



SÉCURITÉ CIVILE

AP4

RAPPORT DE CLÔTURE DU PROJET

LIVRABLE 2

GROUPE 7
HUBER Alexis
BOLIDUM Théo

Durée du projet : Début / fin

Date limite de remise : Samedi 15 Avril 2023

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

SOMMAIRE

Date limite de remise : Samedi 15 Avril 2023	1
1) RESUME DU PROJET	3
1.1) Définitions des rôles et responsabilités.....	3
1.2) Rappel des objectifs fixés	3
2) CONDUITE DU PROJET	4
2.1) Planning prévisionnel VS Planning réel	4
2.2) Ressources prévues VS Ressources utilisées	5
2.3) Problèmes rencontrés et solutions apportées ou envisagées	5
3) RESULTATS	5
3.1) Résultats attendus VS Résultats obtenus.....	5
4) ANALYSE FINALE	5
4.1) Analyse et état finale du projet.....	5
4.2) Améliorations possibles.....	5
5) CONCLUSION	5
6) DOCUMENTATION TECHNIQUE	6
6.1.1)Mise en place d'un active directory redondé	6
6.1.2) Configuration de base	19
6.1.4) ADDS (Active Directory et DNS).....	27
6.1.5) Rejoindre le domaine avec le second serveur.....	34
6.2.1 Mise en place des serveurs PfSense	38
6.2.4) Mise en place de CARP/PFSYNC	53
6.2.4. Installer et configurer un VPN distant (OpenVPN).....	58
Mise en place des règles pour la DMZ.....	72
7.1.1) E-Brigade	77
Configuration de MariaDB.....	78
Installation de E-brigade	80
8.1.1) Installation d'asterisk.....	84
8.1.2) Crédation des utilisateurs :	87
8.1.3) Crédation des boîtes vocales	88
8.1.4) Utilisation d'un softphone.....	89
9.1.1) installation de Hmailserver.....	92

1) RESUME DU PROJET

1.1) Définitions des rôles et responsabilités

- HUBER Alexis : Technicien 1
- BOLIDUM Théo : Technicien 2

Le technicien 1 s'occupe de la documentation technique, du schéma réseau ainsi que de l'ensembles des solutions dont la société à besoin.

Le technicien 2 s'occupe du devis, du planning prévisionnel et réel, ainsi que de l'ensemble des solutions dont la société à besoin.

Nous avons pris la décision de chacun faire toute la partie technique et de travailler ensemble pour fournir le livrable.

1.2) Rappel des objectifs fixés

La sécurité sociale nous engage pour parvenir à leurs besoins. La nécessité de la sécurité sociale est d'avoir un service en haute disponibilités. Il est arrivé à de multiples reprises que la sécurité sociale n'avait plus accès à la téléphonie ou à internet. De plus il peut y avoir un réseau mobile saturé.

Ils ont le devoir d'être entièrement autonome et de garantir l'accès aux données et la maîtrise de leur infrastructure. C'est la raison pour laquelle tous les services seront installés au sein de la sécurité sociale.

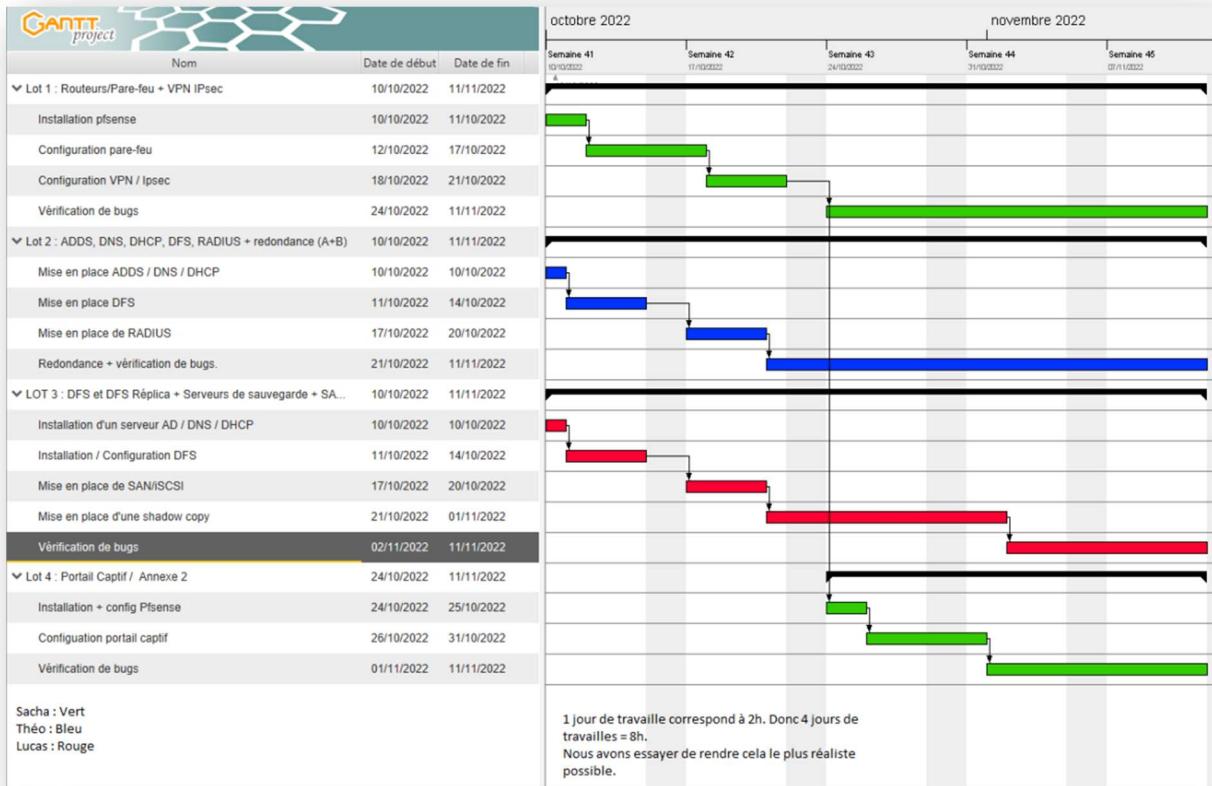
- Mise en œuvre d'une haute disponibilité de routeurs et liaison internet redondée
- Mise en œuvre de 2 serveurs Active Directory
- Mise en œuvre d'un serveur de téléphonie IpBx et déploiement d'un client de messagerie
- Mise en œuvre d'un serveur de supervision et de monitoring
- Mise en œuvre d'une solution de VPN RW
- Mise en œuvre d'une DMZ pour accéder au serveur WEB E-Brigade

2) CONDUITE DU PROJET

2.1) Planning prévisionnel VS Planning réel

Pour le planning, nous nous sommes basés sur l'application GANTT Project.
Tout d'abord, voici notre GANTT prévisionnel

Voici le planning prévisionnel



Voici le planning réel

2.2) Ressources prévues VS Ressources utilisées

Revenez sur les moyens humains, financiers, organisationnels, techniques, etc. dédiés à la conduite de ce projet. Faites le bilan de ce qui a réellement été consommé. Enrichissez le constat à l'aide de commentaires expliquant les écarts.

2.3) Problèmes rencontrés et solutions apportées ou envisagées

3) RESULTATS

3.1) Résultats attendus VS Résultats obtenus

Associez les résultats et commentez les écarts négatifs comme positifs : pourquoi tel objectif n'a pas été atteint ? Ou au contraire : quelles sont les raisons qui expliquent un tel succès ?

En gestion de projet, le meilleur moyen de progresser, c'est d'apprendre de ses erreurs plutôt que de les nier.

4) ANALYSE FINALE

4.1) Analyse et état finale du projet

Evaluer la satisfaction du client ; analyser le résultat final.

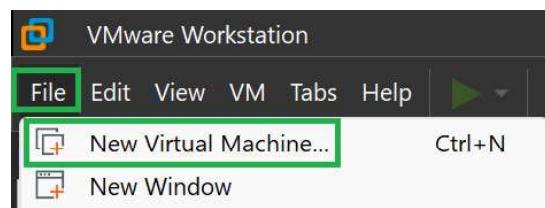
4.2) Améliorations possibles

5) CONCLUSION

6) DOCUMENTATION TECHNIQUE

6.1.1) Mise en place d'un active directory redondé

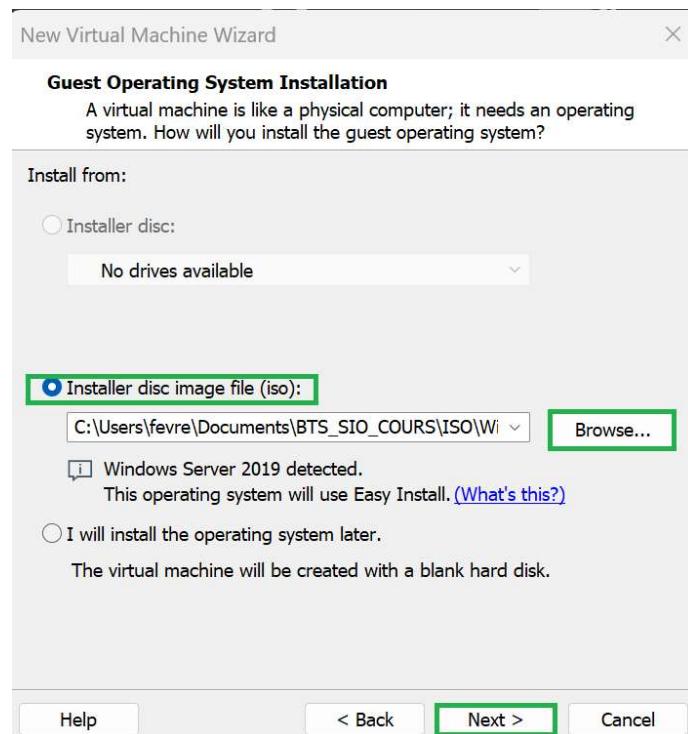
Pour ce projet, nous allons créer une nouvelle machine virtuelle en cliquant sur File -> New Virtual Machine :



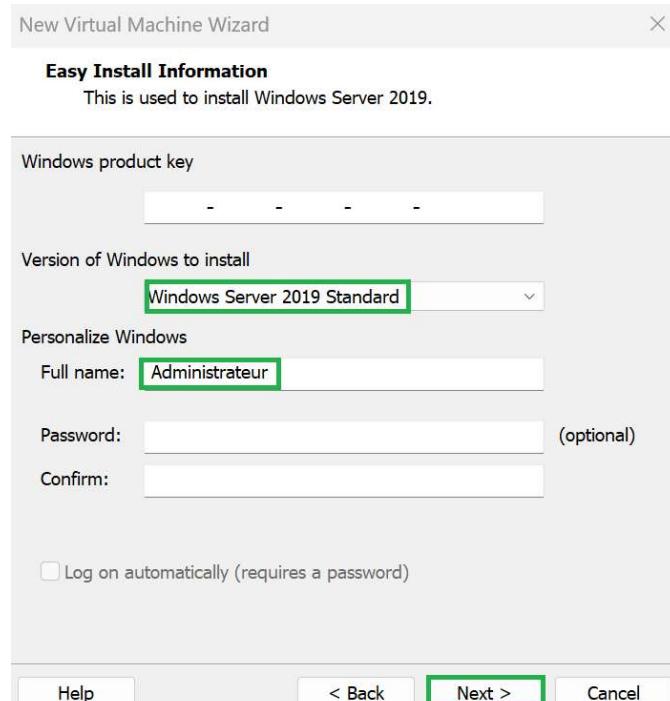
Choisir « Custom » :



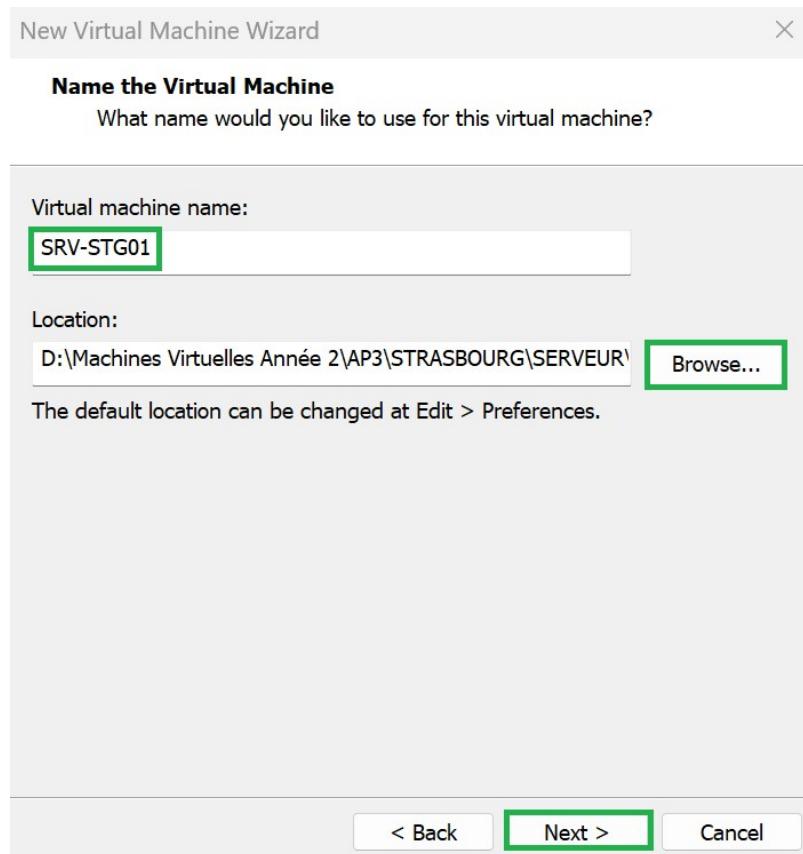
Cliquez ensuite sur **Next**, puis cochez « Installer disc image file (iso) » et cliquez sur **Browse** pour sélectionner le bon fichier iso puis cliquez sur **Next** :



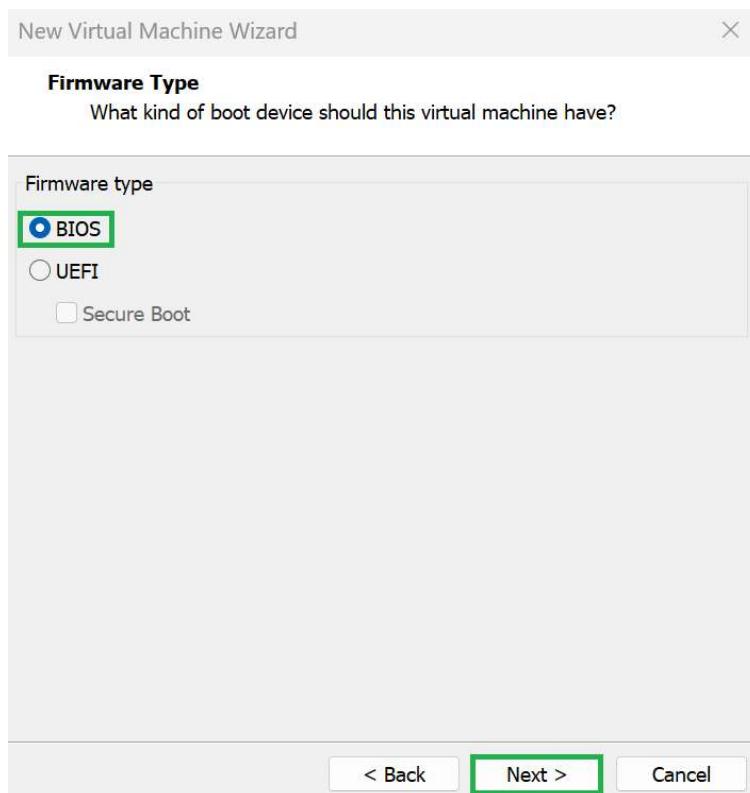
Choisir la version « **Standard** », renseignez un compte pour ouvrir une session au démarrage de la vm (Pour se logger automatiquement, il suffit de cocher « Log on auto » et de renseigner un mot de passe) Nous n'allons pas le faire ici et nous définirons le mot de passe plus tard. Cliquez sur **Next** :



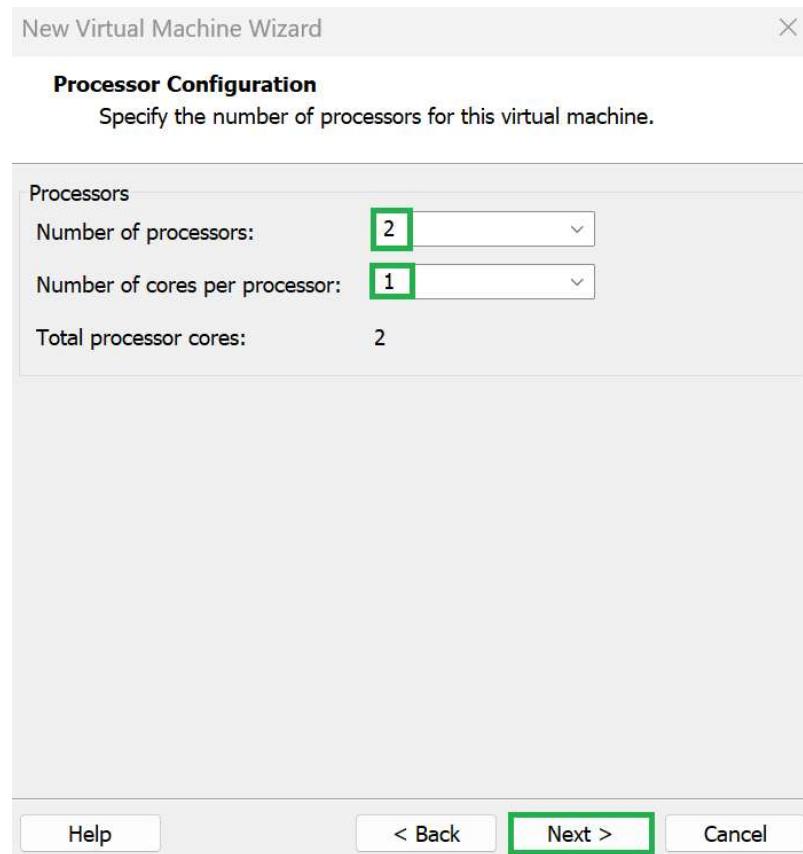
Renseignez le nom de la machine virtuelle puis choisir la localisation avec **Browse** puis cliquez sur **Next** :



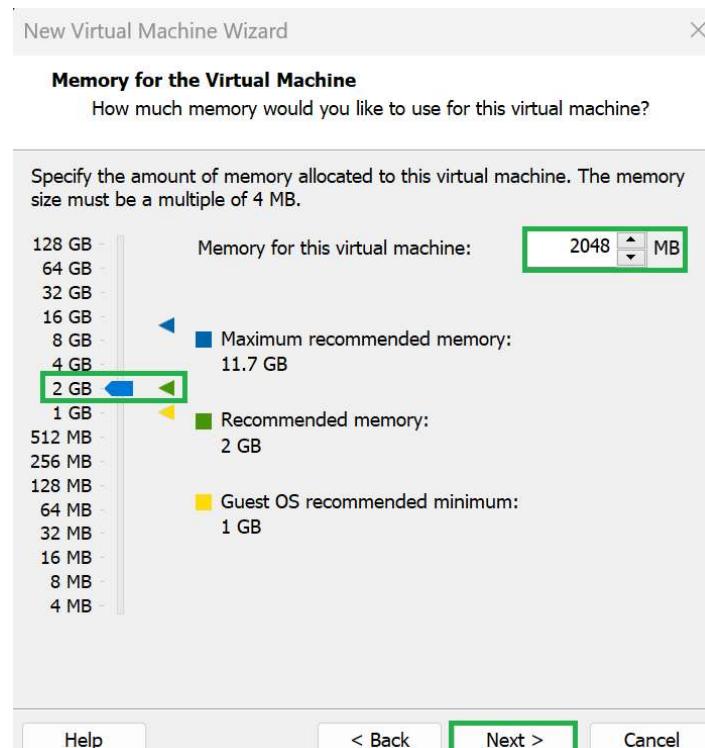
Choisir « Bios » puis cliquez sur **Next** :



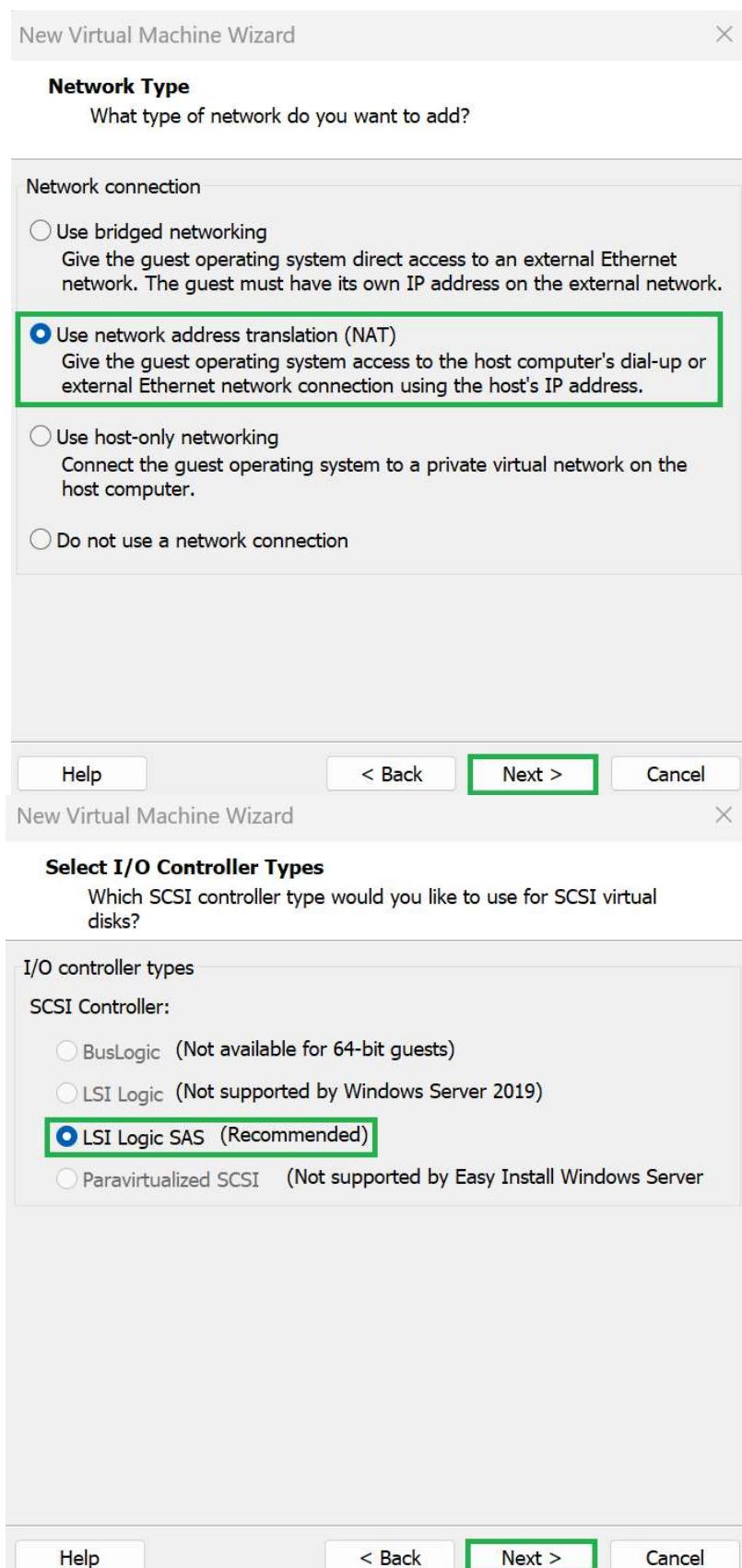
Choisir la configuration suivante :

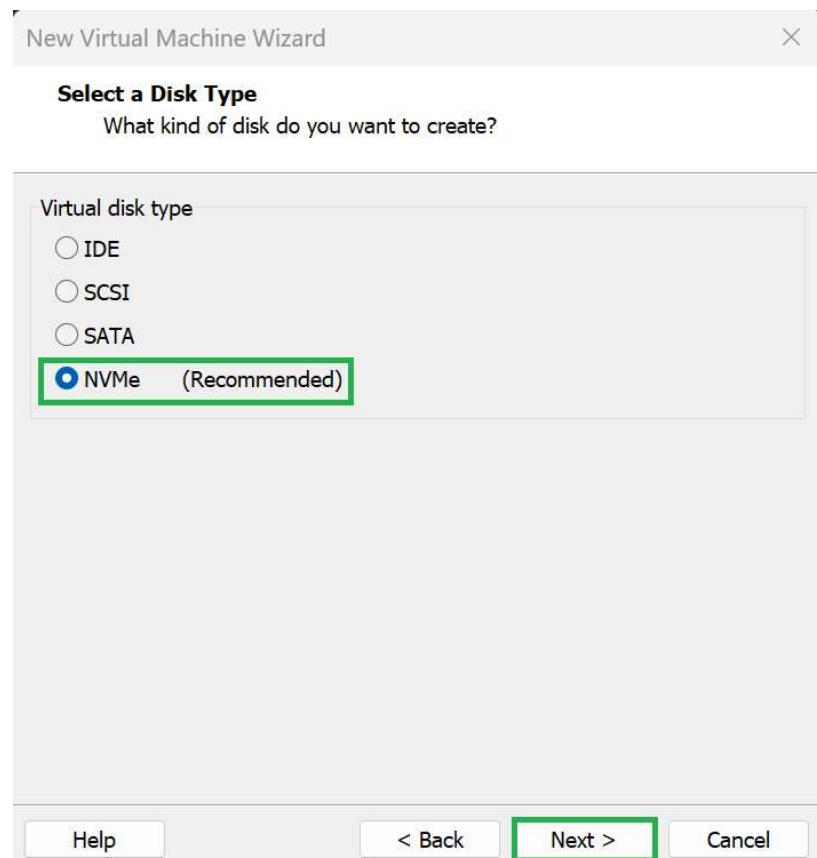


Etant donné que chaque technicien réalise l'ensemble du projet , nous nous tenons à la configuration minimale

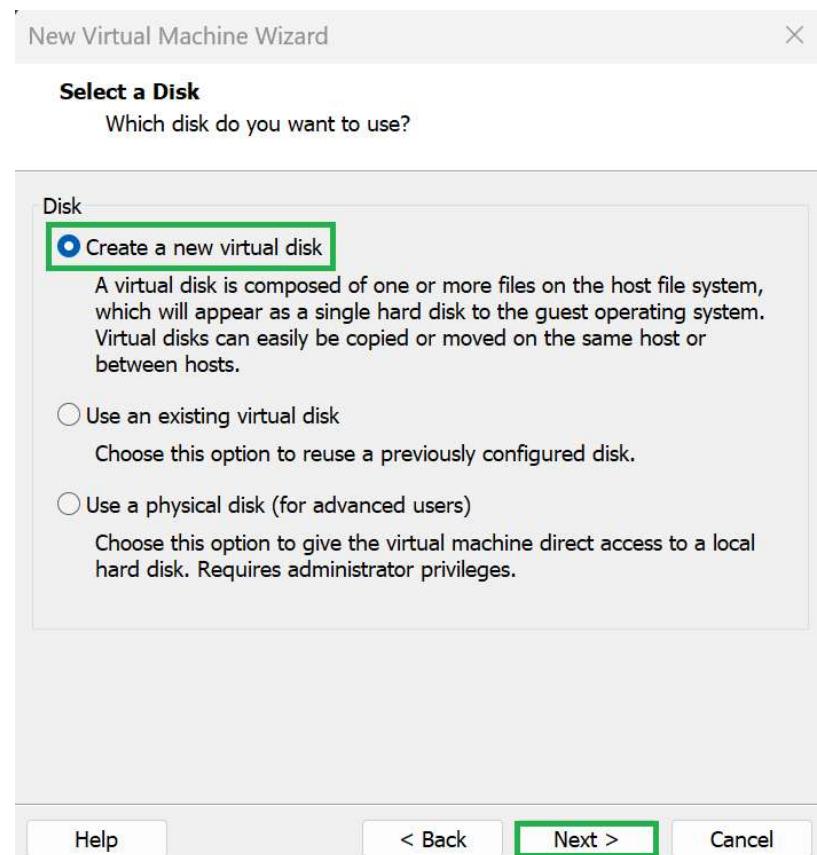


Ensuite :

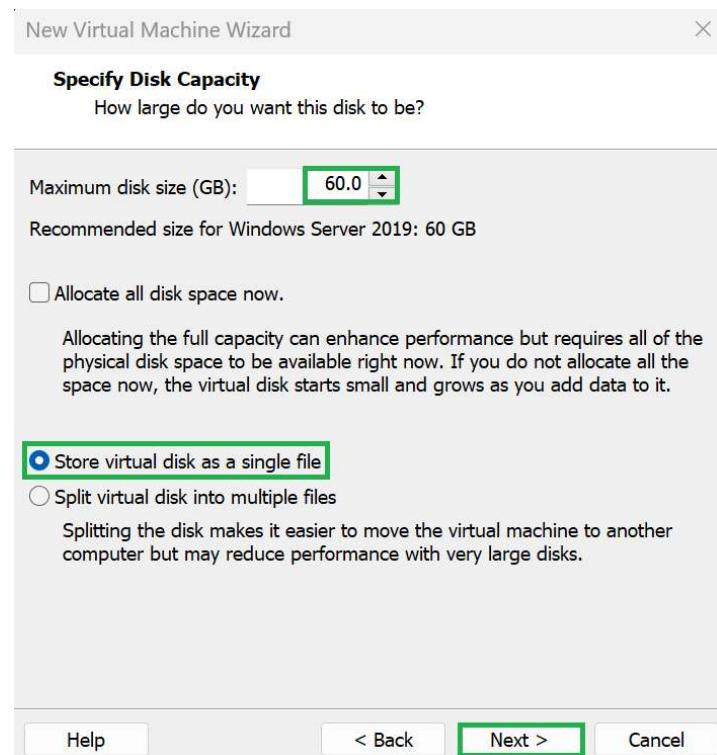




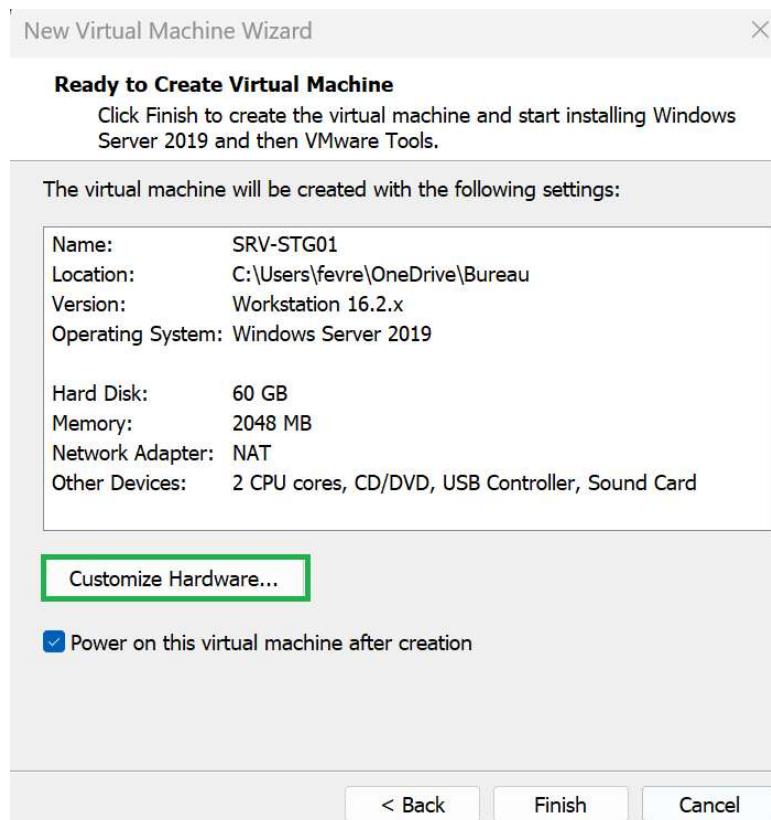
Créer un nouveau disque virtuel et cliquez sur **Next** :



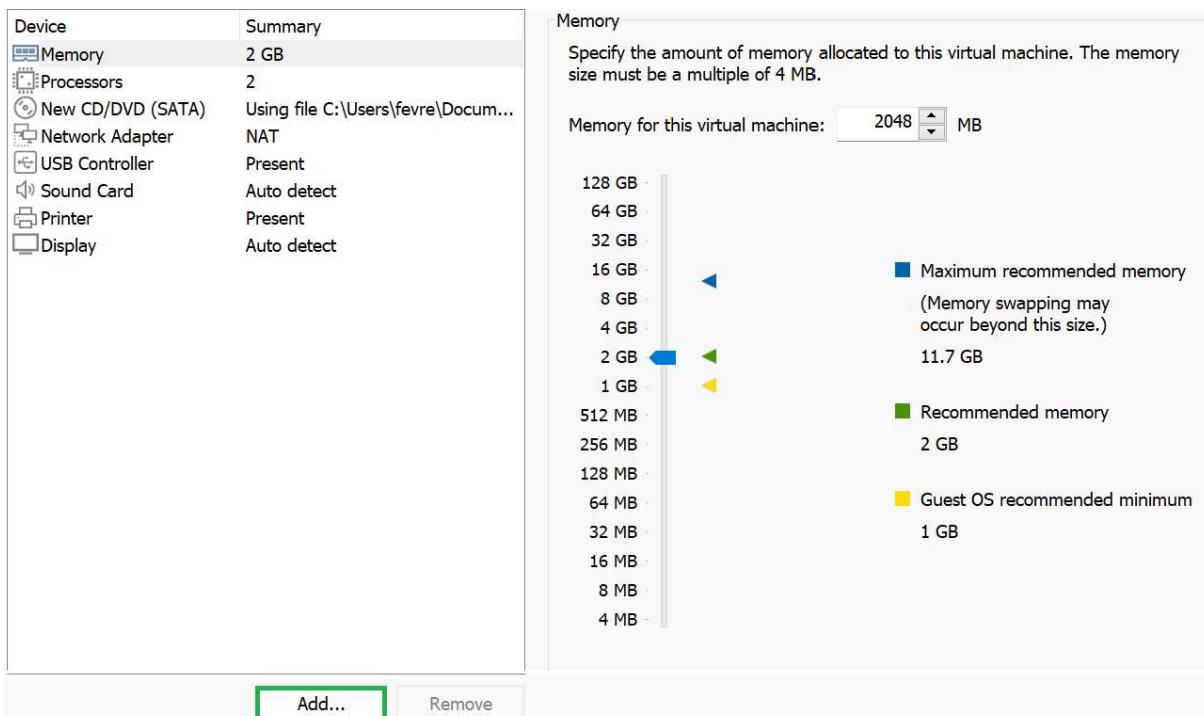
Le disque sera de 60 GB et nous allons choisir la première option et surtout de ne pas l'allouer entièrement pour préserver la place sur le disque dur qui contient la VM puis cliquez sur **Next** :



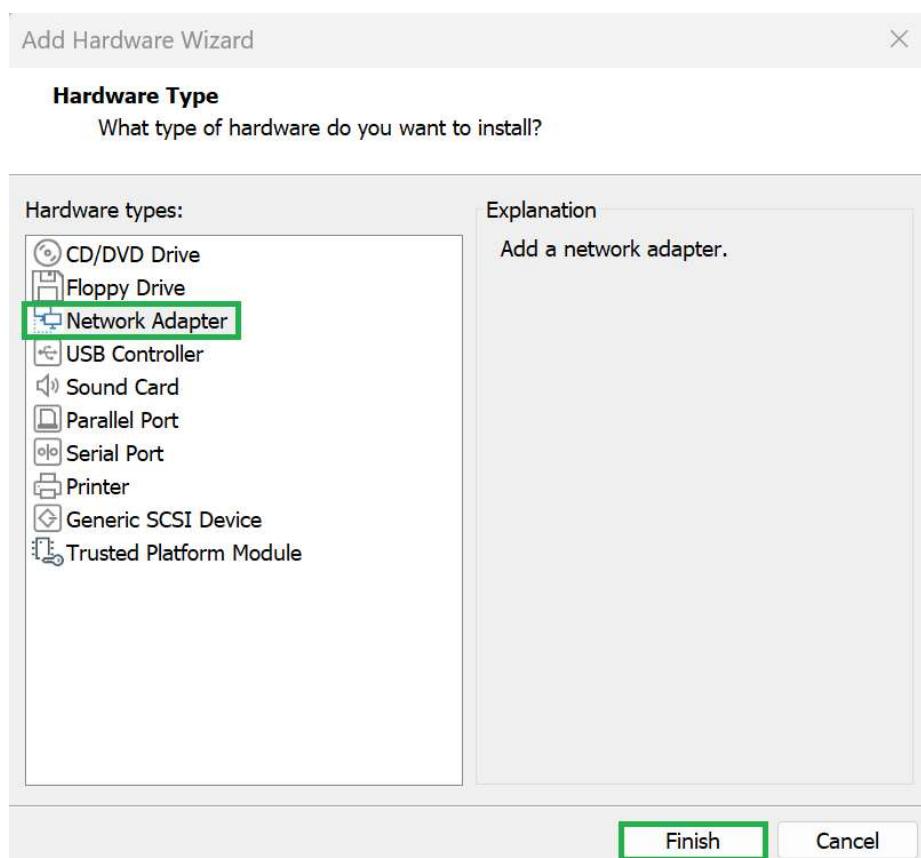
Cliquez sur **Next**, une fenêtre de la sorte se présentera alors à vous. Cliquez sur **Customize Hardware** :



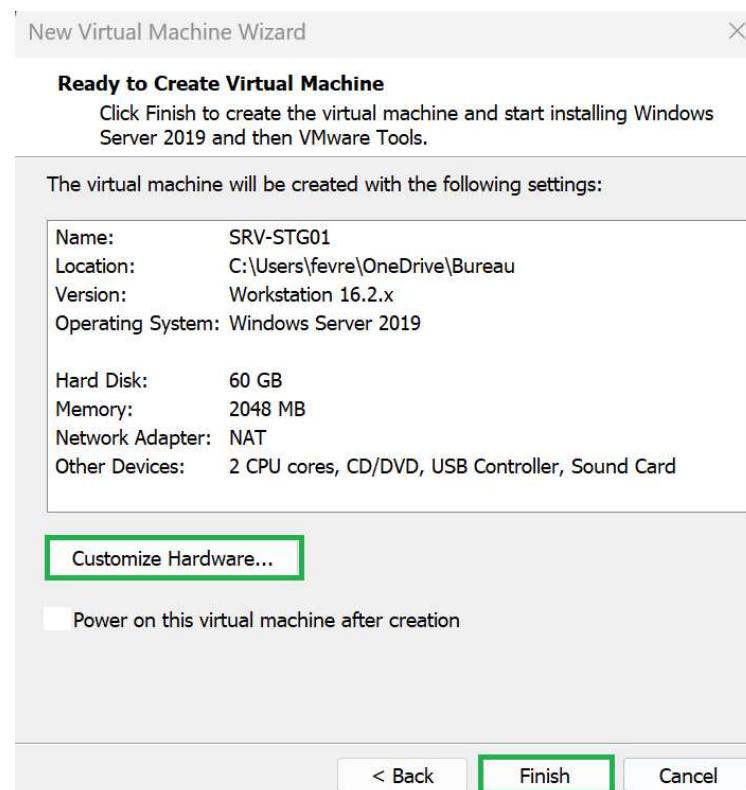
Cliquez sur **Add** :



On va ajouter une deuxième carte réseau, cliquez sur **network Adapter** puis cliquez sur **Next** :



Ensuite cliquez sur ***Finish*** :



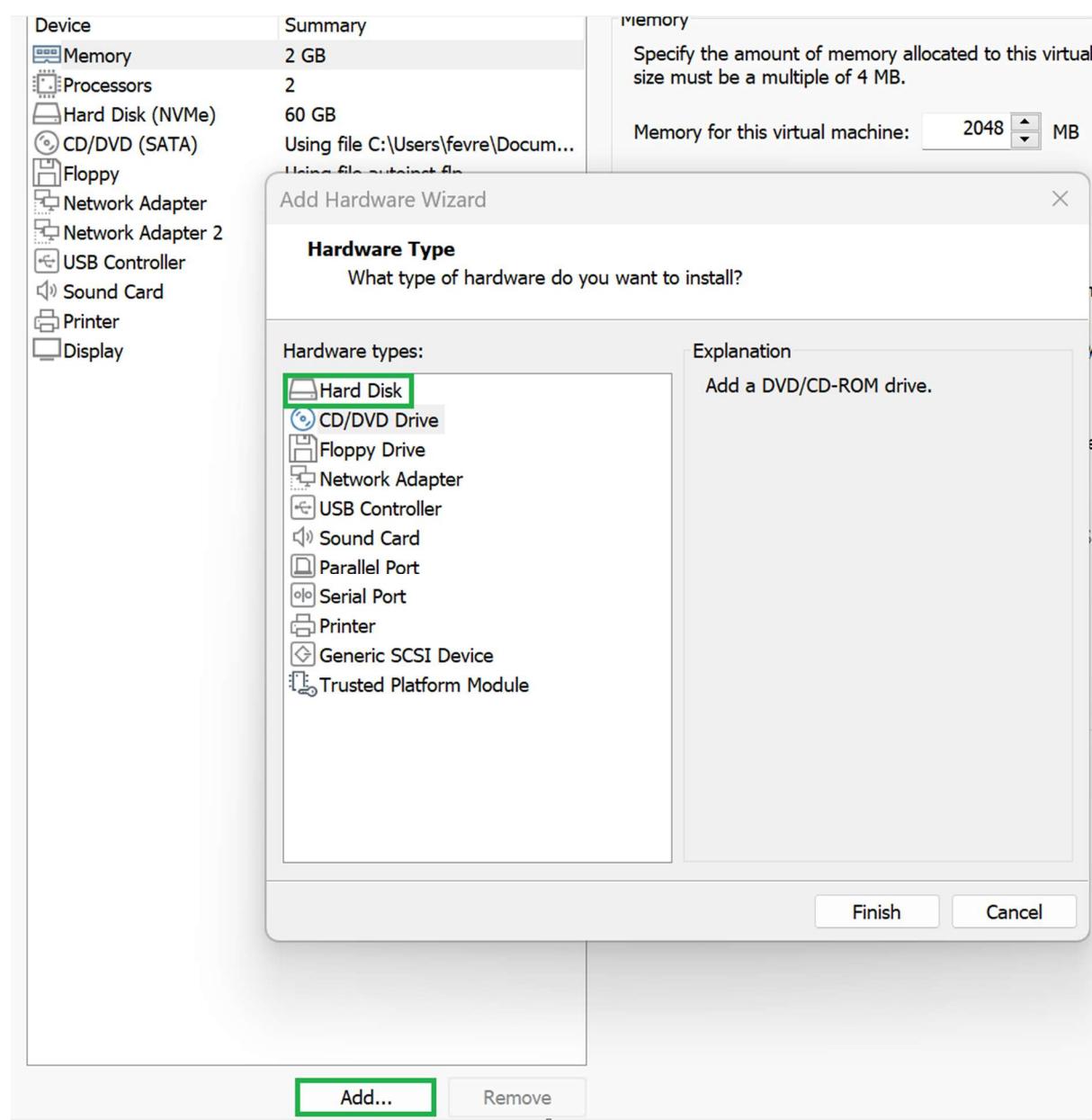
Nous allons maintenant ajouter un deuxième disque comme afin de garantir une haute disponibilité du service.

Pour cela, cliquez sur ***Edit virtual machine settings*** :

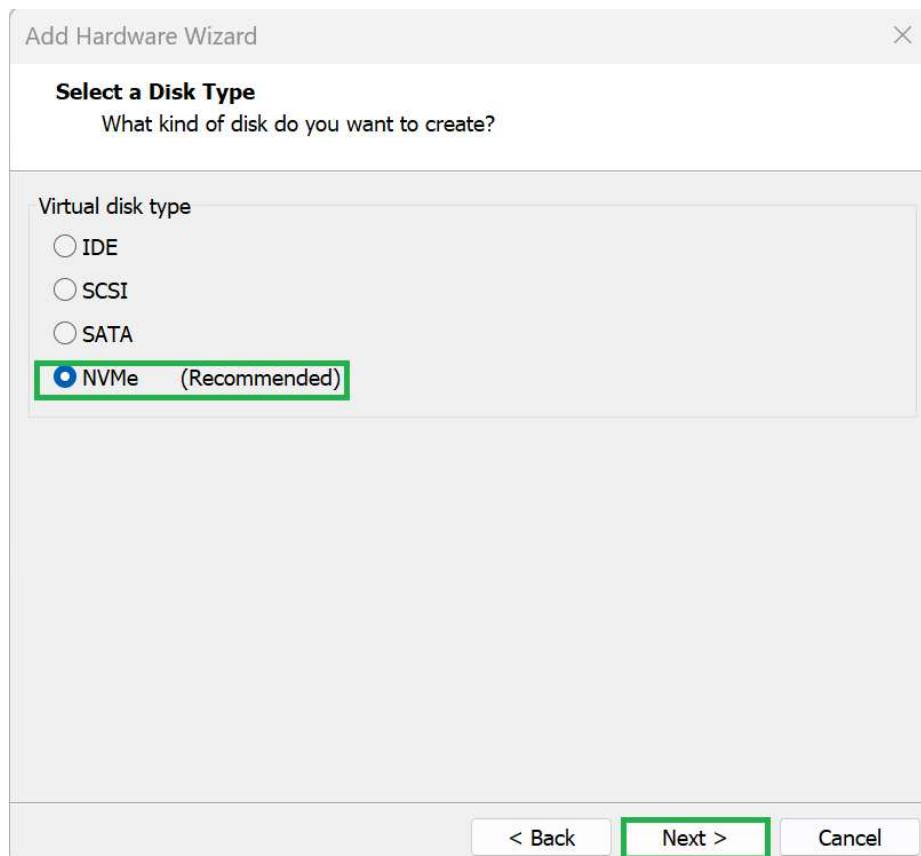
Device	Configuration
Memory	2 GB
Processors	2
Hard Disk (NVMe)	60 GB
Hard Disk 2 (NVMe)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Custom (VMnet1)
Network Adapter 2	Custom (VMnet1)
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Description
Type here to enter a description of this virtual machine.

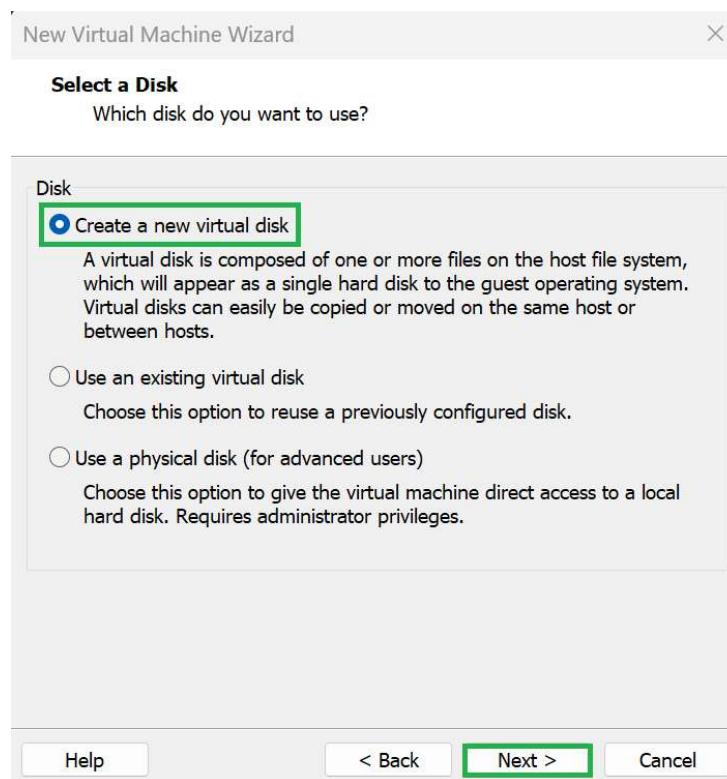
Cliquez sur **Add** puis sur **Hard Disk** :



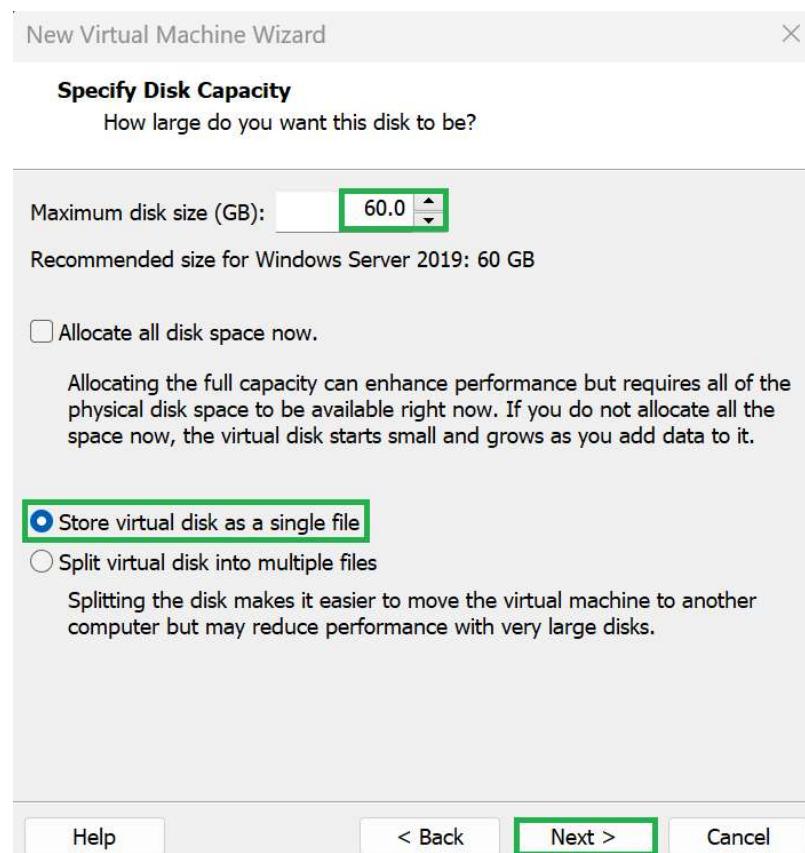
Puis :



Ensuite :



Et comme pour le premier disque :

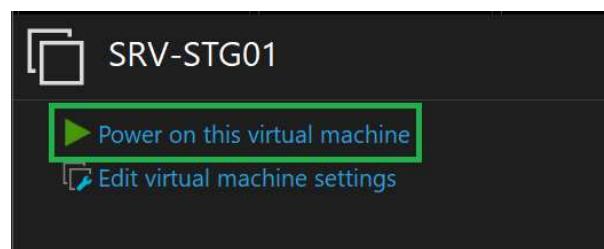


Après validation, nous pouvons voir les deux disques durs ainsi que les deux cartes réseaux qu'on aura mis sur le Vmnet1 en custom :

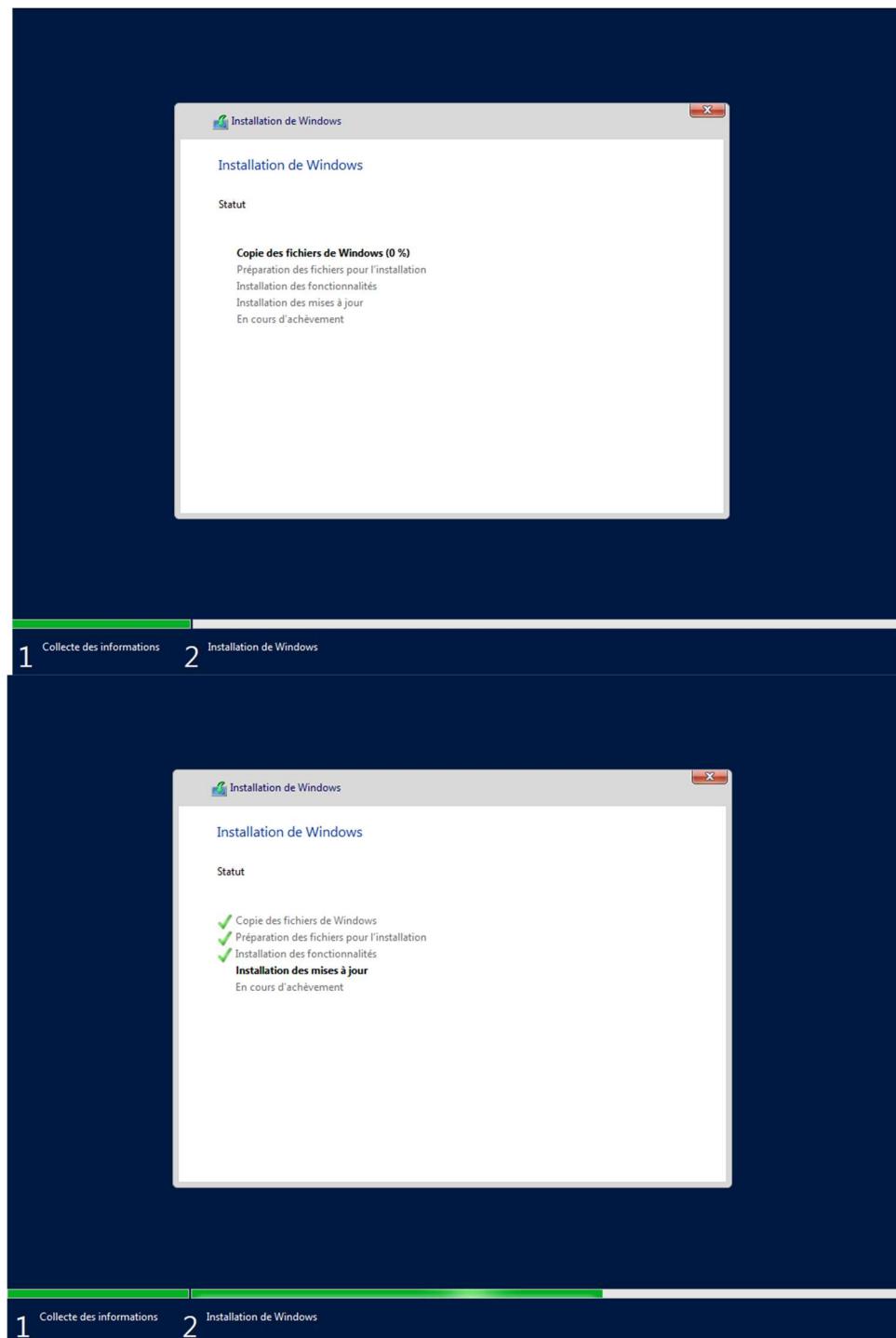
▼ Devices		
	Memory	2 GB
	Processors	2
	Hard Disk (NVMe)	60 GB
	Hard Disk 2 (NVMe)	60 GB
	CD/DVD (SATA)	Auto detect
	Network Adapter	Custom (VMnet1)
	Network Adapter 2	Custom (VMnet1)
	Sound Card	Auto detect
	Printer	Present
	Display	Auto detect

▼ Description		
---------------	--	--

Nous allons maintenant procéder à l'installation. Cliquez sur **Power on this Virtual machine** :

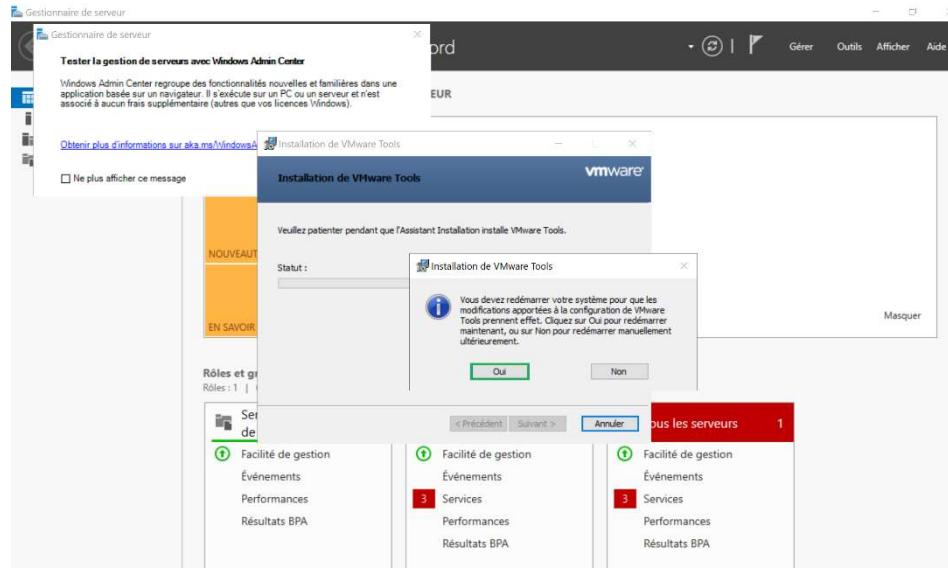


L'installation démarre :

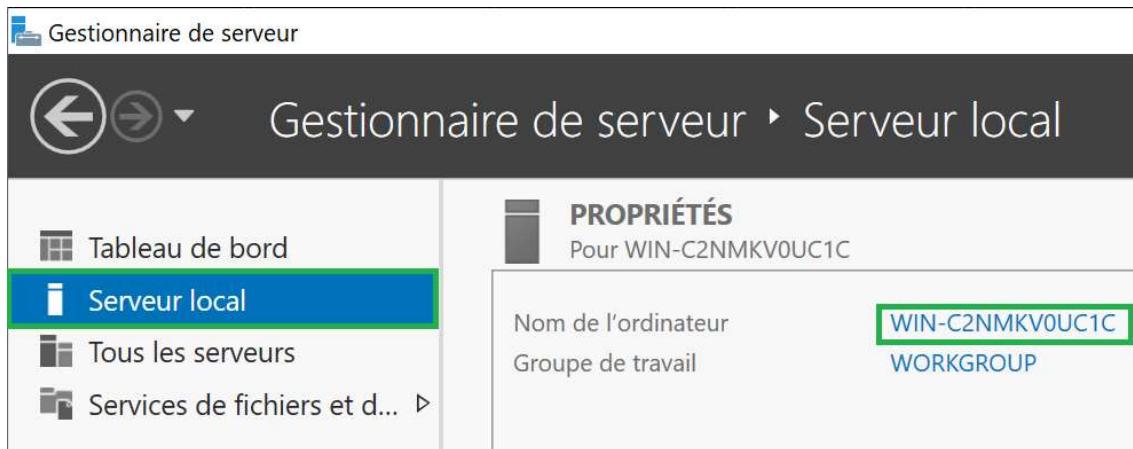


6.1.2 Configuration de base

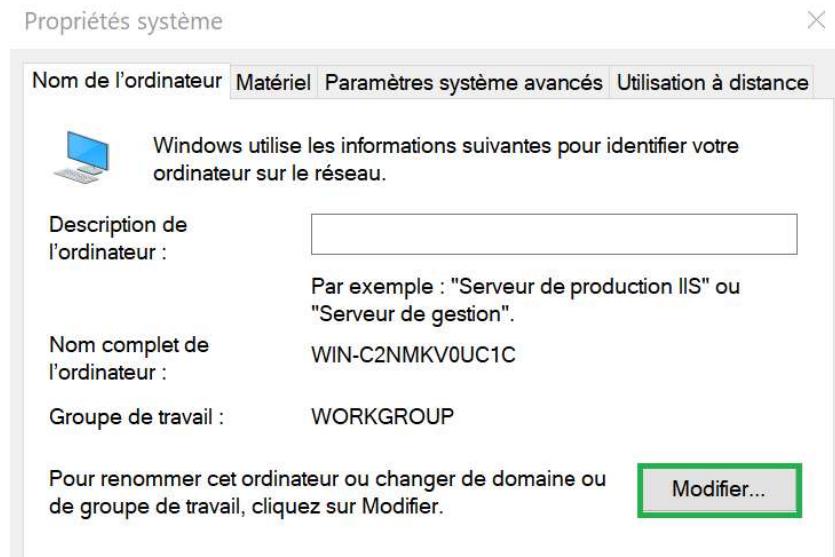
Une fois tout en vert la vm démarre, on arrive ensuite à l'installation des **Vmware Tools**. Cliquez sur oui pour redémarrer la vm et procéder à l'installation :



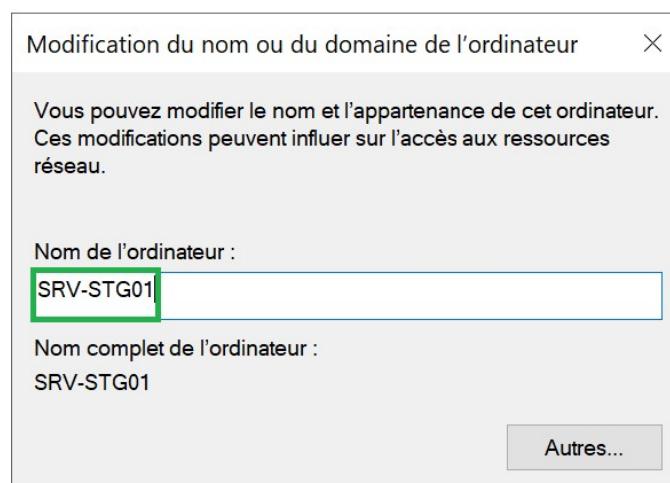
Une fois redémarré, nous allons procéder à la configuration de base de la vm. Tout d'abord, nous allons aller dans le gestionnaire de serveur à l'onglet **Serveur local puis** cliquez sur le nom de l'ordinateur :



Cliquez sur **modifier** :



Assignez le nom puis valider :



La VM devra redémarrer pour prendre en compte la modification :

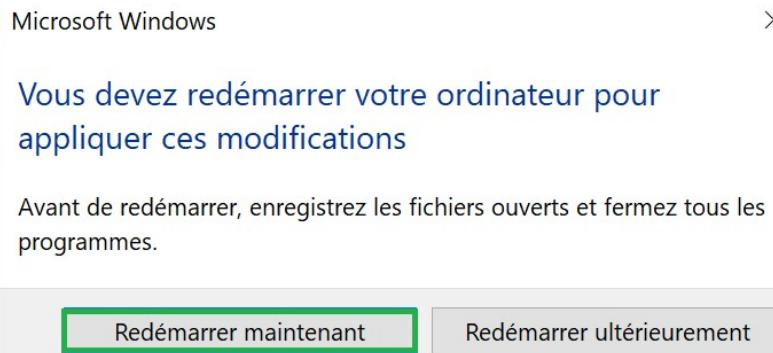
Modification du nom ou du domaine de l'ordinateur



Vous devez redémarrer votre ordinateur pour appliquer ces modifications.

Avant de redémarrer, enregistrez les fichiers ouverts et fermez tous les programmes.

OK



Dans le même onglet qu'avant, on peut voir que le nom à bien été changé. Cette étape doit impérativement se faire avant l'installation de l'AD.



Une fois l'ordinateur redémarré, rendez-vous une fois de plus dans le **Gestionnaire de serveur**, puis dans **Serveur local**, et dans les **Propriétés**. Nous pouvons observer la ligne spécifiant l'état du pare-feu :

Pare-feu Windows Defender Public : Actif

Et un peu plus loin sur cette même ligne :

Antivirus Windows Defender	Protection en temps réel : activée
Configuration de sécurité renforcée d'Internet Explorer Actif	

Commencez par cliquer sur « **Public : Actif** ». Une fenêtre apparaît :

Pare-feu et protection du réseau

Qui et ce qui peut accéder à vos réseaux.

Réseau avec domaine

Le pare-feu est activé.

Réseau privé

Le pare-feu est activé.

Réseau public (actif)

Le pare-feu est activé.

Cliquez sur chaque ligne bleue puis désactivez les pare-feux.

Réseaux avec domaine actifs

Non connecté

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau avec domaine.

Activé

Réseaux avec domaine actifs

Non connecté

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau avec domaine.

Le pare-feu du domaine est désactivé. Votre appareil est peut-être vulnérable.
 Désactivé

Pare-feu privé :

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau privé.

Activé

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau privé.

Le pare-feu privé est désactivé. Votre appareil est peut-être vulnérable.
 Désactivé

Pare-feu public :

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau public.

Activé

Pare-feu Windows Defender

Aide à protéger votre appareil sur un réseau public.

Le pare-feu public est désactivé. Votre appareil est peut-être vulnérable.
 Désactivé

Revenez maintenant dans les propriétés du serveur local, et cliquez sur **Protection en temps réel** :

Protection en temps réel

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.

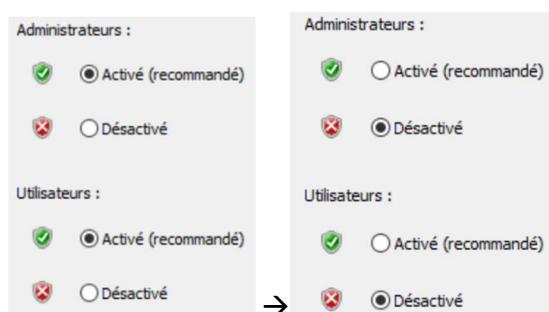
Activé

Protection en temps réel

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.

La protection en temps réel est désactivée, ce qui rend votre appareil vulnérable.
 Désactivé

Pour finir nous allons désactiver la sécurité renforcée d'internet explorer :



6.1.3) Agrégation de carte réseau (IP Bonding)

Comme indiqué dans les spécificités techniques du projet, nous allons procéder à l'IP Bonding. Cela nous permettra une certaine tolérance de panne ainsi qu'une répartition de charges (pour les interfaces réseaux).

Pour réaliser l'agrégation, rendons-nous dans le gestionnaire de serveur, onglet Serveur local. Nous pouvons voir nos deux cartes réseaux :

Ethernet0	Adresse IPv4 attribuée par DHCP, Compatible IPv6
Ethernet1	Adresse IPv4 attribuée par DHCP, Compatible IPv6

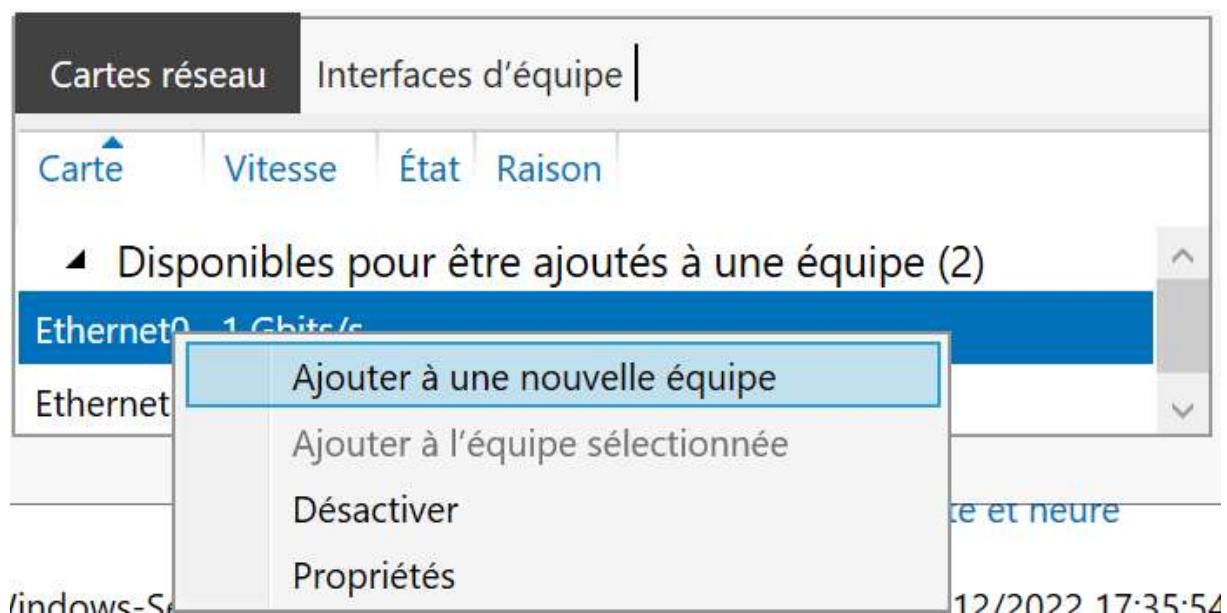
Comme nous l'avons vu plus haut, les deux cartes réseaux sont sur le Vmnet1. Revenez ensuite sur le serveur local dans propriétés et cliquez sur **Désactivé** à droite d'**Association de cartes réseau** :



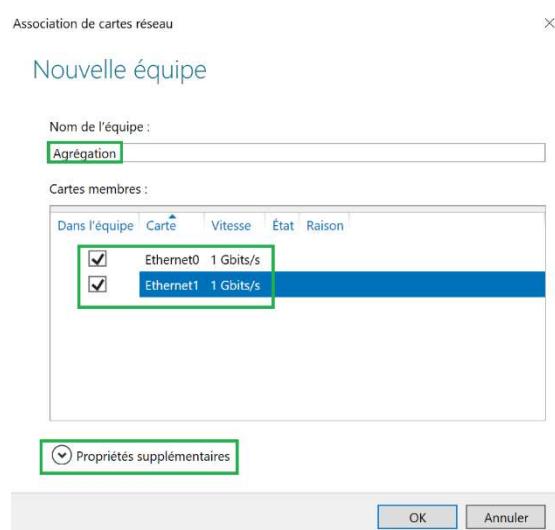
Une fenêtre apparaît :

Carte	Vitesse	État	Raison
Ethernet0	1 Gbits/s	Disponibles pour être ajoutés à une équipe (2)	
Ethernet1	1 Gbits/s		

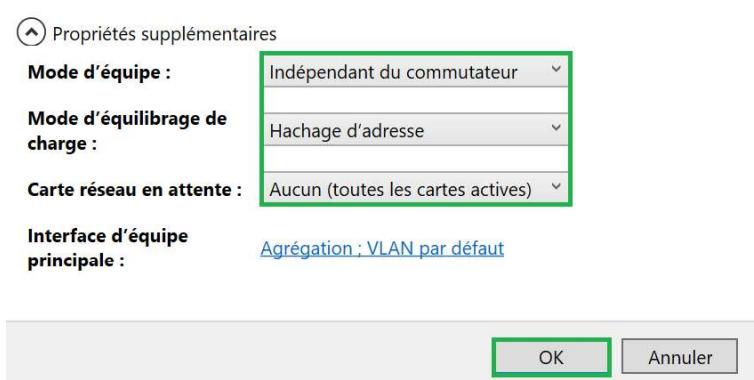
Faites un clic droit sur la première carte puis sélectionnez **Ajoutez à une nouvelle équipe** :



Une fenêtre s'ouvre alors, choisissez le nom puis sélectionnez les deux cartes et cliquez sur **Propriétés supplémentaires** :



Configurez comme ceci puis cliquez sur **OK** :



Cela peut prendre quelques minutes avant que les deux cartes soient actives donc pas de panique :

Nom	Statut	Type de serveur	Version du système d'exploitation	Équipes
SRV-STG01	Avertissement	Physique	Microsoft Windows Server 2019 Standard	1

Toutes les équipes 1 au total			
Équipe	Statut	Mode d'équipe	Équilibrage
Agrégation	Avertissement	Indépendant du commutateur	Hachage

Cartes réseau Interfaces d'équipe			
Carte	Vitesse	État	Raison
Ethernet0	1 Gbits/s	En échec	Connexion en attente
Ethernet1	1 Gbits/s	Actif	

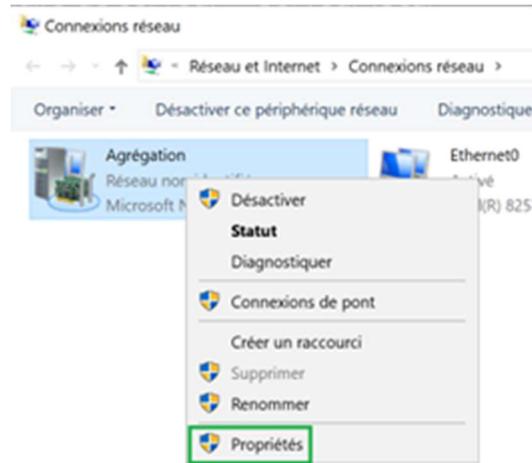
Qui devient :

Nom	Statut	Type de serveur	Version du système d'exploitation	Équipes
SRV-STG01	En ligne	Physique	Microsoft Windows Server 2019 Standard	1

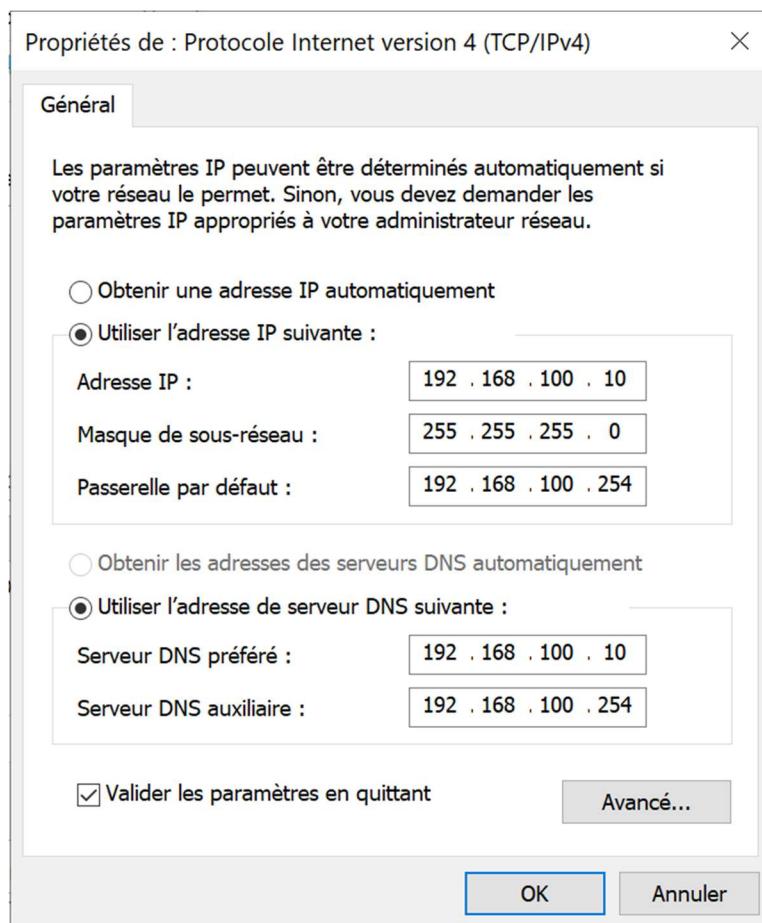
Toutes les équipes 1 au total			
Équipe	Statut	Mode d'équipe	Équilibrage
Agrégation	OK	Indépendant du commutateur	Hachage

Cartes réseau Interfaces d'équipe			
Carte	Vitesse	État	Raison
Ethernet0	1 Gbits/s	Actif	
Ethernet1	1 Gbits/s	Actif	

Nous allons maintenant attribuer l'IP statique que nous avons définis dans le tableau d'adressage.
 Pour cela il suffit de cliquer sur **adresse ipv4** à droite d'**Aggrégation**, puis faites un clic droit sur **Aggrégation** et cliquez sur **Propriétés** :



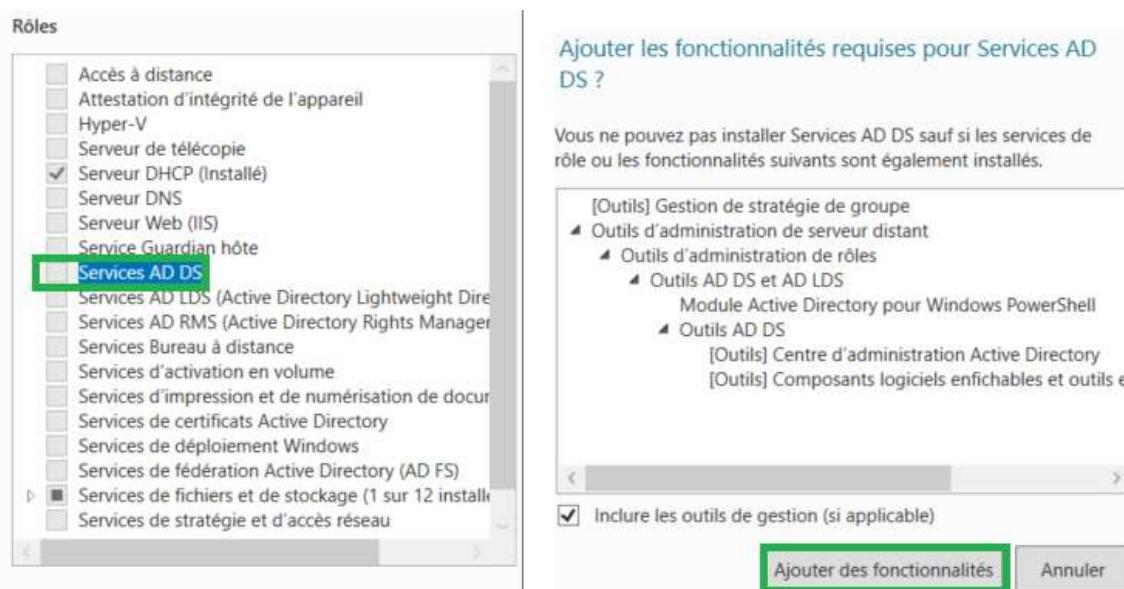
Faites un double clic sur **Protocole Internet version 4** :



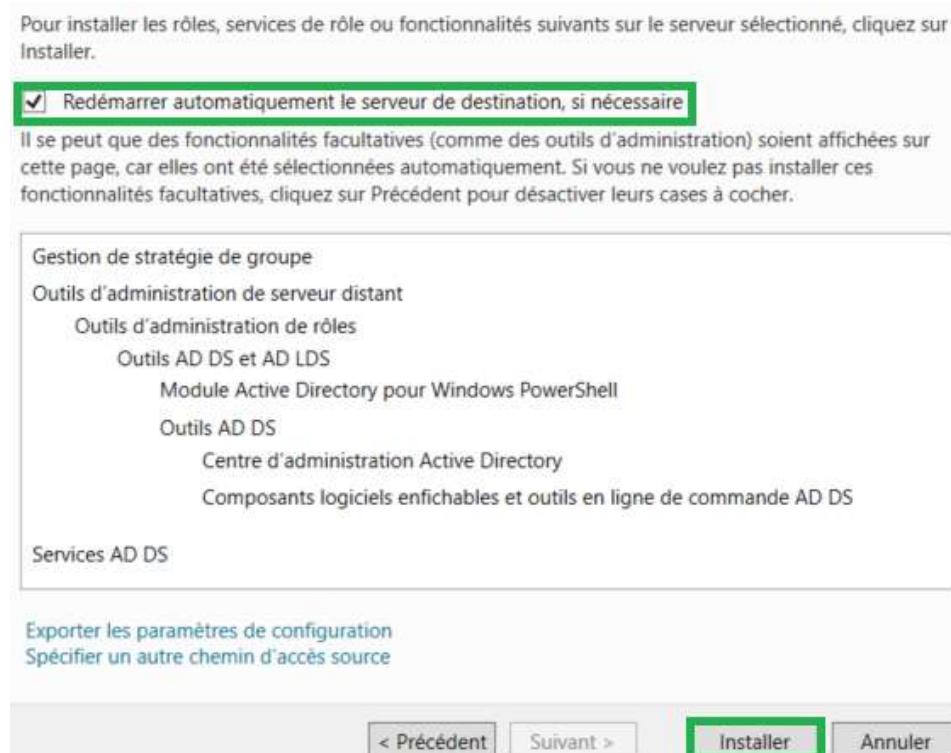
6.1.4) ADDS (Active Directory et DNS)

Nous allons maintenant passer à l'installation du service d'annuaire. Pour cela il existe un rôle qui installe l'Active directory ainsi que le DNS, il s'agit du rôle ADDS.

Cliquez sur **Ajouter des rôles et des fonctionnalités** dans le tableau de bord du **Gestionnaire de serveur**, puis cliquez 3 fois sur **Suivant**. Choisissez ensuite **Services AD DS**, L'assistant s'ouvre, cliquez sur **Ajouter des fonctionnalités** :

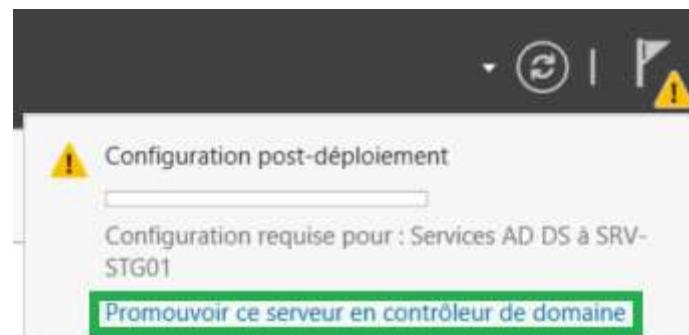


Cochez la case pour que le serveur redémarre automatiquement si nécessaire durant l'installation du rôle, puis cliquez sur **Installer** :



L'installation démarre, cela peut prendre quelques minutes.

Une fois le rôle installé, il nous reste quelques manipulations à effectuer. Pour cela, rendez-vous dans le tableau de bord du serveur et cliquer sur le **drapeau** en haut à droite, puis sur **Promouvoir ce serveur en contrôleur de domaine** :



Cochez la case **Ajouter une nouvelle forêt** et mettez le nom de domaine racine selon les spécifications techniques :

Sélectionner l'opération de déploiement

- Ajouter un contrôleur de domaine à un domaine existant
- Ajouter un nouveau domaine à une forêt existante
- Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine : **CCI-CAMPUS.LAN**

Cliquez sur **Suivant**, puis tapez le mot de passe de restauration que vous avez choisi et cliquez sur **Suivant** :

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt :	Windows Server 2016
Niveau fonctionnel du domaine :	Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

Serveur DNS (Domain Name System)
 Catalogue global (GC)
 Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur les options pour le contrôleur de domaine](#)

[**< Précédent**](#) [**Suivant >**](#) [**Installer**](#)

Ignorez la délégation DNS et faites une nouvelle fois **Suivant** :

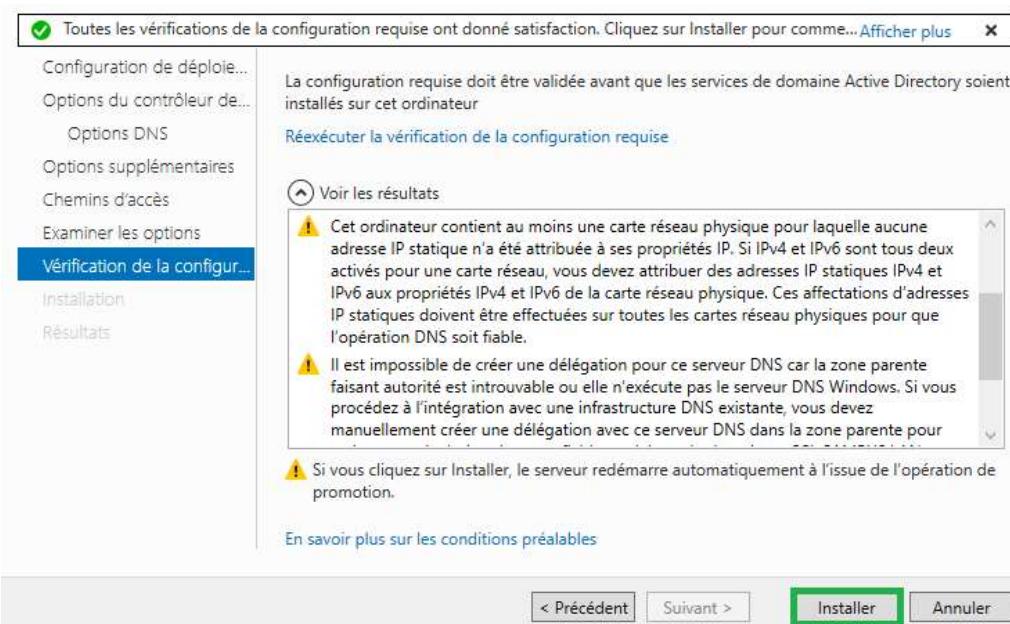
Spécifier les options de délégation DNS
 Crée une délégation DNS

Le nom de domaine NetBIOS devrait être rempli automatiquement :

Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS :

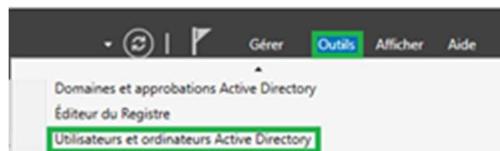
Cliquez sur **Suivant**, jusqu'à l'étape de l'installation puis cliquez sur Installer :



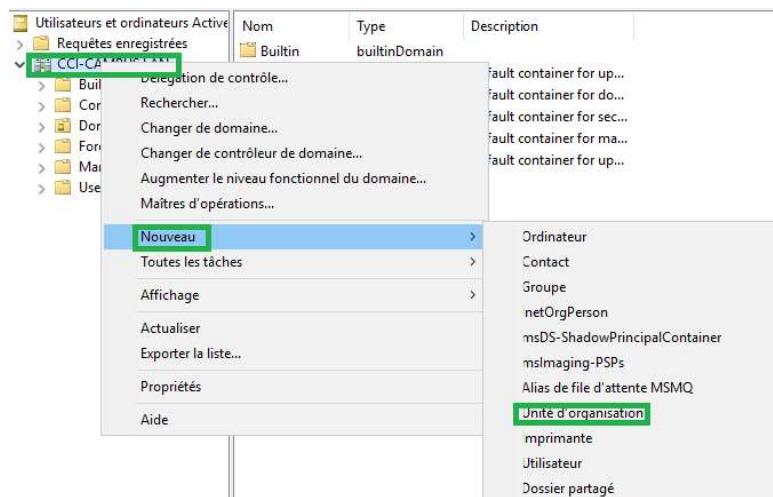
L'installation débute et puis le serveur va redémarrer pour finaliser l'installation, ce qui peut prendre un certain temps. Une fois redémarré, on nous propose de se connecter en **Administrateur du domaine** :



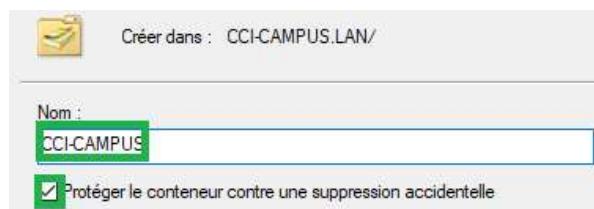
Nous allons maintenant passer à la création des groupes et utilisateurs AD. Pour cela rendez-vous dans l'onglet **Outils** du **Gestionnaire de serveur** puis cliquez sur **Utilisateurs et ordinateurs Active Directory** :



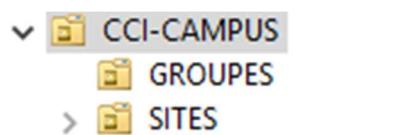
Pour commencer nous allons créer une UO nommé CCI-CAMPUS. Pour cela faites un clic droit sur le domaine puis **Nouveau** et **Unité d'organisation** :



Renseignez **CCI-CAMPUS** et laissez la case **Protéger le contenu coché** et validez :



Dans cette UO, de la même façon, nous allons créer une autre UO, **GROUPES**

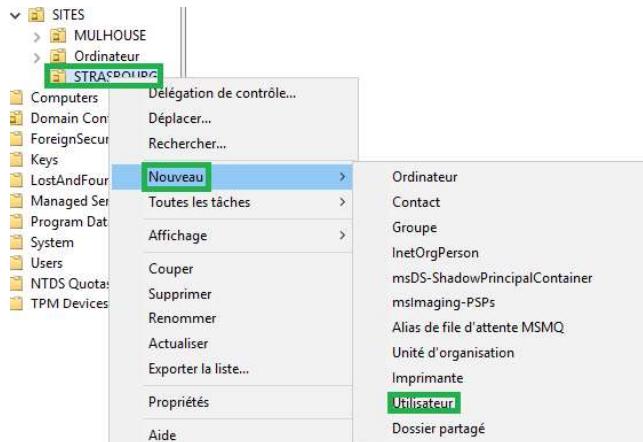


Dans l'UO SITES nous allons créer **3 UO** :

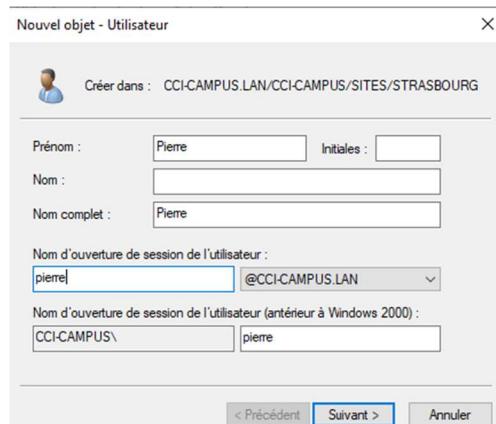
- STRASBOURG
- MULHOUSE
- Ordinateur



Une fois dans l'UO STRASBOURG, commencez par créer un nouvel utilisateur en faisant un clic droit sur STRASBOURG puis Nouveau et Utilisateur :



Ce nouvel utilisateur s'appelle Pierre. Renseignez comme ceci (Comme cet utilisateur est fictif et que nous n'allons pas ajouter d'autre Pierre, nous n'allons pas prendre la peine d'inventer un nom de famille) et cliquez sur **Suivant** :

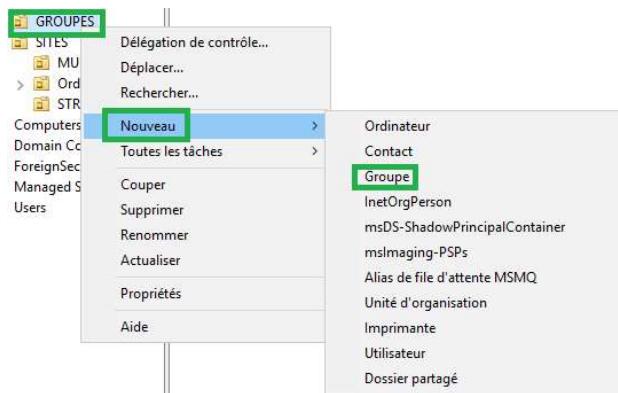


Renseigner le mot de passe de l'utilisateur en respectant toujours les normes de sécurité.

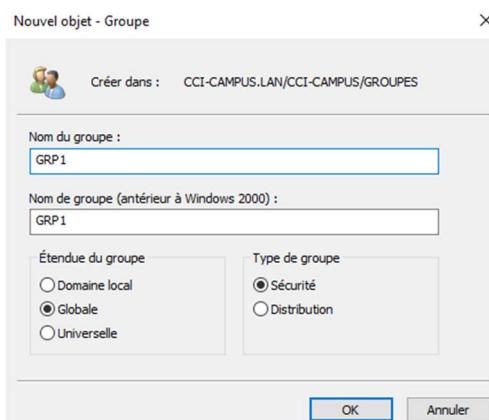
Dans l'UO GROUPES, nous allons créer 3 groupes :

- ADMIN
- GRP1
- GRP2

Pour cela, nous allons faire un clic droit sur l'UO GROUPES puis Nouveau et Groupe :



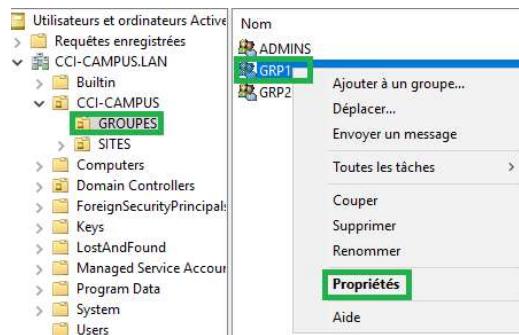
Renseignez le nom du groupe puis laissez-le reste de base puis cliquez sur **OK**.



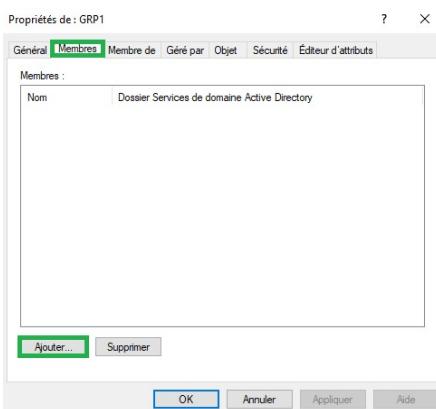
Faites pareil pour le **GRP2** et le groupe **ADMIN**. Après validation, nous pouvons voir que les groupes sont visibles dans l'UO :

	Nom	Type
ADMIN		Groupe de séc...
GRP1		Groupe de séc...
GRP2		Groupe de séc...

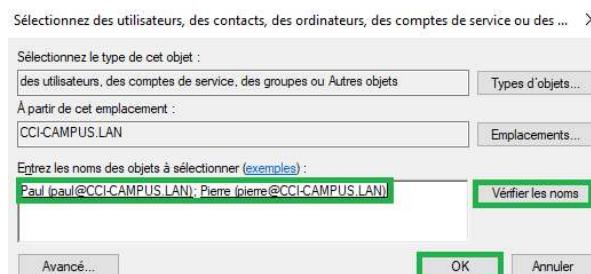
Une fois les groupes créés, selon *l'annexe 2*, nous allons attribuer des utilisateurs à un groupe précis. Paul et Pierre iront dans le **GRP1** et Nathalie et Isabelle iront dans le **GRP2**. Pour cela, nous allons faire un clic droit sur le **GRP1** puis **Propriétés** :



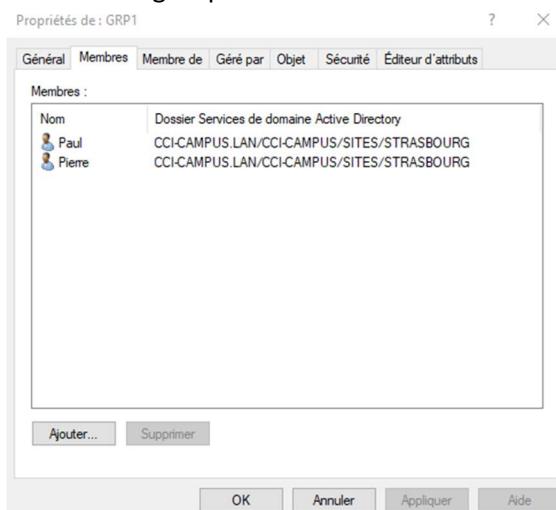
Ensute on clique sur **Membres** et **Ajouter** :



On clique dans l'encadré **Entrez les noms** et on rentre Paul puis on clique sur **Vérifier les noms**, pareil pour Pierre et ensuite on clique sur **OK** :



On peut voir qu'ils sont ajoutés dans le groupe :

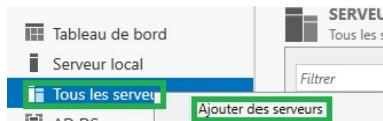


6.1.5) Rejoindre le domaine avec le second serveur

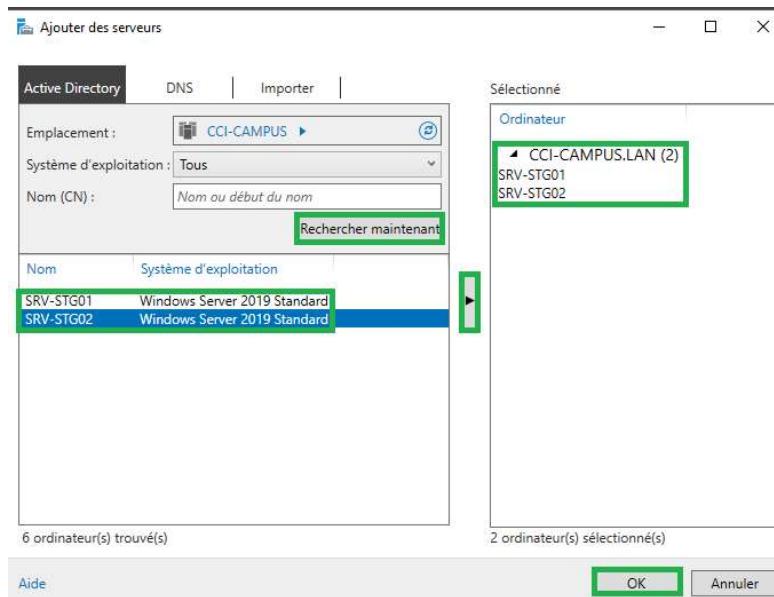
Pour le second serveur, la configuration initiale est identique au premier.

La différence va résider dans le fait qu'on va ajouter le rôle AD DS en rejoignant un domaine et non plus en le créant.

Nous allons ensuite procéder à l'intégration au domaine,pour cela, dans le **Gestionnaire de serveur**, rendez-vous dans l'onglet Tous les serveurs et faites un clic droit puis **Ajouter des serveurs** :

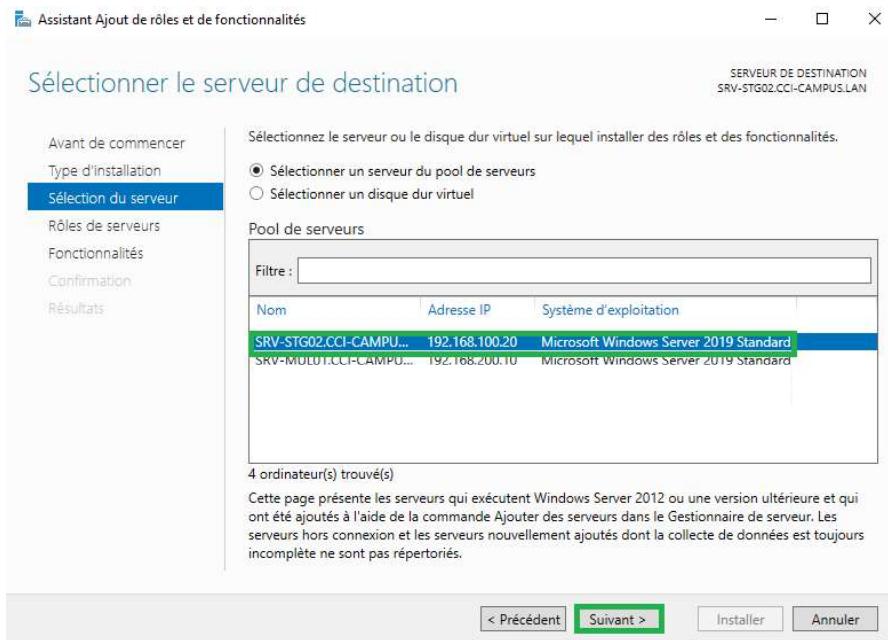


Cliquez sur **Rechercher maintenant**, la liste des serveurs apparaît, il suffit ensuite de cliquer sur le serveur concerné puis de cliquer sur la flèche pour que le nom du serveur se retrouve à droite dans les ordinateurs **Sélectionné**, validez avec **OK** :

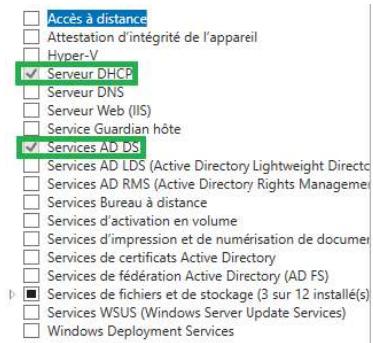


Une fois le serveur ajouté, nous pouvons l'administrer via le premier serveur dans la fenêtre tous les serveur.

Pour cela, rendez-vous dans le tableau de bord pour ajouter un nouveau rôle. Faite deux fois de suite **Sivant**, Sélectionnez ensuite le serveur que vous souhaitez mettre en contrôleur de domaine secondaire :



Cliquez sur **Sivant** puis cochez la case Services AD DS. On va également cocher la case Serveur DHCP pour configurer le basculement plus tard :

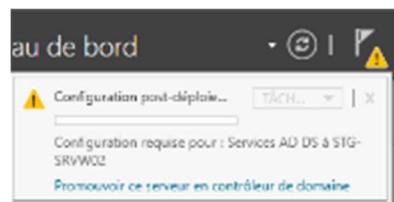


Une nouvelle fenêtre apparaît, cliquez sur **Ajouter des fonctionnalités** puis faites **Sivant** trois fois de suite. Vous pouvez maintenant installer le rôle.

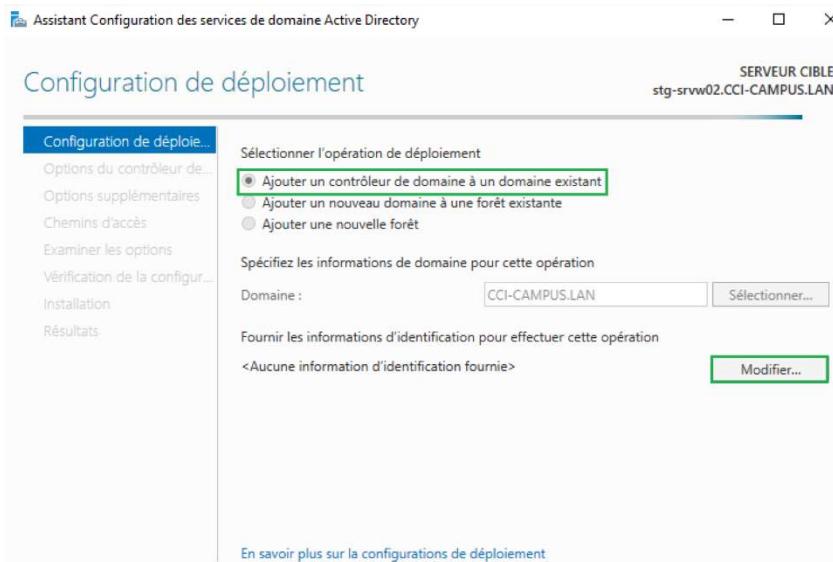
Une fois l'installation terminée, nous pouvons observer :



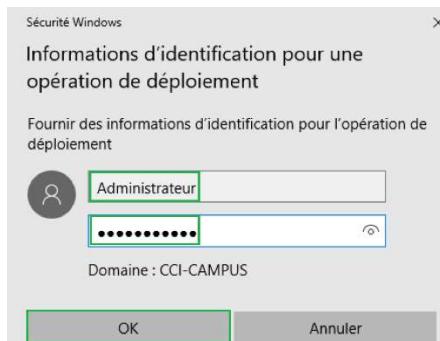
Cliquez ensuite sur l'icône drapeau puis sur **Promouvoir ce serveur en contrôleur de domaine** :



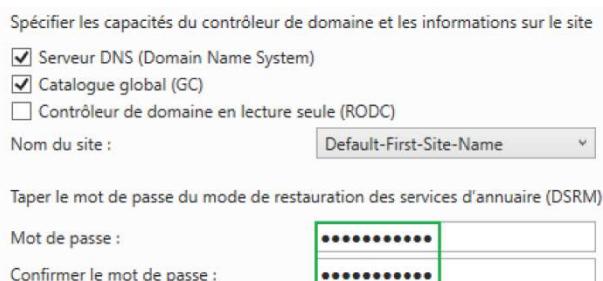
Une nouvelle fenêtre apparaît :



Cliquez sur **Modifier** et compléter avec le compte Administrateur du domaine et mot de passe :



Validez en tapant **OK** Cliquez ensuite sur **Suivant** et compléter en renseignant le mot de passe du **mode de restauration des services d'annuaires** définit sur le premier serveur :



Faites ensuite **Suivant** deux fois de suite et sélectionnez votre serveur principal :

Spécifier les options d'installation à partir du support (IFM)

Installation à partir du support

Spécifier des options de réPLICATION supplémentaires

Répliquer depuis :

Tout contrôleur de domaine

Tout contrôleur de domaine

STG-SRVW01.CCI-CAMPUS.LAN

Cliquez sur **Suivant** trois fois de suite puis lancez l'installation. Une fois terminée, vous pouvez observer :

Résultats

SERVEUR CIBLE
stg-srvw02.CCI-CAMPUS.LAN

 Ce serveur a été correctement configuré en tant que contrôleur de domaine

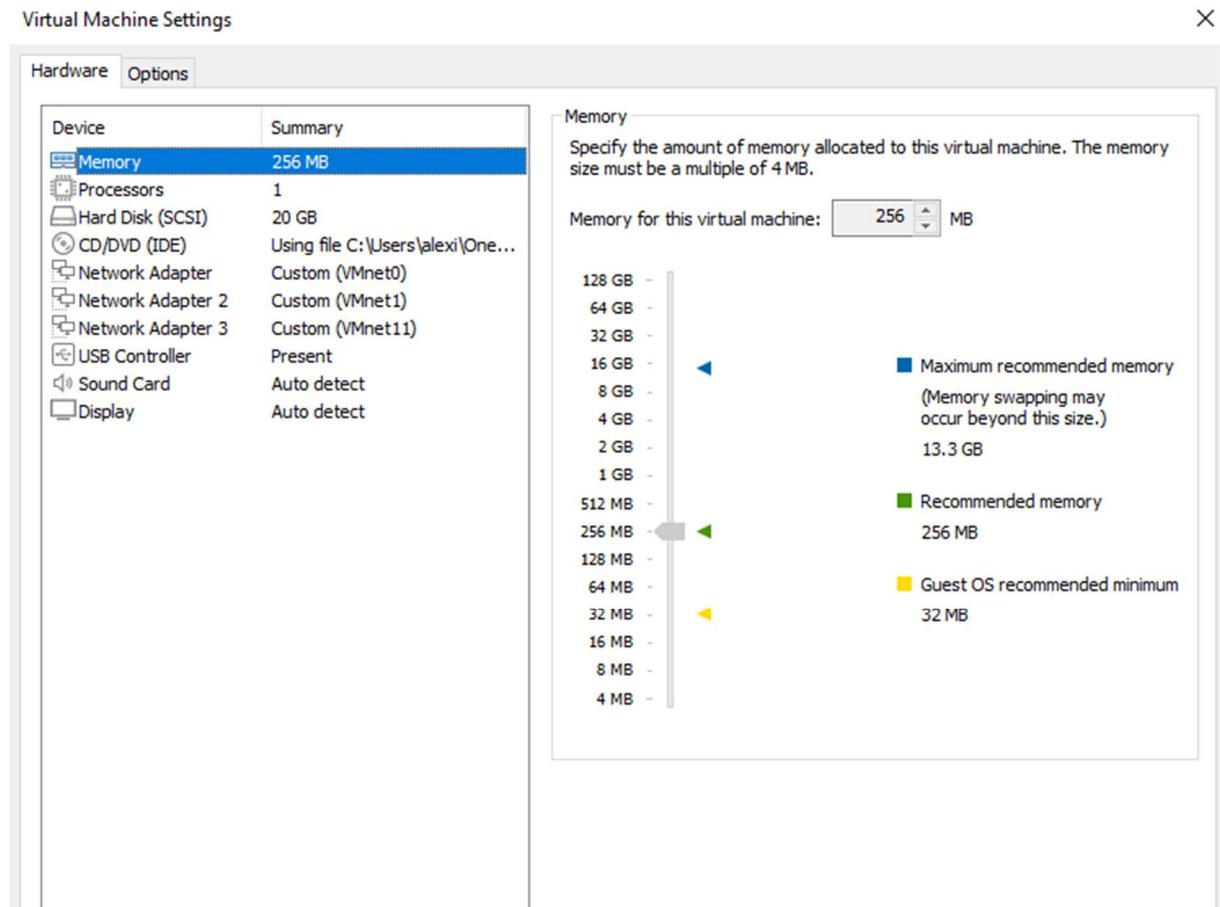
Afficher plus



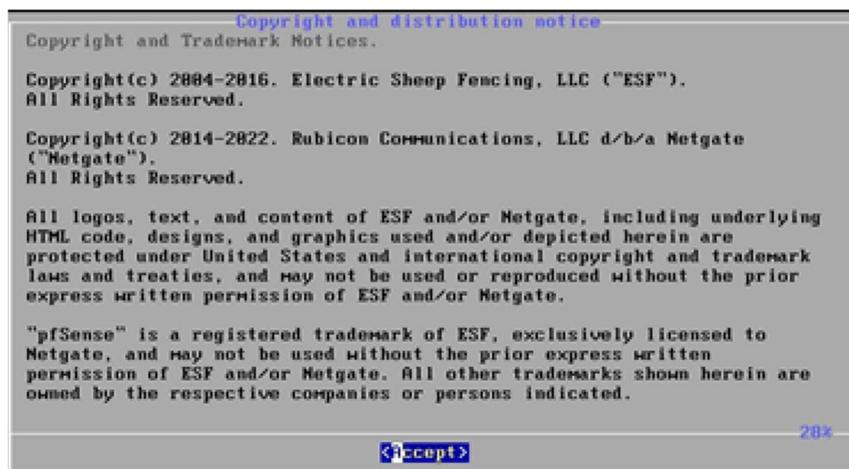
Le serveur est désormais un contrôleur de domaine Active directory. De ce fait les données sont répliquées dans les deux actives directory.

6.2.1 Mise en place des serveurs Pfsense

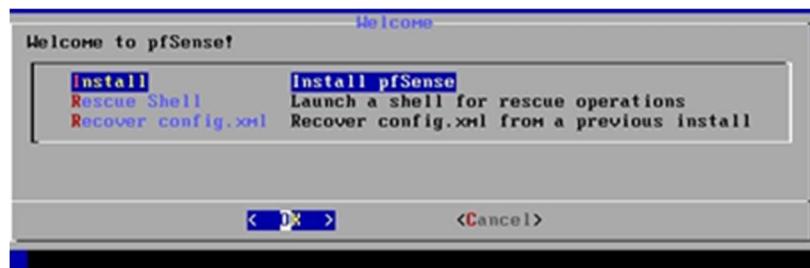
Dans un premier temps, veuillez configurer vos VM pfsense de cette manière avec **deux cartes réseaux**, l'une en **NAT** ou en **Bridge** que l'on a décidé de laisser en **DHCP** et l'autre en **host-only** pour le LAN.



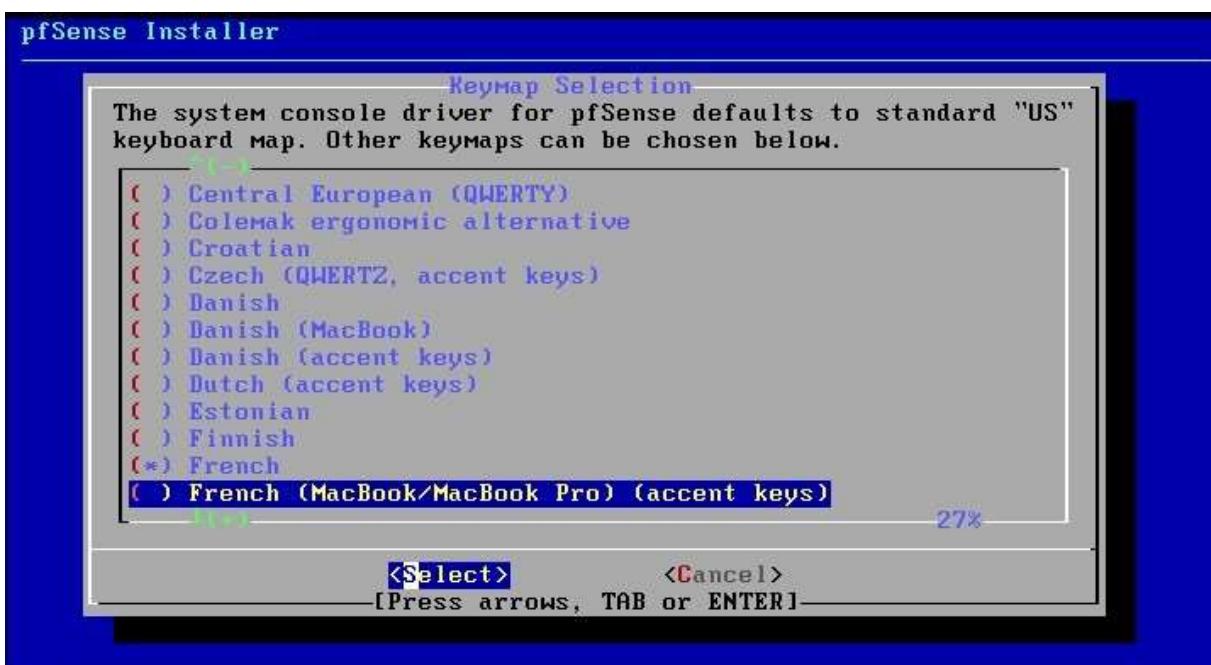
Faire ceci pour les VM PfSense de **Strasbourg** ainsi que **Mulhouse**.



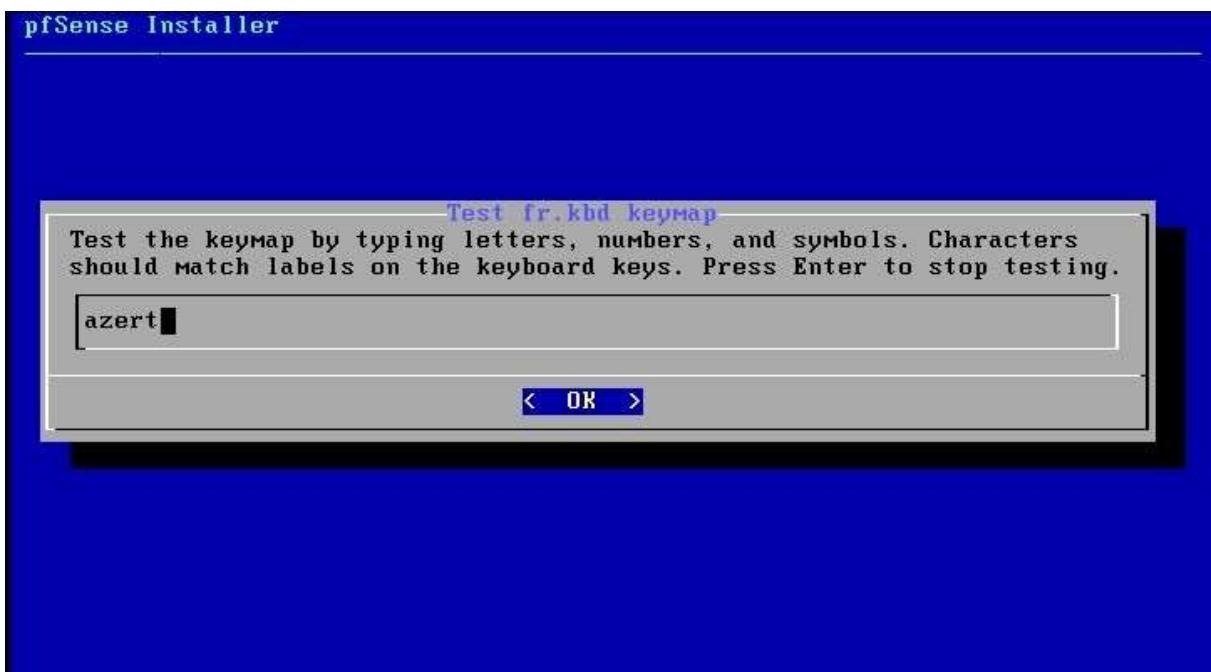
Ici, il faut simplement appuyer sur **accept** et lancer l'installation.



Lancer l'installation qui peut prendre quelques minutes selon votre configuration.

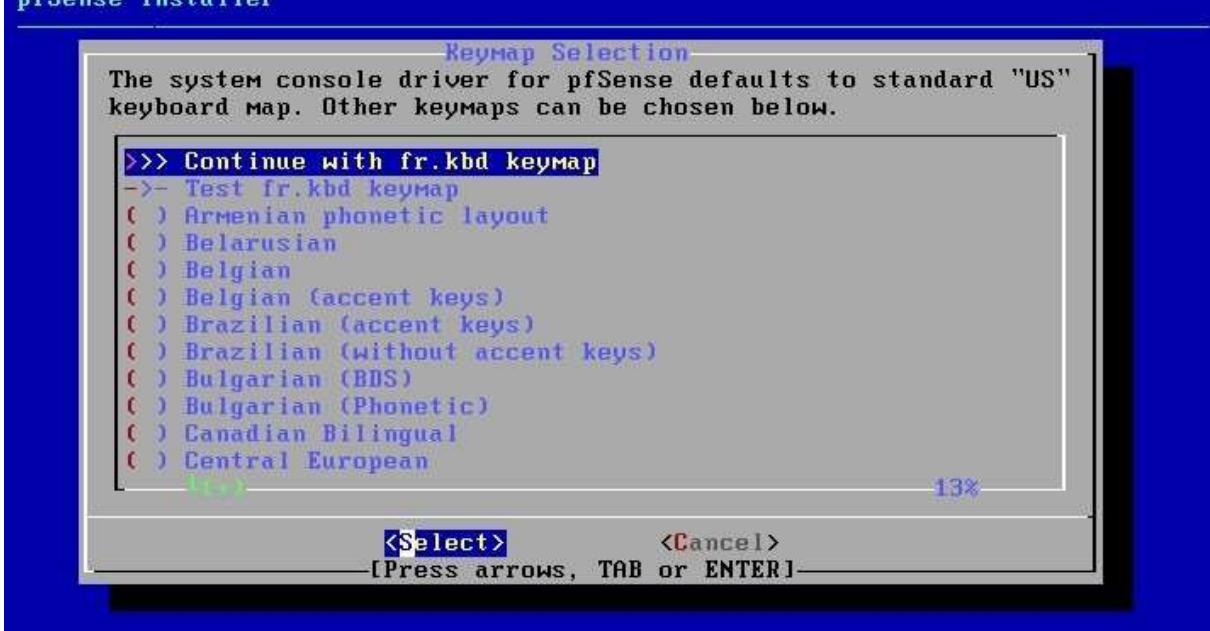


Concernant le clavier, nous allons rechercher le clavier French qui est le clavier français. En remontant tout en haut nous pouvons essayer si le clavier fonctionne correctement en tapant Azerty par exemple.



Ici nous voyons que le clavier est bien en français donc en **Azerty** et non en Qwerty. Nous allons donc pouvoir continuer l'installation.

pfSense Installer



Une fois le clavier configuré, pfsense va nous demander si nous désirons mettre en place une **partition sur les disques**. Ce n'est pas souhaité dans le cadre de cette AP donc nous laissons **Auto (ZFS)**.

pfSense Installer



Une fois appuyé sur « **OK** », il suffit de lancer l'installation en vérifiant les informations sur la fenêtre suivante.



Dans cette partie, nous avons la possibilité de mettre en place un **RAID**.

Dans le cadre de ce projet, nous n'en avons pas la nécessité cependant c'est **vivement conseillé** d'en mettre un en place !

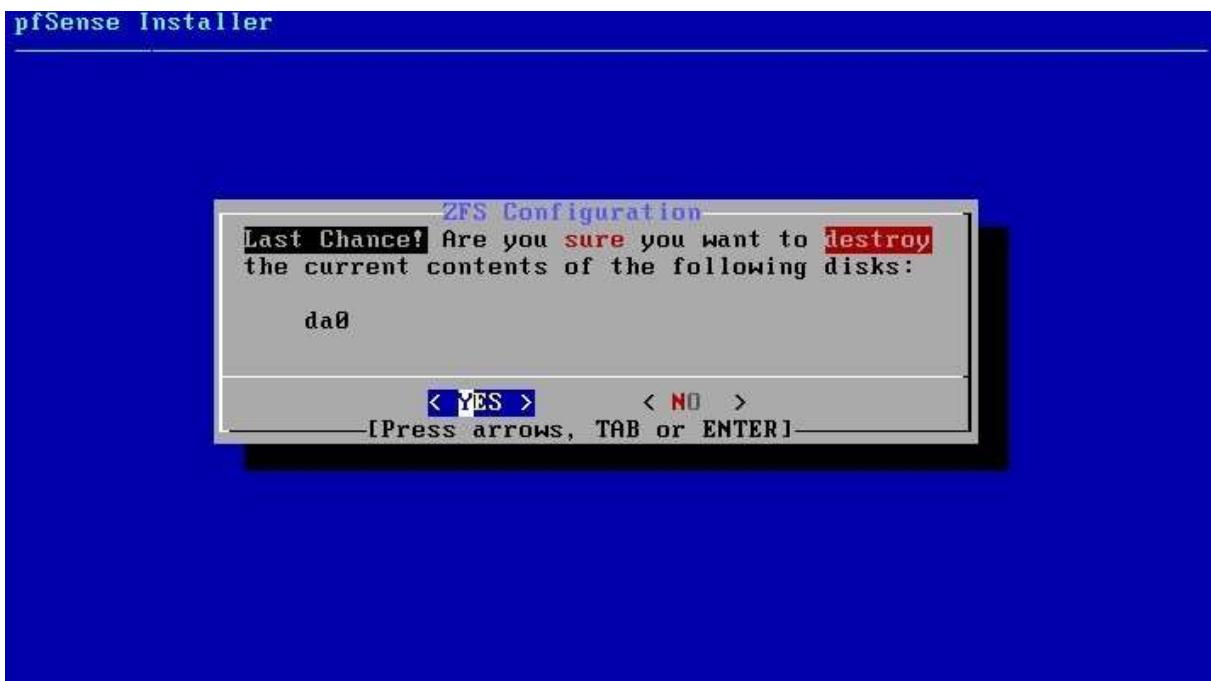
La mise en place d'un RAID 1 permet **d'écrire sur les deux disques** en même temps pour assurer la **haute disponibilité des services**. Ceci permet une grande tolérance en cas de disque dur en panne.



Sélectionnons donc le **seul** disque disponible afin de lancer l'installation.



Pfsense nous avertit que l'ensemble des données du disque vont être **détruite** afin de faire l'installation. Il suffit de dire Oui en ayant bien sûr **aucune donnée sur le disque en question**



Le **Shell** n'est pas obligatoire dans ce cas, cela peut permettre de rentrer des **lignes de commandes** avant de reboot le pc.



Ici nous allons redémarrer la machine car l'installation de l'OS est terminée.



6.2.2) Configuration pfsense

Routeur 1 :

```
Enter an option: 1

Valid interfaces are:
em0      00:0c:29:dc:9d:75  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:dc:9d:7f (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
```

Sélectionner la **première option** dans le menu afin d'assigner les deux cartes réseaux que nous avons ajouté lors de la configuration de la machine virtuelle.

```
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\?n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1

Do you want to proceed [y\?n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
```

Une fois que l'on lance la première option afin d'assigner les cartes réseaux, on nous demande de définir laquelle est sur le réseau WAN et de définir celle qui sera le LAN.

Em0 est notre **WAN**.

EM1 est notre **LAN**.

Afin de configurer les adresses IP, nous devons nous rendre dans la seconde option du menu.

```

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: 2

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

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

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to WAN... █

```

Une fois dans celle-ci, nous avons pris la décision de mettre l'adresse WAN en DHCP avec une carte réseaux en Bridged.

```

Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.254

Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

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

```

Revenons dans l'option 2 mais cette fois-ci nous configurons le LAN. Nous avons défini une adresse IP en **192.168.100.254** pour Strasbourg. Le masque de sous réseaux étant un /24 soit **255.255.255.0**.

Nous n'avons pas renseigné de Gateway. Lorsque la configuration des adresses est achevée, vous devez arriver sur une fenêtre comme celle-ci avec vos adresses IP configurées à l'étape d'avant.

```

FreeBSD/amd64 (UPNStrasbourg.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: c10d7154fa92ddfea836

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on UPNStrasbourg ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.151.121/24
LAN (lan)      -> em1      -> v4: 192.168.101.254/24
OPT1 (opt1)    -> em2      ->

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:
Message from syslogd@UPNStrasbourg at Apr 15 12:03:54 ...
php-fpm[17755]: /vpn_openvpn_server.php: Successful login for user 'admin' from:
192.168.101.10 (Local Database)

```

Configuration 2:

```

Enter an option: 1

Valid interfaces are:

em0      00:0c:29:dc:9d:75  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:dc:9d:7f  (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

```

Comme sur le site de Strasbourg, il vous faut assigner les cartes réseaux que l'on vient d'ajouter à la machine.

EM0 pour le **WAN**

EM1 pour le **LAN**

```

say no here and use the WebConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\?n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1

Do you want to proceed [y\?n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
■

```

Afin de configurer les adresses IP, nous devons nous rendre dans la seconde option du menu.

```

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: 2

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

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

Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to WAN... ■

```

Une fois dans celle-ci, nous configurons l'adresse WAN sur IPv4 que l'on passe en DHCP.
L'adresse IPv6 ici n'est pas utile.

```

Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.200.254

Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

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

```

Une fois l'adresse IPv4 du WAN configurée, nous répétons l'opération pour le LAN mais sans mettre de DHCP donc il faut configurer les adresses IP de la manière ci-dessus.

```

OPT1 -> em2

Do you want to proceed [y:n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VMware Virtual Machine - Netgate Device ID: 1c3e300ef70eb3a05942

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.151.14/24
LAN (lan)      -> em1      -> v4: 192.168.101.253/24
OPT1 (opt1)    -> em2      ->

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: █

```

Lorsque l'on a fini, nous devrions avoir un menu affichant les adresses IP comme celui-ci.

6.2.3) Configuration Pfsense via l'interface WEB

Routeur 1 :

Dans un premier temps, il faudra vous rendre sur un poste client que vous mettez dans **le même sous réseaux que votre pfsense**. Pour l'exemple, mon poste client à l'adresse IP suivante : 192.168.100.3

Une fois cette opération effectuée, je me rends sur Internet et je renseigne en **URL l'adresse IP LAN** de mon serveur Pfsense, ici 192.168.100.254

The screenshot shows the pfSense 2.6.0-RELEASE dashboard. On the left, there's a sidebar with icons for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main area has two tabs: 'System Information' and 'Netgate Services And Support'. The 'System Information' tab displays details like Name (VPNStrasbourg.home.arpa), User (admin@192.168.100.3), System (VMware Virtual Machine), BIOS (Phoenix Technologies LTD, Version 6.00, Release Date Thu Nov 12 2020), Version (2.6.0-RELEASE), CPU Type (Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz), and Hardware crypto (Kernel PTI Disabled). The 'Netgate Services And Support' tab shows Contract type (Community Support, Community Support Only) and NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES. It includes links for Upgrade Your Support, Community Support Resources, Netgate Global Support FAQ, Official pfSense Training by Netgate, and Netgate Professional Services. A note at the bottom of this section states: "If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY." Another note below it says: "If you decide to purchase a Netgate Global TAC Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#)."

Une fois que vous êtes arrivé sur cette page, nous allons désormais nous occuper des règles de pare-feu.

Pour ce faire, rendez-vous dans **Firewall → Rules**

The screenshot shows the pfSense web interface. At the top, there's a navigation bar with links for System, Interfaces, Firewall (which is currently selected), Services, VPN, Status, Diagnostics, and Help. A red arrow points to the 'Rules' link in the Firewall dropdown menu. Below the navigation bar is a status dashboard and a system information table. To the right of the main content area is a sidebar titled 'Netgate Services And Support' which includes a section about community support resources.

This screenshot shows the 'WAN' tab under the 'Rules' section of the pfSense firewall configuration. It lists two default rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0 / 0 B	IPv4 UDP	*	*	WAN address	1195	*	none		OpenVPN wizard	
0 / 0 B	IPv4 TCP/UDP	*	*	192.168.151.100	1194 (OpenVPN)	*	none			

At the bottom of the table are buttons for Add, Delete, Save, and Separator.

Sur le screen ci-dessus, des règles sont déjà mise en place par défaut. Nous n'avons pas la nécessité de les modifier dans le cadre de ce projet.

Nous allons donc ajouter des règles de pare-feu dans l'onglet LAN. Pour créer les règles de pare-feu, rien de plus simple. Rendez-vous dans l'onglet LAN et appuyez sur le bouton vert ADD

[Floating](#) [WAN](#) **LAN** [IPsec](#)
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4 /155 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	<input checked="" type="checkbox"/> 35 /6.17 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

 Add Add
Edit Firewall Rule
Action

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled
 Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

Choose the interface from which packets must come to match this rule.

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source
Source
 Invert match

any

Source Address

/

Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination
Destination
 Invert match

any

Destination Address

/

Destination Port Range

From Custom

To

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Voici le menu de création d'une règle. Comme vu lorsque je me rends sur l'onglet LAN , actuellement des règles sont déjà en place. Prenons la règles ICMP par exemple, pour la créer il suffit de mettre une « **ACTION** » en pass, de changer le **protocole TCP en ICMP** et de valider car nous sommes en Source Any et en destination Any.

Afin d'ajouter une couche de sécurité, il est conseillé d'ajouter des règles de pare-feu bloquant les sources externes de votre entreprise. Actuellement lorsque vous laissez les règles en Any, n'importe qui peut ping vos machines.

6.2.4) Mise en place de CARP/PFSYNC

Dans un premier temps sur le routeur principal, le premier dans mon cas, rendons nous sur Firewall
 → Virtual IP

Firewall / Virtual IPs				
Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.151.100/24 (vhid: 1)	WAN	CARP	carpwan	
192.168.101.100/24 (vhid: 2)	LAN	CARP	carplan	
192.168.100.250/24 (vhid: 3)	OPT1	CARP	carpdmz	

+ Add

Ajouter les règles CARP en ajoutant les **IP VIRTUELS**. Les 3 adresses que l'on ajoute sont les IP VIRTUELS créer pour le WAN, LAN , et la DMZ.

Firewall / Virtual IPs / Edit				
Edit Virtual IP				
Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	WAN			
Address type	Single address			
Address(es)	192.168.151.100	/ 24		
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP Password	*****	*****	Confirm	
Enter the VHID group password.				
VHID Group	1	▼		
Enter the VHID group that the machines will share.				
Advertising frequency	1	Base	100	Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.				
Description	carpwan	A description may be entered here for administrative reference (not parsed).		
<input type="button" value="Save"/>				

Edit Virtual IP

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	LAN			
Address type	Single address			
Address(es)	192.168.101.100		/ 24	v
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP Password	*****		*****	
Enter the VHID group password.				
VHID Group	2			
Enter the VHID group that the machines will share.				
Advertising frequency	1	100	v	
Base Skew				
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.				
Description	carplan			
A description may be entered here for administrative reference (not parsed).				

Save

Edit Virtual IP

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	OPT1			
Address type	Single address			
Address(es)	192.168.100.250		/ 24	v
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP Password	*****		*****	
Enter the VHID group password.				
VHID Group	3			
Enter the VHID group that the machines will share.				
Advertising frequency	1	100	v	
Base Skew				
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.				
Description	carpd mz			
A description may be entered here for administrative reference (not parsed).				

Save

A FAIRE UNIQUEMENT SUR LE SERVEUR 1

Pfsync sur le routeur 1 :

System / High Availability Sync

State Synchronization Settings (pfsync)

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

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

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

Configuration Synchronization Settings (XMLRPC Sync)

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

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

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

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

Select options to sync

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

Toggle All

Sur le routeur 2 :

Pour que la synchronisation se fasse , il suffit de cocher pfsync sur le second serveur et le CARP fera le nécessaire

The screenshot shows the pfSense web interface with the following sections:

- System / High Availability Sync** (Header)
- State Synchronization Settings (pfsync)**
 - Synchronize states**: A checked checkbox with a note explaining pfsync transfers state insertion, update, and deletion messages between firewalls.
 - Synchronize Interface**: Set to LAN with a note about communication via multicast.
 - pfsync Synchronize Peer IP**: An input field for the peer IP address.
- Configuration Synchronization Settings (XMLRPC Sync)**
 - Synchronize Config to IP**: An input field for the XMLRPC sync target IP address.
 - A note stating XMLRPC sync is currently supported over connections using the same protocol and port as this system.
- Remote System Password** (Form):

Remote System Password	<input type="text"/>	Remote System Password
Enter the webConfigurator password of the system entered above for synchronizing the configuration.		
Do not use the Synchronize Config to IP and password option on backup cluster members!		
- Synchronize admin** (Form):

Synchronize admin	<input type="checkbox"/> synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.	
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.	
- Select options to sync** (Form):

Select options to sync	<input type="checkbox"/> User manager users and groups <input type="checkbox"/> Authentication servers (e.g. LDAP, RADIUS) <input type="checkbox"/> Certificate Authorities, Certificates, and Certificate Revocation Lists <input type="checkbox"/> Firewall rules <input type="checkbox"/> Firewall schedules <input type="checkbox"/> Firewall aliases <input type="checkbox"/> NAT configuration <input type="checkbox"/> IPsec configuration <input type="checkbox"/> OpenVPN configuration (Implies CA/Cert/CRL Sync) <input type="checkbox"/> DHCP Server settings <input type="checkbox"/> DHCP Relay settings <input type="checkbox"/> DHCPv6 Relay settings <input type="checkbox"/> WoL Server settings <input type="checkbox"/> Static Route configuration <input type="checkbox"/> Virtual IPs <input type="checkbox"/> Traffic Shaper configuration <input type="checkbox"/> Traffic Shaper Limiters configuration <input type="checkbox"/> DNS Forwarder and DNS Resolver configurations <input type="checkbox"/> Captive Portal
<input type="button" value="Toggle All"/>	
- Save** (Blue button at the bottom right)

Une fois que les règles sont créées de High Availability Sync est sauvegardée sur les deux serveurs, nous pouvons voir dans status → CARP

CARP Interfaces		
CARP Interface	Virtual IP	Status
WAN@1	192.168.151.100/24	MASTER
LAN@2	192.168.101.100/24	MASTER
OPT1@3	192.168.100.250/24	

Le routeur 1 qui est celui qui a toute la configuration initiale est en MASTER

CARP Interfaces		
CARP Interface	Virtual IP	Status
WAN@1	192.168.151.100/24	BACKUP
LAN@2	192.168.101.100/24	BACKUP
OPT1@3	192.168.100.250/24	

Le routeur 2 qui est celui qui reçoit la configuration est en backup

6.2.4. Installer et configurer un VPN distant (OpenVPN)

Création de l'Autorité de Certification – CA

Accédez à System > Certificate Manager > CAs, et cliquez sur le bouton Add en bas à droite.

The screenshot shows the pfSense web interface under the 'System' menu. In the 'Certificate Manager' section, the 'CAs' tab is selected. A search bar at the top has a green arrow pointing to the 'Add' button located at the bottom right of the table. The table headers are Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. The 'Actions' column contains a green 'Add' button with a plus sign.

Remplir le « Descriptive name » (sans espaces, ni caractères spéciaux)
 Faire la même chose pour le Common Name

The screenshot shows the pfSense Certificate Manager interface. In the 'Create / Edit CA' section, the 'Descriptive name' is set to 'CERT_VPN'. The 'Method' is set to 'Create an internal Certificate Authority'. Under 'Trust Store', there is an unchecked checkbox for adding the CA to the operating system's trust store. Under 'Randomize Serial', there is an unchecked checkbox for using random serial numbers. In the 'Internal Certificate Authority' section, the 'Key type' is 'RSA' with a bit length of '2048'. The 'Digest Algorithm' is 'sha256'. The 'Lifetime (days)' is set to '3650'. The 'Common Name' is 'internal-ca'. Below these fields, optional subject components are listed: 'Country Code' (None), 'State or Province' (e.g. Texas), 'City' (e.g. Austin), 'Organization' (e.g. My Company Inc), and 'Organizational Unit' (e.g. My Department Name (optional)). A blue 'Save' button is at the bottom.

Le certificat est créé

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CERT_VPN	✓	self-signed	0	CN=internal-ca		

Création Certificat Serveur

Dans la même rubrique Certificate Manager, accédez à l'onglet Certificat et cliquez sur le bouton Add en bas à droite.

System / Certificate Manager / Certificates

CAs Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (633aa3130ba73) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-633aa3130ba73	Valid From: Mon, 03 Oct 2022 08:53:39 +0000 Valid Until: Sun, 05 Nov 2023 08:53:39 +0000	webConfigurator

Add/Sig

Définir « Method » sur « Create an Internal Certificate », donner un Nom « CERT_SERV » et sélectionner l'autorité de certification « Certificate authority » créé précédemment « CERT_VPN »

System / Certificate Manager / Certificates / Edit

CAs Certificates Certificate Revocation

Add/Sign a New Certificate

Method

Descriptive name

Internal Certificate

Certificate authority

Key type RSA

2048 The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256 The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime (days) 3650 The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name CERT_SERV The following certificate subject components are optional and may be left blank.

Country Code None

State or Province e.g. Texas

City e.g. Austin

Organization e.g. My Company Inc

Organizational Unit e.g. My Department Name (optional)

Certificate Attributes

Sélectionnez « Server Certificate » et sauvegardez

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type

Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

FQDN or Hostname

Type Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add

+ Add

Save

Le certificat est créé

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (633aa3130ba73)	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-633aa3130ba73	webConfigurator	
Server Certificate CA: No Server: Yes		Valid From: Mon, 03 Oct 2022 08:53:39 +0000 Valid Until: Sun, 05 Nov 2023 08:53:39 +0000		
CERT_SERV Server Certificate CA: No Server: Yes	CERT_VPN	CN=CERT_SERV		

+ Add/Sign

Installation du package « OpenVPN-Client-Export »

Sélectionnez : System > Package Manager

The screenshot shows the pfSense web interface with the following details:

- Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.
- Left Sidebar:** Advanced, Cert. Manager, General Setup, High Avail. Sync, Logout (admin), **Installed Packages** (selected), Package Manager, Register, Routing, Setup Wizard, Update, User Manager.
- Middle Content:** A warning message: "WARNING: The password is set to the default value. Change the password in the User Manager." Below it, a link to "System / Installed Packages".
- Bottom Status:** There are no packages installed.

Sélectionnez « Available Packages », rechercher « openvpn » et installer « openvpn-client-export »

The screenshot shows the pfSense web interface with the following details:

- Header:** System / Package Manager / Available Packages.
- Buttons:** Installed Packages, **Available Packages** (selected).
- Search Bar:** Search term: openvpn, Both, Search, Clear.
- Packages Table:**

Name	Version	Description
openvpn-client-export	1.6_4	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.
- Dependencies:** openvpn-client-export-2.5.2, openvpn-2.5.4_1, zip-3.0_1, p7zip-16.02_3.
- Actions:** + Install button.

Puis cliquez sur « Confirm »

Confirmation Required to install package pfSense-pkg-openvpn-client-export.

Confirm

Patinez le temps de l'installation

The screenshot shows the pfSense web interface with the following details:

- Header:** System / Package Manager / Package Installer.
- Message:** Please wait while the installation of pfSense-pkg-openvpn-client-export completes. This may take several minutes. Do not leave or refresh the page!
- Buttons:** Installed Packages, Available Packages, **Package Installer** (selected).
- Log:**

```
>>> Installing pfSense-pkg-openvpn-client-export...
Updating pfSense-core repository catalogue...
```

System / Package Manager / Package Installer

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
--> NOTICE:
The p7zip port currently does not have a maintainer. As a result, it is
more likely to have unresolved issues, not be up-to-date, or even be removed in
the future. To volunteer to maintain this port, please create an issue at:
https://bugs.freebsd.org/bugzilla

More information about port maintainership is available at:
https://docs.freebsd.org/en/articles/contributing/#ports-contributing
>>> Cleaning up cache... done.
Success
```

Configurer OpenVPN

Sélectionnez « VPN » > « OpenVPN » et cliquer sur « + Add »

The screenshot shows the pfSense web interface with the following details:

- Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, **VPN** (highlighted), Status, Diagnostics, Help.
- Message Bar:** WARNING: The 'admin' account password is set to the default value. Change the password as soon as possible.
- Current Path:** VPN / OpenVPN / Servers
- Submenu:** IPsec, L2TP, **OpenVPN** (highlighted).
- Table Headers:** Servers, Clients, Client Specific Overrides, Wizards, Client Export, Shared Key Export. The 'Servers' header is underlined.
- Table:** OpenVPN Servers table with columns: Interface, Protocol / Port, Tunnel Network, Mode / Crypto, Description, Actions. A green '+ Add' button is located in the Actions column.
- Bottom Text:**
 - Server mode : « Remote Access (SSL/TLS) »
 - Local port : 1194 (Port par Défaut)
 - Description : « OpenVPN » (Nom du Tunnel VPN)

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export

General Information

Description **OpenVPN**
A description of this VPN for administrative reference.

Disabled Disable this server
Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode **Remote Access (SSL/TLS)**

Device mode **tun - Layer 3 Tunnel Mode**
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol **UDP on IPv4 only**

Interface **WAN**
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port **1194**
The port used by OpenVPN to receive client connections.

Sélectionnez votre autorité de certification « CERT_VPN » dans « Peer Certificate Authority » et le certificat Server « CERT_SERV » dans « Server certificate ».

Cryptographic Settings

TLS Configuration Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

Peer Certificate Authority **CERT_VPN**

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check Check client certificates with OCSP

Server certificate **CERT_SERV (Server: Yes, CA: CERT_VPN)**

IPv4 Tunnel Network : 192.168.89.0/24 (Adresse du tunnel VPN CIDR. Nous pouvons utiliser n'importe quel adresse IP privé sauf celles définies par la RFC 1918)
 Cocher « Redirect IPv4 Gateway » pour passer en mode full tunnel
 Concurrent connections : Nombre de connexions VPN simultanées (ici 20)

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway
 Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway
 Force all client-generated IPv6 traffic through the tunnel.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections

Specify the maximum number of clients allowed to concurrently connect to this server.

Cocher « Dynamic IP » et laisser « Topology » sur « Subnet – One IP address per client... »

Client Settings

Dynamic IP
 Allow connected clients to retain their connections if their IP address changes.

Topology

Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Indiquez « auth-nocache » dans « Custom options». (Pas de mise en cache des identifiants)

Advanced Configuration

Custom options

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
 EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Puis cliquez sur « save », Le serveur vpn est créé.

Afin de mettre en place une authentication avec radius ou LDAP, pour plus de sécurité, nous devons configurer les Wizards

Wizard / OpenVPN Remote Access Server Setup / ?

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server RADIUS ▼

NOTE: If unsure, leave this set to "Local User Access."

» Next

RADIUS Server Selection

OpenVPN Remote Access Server Setup Wizard

RADIUS Authentication Server List

RADIUS servers SRV-STG1 ▼

» Add new RADIUS server » Next

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Certificate Authority CERT_VPN ▼

» Add new CA » Next

Step 7 of 11

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate CERT ▼

» Add new Certificate » Next

General OpenVPN Server Information	
Interface	<input type="text" value="192.168.151.100 (carpwan)"/> <input type="button" value="▼"/>
The interface where OpenVPN will listen for incoming connections (typically WAN.)	
Protocol	<input type="text" value="UDP on IPv4 only"/> <input type="button" value="▼"/>
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.	
Local Port	<input type="text" value="1195"/>
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.	
Description	<input type="text"/>
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.	
Cryptographic Settings	
TLS Authentication	<input checked="" type="checkbox"/>
Enable authentication of TLS packets.	
Generate TLS Key	<input checked="" type="checkbox"/>
Automatically generate a shared TLS authentication key.	
TLS Shared Key	<input type="text"/>
Paste in a shared TLS key if one has already been generated.	
DH Parameters Length	<input type="text" value="2048 bit"/> <input type="button" value="▼"/>
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.	
Data Encryption Negotiation	<input checked="" type="checkbox"/>
Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.	
Data Encryption Algorithms	<input type="text" value="AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305"/> <input type="button" value="▼"/>
List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.	
Fallback Data Encryption Algorithm	<input type="text" value="AES-256-CBC (256 bit key, 128 bit block)"/> <input type="button" value="▼"/>
The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.	
Auth Digest Algorithm	<input type="text" value="SHA256 (256-bit)"/> <input type="button" value="▼"/>
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.	
Hardware Crypto	<input type="text" value="No Hardware Crypto Acceleration"/> <input type="button" value="▼"/>
The hardware cryptographic accelerator to use for this VPN connection, if any.	
Tunnel Settings	
Tunnel Network	<input type="text" value="192.168.11.0"/> <input type="button" value="▼"/>
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.	
Redirect Gateway	<input checked="" type="checkbox"/>
Force all client generated traffic through the tunnel.	
Local Network	<input type="text" value="192.168.101.0/24"/> <input type="button" value="▼"/>
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.	

Concurrent Connections	<input type="text" value="10"/>	Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	<input type="button" value="Refuse any non-stub compression (Most secure)"/>	
Allow compression to be used with this VPN instance, which is potentially insecure.		
Compression	<input type="button" value="Disable Compression [Omit Preference]"/>	
Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.		
Type-of-Service	<input type="checkbox"/>	
Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.		
Inter-Client Communication	<input type="checkbox"/>	
Allow communication between clients connected to this server.		
Duplicate Connections	<input type="checkbox"/>	
Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.		
Client Settings		
Dynamic IP	<input checked="" type="checkbox"/>	
Allow connected clients to retain their connections if their IP address changes.		
Topology	<input type="button" value="Subnet -- One IP address per client in a common subnet"/>	
Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".		
DNS Default Domain	<input type="text" value="CCI-CAMPUS.LAN"/>	
Provide a default domain name to clients.		
DNS Server 1	<input type="text" value="192.168.101.10"/>	
DNS server IP to provide to connecting clients.		
DNS Server 2	<input type="text"/>	
DNS server IP to provide to connecting clients.		
DNS Server 3	<input type="text"/>	
DNS server IP to provide to connecting clients.		
DNS Server 4	<input type="text"/>	
DNS server IP to provide to connecting clients.		
NTP Server	<input type="text"/>	
Network Time Protocol server to provide to connecting clients.		
NTP Server 2	<input type="text"/>	
Network Time Protocol server to provide to connecting clients.		
NetBIOS Options	<input type="checkbox"/>	
Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.		
NetBIOS Node Type	<input type="button" value="none"/>	
Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).		
NetBIOS Scope ID	<input type="text"/>	
A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.		
WINS Server 1	<input type="text"/>	
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.		

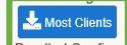
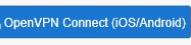
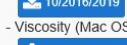
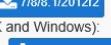
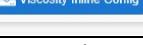
DNS Server 4	<input type="text"/>	DNS server IP to provide to connecting clients.
NTP Server	<input type="text"/>	Network Time Protocol server to provide to connecting clients.
NTP Server 2	<input type="text"/>	Network Time Protocol server to provide to connecting clients.
NetBIOS Options	<input type="checkbox"/>	Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type	<input type="text" value="none"/>	Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Scope ID	<input type="text"/>	A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
WINS Server 1	<input type="text"/>	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2	<input type="text"/>	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.

>> Next

Continuer ensuite jusqu'à la dernière étape en faisant juste suivant.

Ensuite rendons nous sur VPN → OPENVPN → Client Export

Save as default

Search			
Search term	<input type="text"/>	Search	Clear
Enter a search string or *nix regular expression to search.			
OpenVPN Clients			
User	Certificate Name	Export	
Authentication Only (No Cert)	none	Inline Configurations:    Bundled Configurations:   - Current Windows Installer (2.5.8-ix04):   - Legacy Windows Installers (2.4.12-ix01):   - Viscosity (Mac OS X and Windows):  	

Une fois la configuration télécharger, pour tester prenons un ordinateur qui n'est pas dans le même réseau local que notre infrastructure dans le cadre des test j'ai pris mon pc physique

Téléchargeons OpenVPN disponible sur le net

The screenshot shows the Windows Start Menu search interface. In the search bar at the top, the text "OpenVPN GUI" is typed. Below the search bar, the results are displayed under the heading "Meilleur résultat". The first result is "OpenVPN GUI" (Application), which is highlighted with a blue background. Below it is "OpenVPN-2.6.2-I001-amd64.msi" (Application). A sidebar on the left lists "Applications" and "Rechercher sur le Web" with several search suggestions.

OpenVPN GUI

Application

OpenVPN-2.6.2-I001-amd64.msi Application

Applications

- OpenVPN Configuration File Directory

Rechercher sur le Web

- openvpn - Afficher les résultats Web
- openvpn gui
- openvpn connect
- openv
- openvpn community
- openvas
- openverse
- openvpn client

Ensuite nous trouvons le logo dans la barre des tâches

The screenshot shows the Windows taskbar. The OpenVPN icon is visible. A context menu is open over the icon, displaying options: "Connecter", "Déconnecter", "Reconnect", "Afficher le statut", "Voir le log", "Editer la configuration", and "Effacer les mots de passe enregistrés".

Connecter

Déconnecter

Reconnect

Afficher le statut

Voir le log

Editer la configuration

Effacer les mots de passe enregistrés

VPNStrasbourg-UDP4-1195-config

VPNStrasbourg-UDP4-1194-config

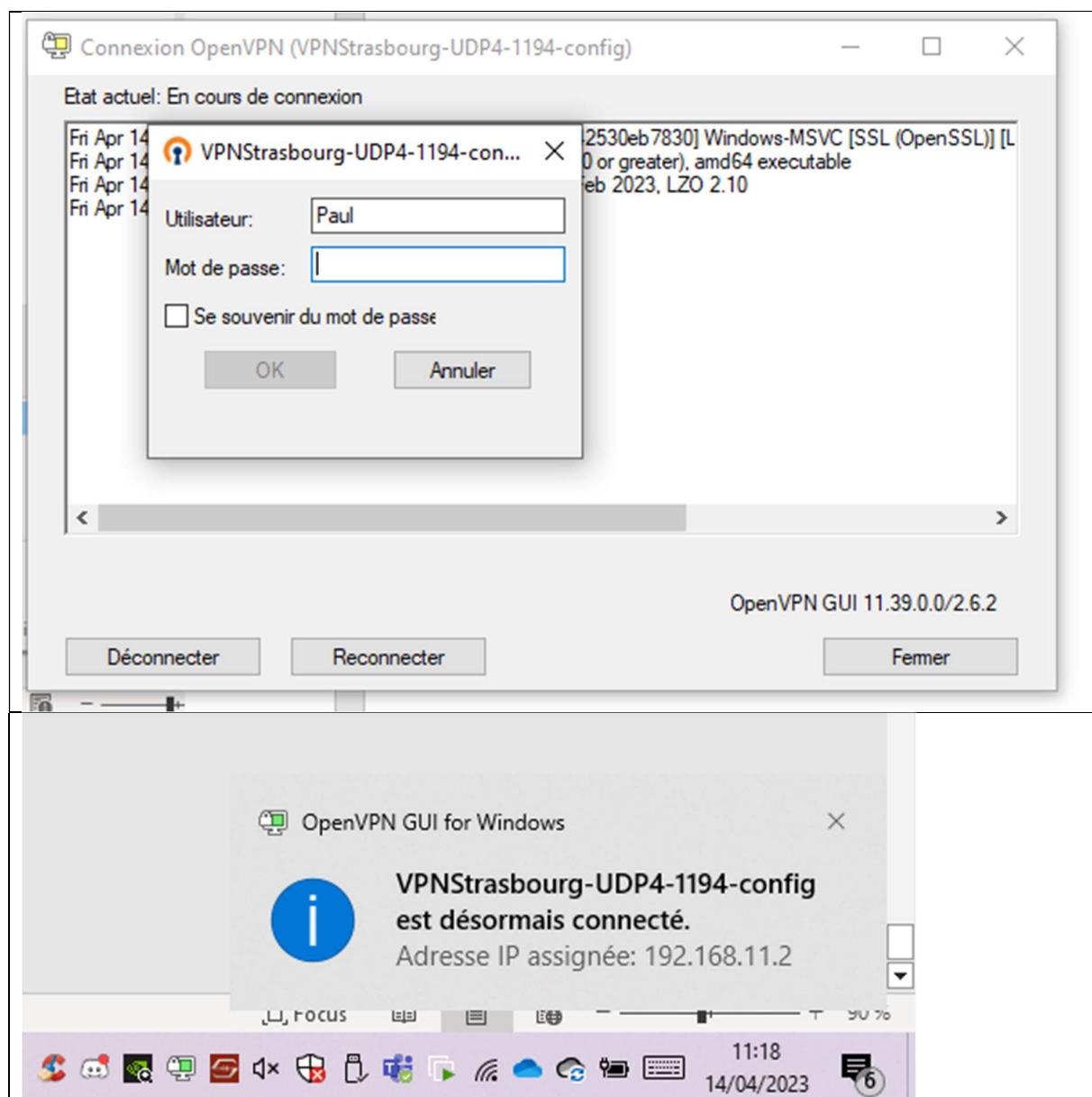
Import

Configuration...

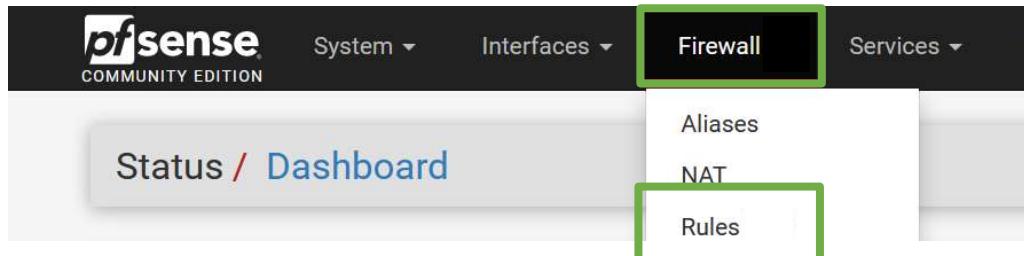
Quitter

P3_DFS - VM

Connectons nous avec un utilisateur de l'AD et dans notre cas un utilisateur faisant partie du groupe RADIUS



Mise en place des règles pour la DMZ



On ajoute une règle de pare-feu pour autoriser le LAN vers la DMZ

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1 /1.18 MiB *	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 /0 B	IPv4 TCP	LAN net	*	This Firewall	443 (HTTPS)	*	none		Autoriser XML-RPC	
<input type="checkbox"/>	0 /96 KIB	IPv4 PFSYNC	LAN net	*	This Firewall	*	*	none		Autoriser pfsync	
<input type="checkbox"/>	3 /25 KIB	IPv4 *	LAN net	*	*	*	WAN_FAILOVER	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Buttons at the bottom: Add Add Delete Save

Il faut Paramétrer la règle comme cela

Edit Firewall Rule

Action	<input type="button" value="Pass"/>
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP) is sent back to the source whereas with block the packet is dropped silently. In either case, the original packet is captured by the system.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="LAN"/>
Choose the interface from which packets must come to match this rule.	
Address Family	<input type="button" value="IPv4"/>
Select the Internet Protocol version this rule applies to.	
Protocol	<input type="button" value="Any"/>
Choose which IP protocol this rule should match.	

Dans la règle, indiquez comme source le réseau **LAN** et comme destination la **DMZ**

Source
Source: LAN net
 Invert match

Destination
Destination: DMZ net
 Invert match

Extra Options

Log: Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description: Autoriser traffic LAN vers DMZ
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Save

Accès WAN vers DMZ

Concernant la DMZ, il est nécessaire de rajouter les accès du réseau WAN vers la DMZ.

Ainsi sur l'interface WAN, rajoutez la règle suivante :

Source
Source: WAN net
 Invert match
 Source Address: /

Destination
Destination: DMZ net
 Invert match
 Destination Address: /

Extra Options

Log: Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description: Autoriser traffic WAN vers DMZ
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Save

Ainsi voici la règle sur le WAN

Floating WAN LAN WAN2 DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 *	WAN net	*	DMZ net	*	*	none		Autoriser traffic WAN vers DMZ	

Actions: Add Add Delete Save Separator

Accès DMZ vers WAN

Puis pour que la DMZ puisse interagir avec le réseau étendu, rajoutez un accès de la DMZ vers le réseau WAN.

Ainsi, sur l'interface de la DMZ, rajoutez une règle d'accès du réseau

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: DMZ

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

Source

Source: Invert match DMZ net Source Address /

Destination

Destination: Invert match WAN net Destination Address /

Bloquer accès DMZ vers le réseau LAN

Encore sur l'interface de la DMZ, rajoutez la règle suivante mais cette fois-ci avec l'action Block.

Il faut impérativement la journaliser afin de voir les paquets bloquer

Edit Firewall Rule

Action: Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: DMZ

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

Source

Source: Invert match DMZ net Source Address /

Destination

Destination: Invert match LAN net Destination Address /

Extra Options

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Règle de redirection NAT vers serveur web DMZ

Pour que le serveur web soit accessible depuis un réseau externe, nous avons besoin de faire un redirection **NAT** en port forward

The screenshot shows a dark-themed user interface for a network device. At the top, there are tabs: System, Interfaces, Firewall (which is highlighted with a green bar), and Services. Below the tabs is a sidebar with several options: Monitoring, Graph, Aliases, NAT (which is also highlighted with a green bar), Rules, Schedules, Traffic Shaper, and Virtual IPs.

The second screenshot shows a sub-menu under Firewall: NAT: Port Forward. It has tabs for Port Forward, 1:1, Outbound, and NPt. The Port Forward tab is currently selected and highlighted with a green bar.

Paramétrer bien la règle comme ceci :

This screenshot displays the detailed configuration for a port forwarding rule. The fields are as follows:

- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** (button labeled "Display Advanced")
- Destination:** 192.168.10.10 (CARP WAN)
- Destination port range:** HTTP (From port: Custom, To port: Custom) - This field is highlighted with a green border.
- Redirect target IP:** 192.168.200.1
- Redirect target port:** 80 (Port: Custom)

Il faut mettre en place une règle de redirection

Description: Redirect WAN to WebServer HTTP
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync: Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being applied.

NAT reflection: Use system default

Filter rule association: Add associated filter rule
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the selected WAN.

Save

Ainsi , nous pouvons effectuer nos test de ping

```
root@secciv-web:/home/sysadmin# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    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
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    link/ether 00:0c:29:b8:9e:a0 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.200.1/24 brd 192.168.200.255 scope global ens33
        valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:feb8:9e%ens33 brd fe80::ff:fe%ens33 scope link
            valid_lft forever preferred_lft forever
root@secciv-web:/home/sysadmin# ping 192.168.100.254
PING 192.168.100.254 (192.168.100.254) 56(84) bytes of data.
^C
--- 192.168.100.254 ping statistics ---
27 packets transmitted, 0 received, 100% packet loss, time 26636ms
root@secciv-web:/home/sysadmin#
```

Ici ça ne passe pas de la DMZ vers le LAN

```
C:\Users\Administrator>ipconfig
Configuration IP de Windows

Carte Ethernet Ethernet0 :
    Suffixe DNS propre à la connexion. . . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::b0a1:602f:a4d8:b8a9%9
    Adresse IPv4. . . . . : 192.168.100.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.100.254

C:\Users\Administrator>ping 192.168.200.254
Envoi d'une requête 'Ping' 192.168.200.254 avec 32 octets de données :
Réponse de 192.168.200.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.200.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Users\Administrator>
```

Et là ça passe du LAN vers la DMZ

7.1.1) E-Brigade

Faire l'installation de base d'un débian en mettant tous à jours

```
$ sudo apt update && sudo apt upgrade -y
```

Ensute il faut attribuer une IP statique au serveur

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address
    netmask
    gateway
```

Address : 192.168.101.123

Netmask : 255.255.255.0

Gateway : 192.168.101.254

Une fois la config IP terminé on restart le service

```
sudo systemctl restart networking.service
```

Vous pouvez avoir besoin de relancer la carte réseau, fait le avec la commande suivante

```
sudo ifup ens33
```

On peut vérifier la configuration IP avec un IP show.

A présent, on va lancer l'installation de tous les services nécessaires au fonctionnement de E-brigade

```
sudo apt install php-mysql php-mbstring php-gd
```

On peut désormais tester si on accède bien à la DMZ depuis un LAN en y renseignant l'ip du serveur



Configuration de MariaDB

Le logiciel e-brigade nécessite une base de données, ainsi pour procéder à l'installation de la base de données, lancez la commande suivante.

```
sudo apt install mariadb-server
```

Faites les étapes suivantes

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

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

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

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
```

Ensuite nous pouvons nous y connecter avec le compte root

Donc la commande à rentrer est Mysql -u root -p
renseignez ensuite le password

```
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.5.18-MariaDB-0+deb11u1 Debian 11

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)]> 
```

On crée une base de données

```
MariaDB [(none)]> CREATE DATABASE ebrigadedb DEFAULT CHARACTER SET latin1 COLLATE latin1_general_cs;
Query OK, 1 row affected (0,002 sec)
```

On lui assigne un utilisateur et on le créer

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON ebrigadedb.* TO ebrigade@localhost IDENTIFIED BY [REDACTED];
Query OK, 0 rows affected (0,014 sec)
```

Installation de E-brigade

E-brigade n'est actuellement plus disponible, de ce fait nous sommes partie sur une version antérieur au format zip

Nous avons donc configuré le protocole scp qui effectuera un transfert par SSH

```
C:\Users\alex>scp ebrigade_5_2_0.zip brigade@192.168.101.84:/home/brigade_
```

On renseigne le mot de passe de la VM

On unzip le document qu'on vient de transferer

```
unzip ebrigade_5.2.0.zip
```

Ensuite on déplace le dossier dans /var/www avec la commande mv ebrigade /var/www

```
sudo mv ebrigade /var/www/  
ls  
ls -l /var/www
```

```
drwxr-xr-x 11 sysadmin sysadmin 20480 1 sept. 2019 ebrigade  
drwxr-xr-x 2 root root 4096 30 mars 17:22 html
```

Ensuite, nous devons configurer le dossier VirtualHost pour E-brigade dans le fichier /etc/apache2/sites-available/ebrigade.conf

```
<VirtualHost *:80>  
    DocumentRoot /var/www/ebrigade  
    ServerName e-brigade.sec-civile.lan  
    <Directory "/var/www/ebrigade">  
        AllowOverride All  
        Require all granted  
    </Directory>  
</VirtualHost>
```

Activez le site ci-présent avec la commande a2ensite, et par la même occasion de désactiver le site par défaut d'Apache avec la commande a2dissite.

```
sudo a2ensite ebrigade
```

Enabling site ebrigade.

To activate the new configuration, you need to run:
 systemctl reload apache2

```
sudo a2dissite 000-default
```

Site 000-default disabled.

To activate the new configuration, you need to run:
 systemctl reload apache2

Nous devons désormais modifier les droits du dossier E-brigade

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

Enfin, on redémarre apache pour accéder au service

```
sudo systemctl restart apache2
```

Maintenant, on ouvre un navigateur web en renseignant l'ip du serveur e-brigade

Configuration Base de données

Paramètres de connexion à la base de données

Server Name	localhost
User	ebrigade
Password	*****
Database name	ebrigadedb

valider

Procédez à la configuration et initialisation de la base de données en renseignant les identifiants configurés précédemment.

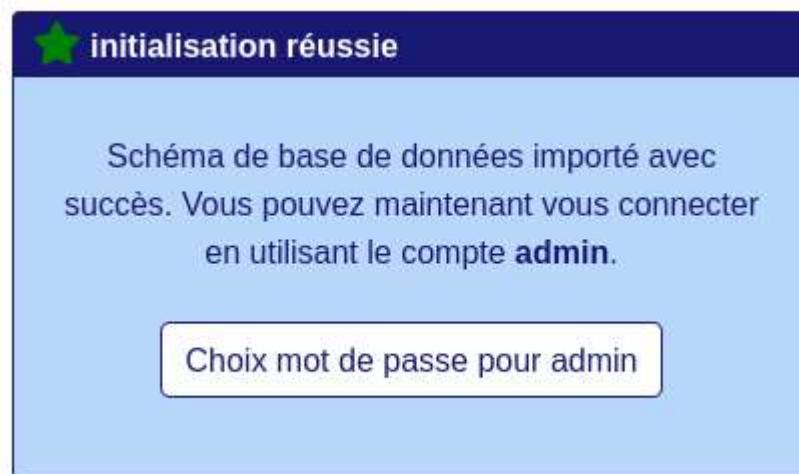
Configuration Base de données

Paramètres de connexion à la base de données

Server Name	localhost
User	ebrigade
Password	*****
Database name	ebrigadedb

valider

La configuration de la base de données est réussie, ensuite définissez le mot de passe du compte admin d'e-brigade en cliquant sur Choix mot de passe pour admin.



On définit le mot de passe et on clique sur sauver



A dialog box titled "Mot de passe eBrigade" featuring a key icon. It contains a message: "Veuillez choisir un mot de passe personnel." Below is a form for entering a password:

Pour admin	
Nouveau mot de passe	*****
Répétez	*****

The message continues below the form: "us de sécurisé, choisissez un mot de passe encore p". At the bottom are two buttons: "sauver" and "annuler".



Ici on renseigne les identifiants précédemment créer

L'accès à l'interface web est OK et l'installation s'est déroulé sans soucis.

8.1.1) Installation d'asterisk

Une fois l'installation de base terminé, veuillez redémarrer, on ouvre le terminal et on se connecte en root pour update et upgrade le server

```
Debian GNU/Linux 11 debian tty1

debian login: root
Password:
Linux debian 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~# apt update_
```

```
root@debian:~# apt update
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
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.
root@debian:~# _
```

```
root@debian:~# apt upgrade
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.
root@debian:~# _
```

On va commencer à installer asterisk, ici deux options, soit nous utilisons l'option vmware tool et un glisser déposer avec une interface en GNU
Ou alors avec la méthode ci-dessous.

```
root@debian:~# apt install -y asterisk asterisk-core-sounds-fr asterisk-mp3 asterisk-mysql_
```

Ensuite on s'assure que Asterisk au démarrage

```
root@debian:~# systemctl enable asterisk
```

Une fois que la commande est faite on redémarre pour vérifier que ça se lance bien au début

```
● asterisk.service - Asterisk PBX
  Loaded: loaded (/lib/systemd/system/asterisk.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2023-03-27 09:00:07 CEST; 2min 30s ago
```

Maintenant rendons nous dans /etc/network/interface avec un nano

on modifie l'ip comme prévu

```
# The second network interface
allow-hotplug ens36
iface ens36 inet static
    address
    netmask
    gateway
```

Address : il faut mettre l'adresse IP LAN soit 192.168.101.79 dans notre cas

Netmask : 255.255.255.0 soit un /24

Gateway : 192.168.101.254 l'adresse du routeur 1

Ensuite, nous devons configurer le fichier sip.conf

```
root@debian:~# nano /etc/asterisk/sip.conf
```

Ligne 333 on enlève le ; ce qui désactive donc tous les codecs et on active le codec ulaw

```
;Disallow=all ; First disallow all codecs
;Allow=ulaw ; Allow codecs in order of preference
;Allow=ilbc ; see https://wiki.asterisk.org/wiki/display/AST/RTP+Packetization
;Autoframing=yes ; for framing options
; Set packetization based on the remote endpoint's (ptime)
; preferences. Defaults to no.

;
; This option specifies a preference for which music on hold class this channel
; should listen to when put on hold if the music class has not been set on the
; channel with Set(CHANNEL(musicclass)=whatever) in the dialplan, and the peer
; channel putting this one on hold did not suggest a music class.

[ ligne 333/1622 (20%), col. 2/60 (3%), car. 18736/95257 (19%) ]
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C EmplacementM-U Annuler
^X Quitter ^R Lire fich. ^N Remplacer ^U Coller ^J Justifier ^_ Aller ligneM-E Refaire
```

```
Disallow=all ; First disallow all codecs
Allow=ulaw ; Allow codecs in order of preference
```

```
;mohsuggest=default
;
;parkinglot=plaza ; Sets the default parking lot for call parking
; This may also be set for individual users/peers
; Parkinglots are configured in features.conf
;language=en ; Default language setting for all users/peers
; This may also be set for individual users/peers
;tonezone=se ; Default tonezone for all users/peers
; This may also be set for individual users/peers

;relaxdtmf=yes ; Relax dtmf handling
;trustrpid = no ; If Remote-Party-ID should be trusted
;sendrpid = yes ; If Remote-Party-ID should be sent (defaults to no)
;sendrpid = rpid ; Use the "Remote-Party-ID" header

[ ligne 358/1622 (22%), col. 1/79 (1%), car. 19968/95255 (20%) ]
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C EmplacementM-U Annuler
^X Quitter ^R Lire fich. ^N Remplacer ^U Coller ^J Justifier ^_ Aller ligneM-E Refaire
```

Ici, modifier la langue pour la mettre en français !

Ensuite, rendons nous à la ligne 414 pour activer le dtmfmode

```
;usereqphone = no ; or performing a "hairpin" call.
; If yes, ";user=phone" is added to uri that contains
;a valid phone number
dtmfmode = rfc2833 ; Set default dtmfmode for sending DTMF. Default: rfc2833
; Other options:
; info : SIP INFO messages (application/dtmf-relay)

[ ligne 414/1622 (25%), col. 1/89 (1%), car. 24576/95254 (25%) ]
^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C EmplacementM-U Annuler
^X Quitter ^R Lire fich. ^N Remplacer ^U Coller ^J Justifier ^_ Aller ligneM-E Refaire
```

Enfin à la ligne 423 pour activer le videosupport

```
;compactheaders = yes ; send compact sip headers.
;
videosupport=yes ; Turn on support for SIP video. You need to turn this
; on in this section to get any video support at all.
; You can turn it off on a per peer basis if the general
; video support is enabled, but you can't enable it for
; one peer only without enabling in the general section.
; If you set videosupport to "always", then RTP ports will
; always be set up for video, even on clients that don't
; support it. This assists callfile-derived calls and
; certain transferred calls to use always use video when

[ ligne 423/1622 (26%), col. 1/86 (1%), car. 25119/95253 (26%) ]
```

8.1.2) Création des utilisateurs :

Il faut aller dans le fichier /etc/asterisk/users.conf

```
[1101]
type=friend
secret=1234
host=dynamic
context=finance
callerid=dylan <1101>

[1102]
type=friend
secret=1234
host=dynamic
context=finance
callerid=aline <1102>
-
[ ligne 128/128 (100%), col. 1/1 (100%), car. 2736/2736 (100%) ]
^G Aide      ^O Écrire    ^W Chercher   ^K Couper     ^T Exécuter   ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich. ^Y Remplacer   ^U Coller     ^J Justifier  ^L Aller ligne M-E Refaire
```

[1101] fait office du numéro du poste à appeler

Type est le type d'objet SIP , ici friend

Secret est le mot de passe de connexion

Host est sur dynamique car l'user n'est pas associé à une IP fixe

Context est sur finance car c'est l'intitulé de sa fonction

Callerid = nom <numéro> pour associer le nom au numéro

```
root@debian:/etc/asterisk# systemctl restart asterisk.service_
```

On restart le service.

Nous pouvons regarder les sip que l'on vient de créer avec la commande

```
debian*CLI> sip show peers
Name/username          Host                               Dyn Forcerport Comedia    ACL Port
Status     Description
1101        (Unspecified)                                D  Auto (No)  No           0
        Unmonitored
1102        (Unspecified)                                D  Auto (No)  No           0
        Unmonitored
2 sip peers [Monitored: 0 online, 0 offline Unmonitored: 0 online, 2 offline]
debian*CLI> _
```

On peut aussi reload avec la commande : sip reload.

8.1.3) Crédation des boîtes vocales

Pour la configuration des boîtes vocales il faut aller dans /etc/asterisk/voicemail.conf

Et on va ajouter les lignes ci-dessous

```
[finance]
1101 => ,dylan
1102 => ,aline_
```

Ensuite, nous devons nous rendre dans /etc/asterisk/extensions.conf

```
[finance]
exten => _110X,1,Dial(SIP/${EXTEN},20)
exten => -110X,2,Hangup()
```

On appelle un poste qui commande par 110 suivis du X qui est le numéro du poste, on prend l'appel et ça sonne pendant 20 secondes

A la fin des 20s on a mis un hangup qui raccroche automatiquement, on va maintenant configurer la boîte vocal On va modifier la ligne hangup qui est pour raccroché, on a mis VoiceMail, pour passer sur la boîte vocale, la troisième ligne est le numéro 888, pour accéder à sa boîte vocal, enfin on enregistre le fichier de configuration

```
[finance]
exten => _110X,1,Dial(SIP/${EXTEN},20)
exten => -110X,2,VoiceMail(${EXTEN}@finance)

exten => 888,1,VoiceMailMain(${CALLERID(num)}@finance)
```

8.1.4) Utilisation d'un softphone

Pour réaliser les tests, je vais avoir besoin d'un softphone et pour ce faire je vais utiliser linphone qui est open source

On l'installe sur Windows et on le lance

Sur la page d'accueil on va créer un compte SIP



On renseigne les infos comme avec les user précédemment créer

UTILISER UN COMPTE SIP

Nom d'utilisateur	Nom d'affichage (optionnel)
<input type="text" value="1101"/>	<input type="text" value="Dylan"/>
Domaine SIP	
<input type="text" value="192.168.100.20"/>	
Mot de passe	
<input type="password" value="****"/>	
Transport	
<input type="button" value="UDP"/> ▼	
<input type="button" value="RETOUR"/>	<input type="button" value="UTILISER"/>

Ensuite on fait OK en laissant par défaut

Faire de même avec le second user

UTILISER UN COMPTE SIP

Nom d'utilisateur	Nom d'affichage (optionnel)
<input type="text" value="1102"/>	<input style="border: 2px solid orange;" type="text" value="Aline"/>
Domaine SIP	
<input type="text" value="192.168.100.20"/>	
Mot de passe	
<input type="text" value="*****"/>	
Transport	
<input type="text" value="UDP"/> ▼	
RETOUR UTILISER	

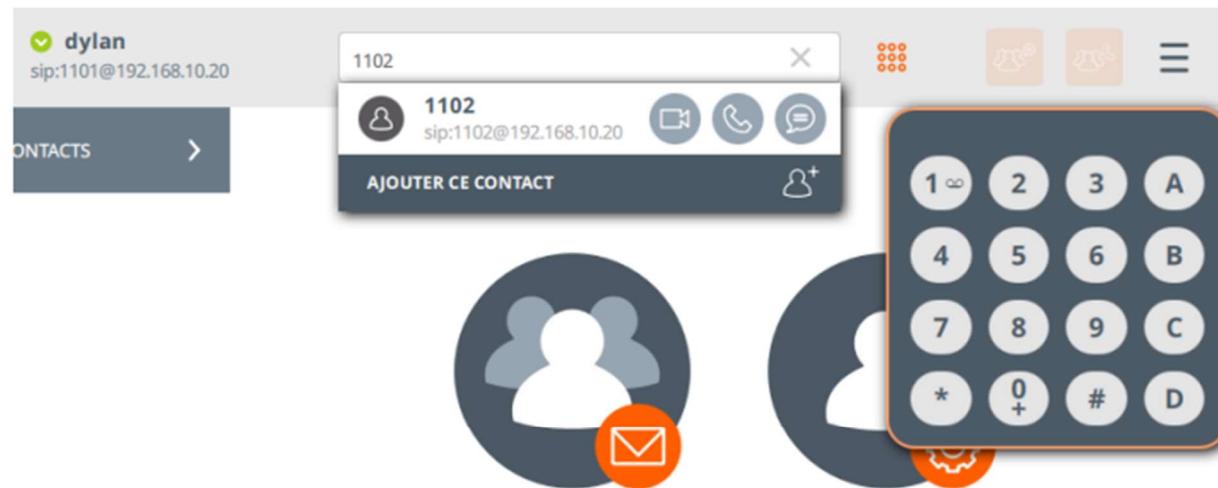


Figure 36

Maintenant la vue du PC de Aline



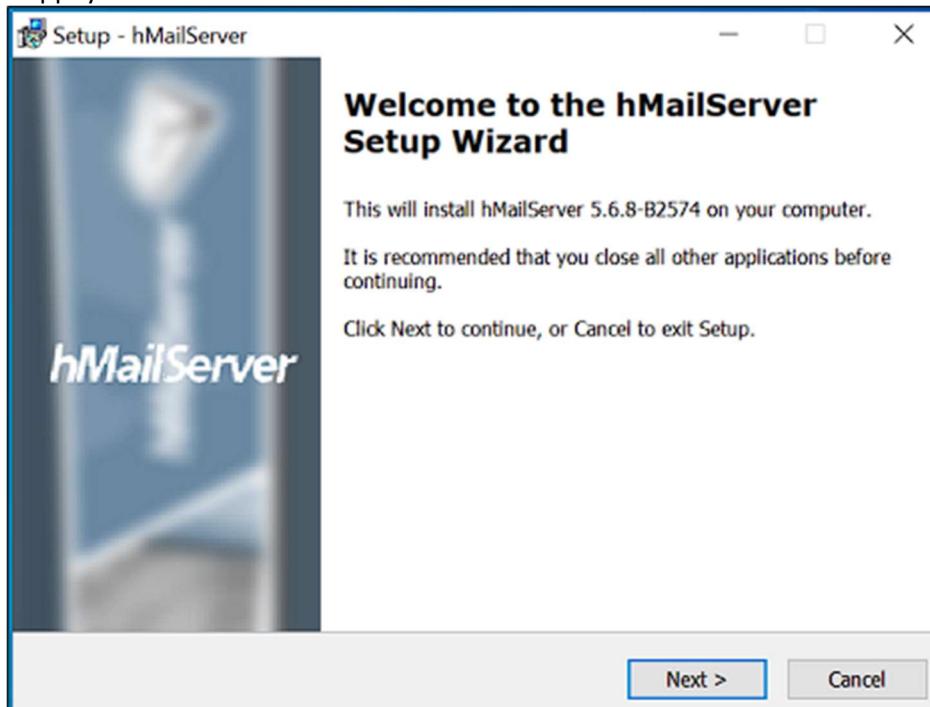
9.1.1) installation de Hmailserver

HmailServer Pour installer le serveur de messagerie HmailServer, veuillez tout d'abord télécharger l'outil d'installation de HmailServer via le lien suivant : <https://www.hmailserver.com/download>, et récupérer la dernière version disponible sur le site officiel :

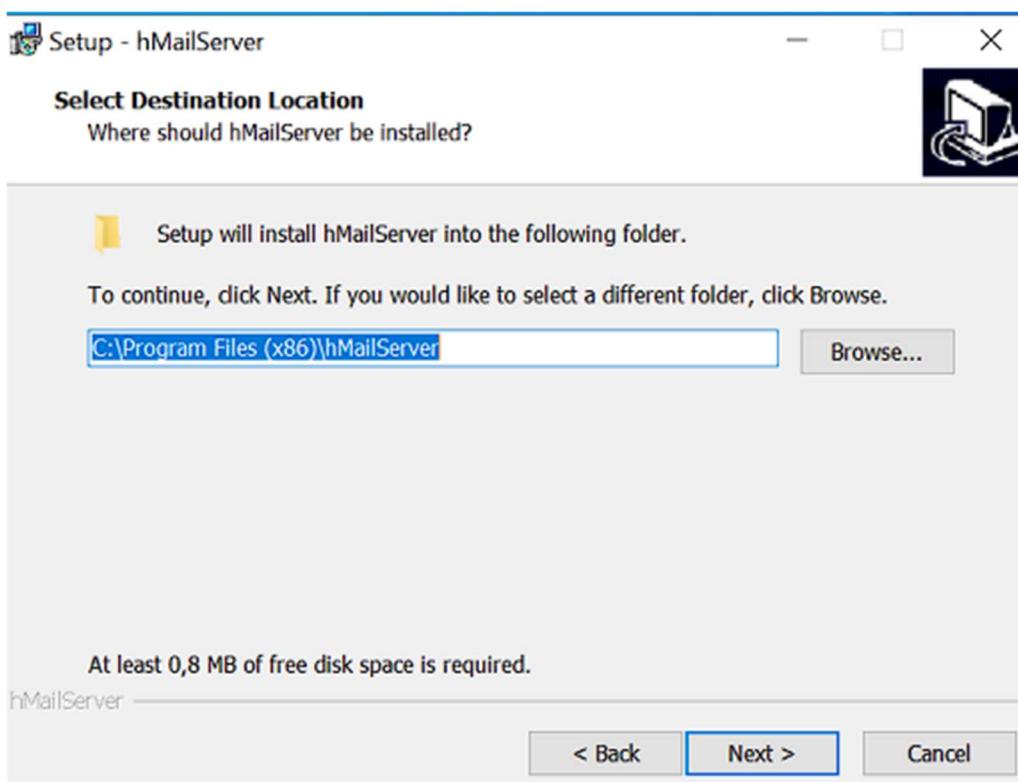
The screenshot shows the 'Download' section of the hMailServer website. A red box highlights the 'Download' button in the top navigation bar. Below it, the 'Latest version' section is shown with a link to 'Download hMailServer 5.6.8 - Build 2574'. A note indicates there have been 193724 downloads since 2021-10-03. A 'Change log' link is also present. Below this, the 'Betas & other downloads' section shows a link to 'Download hMailServer 5.6.9 - Build 2602 (BETA)' with 12709 downloads since 2022-07-22, and a 'Change log' link. A note at the bottom states it's possible to download older releases from the archive download page.

Lors de l'installation, il est demandé de télécharger et installer Microsoft .NET Framework 2.0, nécessitant ainsi d'avoir un accès Internet. Ainsi, afin de simuler un contexte réel, vous pouvez soit mettre en place une passerelle pour avoir accès à Internet (pfSense ou OPNSense), soit configurer la carte réseau du serveur pour avoir directement accès à Internet (Bridge ou en NAT). Pour l'installation, suivez les étapes suivantes :

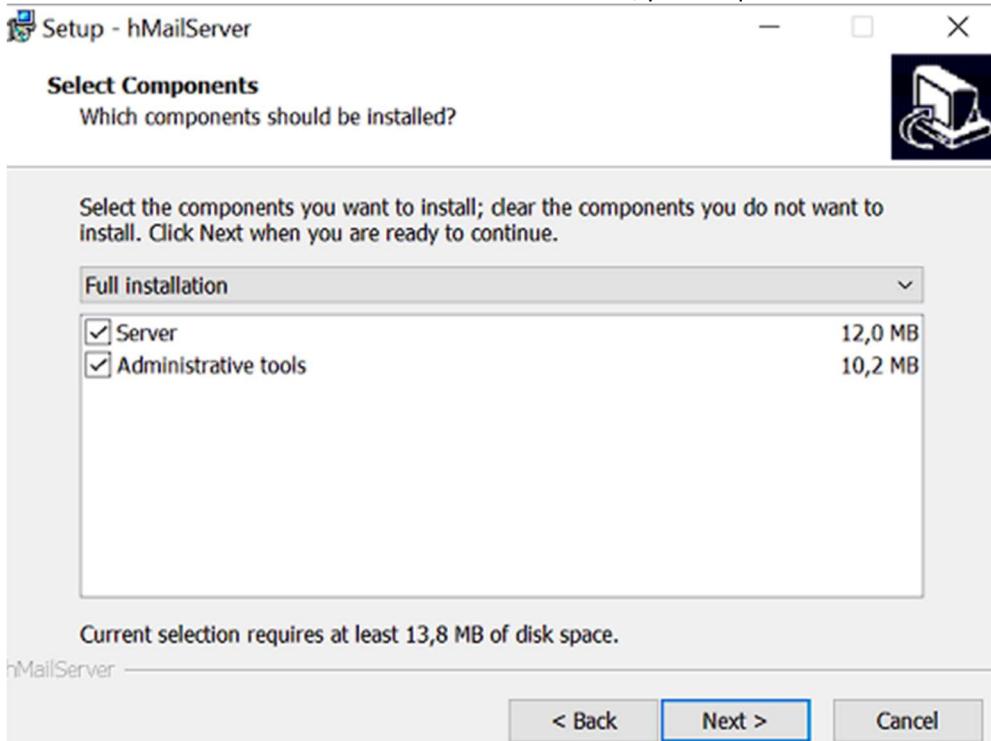
- Appuyez sur **Next**



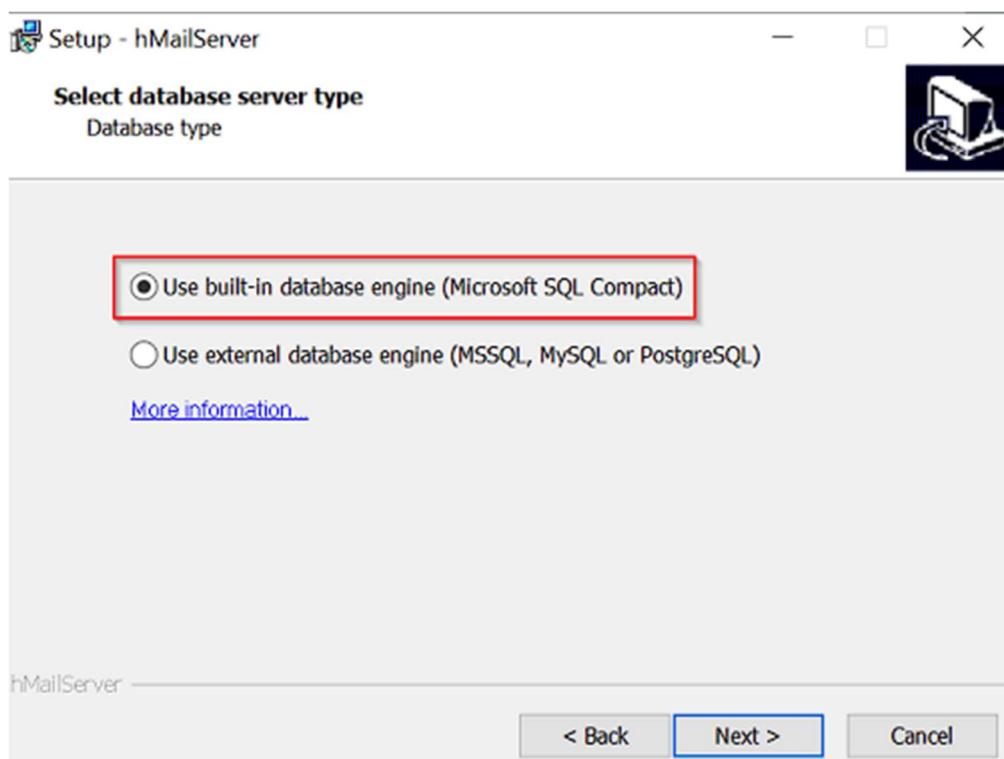
Saisissez le chemin de destination de l'installation ou laissez par défaut puis cliquez sur **Next**



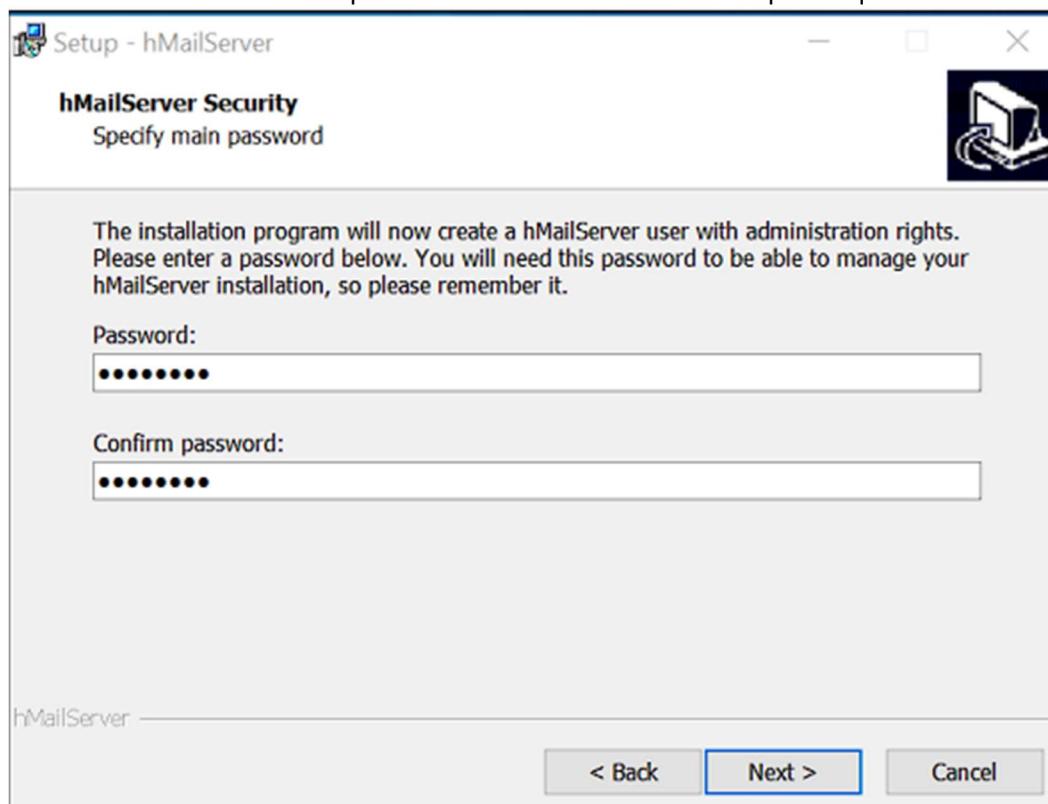
- Choisissez le mode d'installation en Full installation, puis cliquez sur **Next**



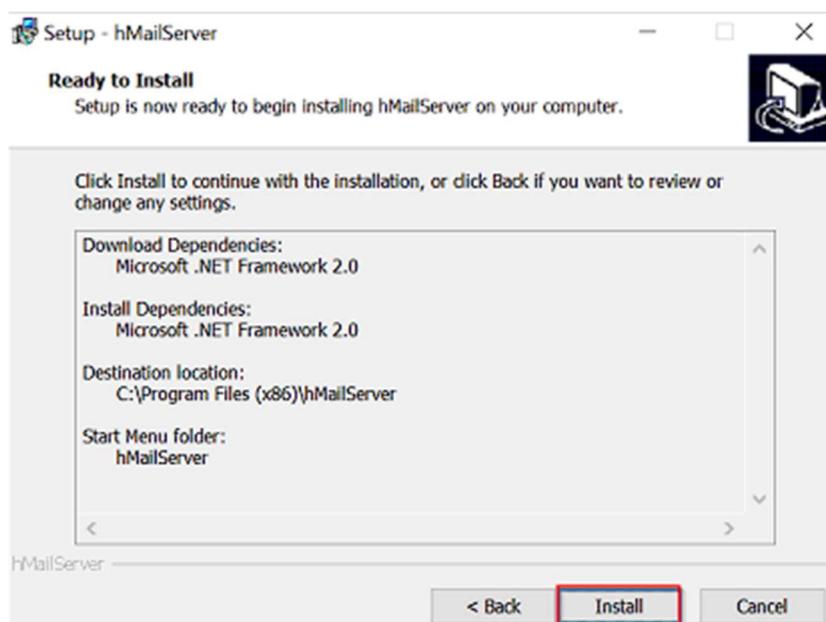
Laissez le type de serveur de base de données par défaut (Microsoft SQL Compact) puis cliquez sur **Next**.



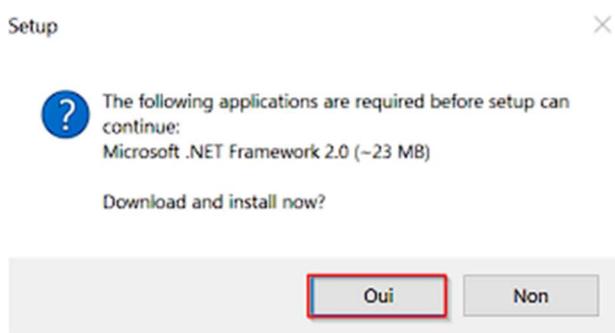
Définissez ensuite le mot de passe de l'administrateur de hmail puis cliquez sur **Next**.



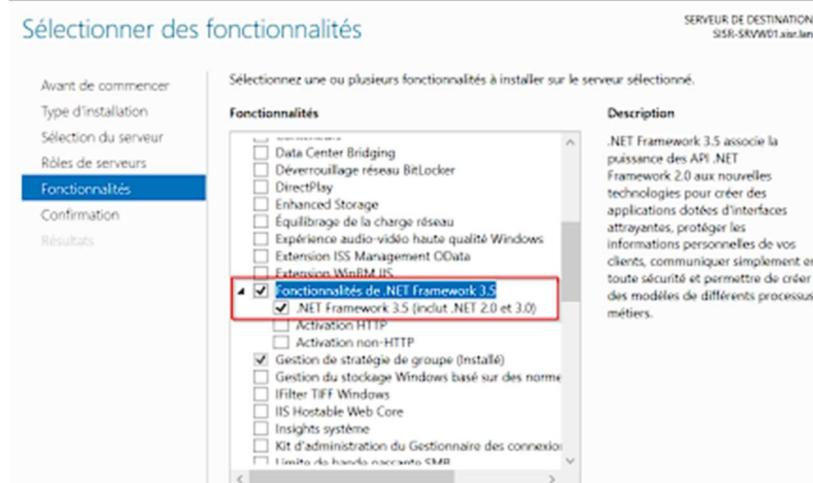
Cliquez sur **Install** pour lancer l'installation



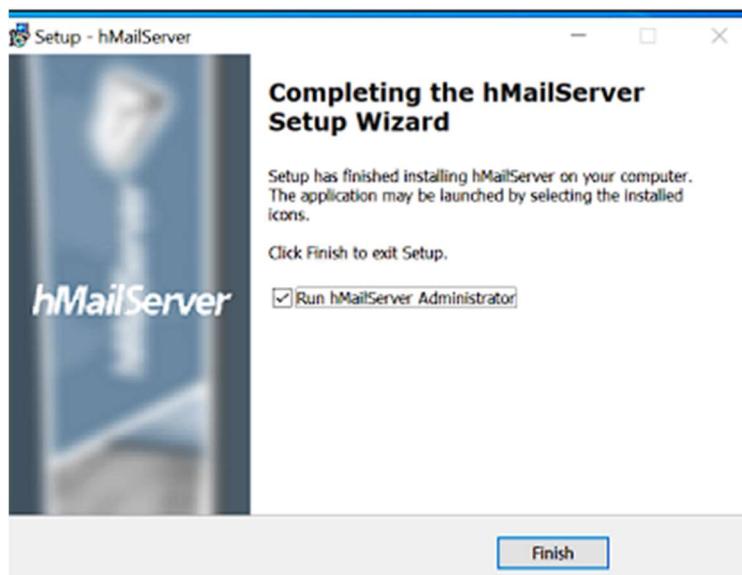
L'utilitaire vous demandera d'installer les dépendances Microsoft .NET Framework 2.0 pour le bon fonctionnement du serveur de messagerie, cliquez sur Oui pour l'installer.



En cas d'erreur, notamment lorsque nous sommes sous Windows Server, rajoutez les fonctionnalités manuellement depuis le Gestionnaire de serveur → Ajout des rôles et fonctionnalités → Fonctionnalités, puis sélectionnez Fonctionnalités de .NET Framework 3.5.



Cliquez enfin sur Finish pour terminer l'installation et lancez l'administration du serveur HmailServer

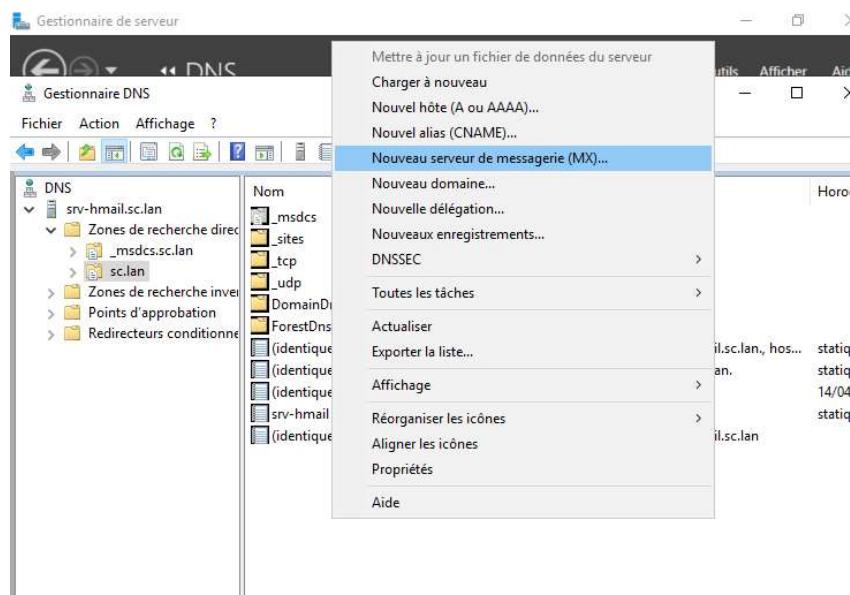


L'installation est à présent achevée, nous pouvons passer à la configuration du serveur de messagerie.

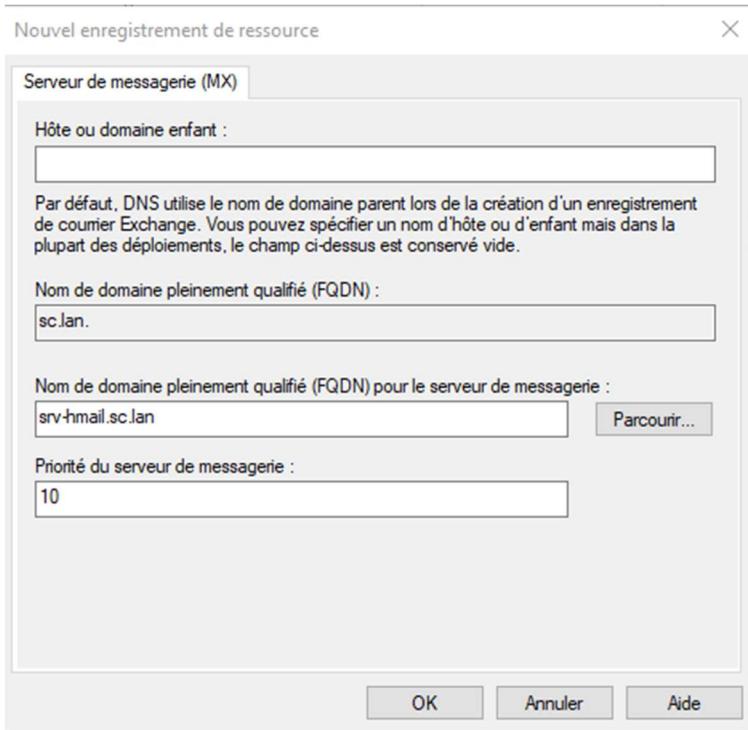
I- Configuration de HmailServer

Avant toute configuration du serveur de messagerie, nous allons rajoutez une entrée DNS de type MX pointant vers le nom du serveur où nous avons installé le serveur hmailServer. Dans notre cas donc, ce sera une entrée DNS sur l'adresse du serveur AD que nous avions installé hmailServer.

- 1- Ajout d'une entrée DNS MX Pour ce faire, dans le gestionnaire de DNS, effectuez un clic-droit sur les zones de recherches directes, puis cliquez sur Nouveau serveur de messagerie (MX) :



Remplissez ensuite le nom FQDN du serveur hébergeant le service de messagerie

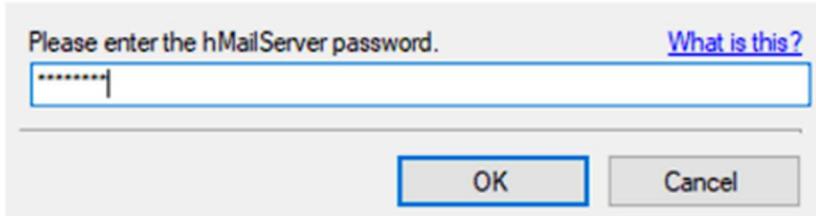


Pour informations, il est important de savoir qu'une entrée DNS MX définit le serveur qui est responsable de courriels sur un domaine donné.

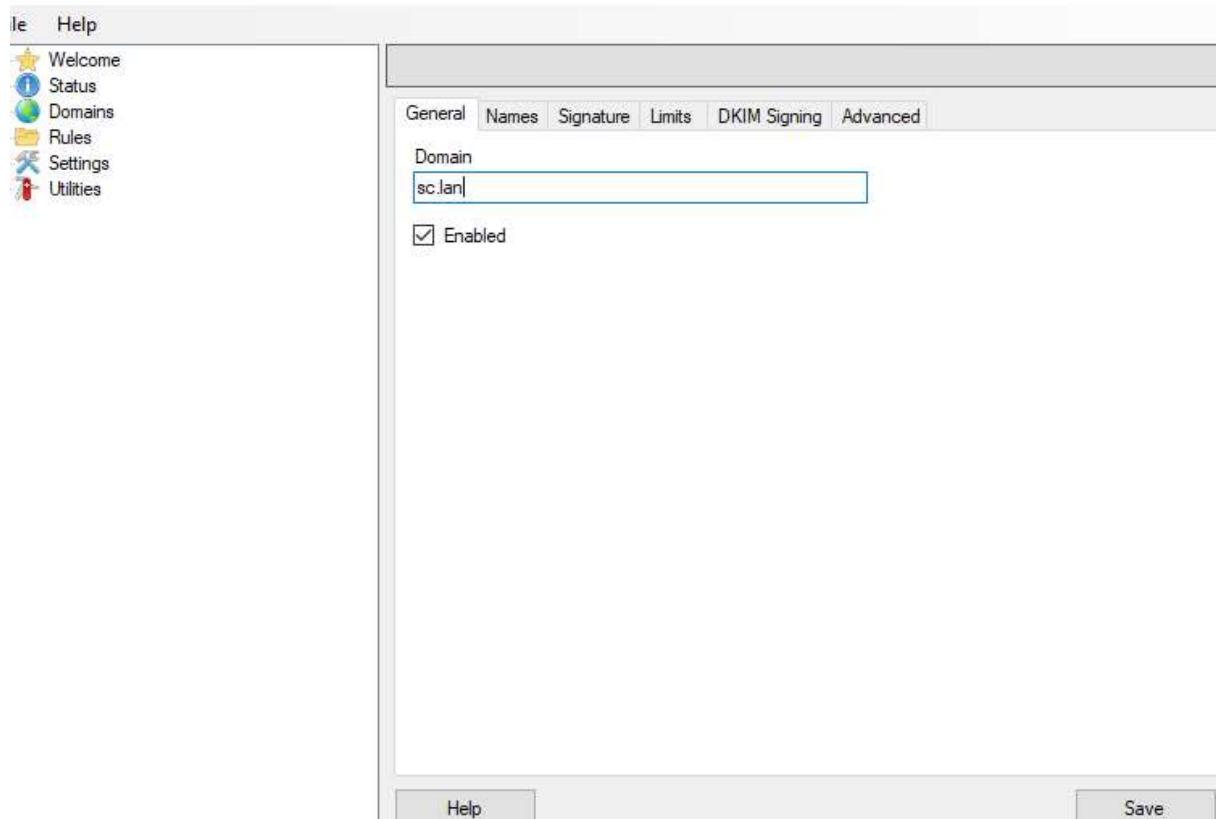
2- Configuration du serveur HmailServer

A présent, nous allons passer à la configuration de hmailServer en ouvrant tout d'abord hmailServer Administrator. Puis, renseignez le mot de passe de l'administrateur renseignée lors de l'installation.

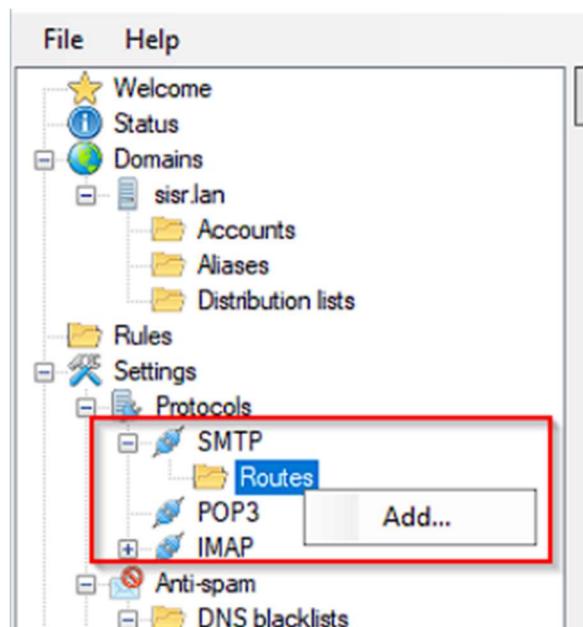
hMailServer password



Ensuite, pour lier le serveur de messagerie au serveur d'annuaire, cliquez sur Domains, et rajoutez le nom de votre domaine Active Directory, puis cliquez sur Save.



Le domaine ajouté, nous allons à présent paramétriser le protocole SMTP en effectuant un clic-droit sous Routes, puis cliquez sur Add.



Renseignez ensuite les informations du domaine, l'adresse IP de l'hôte SMTP, (l'adresse IP du serveur en lui-même), et le port SMTP qui est le port 25. Il est évident qu'en cas d'usage du SSL/TLS sur le protocole SMTP, le numéro de port à renseigner sera différent.

General Addresses Delivery

Domain
sc.lan

Description

Target SMTP host TCP/IP port
10.71.121.13 25

Connection security
None

Renseignez enfin quelques informations sur le serveur SMTP qui se charge de délivrer les courriels, et cliquez sur Save pour sauvegarder les informations renseignées.

SMTP

General Delivery of e-mail Statistics RFC compliance Advanced

Delivery of e-mail

Number of retries Minutes between every retry
4 60

Local host name
SRV-HMAIL

SMTP Relayer

Remote host name Remote TCP/IP port
[] 25

Server requires authentication

User name
[]

Password
[] << Encrypted >>

Connection security
None

⚠ N'oubliez pas de définir le domaine par défaut

Cette dernière configuration est cruciale, notamment si vous voulez utiliser le serveur entrant en IMAP car sans configuration, les noms d'utilisateur lors de la connexion seront uniquement la partie user de la messagerie et non le nom FQDN avec le nom de domaine. Pour le cas de la connexion IMAP, cet oubli de configuration pourrait générer une erreur de connexion erronée.

Pour ce faire, dans l'administration de hmailserver, dans l'onglet Settings → Advanced, puis définissez le domaine et cliquez sur Save.

Advanced

General

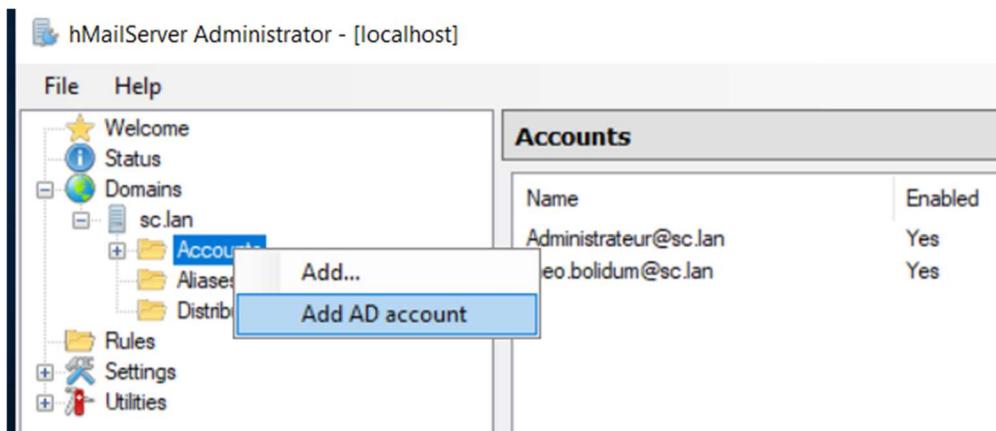
Default domain
sc.lan

Administration password
You need this password to be able to manage your hMailServer installation, so please remember it.

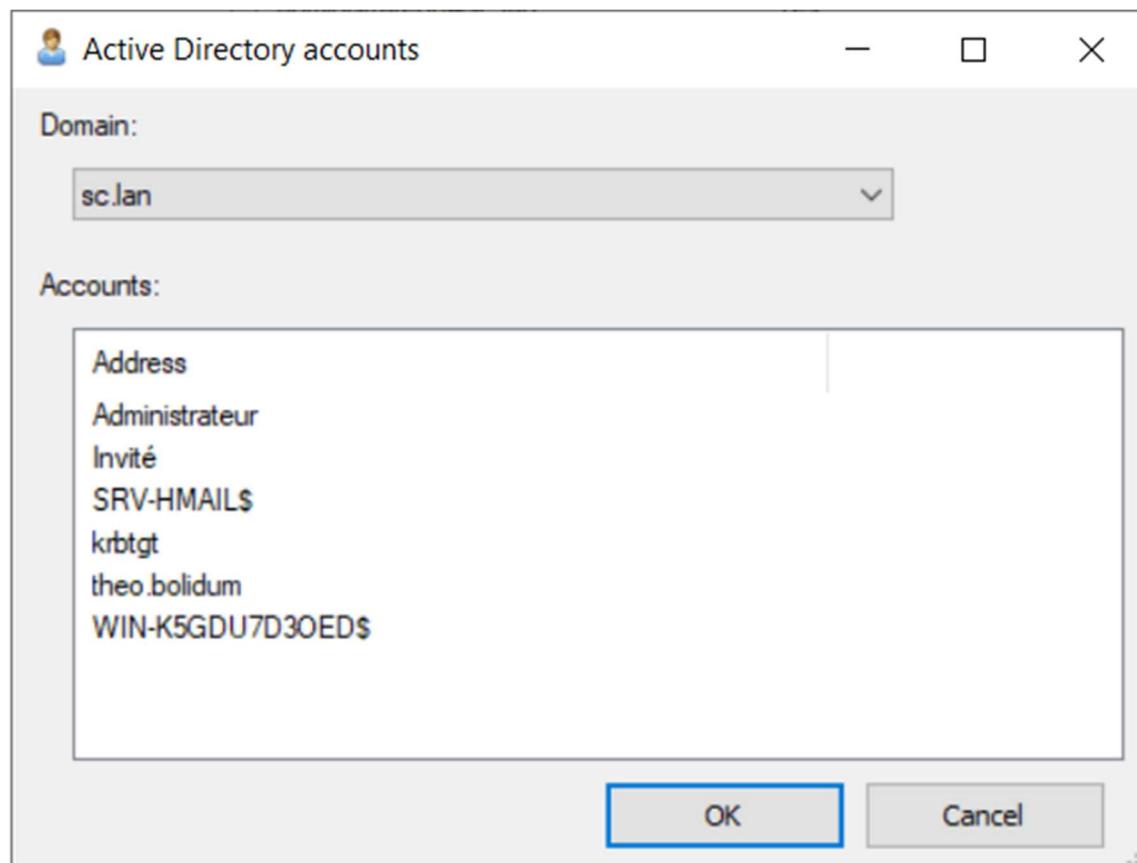
A présent, nous pouvons nous connecter sur une machine cliente pour créer les comptes de messageries et effectuer les tests d'envoi et de réception de courriel électronique.

III- Création des comptes de messagerie

Pour créer les comptes de messageries qui seront liés à la base utilisateur de l'Active Directory, sous Domains → sc.lan → Accounts, effectuez un clic-droit et cliquez sur Add AD account



Ensuite, renseignez le nom du domaine, et sélectionnez un utilisateur pour créer son compte de messagerie.



Name	Enabled
Administrateur@sc.lan	Yes
theo.bolidum@sc.lan	Yes

Les comptes de messagerie sont créés correctement

10.1.1) Installation de Zabbix

Lancer l'installation de base d'un débian 11, faire sudo apt update & upgrade

Ensuite on installe les packages :

```
apt install apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php
libapache2-mod-php7.4 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
libcurl4 libgd3 liblulu5.3-0 libonig5 libsodium23 libxpm4 libxslt1.1 php php-bcmath
php-common php-gd php-ldap php-mbstring php-mysql php-xml php7.4 php7.4-bcmath
php7.4-cli php7.4-common php7.4-gd php7.4-json php7.4-ldap php7.4-mbstring php7.4-
mysql php7.4-opcache php7.4-readline php7.4-xml ssl-cert
```

Pendant l'installation il va démarrer les services automatiquement.

On peut vérifier qu'apache est bien installé avec

```
# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-10-15 08:52:22 UTC; 37min ago
     Docs: https://httpd.apache.org/docs/2.4/
 Main PID: 20506 (apache2)
    Tasks: 6 (limit: 4915)
   Memory: 13.6M
      CPU: 0.000 CPU(s) since start
         CGroup: /system.slice/apache2.service
             └─20506 /usr/sbin/apache2 -k start
                  ├─20508 /usr/sbin/apache2 -k start
                  ├─20509 /usr/sbin/apache2 -k start
                  ├─20510 /usr/sbin/apache2 -k start
                  ├─20511 /usr/sbin/apache2 -k start
                  ├─20512 /usr/sbin/apache2 -k start
                  └─20513 /usr/sbin/apache2 -k start
```

Maintenant, on installe MariaDB

```
apt install mariadb-server mariadb-client
systemctl status mariadb
● mariadb.service - Mariadb 10.5.12 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-10-15 09:34:25 UTC; 7s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
 Process: 22812 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
 Process: 22813 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
 Process: 22815 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR=`cd /usr/bin/../..; /usr/bin/galera_recovery` (code=exited, status=0/SUCCESS)
 Process: 22880 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
 Process: 22882 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 22866 (mariadb)
   Status: "Taking your SQL requests now..."
    Tasks: 20 (limit: 4915)
   Memory: 77.8M
      CPU: 0.000 CPU(s) since start
         CGroup: /system.slice/mariadb.service
             ├─22866 /usr/sbin/mariadb
             ├─22883 /bin/bash /etc/mysql/debian-start
             ├─22885 /usr/bin/mysql_upgrade --defaults-extra-file=/etc/mysql/debian.cnf --version-check
             ├─22886 grep -E -v ^([1-9]had|ERROR (1051|1054|1060|1061|1146|1347|1348))
             ├─22887 logger -p daemon warn -i /tmp/mysql_upgrade-B9xa3D --database=mysql --batch --force
             ├─22907 sh -c '/usr/bin/mysql' --defaults-file=/tmp/mysql_upgrade-B9xa3D --database=mysql --batch --force --silent
             ├─22908 /usr/bin/mysql --defaults-file=/tmp/mysql_upgrade-B9xa3D --database=mysql --batch --force --silent
```

Ensute on se connecte avec le compte root

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

Et on lance ensuite les commandes pour créer la database et l'utilisateur

- ➔ Create database zabbix character set utf8 collate utf8_bin;
- ➔ Grant all privileges on Zabbix.* to zabbix@localhost identified by 'pass';
- ➔ Set global log_bin_trust_function_creators = 1;
- ➔ Quit;

Ensute on installe Zabbix

```
# wget https://repo.zabbix.com/zabbix/6.3/debian/pool/main/z/zabbix-release/zabbix-
release_6.3-1+debian11_all.deb
# dpkg -i zabbix-release_6.3-1+debian11_all.deb
# apt update
```

Ensute on lance l'install de zabbix en GUI

```
# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-
scripts zabbix-agent
```

On import ensuite le schéma de la database dans le nouveau zabbix

- ➔ Zcat /user/share/zabbix-sql-script/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p 'pass' zabbix

Ensute on a besoin de configurer me server Zabbix pour éditer les lignes suivantes

```
vi /etc/zabbix/zabbix_server.conf
```

- ➔ DBHost=localhost
- ➔ DBName=zabbix
- ➔ DBUser=zabbix
- ➔ DBPassword=pass

Ensute on redémarre Apache

```
# systemctl restart apache2
```

Et on démarre Zabbix

```
# systemctl start zabbix-server zabbix-agent
```