.gz
asterisk-20.13.0/
asterisk-20.13.0/.cleancount
asterisk-20.13.0/.gitignore
asterisk-20.13.0/.lastclean
asterisk-20.13.0/.version
asterisk-20.13.0/BSDmakefile
asterisk-20.13.0/BUGS
asterisk-20.13.0/CHANGES.html
asterisk-20.13.0/CHANGES.md
asterisk-20.13.0/COPYING
asterisk-20.13.0/CREDITS
asterisk-20.13.0/ChangeLogs/
asterisk-20.13.0/ChangeLogs/ChangeLog-20.10.0.md
```

sudo :

- Utilisé afin d'exécuter la commande avec les privilèges administratifs requis pour l'extraction des fichiers dans un répertoire système (/usr/src).

tar :

- La commande tar (tape archive) est utilisée pour archiver et désarchiver des fichiers sous Unix/Linux.

Arguments utilisés avec tar :

- x : (extract) extrait le contenu d'une archive.
- v : (verbose) affiche les détails de l'extraction à l'écran, fichier par fichier.
- f : (file) indique que l'on spécifie un fichier d'archive en particulier à manipuler.

Nom de l'archive :

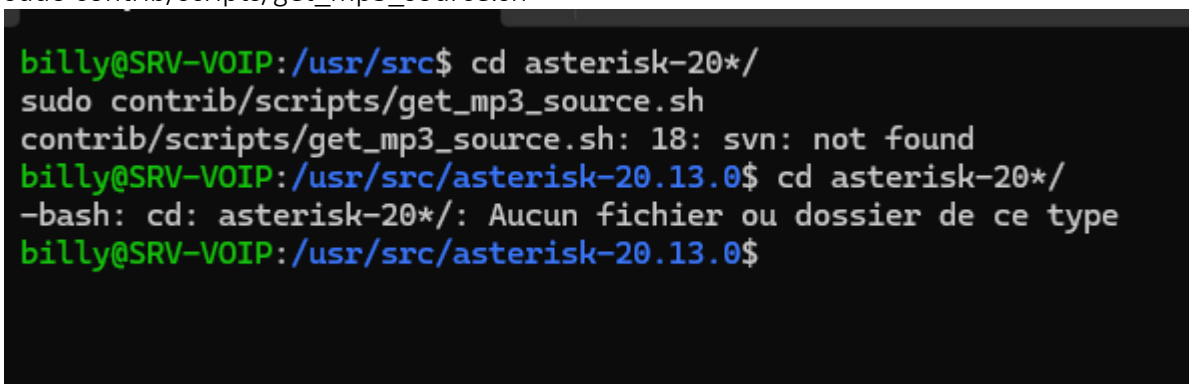
- asterisk-20-current.tar.gz : Archive compressée contenant les fichiers sources nécessaires à la compilation et l'installation du logiciel Asterisk, version 20.

Ces fichiers sont essentiels pour préparer l'environnement de compilation, examiner les notes de version et valider la conformité des licences avant installation.

Compilation d'Asterisk :

Préparation à la compilation :

cd asterisk-20*/
sudo contrib/scripts/get_mp3_source.sh



Dans cette capture d'écran, on observe deux problèmes distincts :

- Erreur lors de l'exécution du script get_mp3_source.sh
- Cette erreur indique que le programme svn (Subversion) n'est pas installé sur ton système Debian. Ce script utilise svn pour récupérer le support MP3 pour Asterisk.
- Solution : Installer subversion avec :
  sudo apt install subversion -y

Problème de chemin (cd asterisk-20*/ ne fonctionne plus) :

-bash: cd: asterisk-20*/: Aucun fichier ou dossier de ce type
Cette erreur survient car tu es déjà à l'intérieur du dossier nommé explicitement asterisk-20.13.0. Une fois dedans, le dossier asterisk-20*/ n'existe plus.

Suite des opérations après la correction du problème MP3 :

Étape suivante (Vérification et compilation) :

Cette commande vérifie que toutes les dépendances nécessaires sont présentes avant la compilation
sudo ./configure

```
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$ sudo ./configure
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether the compiler supports GNU C... yes
checking whether gcc accepts -g... yes
checking for gcc option to enable C11 features... none needed
checking for stdio.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
checking for strings.h... yes
checking for sys/stat.h... yes
```

```
checking for shasum... /usr/bin/shasum
checking for openssl... /usr/bin/openssl
checking for pkg-config... no
configure: error: pkg-config not found
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$
```

Ce message d'erreur provient d'un script configure utilisé lors de la préparation d'une compilation logicielle (dans ce contexte, la préparation de la compilation d'Asterisk depuis ses sources).

- checking for pkg-config... no :
    - Le script vérifie la présence de l'outil **pkg-config**, essentiel à la compilation de certains logiciels. Cet outil permet de récupérer automatiquement les informations nécessaires sur les bibliothèques installées sur le système (chemins, dépendances, versions, etc.).
- configure: error: pkg-config not found :
    - Ce message indique clairement que l'outil requis (pkg-config) est absent du système, entraînant l'arrêt immédiat du script de configuration. Il est impératif d'installer cet outil avant de poursuivre le processus.

Solution immédiate (à exécuter maintenant) :

Installe pkg-config avec la commande suivante :
sudo apt install pkg-config -y

- sudo :
    - Permet d'exécuter la commande avec des privilèges administratifs (nécessaire pour modifier des éléments système).
- apt install pkg-config -y :

- Lance l'installation du paquet logiciel **pkg-config** avec APT, le gestionnaire de paquets utilisé sur Debian.
- L'option -y valide automatiquement toutes les demandes durant l'installation, ce qui évite toute intervention manuelle.

- pkg-config :
  - Outil utilisé durant la compilation de logiciels, permettant de récupérer automatiquement les paramètres de compilation nécessaires à l'intégration de bibliothèques externes.

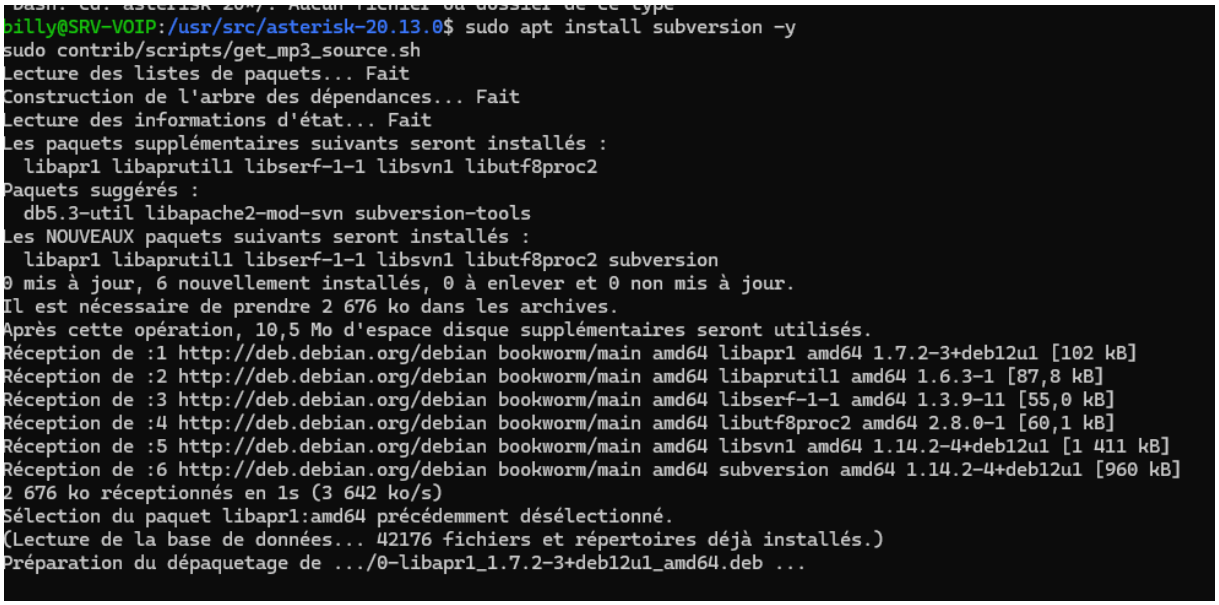
```
configure: error: pkg-config not found
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$ sudo apt install pkg-config -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libpkgconf3 pkgconf pkgconf-bin
Les NOUVEAUX paquets suivants seront installés :
  libpkgconf3 pkg-config pkgconf pkgconf-bin
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 105 ko dans les archives.
Après cette opération, 283 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libpkgconf3 amd64 1.8.1-1 [36,1 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 pkgconf-bin amd64 1.8.1-1 [29,5 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 pkgconf amd64 1.8.1-1 [25,9 kB]
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 pkg-config amd64 1.8.1-1 [13,7 kB]
105 ko réceptionnés en 0s (866 ko/s)
Sélection du paquet libpkgconf3:amd64 précédemment désélectionné.
(Lecture de la base de données... 42323 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libpkgconf3_1.8.1-1_amd64.deb ...
Dépaquetage de libpkgconf3:amd64 (1.8.1-1) ...
Sélection du paquet pkgconf-bin précédemment désélectionné.
Préparation du dépaquetage de .../pkgconf-bin_1.8.1-1_amd64.deb ...
Dépaquetage de pkgconf-bin (1.8.1-1) ...
Sélection du paquet pkgconf:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../pkgconf_1.8.1-1_amd64.deb ...
Dépaquetage de pkgconf:amd64 (1.8.1-1) ...
Sélection du paquet pkg-config:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../pkg-config_1.8.1-1_amd64.deb ...
Dépaquetage de pkg-config:amd64 (1.8.1-1) ...
Paramétrage de libpkgconf3:amd64 (1.8.1-1) ...
Paramétrage de pkgconf-bin (1.8.1-1) ...
Paramétrage de pkgconf:amd64 (1.8.1-1) ...
Paramétrage de pkg-config:amd64 (1.8.1-1) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u10) ...
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$
```

Commandes à exécuter pour corriger immédiatement :

sudo apt install subversion -y
sudo contrib/scripts/get_mp3_source.sh
Installer Subversion (outil de gestion de version) et ses dépendances, nécessaires notamment pour récupérer le code source de modules ou plugins via des dépôts SVN.
Composants installés :

- Paquet principal :
  - subversion
- Dépendances :

- libapr1
- libaprutil1
- libserf-1-1
- libsvn1
- libutf8proc2



Après avoir installé cette dépendance, relance à nouveau la commande :
sudo ./configure

Explication des étapes clés :

- Vérification des dépendances :
  - checking for libxml2.0... yes → La bibliothèque libxml2 est détectée et disponible.
  - checking for gtk+-2.0... no → La bibliothèque GTK+ 2.0 n'est pas présente, mais elle n'est pas indispensable pour la compilation standard d'Asterisk.
- Création des fichiers de configuration :
  - config.status: creating makeopts → Génération du fichier contenant les options de compilation.
  - config.status: creating autoconfig.h → Génération d'un fichier d'en-tête utilisé pour adapter la compilation au système.

- Confirmation de configuration réussie :
    - configure: Menuselect build configuration successfully completed → Le système de configuration interne d'Asterisk (Menuselect) a été généré correctement. Ce composant permet de choisir les modules à inclure dans la compilation.

```
checking for libxml-2.0... yes
checking for gtk+-2.0... no
configure: creating ./config.status
config.status: creating makeopts
config.status: creating autoconfig.h
configure: Menuselect build configuration successfully completed

              .$$$$$$$$$$$$$$=..
           .$7$7..          .7$$7:.
         .$$:.                ,$7.7
       .$7.     7$$$$          .$$77
     ..$$.      $$$$$           .$$$7
    ..7$   .?.   $$$$$   .?.      7$$$.
   $.$.   .$$$7. $$$$7 .7$$$.     .$$$.
 .777.   .$$$$$$77$$$77$$$$$7.     $$$,
 $$$~      .7$$$$$$$$$$$$$7.      .$$$.
.$$7         .7$$$$$$$7:          ?$$$.
$$$         ?7$$$$$$$$$I         .$$$7
$$$       .7$$$$$$$$$$$$$$      :$$$.
$$$       $$$$$$7$$$$$$$$$$    .$$$.
$$$        $$$   7$$$7  .$$$    .$$$.
$$$$              $$$$7         .$$$.
7$$$7             7$$$$       7$$$
 $$$$$                        $$$
  $$$$7.                       $$  (TM)
   $$$$$$$.           .7$$$$$$  $$
     $$$$$$$$$$$$$7$$$$$$$$.$$$$$$
       $$$$$$$$$$$$$$$.

configure: Package configured for:
configure: OS type  : linux-gnu
configure: Host CPU : x86_64
configure: build-cpu:vendor:os: x86_64 : pc : linux-gnu :
configure: host-cpu:vendor:os: x86_64 : pc : linux-gnu :
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$
```

Interface de sélection des modules (menuselect)

sudo make menuselect

```
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$ sudo make menuselect
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="--silent" cmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk-20.13.0/menuselect »
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES -I/usr/include/libxml2   -c -o menuselect.o menuselect.c
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES    -c -o strcompat.o strcompat.c
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES     -c -o menuselect_curses.o menuselect_curses.c
gcc  -o cmenuselect menuselect.o strcompat.o menuselect_curses.o -lncurses  -ltinfo  -lxml2
make[1] : on quitte le répertoire « /usr/src/asterisk-20.13.0/menuselect »
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="--silent" nmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk-20.13.0/menuselect »
make[1]: rien à faire pour « nmenuselect ».
make[1] : on quitte le répertoire « /usr/src/asterisk-20.13.0/menuselect »
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="--silent" gmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk-20.13.0/menuselect »
make[1]: rien à faire pour « gmenuselect ».
make[1] : on quitte le répertoire « /usr/src/asterisk-20.13.0/menuselect »
make[1] : on entre dans le répertoire « /usr/src/asterisk-20.13.0 »
Generating input for menuselect ...
```

make :

- Outil de construction qui lit les fichiers Makefile pour automatiser le processus de compilation.

menuselect :

- Cible spécifique du Makefile d'Asterisk.
- Construit une interface utilisateur en mode texte (TUI) permettant de sélectionner :

- les codecs à activer,
- les modules SIP, IAX, MGCP,
- les bibliothèques facultatives ou expérimentales,
- et autres composants du cœur Asterisk.

Compilation des dépendances :

- On observe la compilation de fichiers comme :
  - menuselect.o, strcompat.o, menuselect_curses.o
- Ces fichiers sont nécessaires au bon fonctionnement de l'interface de configuration.

Utilisation de flags de compilation :

- -Wall : active tous les avertissements du compilateur.
- -Wno-deprecated-declarations : ignore les avertissements liés à l'usage de fonctions obsolètes.
- -DHAVE_NCURSES, -I/usr/include/libxml2 : indique que certaines bibliothèques sont bien disponibles pour la compilation.

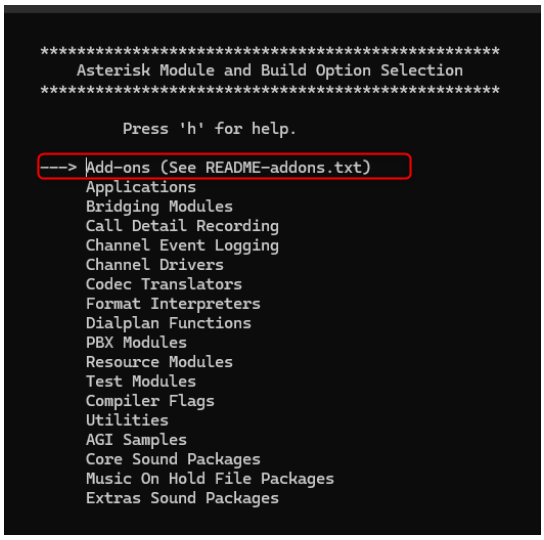
Add-ons :

- Cette section regroupe les **modules supplémentaires non activés par défaut**. Ils offrent des fonctionnalités avancées ou spécifiques, non critiques pour une installation de base.
- Ces modules peuvent dépendre de bibliothèques tierces ou être destinés à des cas d'usage particuliers.
- La mention (See README-addons.txt) renvoie à un fichier inclus dans les sources Asterisk, décrivant en détail chaque module complémentaire.

- Autres sections du menu :
  - **Applications** : modules d'actions dans le dialplan (ex : Dial, Hangup, Voicemail).
  - **Channel Drivers** : pilotes SIP, PJSIP, DAHDI, etc.
  - **Codec Translators** : prise en charge des codecs audio (G.711, G.729, Opus...).
  - **PBX Modules** : fonctionnalités cœur du système PBX d'Asterisk.
  - **Sound Packages** : jeux de fichiers audio utilisés pour les annonces système ou la musique d'attente.

Actions possibles :

- Navigation :
  - Utiliser les flèches du clavier pour se déplacer dans le menu.
  - Appuyer sur Entrée pour accéder aux sous-menus.
  - Utiliser la touche s pour (dé)sélectionner un module.
  - Permet à l'administrateur de **personnaliser finement** l'installation pour ne compiler que les composants nécessaires, optimisant ainsi la performance et la sécurité de l'instance Asterisk.



Symboles affichés :

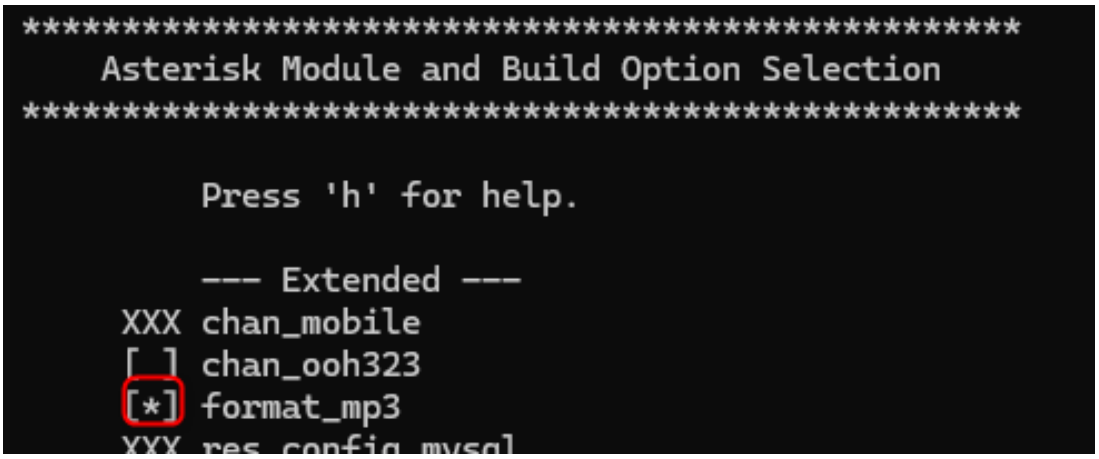
- XXX : le module est **désactivé** et **non disponible** pour compilation, souvent en raison d'une dépendance manquante.
- [ ] : le module est **disponible mais non sélectionné**.
- [*] : le module est **sélectionné pour compilation**.
- **Module sélectionné :**
- **[*] format_mp3** :

Ce module est activé pour la compilation.

- Il permet à Asterisk de **lire ou d'écrire des fichiers audio au format MP3**.
- Nécessite généralement la bibliothèque mp3 et l'exécution du script contrib/scripts/get_mp3_source.sh (comme effectué précédemment dans le processus).
- Ce module est particulièrement utile si le système doit gérer de la messagerie vocale, des musiques d'attente ou des enregistrements au format .mp3.

Modules non activés :

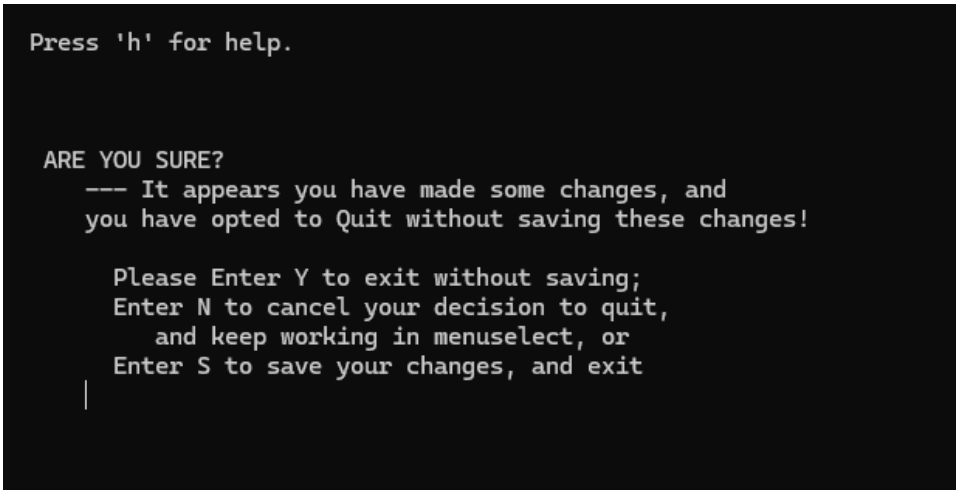
- **chan_mobile** : non compilé, dépend d'une pile Bluetooth (désactivé — XXX).
- **chan_ooh323** : désactivé par défaut, prend en charge le protocole H.323.



Après avoir modifié la configuration des modules dans **Menuselect** (comme l'activation de format_mp3), une tentative de quitter le menu sans sauvegarder a été détectée. Menuselect interrompt alors l'action pour demander confirmation.

Options proposées :

- Y (Yes) :
  - Quitter **sans enregistrer** les modifications.
  - Tout changement effectué (par exemple l'activation de modules) sera perdu.
- N (No) :
  - Annuler la sortie.
  - Retour immédiat à l'interface Menuselect pour poursuivre la configuration.
- S (Save) :
  - **Enregistrer** les modifications apportées.
  - Puis **quitter proprement** Menuselect.
  - C'est cette option qui doit être choisie si les sélections sont définitives et prêtes à être prises en compte dans la compilation.

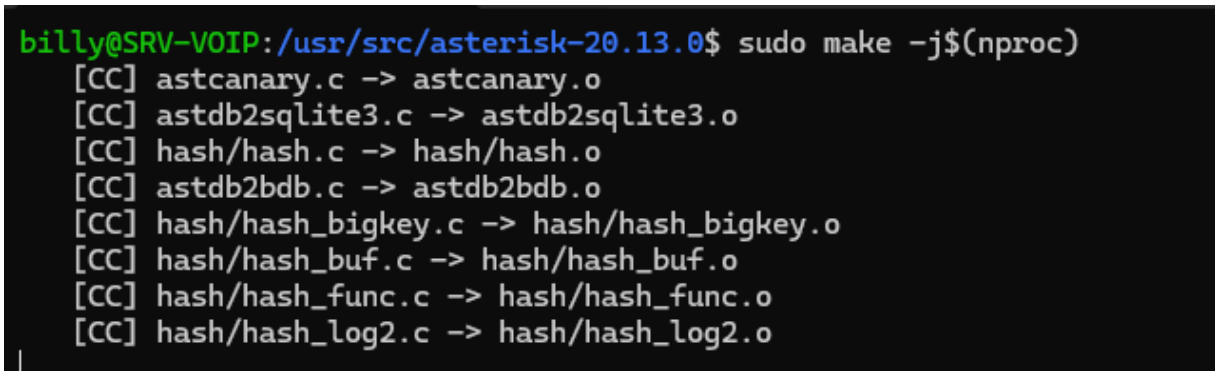


Compilation d'Asterisk

Cette commande compile Asterisk en utilisant tous les cœurs disponibles de ton processeur pour aller plus vite.
sudo make -j$(nproc)

Détail des composants de la commande :

- sudo :
  - Nécessaire pour exécuter la compilation dans un répertoire système comme /usr/src, ou pour installer ensuite les fichiers binaires dans des emplacements système.
- make :
  - Outil qui automatise le processus de compilation selon les instructions définies dans un fichier Makefile.
- -j$(nproc) :
  - Option **-j** (jobs) indique le nombre de tâches (compilations) à exécuter en parallèle.
  - $(nproc) est une substitution de commande shell renvoyant **le nombre de cœurs CPU** disponibles sur la machine.
  - Exemple : si nproc retourne 4, alors make -j4 lancera 4 processus de compilation en parallèle.
  - Cette approche permet de **réduire considérablement le temps de compilation**, en exploitant pleinement les ressources matérielles.



Installation des binaires + fichiers de config par défaut

sudo make install
sudo make samples
sudo make config
sudo ldconfig

Étapes automatiques lancées durant l'installation :
sudo make samples :

- Installe les **fichiers de configuration exemples** dans /etc/asterisk.
- Ces fichiers servent de base pour personnaliser le comportement d'Asterisk.
- Recommandé lors d'une première installation pour disposer d'une configuration fonctionnelle minimale.

sudo make config :

- Installe les **fichiers de service** nécessaires pour démarrer Asterisk via systemd (ou init.d selon la distribution).
- Permet d'exécuter des commandes comme :

sudo ldconfig :
Met à jour le cache des bibliothèques partagées du système, assurant que les bibliothèques compilées sont détectées correctement par le système au moment de l'exécution.

```
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$ sudo make install
sudo make samples
sudo make config
sudo ldconfig
Installing modules from channels...
Installing modules from pbx...
Installing modules from apps...
```

```
Installing file configs/samples/udptl.conf.sample
Installing file configs/samples/unistim.conf.sample
Installing file configs/samples/users.conf.sample
Installing file configs/samples/voicemail.conf.sample
Installing file configs/samples/xmpp.conf.sample
Updating asterisk.conf
/usr/bin/install -c -d "/var/spool/asterisk/voicemail/default/1234/INBOX"
build_tools/make_sample_voicemail "//var/lib/asterisk" "//var/spool/asterisk"
Installing file phoneprov/000000000000.cfg
Installing file phoneprov/000000000000-directory.xml
Installing file phoneprov/000000000000-phone.cfg
Installing file phoneprov/polycom_line.xml
Installing file phoneprov/polycom.xml
Installing file phoneprov/snom-mac.xml
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$
```

Lancer et activer Asterisk

sudo systemctl start asterisk
sudo systemctl enable asterisk
Résultat :

- Le service Asterisk a bien été démarré.

- Un message indique :

asterisk.service is not a native service, redirecting to systemd-sysv-install.
Cela signifie qu'Asterisk utilise un script SysV init (/etc/init.d/asterisk) et non une unité native systemd. → Ce comportement est normal et attendu sur certaines installations manuelles ou personnalisées.

```
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$ sudo systemctl start asterisk
sudo systemctl enable asterisk
asterisk.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable asterisk
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$
```

Vérifie que tout fonctionne :
sudo systemctl status asterisk
Service actif et en cours d'exécution :

```
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$ sudo systemctl status asterisk
● asterisk.service - LSB: Asterisk PBX
     Loaded: loaded (/etc/init.d/asterisk; generated)
     Active: active (running) since Sun 2025-04-20 20:12:36 CEST; 56s ago
       Docs: man:systemd-sysv-generator(8)
      Tasks: 66 (limit: 2273)
     Memory: 43.3M
        CPU: 3.016s
     CGroup: /system.slice/asterisk.service
             └─34828 /usr/sbin/asterisk

avril 20 20:12:36 SRV-VOIP systemd[1]: Starting asterisk.service - LSB: Asterisk PBX...
avril 20 20:12:36 SRV-VOIP asterisk[34816]: Starting Asterisk PBX: asterisk.
avril 20 20:12:36 SRV-VOIP systemd[1]: Started asterisk.service - LSB: Asterisk PBX.
billy@SRV-VOIP:/usr/src/asterisk-20.13.0$
```

Le service Asterisk est démarré avec succès, tourne actuellement, et a bien été activé pour démarrage automatique au prochain boot.

Configuration SIP avec PJSIP

Éditer le fichier pjsip.conf pour ajouter les comptes utilisateurs SIP

sudo nano /etc/asterisk/pjsip.conf
Ce fichier constitue un guide de référence rapide pour la configuration du module PJSIP dans Asterisk. Il ne remplace pas une documentation complète mais fournit :

- Des exemples de configuration minimale, utiles comme point de départ.
- Une liste condensée des options de configuration extraites depuis les fichiers XML de configuration.

Important : Le fichier ne contient pas la documentation exhaustive de toutes les options possibles. Il est recommandé de se référer à la documentation officielle pour des configurations complexes ou spécifiques.

Descendre jusqu'en bas du fichier

Définition du transport SIP

```
; === TRANSPORT ===
[transport-udp]
type=transport
protocol=udp
bind=0.0.0.0
```

section

- type=transport : Spécifie que cette définit un mécanisme de transport.
- protocol=udp : Utilise le protocole UDP pour les communications SIP.
- bind=0.0.0.0 : Écoute sur toutes les interfaces réseau disponibles.

Utilisateur Alice (poste 1001)

```
; === UTILISATEUR ALICE (1001) ===
[alice]
type=endpoint
transport=transport-udp
context=from-internal
disallow=all
allow=ulaw
auth=alice-auth
aors=alice
```

Endpoint – [alice]
type=endpoint : Déclare un terminal SIP (ici, Alice).
transport=transport-udp : Associe le transport défini plus haut.
context=from-internal : Définit le contexte du dialplan utilisé pour cet utilisateur.
disallow=all / allow=ulaw : Bloque tous les codecs sauf ulaw.
auth=alice-auth : Associe la section d'authentification définie ci-dessous.
aors=alice : Associe le point de contact (AOR).

Auth – [alice-auth]

type=auth : Déclare une méthode d'authentification.
auth_type=userpass : Authentification par nom d'utilisateur / mot de passe.
username / password : Identifiants SIP de connexion.

```
[alice-auth]
type=auth
auth_type=userpass
username=alice
password=alice123
```

AOR – [alice]

```
[alice]
type=aor
max_contacts=1
```

type=aor : Déclare un "Address Of Record", qui gère l'enregistrement de l'utilisateur.
max_contacts=1 : Autorise un seul contact enregistré simultanément.

Utilisateur Bob (poste 1002)
Même structure que pour Alice, dupliquée avec ses propres identifiants.

```
; === UTILISATEUR BOB (1002) ===
[bob]
type=endpoint
transport=transport-udp
context=from-internal
disallow=all
allow=ulaw
auth=bob-auth
aors=bob
```

```
[bob-auth]
type=auth
auth_type=userpass
username=bob
password=bob123
```

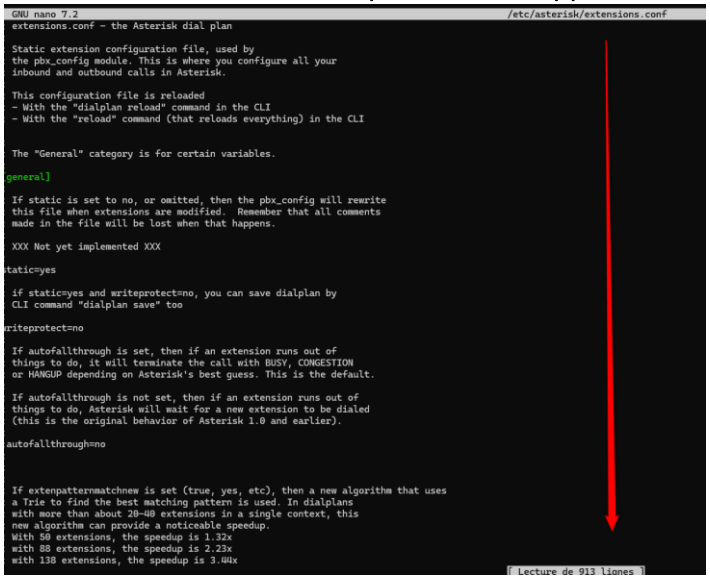
```
[bob]
type=aor
max_contacts=1
```

Les mots de passe utilisés dans cet exemple sont **simples** à des fins pédagogiques.
En production, il est impératif d'utiliser des **mots de passe complexes** pour éviter toute compromission SIP.

Éditer le fichier extensions.conf

sudo nano /etc/asterisk/extensions.conf

Ce fichier est le cœur du comportement d'appel dans Asterisk. Il permet de définir :



- les règles de traitement des appels entrants et sortants,
- les actions à exécuter selon les numéros composés,
- l'utilisation de contextes pour segmenter les droits et flux.

Descendre jusqu'en bas du fichier

Cette section est un **contexte logique du plan de numérotation** (dialplan) dans Asterisk.
Elle est utilisée pour **diriger les appels internes** des utilisateurs SIP déclarés (ex. alice et bob).

```
[from-internal]
exten => 1001,1,Dial(PJSIP/alice,20)
exten => 1002,1,Dial(PJSIP/bob,20)
```

- exten => 1001,1,Dial(PJSIP/alice,20)

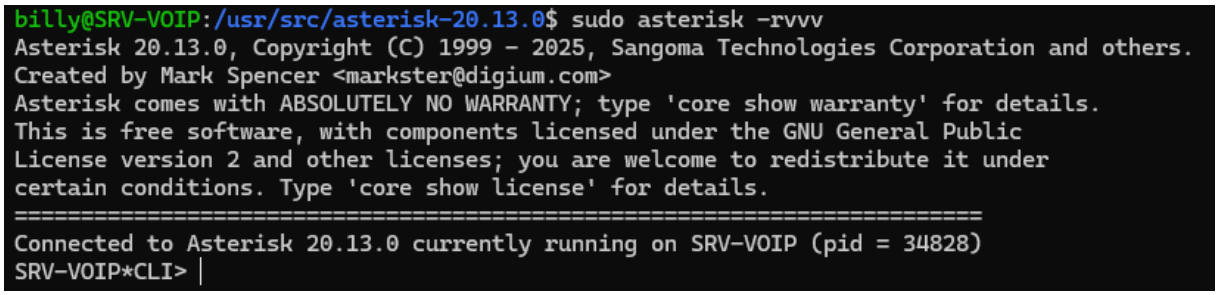
- 1001 : Numéro d'extension que l'utilisateur peut composer.
- 1 : Priorité d'exécution dans le dialplan.
- Dial(PJSIP/alice,20) :
  - Demande à Asterisk de joindre l'utilisateur alice via le canal PJSIP.
  - La sonnerie durera 20 secondes maximum avant d'échouer ou de passer à une priorité suivante (si définie).

- exten => 1002,1,Dial(PJSIP/bob,20)
- Fonctionnement identique, mais pour l'utilisateur bob.
- Lorsqu'un utilisateur compose 1001, l'appel sera redirigé vers le terminal Alice.
- Lorsqu'un utilisateur compose 1002, l'appel sera redirigé vers le terminal Bob.
- Ce contexte doit être référencé dans chaque endpoint SIP comme suit :

context=from-internal

Recharger les fichiers depuis la console CLI Asterisk

Accède à la console :
sudo asterisk -rvvv
sudo : Nécessaire pour accéder au processus Asterisk avec les privilèges adéquats.
asterisk : Lance le client d'Asterisk.
-r : Se connecte à une instance Asterisk déjà en cours d'exécution (mode *remote console*).
-vvv : Définit le niveau de verbosité à 3, permettant d'obtenir un retour détaillé sur les événements en temps réel (enregistrement, appels, erreurs, etc.).

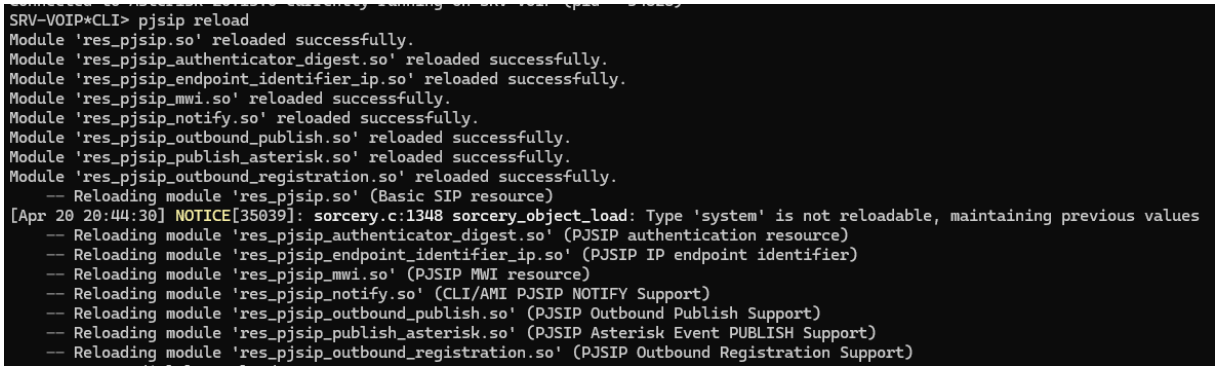


La connexion au service Asterisk a réussi.
L'instance tourne sous la version 20.13.0.
Le processus principal Asterisk a pour PID 34828.
Le prompt interactif SRV-VOIP*CLI> indique que la console CLI d'Asterisk est accessible, prête à recevoir des commandes comme :

cette commande permet de recharger dynamiquement les modules PJSIP à partir des fichiers de configuration (pjsip.conf, etc.) sans redémarrer Asterisk.
Modules rechargés avec succès :

- res_pjsip.so : composant principal du moteur SIP PJSIP.
- res_pjsip_authenticator_digest.so : gestion de l'authentification digest SIP.
- res_pjsip_endpoint_identifier_ip.so : identification des endpoints par adresse IP.
- res_pjsip_mwi.so : gestion des notifications de message en attente (MWI).

- res_pjsip_notify.so : support pour les messages NOTIFY SIP.
- res_pjsip_outbound_publish.so : publication d'événements SIP.
- res_pjsip_publish_asterisk.so : publication des événements internes Asterisk.
- res_pjsip_outbound_registration.so : enregistrement SIP vers des serveurs externes



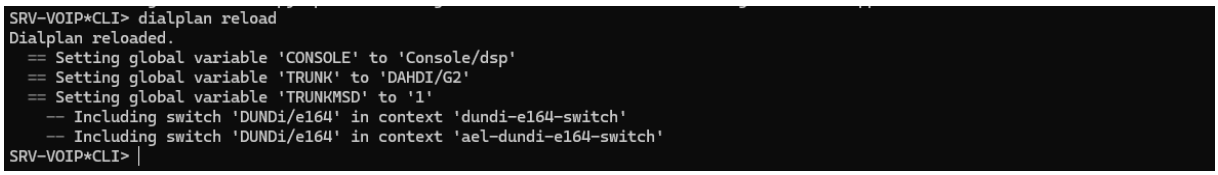
Ceci n'est pas une erreur mais une notification informative. Certains objets internes (system) ne peuvent pas être rechargés dynamiquement ; les anciennes valeurs sont donc conservées.

Commande 2 : dialplan reload

Recharge le fichier /etc/asterisk/extensions.conf et toute autre source de plan de numérotation.

Confirmation affichée :

Variables et éléments inclus :



- Variables globales définies :
  - CONSOLE → Console/dsp
  - TRUNK → DAHDI/G2
  - TRUNKMSD → 1

- Switches inclus :
    - DUNDI/e164 et ael-dundi-e164-switch :
        - Ces entrées indiquent que des composants AEL (Asterisk Extension Language) ou DUNDi (Distributed Universal Number Discovery) sont présents ou référencés.

Les commandes de rechargement ont été exécutées avec succès, ce qui confirme que :

- Les modifications des fichiers pjsip.conf et extensions.conf ont bien été prises en compte.
- Le système est prêt à traiter les appels selon la configuration en place.

Étape 1 – Télécharger Zoiper 5

1. Ouvrir un navigateur web.
2. Accéder au site officiel de Zoiper à l'adresse suivante : https://www.zoiper.com/en/voip-softphone/download/current
3. Cliquer sur "Download" sous la version correspondant à votre système d'exploitation :
    - Windows
    - macOS
    - Linux
    - Mobile (Android / iOS)

Étape 2 – Installer Zoiper

Pour Windows :

1. Exécuter le fichier téléchargé (Zoiper5_Installer.exe).
2. Accepter les conditions d'utilisation.
3. Cliquer sur "Next" jusqu'à la fin de l'installation.
4. Une fois installé, lancer Zoiper 5.

Étape 3 – Lancer Zoiper (Community Edition)

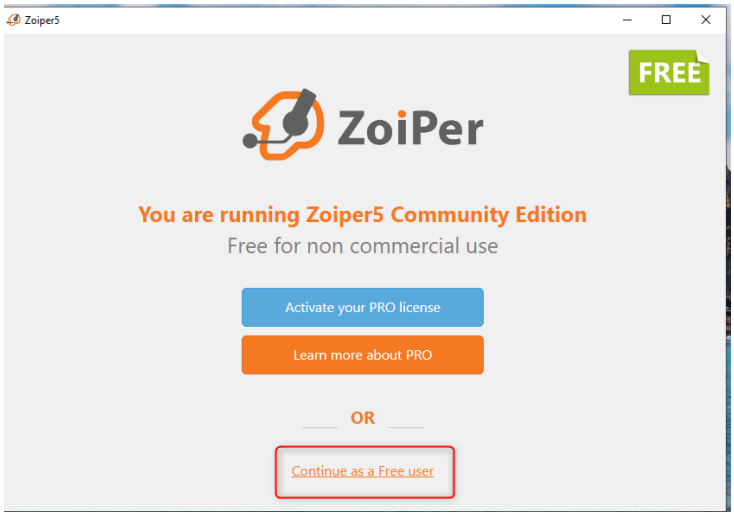
Après avoir validé les identifiants et la connexion, Zoiper vous propose de choisir entre la version gratuite (Community Edition) et la version payante (PRO).

Édition Community Edition détectée

Le message vous informe que vous utilisez Zoiper5 Community Edition, qui est gratuite pour une utilisation non commerciale. Cette version permet les appels VoIP de base avec les fonctionnalités essentielles.

Choisir l'option gratuite

Pour continuer avec la version gratuite, cliquez simplement sur le lien "Continue as a Free user".
Cette action permet d'utiliser Zoiper sans licence payante tout en conservant les fonctionnalités de base nécessaires pour s'enregistrer et passer des appels.



Cliquez sur "Continue as a Free user".

Après avoir défini l'adresse du serveur VoIP, l'utilisateur est invité à **renseigner ses identifiants de connexion SIP** afin de s'enregistrer auprès du serveur.

1️⃣Champ "Username / Login"

Il faut saisir ici **le nom d'utilisateur SIP** attribué. Ce nom est généralement fourni par l'administrateur système ou configuré sur le serveur VoIP (par exemple : 101, alice, techsupport, etc.).

Champ "Password"

Dans ce champ, saisir **le mot de passe associé** au compte SIP utilisé. Ce mot de passe est requis pour permettre l'authentification sécurisée de l'utilisateur auprès du serveur.

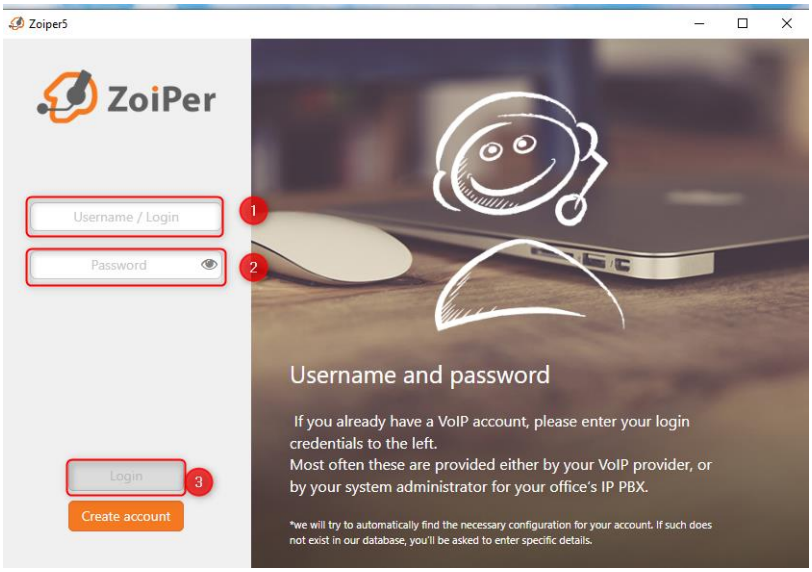
Connexion

Une fois les deux champs correctement remplis, cliquer sur **"Login"** pour tenter une connexion au serveur VoIP.

Si les identifiants sont valides, l'enregistrement SIP sera effectué et l'utilisateur pourra ensuite émettre et recevoir des appels.

En cas d'échec, vérifier l'exactitude des informations saisies ainsi que la configuration du compte côté serveur.

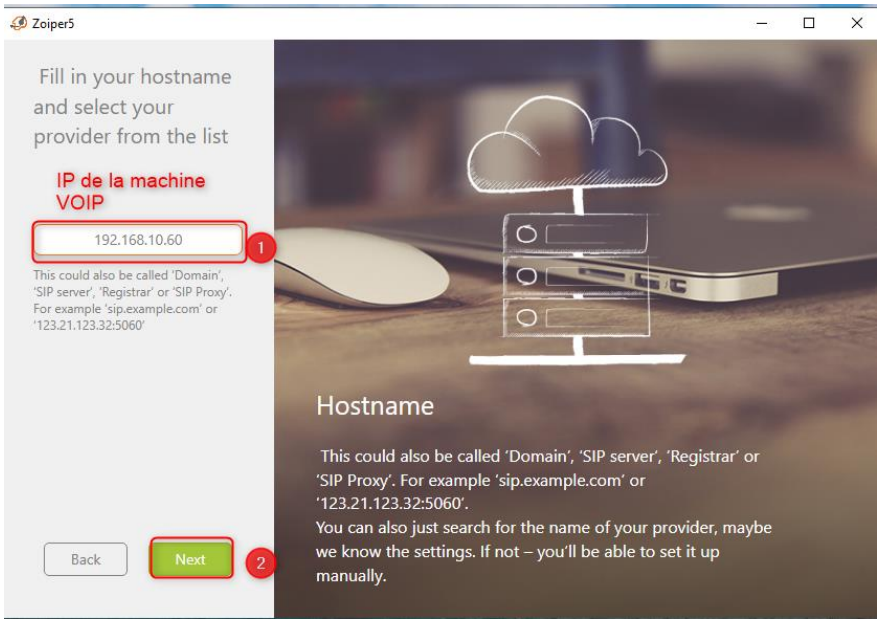
(1) **Username** : alice
(2) **Password** : alice123
(3) Cliquer sur Login



Lors de cette étape, il est nécessaire de spécifier l'adresse du serveur SIP auquel le client Zoiper devra se connecter pour établir la communication VoIP.

Champ Hostname

Dans le champ "Hostname", il convient de renseigner **l'adresse IP de la machine hébergeant le serveur VoIP** (généralement Asterisk, FreePBX ou équivalent).



Dans cet exemple, l'adresse renseignée est : 192.168.10.60
Cette adresse correspond à la **machine serveur VoIP située sur le réseau local**. Elle peut aussi être un nom de domaine si le serveur est accessible via Internet (ex. voip.entreprise.fr).

✅ **Valider avec "Next"**

Après avoir saisi correctement l'adresse IP ou le nom de domaine, cliquer sur le bouton **Next** pour valider cette configuration et passer à l'étape suivante de l'assistant.
Remarque : Veillez à ce que le poste client ait un accès réseau direct à cette adresse IP, et que les ports SIP (ex : 5060 pour UDP) soient ouverts sur le serveur.

À ce stade, Zoiper propose de configurer des paramètres supplémentaires liés à l'authentification avancée et à l'utilisation d'un **proxy SIP sortant**.

Authentication username

Ce champ permet de spécifier un nom d'utilisateur différent pour l'authentification, dans le cas où celui-ci ne correspond pas exactement au nom de compte SIP utilisé pour l'enregistrement.
Exemple d'usage : lorsque le login est différent de l'extension SIP (cas rare dans un environnement standard).

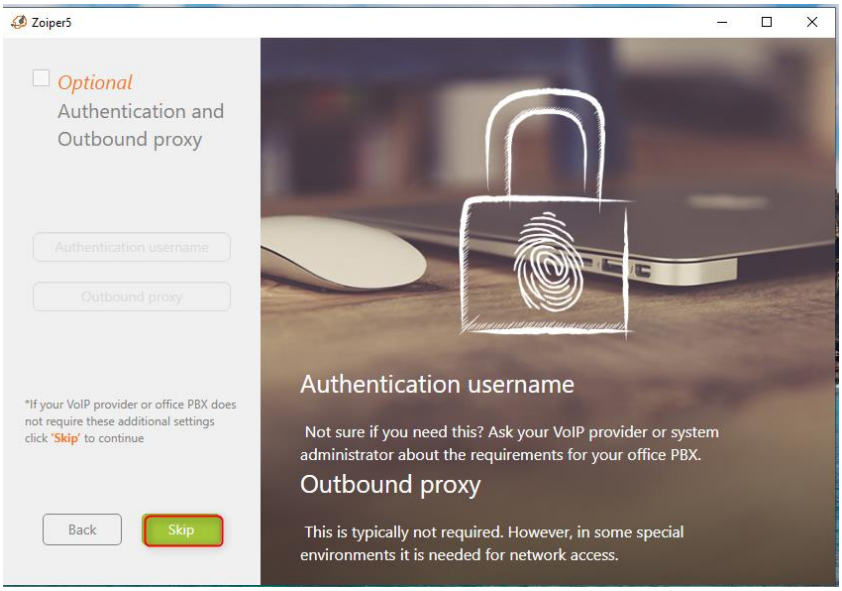
Outbound proxy

Ce champ est destiné aux infrastructures où un **proxy SIP** est nécessaire pour le routage des paquets VoIP, notamment dans des environnements réseau complexes ou avec inspection approfondie (firewall/proxy d'entreprise).

Choix recommandé :

Dans le cadre d'un déploiement simple ou classique (comme avec un serveur Asterisk local ou distant sans proxy spécifique), **aucun paramètre supplémentaire n'est requis** à cette étape.

Il convient donc de cliquer sur **Skip** (bouton en bas à gauche) pour ignorer cette configuration et passer à l'étape suivante.



À cette étape de la configuration, **Zoiper5** teste automatiquement les types de transport disponibles pour établir une connexion avec le serveur SIP. Il s'agit d'une phase essentielle permettant de garantir la compatibilité entre le client (Zoiper) et le serveur VoIP (ex. : Asterisk, FreePBX, etc.).

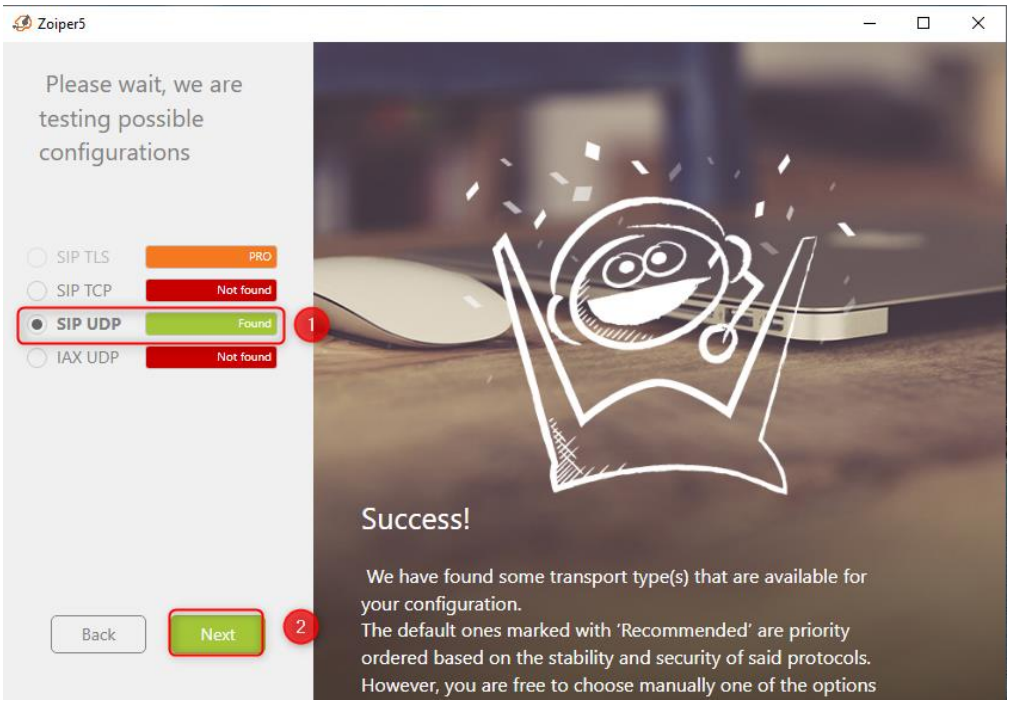
Résultat du test :

- **SIP UDP : Found**
  → Le protocole SIP en UDP a été détecté avec succès. C'est le mode de transport le plus couramment utilisé dans les environnements VoIP classiques car il est léger et efficace pour les communications en temps réel.
- **SIP TCP : Not found**
  → Le protocole SIP en TCP n'a pas été détecté. Cela signifie que le serveur ne prend pas en charge ce mode, ou que le port correspondant n'est pas accessible.
- **SIP TLS : PRO (non disponible dans la version gratuite)**
  → Le protocole chiffré SIP TLS est réservé à la version professionnelle de Zoiper.
- **IAX UDP : Not found**
  → Le protocole IAX n'a pas été détecté. Il est moins utilisé mais parfois préféré pour les communications inter-Asterisk.

Action recommandée :

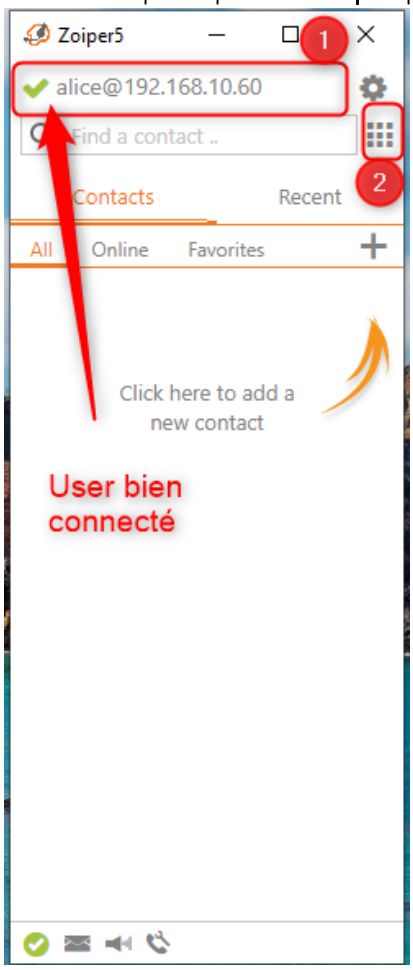
Sélectionner **SIP UDP** (qui est déjà mis en surbrillance en vert) et cliquer sur **Next** pour poursuivre la configuration.

C'est le protocole recommandé dans la majorité des cas, sauf environnement spécifique avec exigences de sécurité élevées (où SIP TLS serait utilisé).



Vérification de la connexion sur Zoiper

Une fois les étapes précédentes finalisées, l'interface principale de **Zoiper** permet de valider que l'utilisateur est bien enregistré sur le serveur VoIP.



1 Confirmation de l'enregistrement

- En haut à gauche, la mention **alice@192.168.10.60** indique que l'utilisateur **Alice** est connecté avec succès au serveur SIP situé à l'adresse IP **192.168.10.60**.

- La présence de la **coche verte** confirme l'état « **connecté** » (enregistré avec succès auprès du serveur IPBX/Asterisk).

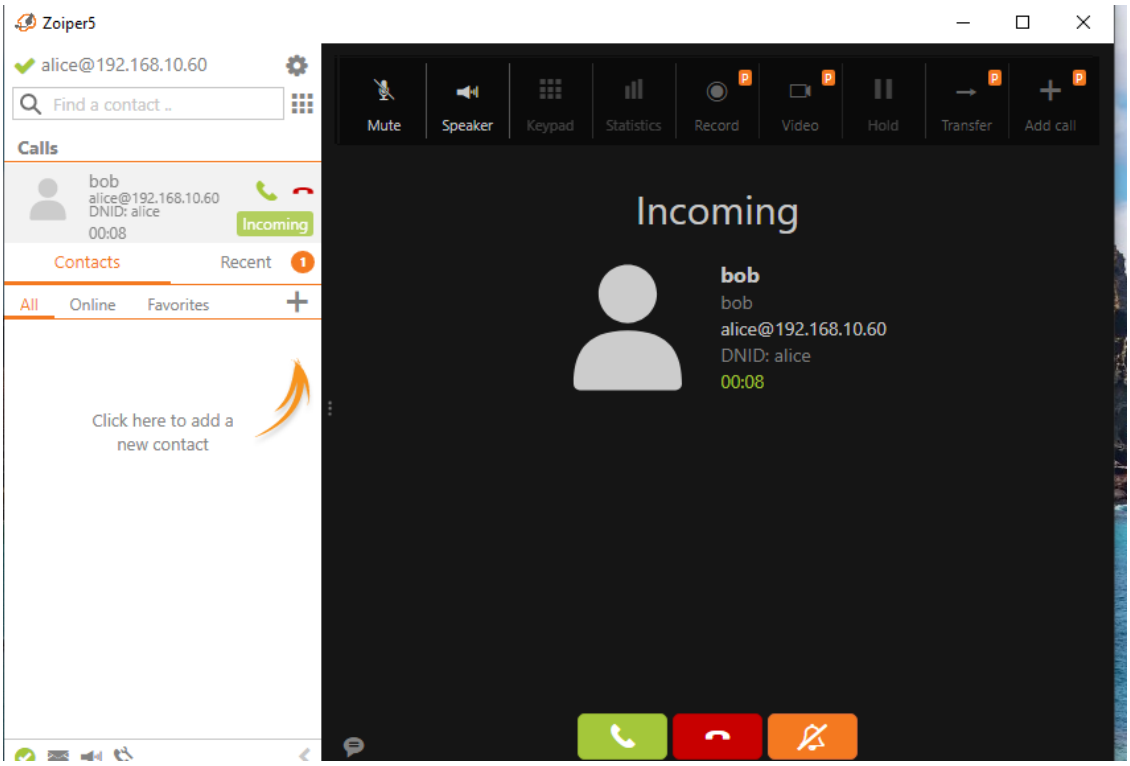
2Accès à l'interface d'appel

- Le bouton représentant un **clavier téléphonique** permet d'ouvrir le **pavé numérique** afin de composer un numéro ou un identifiant SIP pour passer un appel.

🔎 À ce stade, l'utilisateur est prêt à **émettre** ou **recevoir** des appels via le système VoIP.

Étapes de configuration et de test

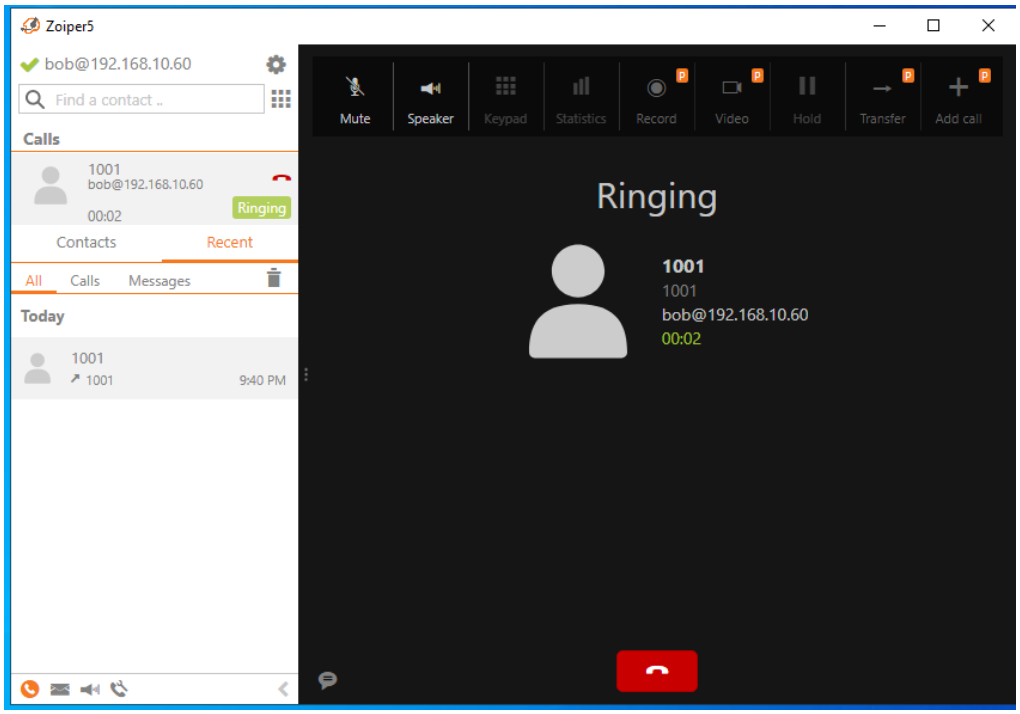
1. Connexion des deux utilisateurs :
    - Les deux utilisateurs ont été connectés à l'aide de leur identifiant SIP fourni par le serveur IPBX.
    - La capture montre que l'utilisateur **alice** est bien authentifié sur le serveur VOIP à l'adresse IP **192.168.10.60**, ce qui est confirmé par la coche verte à côté de son identifiant : alice@192.168.10.60.



2. Composition du numéro :
    - Dans l'interface de Zoiper, l'utilisateur a accédé au pavé numérique via l'icône du clavier (visible dans la barre supérieure).
    - Le numéro ou l'identifiant SIP de l'utilisateur à contacter (**bob**) a été saisi, puis l'appel a été initié en cliquant sur **Dial** (composer).
3. Établissement de l'appel :

- Une fois l'appel lancé, la fenêtre d'appel s'affiche avec les informations de contact de **bob**, telles que son identifiant SIP, l'état de la connexion (barres de signal), et la durée de l'appel.
- L'appel est actif comme l'indique le compteur de durée (ici 00:02 secondes).

4. **Réception de l'appel par le correspondant :**



- L'utilisateur **bob** reçoit un appel entrant provenant de **alice**.
- Zoiper affiche la fenêtre de notification de l'appel entrant avec trois options :
  - ✅ **Accepter**
  - ❌ **Refuser**
  - 🔁 **Transférer**

5. **Communication active :**
   - Une fois l'appel accepté, les deux utilisateurs sont en communication bidirectionnelle.
   - Les boutons de gestion d'appel (mute, haut-parleur, statistiques, transfert, etc.) deviennent accessibles pour ajuster la session selon les besoins.

✅ Résultat du test

Le test est concluant. La communication entre les deux utilisateurs **alice** et **bob** a bien été établie via le protocole **SIP UDP**, qui a été validé lors de la phase de détection des services VoIP disponibles.
Cela confirme que :

- Le serveur IPBX est opérationnel,

- Les comptes SIP sont fonctionnels et correctement configurés,
- Les flux réseau ne sont pas bloqués par un pare-feu,
- L'environnement réseau autorise bien le transport UDP sur les ports SIP.

Annexe – Définitions des termes techniques

1. VM (Virtual Machine)
Machine virtuelle qui simule un ordinateur physique dans un environnement logiciel, permettant de tester ou déployer des systèmes indépendamment du matériel réel.

VMware
Logiciel de virtualisation qui permet de créer et gérer des machines virtuelles.

Bridge (mode réseau)
Mode de connexion réseau dans VMware où la machine virtuelle est connectée comme un poste du réseau local.

Debian
Distribution GNU/Linux stable et utilisée en environnement serveur, ici version 12 (Bookworm).

SRV-VOIP
Nom d'hôte attribué au serveur dédié à la téléphonie VoIP avec Asterisk.

Adresse IP
Identifiant unique d'un appareil sur un réseau (exemple : 192.168.10.60).

Masque de sous-réseau
Paramètre qui détermine la taille d'un réseau local (ex : 255.255.255.0 = /24).

Passerelle (Gateway)
Routeur qui permet à une machine de communiquer avec des réseaux extérieurs, comme Internet.

DNS (Domain Name System)
Système de résolution de noms permettant de traduire un nom (ex. google.com) en adresse IP.

APT
Gestionnaire de paquets utilisé dans Debian pour installer, mettre à jour ou supprimer des logiciels.

Sudo
Commande permettant d'exécuter une action en tant qu'administrateur (root).

Root
Compte administrateur principal sous Linux, ayant tous les droits.

Utilisateur standard
Compte utilisateur limité, utilisé pour les tâches courantes, sans accès complet au système.

Partition
Partie d'un disque dur utilisée pour organiser les données (ex : partition système, swap...).

Swap
Zone du disque utilisée comme mémoire virtuelle quand la RAM est saturée.

GRUB
Chargeur de démarrage qui permet de lancer le système d'exploitation installé.

Terminal (console TTY)
Interface en ligne de commande permettant d'interagir avec le système via du texte.

Make / Makefile
Outil et fichier permettant d'automatiser la compilation d'un logiciel.

wget / curl
Commandes permettant de télécharger des fichiers depuis Internet via ligne de commande.
build-essential
Paquet contenant les outils de base pour compiler des logiciels (gcc, make, etc.).
lib…-dev
Bibliothèques de développement nécessaires à la compilation de logiciels (ex. : libxml2-dev).
pkg-config
Outil pour obtenir des informations de compilation sur les bibliothèques installées.
tar.gz
Archive compressée contenant souvent des fichiers sources à extraire avant compilation.

Asterisk & VoIP
Asterisk
Logiciel libre de téléphonie IP (PBX), permettant de gérer appels, messagerie vocale, conférences, etc.
VoIP (Voice over IP)
Technologie permettant de passer des appels téléphoniques via Internet ou réseau IP.
IPBX
Standard téléphonique IP, souvent basé sur Asterisk, qui gère les appels internes et externes.
SIP (Session Initiation Protocol)
Protocole réseau utilisé pour établir, modifier et terminer des appels VoIP.
PJSIP
Nouvelle implémentation du protocole SIP intégrée dans Asterisk, plus performante et modulaire.
pjsip.conf
Fichier de configuration d'Asterisk pour les utilisateurs SIP avec PJSIP.
extensions.conf
Fichier de configuration du plan de numérotation (dialplan) d'Asterisk.
Endpoint
Équipement ou logiciel (comme Zoiper) qui se connecte à Asterisk pour passer/recevoir des appels.
AOR (Address of Record)
Point de contact SIP permettant de localiser un utilisateur dans un réseau VoIP.
Auth
Section du fichier PJSIP définissant le mode d'authentification d'un utilisateur SIP.
Context
Groupe logique de règles dans le dialplan, associé à un ou plusieurs endpoints.
Dialplan
Ensemble de règles définissant comment les appels sont traités et routés dans Asterisk.

Zoiper
Client SIP (softphone) permettant de passer des appels via un ordinateur ou smartphone.

Softphone
Logiciel qui simule un téléphone, utilisé pour la téléphonie sur IP.

SIP UDP / TCP / TLS
Méthodes de transport du protocole SIP :

- UDP : rapide, non sécurisé (le plus courant),
- TCP : plus fiable mais moins courant,
- TLS : sécurisé (crypté), réservé aux versions pro de Zoiper.

Outbound Proxy
Serveur intermédiaire qui achemine les messages SIP, utilisé dans des réseaux complexes.

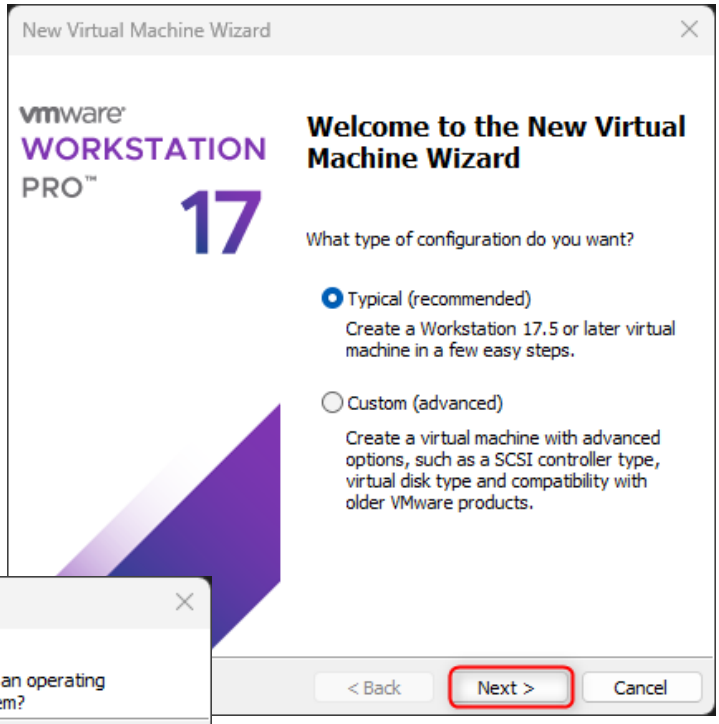
Authentication Username
Identifiant utilisé pour s'enregistrer auprès du serveur SIP.

Création, d'une VM sur VM WARE

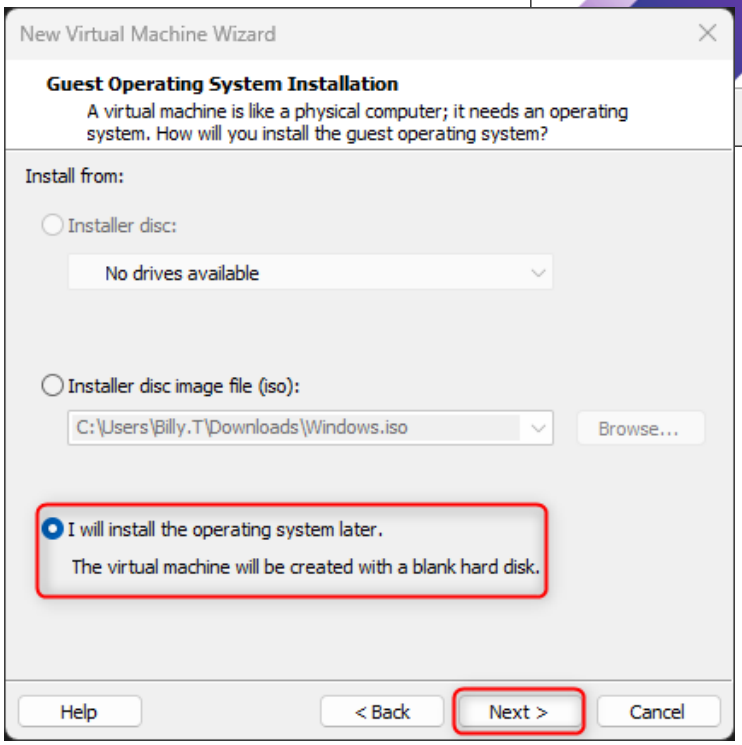
Lorsque vous créer une machine virtuelle l'option « Typical (recommended) est cocher de base.

Cliquer sur « Next » pour passer à la prochaine étape.

Cliquer sur « Next »



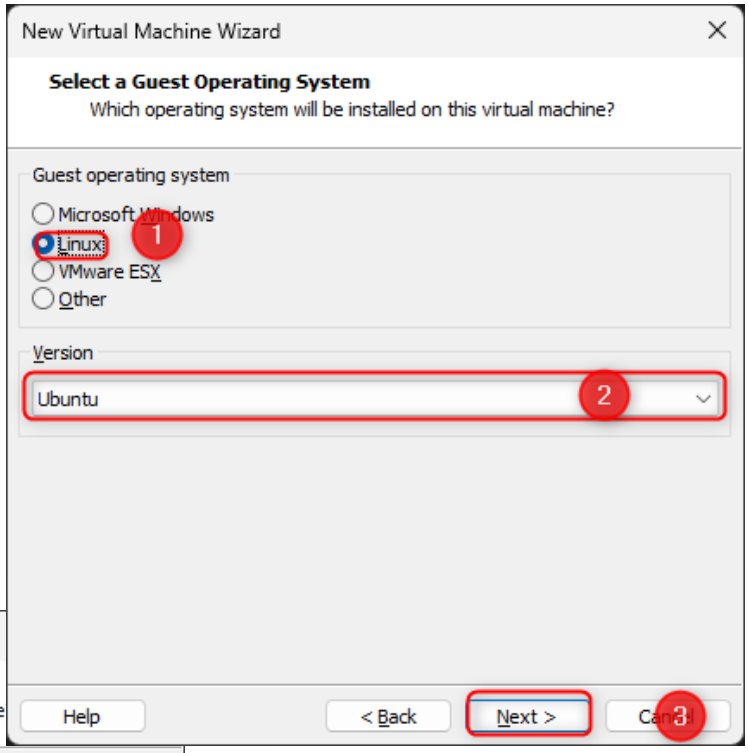
Cliquer sur « Next » pour passer à la prochaine étape



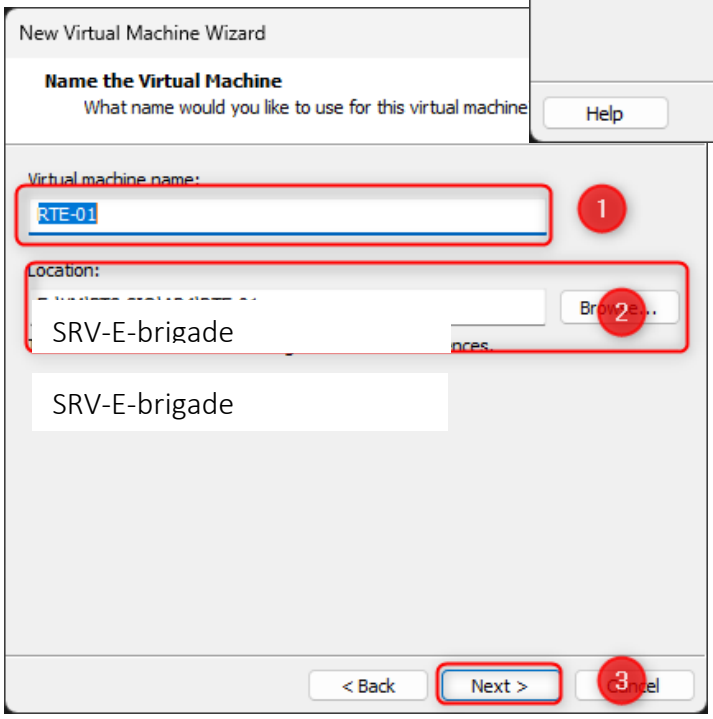
Dans notre cas à nous allons choisir « Linux » car nous auront besoin d'installer d'un pare-feu sur le serveur

Cliquer dans le menu déroulant puis sélectionner « Linux»

Cliquer sur « Next » pour passer à la prochaine étape



Dans cette étape nous allons devoir nommer le serveur ainsi que choisir l'emplacement de la VM



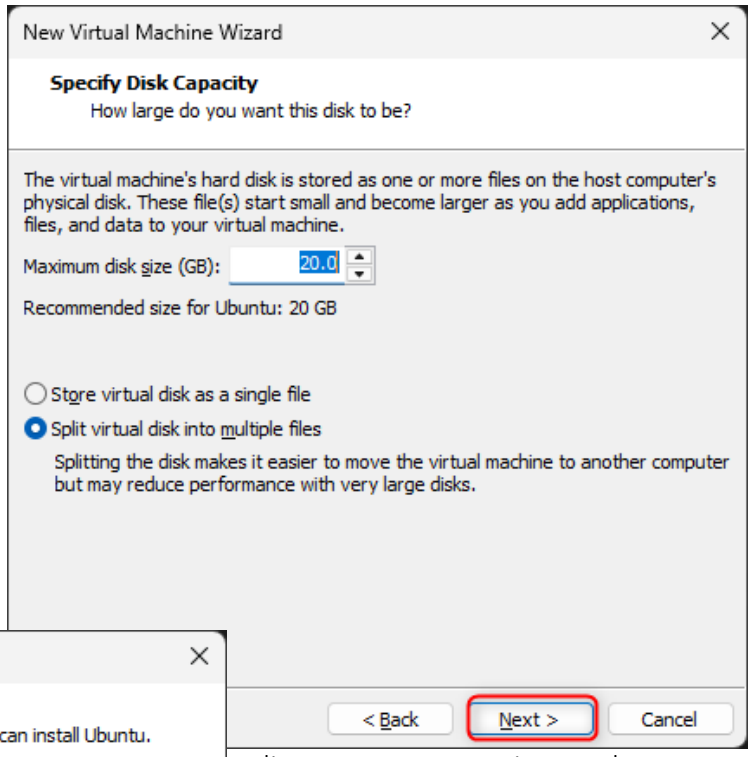
(1) Ensuite nous allons nommer le server

(2) Choisir l'emplacement ou sera situé la VM

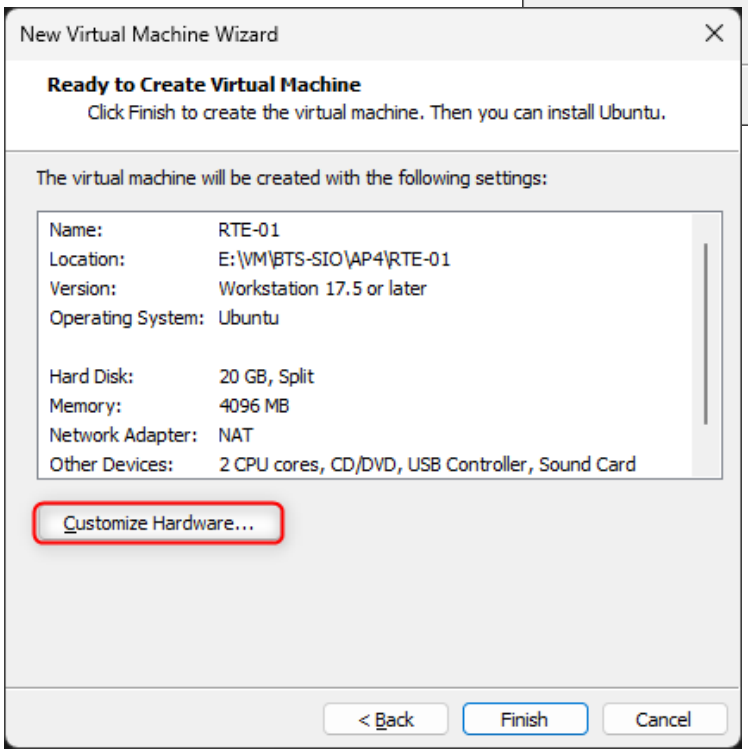
(3) Cliquer sur « Next » pour passer à la prochaine étape

Ensuite sur cette étape nous allons allouer l'espace du disque pour notre serveur. Dans notre cas il n'est pas nécessaire d'avoir un gros espace de stockage sur notre serveur.

Cliquer sur « Next » pour passer à la prochaine étape



Ensuite dans cette partie-là nous allons configurer les options suivantes :

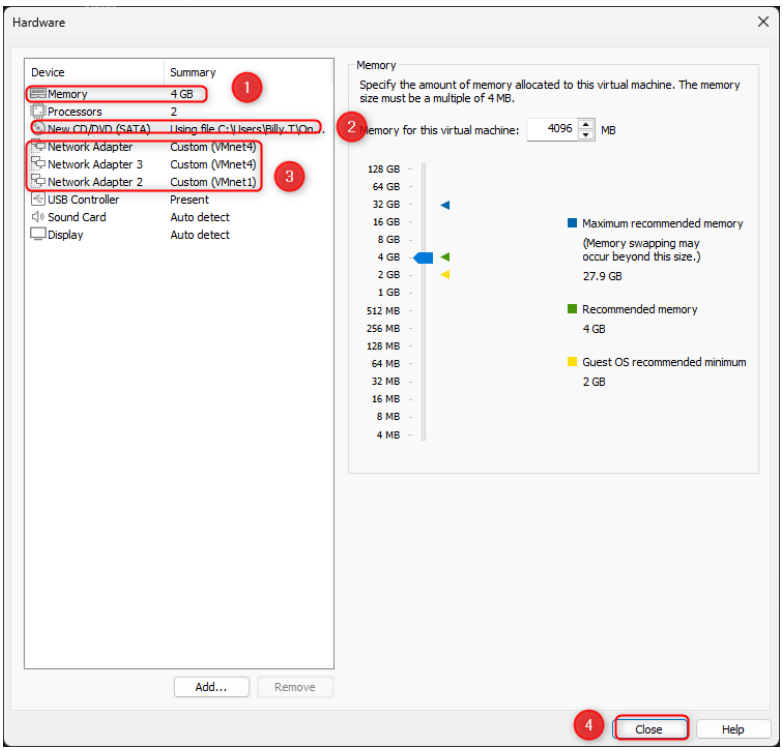


Cliquer sur « Customize Hardware »

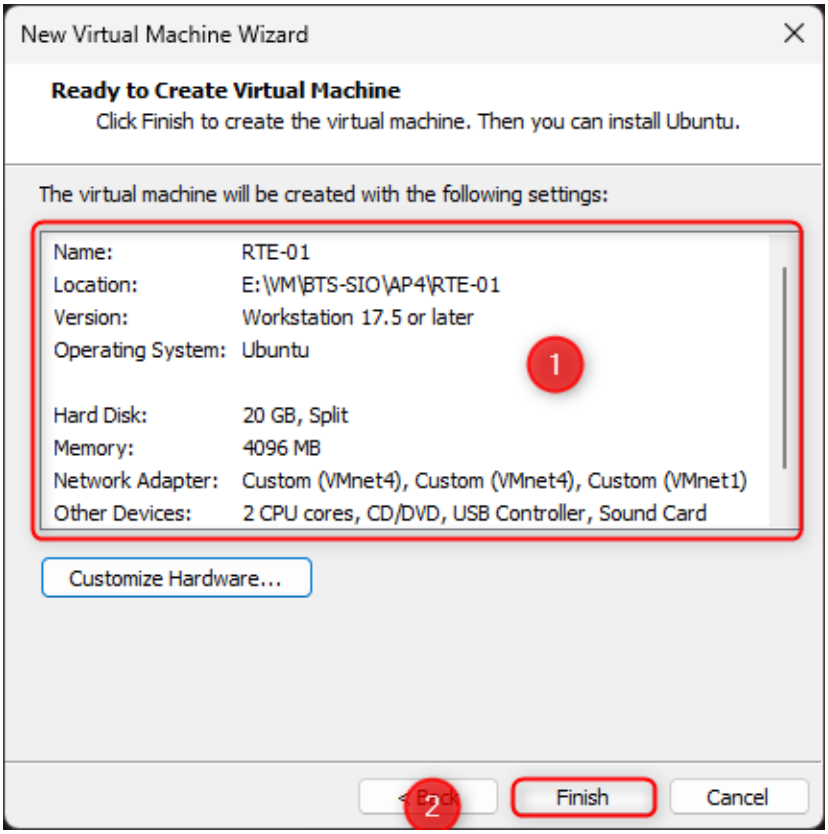
Dans cette partis nous allons paramétrer selon nos besoins :

(9) Memory = 4 GB
(10)CD/ DVD = Pfsens
(11)Network Adapter = Vmnet 4 (bridge)
Network Adapter = Vmnet 4 (bridge)

Network adapter = Vmnet 1
(12)Cliquer sur « Close » pour fermer la fenêtre

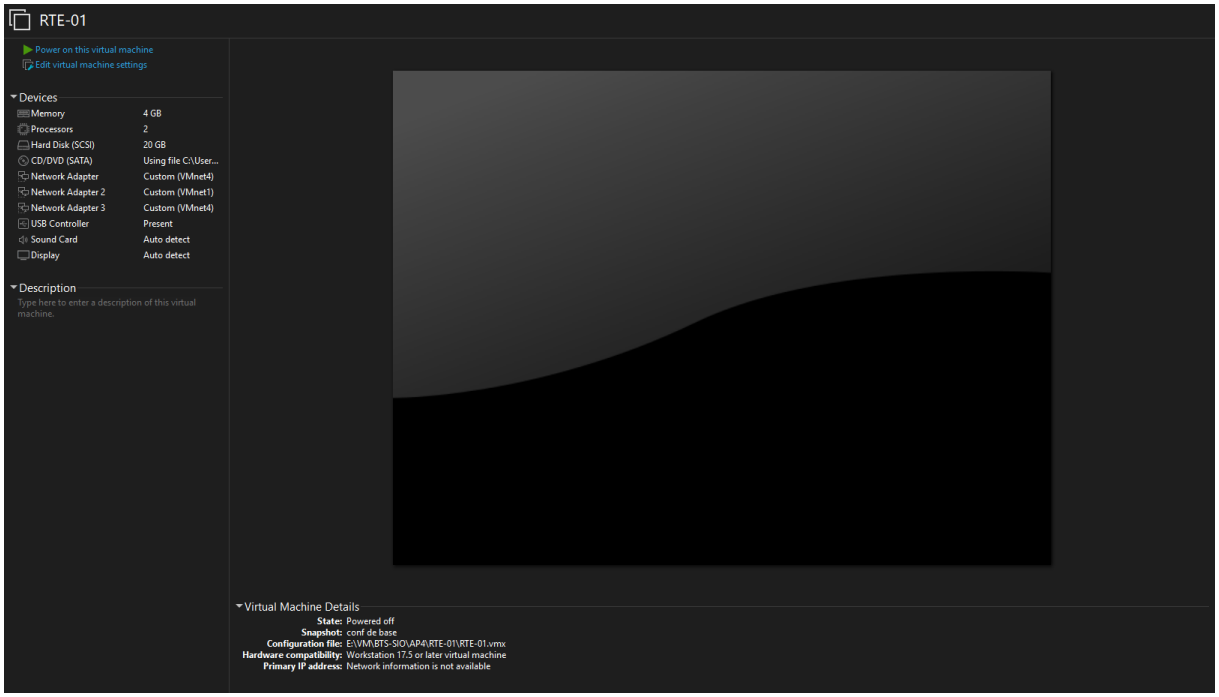


Une fois que la configuration est finit vous aller avoir ce menu-là :



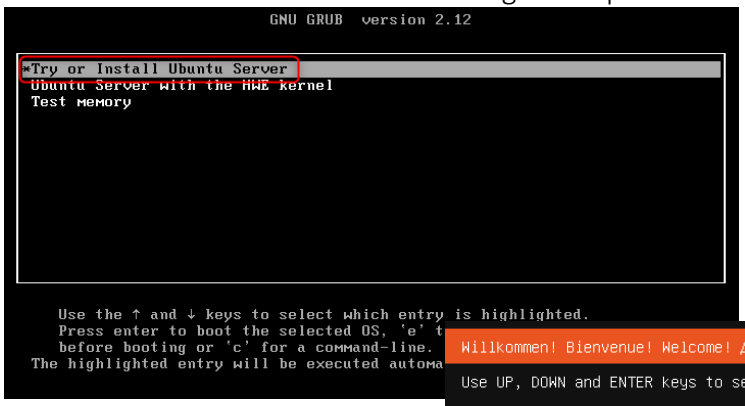
(5) Récapitulatif de la configuration du serveur.
(6) Cliquer sur « Finish » pour passer à la prochaine étape

Une fois avoir fini de vérifier les information du serveur, la VM (Virtual Machine) va se créer ainsi vous pouvez le lancer.


RTE-01
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 4 GB
Processors 2
Hard Disk (SCSI) 20 GB
CD/DVD (SATA) Using file C:\User...
Network Adapter Custom (VMnet4)
Network Adapter 2 Custom (VMnet1)
Network Adapter 3 Custom (VMnet4)
USB Controller Present
Sound Card Auto detect
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Snapshot: conf de base
Configuration file: E:\VM\BTS-SIO\AP4\RTE-01\RTE-01.vmx
Hardware compatibility: Workstation 17.5 or later virtual machine
Primary IP address: Network information is not available

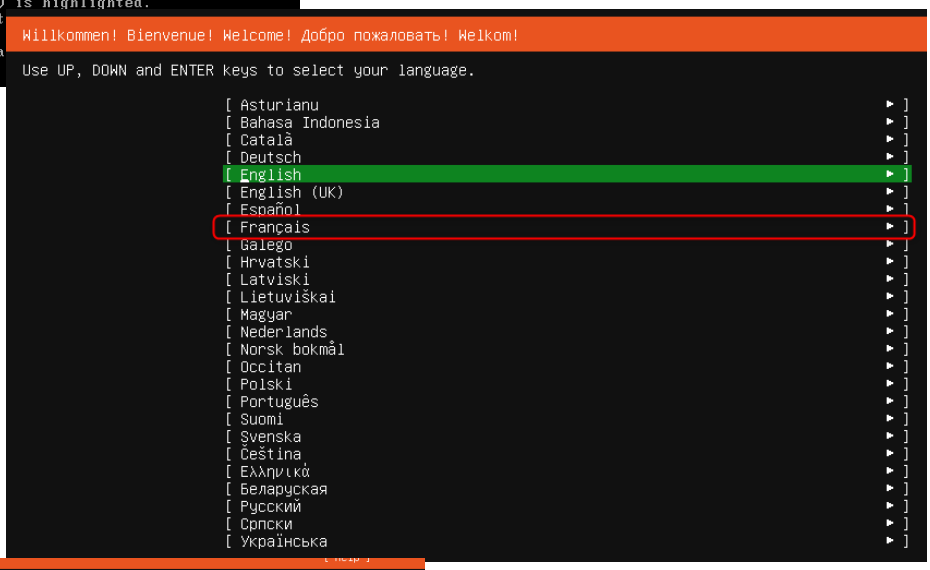
Installation Ubuntu Server 22.04

Lors du démarrer vous aurez un message avec plusieurs choix possible :

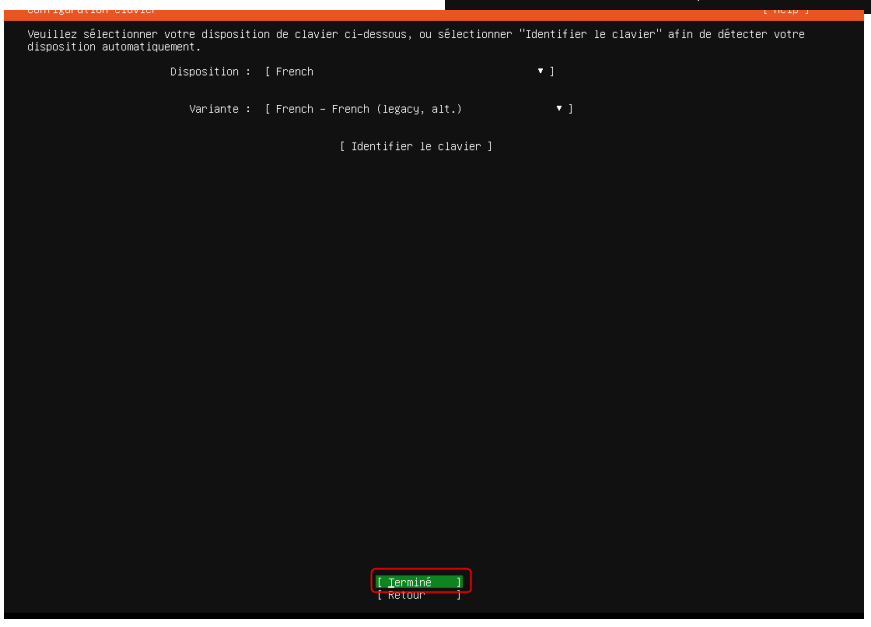


Sélectionner « Try or Install Ubuntu Server »

Car dans notre cas nous auront besoin d'installer le serveur

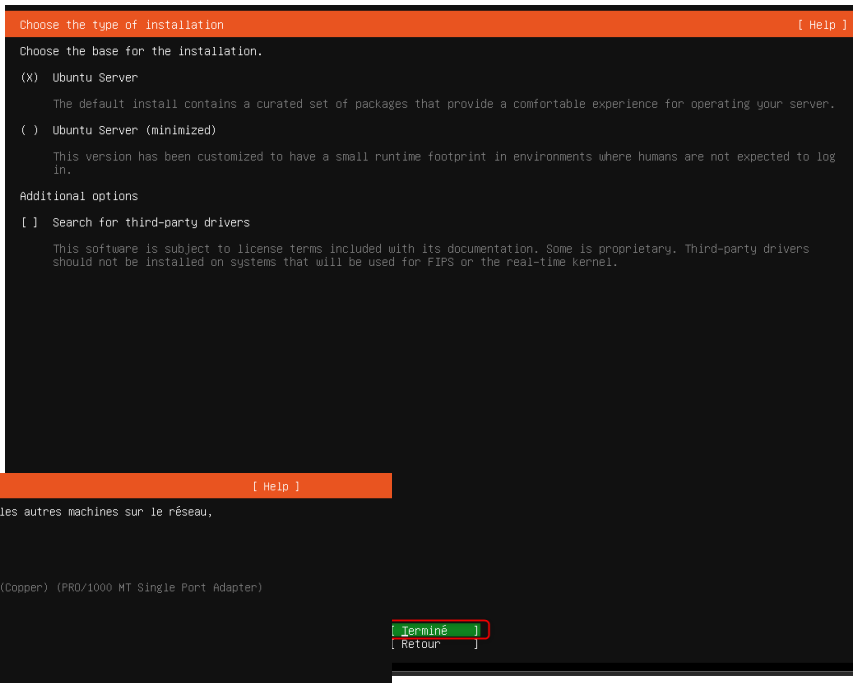


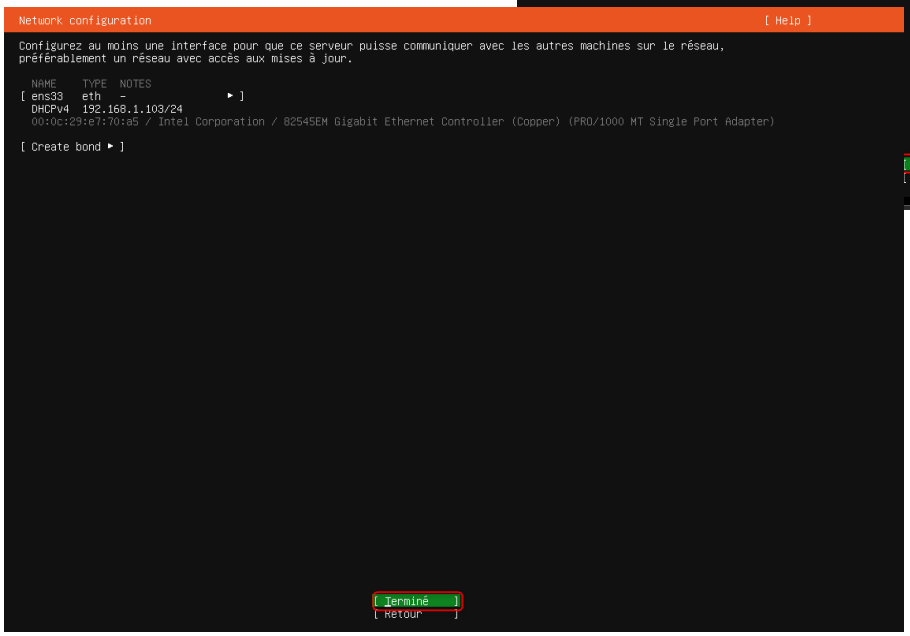
Choisir la langue française



Sélectionner Terminé

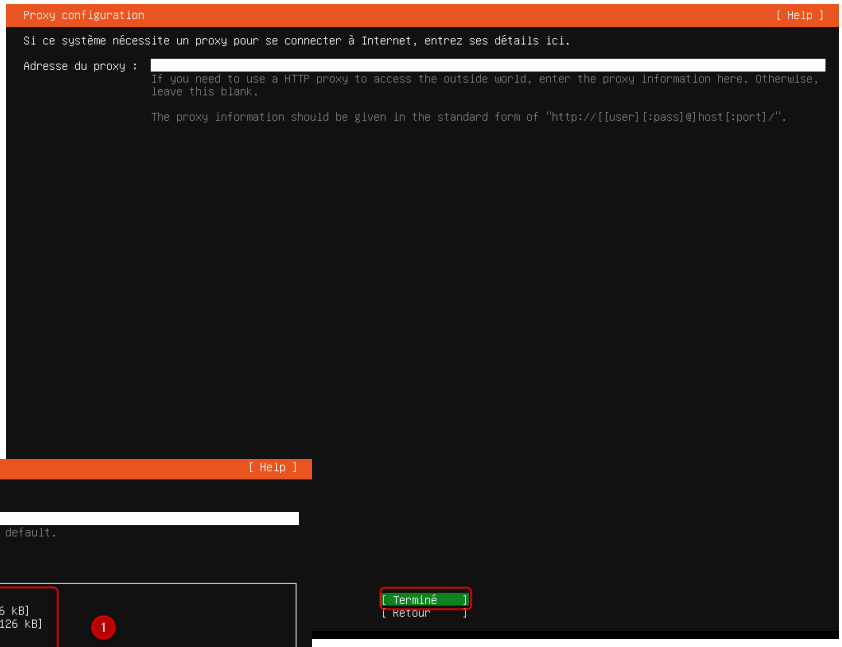
Sélectionné Terminé

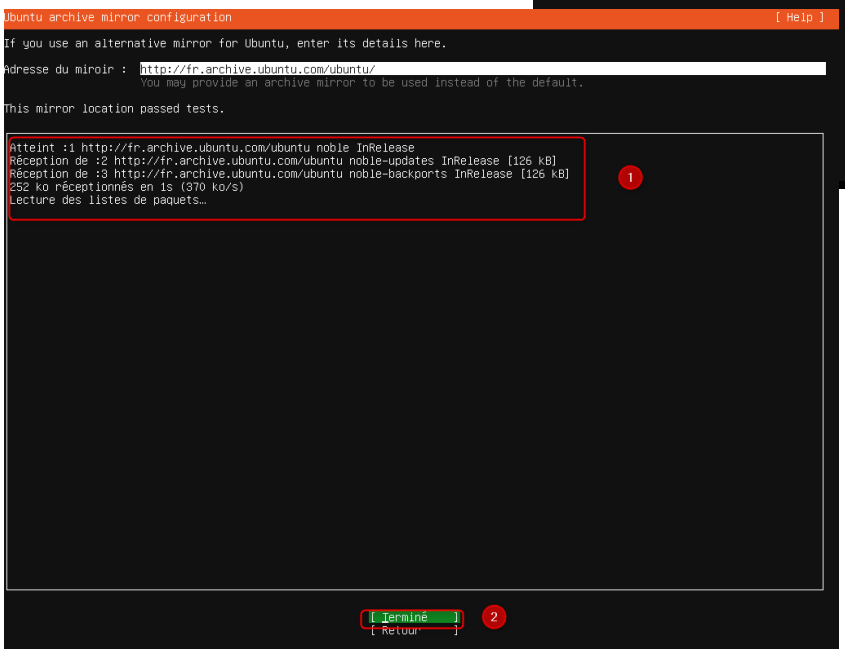




Sélectionner Terminé

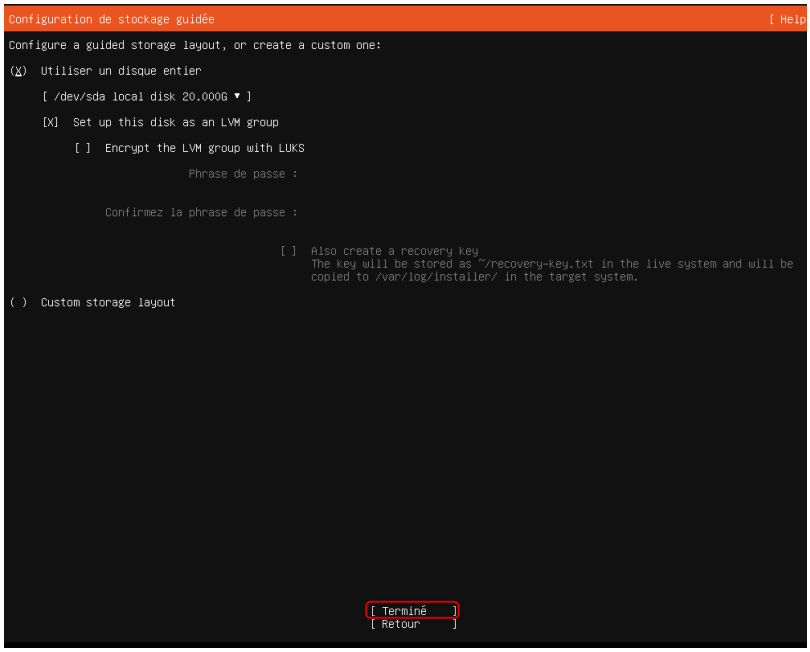
Sélectionner Terminer

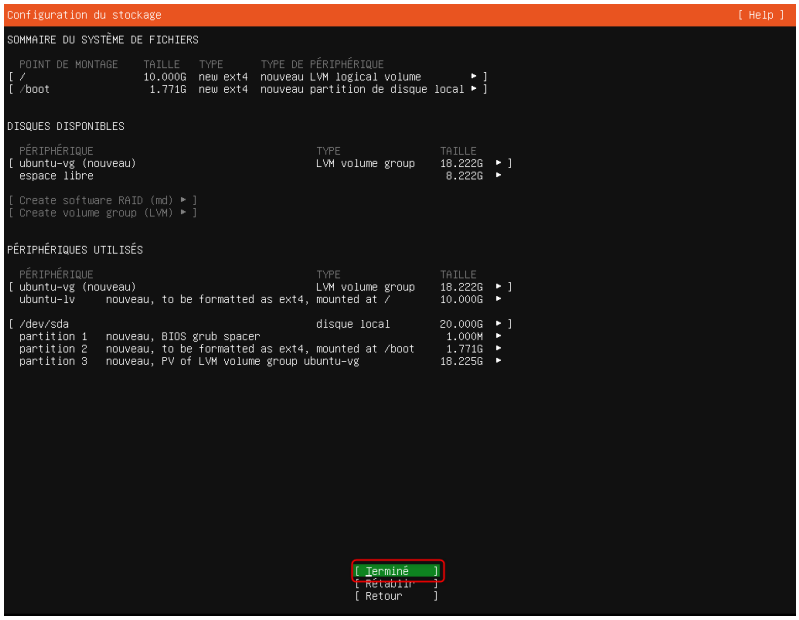




(1) Attendre que les tests aient fini
(2) Sélectionner Terminé

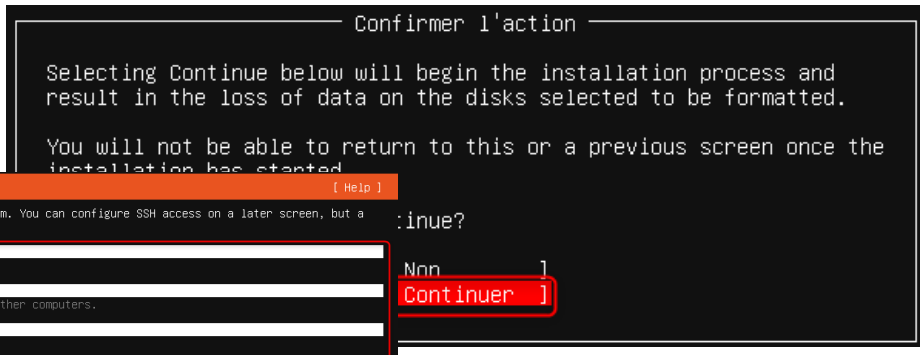
Sélectionner Terminer

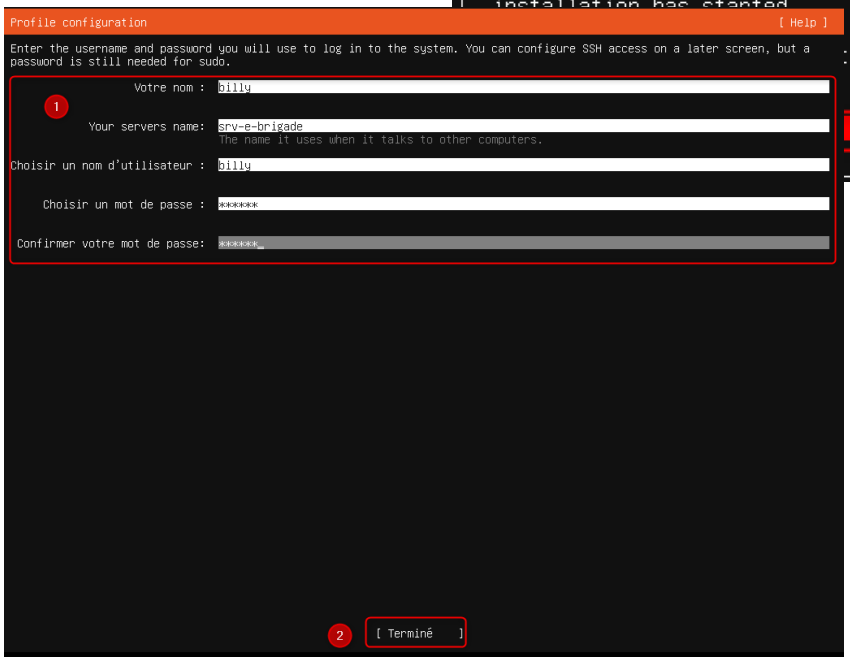




Sélectionner Terminé

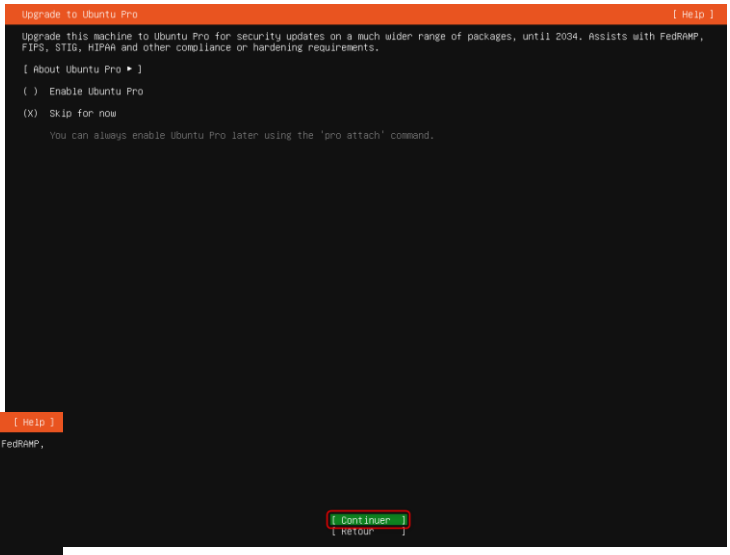
Sélectionner Continuer

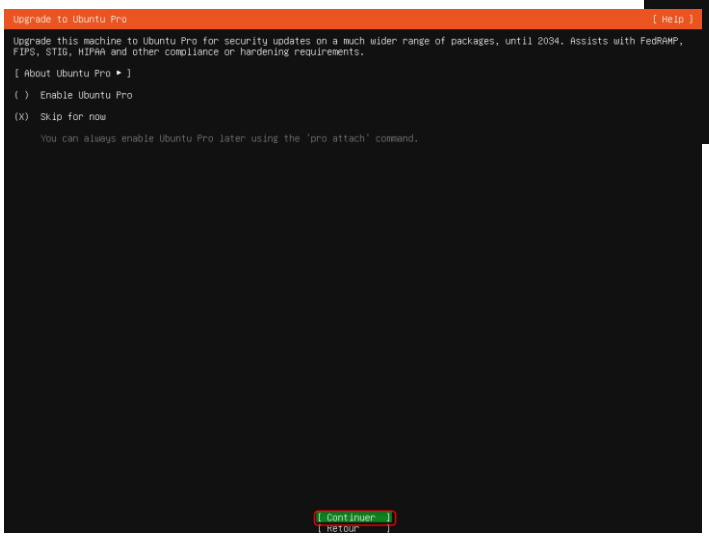




(1) Rentrer les informations demandées
(2) Sélectionner Terminé

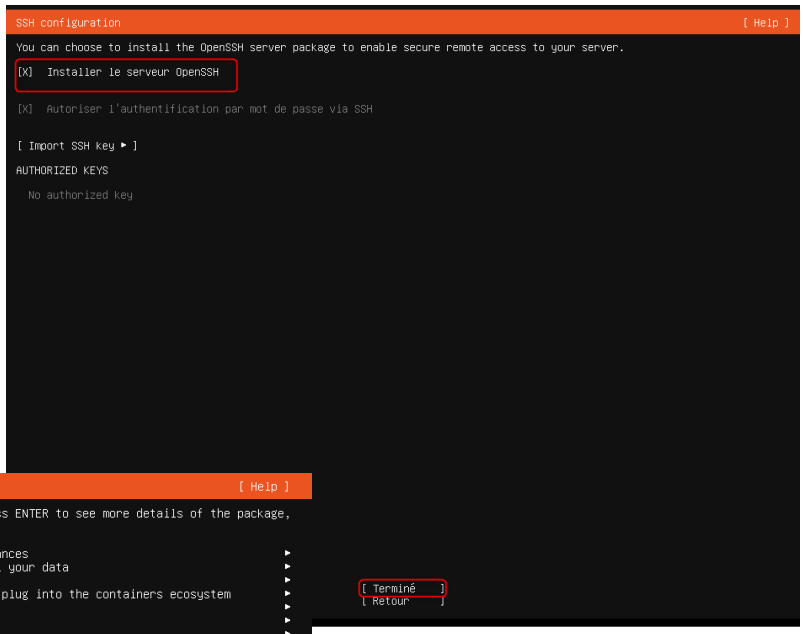
Sélectionner Continuer

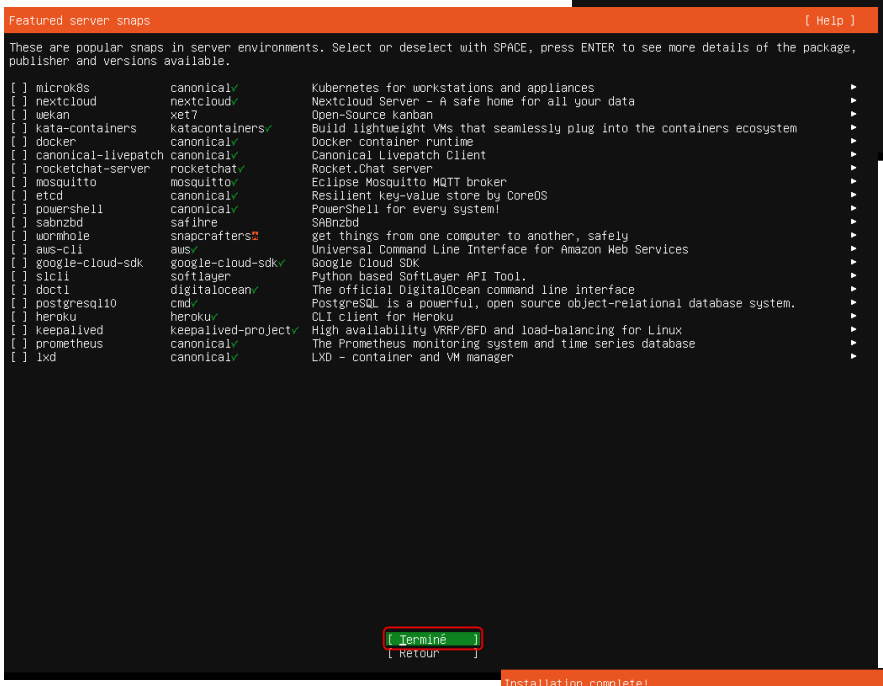




Sélectionner Continuer

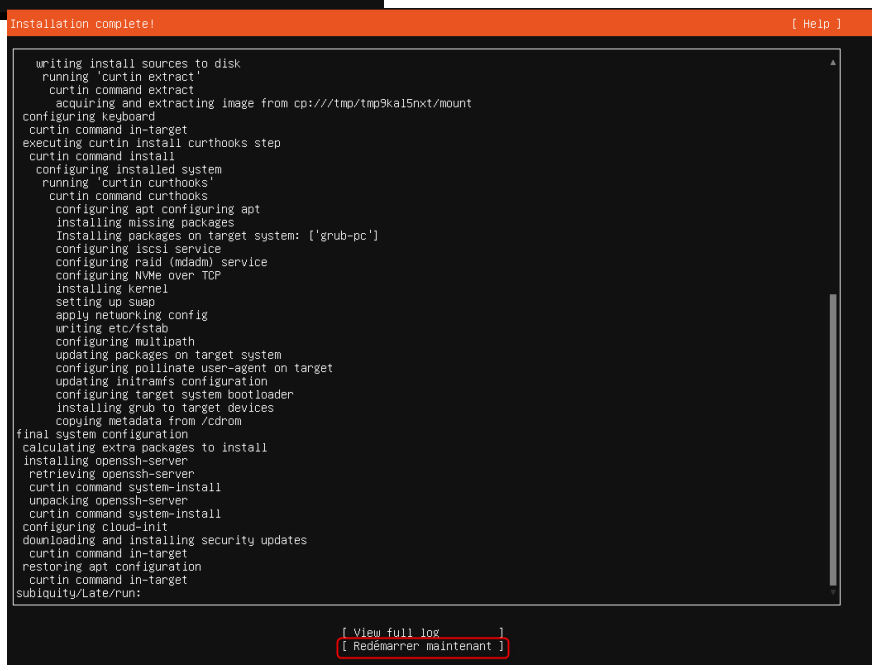
Cocher la case Installer le serveur OpenSSH
Sélectionner Terminé



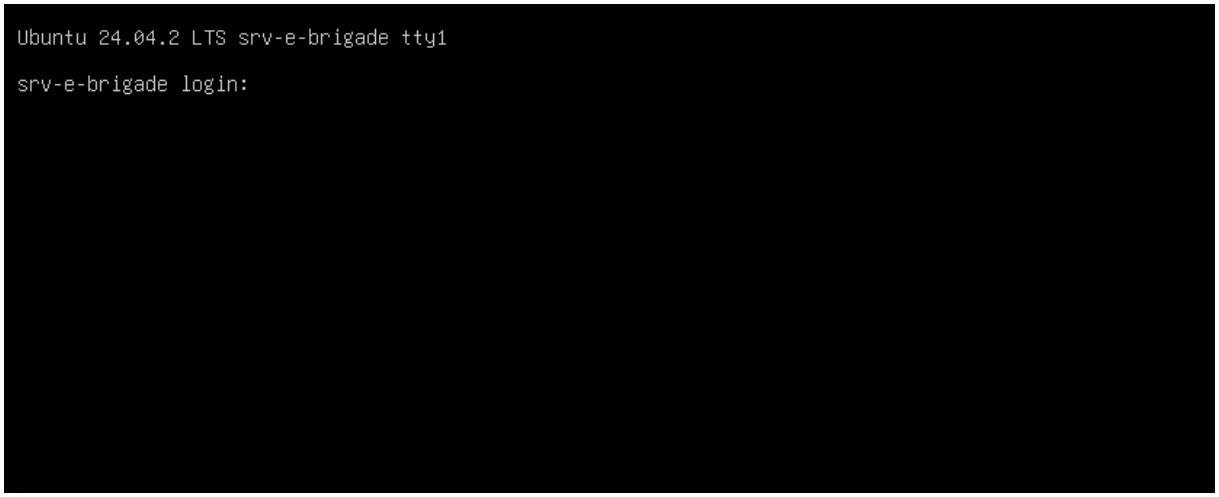


Sélectionner Terminé

Sélectionner Redémarrer maintenant



Une fois que le serveur à redémarre vous allez avoir une page de connexion


Ubuntu 24.04.2 LTS srv-e-brigade tty1
srv-e-brigade login:

Fixer une IP sur Ubuntu

Donc lorsque la machine vient de booter sur l'os Ubuntu nous allons fixer l'IP via cette commande :

sudo nano /etc/netplan/00-installer-config.yaml

```
  GNU nano 7.2
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.20.11/24
      routes:
        - to: default
          via: 192.168.20.254
      nameservers:
       addresses:
         - 8.8.8.8
         - 1.1.1.1
```

Une fois après avoir quitter le fichier de conf taper les commande suivantes

sudo netplan apply

sudo chmod 600 /etc/netplan/00-installer-config.yaml

(1) Problème de droit donc taper la commande avec sudo chmod

(2) Puis appliquer la configuration

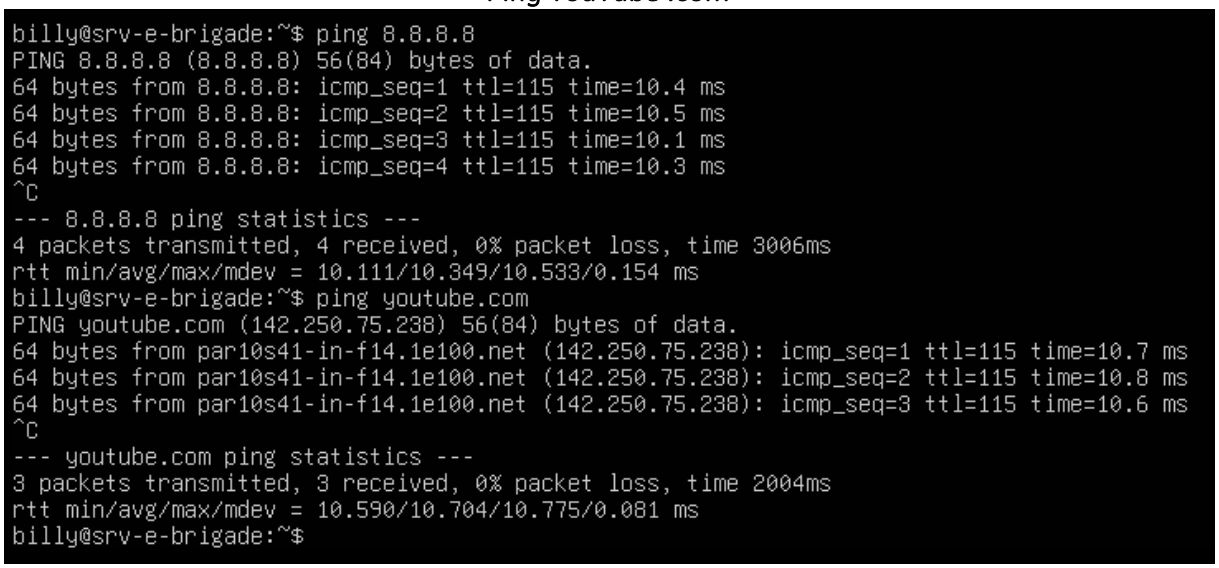
Une fois fait vérifier si l'ip c'est bien en statique via la commande suivante :

Ip a

```
billy@srv-e-brigade:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:e7:70:a5 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.11/24 brd 192.168.20.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee7:70a5/64 scope link
       valid_lft forever preferred_lft forever
billy@srv-e-brigade:~$ _
```

Pour finir nous allons vérifier si le serveur E-brigade est bien connecter au réseau via les commande suivantes :

Ping 8.8.8.8
Ping YouTube .com



Comme vous pouvez le constater le ping fonctionne bien avec l'ip ou le nom de domaine .

Installation e- brigade

Avant de réaliser l'installation assurer-vous que votre Ubuntu soit bien à jour via cette commande

sudo apt update && sudo apt upgrade -y

```
La maintenance de sécurité étendue pour Applications n'est pas activée.

0 mise à jour peut être appliquée immédiatement.

Activez ESM Apps pour recevoir des futures mises à jour de sécurité supplémentaires.
Visitez https://ubuntu.com/esm ou executez : sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
```

```
billy@srv-e-brigade:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for billy:
Atteint :1 http://archive.ubuntu.com/ubuntu noble InRelease
Réception de :2 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Réception de :3 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Réception de :4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Réception de :5 http://archive.ubuntu.com/ubuntu noble/main Translation-fr [491 kB]
Réception de :6 http://archive.ubuntu.com/ubuntu noble/main amd64 c-n-f Metadata [30,5 kB]
Réception de :7 http://archive.ubuntu.com/ubuntu noble/restricted Translation-fr [3 292 B]
Réception de :8 http://archive.ubuntu.com/ubuntu noble/restricted amd64 c-n-f Metadata [416 B]
Réception de :9 http://archive.ubuntu.com/ubuntu noble/universe Translation-fr [3 898 kB]
Réception de :10 http://archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Réception de :11 http://archive.ubuntu.com/ubuntu noble/multiverse Translation-fr [89,0 kB]
Réception de :12 http://archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8 328 B]
Réception de :13 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [979 kB]
Réception de :14 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [215 kB]
Réception de :15 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Réception de :16 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [13,5 kB]
Réception de :17 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [876 kB]
Réception de :18 http://archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [177 kB]
Réception de :19 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Réception de :20 http://archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [492 B]
Réception de :21 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1 046 kB]
Réception de :22 http://archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [263 kB]
Réception de :23 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [365 kB]
Réception de :24 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [26,0 kB]
Réception de :25 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [21,5 kB]
Réception de :26 http://archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [4 788 B]
Réception de :27 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Réception de :28 http://archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [592 B]
0% [18 Translation-en store 0 B] [Attente des fichiers d'en-tête]
```

Taper le mot de passe

Une fois après avoir réaliser la mise à jour nous allons installer maria db via cette commande :

sudo apt install mariadb-server -y

```
billy@srv-e-brigade:~$ sudo apt install mariadb-server -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  galera-4 libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifiles-perl libdbd-mysql-perl libdbi-perl libencode-locale-perl libfcgi-bin
  libfcgi-perl libfcgi0t64 libhtml-parser-perl libhtml-tagset-perl libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl
  liblwp-mediatypes-perl libmariadb3 libmysqlclient21 libsnappy1v5 libtimedate-perl liburi-perl liburing2 mariadb-client mariadb-client-core
  mariadb-common mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
  mariadb-plugin-provider-snappy mariadb-server-core mysql-common pv socat
Paquets suggérés :
  libmldbm-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl libipc-sharedcache-perl libio-compress-brotli-perl libbusiness-isbn-perl
  libregexp-ipv6-perl libwww-perl mailx mariadb-test doc-base
Les NOUVEAUX paquets suivants seront installés :
  galera-4 libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifiles-perl libdbd-mysql-perl libdbi-perl libencode-locale-perl libfcgi-bin
  libfcgi-perl libfcgi0t64 libhtml-parser-perl libhtml-tagset-perl libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl
  liblwp-mediatypes-perl libmariadb3 libmysqlclient21 libsnappy1v5 libtimedate-perl liburi-perl liburing2 mariadb-client mariadb-client-core
  mariadb-common mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma mariadb-plugin-provider-lzo
  mariadb-plugin-provider-snappy mariadb-server mariadb-server-core mysql-common pv socat
0 mis à jour, 37 nouvellement installés, 0 à enlever et 1 non mis à jour.
Il est nécessaire de prendre 19,7 Mo dans les archives.
Après cette opération, 201 Mo d'espace disque supplémentaires seront utilisés.
0% [En cours]
```

Puis nous allons sécuriser maria db via cette commande :

sudo mysql_secure_installation

```
billy@srv-e-brigade:~$ sudo mysql_secure_installation

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):
```

Entrer un mot de passe

Voici ce que vous devez répondre

```
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] y
 ... 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] y
 ... Success!

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] y
 - 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] y
 ... Success!

Cleaning up...
```

Création de la base de données e-bigade

Pour cela nous allons créer la base via cette commande :

sudo mysql -u root
CREATE DATABASE ebrigade_db;
CREATE USER 'billy'@'localhost' IDENTIFIED BY 'Testap04@';
GRANT ALL PRIVILEGES ON ebrigade_db. TO 'billy'@'localhost';*

```
billy@srv-e-brigade:~$ sudo mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 10.11.11-MariaDB-0ubuntu0.24.04.2 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE ebrigade_db;
Query OK, 1 row affected (0,005 sec)

MariaDB [(none)]> CREATE USER 'billy'@'localhost' IDENTIFIED BY 'Testap04@';
N ebrigade_db.* TO 'billy'@'localhost';
Query OK, 0 rows affected (0,016 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON ebrigade_db.* TO 'billy'@'localhost';
Query OK, 0 rows affected (0,005 sec)

MariaDB [(none)]>
```

Comme vous pouvez le voir les commandes ont était prise en compte

FLUSH PRIVILEGES;
EXIT;

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON ebrigade_db.* TO 'billy'@'localhost';
Query OK, 0 rows affected (0,005 sec)

MariaDB [(none)]>  FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,005 sec)

MariaDB [(none)]> EXIT;
Bye
billy@srv-e-brigade:~$
```

Comme vous pouvez le voir les commandes ont était prise en compte

Installation Apache 2

Dans cette partie nous allons installer apache 2 via cette commande :

sudo apt install apache2 -y

```
Bye
billy@srv-e-brigade:~$ sudo apt install apache2 -y
Lecture des listes de paquets… 77%
```

Une fois avoir installer nous allons télécharger les indépendances via cette commandes :

sudo apt install software-properties-common -y
sudo add-apt-repository ppa:ondrej/php -y
sudo apt update

```
*** Le système doit être redémarré ***
Last login: Tue Apr  1 09:12:27 2025 from 192.168.20.1
billy@srv-e-brigade:~$ sudo apt install software-properties-common -y
sudo add-apt-repository ppa:ondrej/php -y
sudo apt update
[sudo] password for billy:
Lecture des listes de paquets… 99%
```

Puis nous allons installer PHP 7.4 + extension via cette commande :

sudo apt install php7.4 libapache2-mod-php7.4 php7.4-mysql php7.4-xml php7.4-gd php7.4-curl -y

```
billy@srv-e-brigade:~$ sudo apt install php7.4 libapache2-mod-php7.4 php7.4-mysql php7.4-xml php7.4-gd
php7.4-curl -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  php-common php7.4-cli php7.4-common php7.4-json php7.4-opcache php7.4-readline
Paquets suggérés :
  php-pear
Les NOUVEAUX paquets suivants seront installés :
  libapache2-mod-php7.4 php-common php7.4 php7.4-cli php7.4-common php7.4-gd php7.4-json php7.4-mysql php7.4-opcache php7.4-readline php7.4-xml
0 mis à jour, 11 nouvellement installés, 0 à enlever et 2 non mis à jour.
Il est nécessaire de prendre 4 359 ko dans les archives.
Après cette opération, 18,8 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
Réception de :1 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 php-common all 2:95+ubuntu24.04.1+deb.sury.org+2 [13,2 kB]
Réception de :2 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 php7.4-common amd64 1:7.4.33-18+ubuntu24.04.1+deb.sury.org+1 [687 kB]
Réception de :3 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 php7.4-json amd64 1:7.4.33-18+ubuntu24.04.1+deb.sury.org+1 [20,6 kB]
Réception de :4 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 php7.4-opcache amd64 1:7.4.33-18+ubuntu24.04.1+deb.sury.org+1 [219 kB]
Réception de :5 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 php7.4-readline amd64 1:7.4.33-18+ubuntu24.04.1+deb.sury.org+1 [13,3 kB]
Réception de :6 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 php7.4-cli amd64 1:7.4.33-18+ubuntu24.04.1+deb.sury.org+1 [1 573 kB]
Réception de :7 https://ppa.launchpadcontent.net/ondrej/php/ubuntu noble/main amd64 libapache2-mod-php7.4 amd64 1:7.4.33-18+ubuntu24.04.1+deb.sury.org+1 [1
510 kB]
58% [7 libapache2-mod-php7.4 17,5 kB/1 510 kB 1%]
```

Puis ensuite nous allons redémarrer apache 2 via cette commande :

sudo systemctl restart apache2

```
billy@srv-e-brigade:~$ sudo systemctl restart apache2
billy@srv-e-brigade:~$
```

Une fois que PHP est installer nous allons vérifier la version via cette commande :

php -v

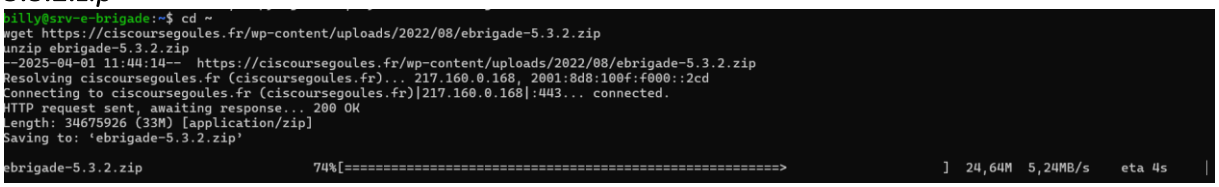
```
billy@srv-e-brigade:~$ php -v
PHP 7.4.33 (cli) (built: Dec 24 2024 07:12:16) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.33, Copyright (c), by Zend Technologies
billy@srv-e-brigade:~$
```

Version sur 7.3 ou plus

Téléchargement de l’archive depuis la source officielle

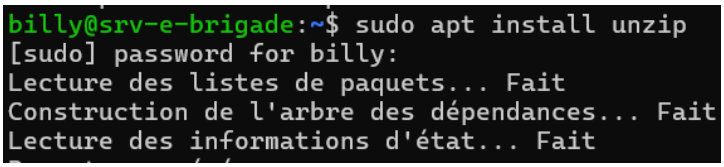
Une fois que la bonne version de PHP est installé nous allons extraire le fichier via cette commande :

cd ~ wget https://ciscoursegoules.fr/wp-content/uploads/2022/08/ebrigade-5.3.2.zip unzip ebrigade-5.3.2.zip



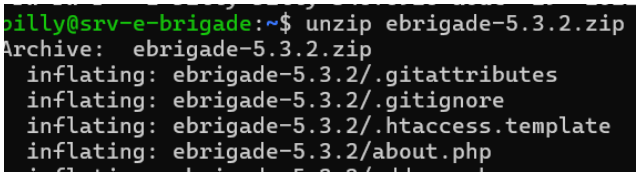
Une fois après avoir télécharger l'archive le serveur va vous demander d'installer unzip dans le cas ou votre machine na pas le logiciel

Taper le mot de passe sudo



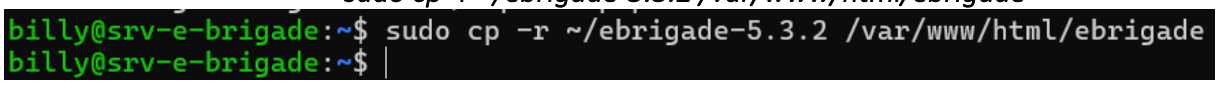
Après avoir taper le mot de passe ainsi avoir extrai le fichier via cette commande :

unzip ebrigade-5.3.2.zip



Une fois faits-nous allons copier le repertoire web via cette commande :

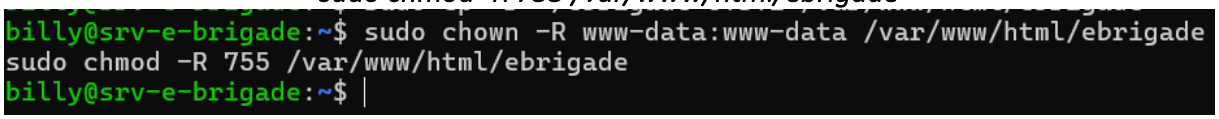
sudo cp -r ~/ebrigade-5.3.2 /var/www/html/ebrigade



Après avoir copier nous allons attribuer les permission via ces commandes :

sudo chown -R www-data:www-data /var/www/html/ebrigade

sudo chmod -R 755 /var/www/html/ebrigade

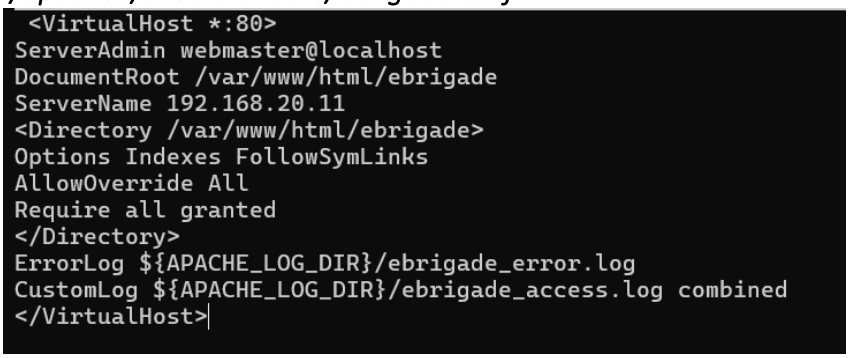


Configuration Apache pour E-brigade

Pour cela nous allons créer un fichier de configuration via cette commande :

sudo nano /etc/apache2/sites-available/ebrigade.conf

Une fois avoir rentrer ces information là faite ctr + x puis appuyer sur entrer pour valider



Une fois après avoir rentré les information nécessaire nous allons activer le site ainsi que le module via les commandes suivantes :

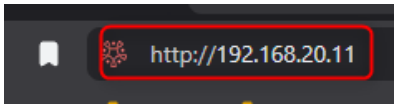
sudo a2ensite ebrigade.conf
sudo a2enmod rewrite
sudo systemctl reload apache2

```
billy@srv-e-brigade:~$ sudo a2ensite ebrigade.conf
sudo a2enmod rewrite
sudo systemctl reload apache2
Enabling site ebrigade.
To activate the new configuration, you need to run:
  systemctl reload apache2
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
billy@srv-e-brigade:~$
```

Connexion E-brigade à partir d'un navigateur

Alors une fois avoir finaliser l'installation nous allons prendre un navigateur et donc taper cette ip :

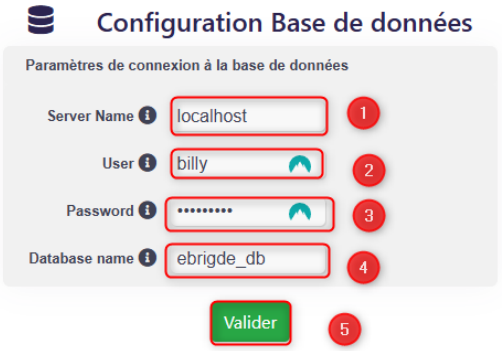
http://192.168.20.11/



Paramétrage E-brigade

Une fois avoir taper nous allons atterrie sur cette page de configuration de base de donnée

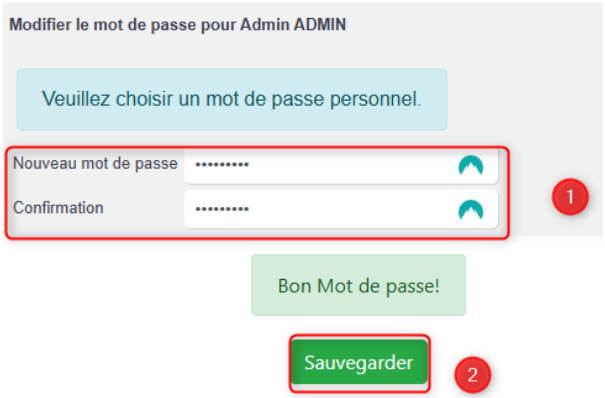
(1) Rentrer le nom du serveur
(2) Rentrer l'utilisateur
(3) Rentrer le mot de passe
(4) Rentrer le nom de la data base
(5) Cliquer sur valider



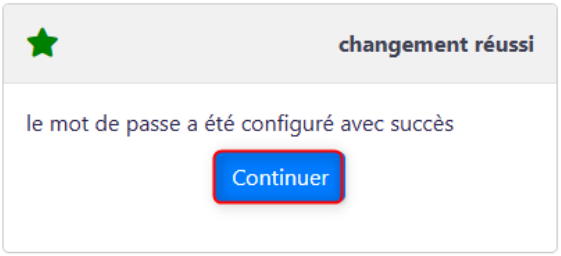
Une fois après avoir rentrer les bonne information nous allons devoir changer le mot de passe

Cliquer sur Choix mot de passe pour admin

(1) Définir un mot de passe puis confirmer
(2) Cliquer sur Sauvegarder



Une fois après avoir fait des modifications vous aurez un message de confirmation

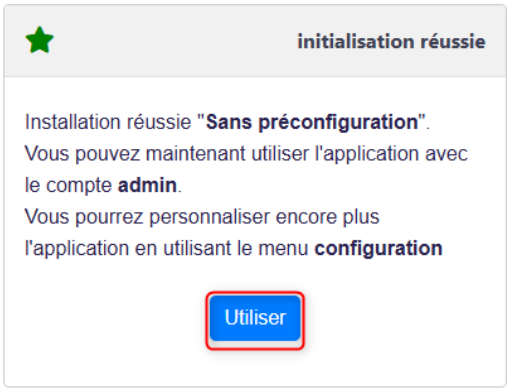


Cliquer sur continuer

Une fois cela fait nous allons configurer Ebrigade

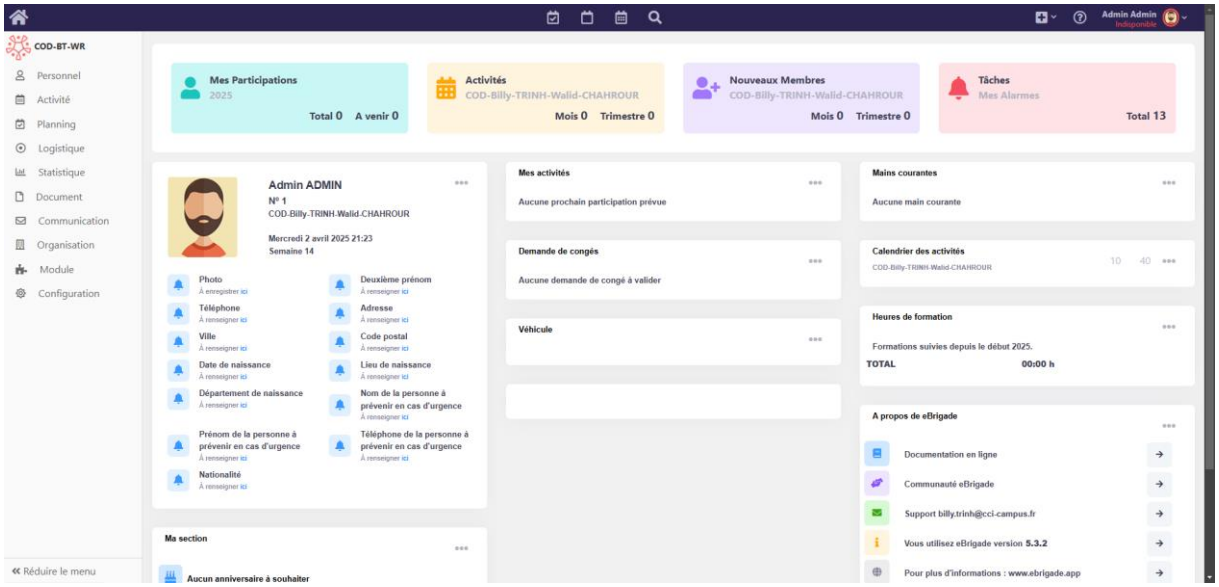
(1) Mettre sans préconfigurassions dans le type d'organisation
(2) Mettre le nom de l'organisation
(3) Puis mettre le nom de l'organisation
Mettre une adresse mail
(4) Cliquer sur Valider

Un autre message de confirmation



Cliquer sur utiliser

Une fois après avoir cliquer sur utiliser nous allons avoir l'interface de E-brigade



Fixation IP sur Ubuntu 22.04

sudo nano /etc/netplan/00-installer-config.yaml :

```
billy@srv-mail:~$ sudo nano /etc/netplan/00-installer-config.yaml
[sudo] password for billy:
```

- billy@srv-mail:~$: Invite de commande du terminal, utilisateur billy connecté sur la machine nommée srv-mail.
- sudo nano /etc/netplan/00-installer-config.yaml :
  - Utilise sudo pour ouvrir le fichier système en tant qu'administrateur.
  - Utilise l'éditeur de texte nano pour modifier le fichier YAML de configuration réseau situé dans /etc/netplan/.
- [sudo] password for billy: : Le système demande maintenant le mot de passe de l'utilisateur billy pour exécuter la commande avec privilèges.

Contenu du fichier /etc/netplan/00-installer-config.yaml

```
network:
  version: 2
  ethernets:
    ens33:
      dhcp4: no
      addresses:
        - 192.168.20.30/24
      routes:
        - to: default
          via: 192.168.20.254
      nameservers:
       addresses:
         - 8.8.8.8
         - 1.1.1.1
```

Sauvegarder avec CTRL + O, puis quitter avec CTRL + X.
Appliquer les changements Netplan avec :

sudo netplan apply

Ligne Élément Description

network: Début du bloc de configuration réseau.

version: 2 Indique la version du format Netplan (obligatoire).

ethernets: Définit les interfaces réseau de type Ethernet.

ens33: Nom de l'interface réseau configurée (à adapter selon votre machine).

dhcp4: no Désactive l'attribution automatique via DHCP (IPv4).

addresses: Adresse IP statique assignée à l'interface.

- 192.168.20.30/24 IP statique + masque CIDR (/24 = 255.255.255.0).

routes: Définition des routes par défaut.

- to: default Route par défaut.

via: 192.168.20.254 Passerelle (gateway) utilisée pour sortir du réseau local.

nameservers: Bloc DNS.

addresses: Liste des serveurs DNS utilisés.

- 8.8.8.8, - 1.1.1.1 DNS publics de Google et Cloudflare.

Installation de Modoboa via Git et l'installateur

cd /opt
C'est un emplacement standard sous Linux destiné à accueillir des **applications tierces** ou **personnalisées**.
Typiquement utilisé pour :

- Déployer des logiciels compilés manuellement ;
- Installer des outils comme zimbra, sonarqube, ou asterisk (hors paquets apt).

```
billy@srv-mail:~$ cd /opt
billy@srv-mail:/opt$
```

Se place dans le répertoire /opt (classiquement utilisé pour les logiciels tiers).

sudo git clone https://github.com/modoboa/modoboa-installer

```
billy@srv-mail:/opt$ sudo git clone https://github.com/modoboa/modoboa-installer
Cloning into 'modoboa-installer'...
remote: Enumerating objects: 3434, done.
remote: Counting objects: 100% (937/937), done.
remote: Compressing objects: 100% (259/259), done.
remote: Total 3434 (delta 784), reused 758 (delta 671), pack-reused 2497 (from 3)
Receiving objects: 100% (3434/3434), 695.79 KiB | 11.79 MiB/s, done.
Resolving deltas: 100% (2386/2386), done.
billy@srv-mail:/opt$
```

Élément	Détail
sudo	Permet d'exécuter la commande avec les privilèges administrateur (indispensable dans /opt).
git clone	Clone (copie) un dépôt Git distant vers le système local.
https://github.com/modoboa/modoboa-installer	URL du dépôt Git contenant le script d'installation de la solution **Modoboa** (serveur de messagerie complet).

- Le dossier **modoboa-installer** a été créé dans le répertoire actuel (/opt).
- Le dépôt comprend **3 434 objets**, pour une taille d'environ **695 Ko**, et a été transféré à **11.79 MiB/s**.
- Tous les objets ont été correctement compressés, reçus et les **delta (différences internes Git)** ont été résolus avec succès.

Clone le dépôt Git contenant le Modoboa Installer.

cd modoboa-installer

```
billy@srv-mail:/opt$ cd modoboa-installer
billy@srv-mail:/opt/modoboa-installer$
```

Élément	Explication
cd modoboa-installer	Commande utilisée pour accéder au répertoire modoboa-installer, qui vient d'être cloné depuis GitHub.
billy@srv-mail:/opt/modoboa-installer$	Confirmation que l'utilisateur est maintenant positionné **dans le dossier du script d'installation** de Modoboa.

Étape suivante (logique) dans une procédure d'installation :

Il est généralement recommandé d'exécuter le script suivant :

sudo ./run.py cod.local

```
billy@srv-mail:/opt/modoboa-installer$ sudo ./run.py cod.local
Welcome to Modoboa installer!

Checking the installer...
Installer seems up to date!
Checks complete

Configuration file installer.cfg not found, creating new one.
Notice:
It is recommanded to run this installer on a FRESHLY installed server.
(ie. with nothing special already installed on it)

Warning:
Before you start the installation, please make sure the following DNS records exist for domain 'cod.local':
  mail IN A   <IP ADDRESS OF YOUR SERVER>
     @ IN MX  mail.cod.local.

Your mail server will be installed with the following components:
fail2ban modoboa automx amavis clamav dovecot nginx razor postfix postwhite spamassassin uwsgi radicale opendkim
Do you confirm? (Y/n) y
The process can be long, feel free to take a coffee and come back later ;)
Starting...
```

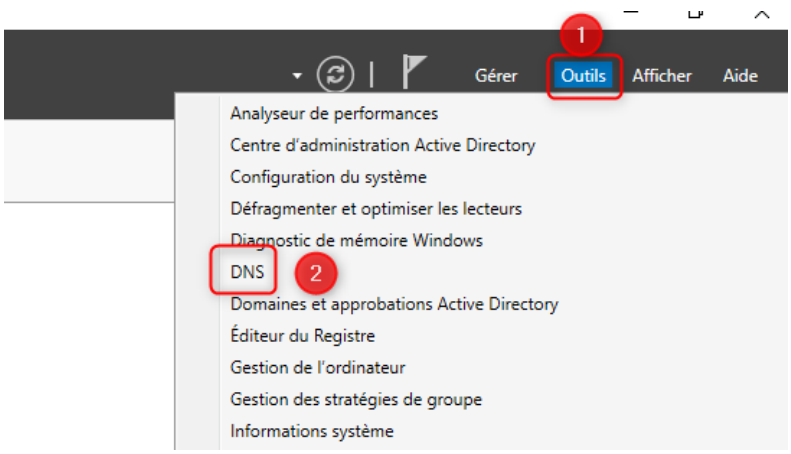
Élément	Description
sudo ./run.py cod.local	Lance le script principal d'installation de Modoboa avec le domaine principal cod.local.
installer.cfg not found	Le fichier de configuration n'existe pas encore, il va être généré automatiquement.
recommended to run on a FRESHLY installed server	Recommandation forte : le serveur doit être neuf, sans autres services installés pour éviter les conflits.

Élément	Description
DNS requirements	Vous devez avoir les enregistrements suivants configurés (localement ou en DNS interne si en .local) : ➤ mail.cod.local doit pointer vers l'IP du serveur (A record) ➤ @ doit avoir une entrée MX pointant vers mail.cod.local.
Modules installés	Le script va installer **toute la pile mail complète**, notamment : - Sécurité : fail2ban, postwhite, opendkim - MTA/IMAP : postfix, dovecot - Antispam/antivirus : amavis, clamav, spamassassin, razor - Webmail/portail : modoboa, nginx, uwsgi, automx, radicale
Do you confirm?	Vous avez validé l'installation complète en répondant y.
Starting...	Le processus d'installation est en cours. ⚠️ Cela peut prendre plusieurs dizaines de minutes.

Une fois terminer voici le résultat .

```
Installing dovecot
User dovecot already exists, skipping creation but please make sure the /srv/vmail directory exists.
Congratulations! You can enjoy Modoboa at https://mail.cod.local (admin:password)

Modoboa is a free software maintained by volunteers.
You like the project and want it to be sustainable?
Then don't wait anymore and go sponsor it here:

https://github.com/sponsors/modoboa

Thank you for your help :-)

billy@srv-mail:/opt/modoboa-installer$
```

Configuration du DNS pour modoboa

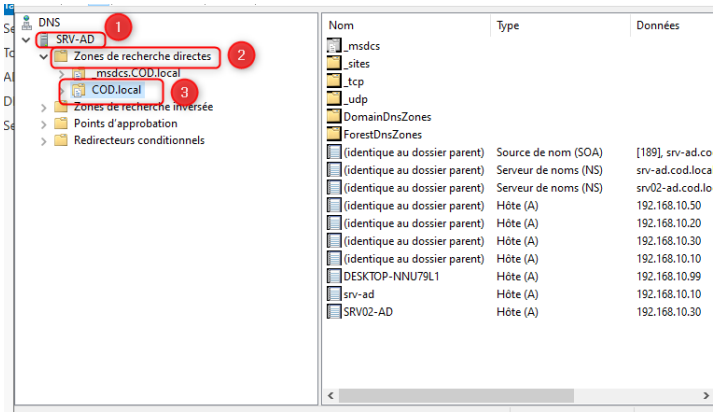


1. Cliquez sur l'onglet **Outils** (en haut à droite de la fenêtre principale du Gestionnaire de serveur).
(Encadré en bleu avec le repère ① dans la capture)

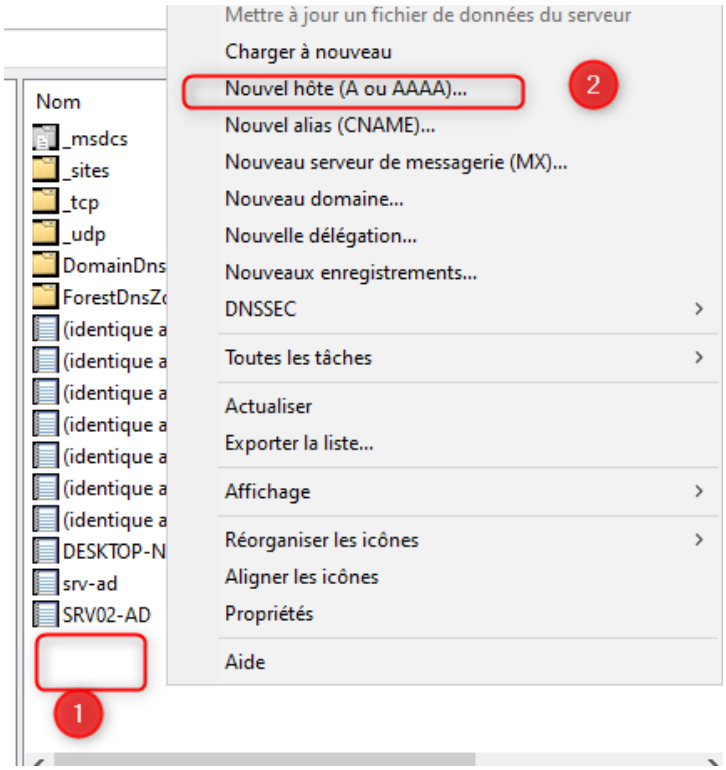
2. Dans le menu déroulant, sélectionnez l'élément **DNS**.
(Encadré en rouge avec le repère ② dans la capture)

Structure affichée dans la console DNS :

1. SRV-AD – Le serveur DNS (nom de l'hôte du contrôleur de domaine).
2. Zones de recherche directes – Regroupe les zones DNS pour la résolution de noms → IP.
3. COD.local – La zone de recherche directe utilisée pour votre domaine local (cod.local).



Dans le panneau de droite, on observe plusieurs enregistrements de type A (adresse IPv4) déjà définis.



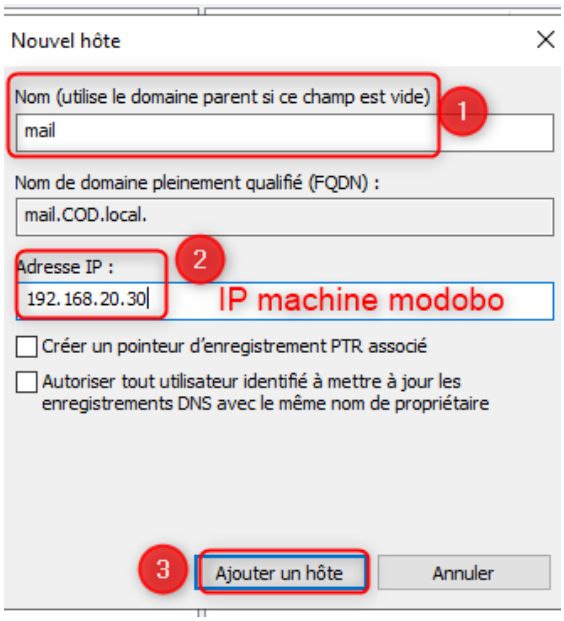
1. Clic droit sur la zone COD.local dans l'arborescence DNS (repère ● ①)

2. Sélectionner "Nouvel hôte (A ou AAAA)..." dans le menu contextuel (repère ● ②)

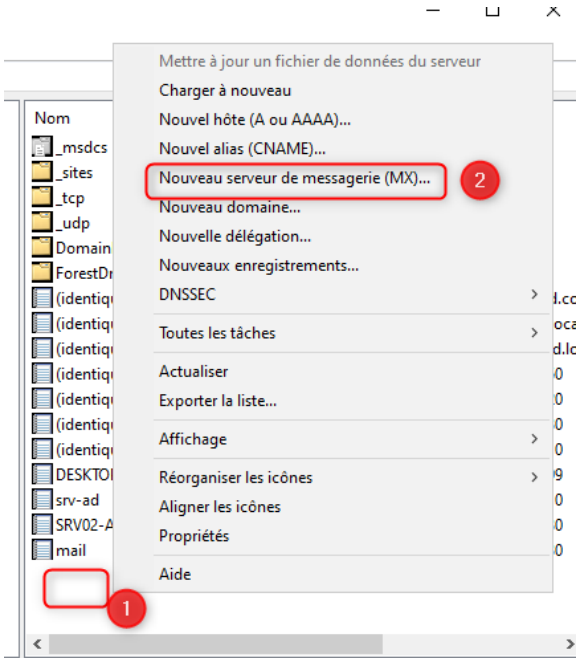
- Ajouter un enregistrement A pointant un nom de machine (ex. mail) vers une adresse IP (ex. 192.168.20.30).
- Indispensable pour permettre aux clients et serveurs d'atteindre mail.cod.local via une résolution DNS interne.

Création d'un enregistrement de type A pour Modoboa

(1) **Nom** *(utilise le domaine parent si ce champ est vide)* :
(2) **Adresse IP** *(IP machine modobo)* :
(3) Valide la création de l'enregistrement A.

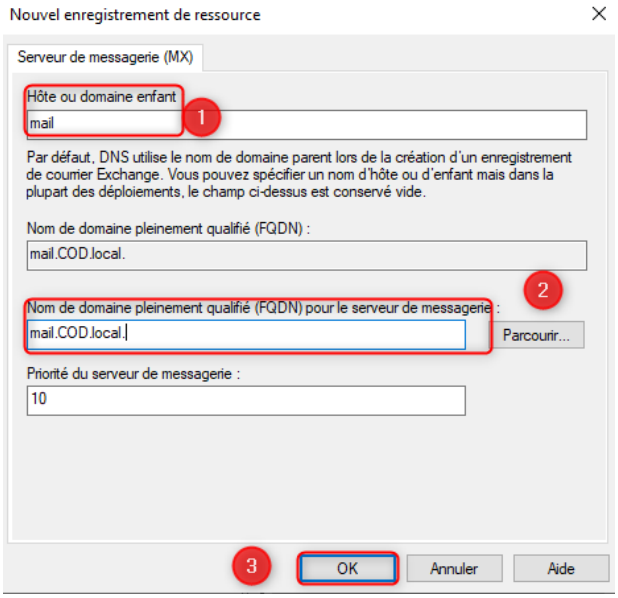


Création d'un enregistrement de type MX pour Modoboa



(1) Clic droit sur la zone **COD.local**

(2) Sélection de l'option : Nouveau serveur de messagerie (MX)...

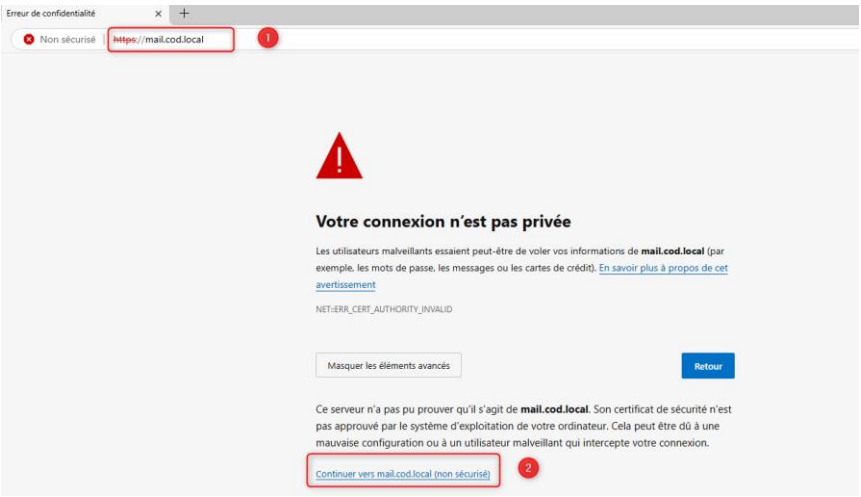


(1) Hôte ou domaine enfant *(repère ①)* :

(2) Nom de domaine pleinement qualifié (FQDN) pour le serveur de messagerie

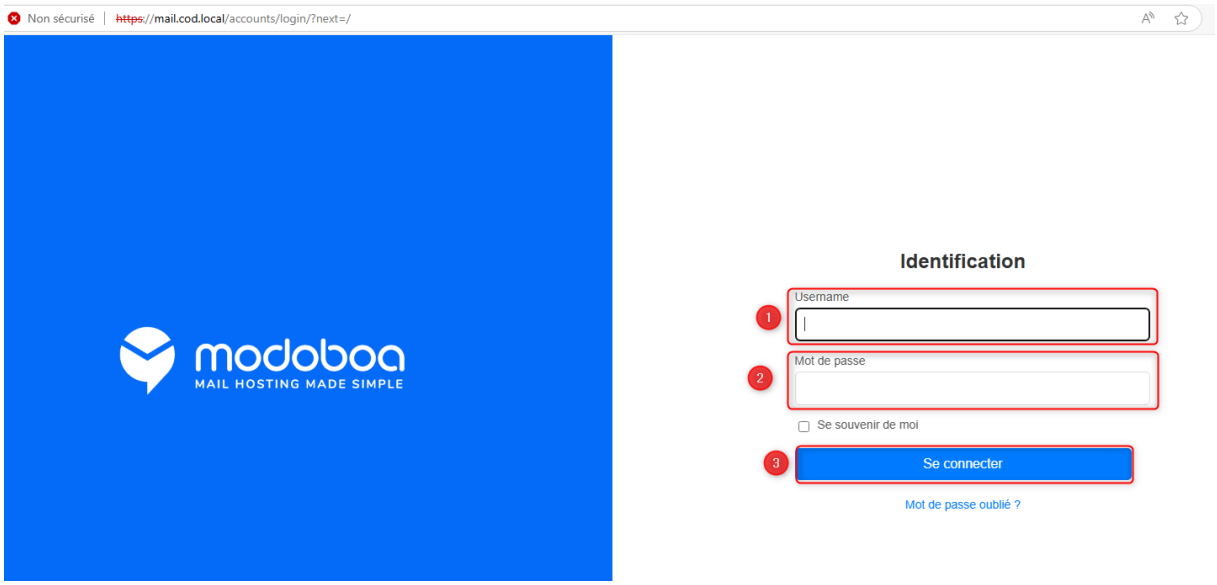
Accès à l'interface Web de Modoboa

Une fois que Mex est créer cliquer sur un navigateur internet puis taper le mot suivant : mail.cod.local



Barre d'adresse du navigateur *(repère ①)* : https://mail.cod.local
Message du navigateur (Firefox ou Chrome) :
Lien d'action (repère ②) : Continuer vers mail.cod.local (non sécurisé)
Permet de forcer l'accès à l'interface, malgré l'avertissement de sécurité.

Page de connexion à Modoboa (mail.cod.local)



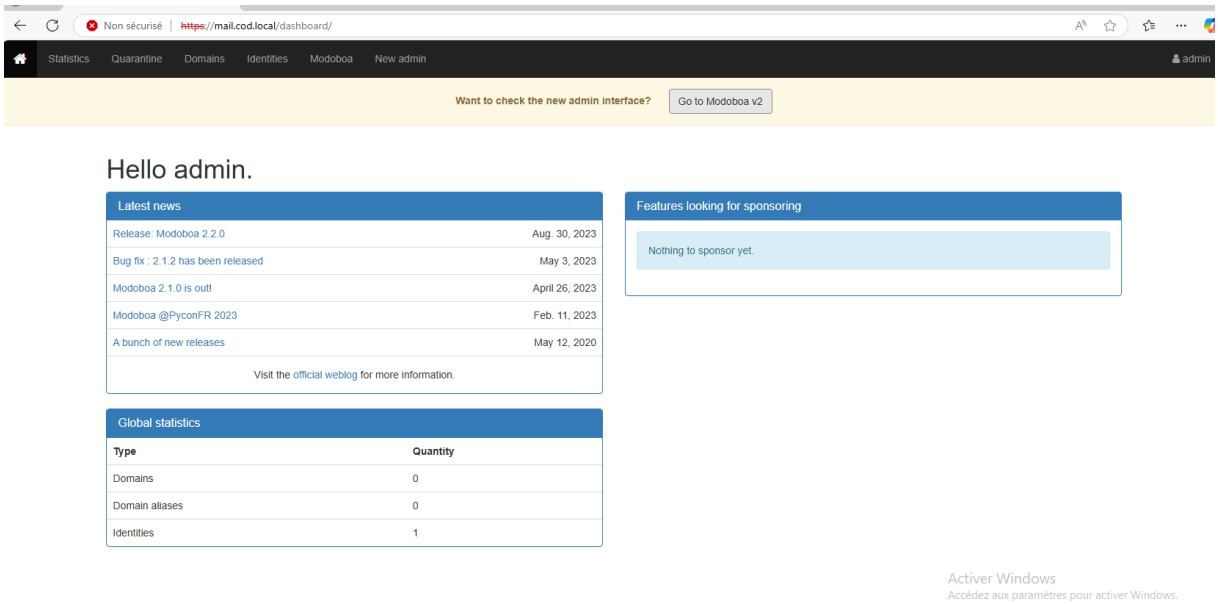
1. **Champ "Username"** *(repère ①)*
   ➤ Saisir le **nom d'utilisateur** administrateur par défaut (en général admin).
2. **Champ "Mot de passe"** *(repère ②)*
   ➤ Saisir le **mot de passe défini** lors de l'installation.
   (Ce mot de passe est affiché dans le terminal à la fin de l'installation de Modoboa. = password)
3. **Bouton "Se connecter"** *(repère ③)*
   ➤ Cliquer ici pour valider les identifiants et accéder au tableau de bord d'administration.

Barre de navigation (haut de page) :

- Statistics, Quarantine, Domains, Identities, Modoboa, New admin
- Nom de l'utilisateur connecté : admin

Message de bannière :
Want to check the new admin interface?
➤ Bouton : Go to Modoboa v2
Encadré "Latest news" :
➤ Informations sur les dernières mises à jour publiées.

- Encadré “Global statistics” :

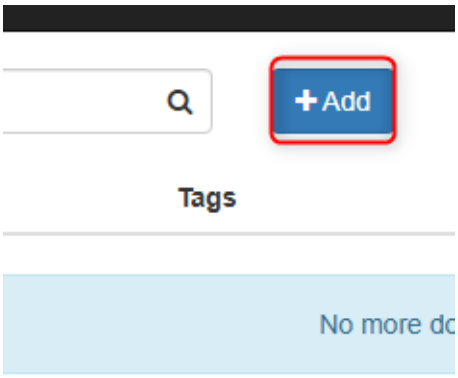


Accéder à la gestion des domaines dans Modoboa

L’onglet **Domains** (encadré rouge) est situé dans la **barre de navigation supérieure**, aux côtés des menus :

- Statistics
- Quarantine
- Identities
- Modoboa
- New admin

Bouton d'ajout (repère encadré) :
+ Add



Ajout d'un domaine – Formulaire de création dans Modoboa

- **Name** *(repère ①)*

➤ Nom du domaine à créer : ici COD.local

Ce domaine sera utilisé pour l'ensemble des adresses mail (ex. utilisateur@cod.local).

- **Type**

➤ Laisser sur Domain (valeur par défaut).

- **Quota**

➤ Quota global du domaine en Mo (0 = illimité).

- **Default mailbox quota**

➤ Quota par boîte mail (en Mo), attribué automatiquement à chaque utilisateur (0 = illimité).

- **Message sending limit**

➤ Limite de mails pouvant être envoyés par utilisateur (optionnel).

- **Alias(es)**

➤ Ajouter ici un ou plusieurs alias de domaine, séparés par une virgule (facultatif).

- **Enabled**

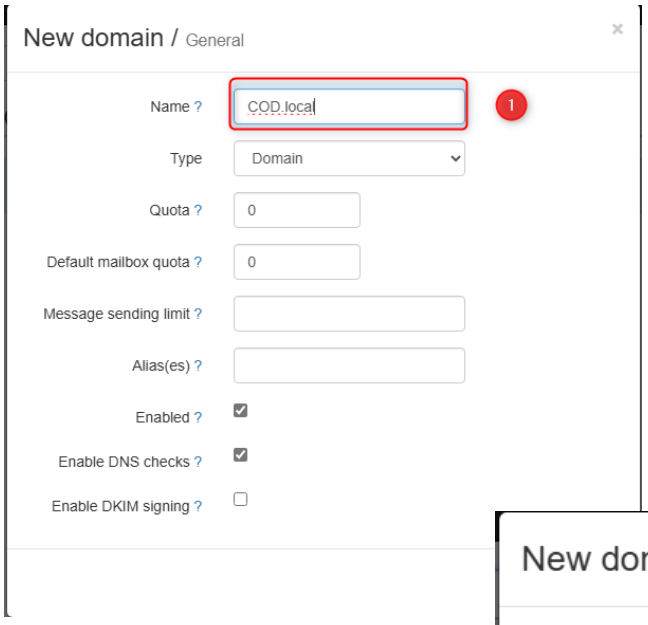
✔ Coche activée – permet l'activation immédiate du domaine.

- **Enable DNS checks**

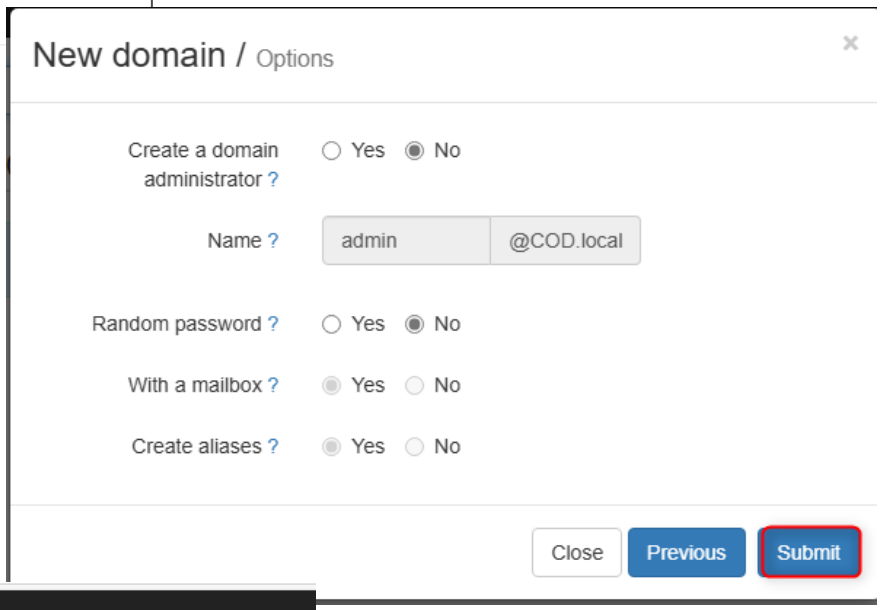
✔ Coche activée – vérifie la cohérence des enregistrements DNS (MX, SPF, etc.).

- **Enable DKIM signing**

➤ Cochez si vous souhaitez activer la signature DKIM (recommandé en production).

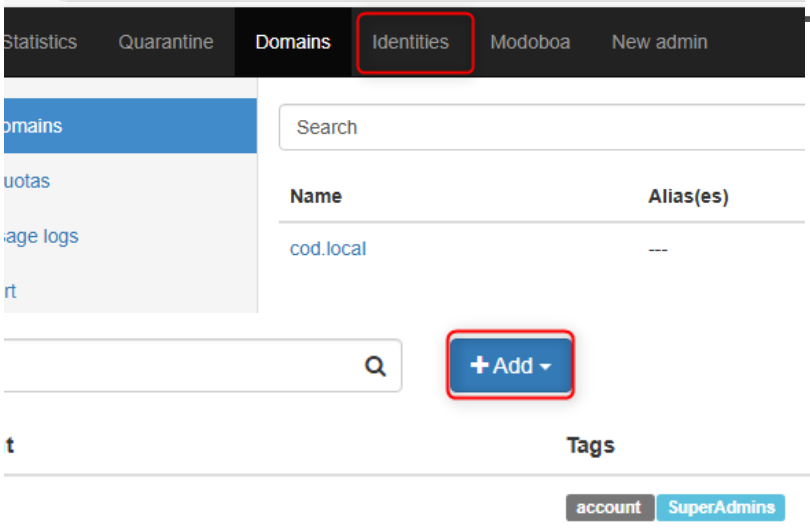


Cette section permet de définir les options supplémentaires liées au domaine fraîchement saisi (COD.local).



Cliquer sur le bouton **Submit** *(encadré rouge)* pour **valider la création du domaine COD.local**.

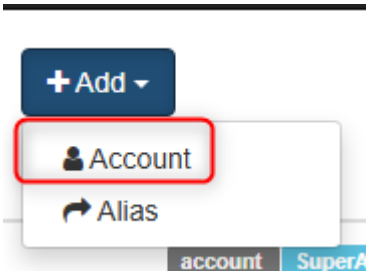
Domaine cod.local ajouté avec succès



Cliquer sur l'onglet **Identities** (encadré rouge) pour créer une ou plusieurs **identités utilisateur** (adresses e-mail personnelles).

Ajout d'une identité (utilisateur)

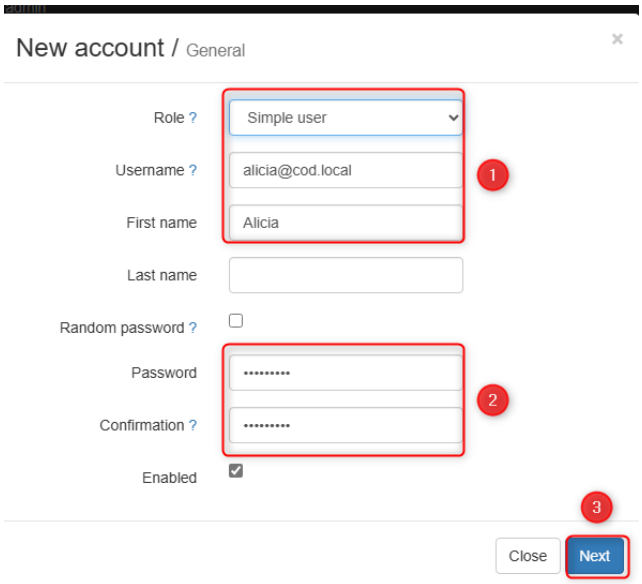
Onglet Identities → Bouton bleu **+ Add** (encadré en rouge).



- Dans le menu **Identities**, cliquez sur le bouton bleu **+ Add**.

- Sélectionnez l'option **Account** (icône utilisateur noire).

Création d'un compte utilisateur dans Modoboa

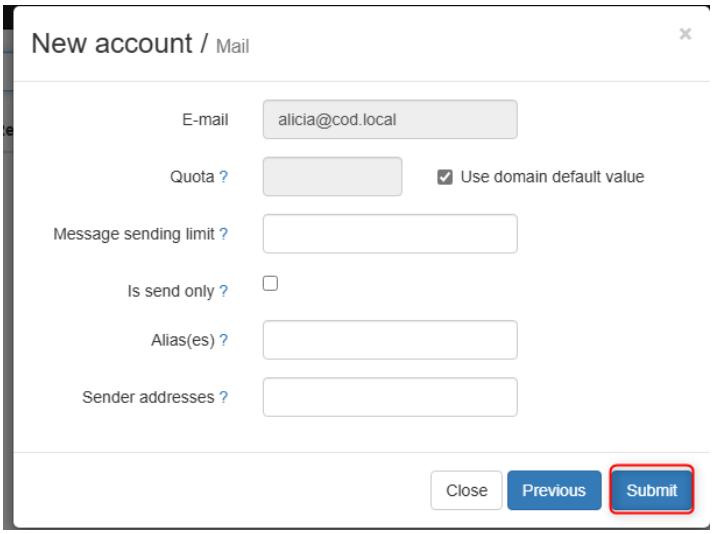


Rôle :
Sélectionner **Simple user** dans le menu déroulant.
Informations de l'utilisateur :

- **Username** : alicia@cod.local
- **First name** : Alicia
- **Last name** : *(optionnel, laissé vide ici)*
- **Password** : entrer le mot de passe souhaité
- **Confirmation** : répéter le mot de passe

Activation du compte :
La case **Enabled** est cochée par défaut .
Valider :
Cliquer sur **Next** pour continuer la configuration du compte.

finalisation du compte mail "Alicia" :



E-mail :
Le champ est prérempli avec l'adresse : alicia@cod.local
Quota :
La case **"Use domain default value"** est cochée ✅
→ Cela applique automatiquement la limite définie au niveau du domaine.

Message sending limit :
Laisser vide pour ne pas appliquer de limite spécifique.

Is send only :
Laisser décoché si l'utilisateur doit **recevoir** et **envoyer** des mails.

Alias(es) :
Laisser vide si aucun alias n'est nécessaire.

Sender addresses :
Laisser vide si l'adresse principale suffit pour l'envoi.

Valider :
Cliquer sur **Submit** pour enregistrer et créer le compte.

Donc pour éviter tout répétition dans la manipulation réaliser pour les deux utilisateurs :

- Bob
- Prtg

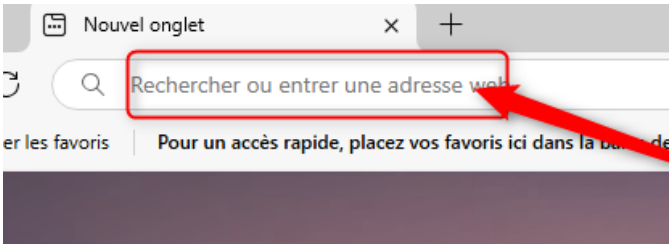
Installation PRTG depuis un navigateur web

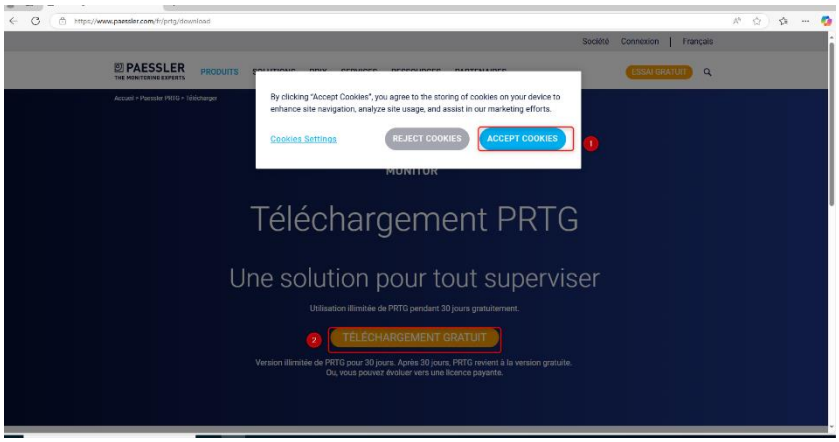
Dans cette partie là nous allons télécharger

Cliquer sur l'icône Microsoft Edge (cercle bleu-vert) située dans la barre en bas de l'écran pour lancer le navigateur.

Cliquez dans la **barre d'adresse** (comme sur ta capture).
Tape cette URL

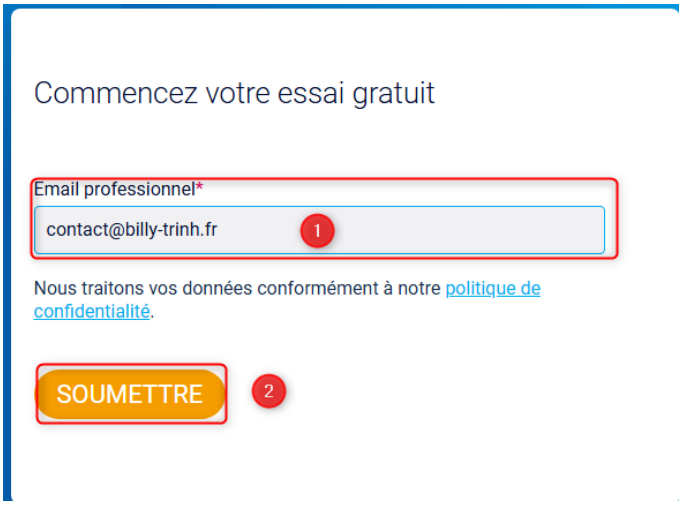
https://www.paessler.com/fr/prtg/download





Accepter les cookies
Clique sur le bouton **"ACCEPT COOKIES"** pour faire disparaître le bandeau (repère 1).
Lancer le téléchargement
Clique ensuite sur le bouton **"TÉLÉCHARGEMENT GRATUIT"** (repère 2).
Ce bouton lance la version d'essai gratuite de 30 jours de **PRTG Network Monitor**.

1. **Saisir ton adresse e-mail professionnelle**
   le champ indiqué (repère 1), adresse, par exemple : contact@billy-trinh.fr
2. **Soumettre le formulaire**
   sur le bouton **"SOUMETTRE"** 2).



➤ Dans entre ton

➤ Clique (repère

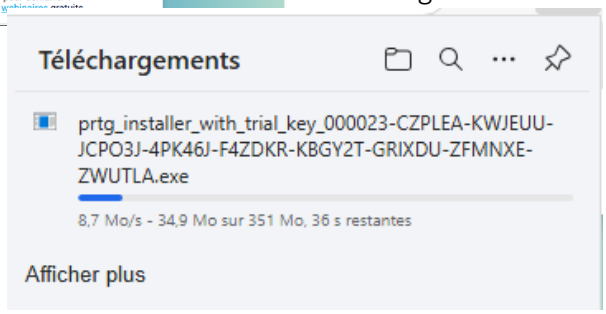
tape de confirmation : téléchargement **en cours**

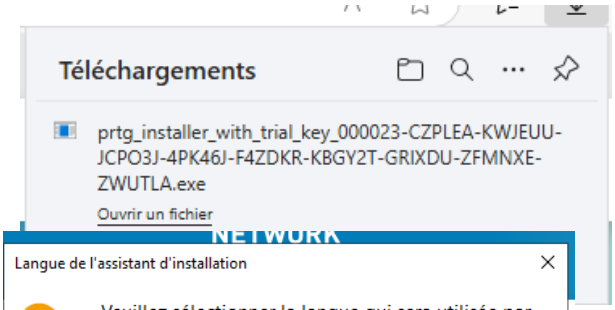
Merci d'avoir téléchargé PRTG.

○ La page t'indique que le téléchargement a commencé automatiquement.

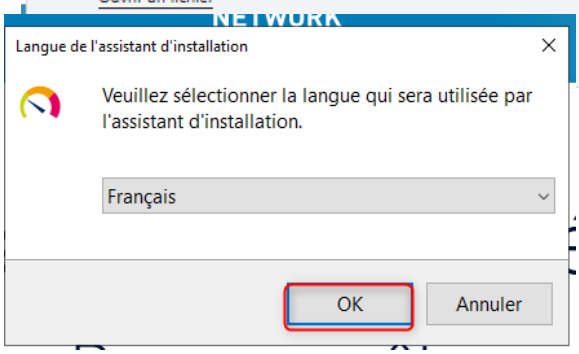
Le fichier d'installation de **PRTG** est bien en cours de téléchargement

Attendre que le fichier à finit de télécharger



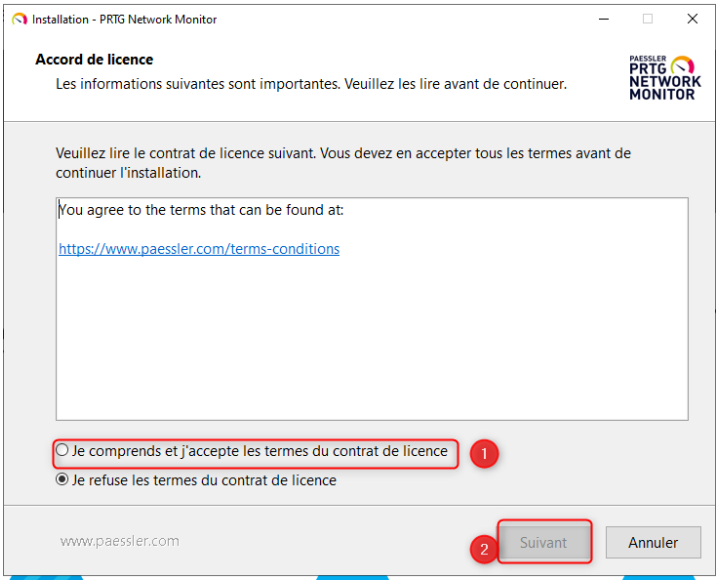


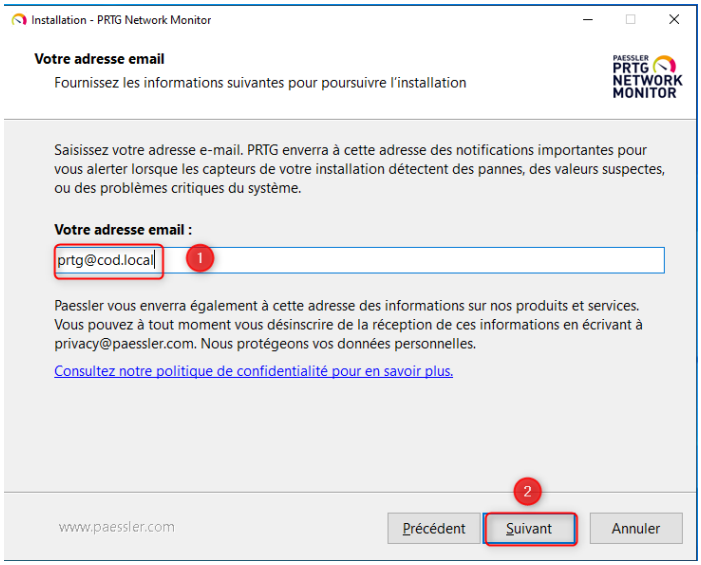
Double-clique sur le fichier .exe



Langue sélectionnée : Français (par défaut)
Clique sur **OK** pour continuer

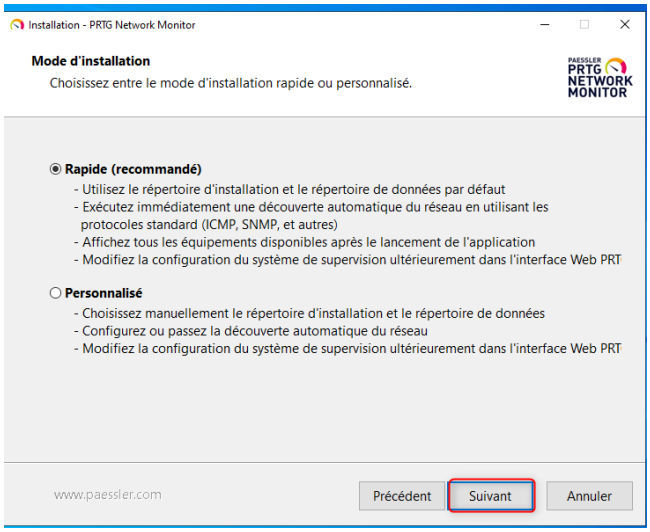
Cocher : Je comprends et j'accepte les termes du contrat de licence
Le bouton **Suivant** va se dégriser. Clique ensuite sur **Suivant** pour continuer l'installation.



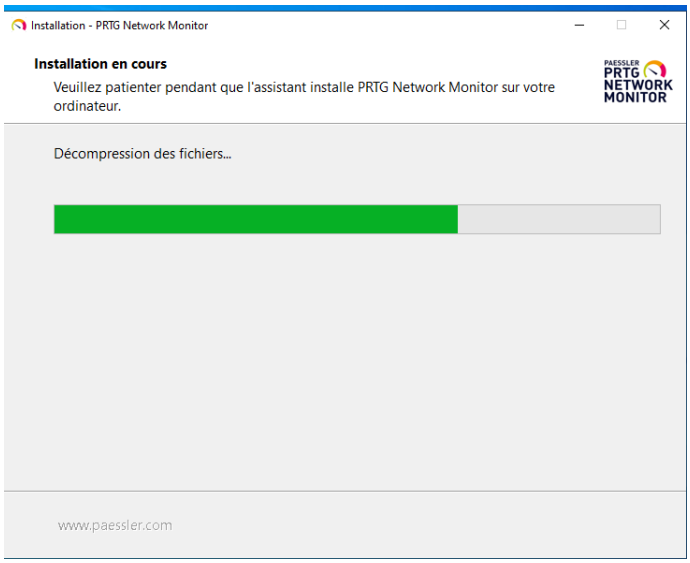


1. **Vérifie** que l'adresse saisie est correcte (ici : prtg@cod.local) – elle sera utilisée pour les alertes.
2. Clique sur **Suivant** pour continuer l'installation.

1. Le mode **Rapide (recommandé)** est sélectionné par défaut — garde cette option sauf si tu veux une configuration spécifique.
2. Clique sur **Suivant** pour continuer l'installation de PRTG.



L'installation de **PRTG Network Monitor** est en cours — la barre de progression montre la **décompression des fichiers**.



Installation en cours, tout se passe bien.
Il suffit maintenant **d'attendre que la décompression et l'installation se terminent**.

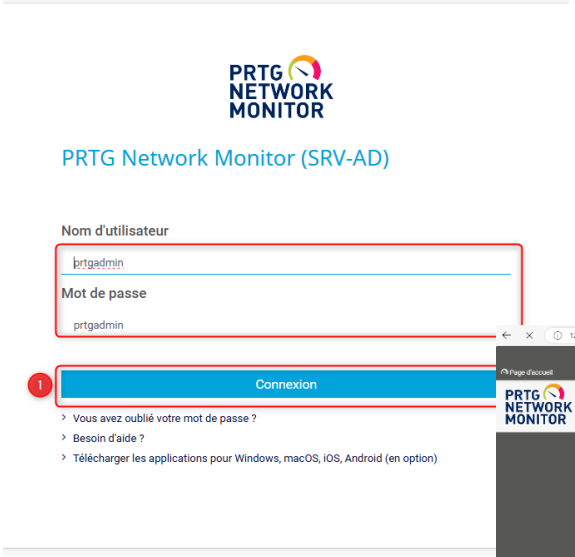
Parfait, l'interface Web de **PRTG Network Monitor** est bien lancée sur l'adresse locale http://127.0.0.1/home

- Le **serveur PRTG est en cours d'initialisation**.
- Il passe différentes étapes :
  - Initialisation de la licence
  - Lancement du Core Server
  - Chargement des définitions de modèles, types de capteurs, etc.

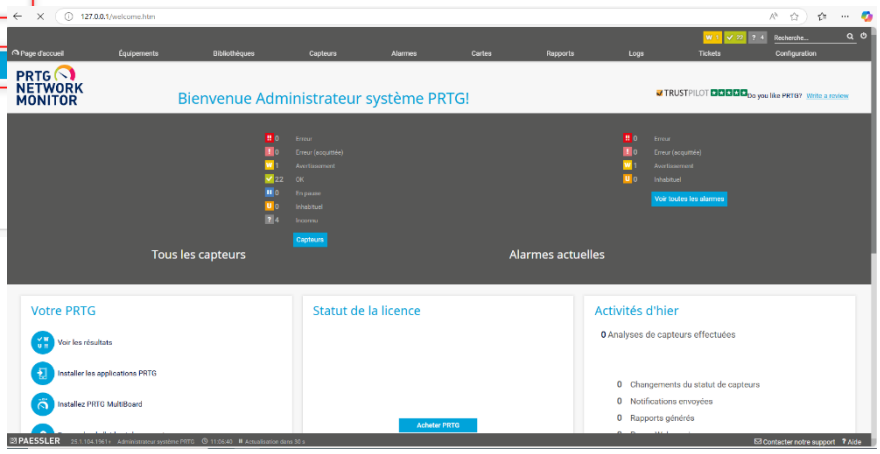
base,

Connexion depuis l'interface WEB

Nous sommes , arrivé à l'écran de connexion de l'interface Web de PRTG Network Monitor



Voici les informations saisies :
Nom d'utilisateur : prtgadmin
Mot de passe : prtgadmin (par défaut, lors de l'installation)
Cliquer sur Connexion



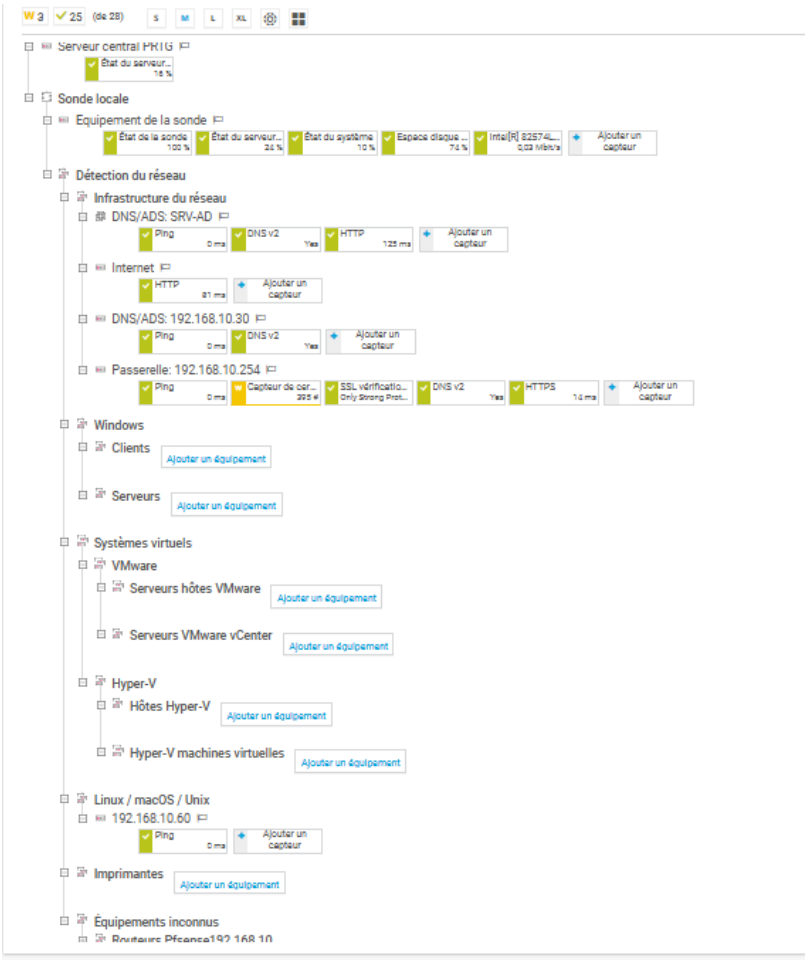
Bienvenue Administrateur système PRTG !
Résumé des capteurs :
22 capteurs fonctionnels (OK)
1 avertissement
4 capteurs inconnus (peut-être mal configurés ou injoignables)

Étapes pour ajouter un nouvel équipement à superviser :

Clique sur "Équipements" (tu y es déjà).

État général :

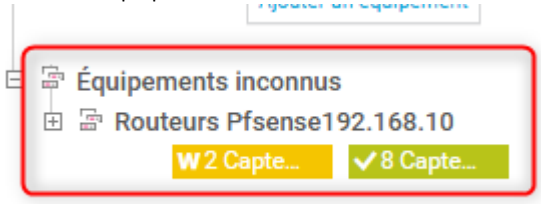
Sonde locale (poste sur lequel PRTG est installé) → capteurs OK mais quelques alertes jaunes (= avertissements).
DNS/ADS SRV-AD (192.168.10.30) : Supervision active (Ping, DNS v2, HTTP...).
Passerelle (192.168.10.254) : Suivie avec SSL, DNS, HTTPS.



Équipements détectés :

Internet : Ping et HTTP OK.
Serveurs Windows / Linux / VM : en attente d'ajout.
192.168.10.60 (Linux/Unix) : supervisé par Ping.

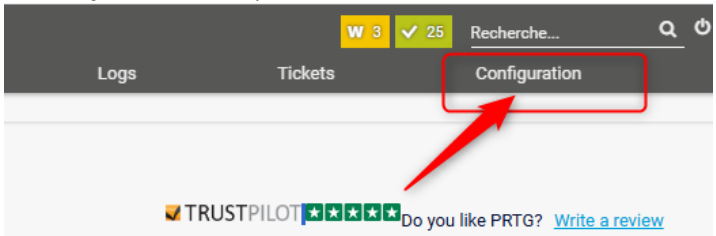
On peut voir que tous mes appareils sont bien remonté y compris les routeur qui sont dans les équipements inconnus



Identification des 2 routeurs en renommant

Configuration des mails remontant

Dans cette partie nous allons configurer les remonter d'alerte et tester avec un compte utilisateur pour voir si ça communique bien



Cliquer sur configuration

Les options possibles dans cette onglets :

. Gérer les utilisateurs et rôles
- Ajouter ou modifier des comptes utilisateurs.
- Attribuer des rôles (Simple user, Read-only, Admin...).

2. Modifier les notifications
- Définir des alertes email, SMS, ou autres (quand un capteur est en erreur, par exemple).

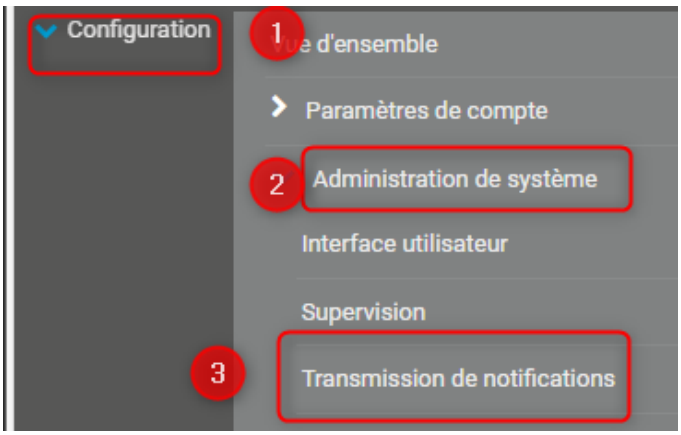
3. Configurer les sondes
- Gérer les sondes locales ou distantes.
- Ajouter une nouvelle sonde distante si tu surveilles plusieurs sites.

4. Définir des modèles de capteurs
- Pour appliquer rapidement un ensemble de capteurs prédéfinis sur plusieurs équipements.

5. Paramètres système
- Modifier l'adresse IP d'écoute, le port Web, les langues, etc.

1. Gérer les utilisateurs et rôles
- Ajouter ou modifier des comptes utilisateurs.
- Attribuer des rôles (Simple user, Read-only, Admin...).

2. Modifier les notifications
- Définir des alertes email, SMS, ou autres (quand un capteur est en erreur, par exemple).



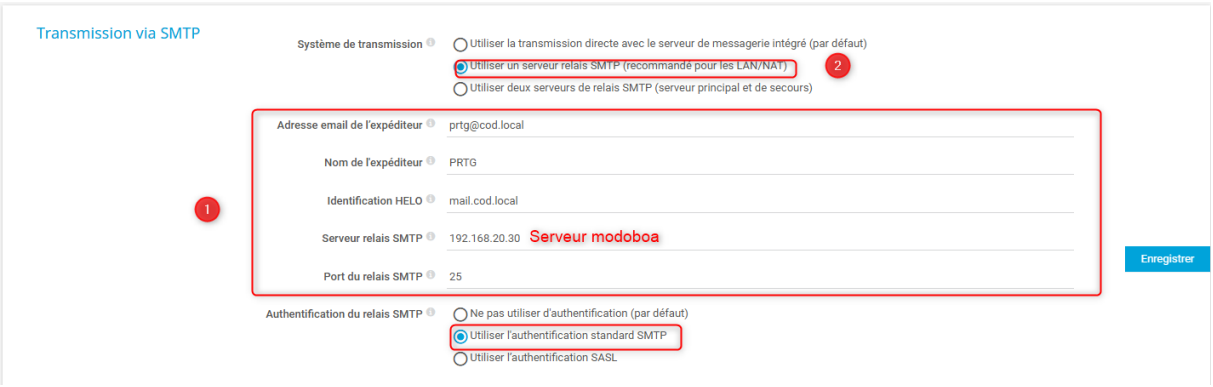
3. Configurer les sondes
- Gérer les sondes locales ou distantes.
- Ajouter une nouvelle sonde distante si tu surveilles plusieurs sites.

4. Définir des modèles de capteurs
- Pour appliquer rapidement un ensemble de capteurs prédéfinis sur plusieurs équipements.

5. Paramètres système
- Modifier l'adresse IP d'écoute, le port Web, les langues, etc.

Configuration de l'envoi de mails via SMTP dans PRT

Système de



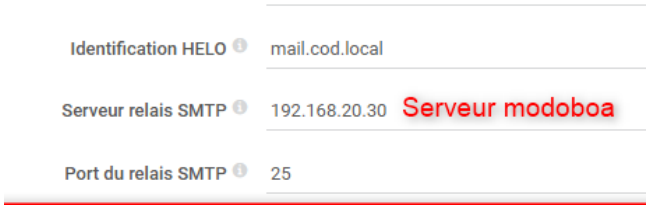
transmission :
Utiliser un serveur relais SMTP (recommandé pour les LAN/NAT)
Détails de la configuration SMTP :

- Adresse email de l'expéditeur : prtg@cod.local
- Nom de l'expéditeur : PRTG
- Identification HELO : mail.cod.local
- Serveur relais SMTP : 192.168.20.30 *(adresse IP de Modoboa)*
- Port du relais SMTP : 25

Authentification SMTP : *Utiliser l'authentification standard SMTP*

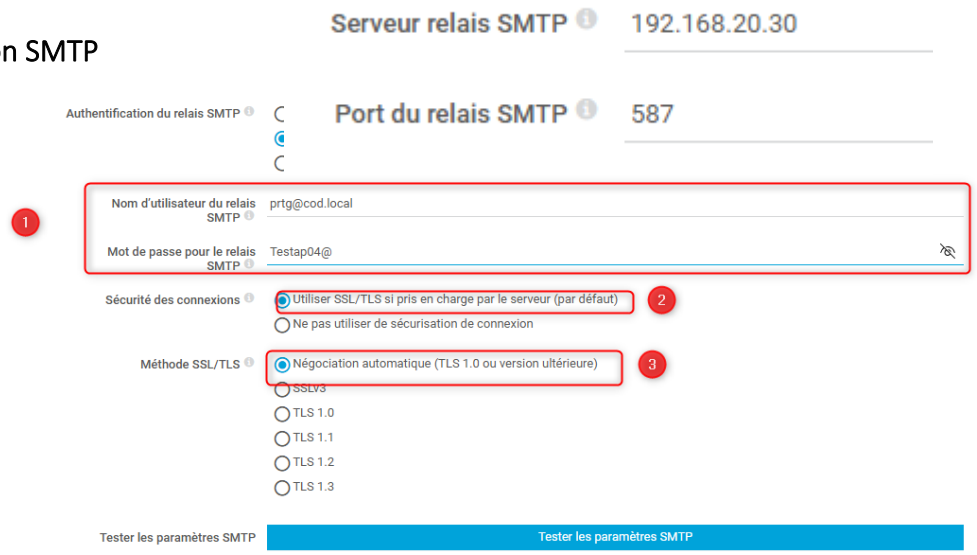
Incident résolut

Attention : Par défaut, le **port SMTP 25** est utilisé dans la configuration de l'envoi de mails via le serveur relais (ici **Modoboa** : 192.168.20.30).
Cependant, **ce port est souvent bloqué ou filtré** par les fournisseurs ou les pare-feux, ce qui peut empêcher l'envoi ou la réception des messages.



Il est donc recommandé de remplacer le port 25 par le port 587, qui est le port standard pour l'envoi de mails avec authentification SMTP sécurisée (STARTTLS).

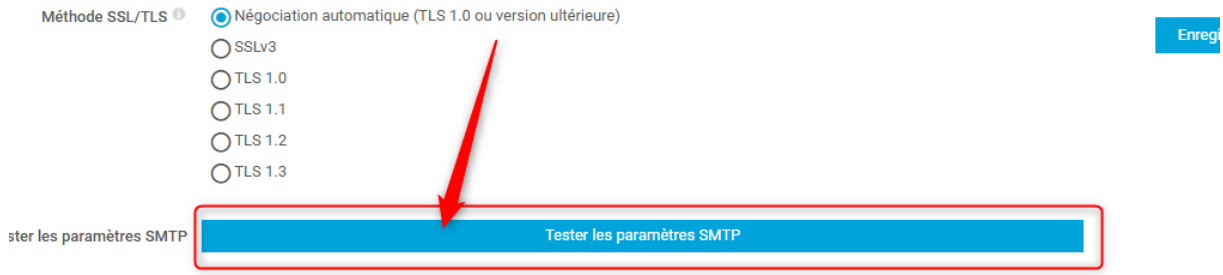
Paramètres d'authentification SMTP



1. Authentification du relais SMTP :
    - *Utiliser l'authentification standard SMTP*
2. Identifiants SMTP :
    - Nom d'utilisateur : prtg@cod.local
    - Mot de passe : Testap04@
3. Sécurité des connexions :
    - *Utiliser SSL/TLS si pris en charge par le serveur (par défaut)*
4. Méthode SSL/TLS :
    - *Négociation automatique (TLS 1.0 ou version ultérieure)*

Test envois

Tester les paramètres SMTP

Cela va 

permettre à PRTG de vérifier si la connexion au **serveur Modoboa (192.168.20.30)** fonctionne correctement en utilisant :

- l'adresse d'expéditeur prtg@cod.local
- le mot de passe Testap04@
- la méthode d'authentification standard SMTP
- la négociation TLS automatique sur le port 25

Si tout est correct :
Tu devrais voir un message de confirmation indiquant que **le test SMTP a réussi**.
Si le test échoue :
Tu recevras une erreur du type "authentication failed" ou "unable to connect to SMTP server", auquel cas il faudra :

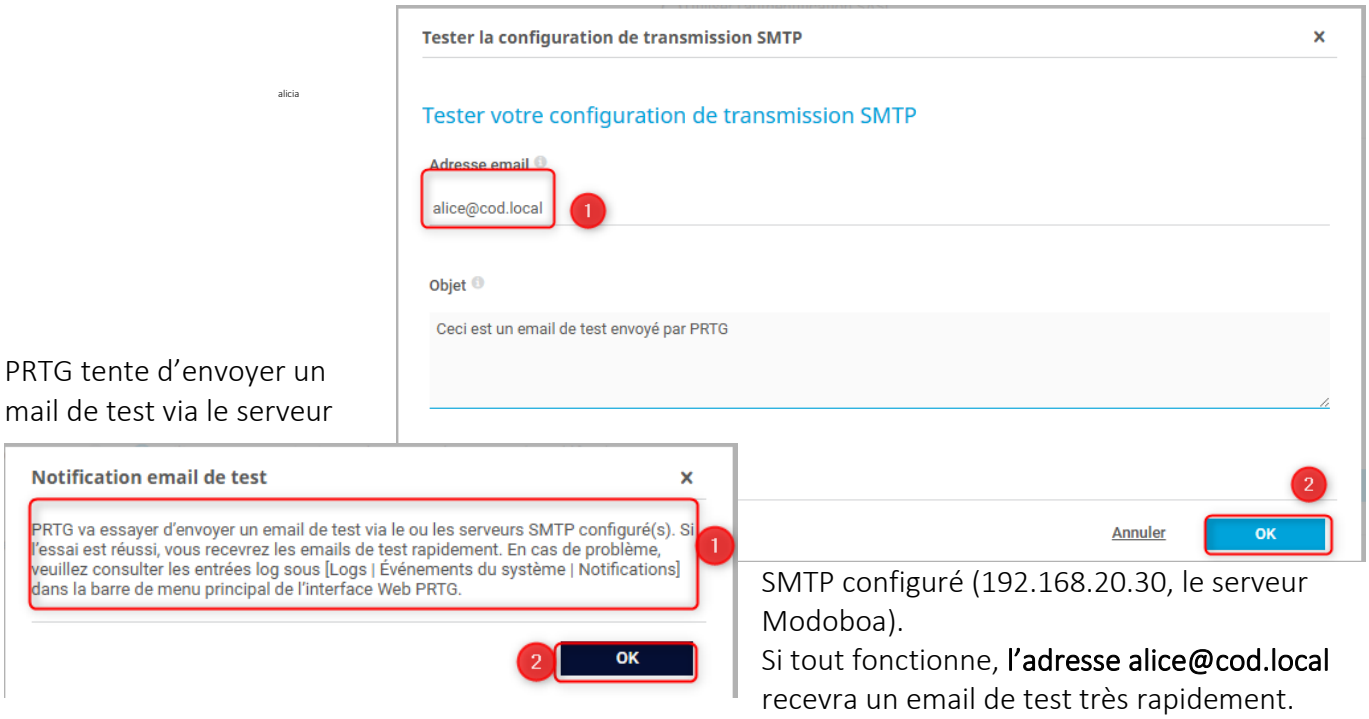
- vérifier l'ouverture du **port 25** sur le pare-feu du serveur Modoboa
- vérifier que l'utilisateur prtg@cod.local existe bien dans Modoboa avec le bon mot de passe
- activer l'authentification SMTP sur Modoboa si ce n'est pas déjà le cas

Détail du test :

- **Adresse email de destination** : alice@cod.local
- **Objet** : *Ceci est un email de test envoyé par PRTG*
- L'expéditeur configuré dans les paramètres SMTP est prtg@cod.local

En cliquant sur **"OK"**, PRTG va tenter d'envoyer ce mail via le serveur Modoboa (192.168.20.30).

PRTG tente d'envoyer un mail de test via le serveur SMTP configuré (192.168.20.30, le serveur Modoboa).



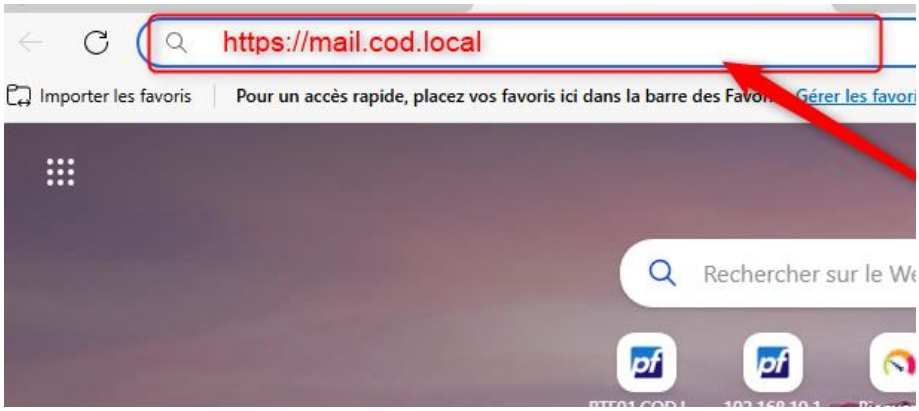
Si tout fonctionne, **l'adresse alice@cod.local** recevra un email de test très rapidement.

En cas d'échec, il faudra consulter :

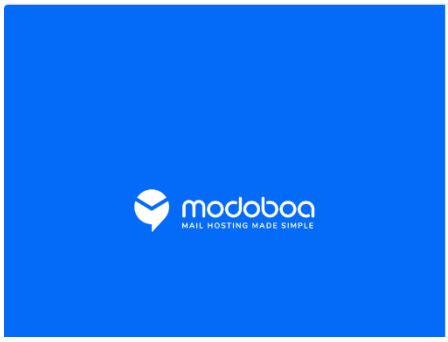
- **PRTG** : Logs > Événements du système > Notifications
- **Modoboa (Postfix)** : /var/log/mail.log

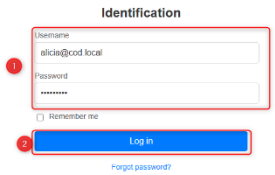
Vérification depuis l'interface WEB Modoboa

Ouvrer Modoboa via l'URL https://mail.cod.local : c'est bien ce qu'il faut faire pour accéder à la messagerie web et vérifier si le mail de test envoyé depuis PRTG a bien été reçu.



Nous sommes sur le point de te connecter à l'interface **Modoboa** avec l'utilisateur alicia@cod.local.

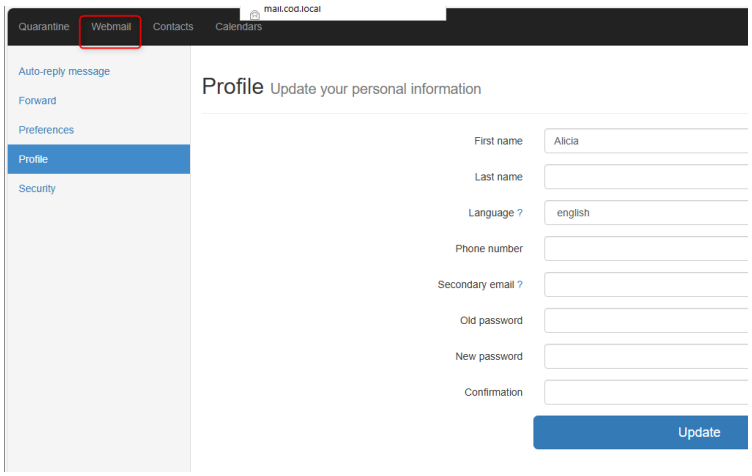




(1) alicia@cod.local
(2) Testap04@

Nous sommes dans les paramètres de profil de l'utilisateur Alicia dans l'interface Modoboa. Nous pouvons faire :

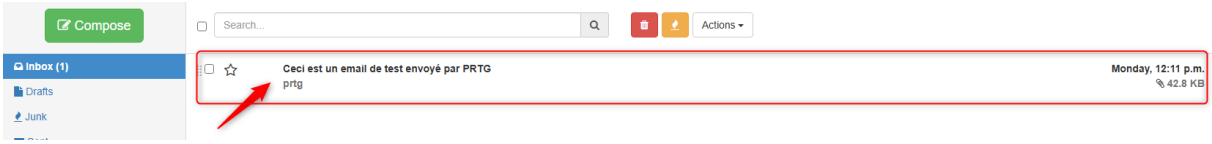
- mettre à jour le nom affiché.
- Language : tu peux passer l'interface en français si besoin.
- Phone number / Secondary email : facultatif mais utile pour les notifications ou récupérations.



Cliquer sur Webmail pour accéder à la boite mail

L'email de test **"Ceci est un email de test envoyé par PRTG"** est bien arrivé dans la

boîte de réception de alicia@cod.local, ce qui confirme que :
Le relais SMTP via Modoboa fonctionne
PRTG est correctement configuré pour envoyer des notifications
La boîte mail reçoit bien les alertes



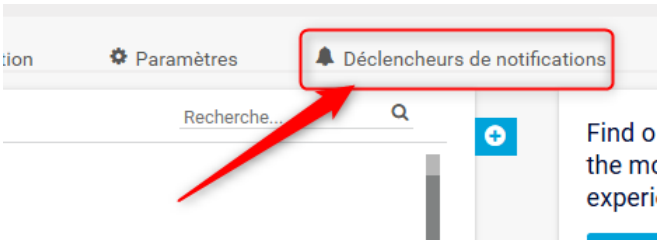
Configuration capteur alerte

Pour créer une alerte personnalisée dans **PRTG Network Monitor**, commencez par accéder à l'équipement sur lequel vous souhaitez appliquer une alerte.

Aller dans le menu latéral gauche.

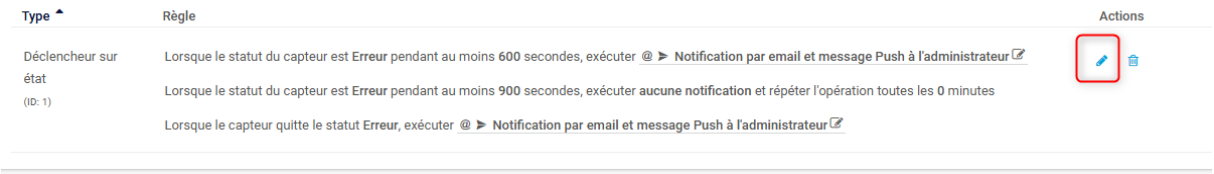
1. Cliquer sur **Équipements** (1).
2. Puis sélectionner **Tous** (2) pour afficher l'ensemble des équipements surveillés.

Nous sommes dans l'onglet **Déclencheurs de notifications**, ce qui signifie que tu vas pouvoir **créer ou modifier une règle d'alerte** dans PRTG.



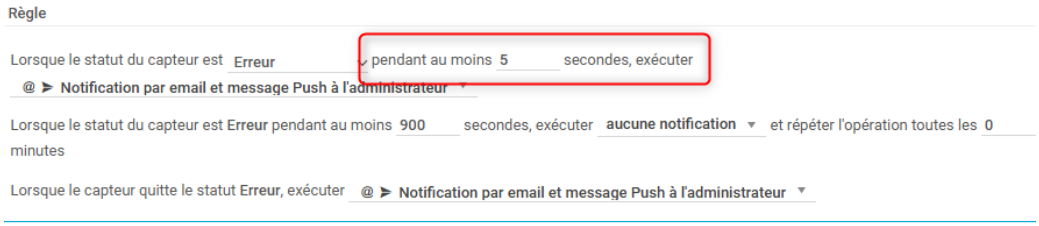
Pour configurer une alerte sur un capteur spécifique :
Sélectionner un **capteur** (par exemple Ping, CPU Load, etc.).
Cliquer sur l'onglet **Déclencheurs de notifications**, situé en haut à droite de la fenêtre.
Cet onglet permet de définir les **conditions qui déclencheront une notification** : par exemple, si un capteur passe en état d'erreur ou reste en panne pendant un certain temps.

Nous sommes sur l'écran de gestion des **déclencheurs de notifications** pour un capteur. Voici comment comprendre et ajuster ce qui s'y trouve :



Lorsque le capteur est en **Erreur pendant 600 secondes** (soit 10 minutes), il **envoie un e-mail et un push** à l'administrateur.
Si l'erreur persiste **pendant 900 secondes supplémentaires**, il **n'effectue plus d'action**.
Dès que le capteur **quitte l'état d'erreur**, il **renvoie une notification** (retour à l'état normal).

Nous avons bien modifié le **déclencheur de notification** pour qu'il se déclenche **après seulement 5 secondes** d'état "Erreur".



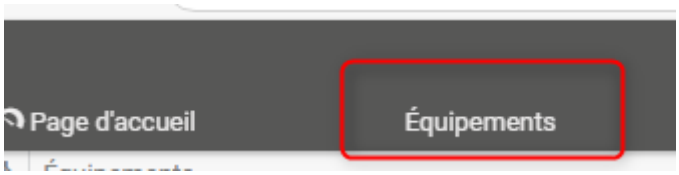
Pourquoi ce réglage est utile ?
Ce type de configuration permet de :

- **Être alerté quasi immédiatement** en cas de panne ou d'incident critique.
- Réagir plus rapidement (ex : intervention manuelle ou redémarrage automatique via script).
- S'assurer que l'équipe d'administration reçoit bien la notification sans attendre.

Application de règle à un appareil spécifique pour le test

Associer le déclencheur de notification à un hôte ou un équipement afin de recevoir des alertes en cas de panne ou comportement anormal.

Accéder à la liste des équipements
Depuis le menu principal, cliquer sur « **Équipements** ».



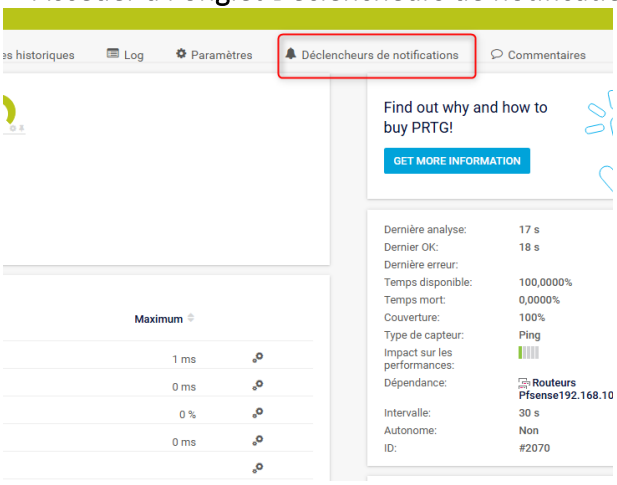
Le capteur **Ping** surveille la disponibilité réseau de l'équipement. En cas d'inaccessibilité (perte de ping), une notification est essentielle pour intervenir rapidement.

1. **Accéder à l'équipement cible**
Dans la section **Équipements inconnus > Routeurs PfSense > 192.168.10.251**, localiser le capteur **Ping**.

Cliquer sur Ping

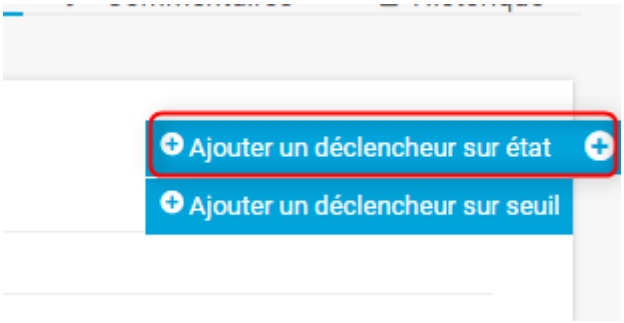
Accéder à l'onglet Déclencheurs de notifications

- Comme indiqué dans la capture, cliquez sur l'icône 🔔 en haut à droite.
- Cet onglet vous permet de définir **comment PRTG doit alerter l'administrateur** en cas de problème.



Parfait, vous êtes sur le point **d'ajouter une notification personnalisée** à ce capteur. Le **règle de** bouton bleu avec le + (en haut à droite de l'encadré) permet d'ajouter un **déclencheur de notification**.

Nous sommes maintenant à l'étape clé de l'ajout du déclencheur.

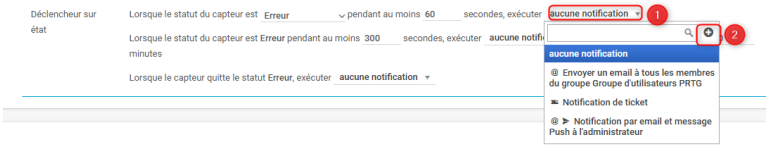


Depuis le capteur ciblé (ex. **Ping** de 192.168.10.251), cliquez sur :

- **Ajouter un déclencheur sur état**

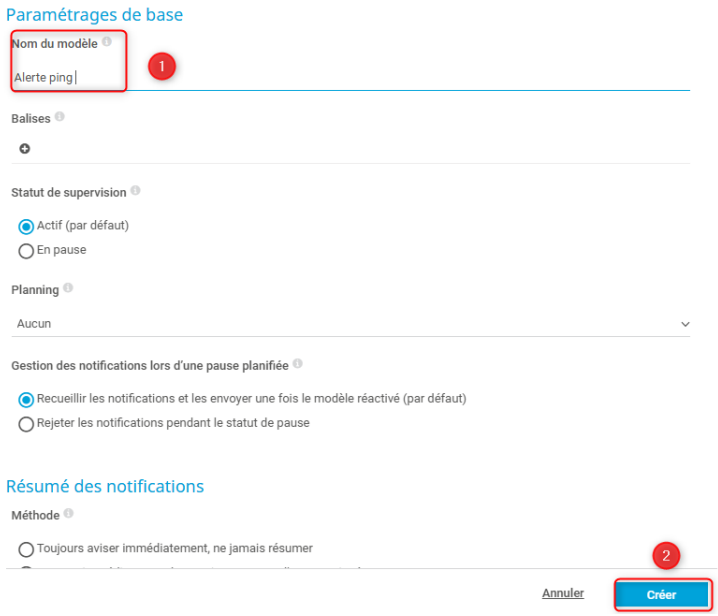
Cela permet de générer une alerte dès que le capteur rencontre un changement d'état (par exemple : Erreur, Avertissement, Inhabituel).
Ce type de déclencheur est idéal pour la supervision **en temps réel** de la disponibilité réseau.

Nous sommes en train d'appliquer la règle de notification à votre capteur sélectionné. Voici comment résumer cette étape dans un ton professionnel pour votre documentation :
Accéder à l'onglet **Déclencheurs de notifications** depuis le capteur ciblé.
Cliquer sur **Ajouter un déclencheur sur état**.



Création d'un modèle de notification – Alerte Ping

Pour une meilleure gestion des alertes, nous créons un modèle dédié aux incidents détectés par le capteur Ping.



Nom du modèle : Entrer un nom explicite, par exemple Alerte ping (voir image point 1).
Laisser le **Statut de supervision** sur Actif (par défaut), sauf si le modèle ne doit pas être actif immédiatement.
Dans la section **Gestion des notifications lors d'une pause planifiée**, conserver l'option : Recueillir les notifications et les envoyer une fois le modèle réactivé pour ne rien perdre des événements.

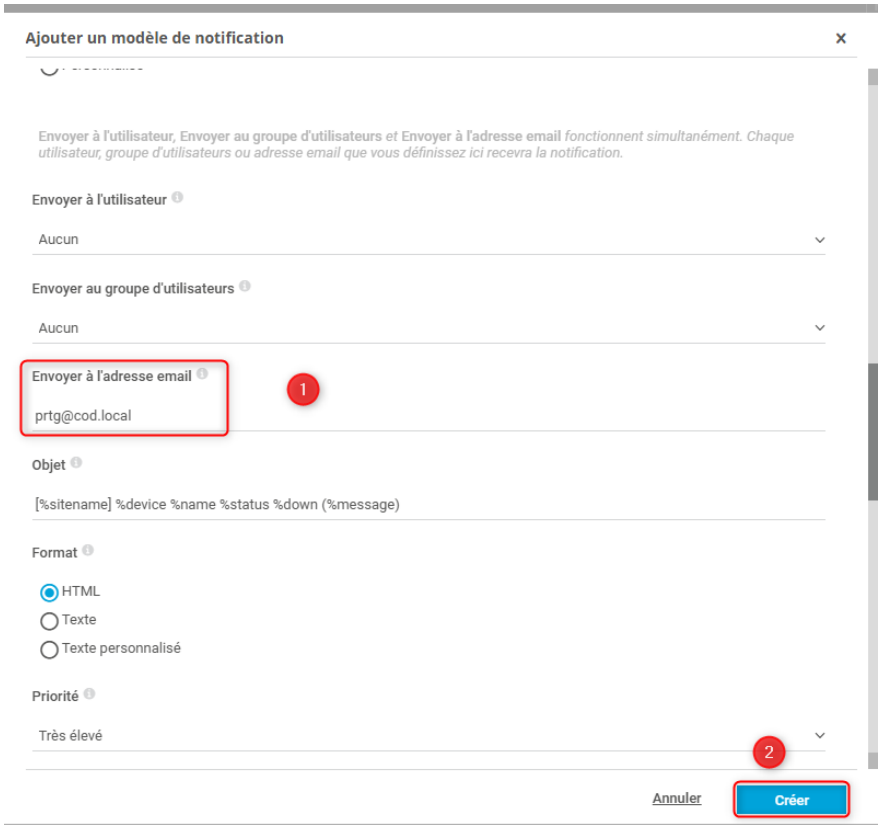
Activation de l'envoi de notifications par email

Pour que le modèle *Alerte ping* envoie un message en cas de déclenchement, il faut **activer explicitement** l'option d'envoi par email :

Étapes :

1. **Activer l'option "Envoyer un email"** en cliquant sur le bouton à bascule (voir l'encadré rouge sur l'image ci-dessus).

Ce modèle a pour but d'envoyer une notification par email lorsqu'un capteur de type **Ping** entre dans l'état "Erreur" ou retrouve un état "OK". Il permet d'être alerté rapidement en cas d'indisponibilité réseau.



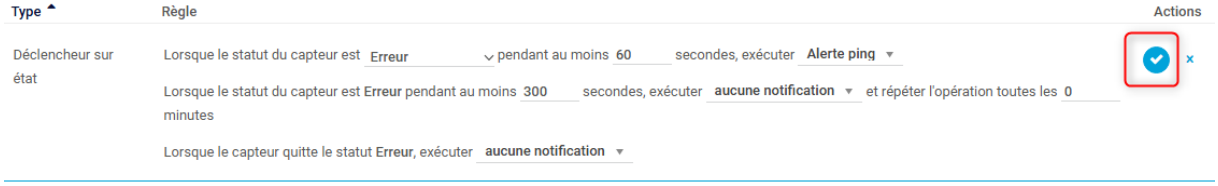
Paramètre	Valeur
Nom du modèle	Alerte ping
Type de notification	Email
Adresse de destination	prtg@cod.local
Objet de l'email	[%sitename] %device %name %status %down (%message)
Format	HTML
Priorité	Très élevé
Destinataires PRTG	Aucun utilisateur / Aucun groupe

Une fois le **modèle de notification "Alerte ping"** créé, nous l'avons appliqué à un **capteur de type Ping** sur l'équipement 192.168.10.251.

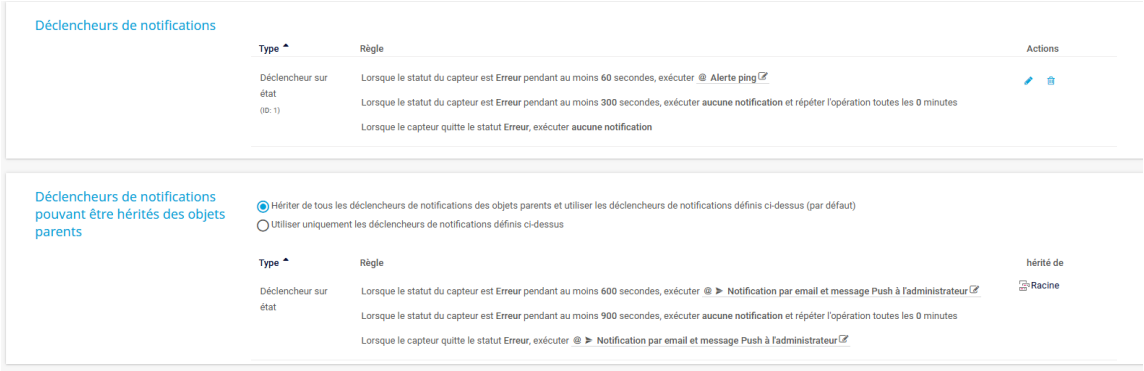
Déclencheur configuré :

- **Type** : Déclencheur sur état
- **Condition** : Lorsque le capteur est en **Erreur** pendant **60 secondes**
- **Action** : Exécuter la notification **Alerte ping**
- **Répétition** : Pas de répétition automatique
- **Fin d'erreur** : Aucune notification à la sortie de l'état Erreur

Cette configuration garantit une réactivité rapide en cas d'interruption réseau détectée par le capteur.

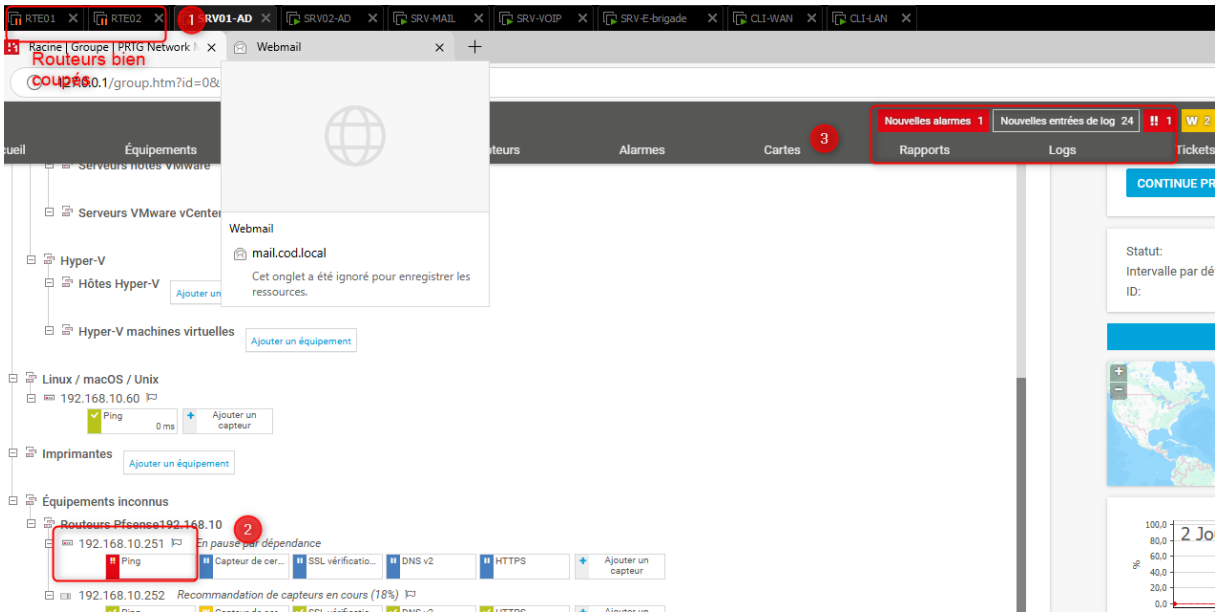


Une fois que l'utilisateur à cliquer sur le bouton bleu cela va enregistrer la règle



Conclusion – Test de déclenchement d'alerte

Ce scénario constitue un **test volontaire** visant à vérifier que le système de surveillance PRTG est capable de détecter une **perte de connectivité** et de **déclencher automatiquement une alerte** via les mécanismes configurés.



- Simuler une coupure réseau en désactivant volontairement les routeurs RTE01 et RTE02.
- Observer la réaction de PRTG en termes de détection, pause des capteurs dépendants et génération d'alertes.
- Vérifier la réception des notifications (email) pour confirmer l'efficacité du modèle de notification configuré précédemment.

Résultats obtenus :

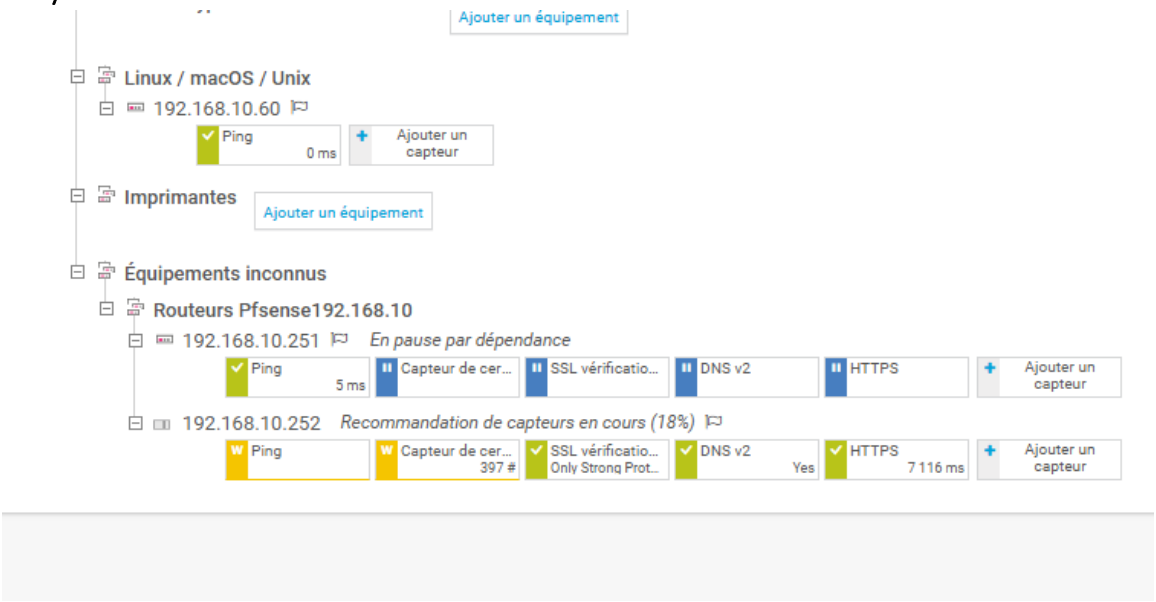
- Les équipements liés aux routeurs ont bien été **mis en pause automatiquement**.
- Le capteur de type **Ping** a basculé en état "en pause par dépendance", ce qui montre que les règles de hiérarchie et de dépendance sont bien fonctionnelles.
- Des **logs et une alarme** ont bien été générés.
- Le test démontre que la configuration actuelle est **opérationnelle et réactive** face à un incident de type "perte de connexion".

Ce test valide le bon fonctionnement de l'infrastructure de supervision ainsi que des notifications critiques.

Comportement observé après réactivation des routeurs

Après la remise en ligne des routeurs **RTE01** et **RTE02**, les capteurs associés dans PRTG sont passés brièvement en **état clignotant** (alternance entre actif et pause). Ce comportement est **normal et attendu** dans le cadre d'un test avec **délai de déclenchement configuré**.

Analyse :



- L'état "clignotant" reflète une **période d'instabilité momentanée** où le système tente de confirmer le retour à la normale.

- Cette phase de transition est influencée par les **valeurs de délais** définies dans les déclencheurs (ex. : 60 secondes avant exécution de la notification, ou 300 secondes pour l'arrêt).
- Dans ce cas précis, la **latence de confirmation** combinée à l'état antérieur en erreur a pu ralentir la réactivation complète des capteurs dépendants.

Action corrective :

Face à cette instabilité temporaire, un **redémarrage manuel des routeurs** a été effectué. Ce redémarrage a permis de **stabiliser la connectivité réseau**, entraînant le **retour à l'état "OK"** pour tous les capteurs associés.