

# BTS SIO 2023

Administration des systèmes et des réseaux (E5 – SISR)

ou

Conception et développement d'applications (E5 – SLAM)

PAGE DE PRÉSENTATION DU DOSSIER

N° d'inscription<sup>1</sup> : | 0 | 2 | 2 | 4 | 6 | 2 | 1 | 8 | 4 | 6 | 3 |

NOM : GUELLUY

Prénom : Pascal

|  |   |
|--|---|
| Date de passage <sup>1</sup> : ..... / ..... /2023 | Heure de passage <sup>1</sup> : .....h..... |
|--|---|

## CATEGORIE CANDIDAT<sup>2</sup> (UNE CASE A COCHER)

|   |  |
|---|--|
| <input type="checkbox"/> Scolaire<br><input checked="" type="checkbox"/> Apprenti<br><input type="checkbox"/> Formation professionnelle continue<br><input type="checkbox"/> Expérience professionnelle 3 ans | <input type="checkbox"/> Ex-scolaire<br><input type="checkbox"/> Ex-apprenti<br><input type="checkbox"/> Ex-formation professionnelle continue |
|---|--|

<sup>1</sup>Informations communiquées sur votre convocation envoyée en mars-avril 2022

<sup>2</sup>Informations communiquées sur votre confirmation d'inscription

Tampon de  
l'établissement



## Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

## ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

| DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE  |                          | N° réalisation : 1             |                          |                              |
|--|--------------------------|--------------------------------|--------------------------|------------------------------|
| Nom, prénom : GUELLUY, Pascal  |                          | N° candidat : 02246218463      |                          |                              |
| Épreuve ponctuelle   | <input type="checkbox"/> | Contrôle en cours de formation | <input type="checkbox"/> | Date : ..... / ..... / ..... |
| <b>Organisation support de la réalisation professionnelle</b>  |                          |                                |                          |                              |
| <b>Intitulé de la réalisation professionnelle :</b> Mise en place de Windows Serveur 2016 avec les services AD DS, DNS, DHCP, ainsi que des GPO  |                          |                                |                          |                              |
| <b>Période de réalisation :</b><br>Modalité : <input type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe  |                          | Lieu : Montpellier - Esicad    |                          |                              |
| <b>Compétences travaillées</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau</li> <li><input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau</li> <li><input type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau</li> </ul> |                          |                                |                          |                              |
| <b>Conditions de réalisation<sup>1</sup> (ressources fournies, résultats attendus)</b>   |                          |                                |                          |                              |
| Les ressources ainsi que les différents services installés, sont fonctionnelles et prêt à l'emploi   |                          |                                |                          |                              |
| <b>Description des ressources documentaires, matérielles et logicielles utilisées<sup>2</sup></b>  |                          |                                |                          |                              |
| <ul style="list-style-type: none"> <li>- Documentation</li> <li>- VMware Workstation Pro (clé de licence fournie)</li> </ul>   |                          |                                |                          |                              |
| <b>Modalités d'accès aux productions<sup>3</sup> et à leur documentation<sup>4</sup></b>   |                          |                                |                          |                              |
| https://pascal-guelluy.fr/   |                          |                                |                          |                              |

<sup>1</sup> En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

<sup>2</sup> Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

<sup>3</sup> Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

<sup>4</sup> Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemple schéma complet de réseau mis en place et configurations des services.

**Épreuve E5 - Administration des systèmes et des réseaux (option SISR)****ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle  
(verso, éventuellement pages suivantes)****Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs**

L'entreprise La Compagnie de Formation souhaite s'implanter sur un autre site afin de développer son activité.

Nous avons pour missions d'installer une infrastructure réseau sous Windows Server 2016 avec les services AD DS, DNS, DHCP ainsi qu'un partage de fichier en RAID 5.

J'ai donc répliqué cette tâche via VMware Workstation Pro afin de montrer les actions réalisées pour ce projet en installant un Windows Server 2016 avec les services demandés, ainsi qu'un autre Windows Server 2016 afin d'assurer la continuité des services via leur réPLICATION en cas de panne sur le premier serveur.

Un AD DS a été créé ainsi que groupes et des utilisateurs (fictif) afin de simuler à la tâche réaliser.

Un DNS a été paramétré afin de créer un nom de domaine que les utilisateurs le rejoignent et puisse s'identifier via leur identifiant créé dans l'AD.

Un DHCP a été ajouté afin d'attribuer automatiquement une adresse IP pour chaque utilisateur dans le domaine.

Un Partage de Fichier a été créé sur le serveur afin que les utilisateurs disposent d'un endroit commun sur lequel déposer leur document, les utilisateurs sont attribués à des groupes spécifique afin de limiter leur accès uniquement aux ressources dont ils ont besoin dans leur service.

Des GPO ont été mis en place afin de limiter les interactions des utilisateurs en bloquant par exemple les accès à l'invite de commande ou au panneau de configuration. Des identifiants administrateurs seront requis pour interagir avec ces éléments.

# PPE 1 : Mise en place d'une infrastructure réseau sur Windows Server 2016

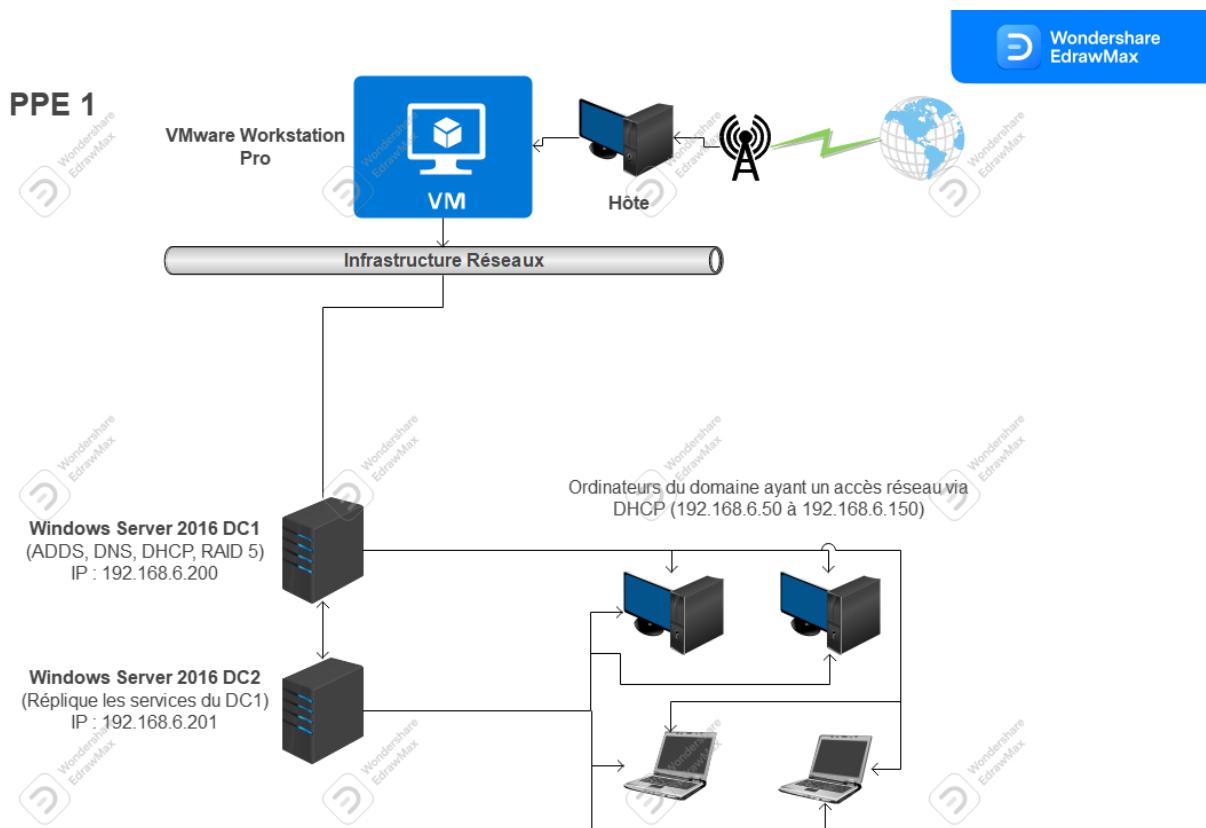
## Sommaire

|       |  |    |
|-------|--|----|
| I)    | Schéma Réseau du projet .....                | 6  |
| II)   | Sconfig .....                                | 7  |
| III)  | Installation des services .....              | 11 |
| IV)   | Configuration de l'AD DS .....               | 13 |
| V)    | Configuration du service DNS .....           | 15 |
| VI)   | Configuration du service DHCP .....          | 19 |
| VII)  | Création d'un dossier partagé en RAID 5..... | 25 |
| VIII) | Création de GPO .....                        | 37 |

## I) Schéma Réseau du projet

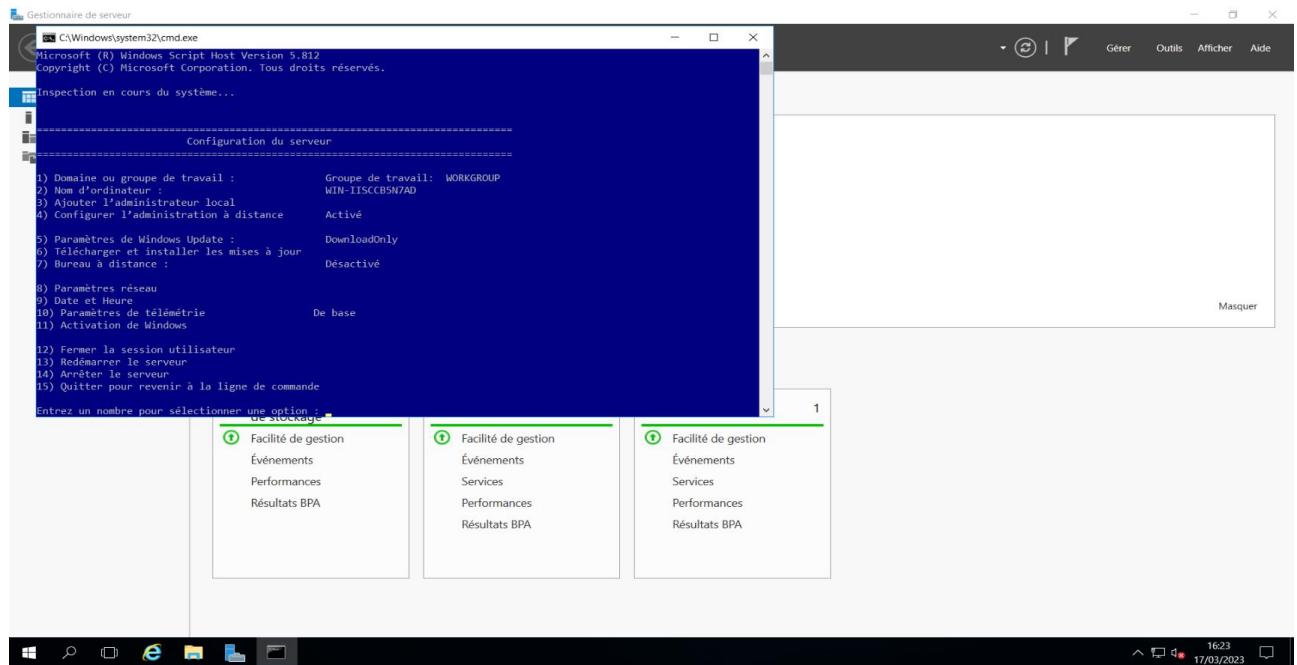
Afin de réaliser notre projet, un schéma réseau a été établis pour bien comprendre ce qui est attendu à travers cette intervention.

Nous passons donc par une machine hôte qui dispose du logiciel VMware Workstation Pro afin d'émuler un Windows Server 2016 en tant que contrôleur de domaine principal avec les services AD DS, DNS, DHCP, avec un RAID 5. Un deuxième Windows Server 2016 est aussi émuler afin d'assurer la continuité des services en cas de panne sur le premier. Quelques machines virtuelles cliente ont aussi été créée afin de s'assurer que les utilisateurs du domaine aient bien accès uniquement aux ressources auquel ils sont censé avoir accès.

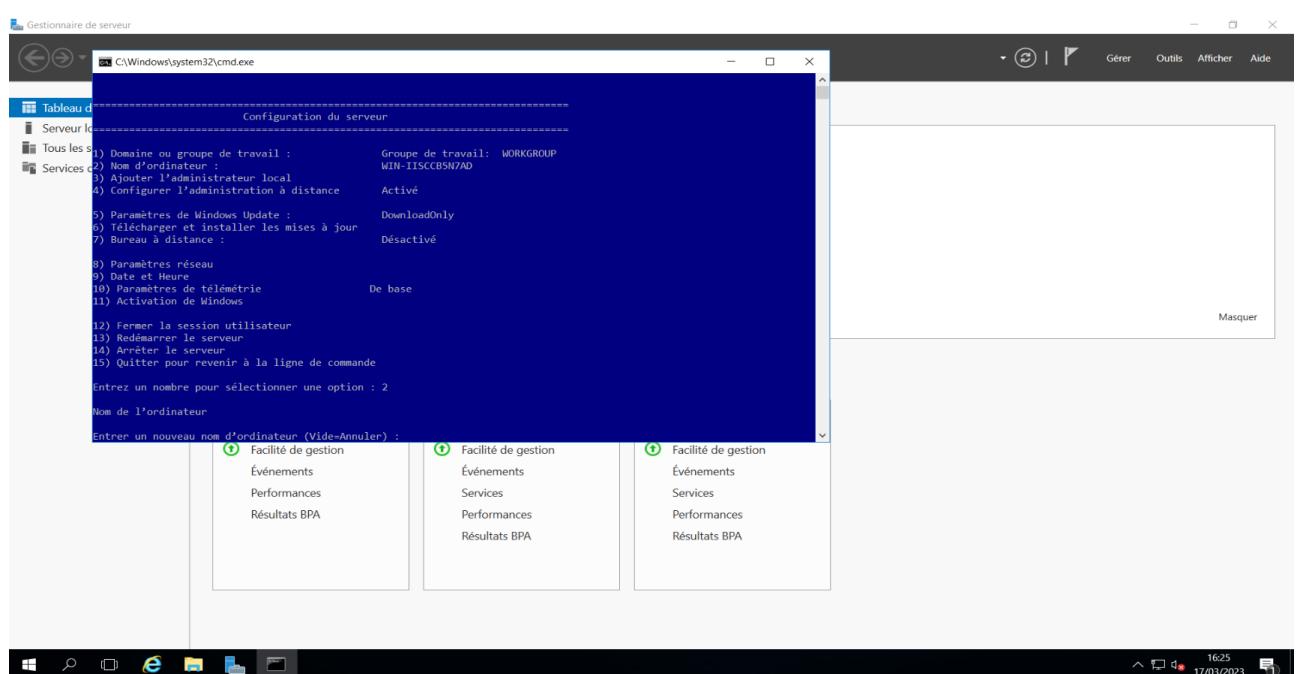


## II) Sconfig

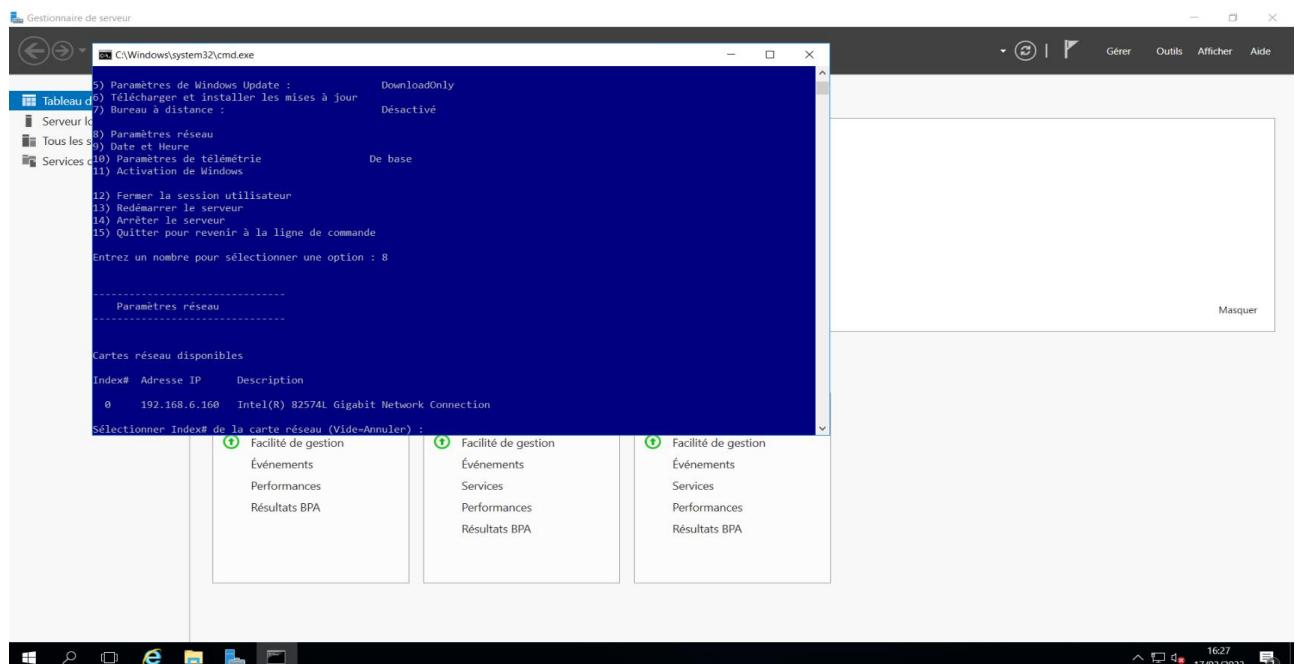
Après avoir installé notre Windows Server 2016, nous devons installer les services désirés afin de les configurer en fonction des normes de l'entreprise. Mais avant cela nous devons configurer les paramètres réseaux de notre Contrôleur de domaine, pour cela nous allons exécuter le programme Sconfig.



Nous allons commencer par renommer notre Contrôleur de Domaine, on appuis donc sur la touche « 2 ».

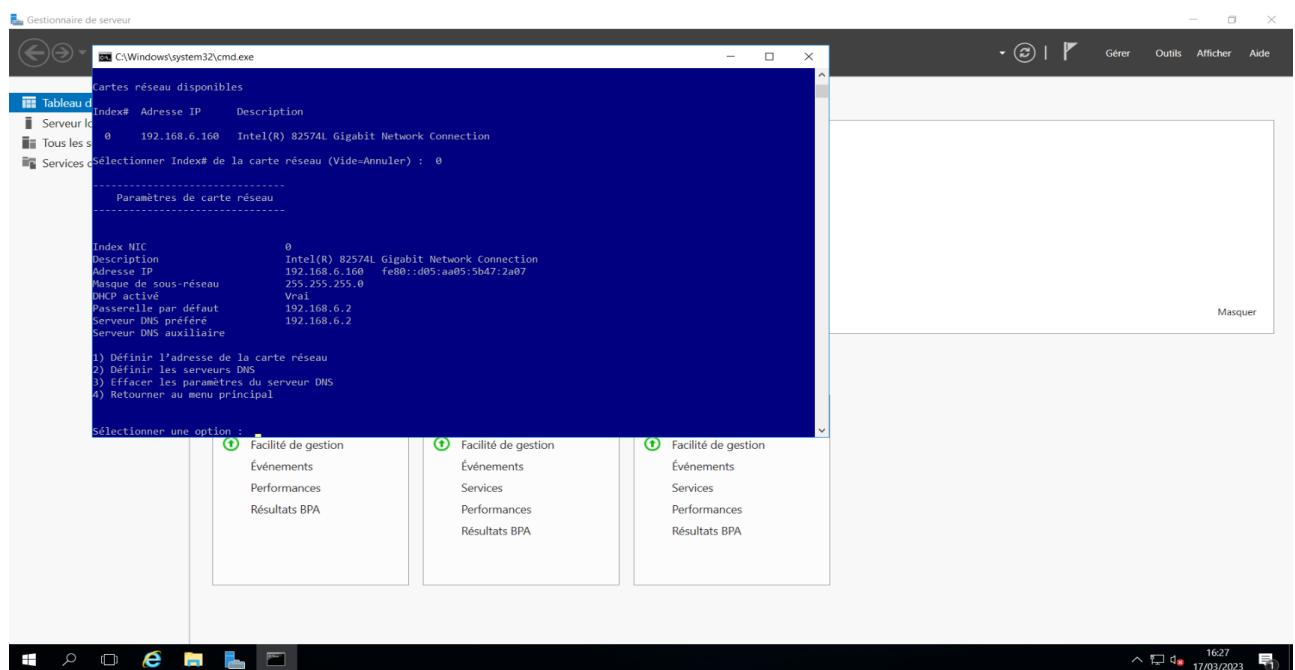


Après avoir renommé notre Serveur, on appuie sur « 8 » afin d'accéder aux paramètres réseaux.

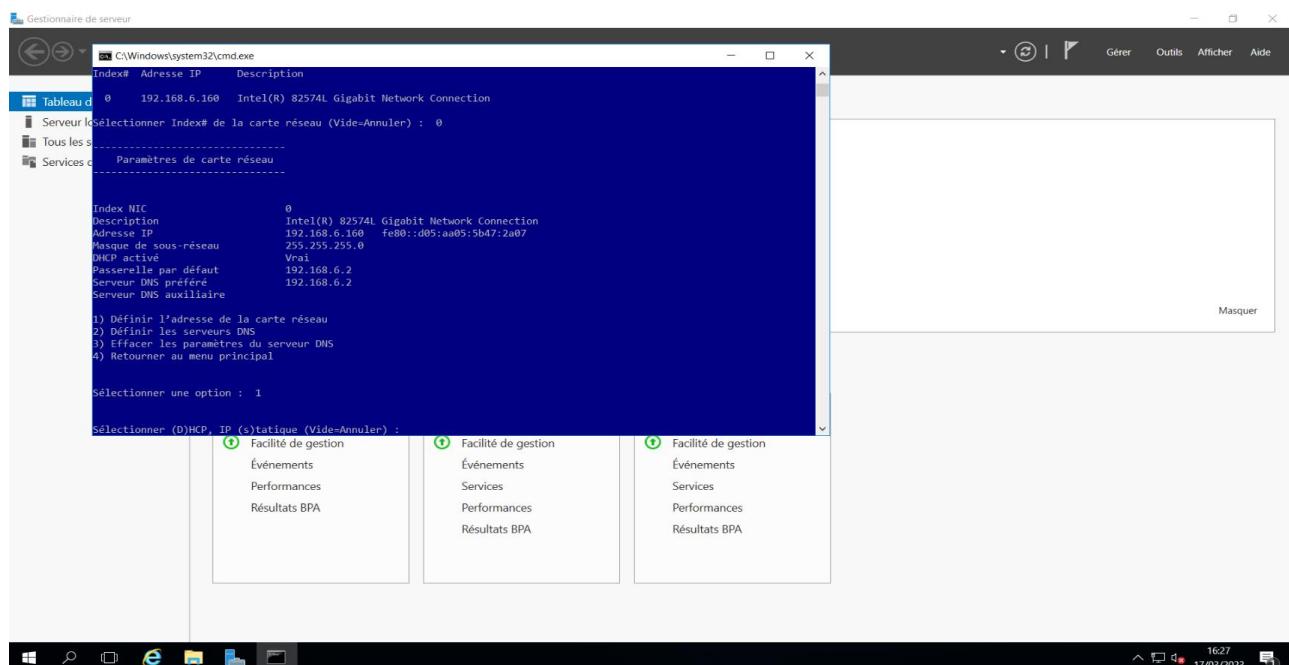


On sélectionne notre carte réseau en appuyant sur le chiffre correspondant (ici 0).

Ensuite nous arrivons sur cette interface.



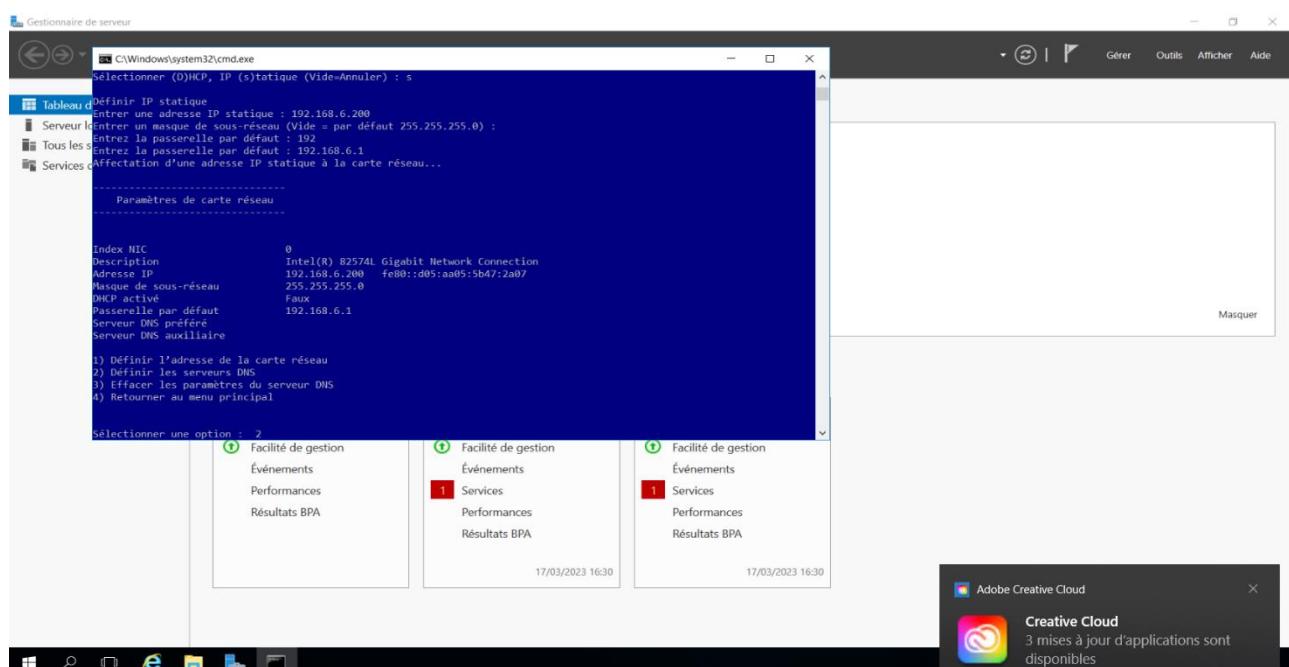
D'ici on appuie sur « 1 » afin de paramétrer l'adresse IP de notre serveur.



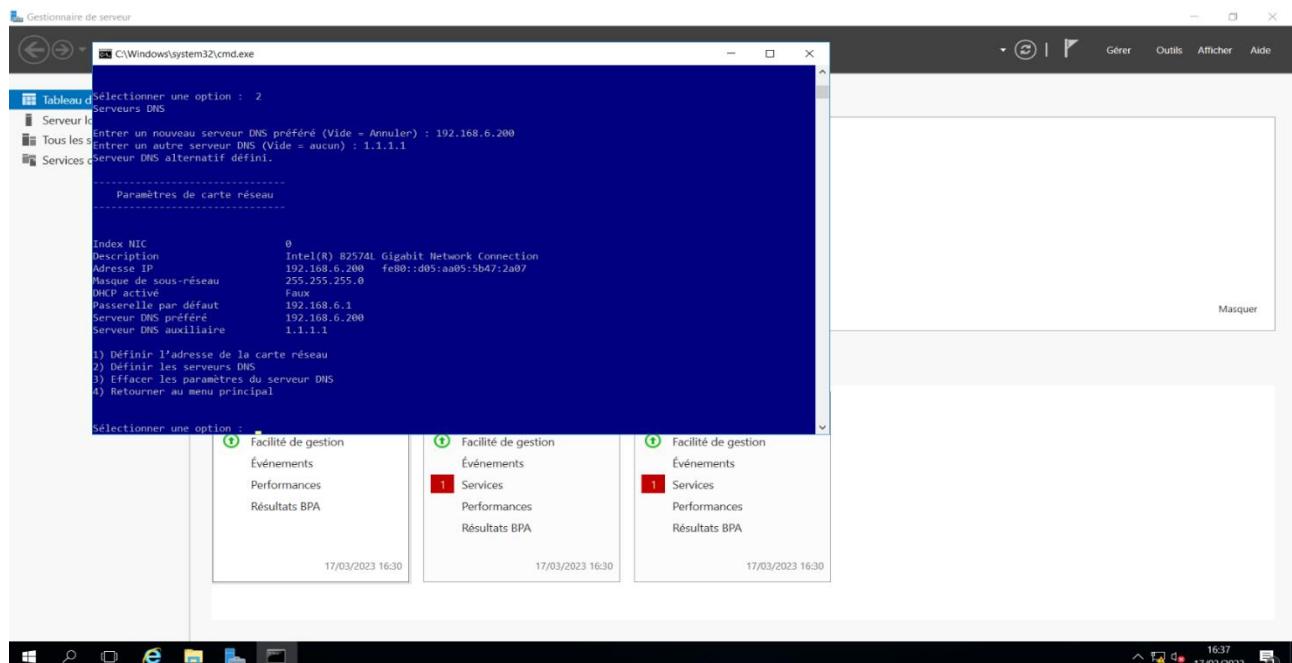
On nous propose alors le choix entre une adresse attribué par DHCP ou une adresse IP statique rentré manuellement, on choisit de lui attribuer une IP statique.

On suit la procédure jusqu'à avoir configuré entièrement notre réseau.

Il reste maintenant les DNS à configurer, on appuie donc sur 2.



On paramètre nos serveurs DNS comme ceci.

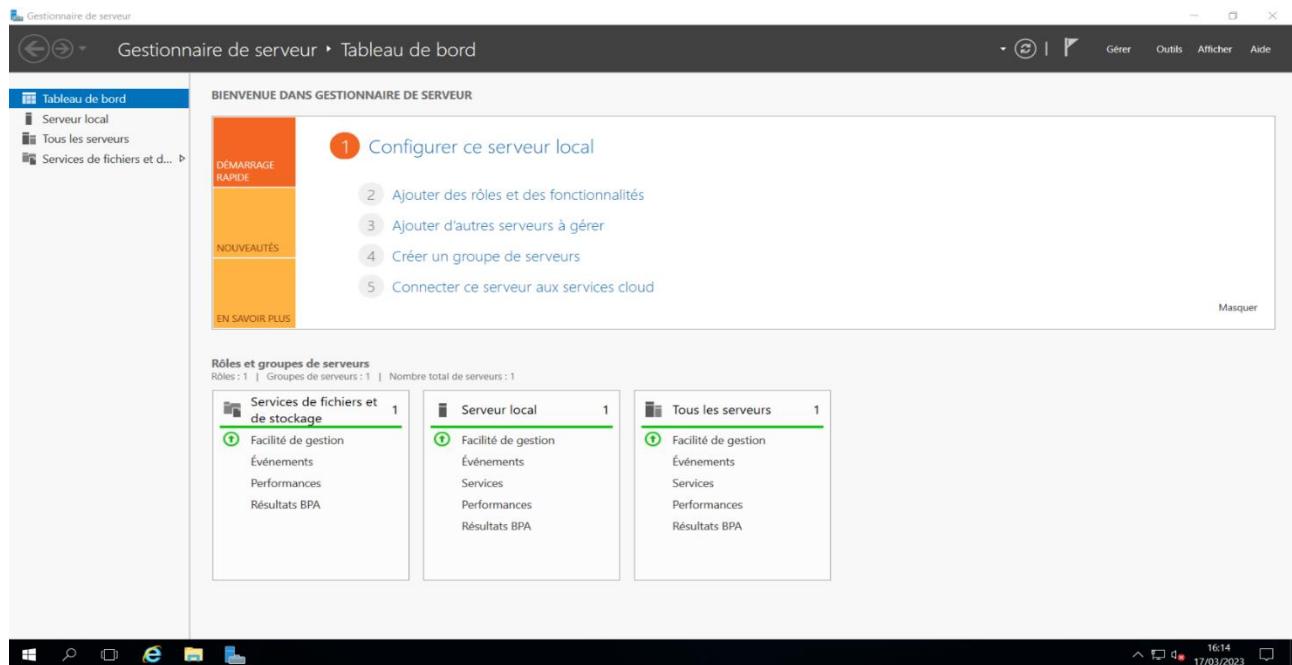


Notre paramétrage dans le Sconfig est maintenant terminé.

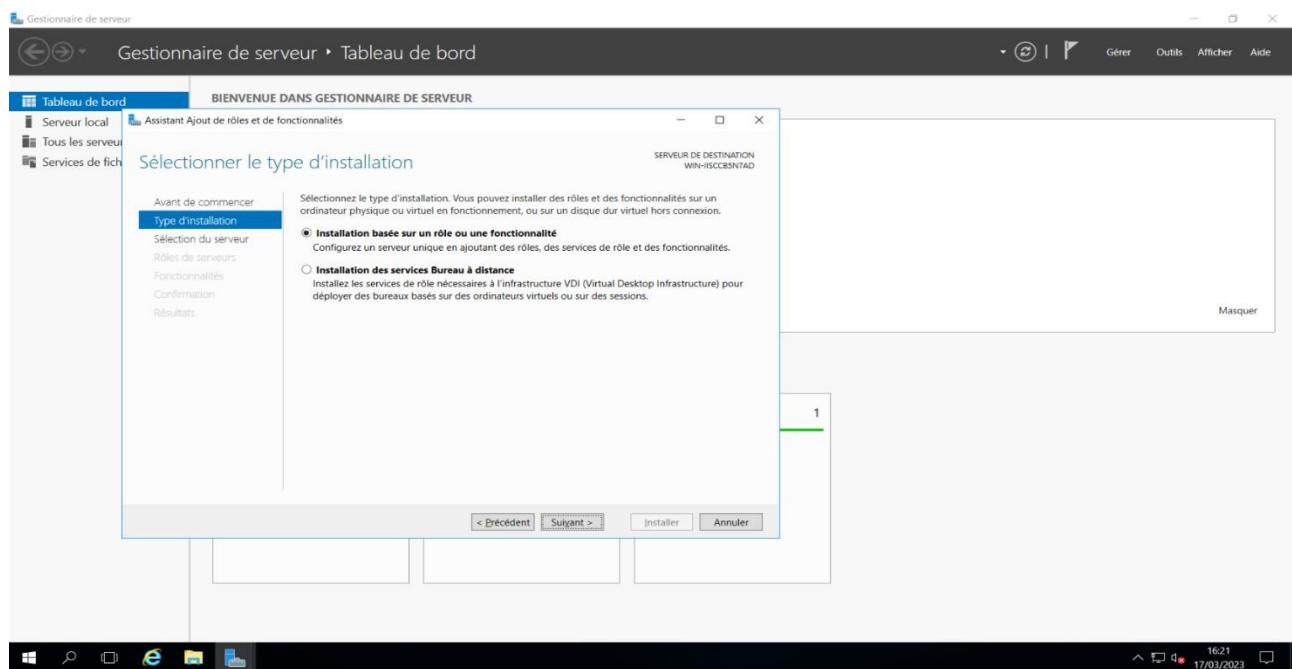
### III) Installation des services

Maintenant que notre réseau est correctement configuré, il faut maintenant installer les différents services dont nous avons besoins.

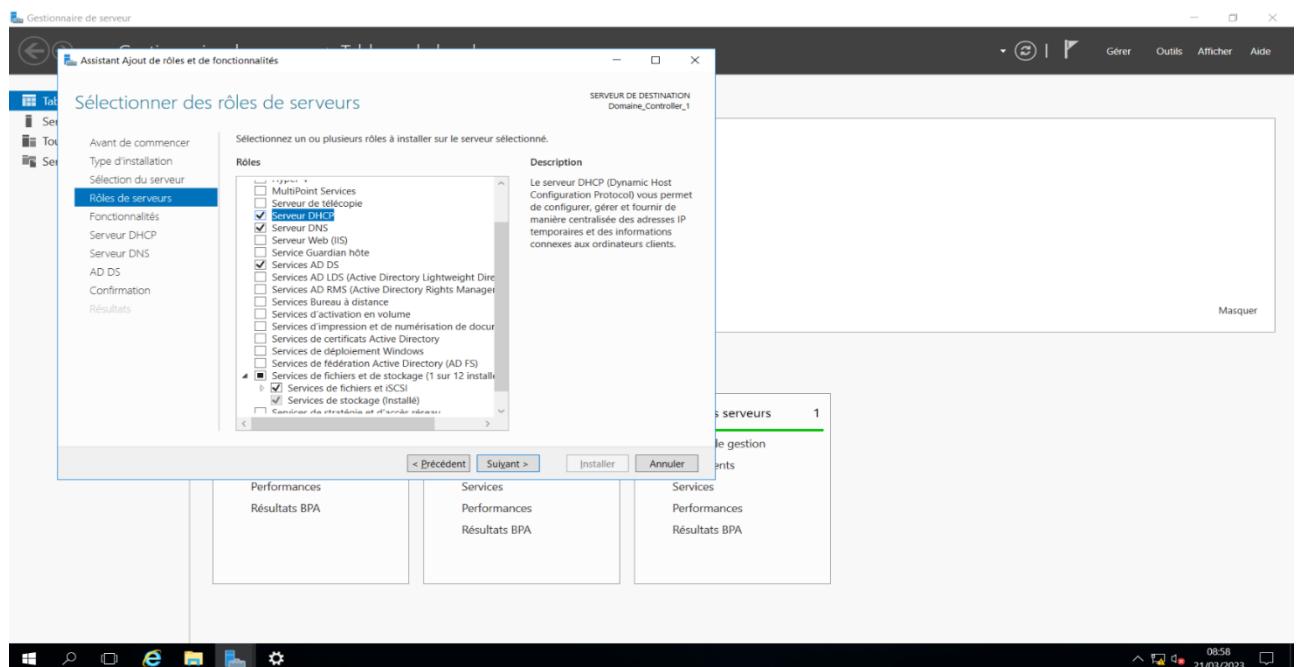
Une fois sur notre page tableau de bord, on clique sur « ajouter des rôles et des fonctionnalités ».



On sélectionne « installation basé sur un rôle ou une fonctionnalité » puis on clique sur « suivant ».



On sélectionne les services que l'on veut installer, ici on sélectionne « Serveur DHCP », « Serveur DNS », « Services AD DS » ainsi que « Services de fichier et de stockage » puis on clique sur « suivant ».



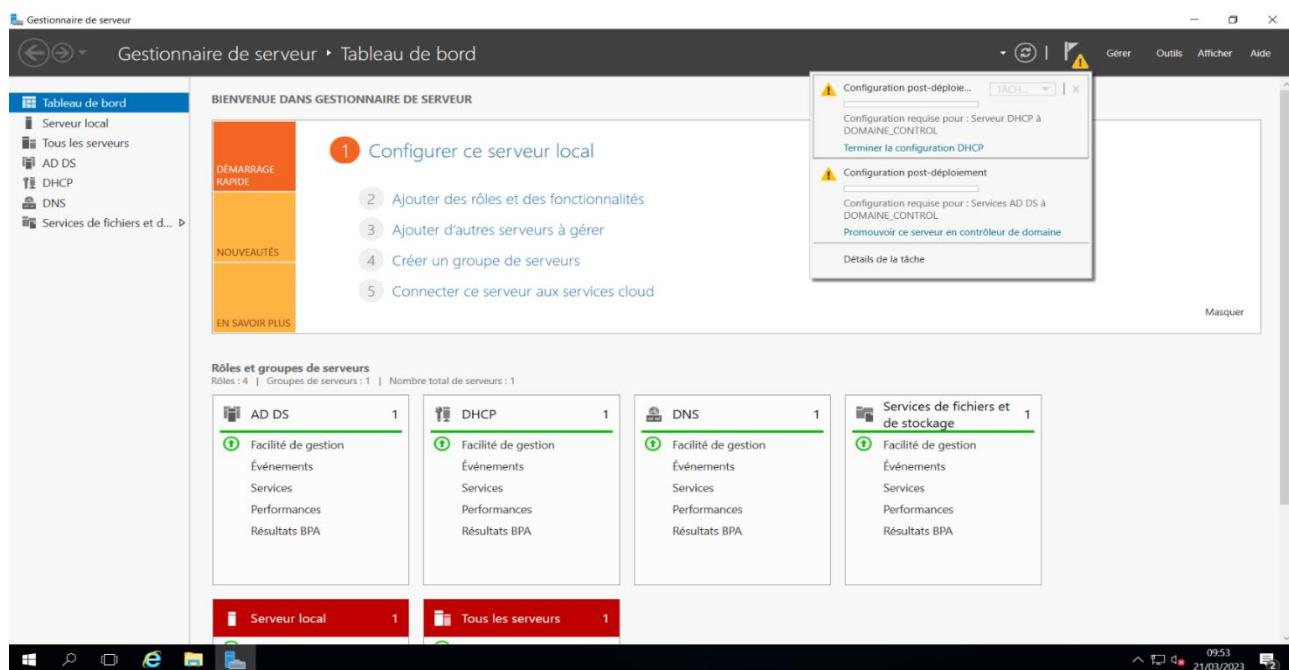
On va jusqu'au bout de l'assistant en cliquant sur « suivant » à chaque fois, puis on clique sur « installer » puis on peut fermer la fenêtre en attendant que les services s'installent en arrière-plan.

Maintenant que nos services ont été installé, il faut maintenant les configurer.

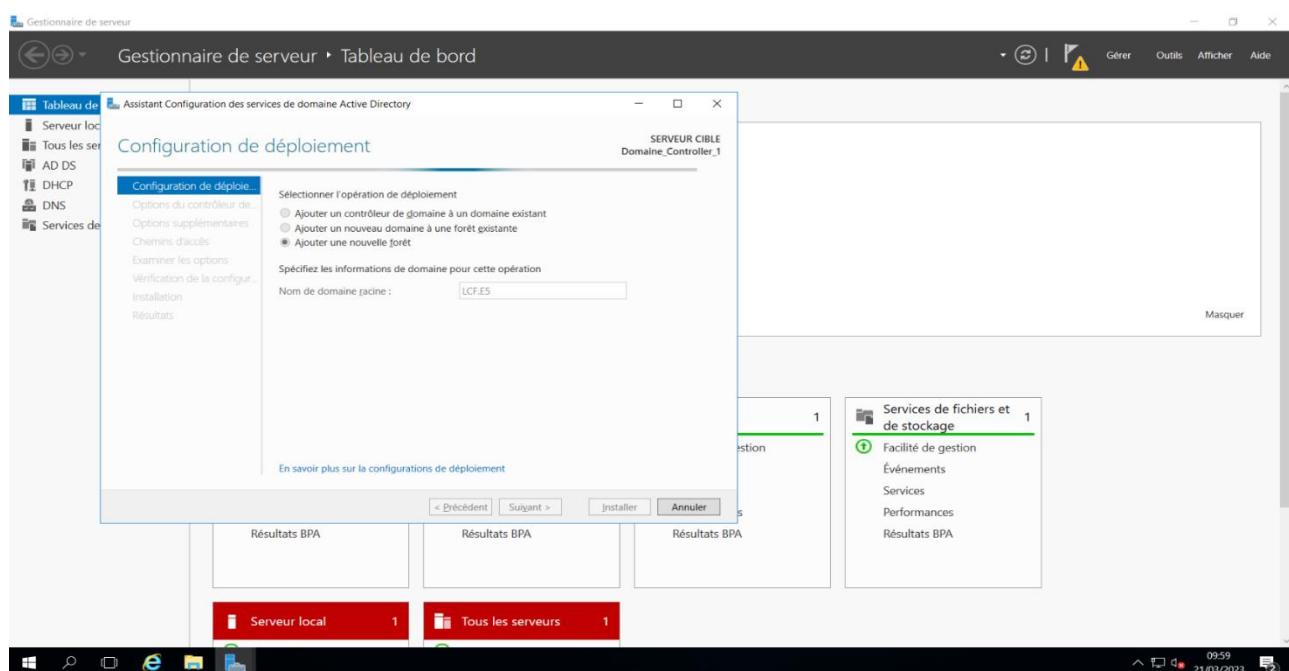
## IV) Configuration de l'AD DS

On peut remarquer désormais qu'un symbole jaune est apparu à côté du drapeau en haut à droite de notre tableau de bord.

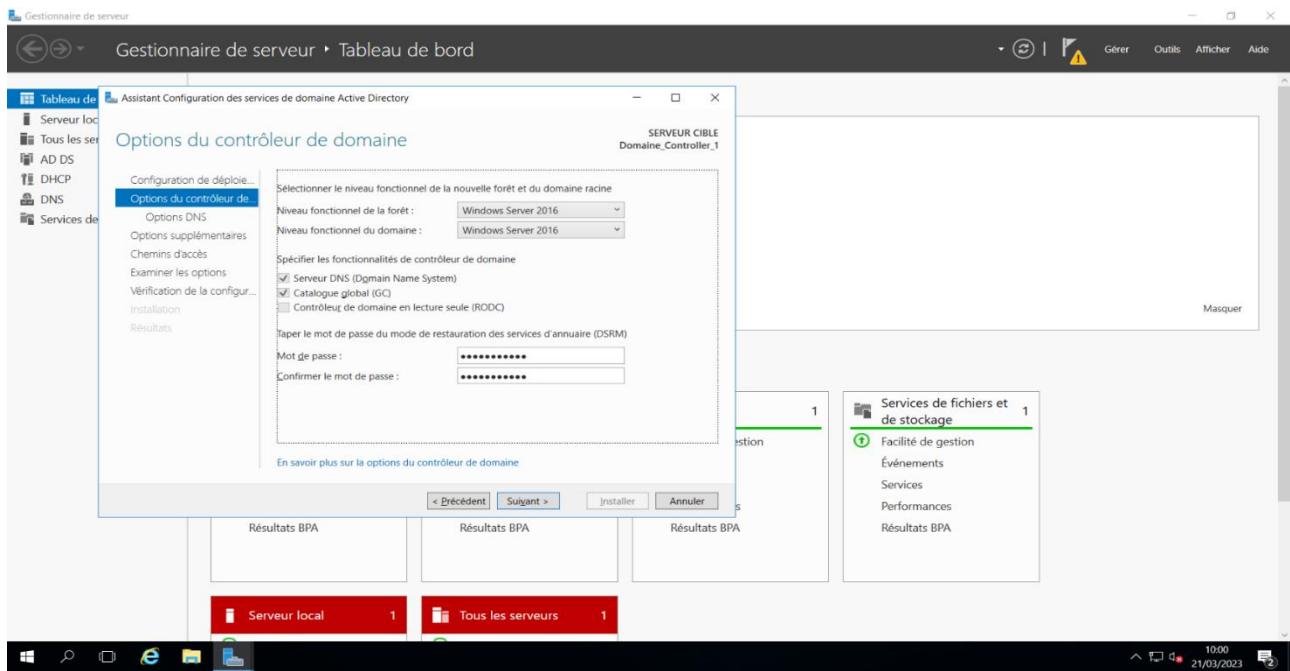
Afin de configurer notre AD DS, il faut cliquer sur « Promouvoir ce serveur en contrôleur de domaine ».



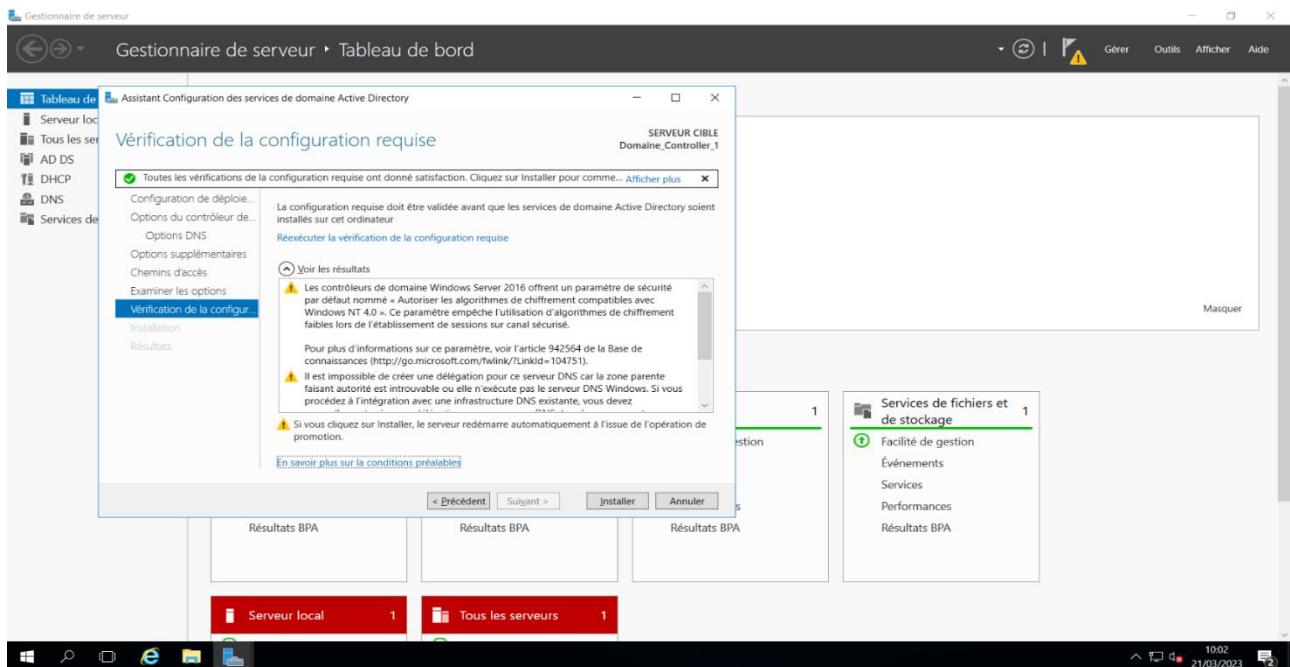
Un assistant va s'ouvrir, on clique sur « ajouter une nouvelle forêt » puis on nomme notre domaine.



On configure un mot de passe en cas de besoin de restauration des services.



On va jusqu'au bout de l'assistant en remplaçant les différentes informations qu'il faut renseigner , puis après les vérifications, on clique sur « Installer ».

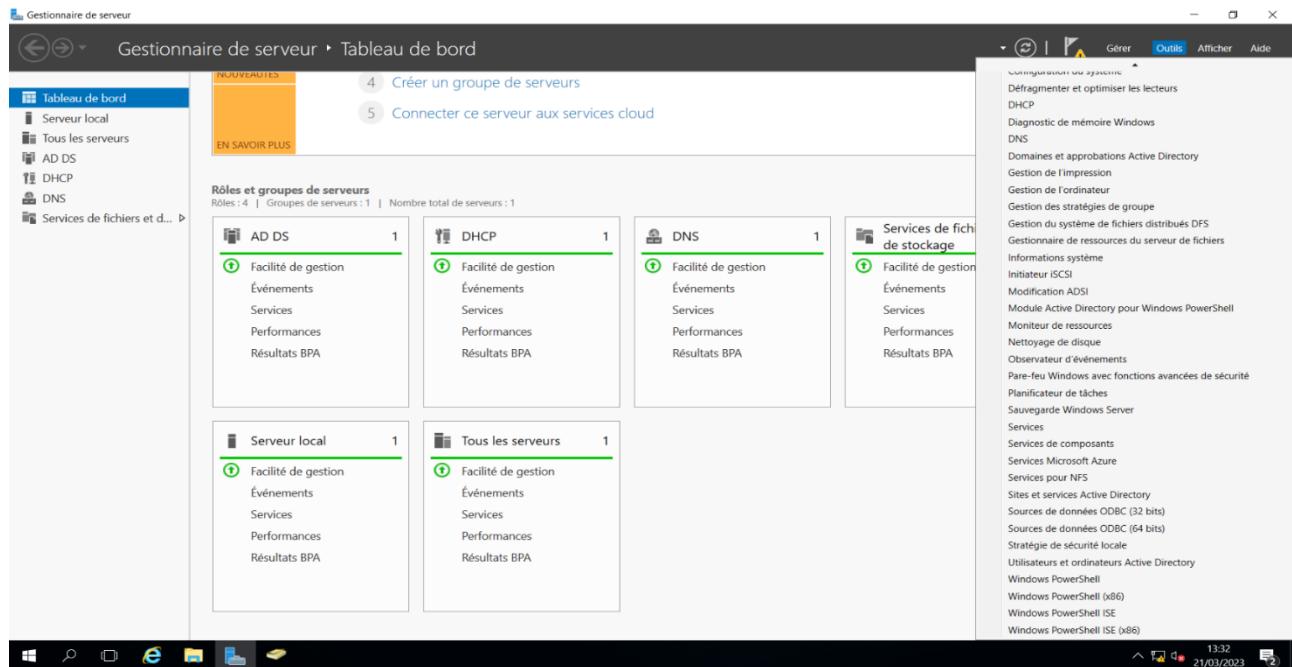


Nous pouvons désormais ajouter des utilisateurs avec leurs identifiants, des groupes globaux et de domaine locaux, ainsi que les différentes machines sur notre domaine.

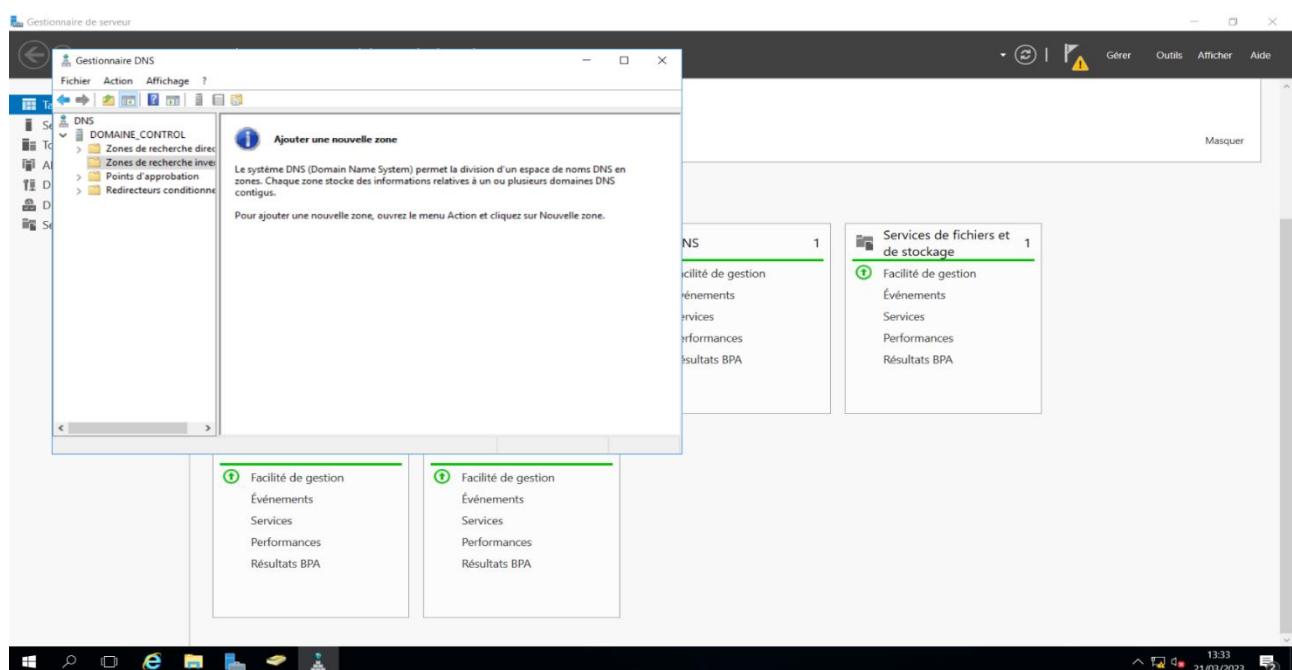
## V) Configuration du service DNS

Maintenant que notre AD DS est configuré, on peut passer au DNS avant de s'occuper du DHCP.

Pour ce faire, on clique sur outils en haut à droite de notre tableau de bord, puis on clique sur « DNS ».

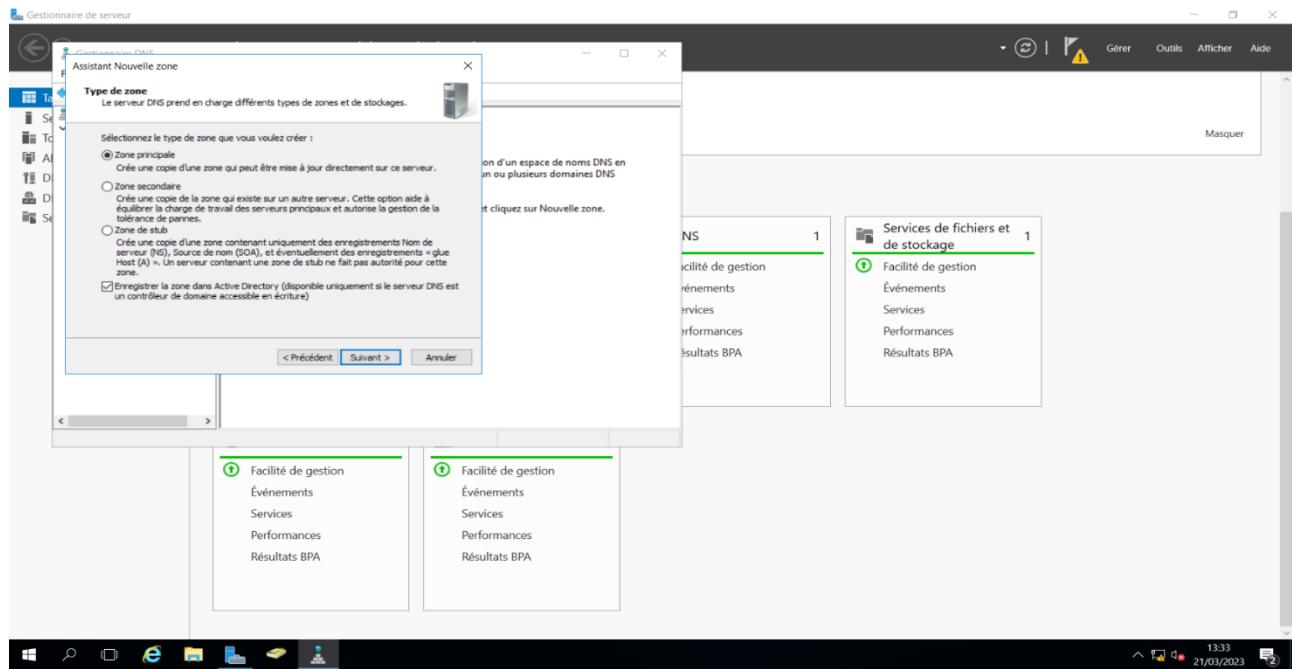


On sélectionne « Zone de recherche inversé » puis on clique sur Action > Nouvelle Zone.

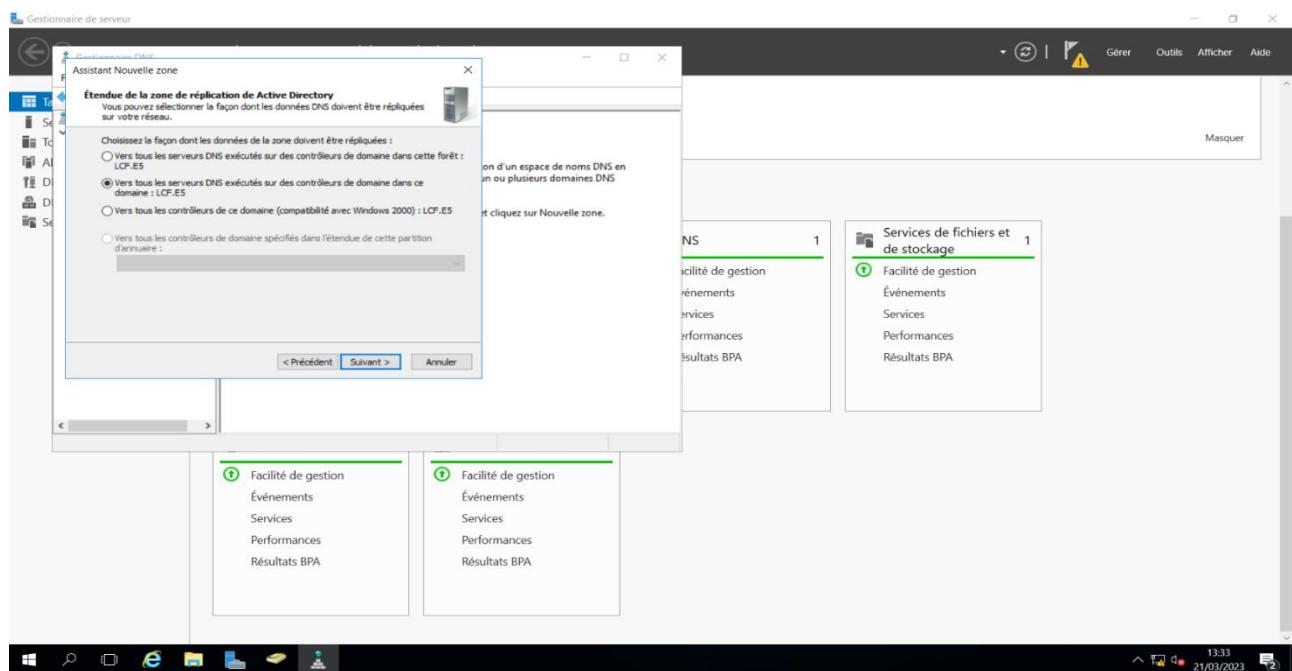


Un assistant s'ouvre.

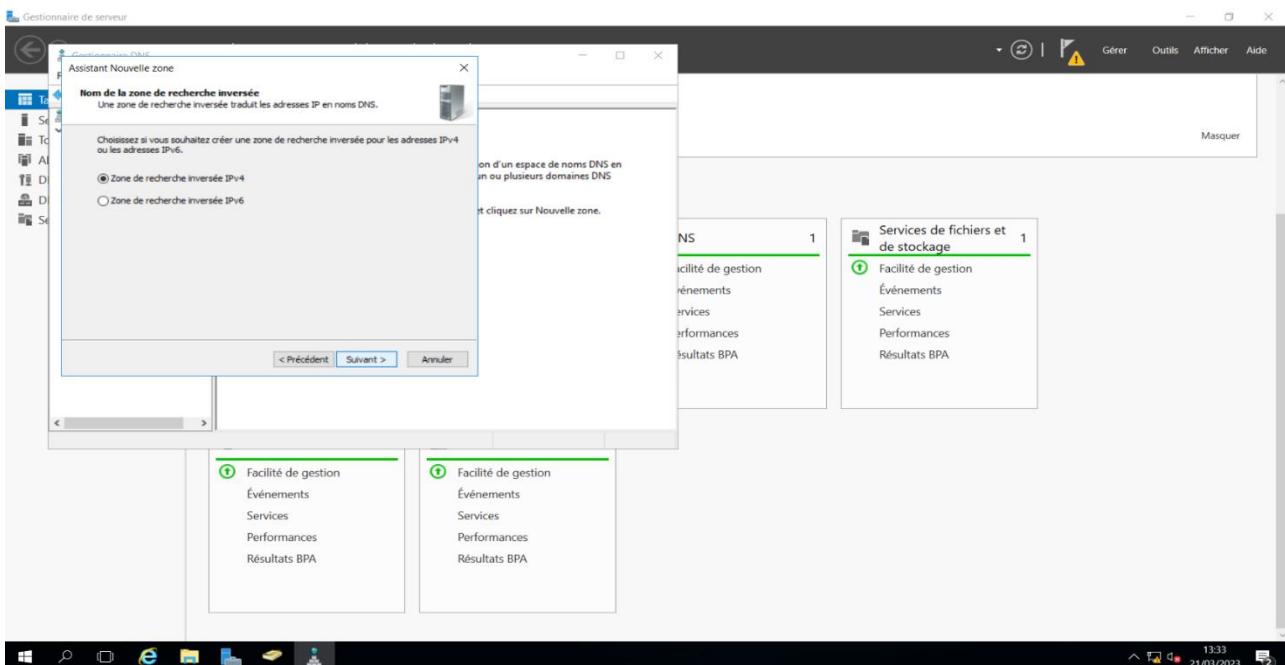
On coche « Zone principale » puis on clique sur « suivant ».



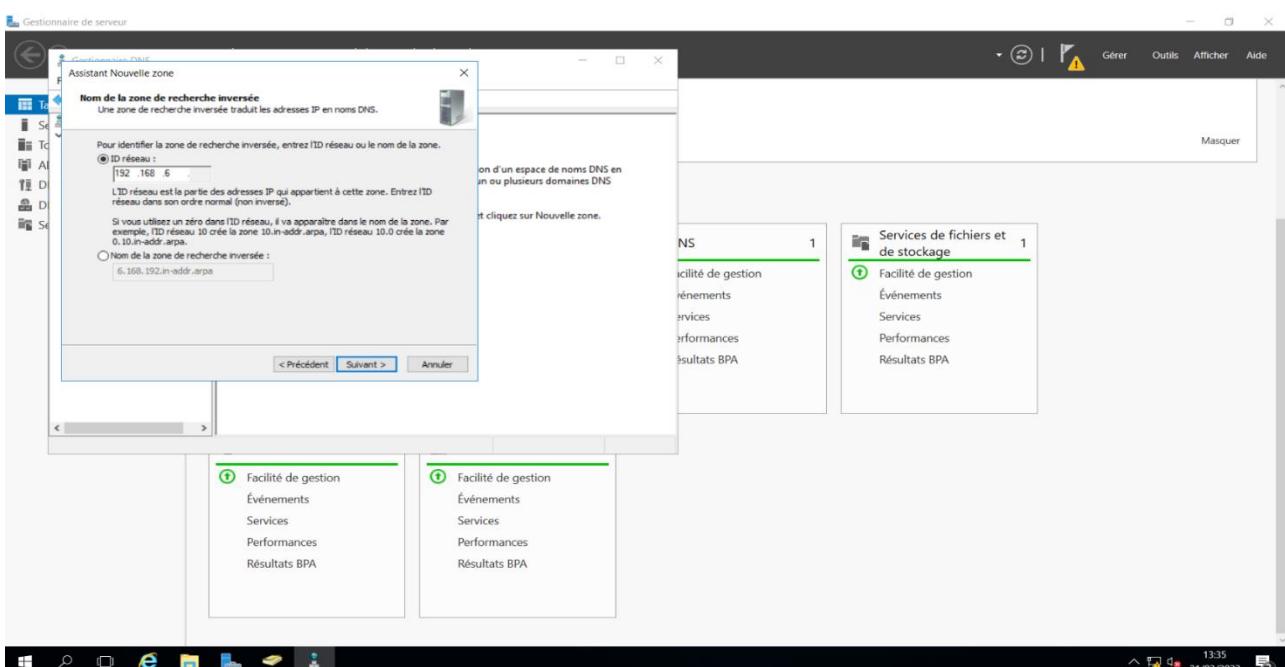
On coche « Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : \*nom de domaine\* » puis on clique sur « suivant ».



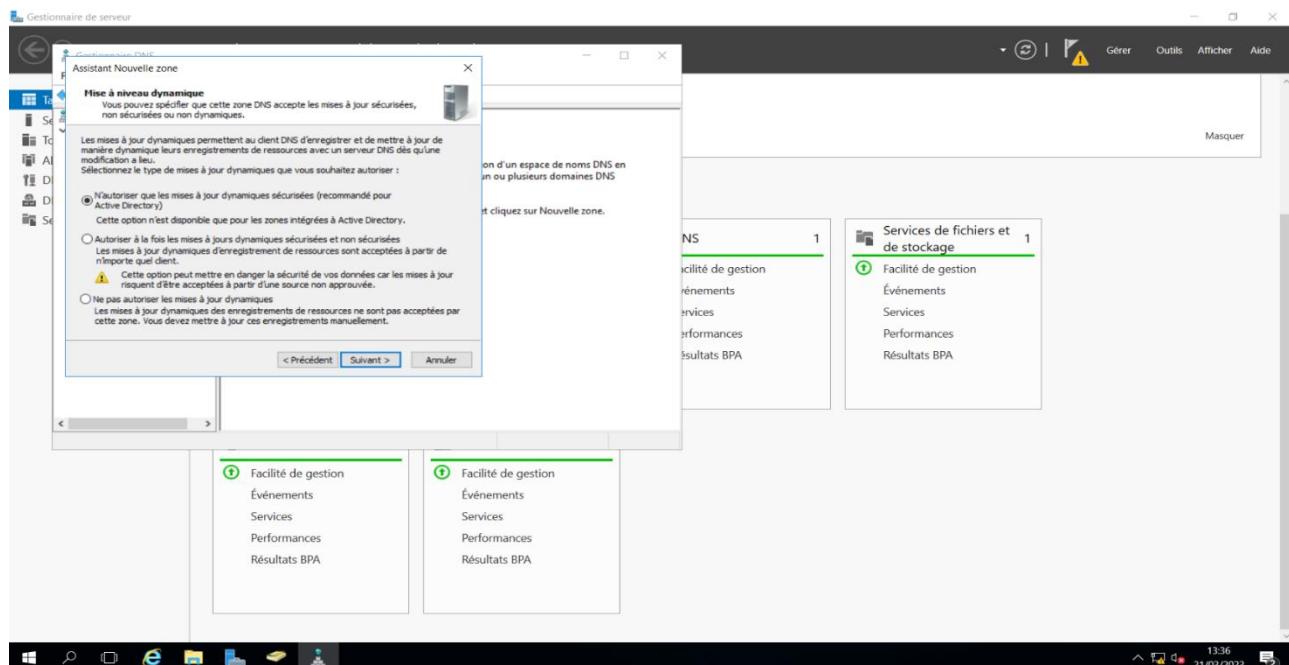
On coche « Zone de recherche inversée IPv4 » puis on clique sur « suivant ».



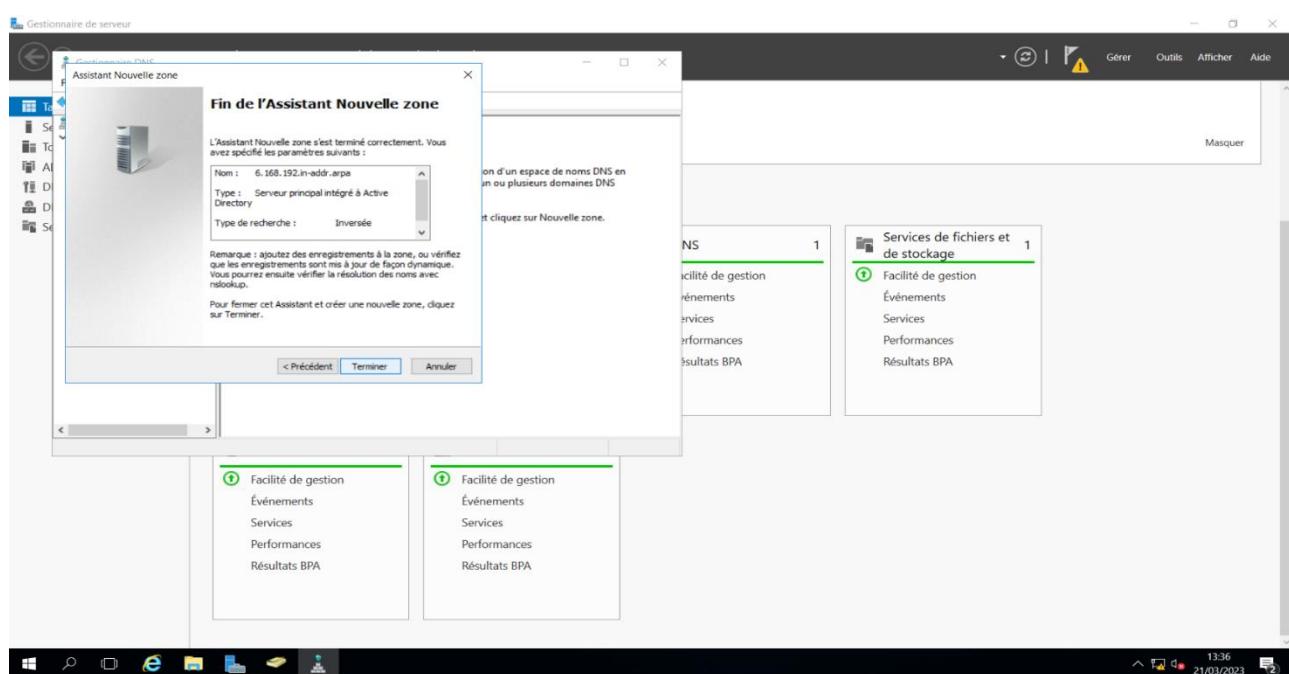
Dans « ID réseau », on indique l'adresse sur lequel notre serveur se trouve, ici 192.168.6.



On coche la case « N'autoriser que les mises à jour dynamiques sécurisées (recommandé pour Active Directory). »



On clique sur « Terminer ».

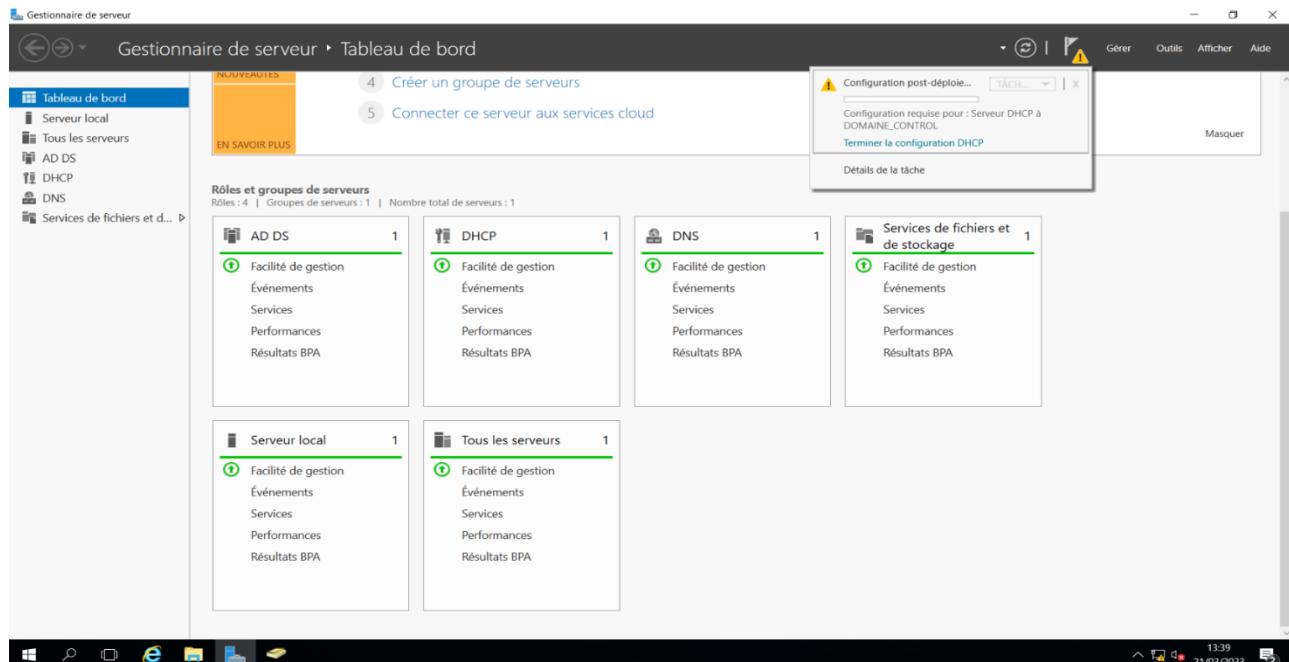


Nous avons donc fini de configurer notre DNS, les recherches directes ainsi que les pointeurs vers les machines du domaine sont configurées automatiquement dès qu'une machine est identifié sur notre domaine.

## VI) Configuration du service DHCP

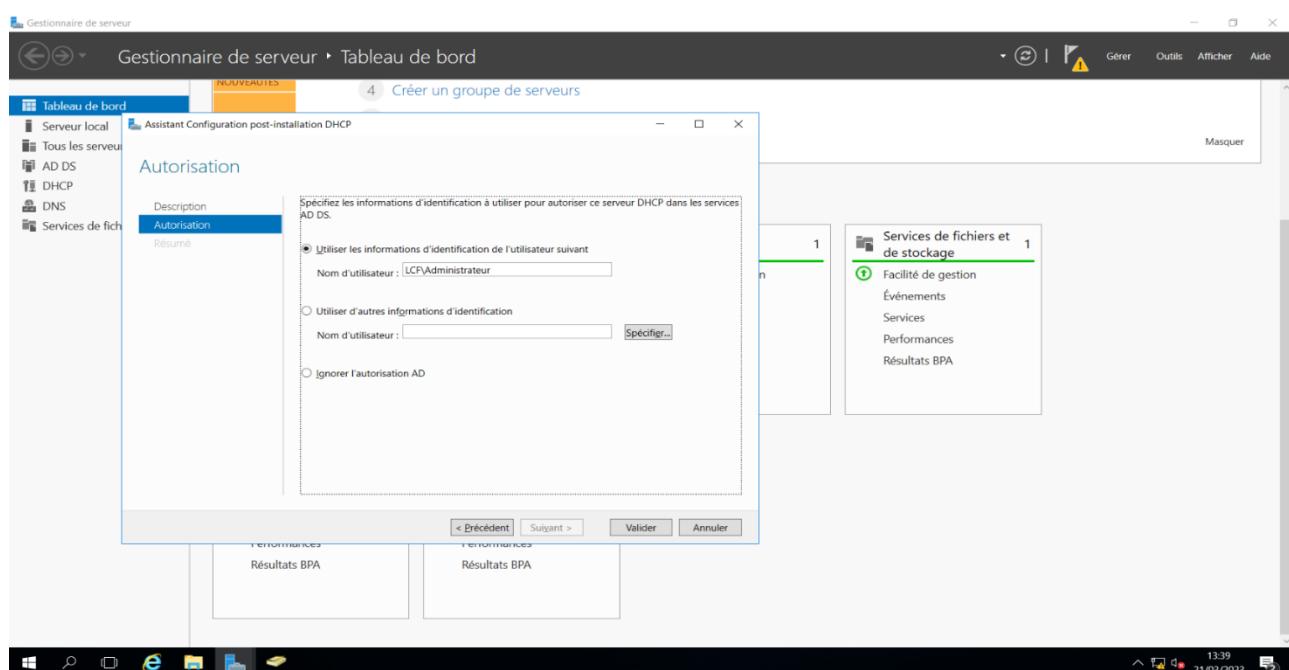
Il nous reste maintenant à configurer notre service DHCP afin de distribuer automatique des adresses IP à nos utilisateurs du domaine afin qu'ils puissent accéder à internet.

Pour ce faire, on clique sur le drapeau en haut à droite de notre tableau de bord et on clique sur « Terminer la configuration DHCP ».



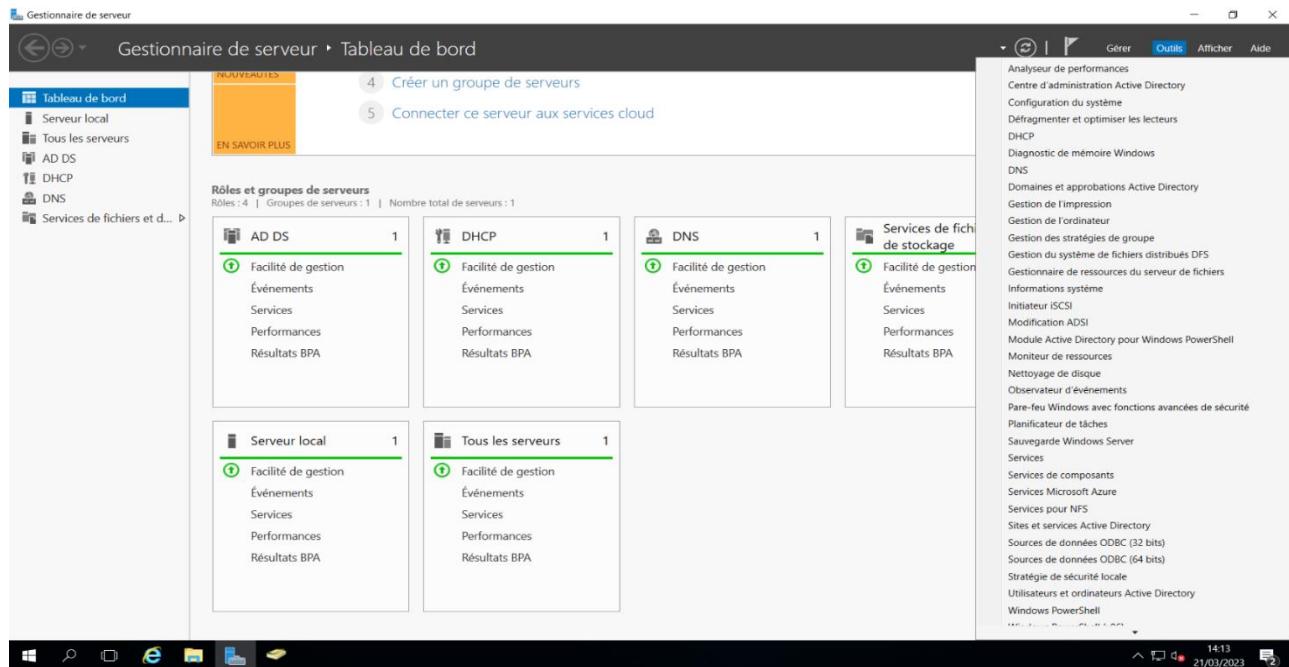
Un assistant s'ouvre, on clique sur « suivant ».

On clique sur la première case et on continue.

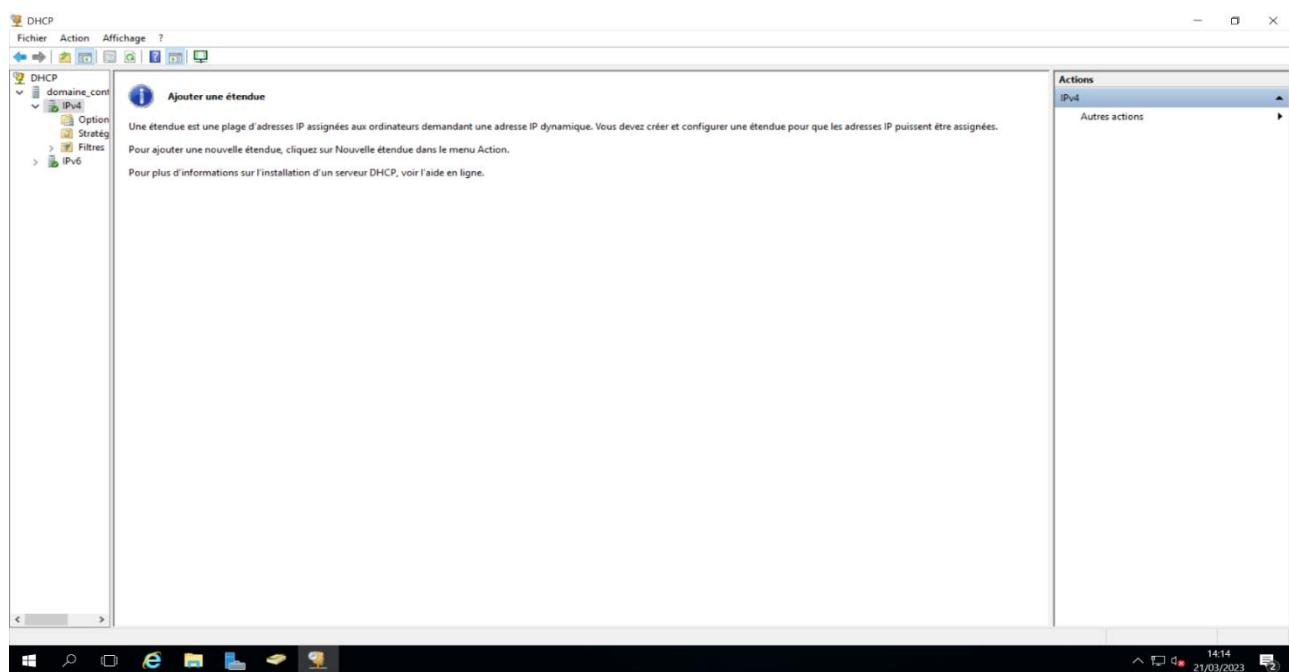


On clique sur « Fermer » sur la page suivante.

Maintenant il faut cliquer sur « Outils » en haut à droite de notre tableau de bord et on clique sur « DHCP ».

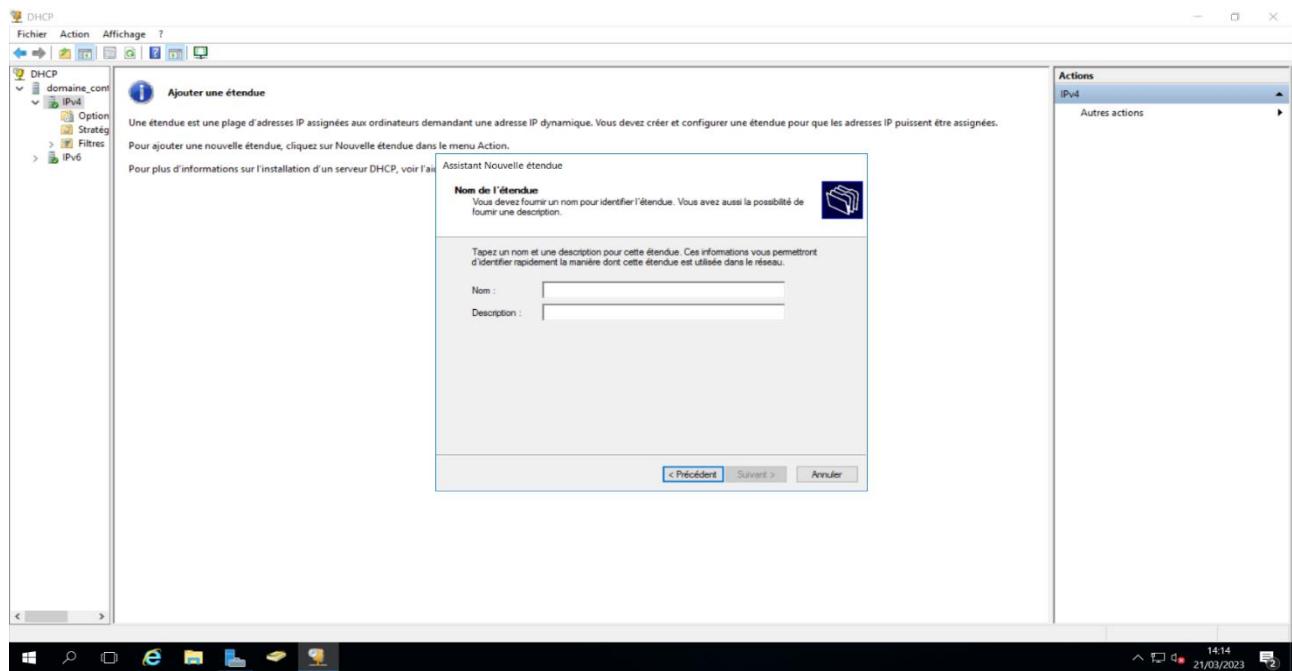


On sélectionne IPv4 puis on clique sur Action > Nouvelle étendue.

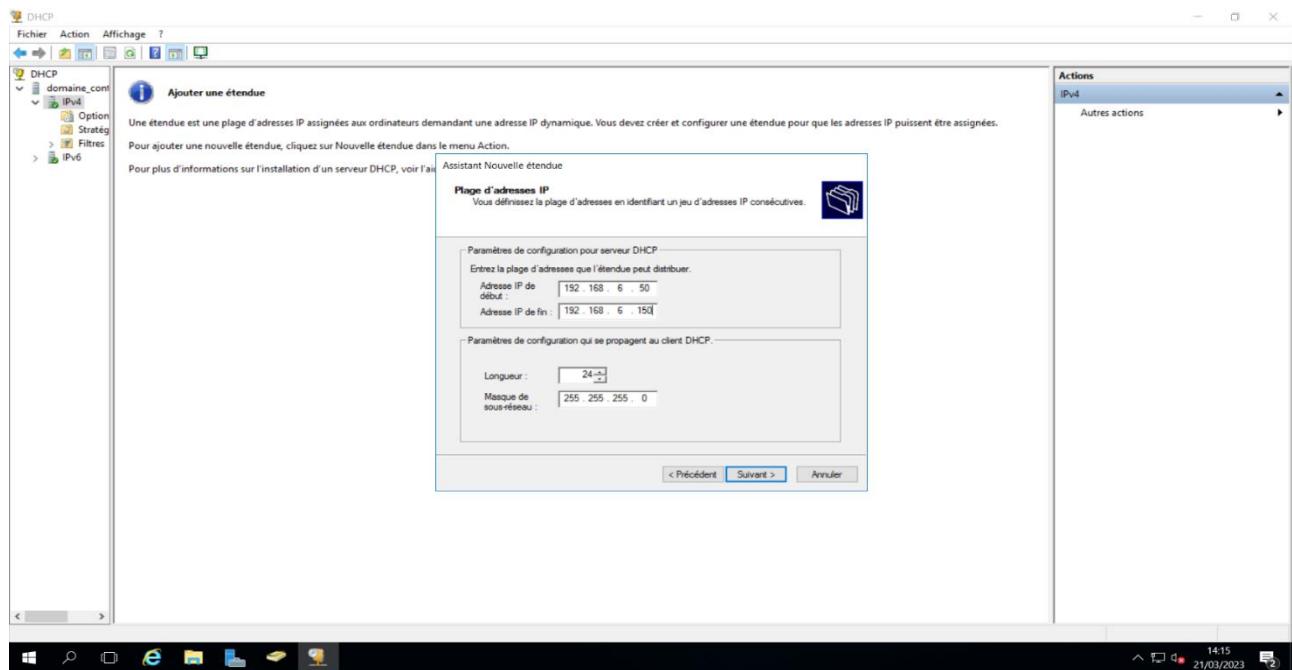


Un assistant s'ouvre alors.

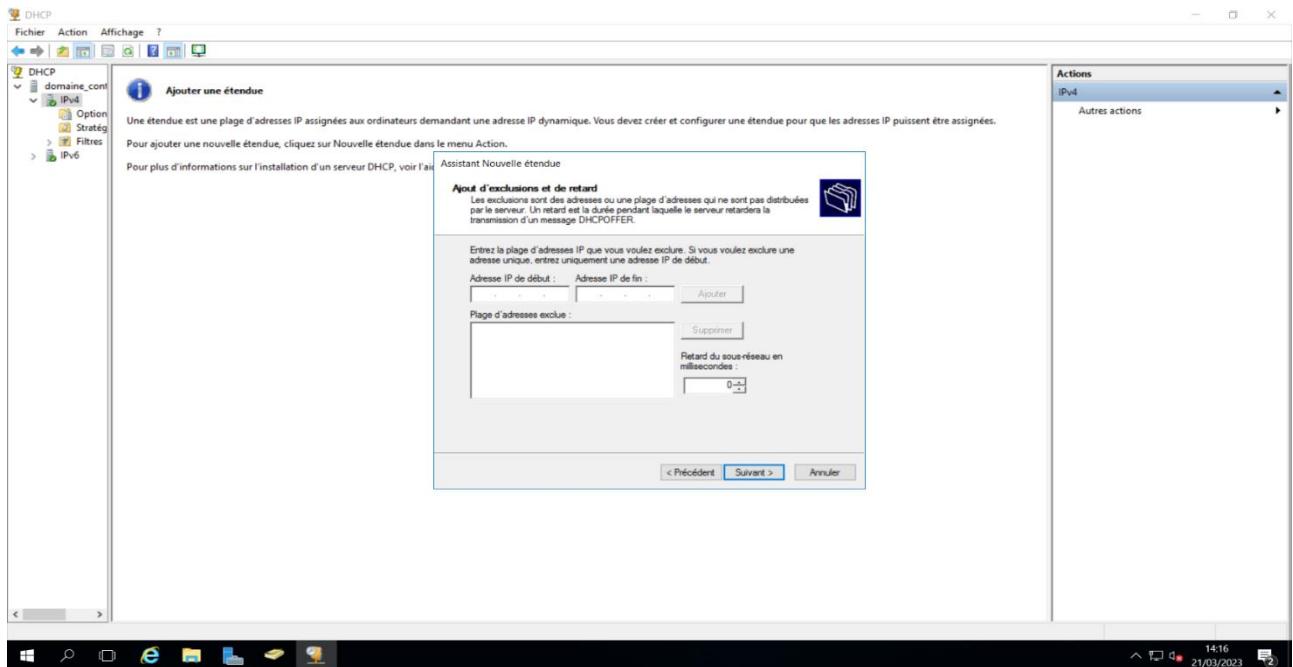
On donne un nom ainsi qu'une description à notre étendue puis on clique sur « suivant ».



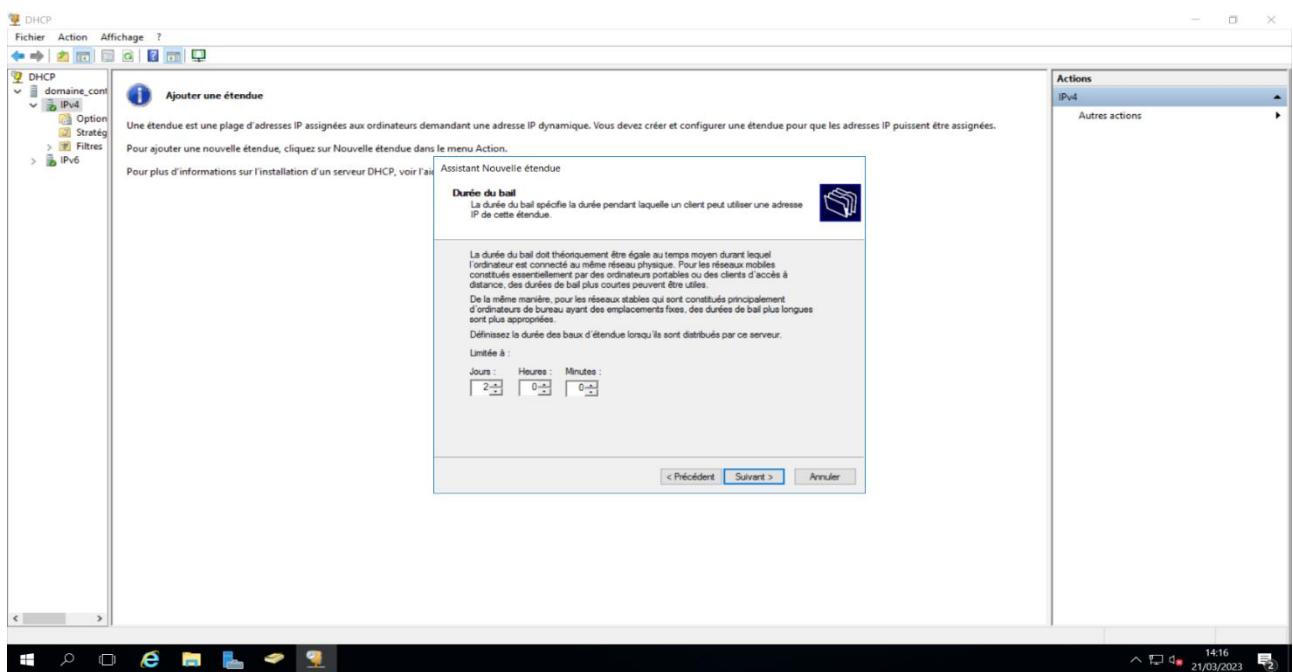
On définit notre plage d'adresse IP du DHCP comme on le souhaite, ici de 192.168.6.50/24 à 192.168.6.150/24.



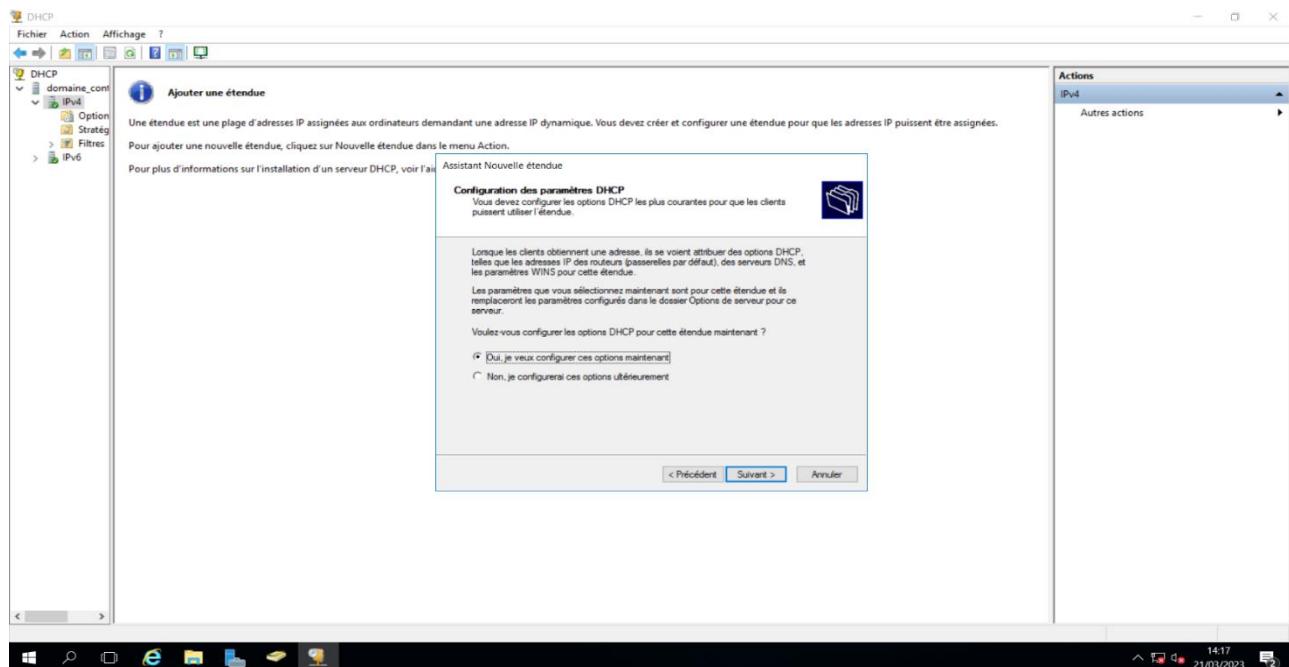
On peut ajouter une exclusion dans notre plage d'adresse si nécessaire, et on clique sur « suivant ».



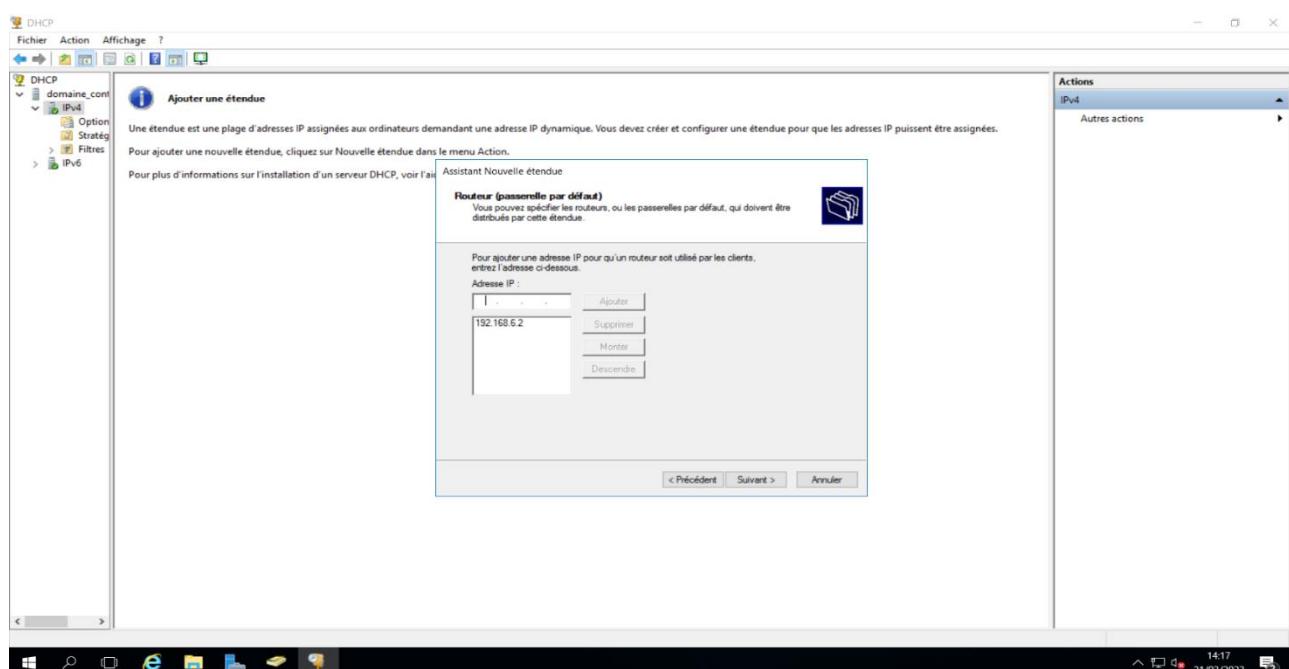
On définit la durée du bail (durée pour laquelle l'utilisateur garde la même adresse IP du DHCP).



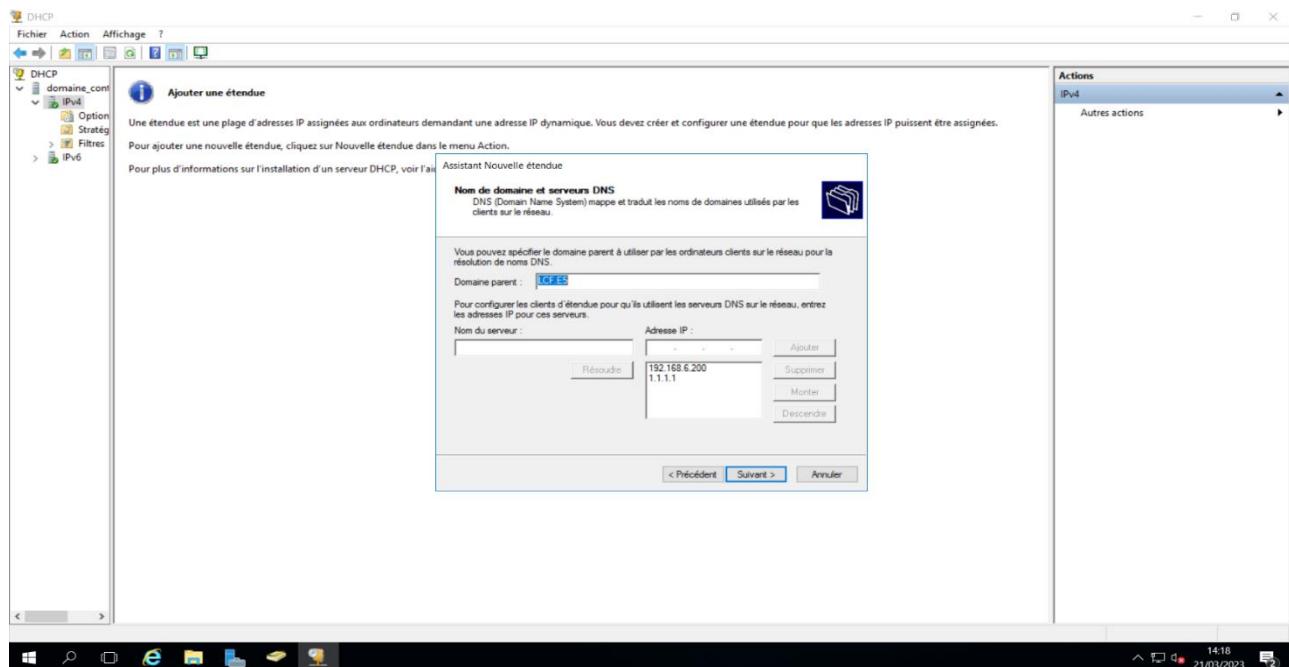
On coche la case « Oui, je veux configurer ces options maintenant » puis on clique sur « Suivant ».



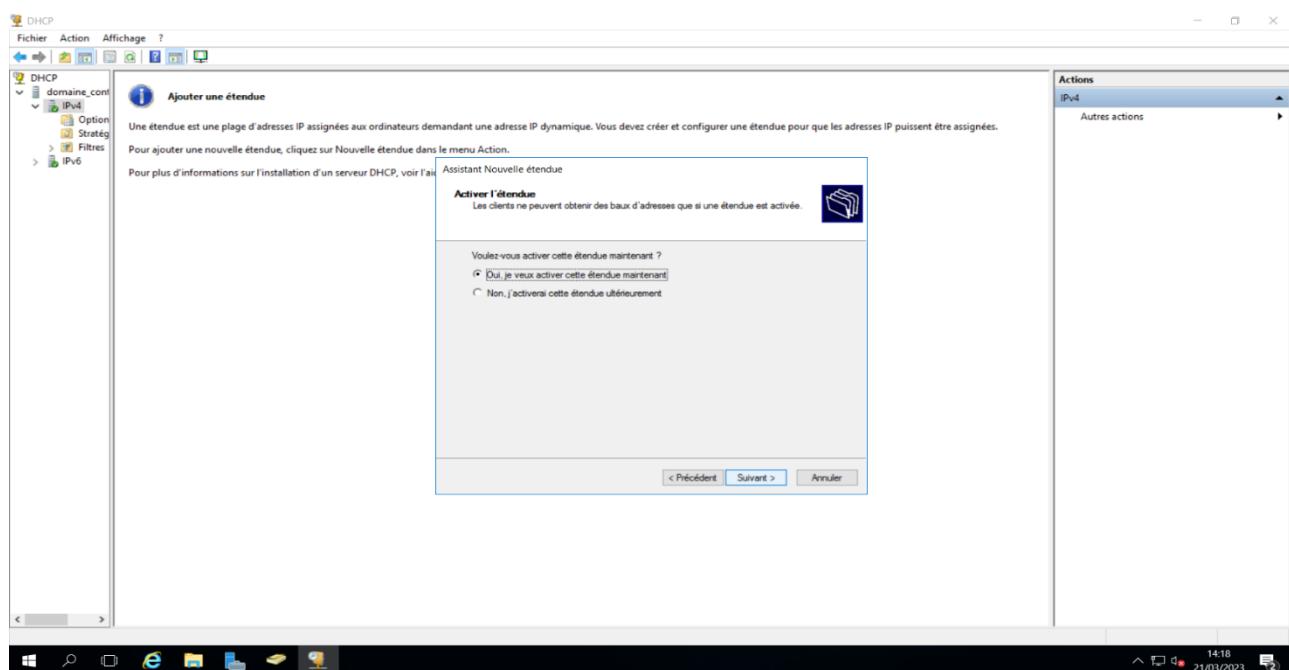
On définit l'adresse notre passerelle par défaut, ici 192.168.6.2.



On configure le nom de domaine ainsi que son adresse IP afin que le DHCP soit rattaché au domaine.



On coche « Oui, je veux activer cette étendue maintenant ».



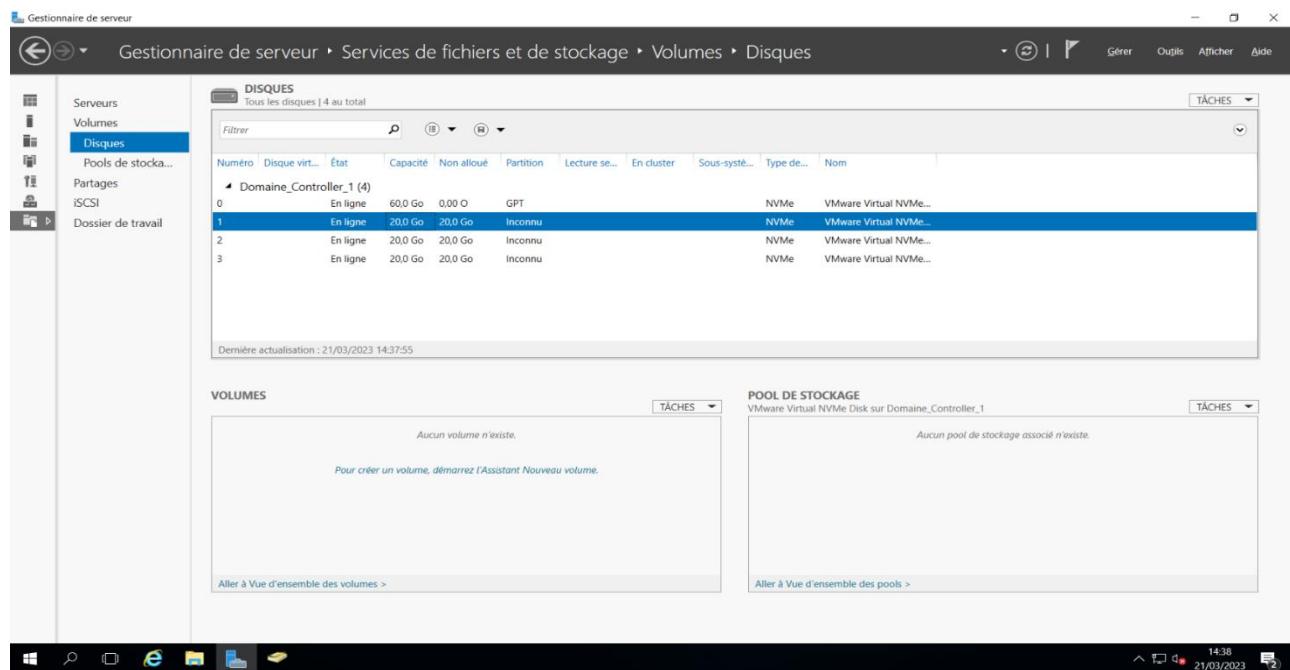
On clique sur « Terminer » sur la page suivante.

Notre étendu DHCP pour notre domaine est maintenant créé et effectif.

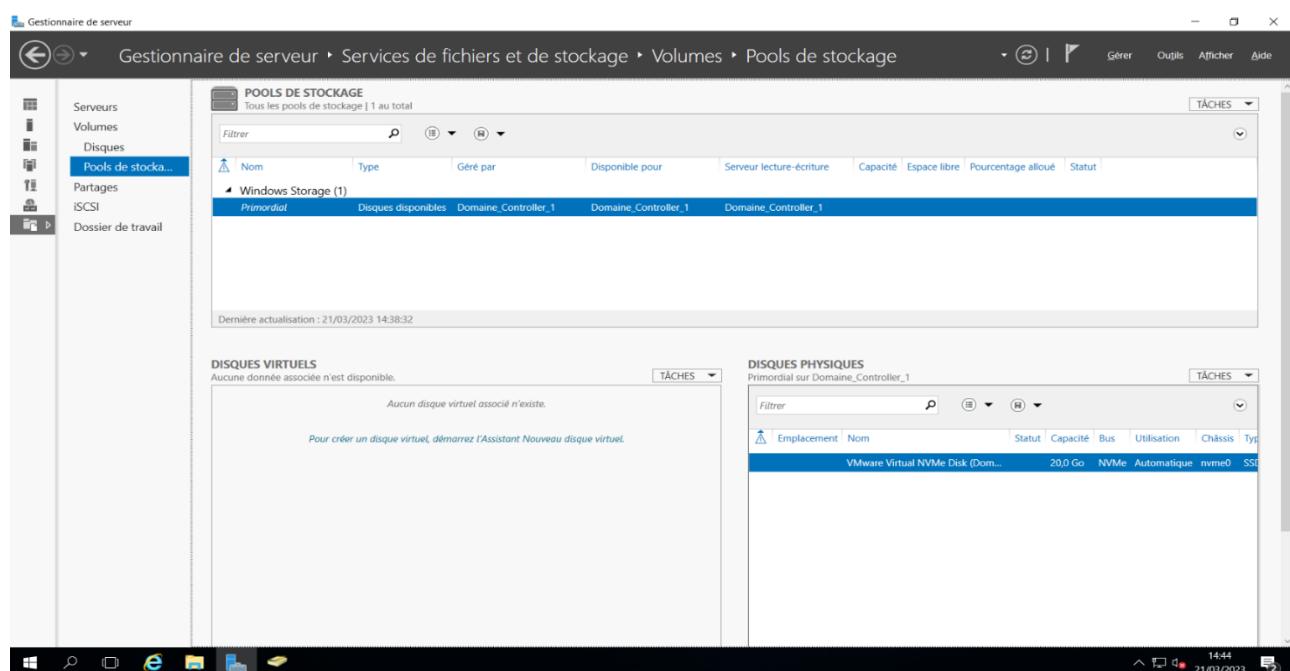
## VII) Création d'un dossier partagé en RAID 5

Afin que les utilisateurs disposent d'un dossier dans lequel déposer leurs fichiers en rapport avec leur service, la création d'un dossier partagé s'impose. Les utilisateurs auront, dans ce dossier, uniquement accès aux ressources nécessaires à leur environnement de travail. Leur accès à ces dossiers a été géré par la création de groupe dans l'AD DS.

Pour faire ce dossier partagé en RAID 5 (une technologie visant à répartir les données de chaque disque de manière sécurisée), on ajoute 3 disques dur sur notre VM Windows Server 2016 puis on va dans l'onglet « Services de fichiers et de stockage » puis Volumes > Disques.

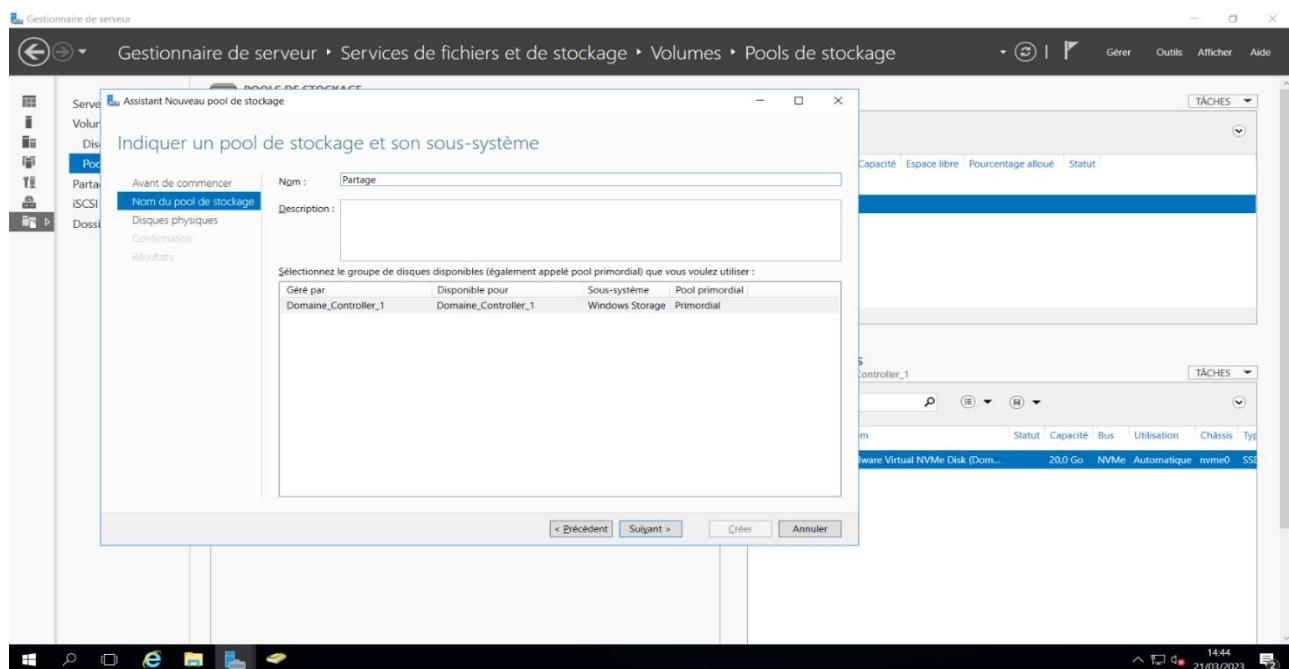


Après les avoir initialisés, on se dirige maintenant dans l'onglet « Pools de stockage » puis on fait un clic droit sur notre disque puis on clique sur « créer un pool de stockage ».

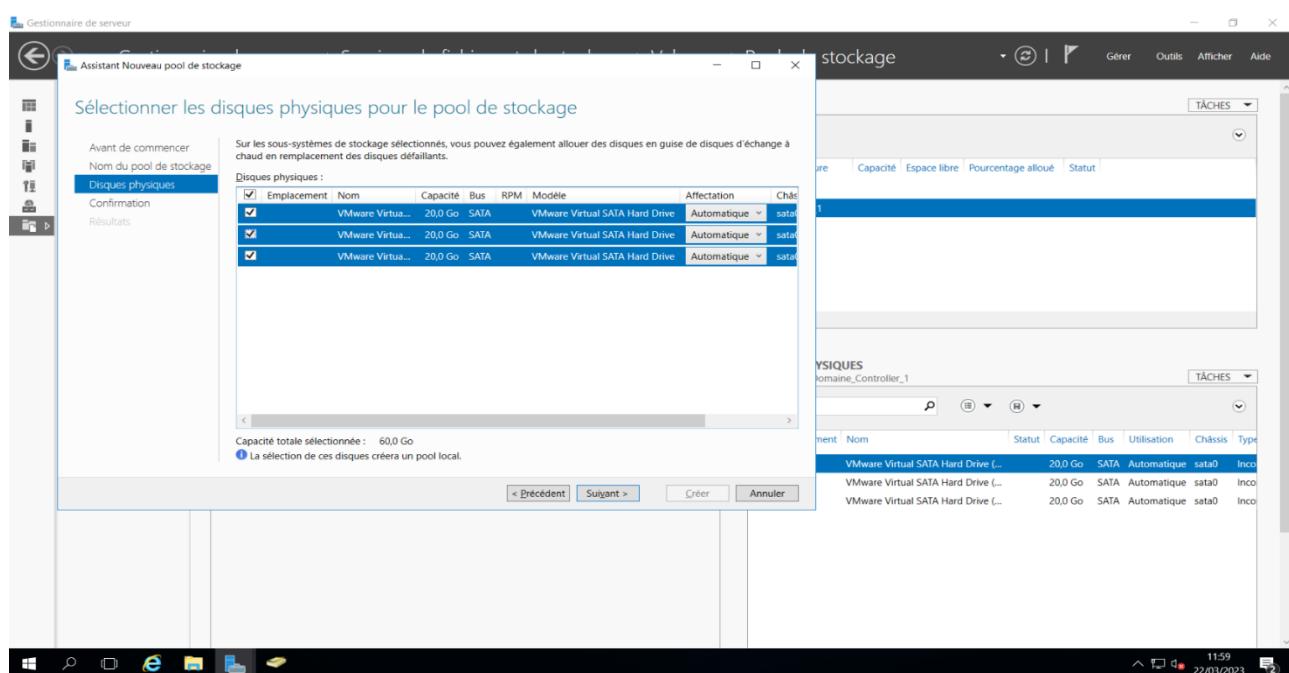


Un assistant s'ouvre.

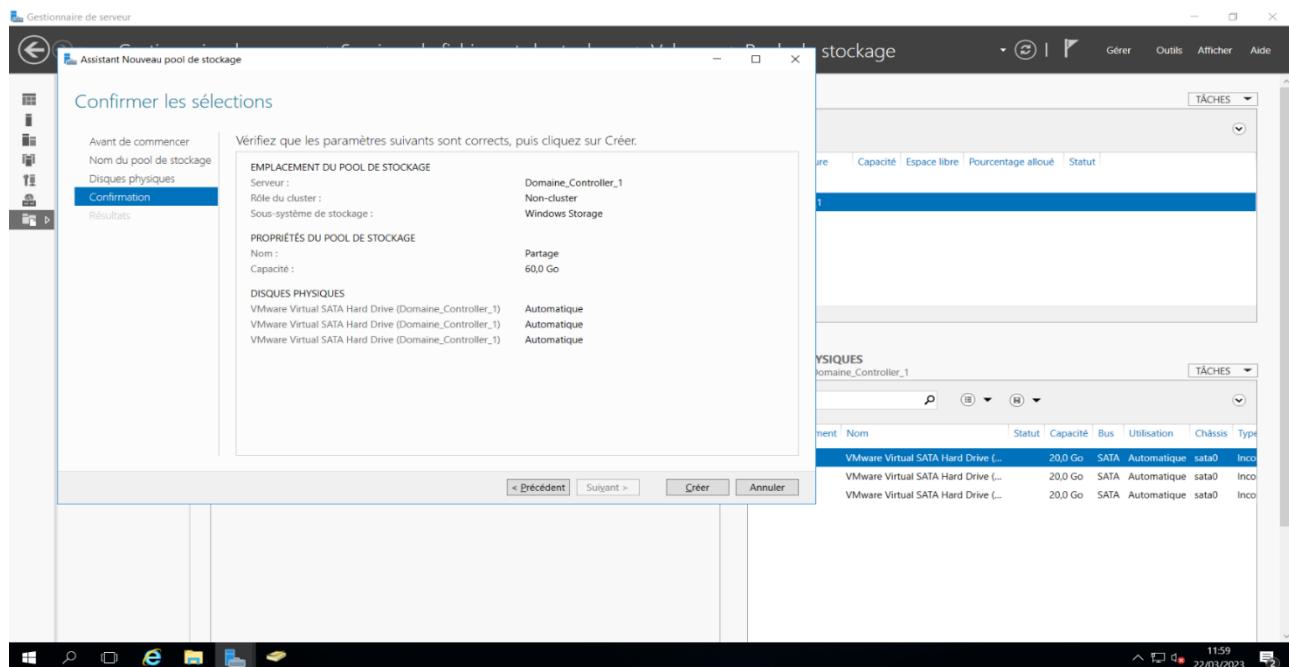
On définit le nom puis on clique sur « Suivant ».



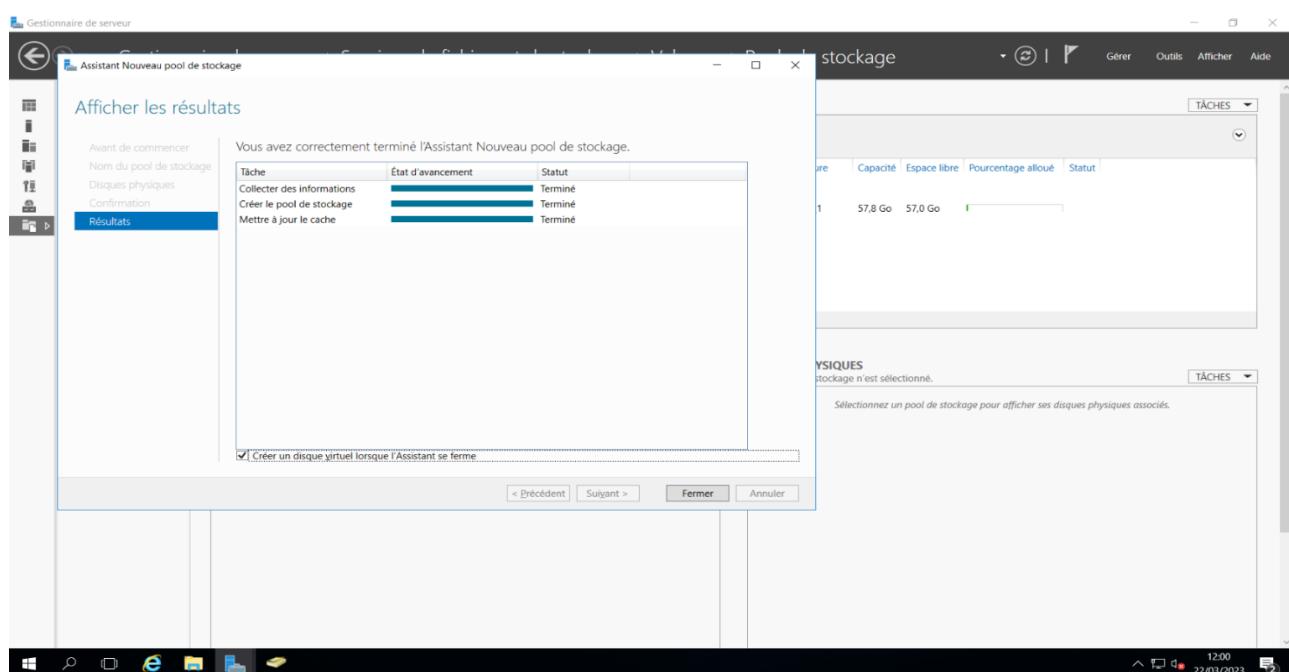
On sélectionne nos disques désirés pour créer notre pool de stockage.



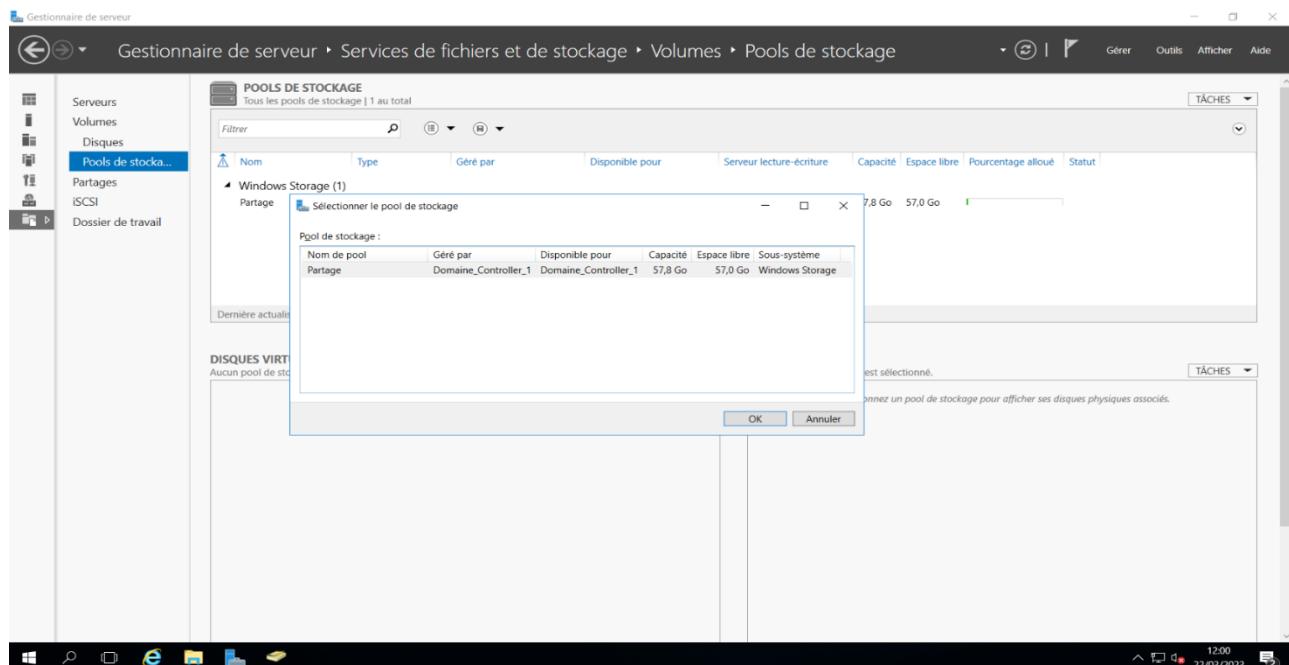
On clique sur « Crée ».



Après la création, on clique sur « Fermer » en vérifiant que la case « Crée un disque virtuel lorsque l'assistant se ferme » est cochée.

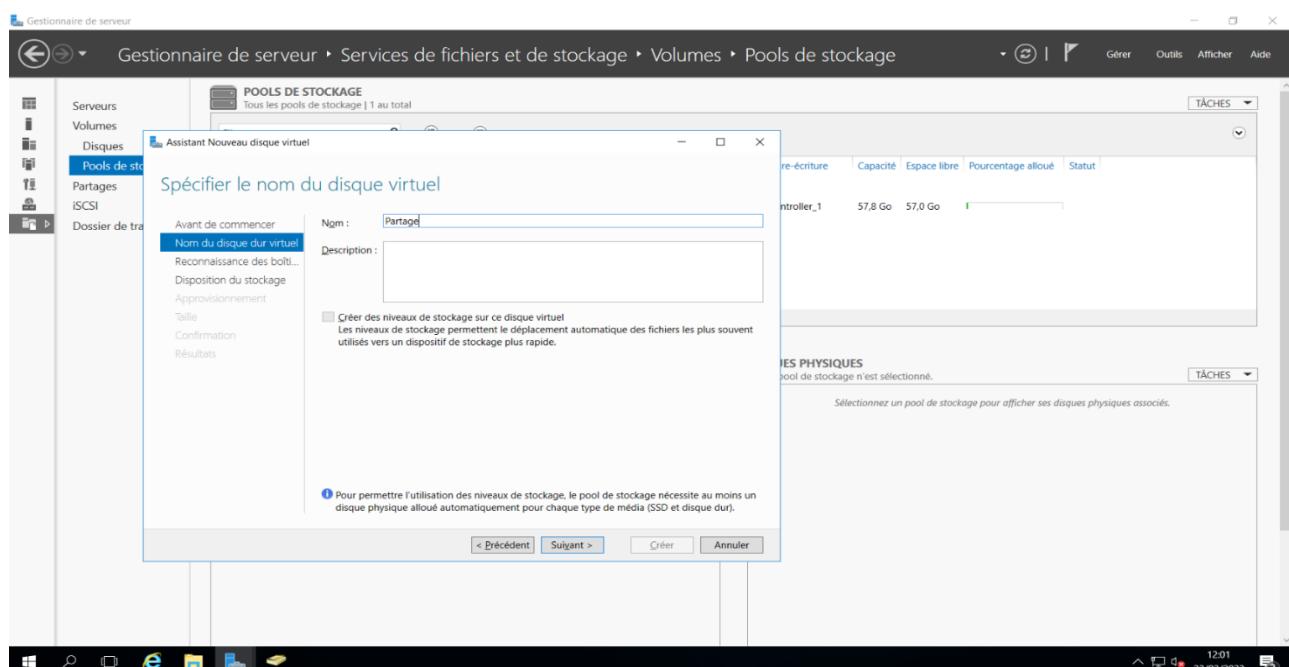


On sélectionne alors notre pool de stockage fraîchement créée.

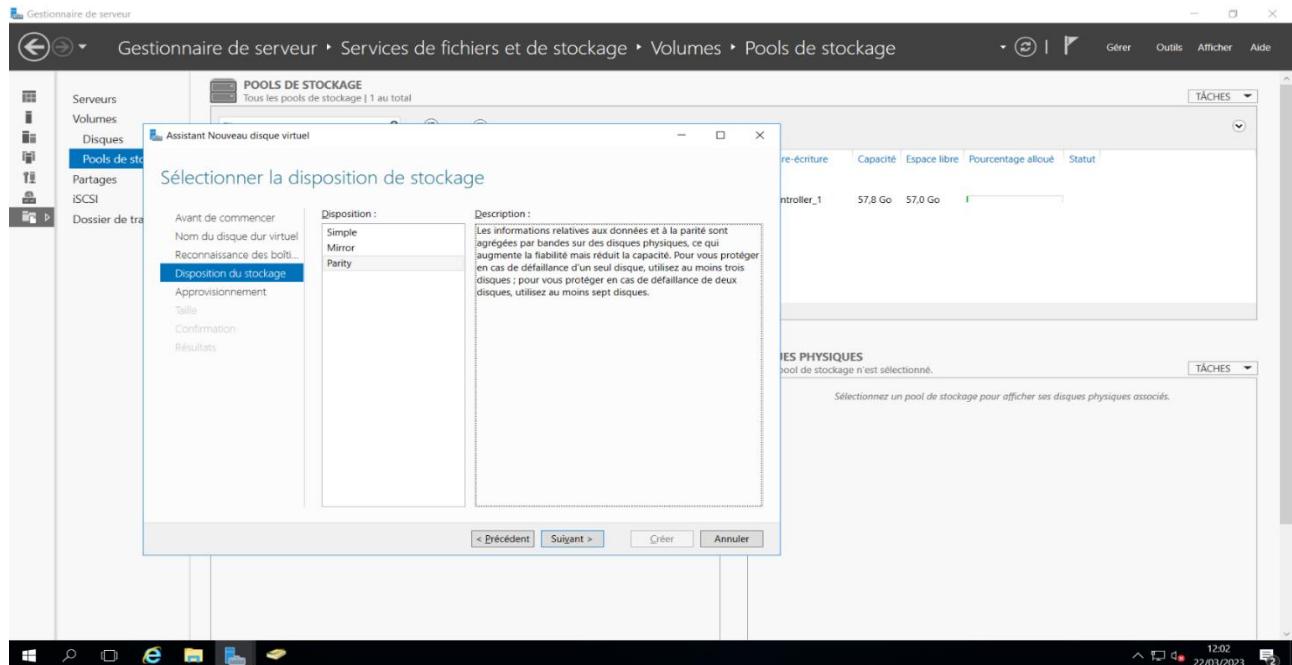


Un nouvel assistant s'ouvre.

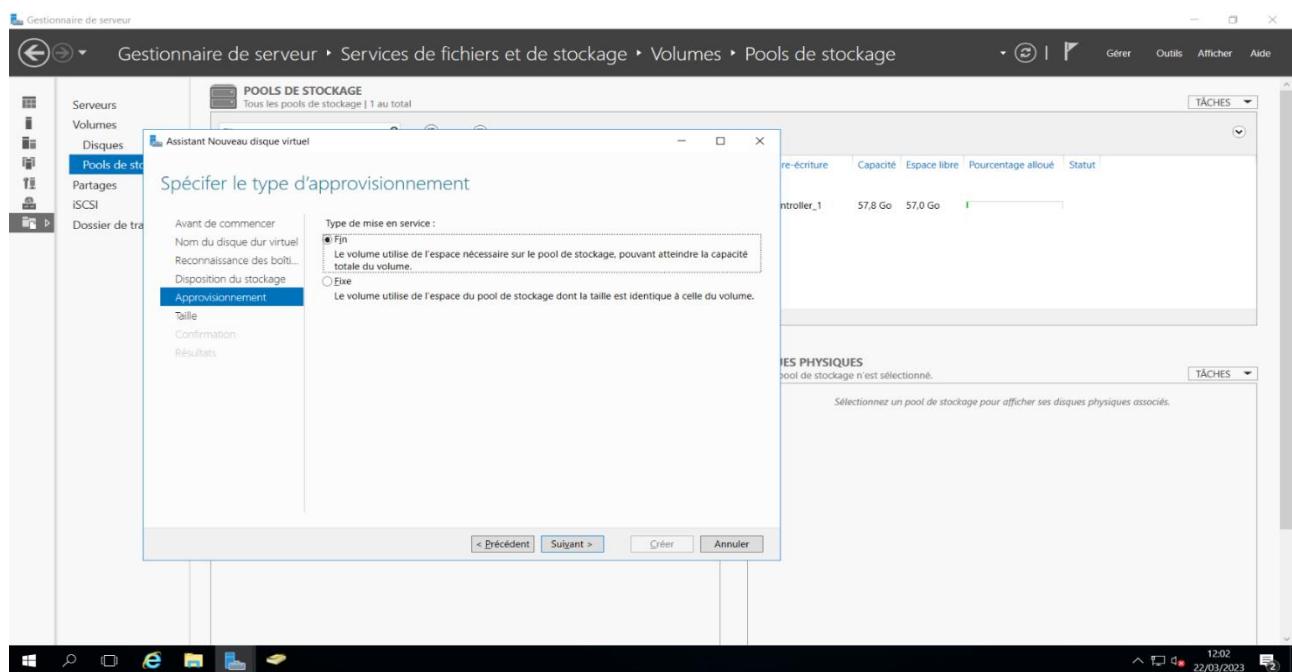
On nomme notre disque dur virtuel puis on clique sur « Suivant ».



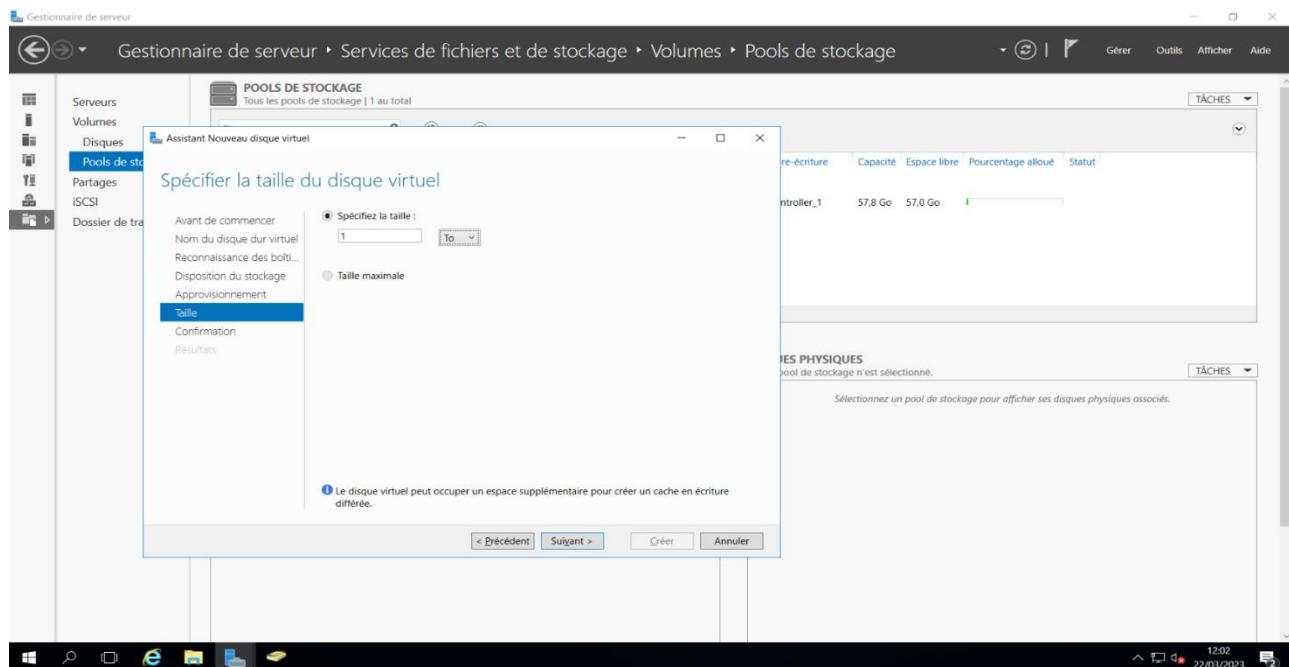
On sélectionne « Parity » puis on clique sur « Suivant ».



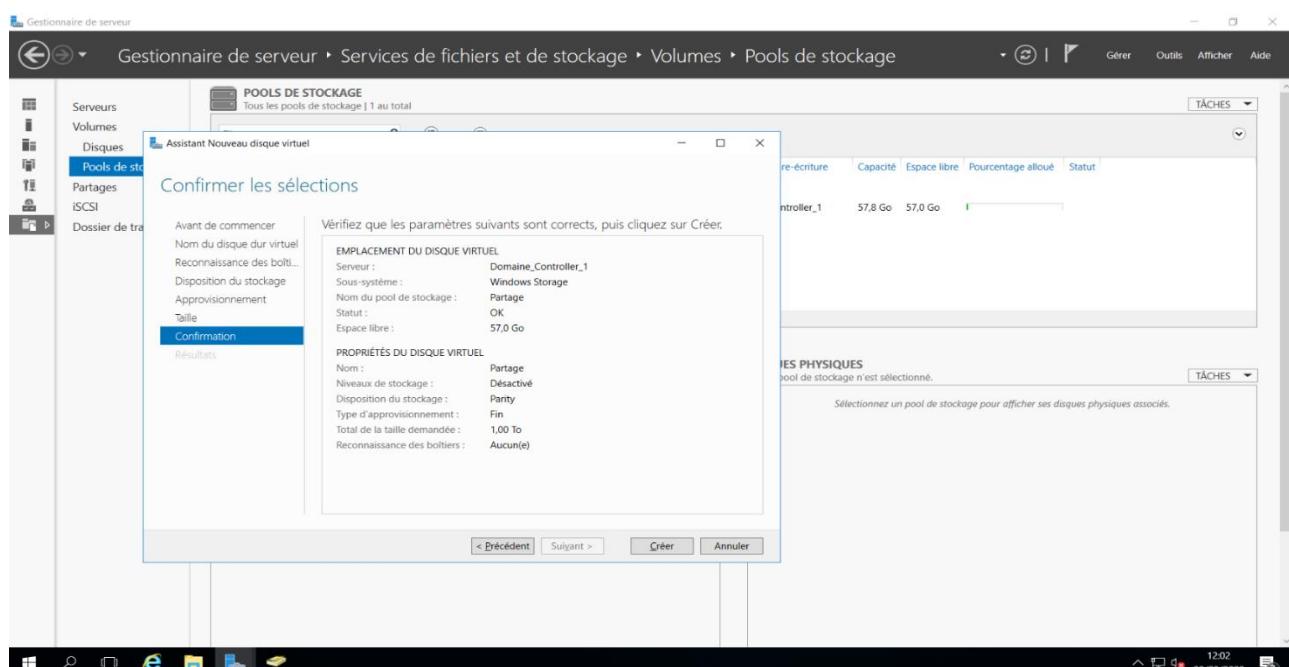
On coche « Fin » puis on clique sur « Suivant ».



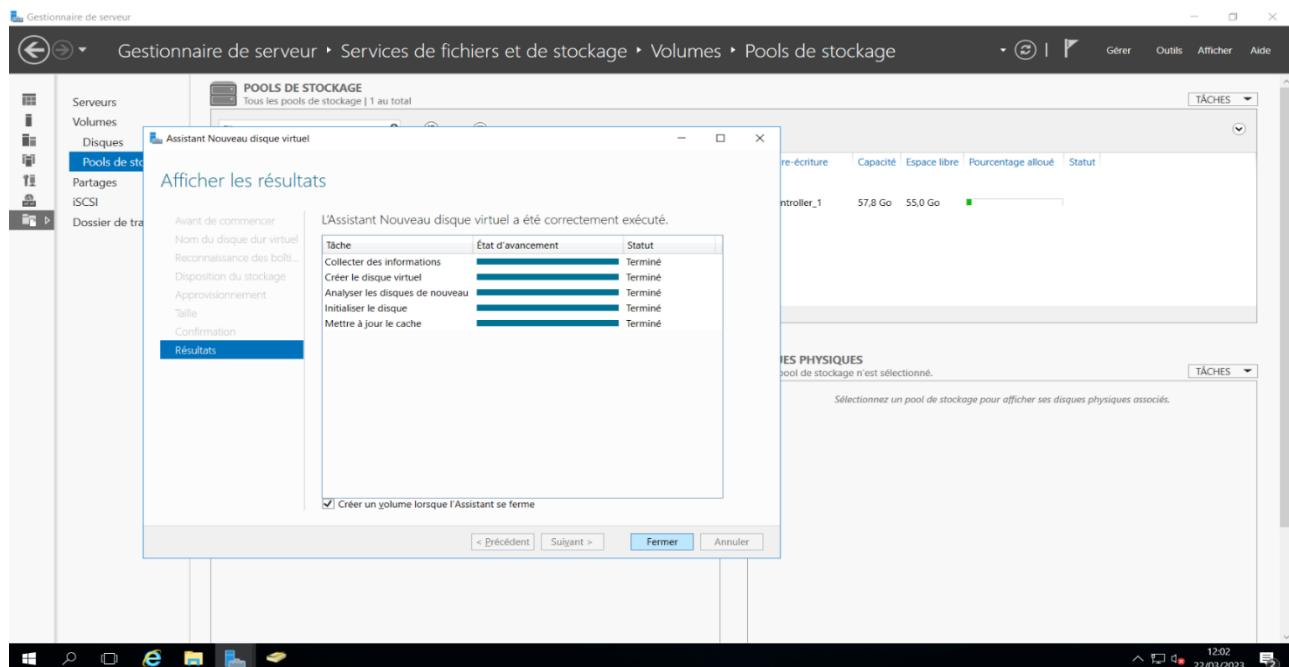
On spécifie la taille puis on clique sur « Suivant ».



On clique sur « Crée ».

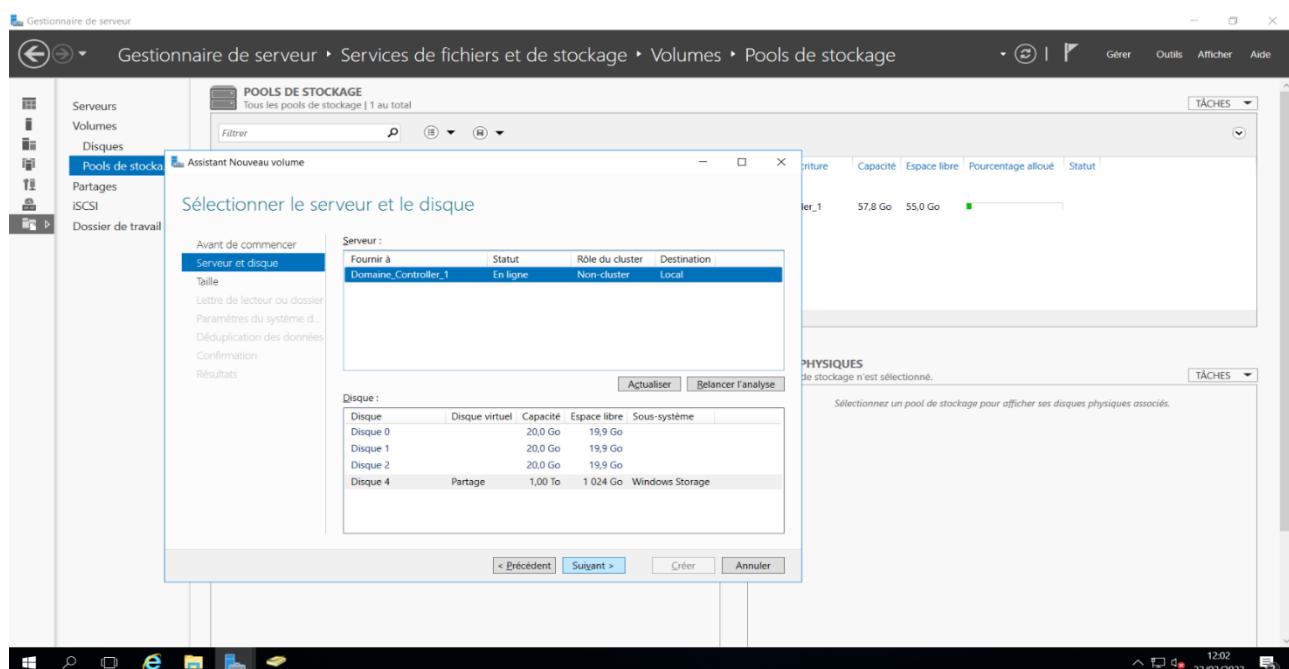


On clique sur « Fermer » en vérifiant que la case « Créer un Volume lorsque l'Assistant se ferme » est cochée.

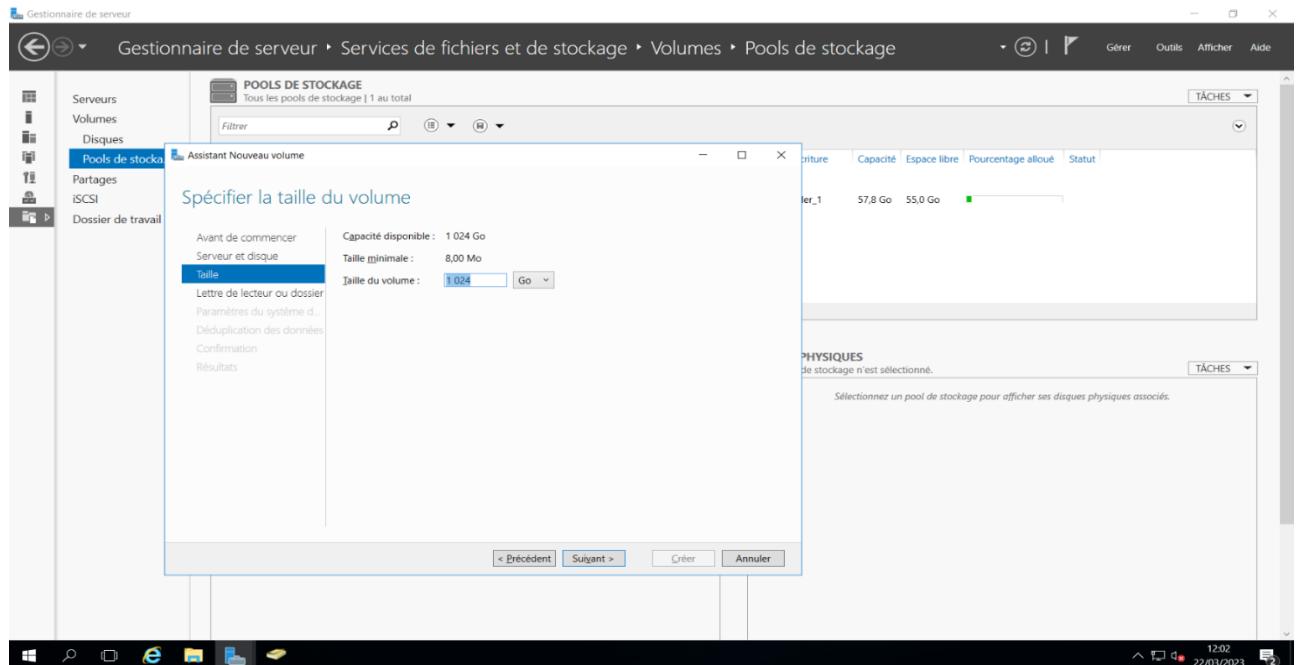


L'assistant pour créer un nouveau volume s'ouvre.

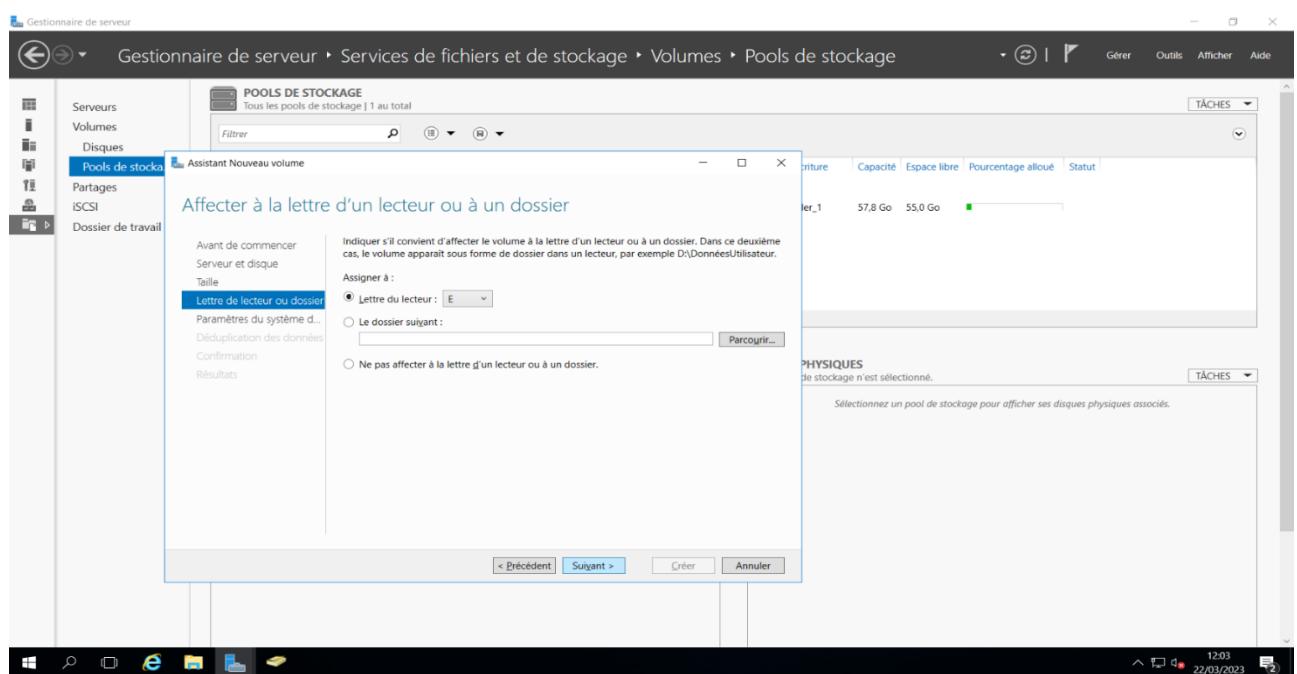
On sélectionne notre disque virtuel puis on clique sur « Suivant ».



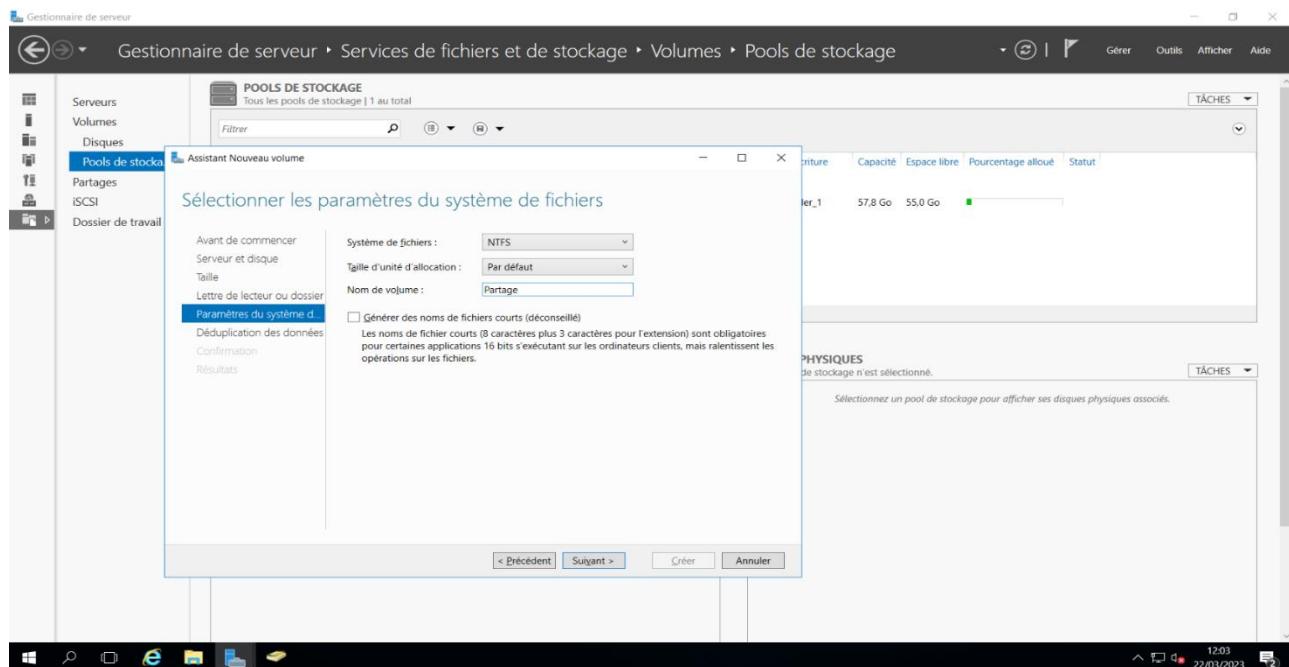
On spécifie la taille puis on clique sur « Suivant ».



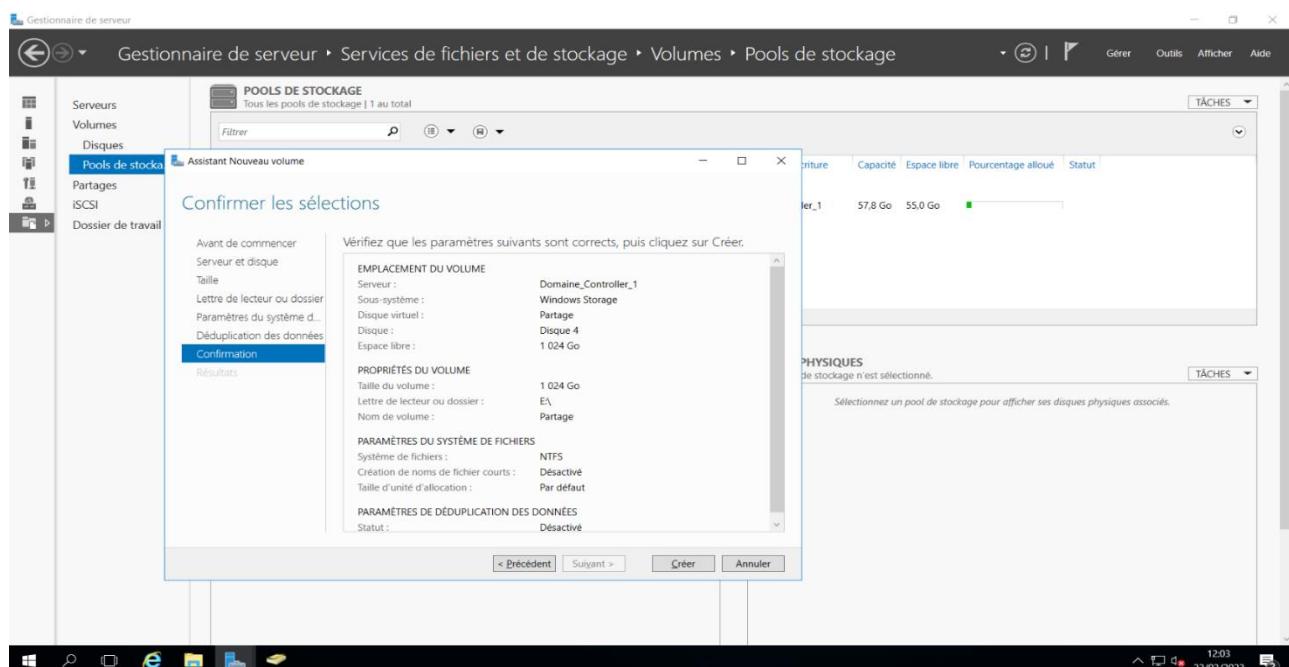
On lui donne une lettre puis on clique sur « Suivant ».



On le nomme puis on clique sur « Suivant ».

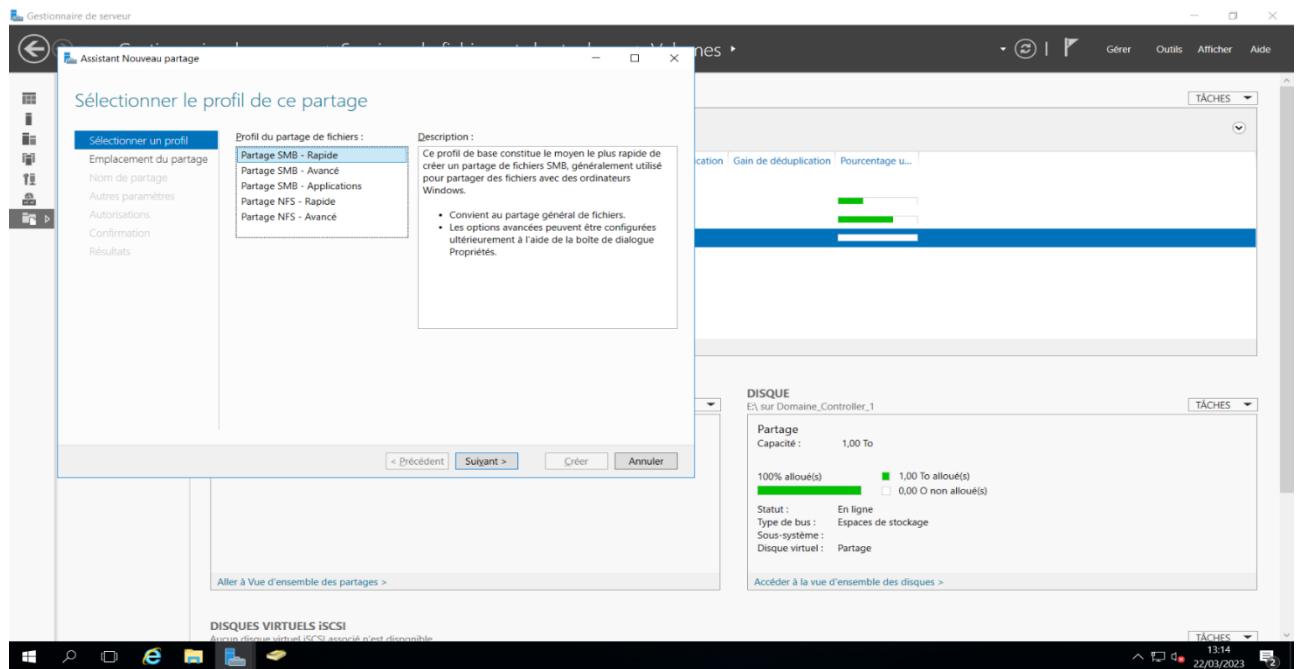


On clique sur « Crée ».

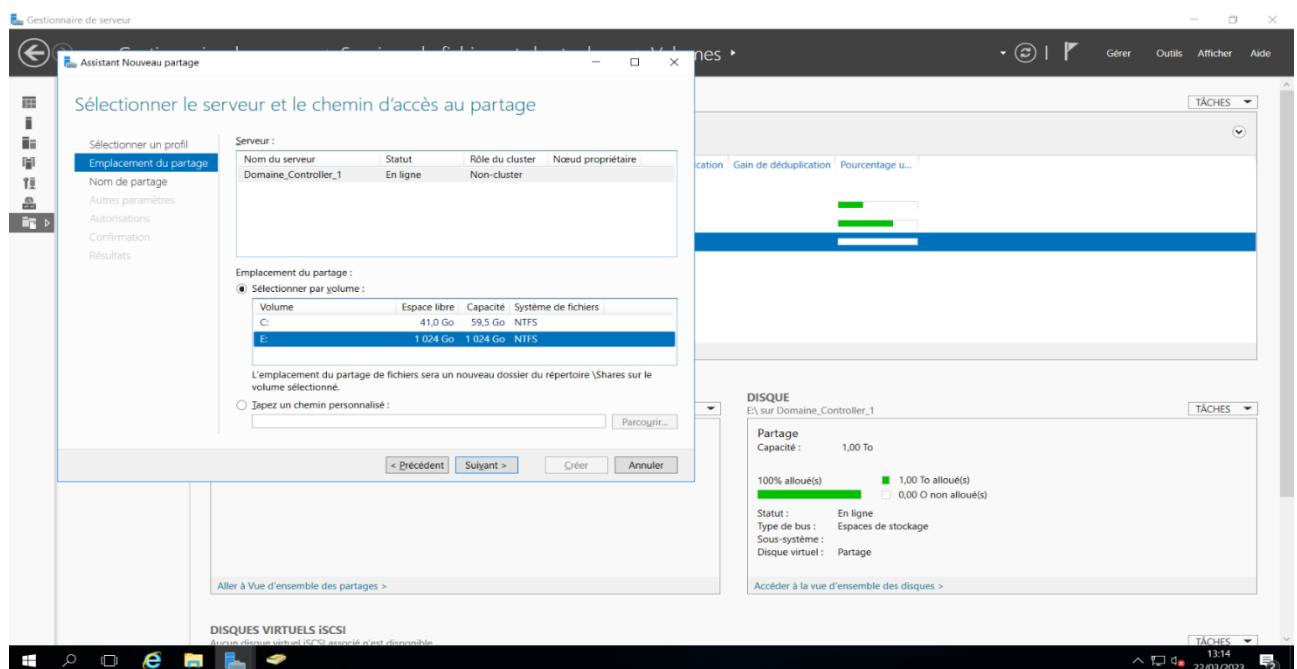


Puis on clique sur « Fermer ».

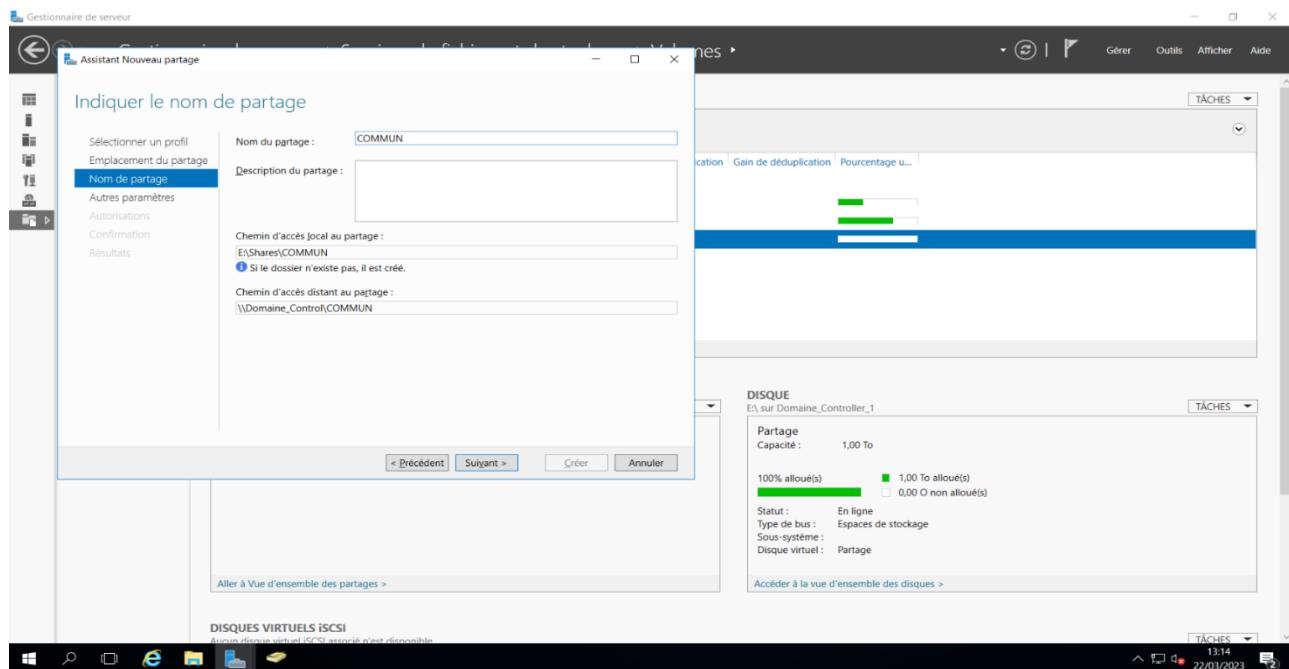
Maintenant que notre volume est créé, on retourne dans le volet « Volumes » puis on fait clic droit sur notre Volume destiné au Partage, puis on clique sur « Nouveau partage », et un assistant s'ouvre. On clique sur « Suivant ».



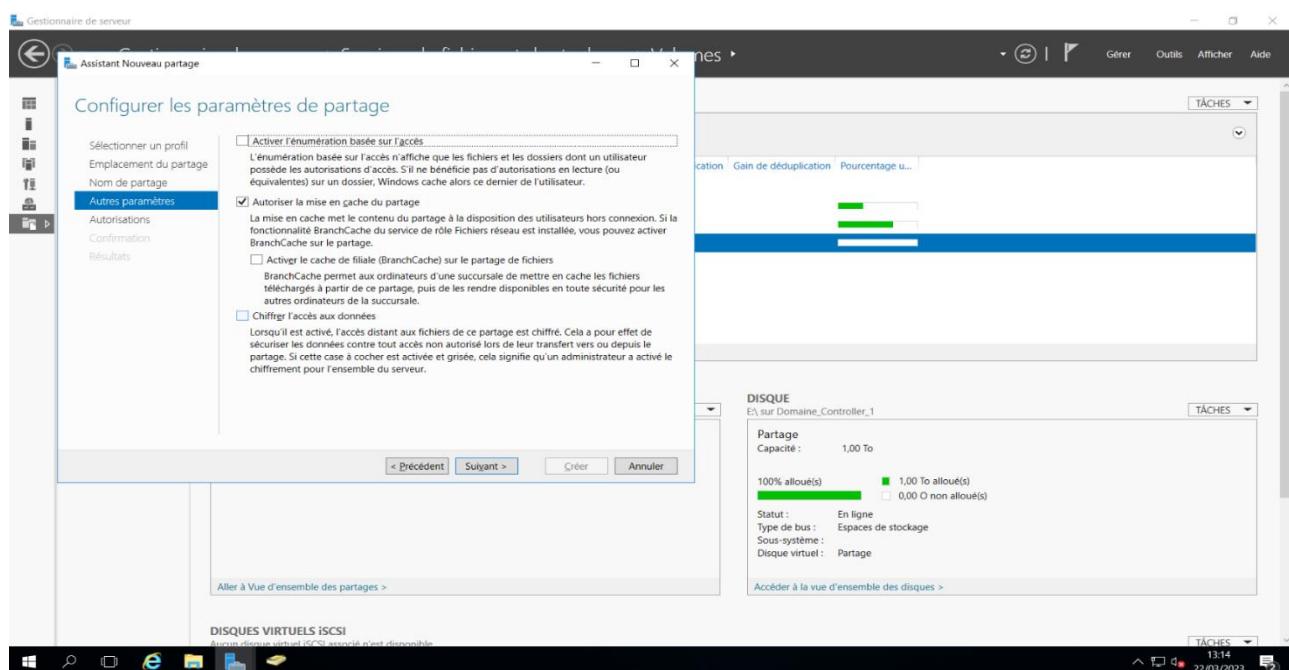
On coche « Sélectionner par volume », on sélectionne notre disque puis on clique sur « Suivant ».



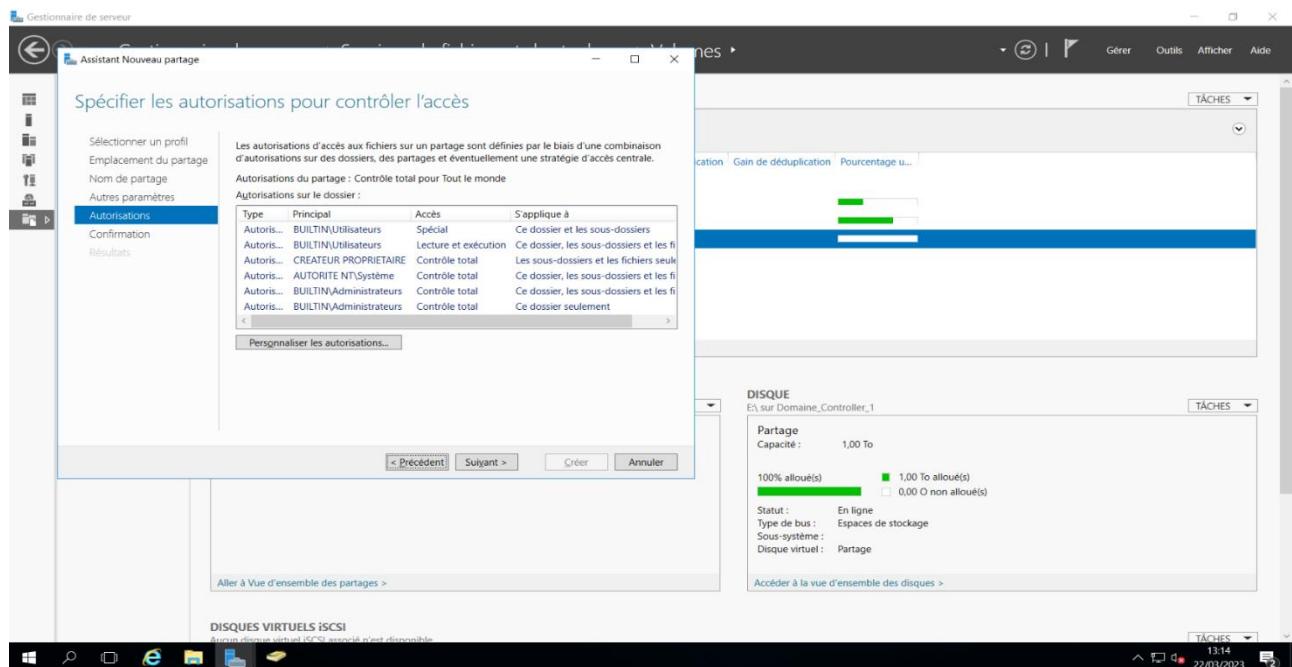
On nomme notre partage, on spécifie le chemin d'accès de ce dernier puis on clique sur « Suivant ».



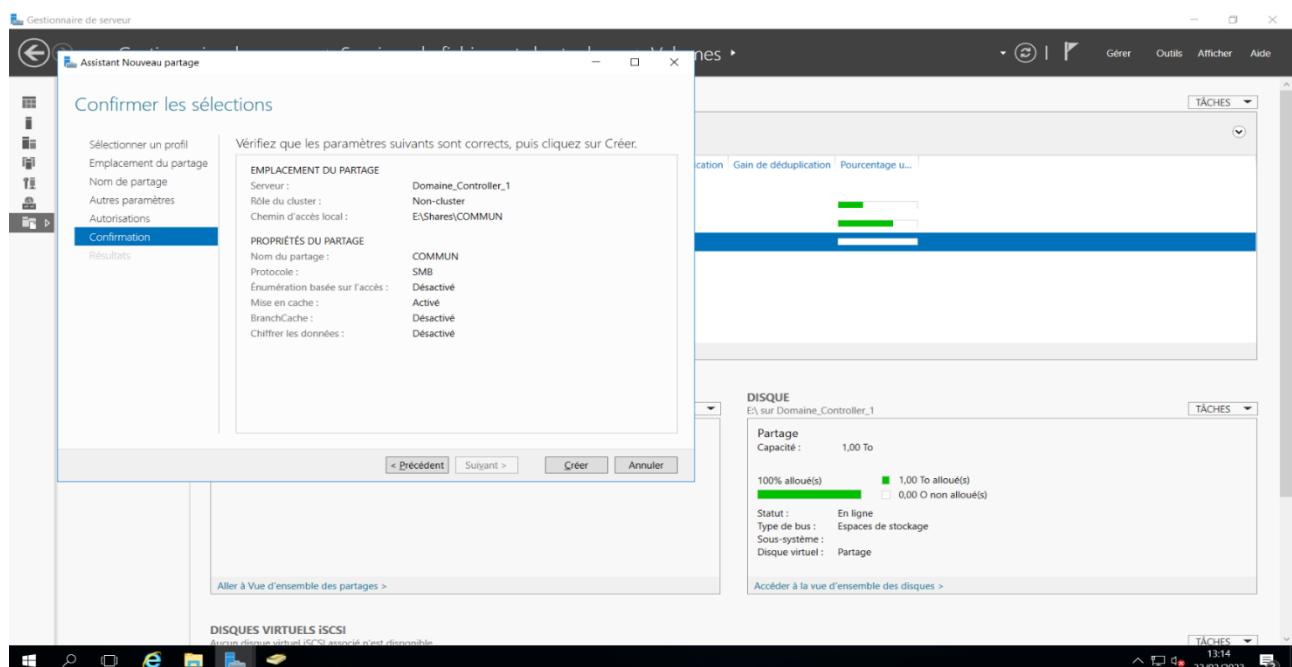
On laisse comme tel et on clique sur « Suivant ».



On spécifie les autorisations puis on clique sur « Suivant ».



On clique sur « Crée »



On attend la fin de la création, puis on clique sur « Fermer ».

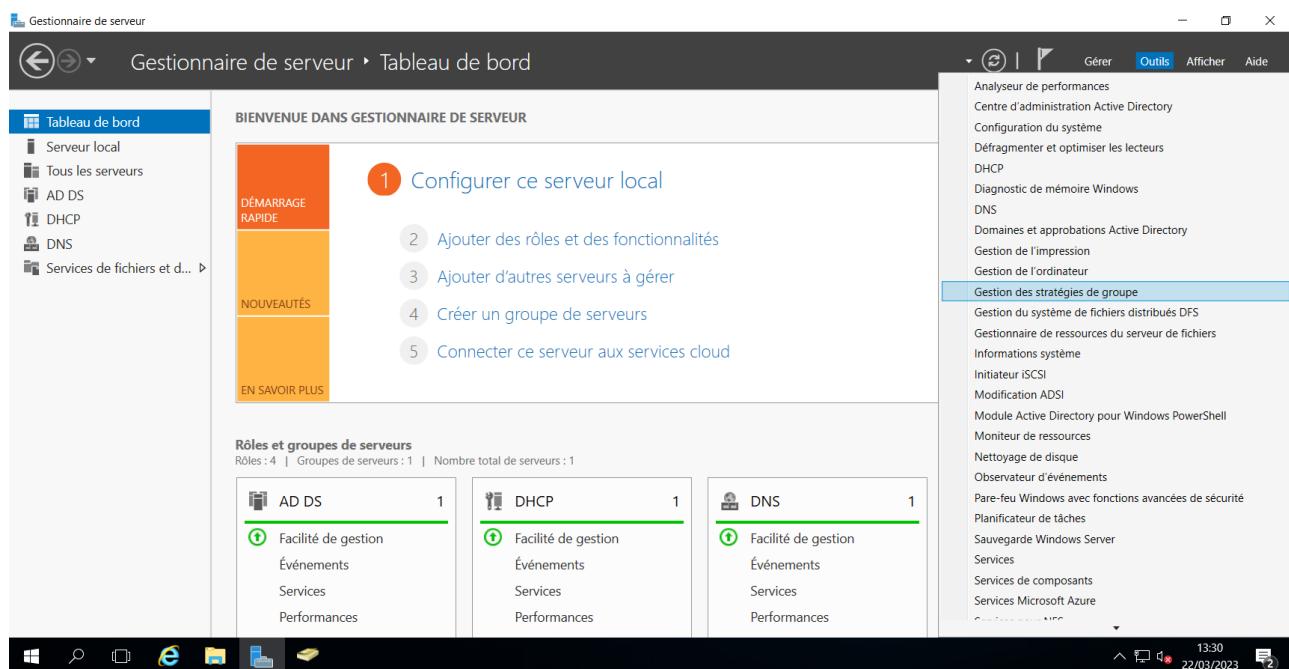
Notre partage est désormais créé et est accessible par nos utilisateurs dans le domaine.

## VIII) Création de GPO

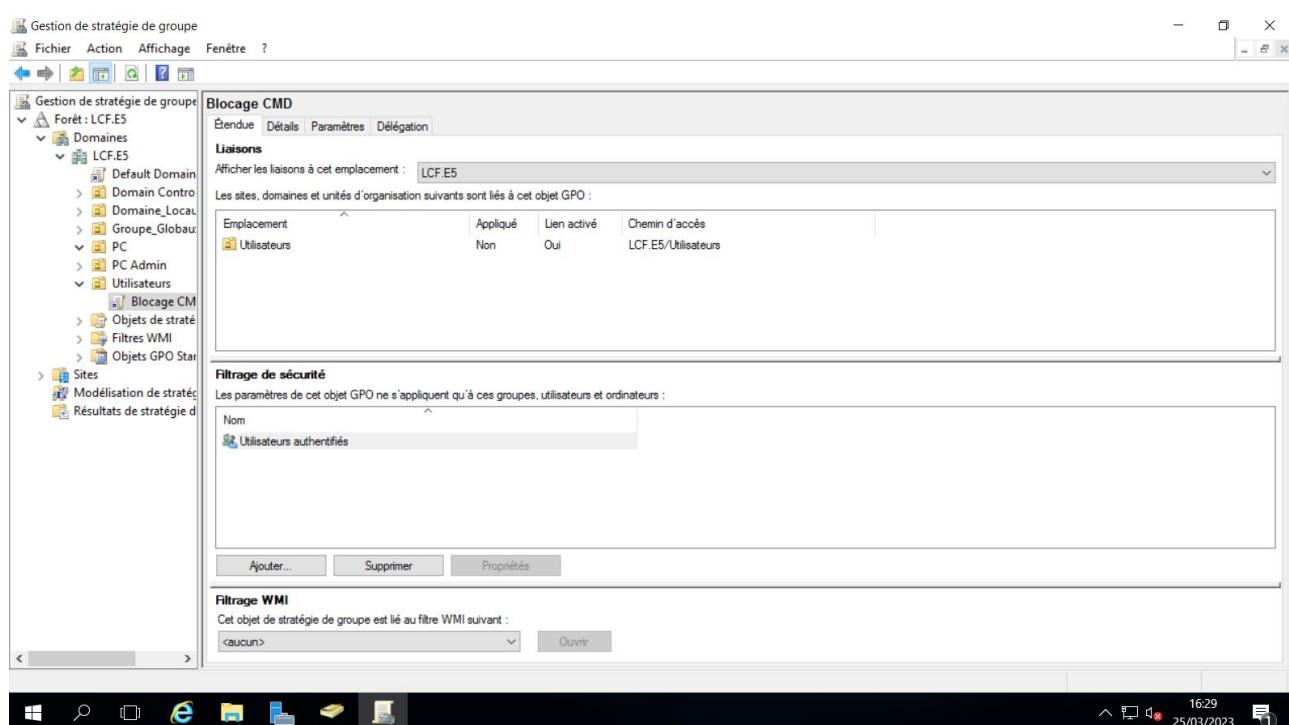
Maintenant que tous nos services sont effectifs et qu'un Dossier partagé a été créé, on peut mettre en place des GPO pour limiter l'accès des utilisateurs aux ressources sensibles.

Pour ce faire, un blocage du cmd a été mis en place pour empêcher les utilisateurs de l'utiliser.

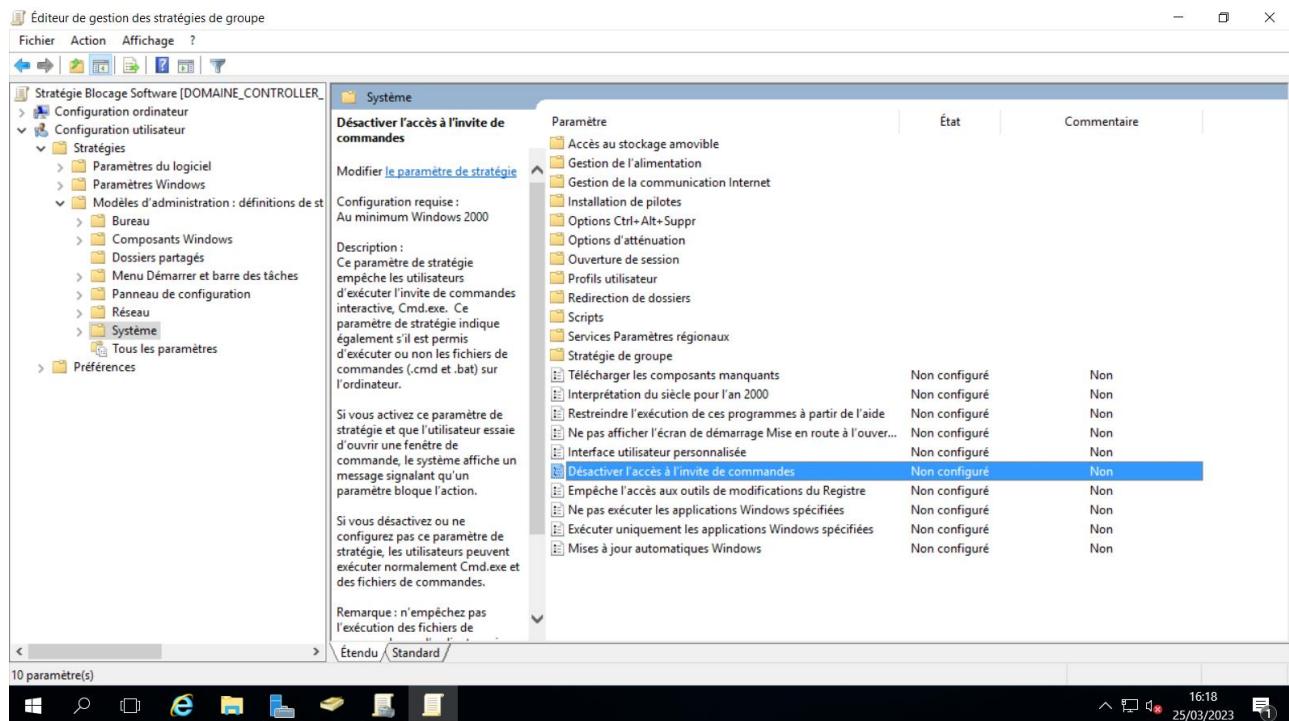
Pour faire ceci, on clique sur « Outils » en haut à droite de notre tableau de bord, puis on clique sur « Gestion des stratégies de groupe ».



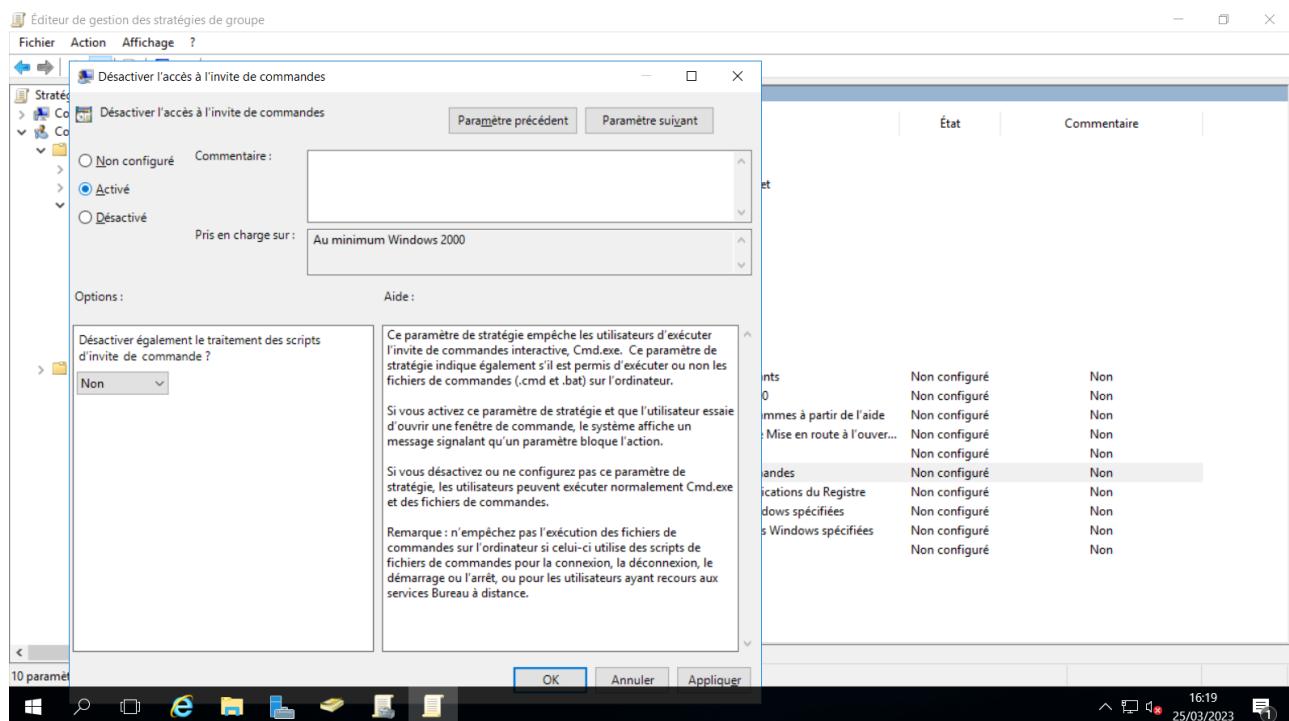
On va dans les répertoires de notre domaine, puis on fait un clic droit sur notre dossier utilisateurs, et on clique sur « créer un objet et le lier ici » on va alors le nommer.



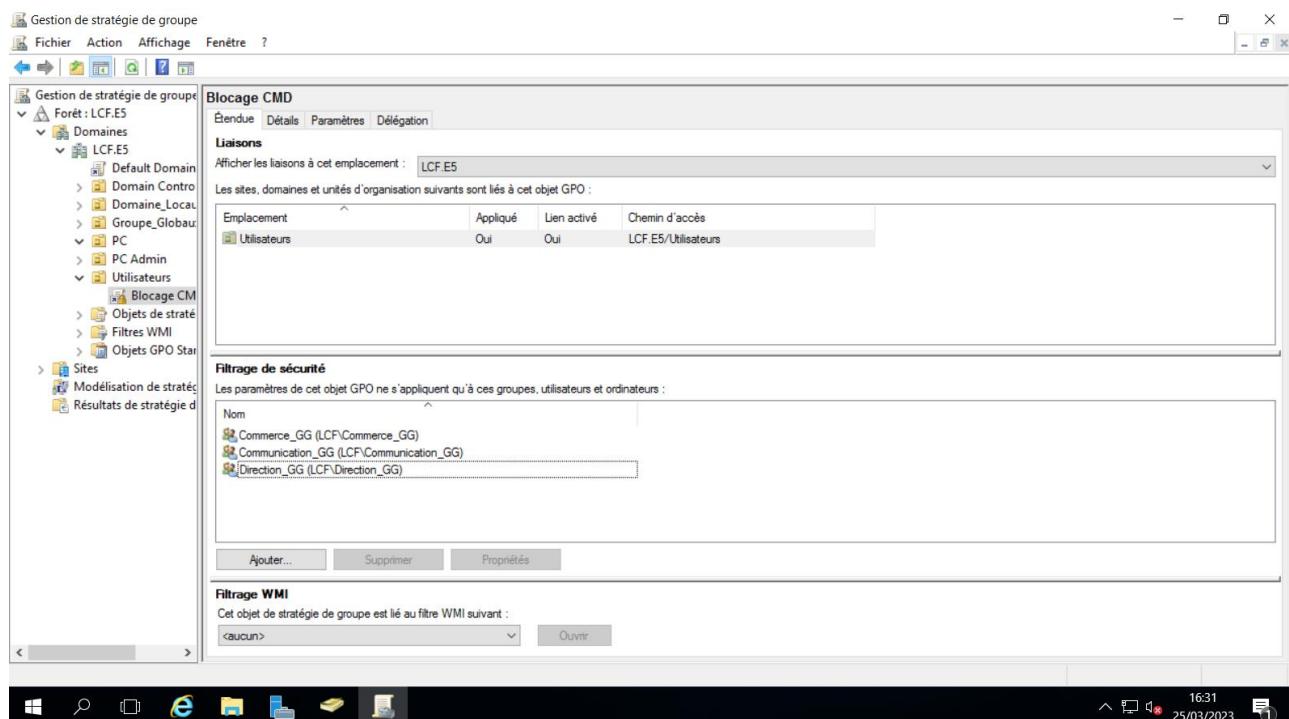
On va dans l'onglet « Système », sous « Configuration utilisateur », puis on clique sur « Désactiver l'accès à l'invite de commande ».



On coche la case « Activé » puis on clique sur « Appliquer ».



On configure donc nos groupes auquel notre GPO va s'appliquer.



Notre GPO est désormais active. Pour l'activer immédiatement, on ouvre notre CMD sur notre Windows Server 2016 et on tape « gpupdate /force ».

Suite à ça, notre GPO est active sur nos utilisateurs dans le domaine, l'invite de commande est donc bloquée à moins d'être un administrateur du domaine.

## Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

## ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

| DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE  |   | N° réalisation : 2           |
|--|---|------------------------------|
| Nom, prénom : GUELLUY, Pascal  |   | N° candidat : 02246218463    |
| Épreuve ponctuelle <input type="checkbox"/>  | Contrôle en cours de formation <input type="checkbox"/> | Date : ..... / ..... / ..... |
| Organisation support de la réalisation professionnelle   |   |                              |
| Intitulé de la réalisation professionnelle : Sécurisation d'un environnement Windows Server 2016 avec un pare feu et une solution de supervision   |   |                              |
| Période de réalisation :   | Lieu : Montpellier - Esicad                             |                              |
| Modalité : <input type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe   |   |                              |
| <b>Compétences travaillées</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> Concevoir une solution d'infrastructure réseau</li> <li><input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau</li> <li><input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau</li> </ul> |   |                              |
| <b>Conditions de réalisation<sup>5</sup> (ressources fournies, résultats attendus)</b> <p>Les ressources ajoutées sont correctement liées au contrôleur de domaine et sont effectives.</p>   |   |                              |
| <b>Description des ressources documentaires, matérielles et logicielles utilisées<sup>6</sup></b> <ul style="list-style-type: none"> <li>- Documentation technique</li> <li>- Vmware Workstation Pro (clé de licence fournie)</li> </ul>   |   |                              |
| <b>Modalités d'accès aux productions<sup>7</sup> et à leur documentation<sup>8</sup></b> <p><a href="https://pascal-guelluy.fr/">https://pascal-guelluy.fr/</a></p>  |   |                              |

<sup>5</sup> En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

<sup>6</sup> Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

<sup>7</sup> Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

<sup>8</sup> Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemple schéma complet de réseau mis en place et configurations des services.

**Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs**

Après avoir installé et configurer nos Windows Server 2016, il faut désormais pouvoir les sécuriser et les superviser.

Pour ce faire, l'installation d'un Firewall et d'un outil de supervision est demandé.

Nous allons donc installer le Firewall Pfsense, ainsi que Nagios afin de superviser notre serveur.

Pour simuler ces installations, nos 2 solutions seront installées en machine virtuelle, Nagios sera installer via un serveur apache2 sur Debian 11.

# **PPE 2 : Sécurisation d'un environnement Windows Server 2016 avec un pare feu et une solution de supervision**

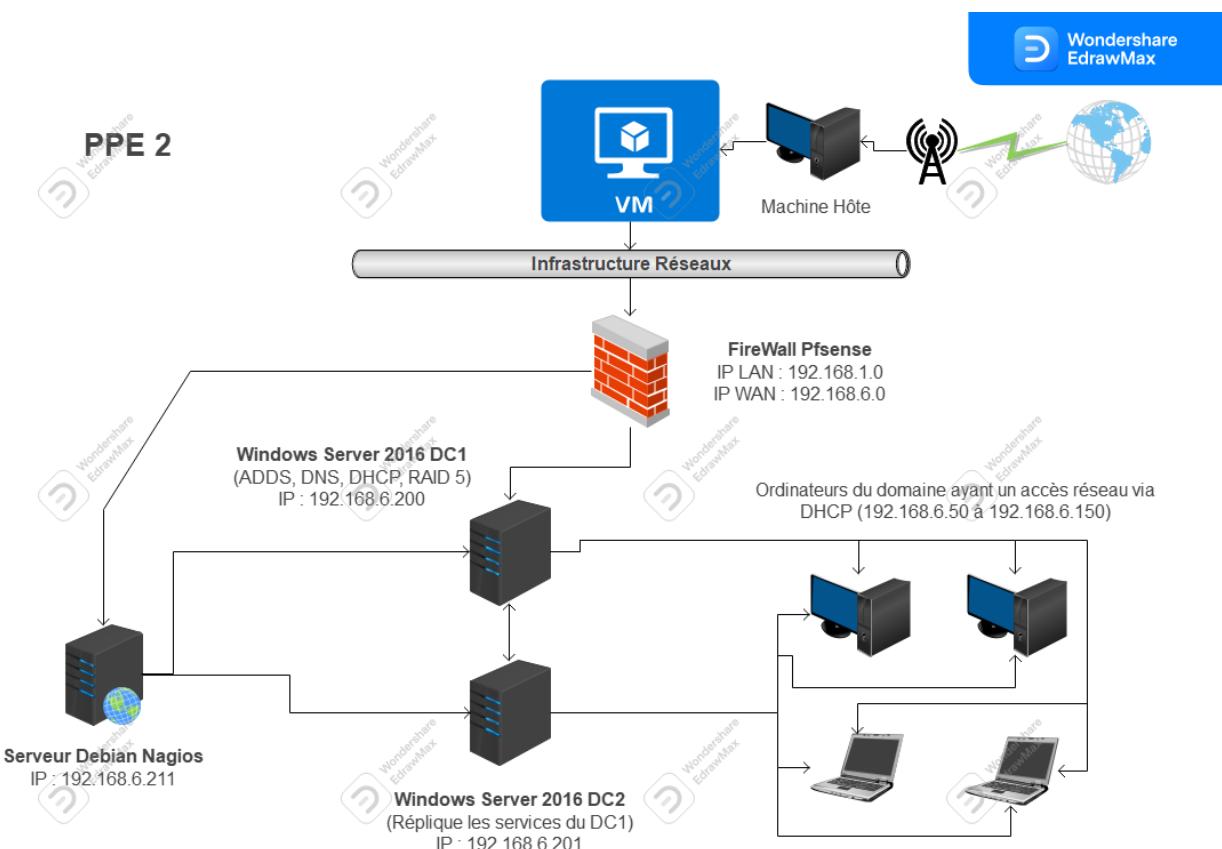
## Sommaire

|      |                                      |    |
|------|--------------------------------------|----|
| I)   | Schéma Réseau du projet .....        | 43 |
| II)  | Installation de pfSense.....         | 44 |
| III) | Installation d'Eyes Of Network ..... | 64 |

## I) Schéma Réseau du projet

Afin de réaliser notre projet, un schéma réseau a été établis pour bien comprendre ce qui est attendu à travers cette intervention.

Nous avons donc ajouté un Firewall pfSense afin de sécuriser notre infrastructure mais aussi la solution Eyes of Network qui permet de vérifier l'état de nos machines sur le réseau.



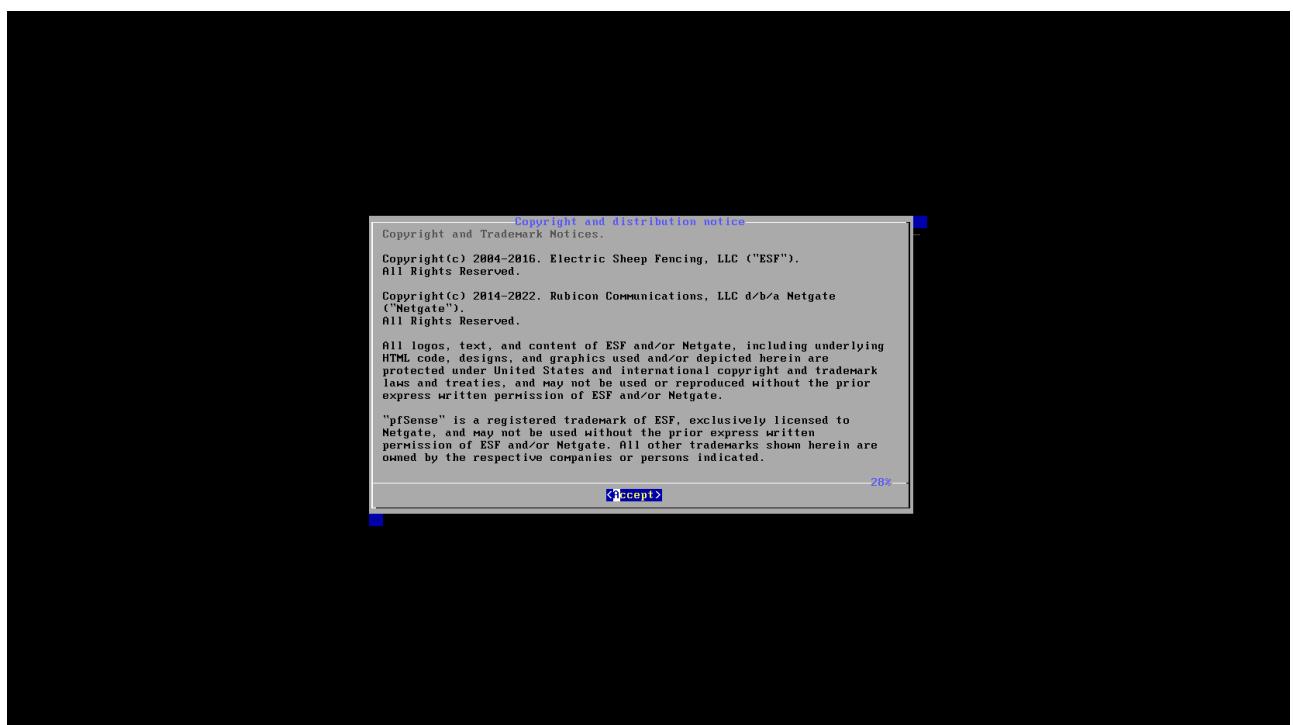
## II) Installation de pfSense

Afin de sécuriser notre environnement, nous allons installer pfSense sur VMware Workstation Pro et le rattacher à notre Windows Server 2016.

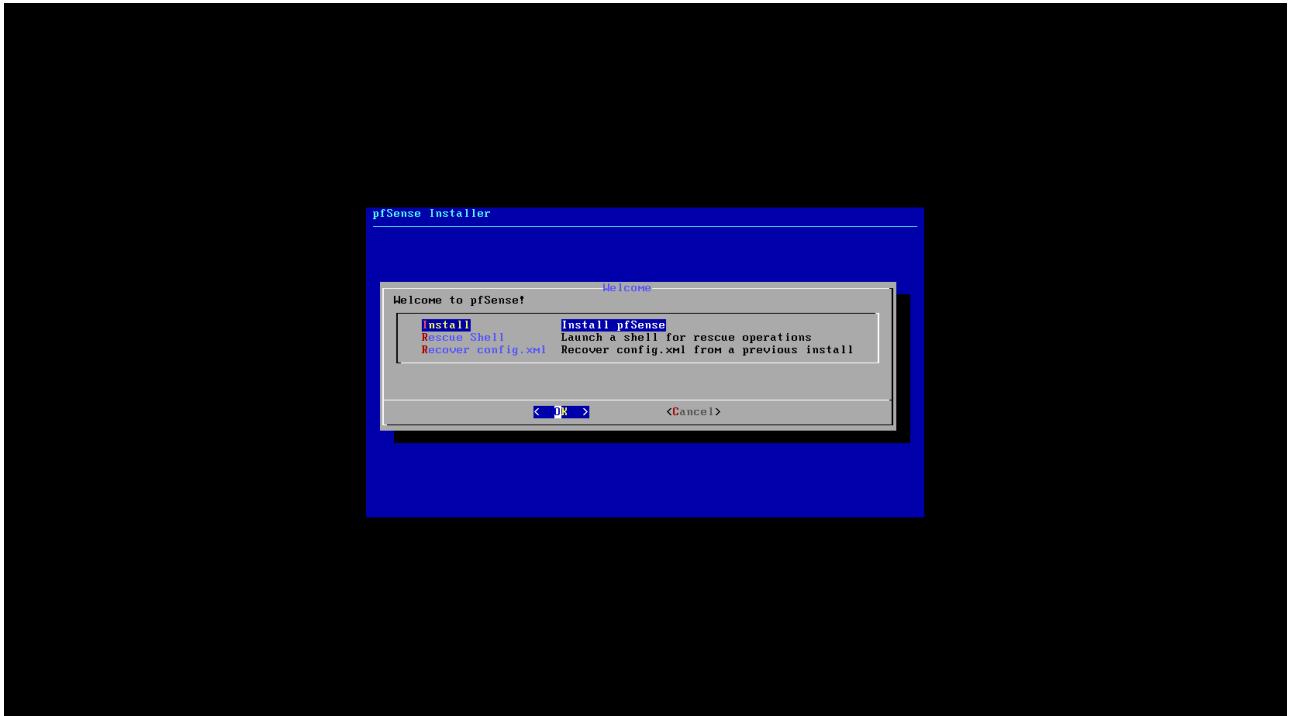
Au premier lancement de pfSense, nous arrivons sur cette page, il suffit d'attendre pour passer à la suivante.



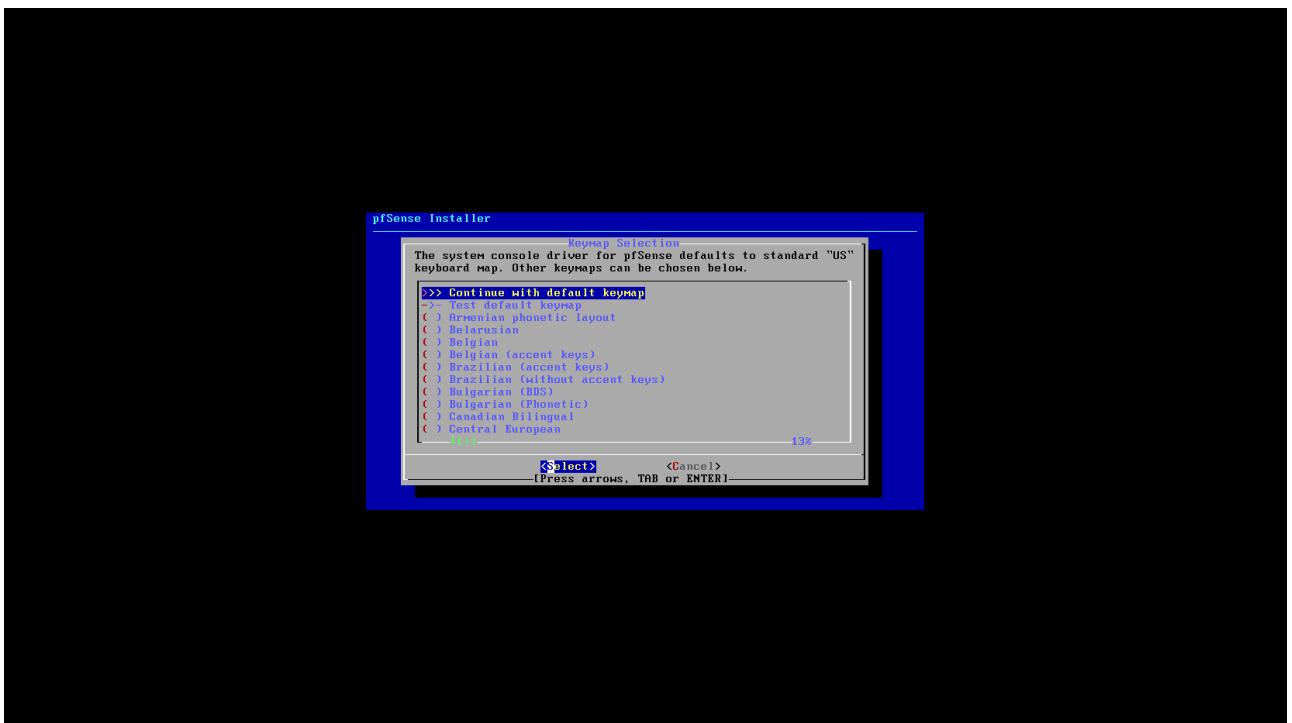
On clique sur « Accept » quand la nouvelle page s'ouvre.



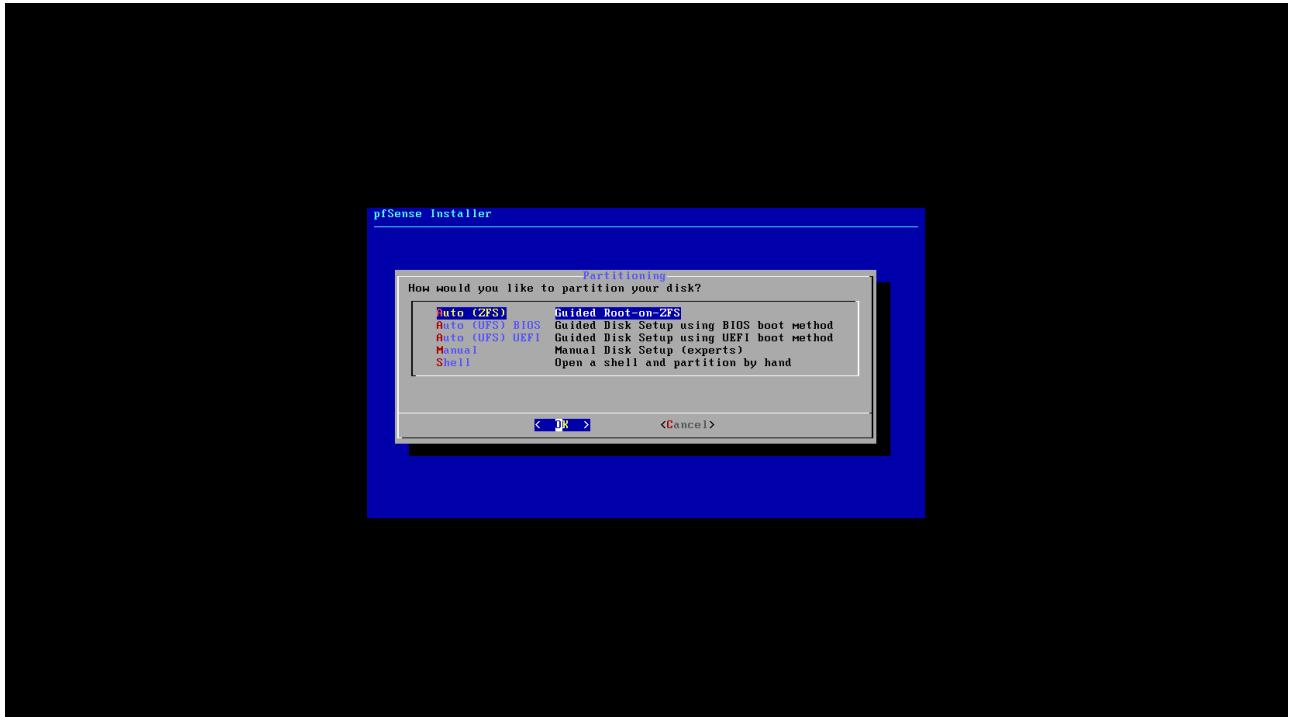
On clique sur « Install ».



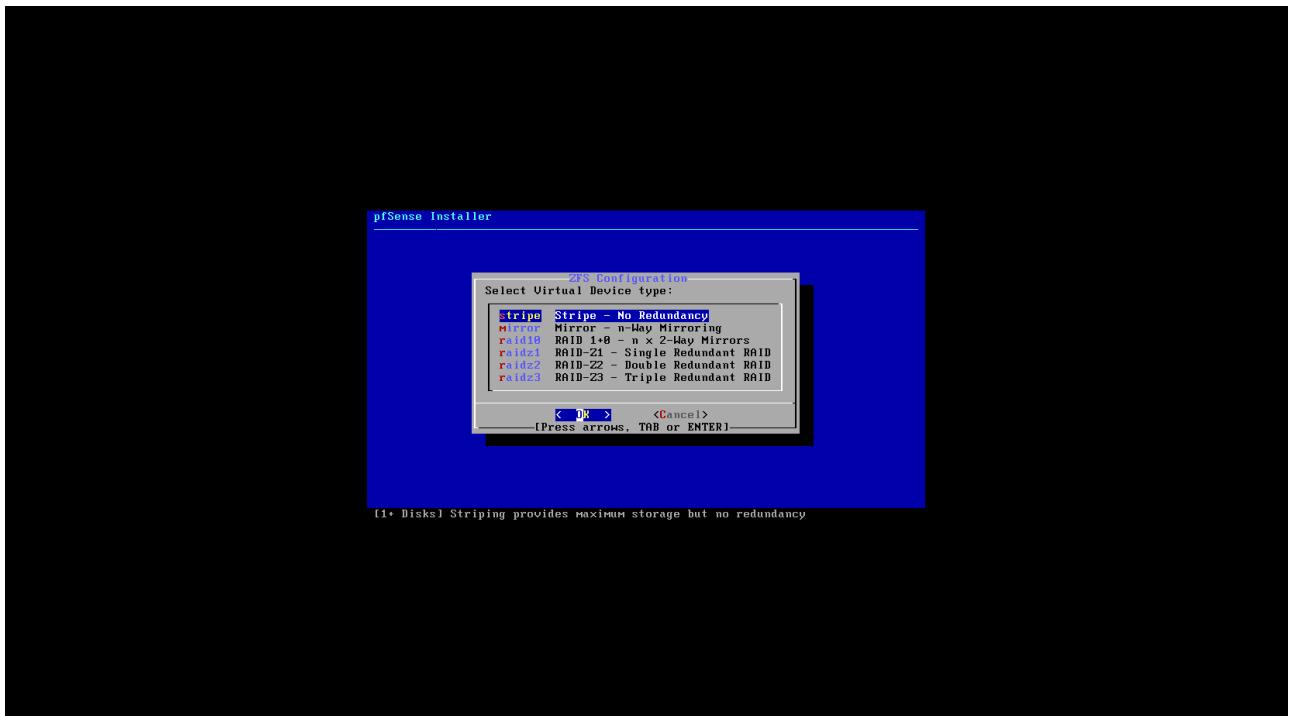
On choisit la langue de notre clavier puis on appuie sur entrer de notre clavier.



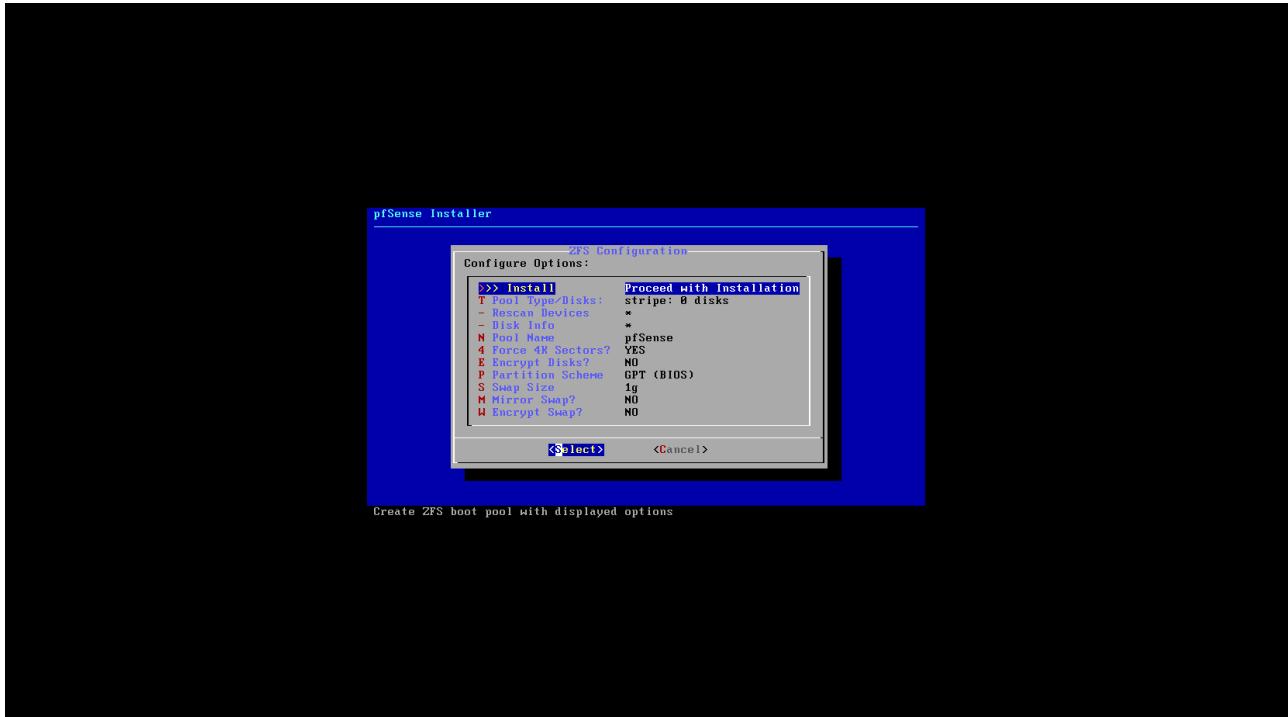
On choisit « Auto (ZFS) » puis on appuie sur entrer.



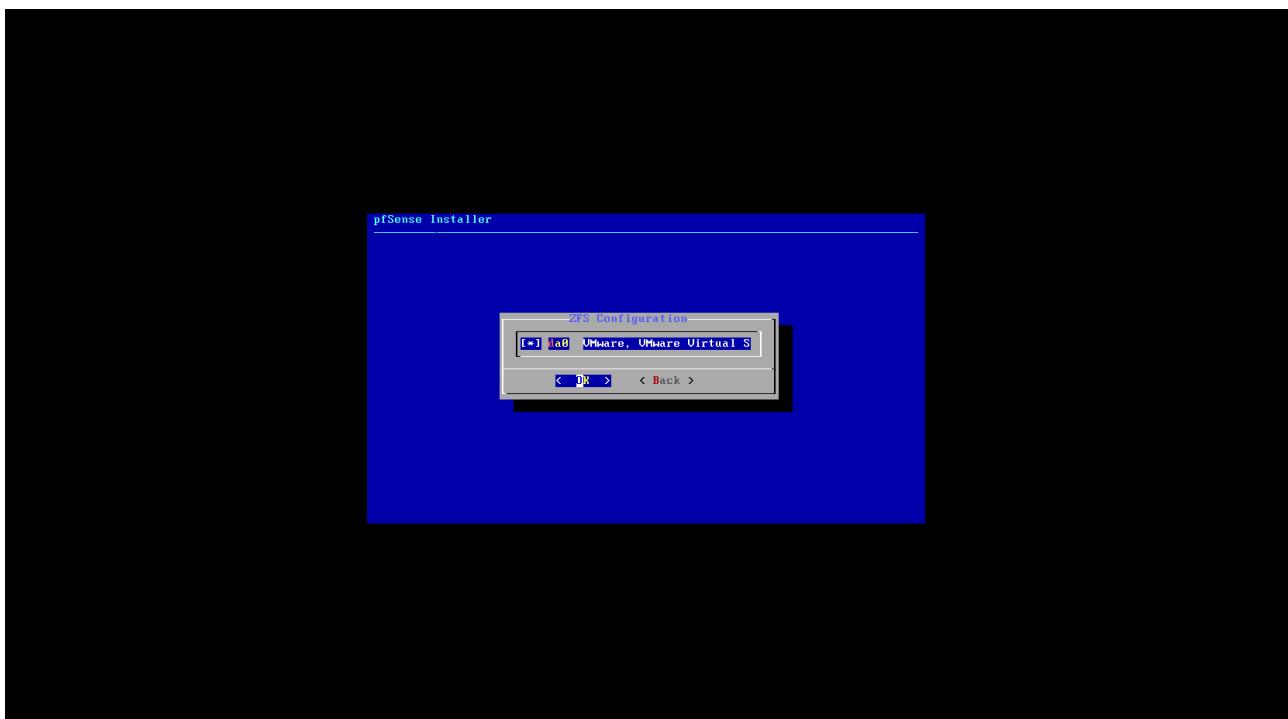
On choisit « Stripe ».



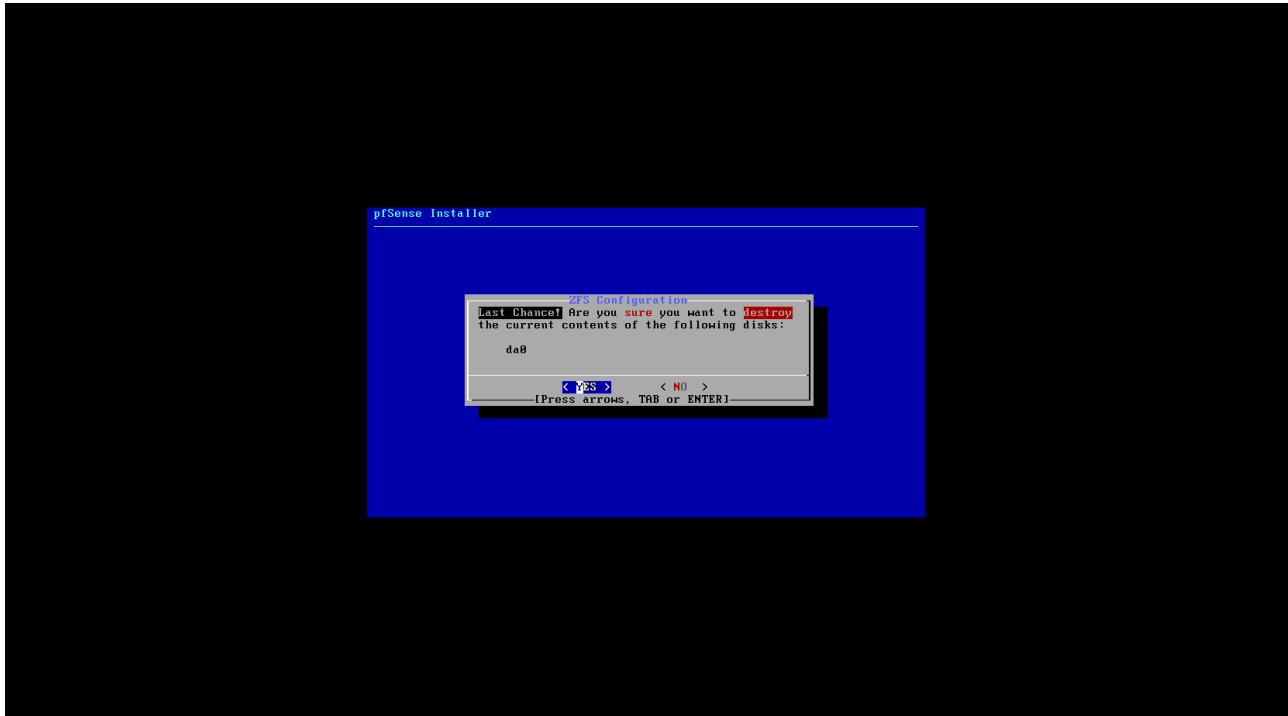
On sélectionne « Install ».



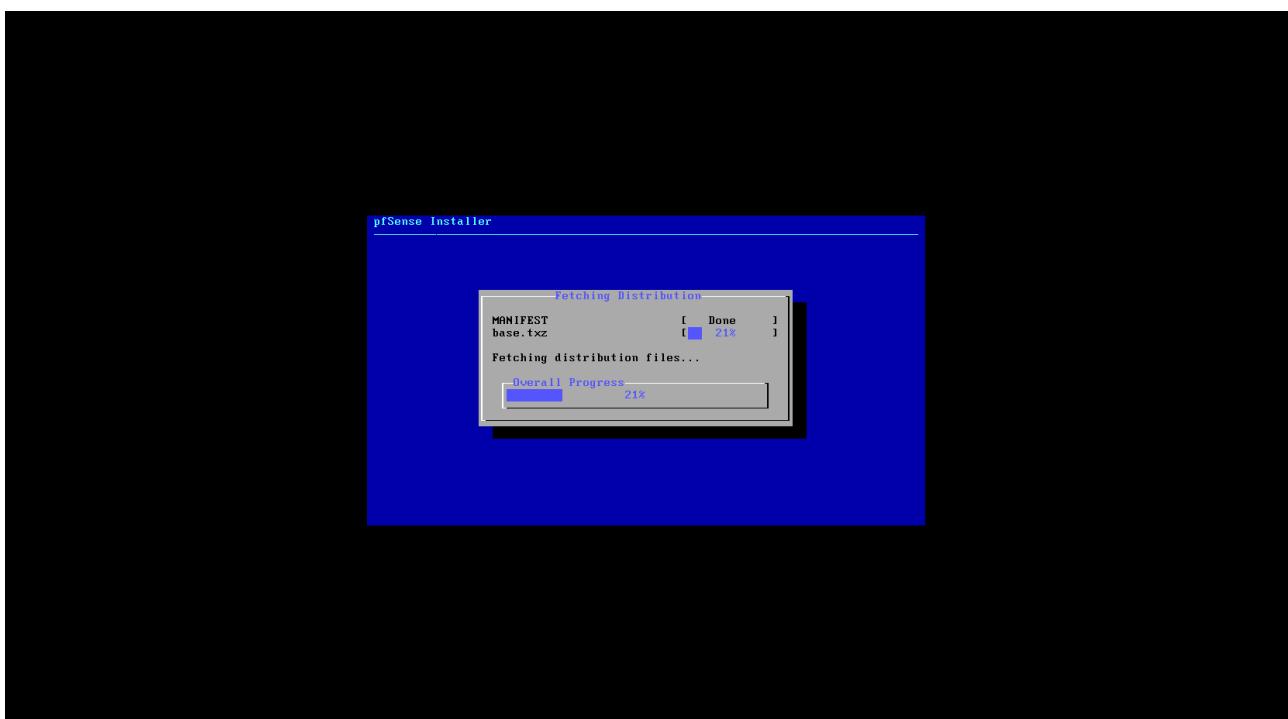
On appuie sur la touche espace de notre clavier pour cocher la case, puis on fait « OK ».



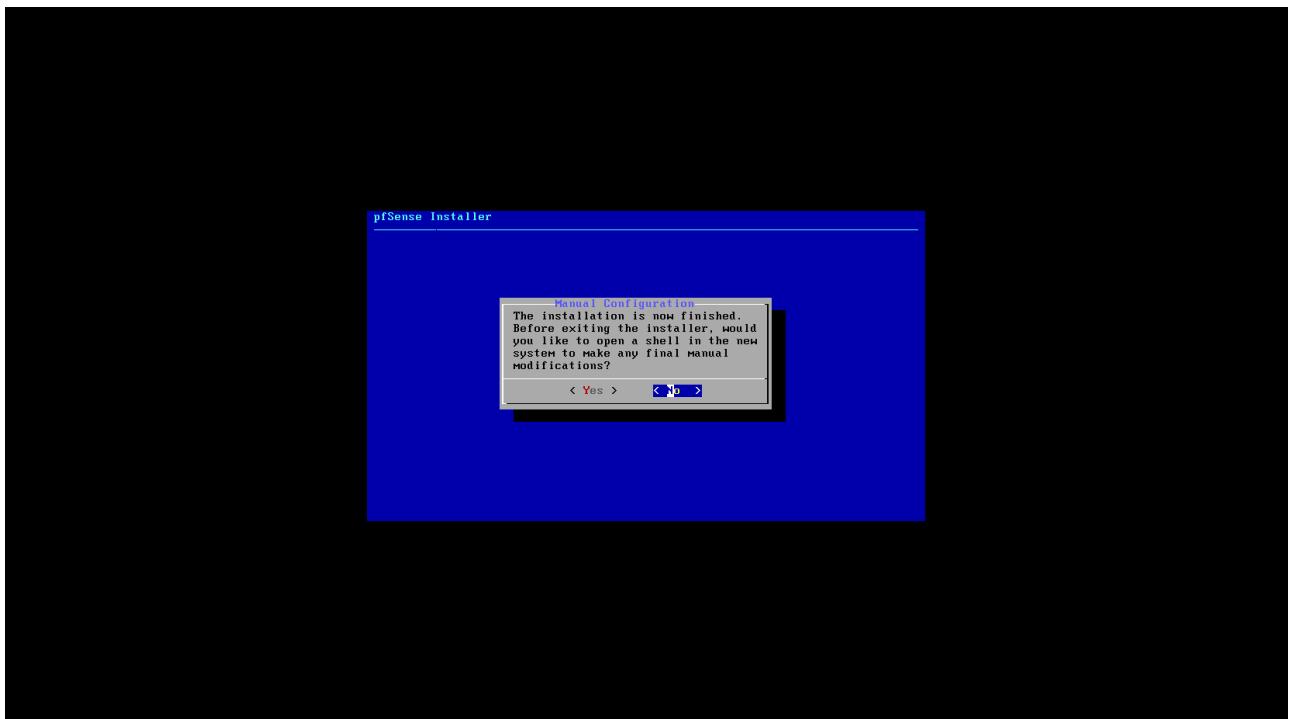
On choisit « YES ».



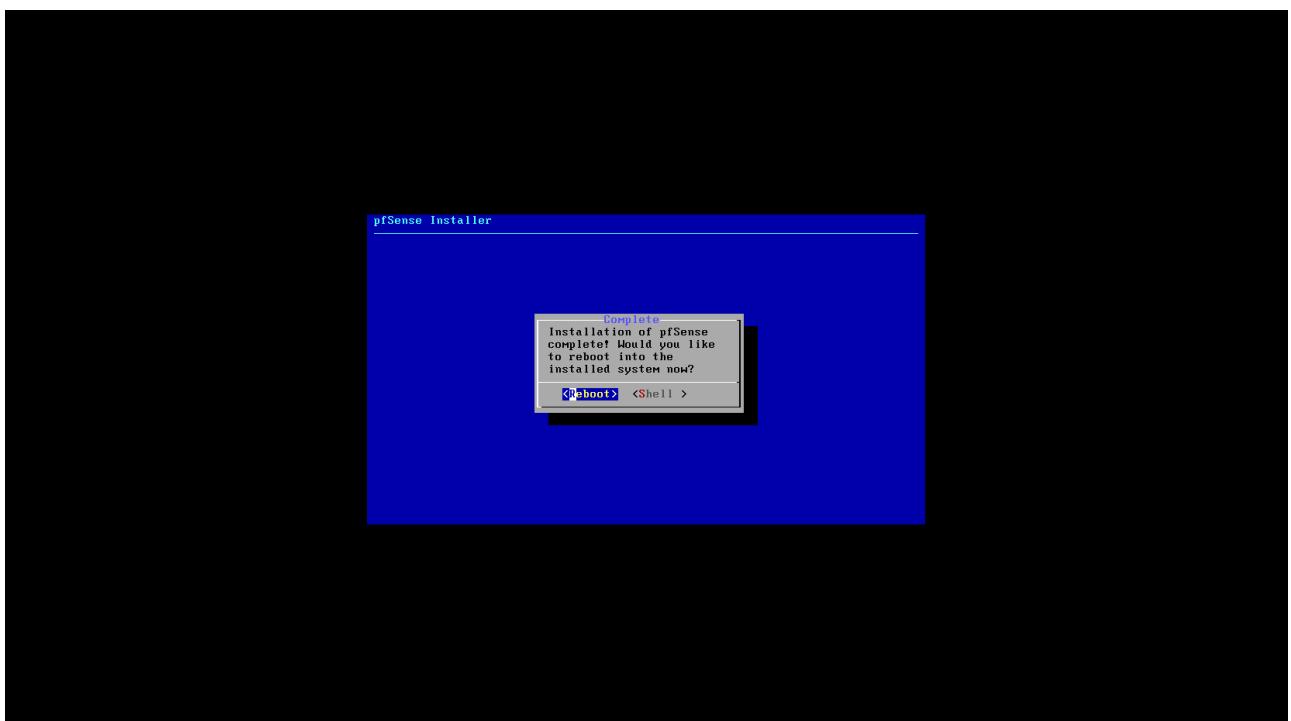
On attend l'installation.



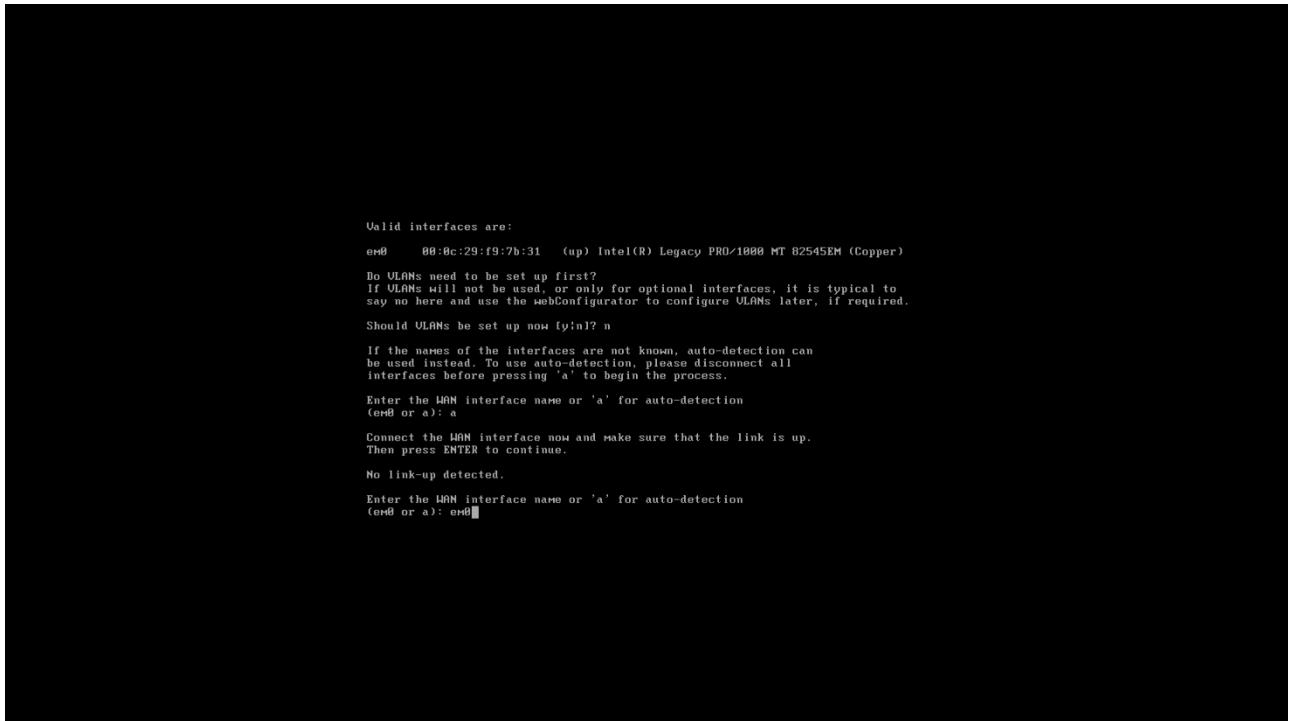
Après l'installation terminé, on choisit « NO » si on ne souhaite pas ouvrir d'invite de commande.



Il faut maintenant reboot notre machine.

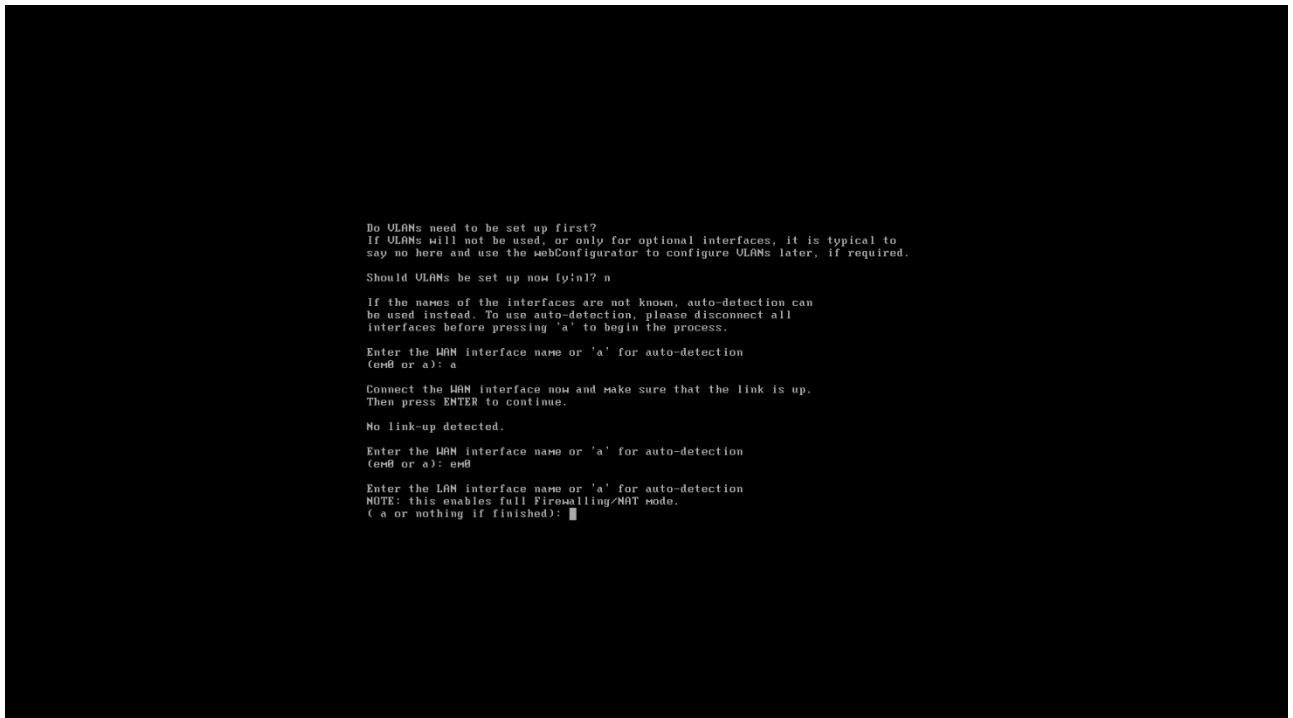


Après le reboot, on nous demande si nous souhaitons configurer nos VLAN maintenant, on appuis sur notre touche « n » pour dire non, puis on sélectionne notre carte réseau pour le réseau WAN (ici em0).



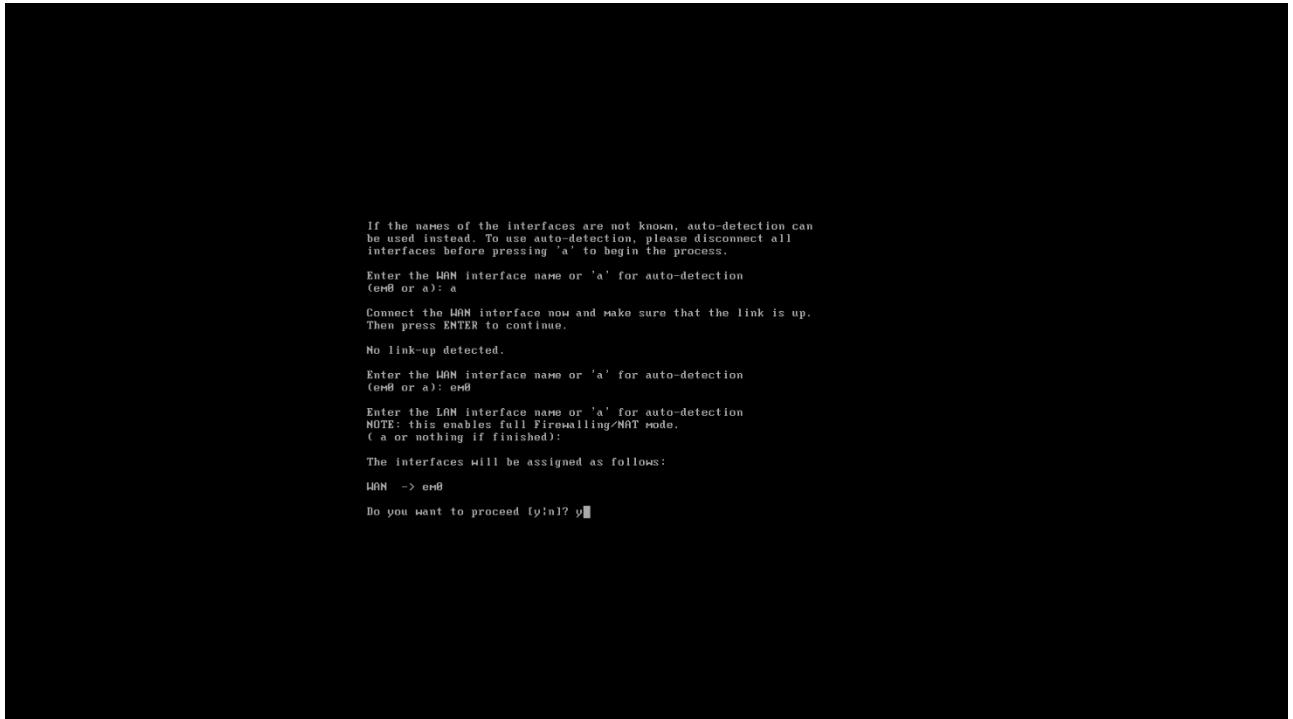
```
Valid interfaces are:  
em0      00:0c:29:f9:7b:31  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)  
Do VLANs need to be set up first?  
If VLANs will not be used, or only for optional interfaces, it is typical to  
say no here and use the webConfigurator to configure VLANs later, if required.  
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 or a): a  
Connect the WAN interface now and make sure that the link is up.  
Then press ENTER to continue.  
No link-up detected.  
Enter the WAN interface name or 'a' for auto-detection  
(em0 or a): em0
```

On nous demande la même chose pour le LAN, on appuie sur entrer car nous n'avons pas encore ajouté d'autres cartes réseaux.



```
Do VLANs need to be set up first?  
If VLANs will not be used, or only for optional interfaces, it is typical to  
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 or a): a  
Connect the WAN interface now and make sure that the link is up.  
Then press ENTER to continue.  
No link-up detected.  
Enter the LAN interface name or 'a' for auto-detection  
(em0 or a): em0  
NOTE: this enables full Firewalling/NAT mode.  
( a or nothing if finished):
```

On appuie sur « y » pour continuer.



```
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 or a): a

Connect the WAN interface now and make sure that the link is up.
Then press ENTER to continue.

No link-up detected.

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

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

The interfaces will be assigned as follows:

WAN -> em0

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

On arrive donc maintenant sur cette interface avec plusieurs menus à notre disposition.



```
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

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

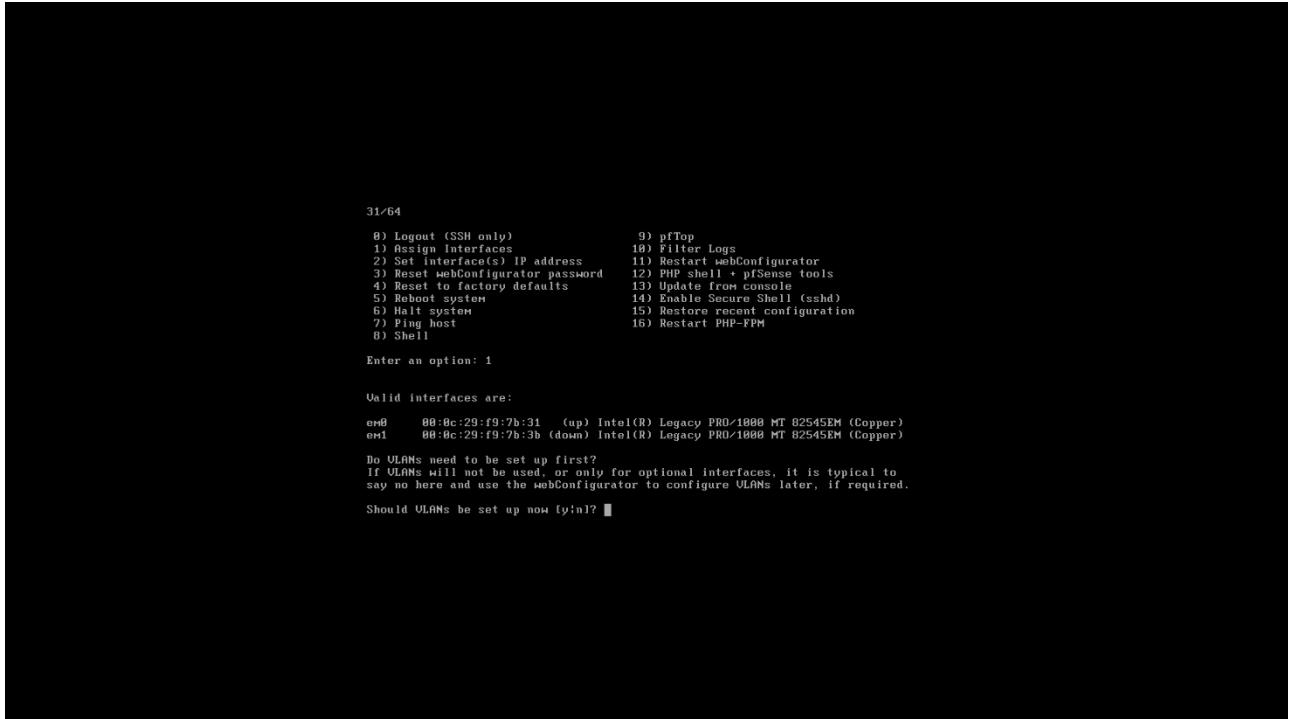
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
*** Please select an option from the menu below ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.13/24
                           v6/DHCP6: 2a01:cbid:8db6:3900:28c:29ff:fe9:7b
31/64

 8) 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-FFM

Enter an option: 1
```

Après avoir ajouté une autre carte réseau afin de configurer le LAN, on appuie sur « 1 », puis sur « y ».



```
31/64
 8) 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) Info about system           14) Enable Secure Shell (sshd)
 6) Help system                 15) Restore recent configuration
 7) Ping host                   16) Restart PHP-PPM
 8) Shell

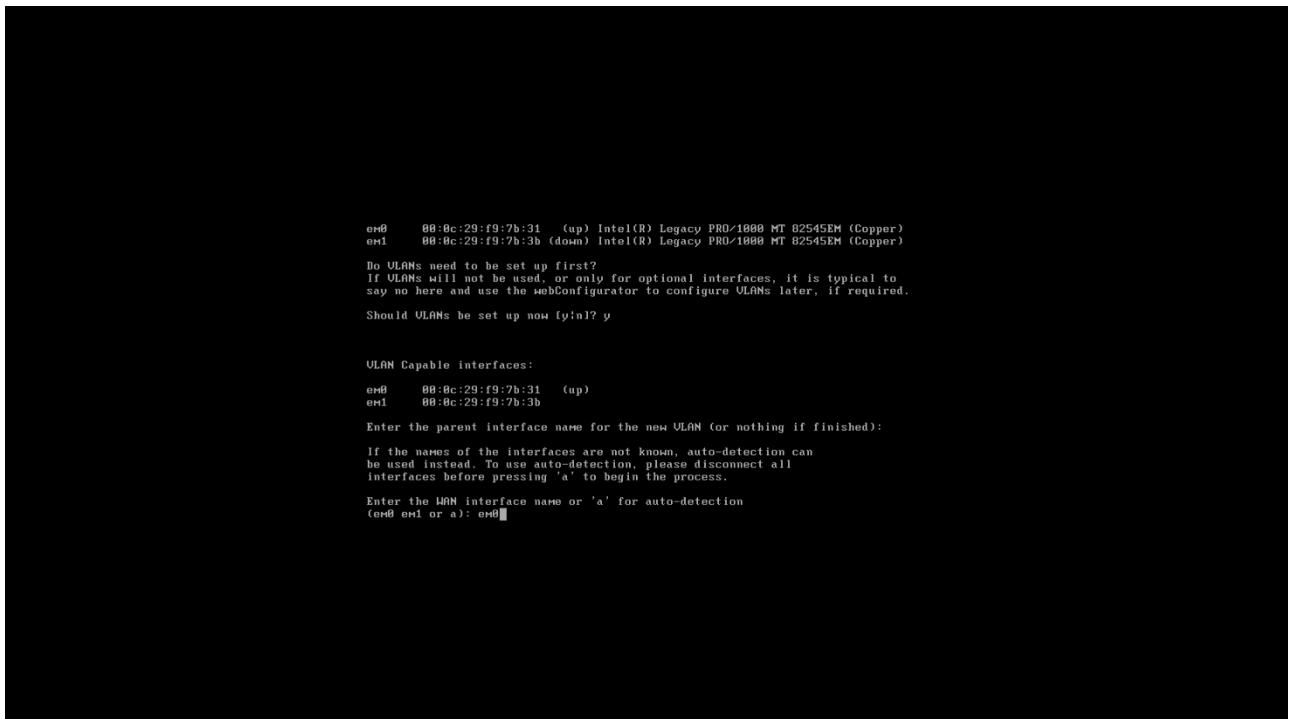
Enter an option: 1

Valid interfaces are:
em0      00:0c:29:f9:7b:31  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:f9:7b:3b (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? ■
```

On sélectionne notre carte réseau pour le WAN (ici em0).



```
em0      00:0c:29:f9:7b:31  (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:f9:7b:3b (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

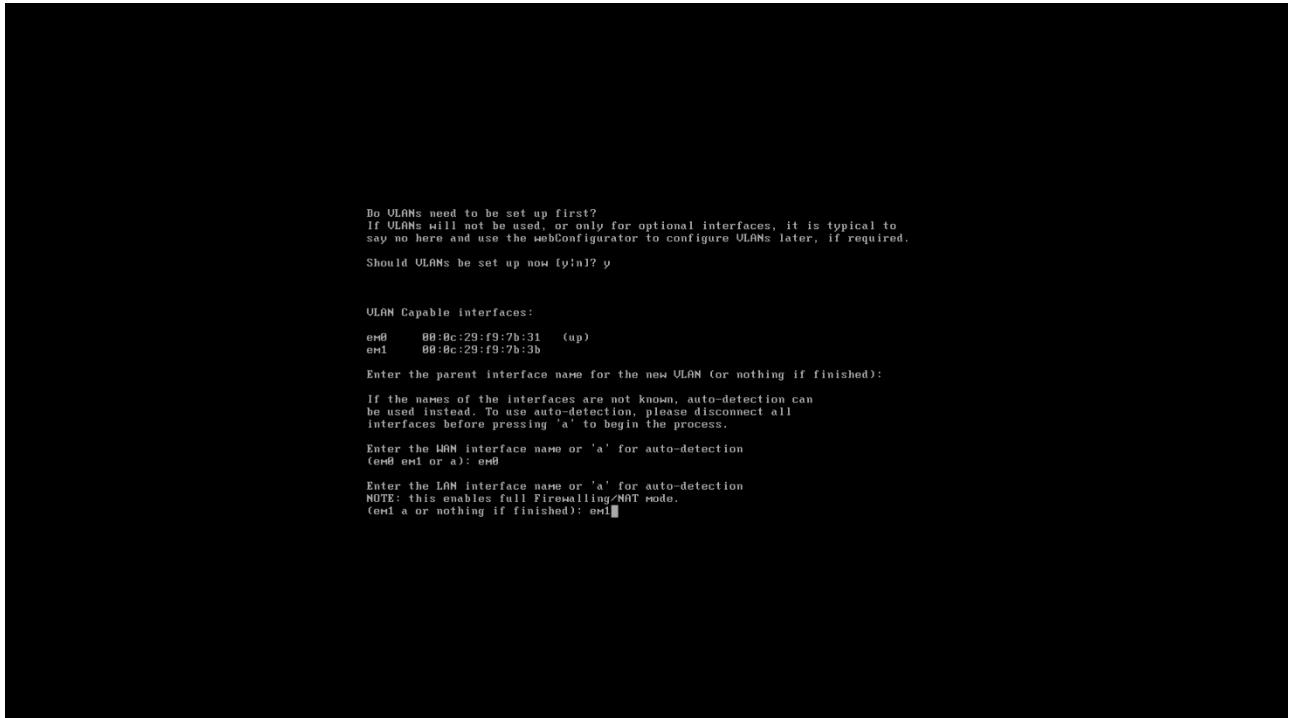
Should VLANs be set up now [y|n]? y

VLAN Capable interfaces:
em0      00:0c:29:f9:7b:31  (up)
em1      00:0c:29:f9:7b:3b

Enter the parent interface name for the new VLAN (or nothing if finished):
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■
```

On sélectionne notre carte réseau pour le LAN (ici em1).



On appuie sur « y » pour valider.



Maintenant il faut configurer les IP de nos réseau WAN et LAN, donc on appuie sur « 2 » et on sélectionne notre carte réseau WAN en appuyant sur « 1 ».

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.13/24
                           v6/DHCP6: 2a01:cb1d:8dbb:3900:20c:29ff:fe9:7b
31/64
LAN (lan)      -> em1      ->
8) 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: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1)

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

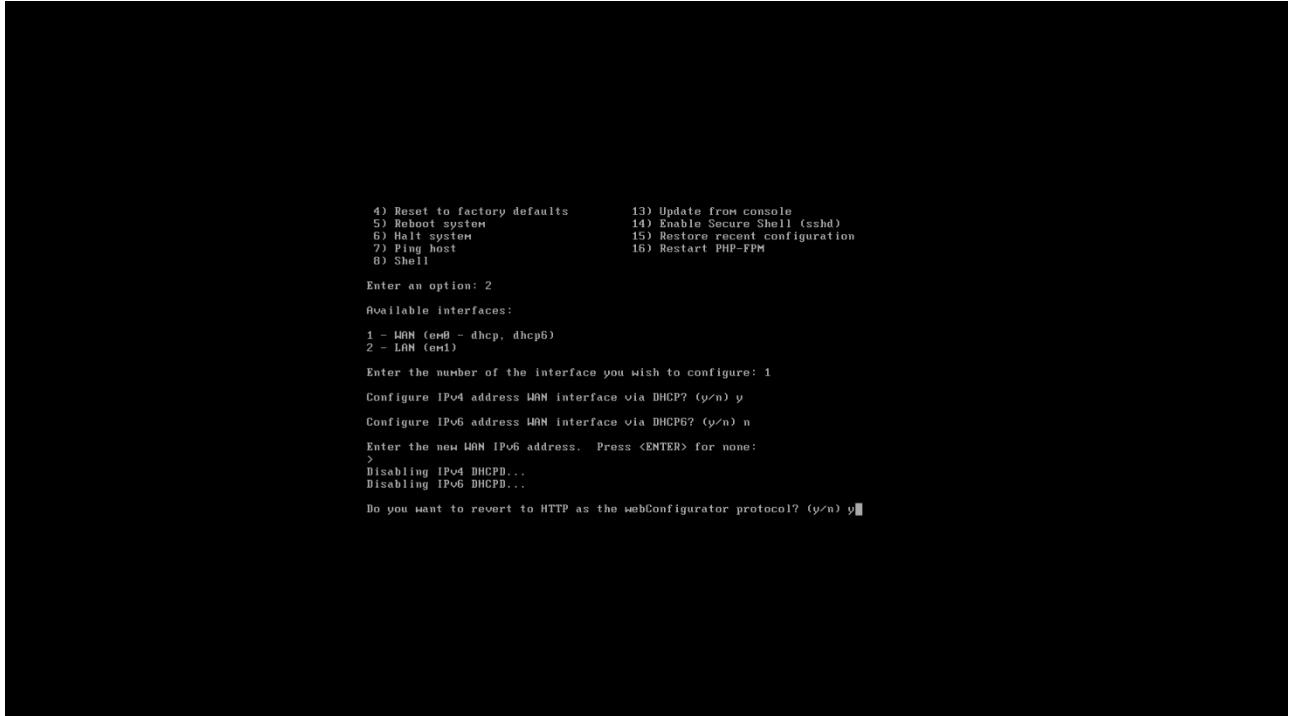
On choisit de configurer notre WAN via DHCP car notre carte réseau est en bridge mais on ne configure pas l'IPv6.

```
31/64
LAN (lan)      -> em1      ->
8) 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: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
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
```

On appuie sur entrer pour ne pas définir d'adresse IPv6 puis on appuie sur « y ».



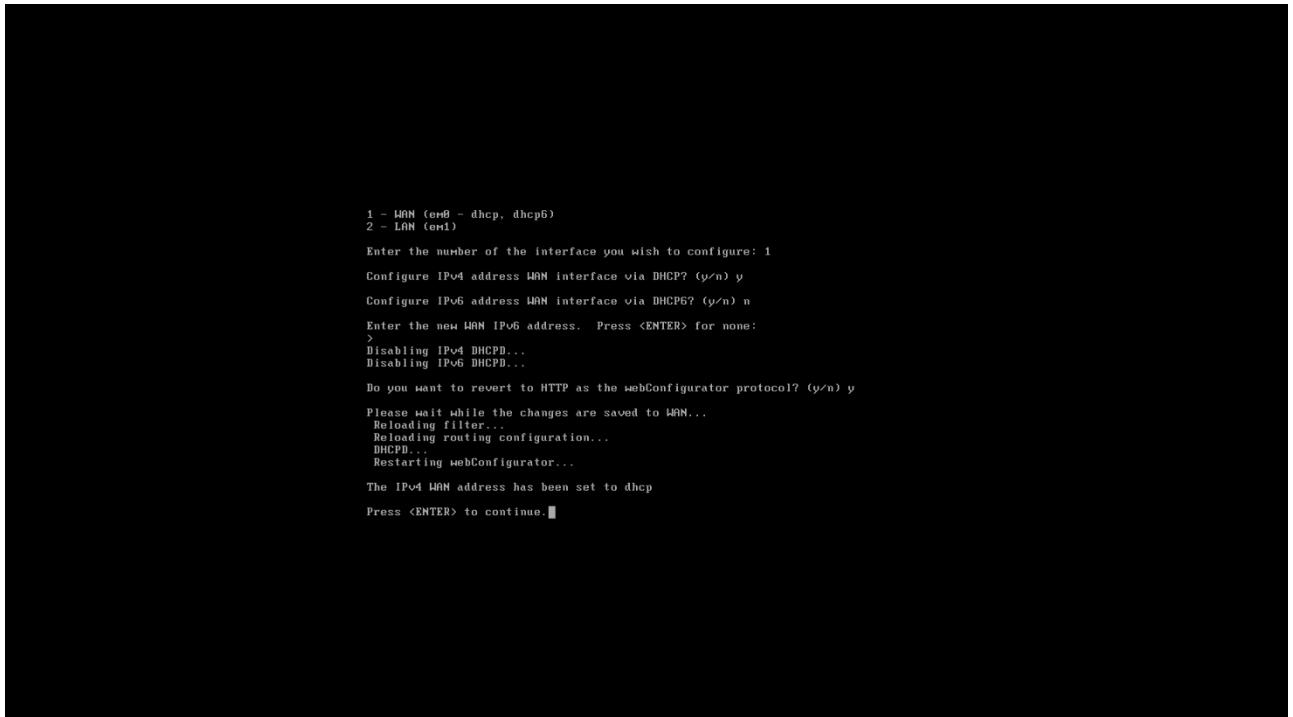
```
4) Reset to factory defaults      13) Update from console
5) Reboot system                 14) Enable Secure Shell (sshd)
6) Exit system                   15) Restore recent configuration
7) Ping host                     16) Restart PFR-FPM
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
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...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

On appuie sur entrer pour continuer.



```
1 - WAN (em0 - dhcp, dhcp6)
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...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 WAN address has been set to dhcp
Press <ENTER> to continue.
```

On retourne alors sur notre menu de base.



```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: ^CVMware Virtual Machine
e - Netgate Device ID: b1616f10245bb76855e4

*** Welcome to pfSense 2.6.0-RELEASE (arm64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.13/24
                           v6/DHCP6: 2a01:cb1d:8db6:3900:20c:29ff:fe9:7b
31/64
LAN (lan)      -> em1      -> v4: 192.168.6.210/24

  8) 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: ■
```

On fait le même procédé que pour notre carte WAN, on appuie sur « 2 » mais cette fois ci on sélectionne notre carte LAN et on indique son IPv4.



```
v6/DHCP6: 2a01:cb1d:8db6:3900:20c:29ff:fe9:7b
31/64
LAN (lan)      -> em1      -> v4: 192.168.6.210/24

  8) 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

Enter an option: 2
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
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:
> ■
```

On indique son masque de sous réseau en notation CIDR.

```
4) Reset to factory defaults          13) Update from console
5) Reboot system                     14) Enable Secure Shell (sshd)
6) Rebuild system                   15) Restore recent configuration
7) Ping host                         16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
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:
> 192.168.6.210

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
```

On appuie sur Entrer.

```
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

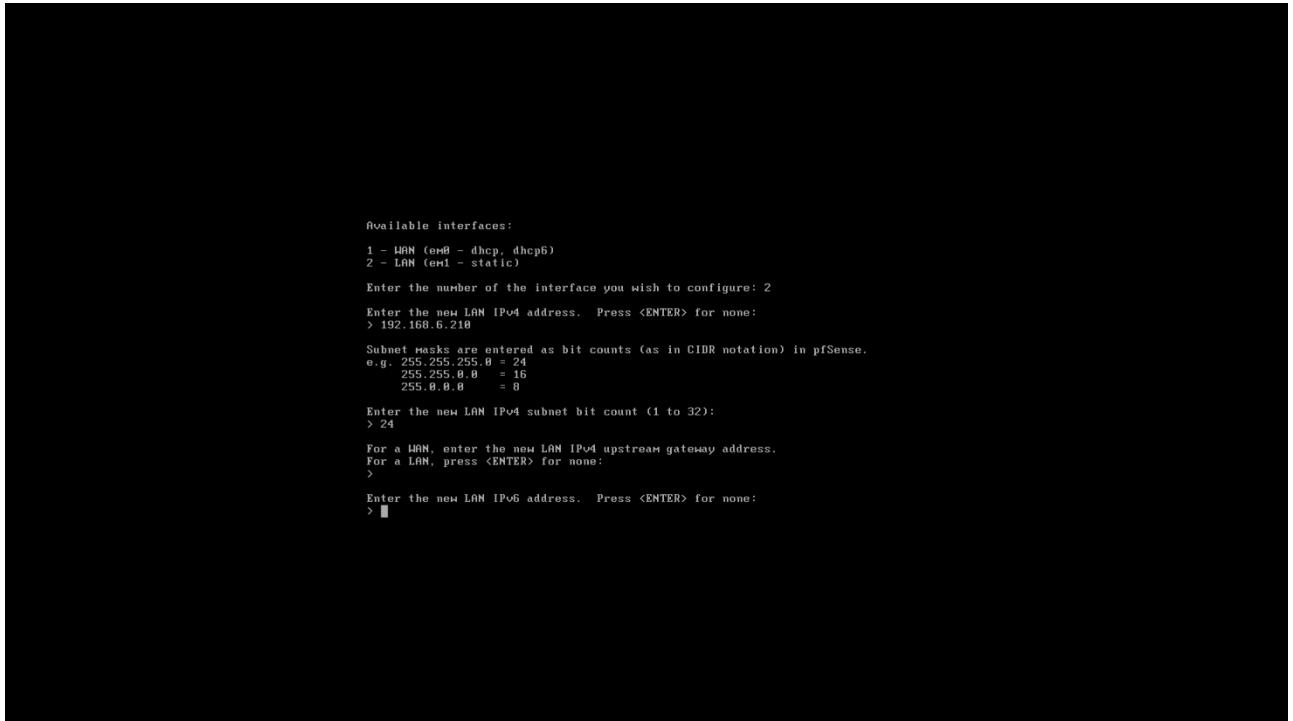
Enter the number of the interface you wish to configure: 2
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.6.210

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

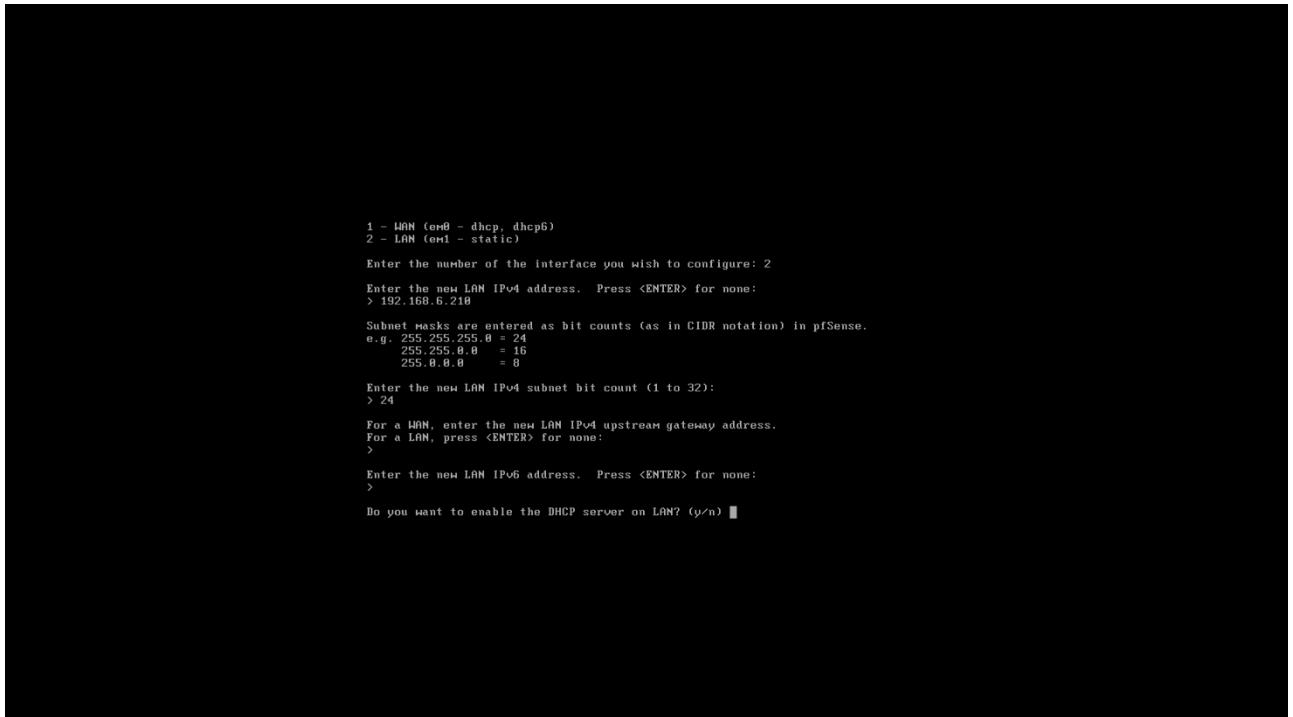
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

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

On appuie sur Entrer.



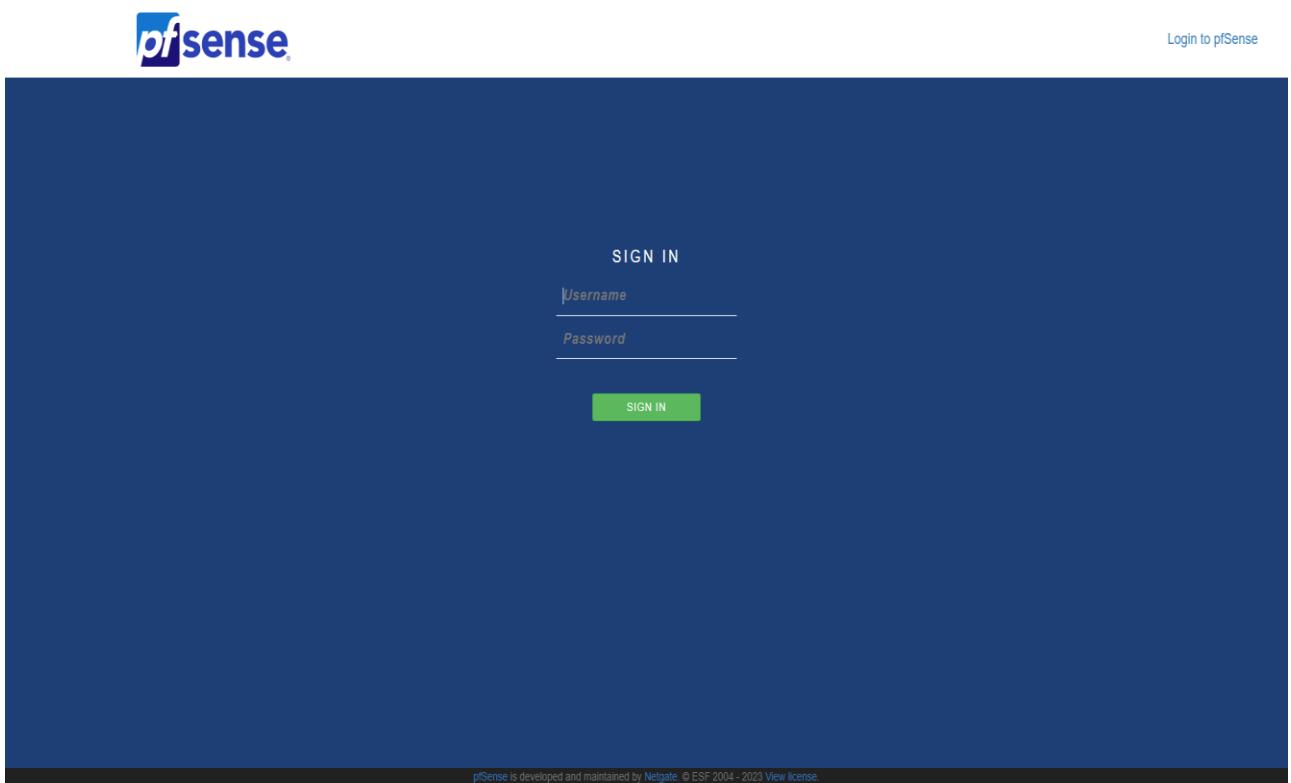
On appuie sur « n » pour ne pas activer le DHCP.



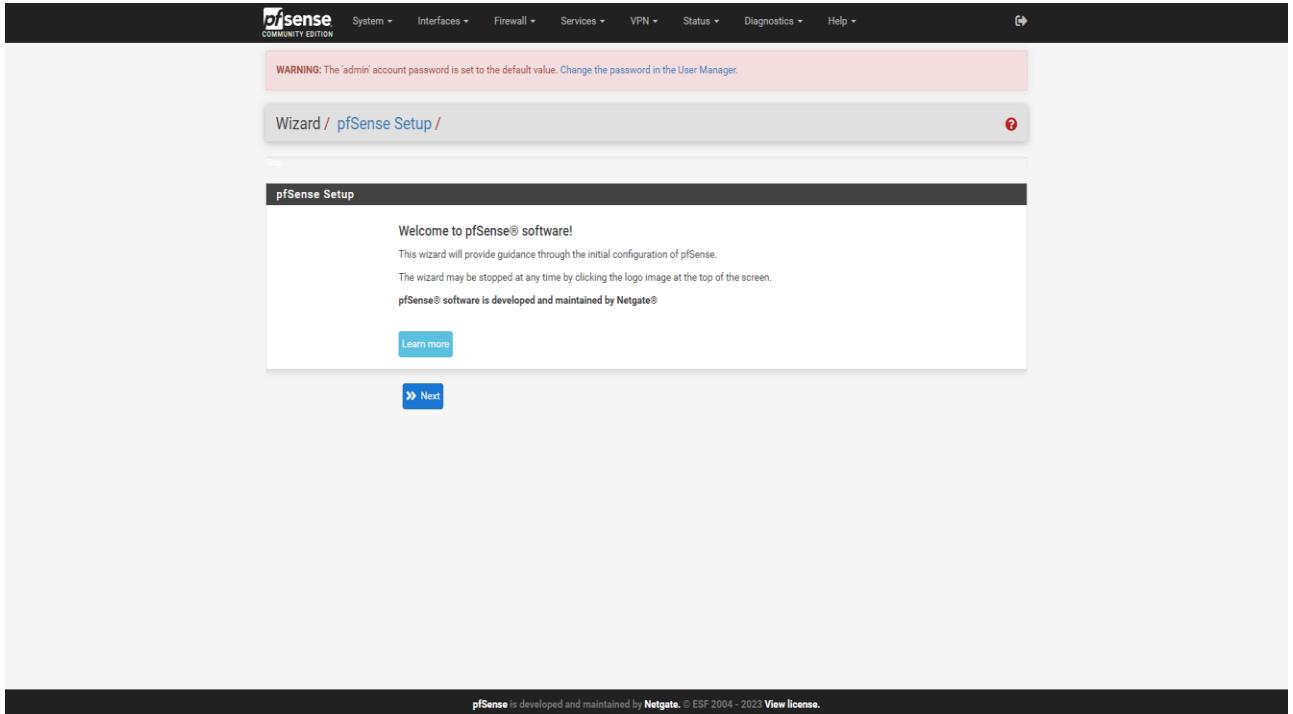
On nous indique sur quelle adresse se connecter pour accéder à l'interface web, puis on appuie sur entrer.

```
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:  
>  
Do you want to enable the DHCP server on LAN? (y/n) n  
Disabling IPv4 DHCP...  
Disabling IPv6 DHCP...  
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPB...  
The IPv4 LAN address has been set to 192.168.6.210/24  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
http://192.168.6.210/  
Press <ENTER> to continue.■
```

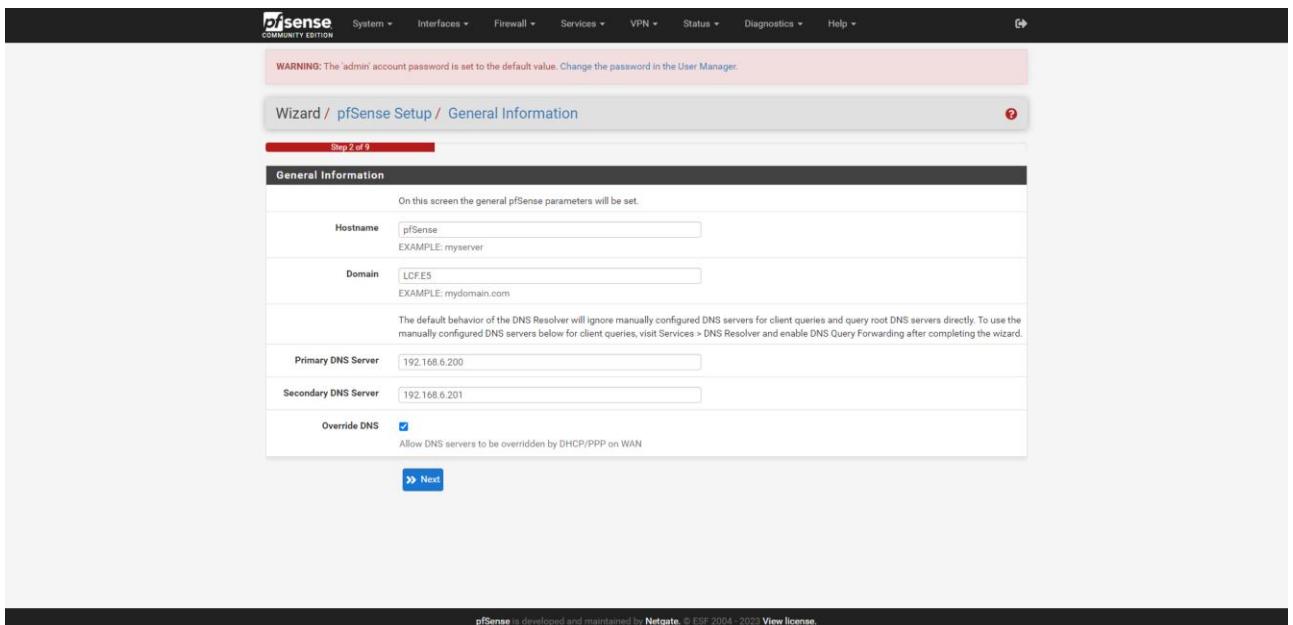
Après avoir configuré notre WAN et notre LAN, on accède à notre interface web afin de configurer notre pfSense. On rentre alors l'adresse indiqué précédemment avec les identifiants par défaut « admin » et le mot de passe « pfSense ».



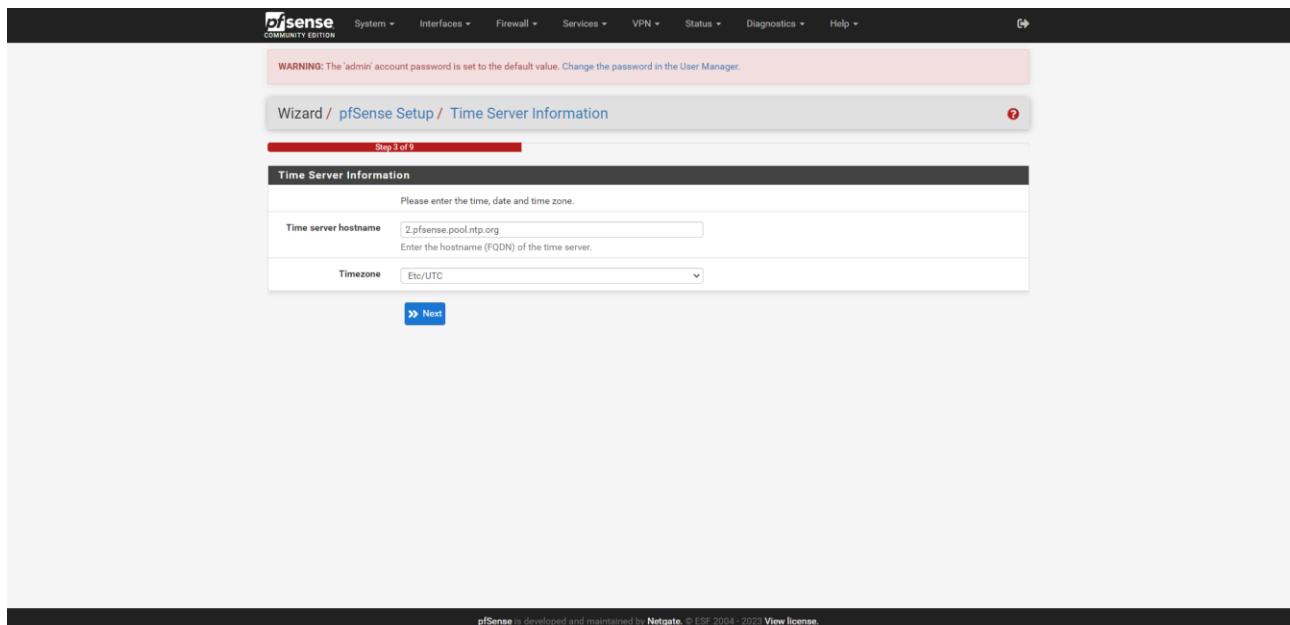
On clique sur « Next » pour finaliser la configuration.



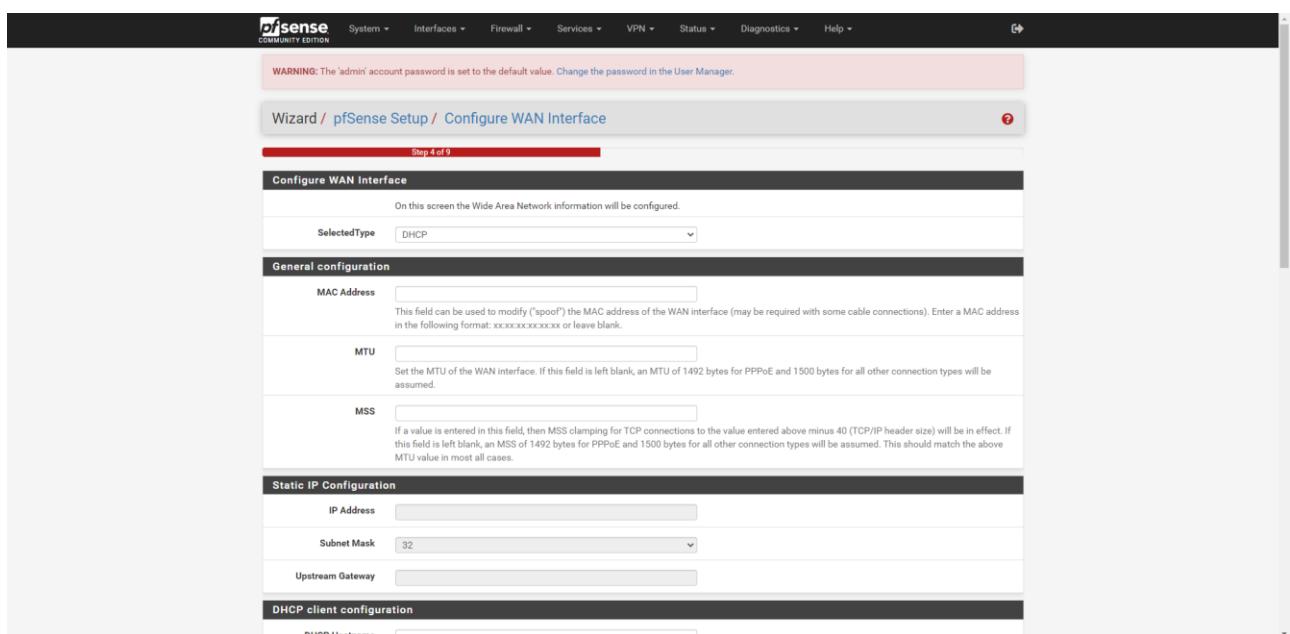
On indique le nom de notre pfSense ainsi que le domaine auquel on veut qu'il soit rattaché puis on configurer les DNS pour correspondre.



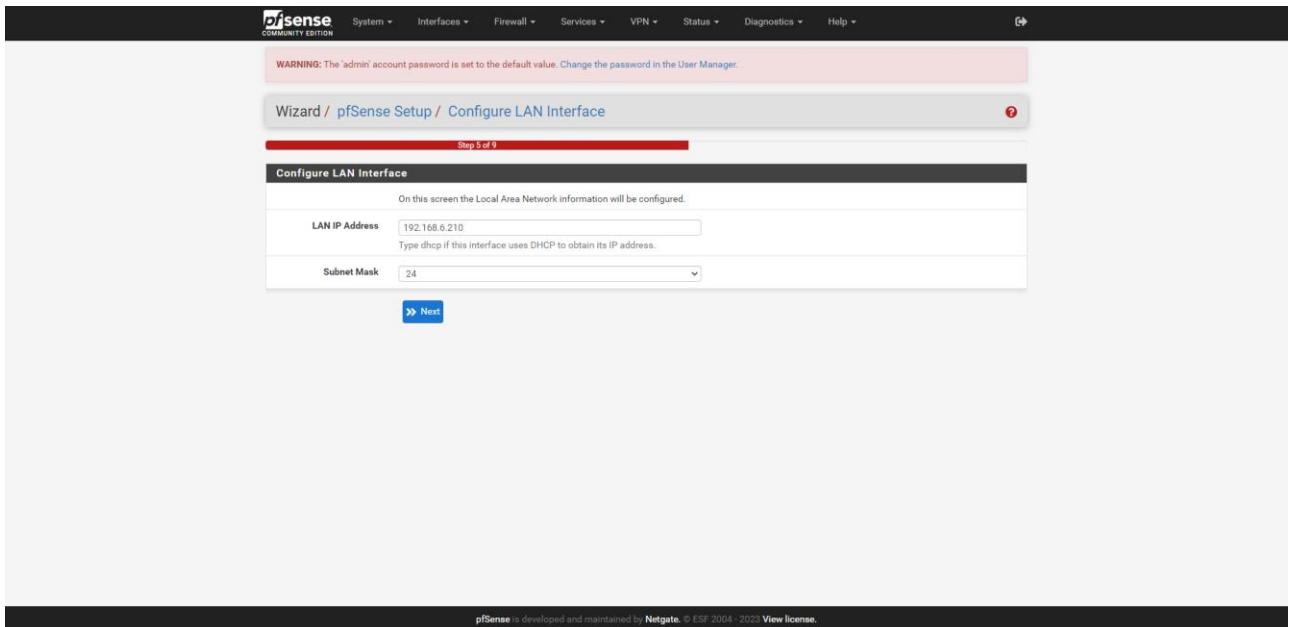
On choisit la Timezone puis on clique sur « Next ».



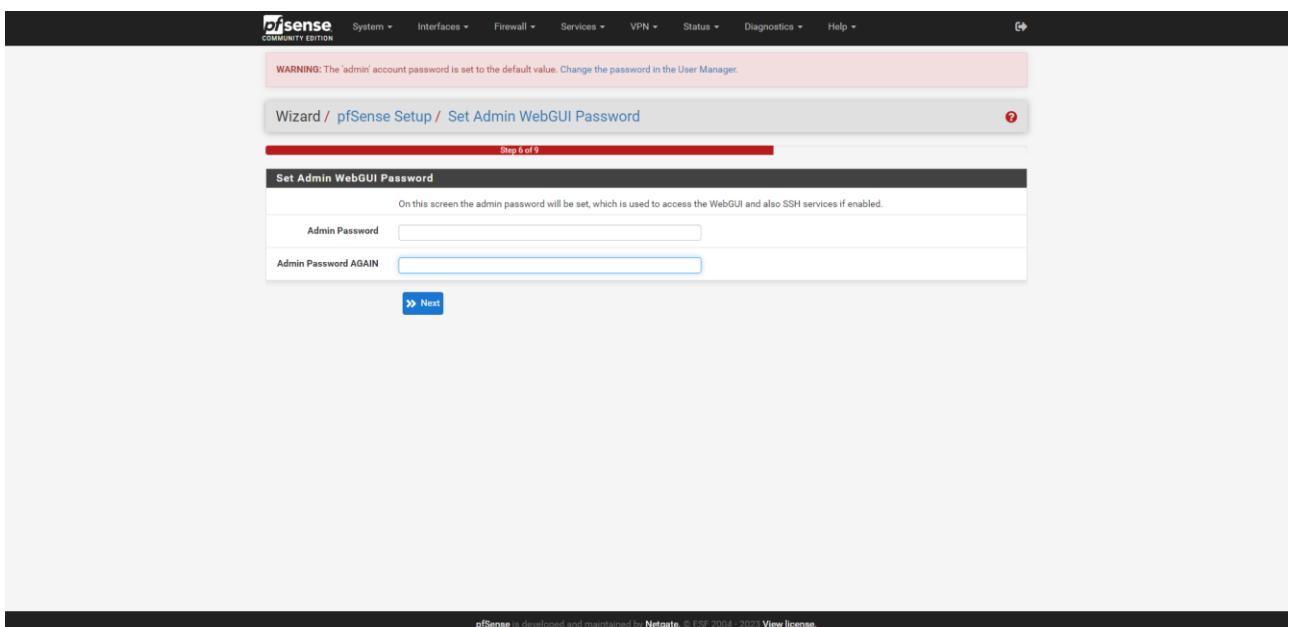
On configurer notre WAN et on clique sur « Next ».



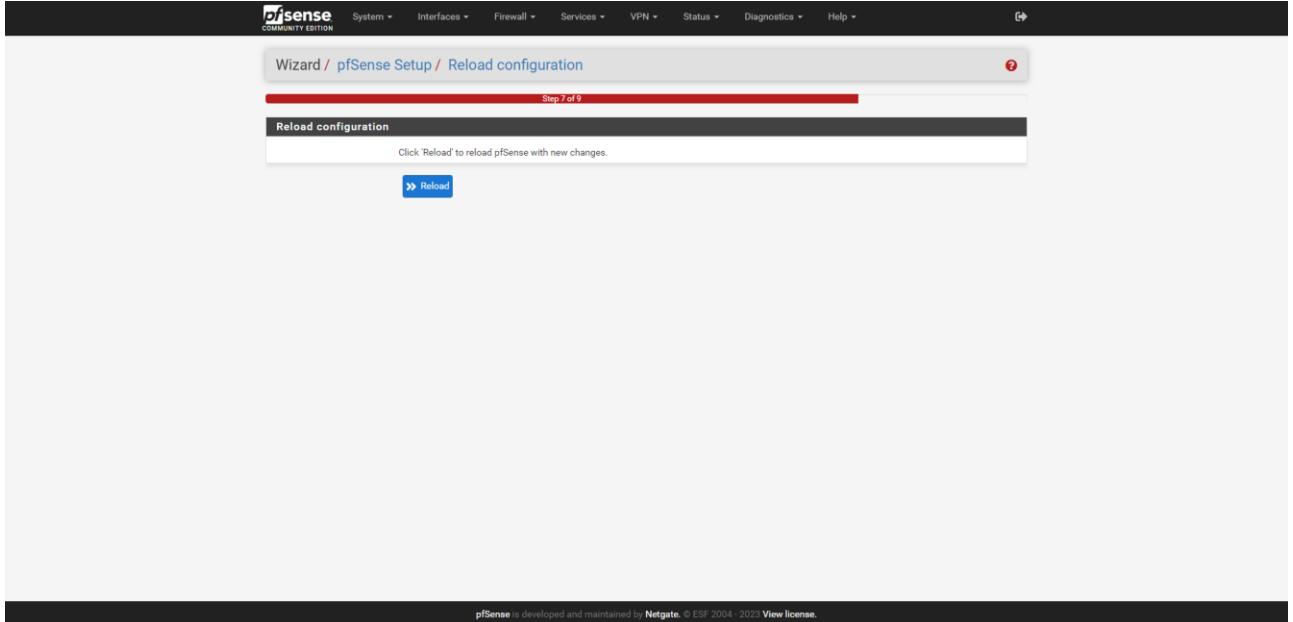
On configurer notre LAN et on clique sur « Next ».



On définit un nouveau mot de passe administrateur puis on clique sur « Next ».



On clique sur « Reload » puis on patiente.



On clique ensuite sur « Finish ».

On arrive alors sur notre tableau de bord du pfSense.

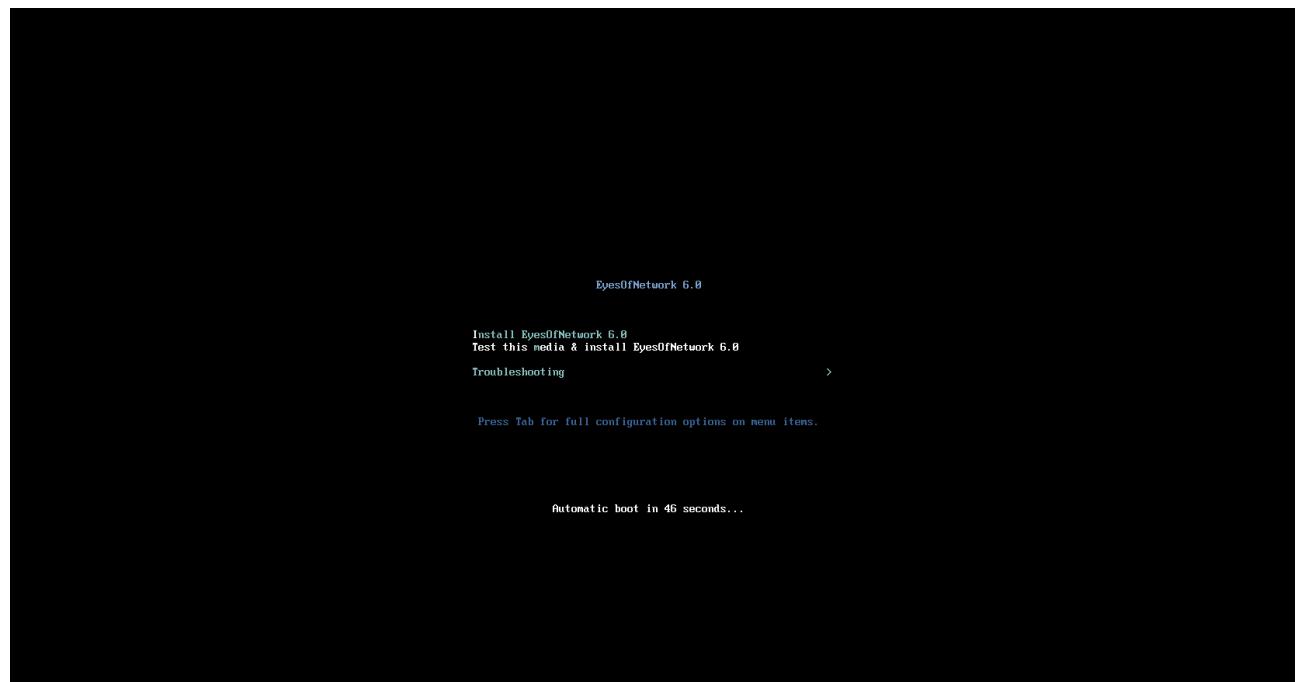
A screenshot of the pfSense Dashboard. On the left, the "System Information" panel displays various system details: Name (pfSense.LCF.E5), User (admin@192.168.6.1), System (VMware Virtual Machine, Netgate Device ID: b1616f102a5bb76855e4), BIOS (Phoenix Technologies LTD, Version 6.00, Release Date: Thu Nov 12 2020), Version (2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022, FreeBSD 12.3-STABLE), CPU Type (Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No), Hardware crypto (Kernel PTI: Disabled), MDS Mitigation (Inactive), Uptime (00 Hour 11 Minutes 45 Seconds), Current date/time (Thu Mar 30 19:48:45 UTC 2023), DNS server(s) (127.0.0.1, 192.168.1.1, 2a01:cb1d:8db6:3900:6a3f:7dff:fee1:d900, 192.168.6.200, 192.168.6.201), Last config change (Thu Mar 30 19:47:52 UTC 2023), and State table size (0). On the right, the "Netgate Services And Support" panel shows Contract type (Community Support, Community Support Only) and a section about NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES. It includes links for upgrading support, viewing the support FAQ, attending official pfSense training, and professional services. A note at the bottom encourages purchasing TAC support if you have a Netgate Device ID.

Notre Firewall pfSense est désormais actif.

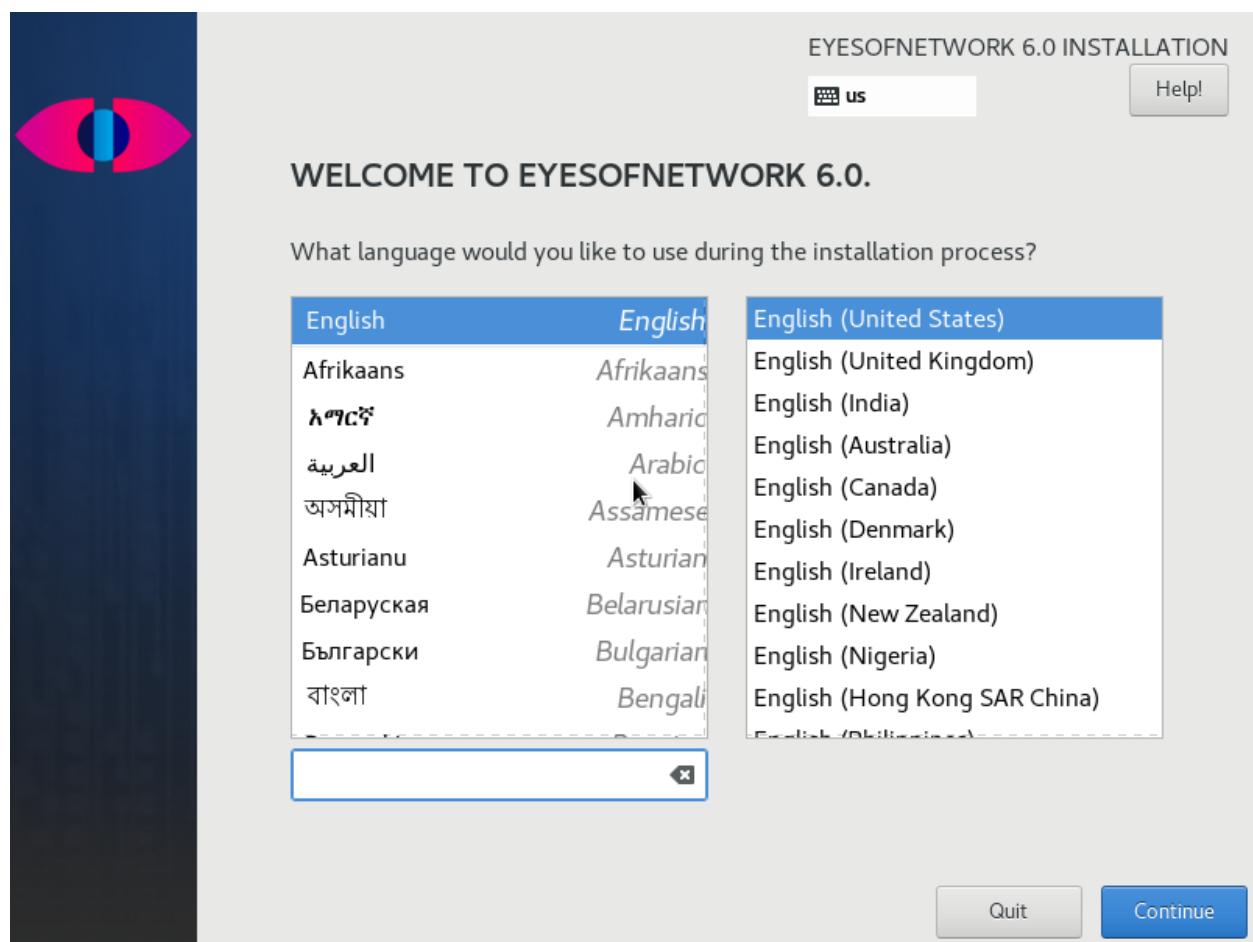
### III) Installation d'Eyes Of Network

Pour installer Nagios, on se rend sur le site d'Eyes of Network afin d'y télécharger l'ISO nous permettant de l'installer.

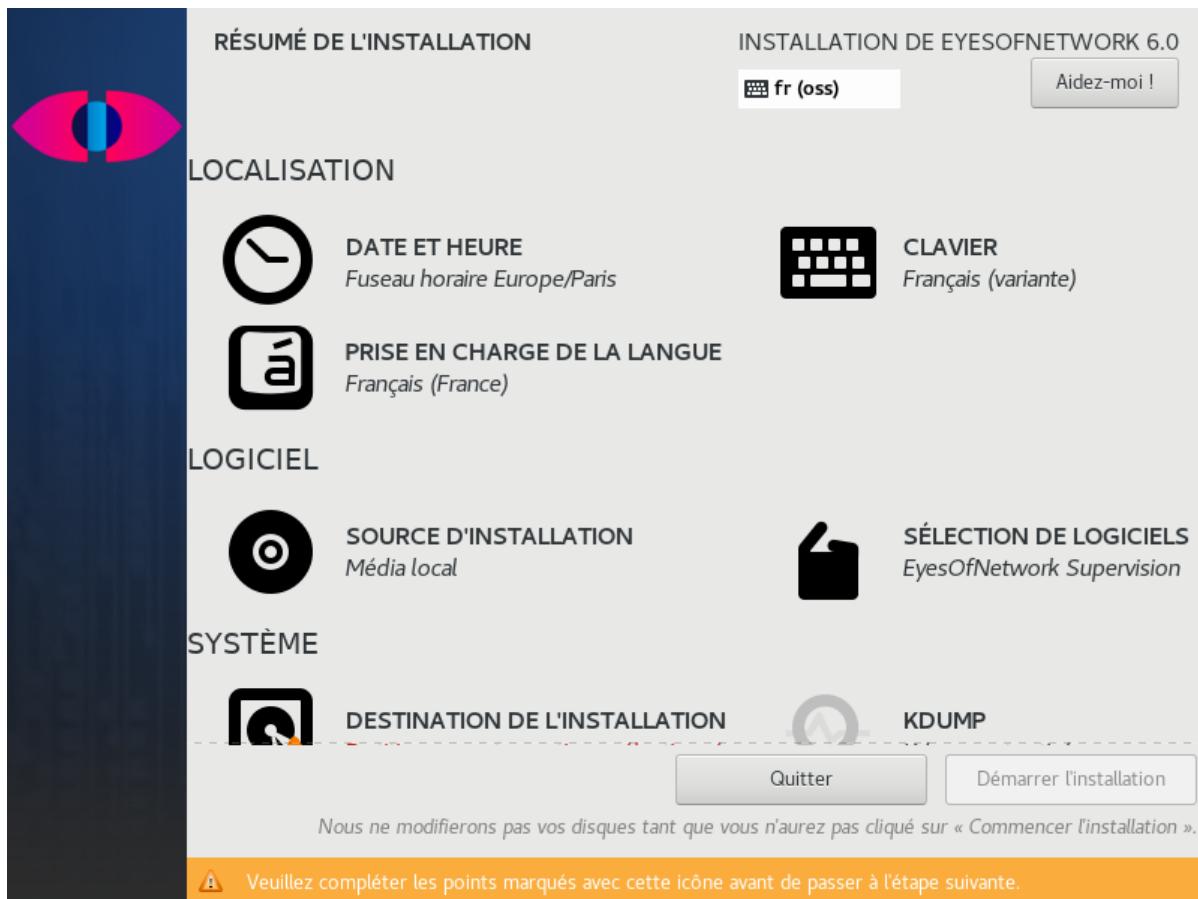
En lançant notre machine, on arrive sur cette interface, on clique sur « Install ».



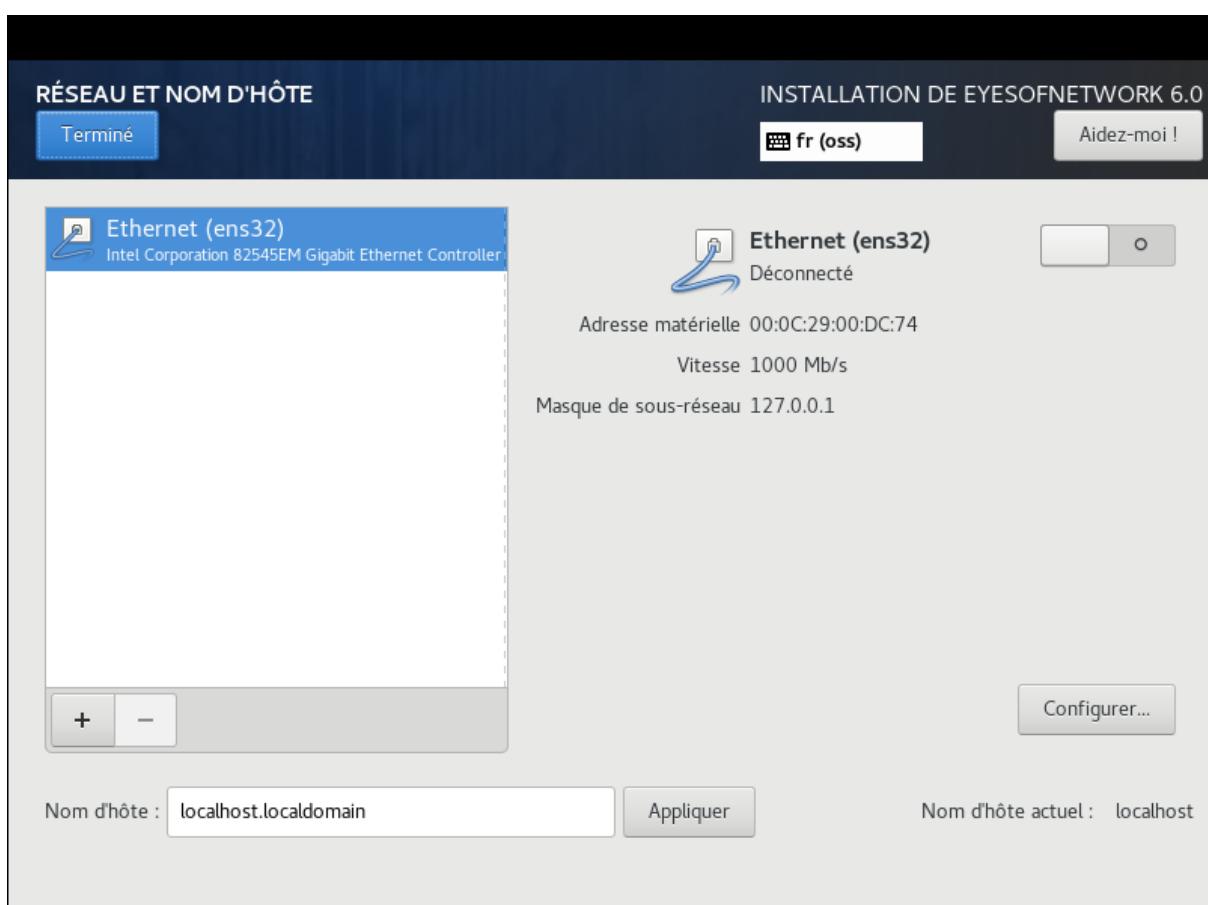
À la fin de l'installation, on choisit notre langue et on clique sur « continuer ».



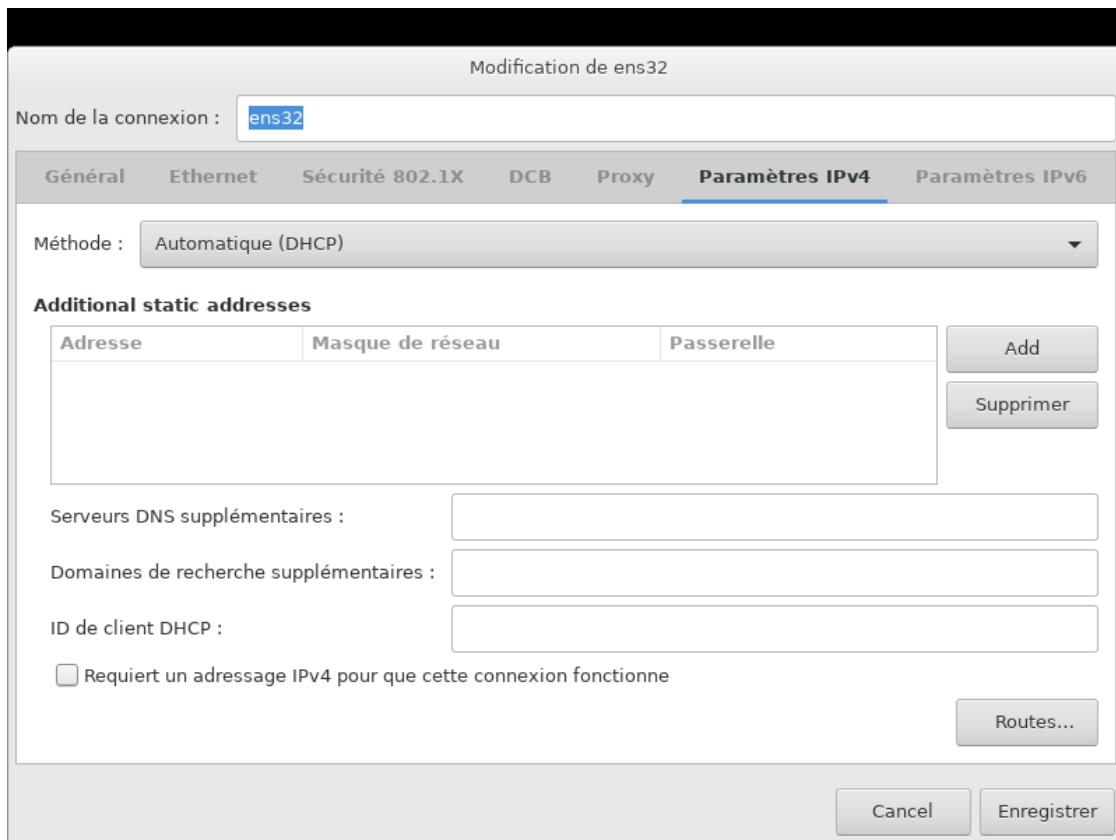
On descend dans la page puis on clique sur « Réseau et nom d'hôte ».



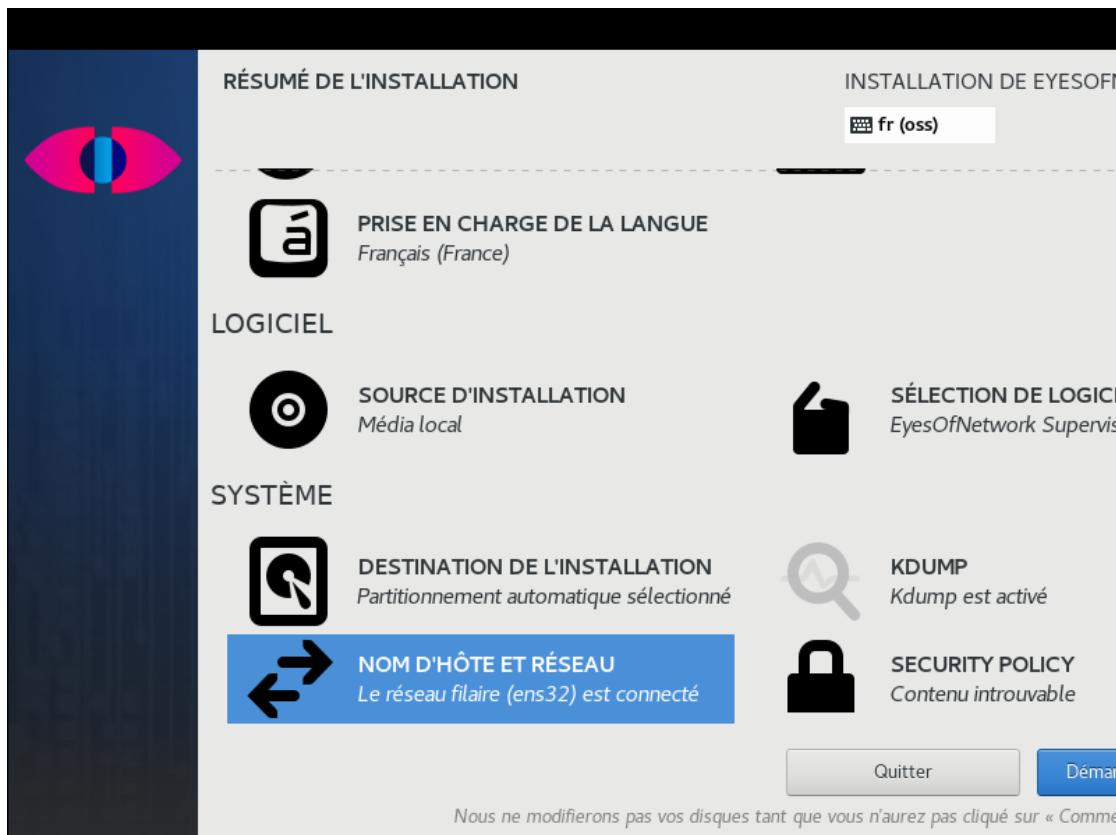
On clique sur le bouton en haut à droite puis on clique sur « configurer ».



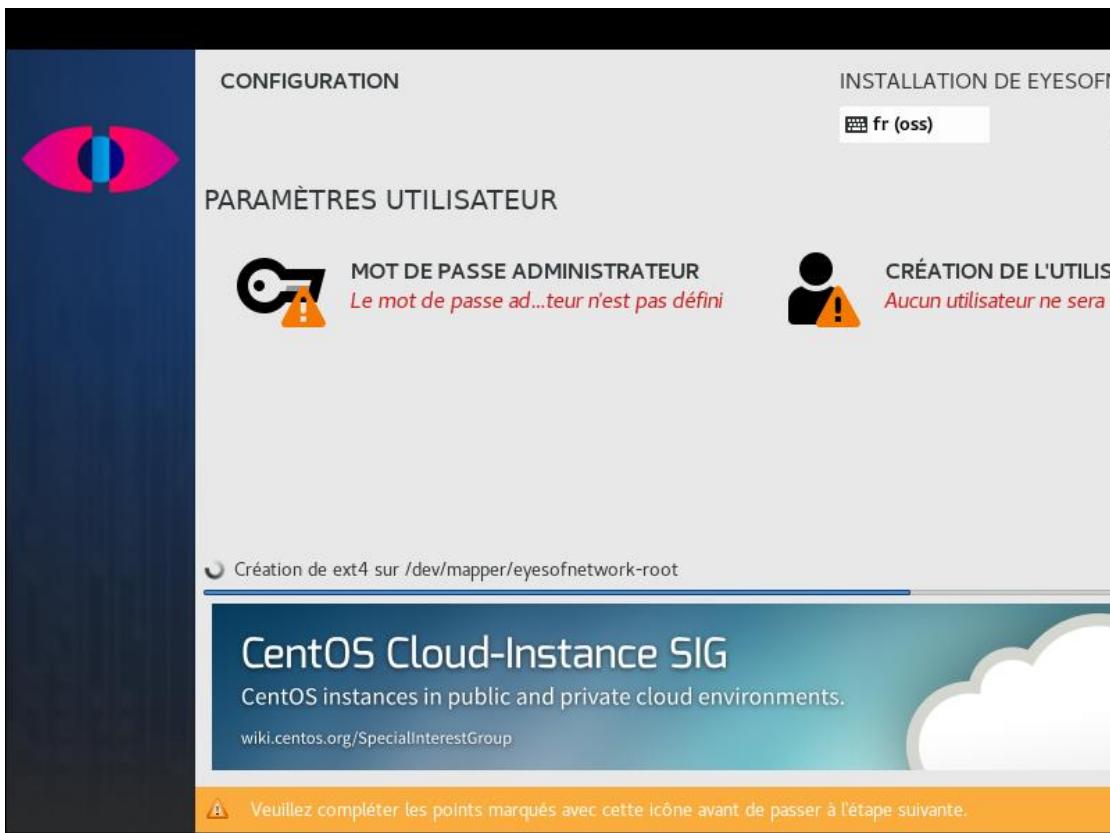
On va sous l'onglet IPv4, puis on définit notre adresse, son masque et sa passerelle.



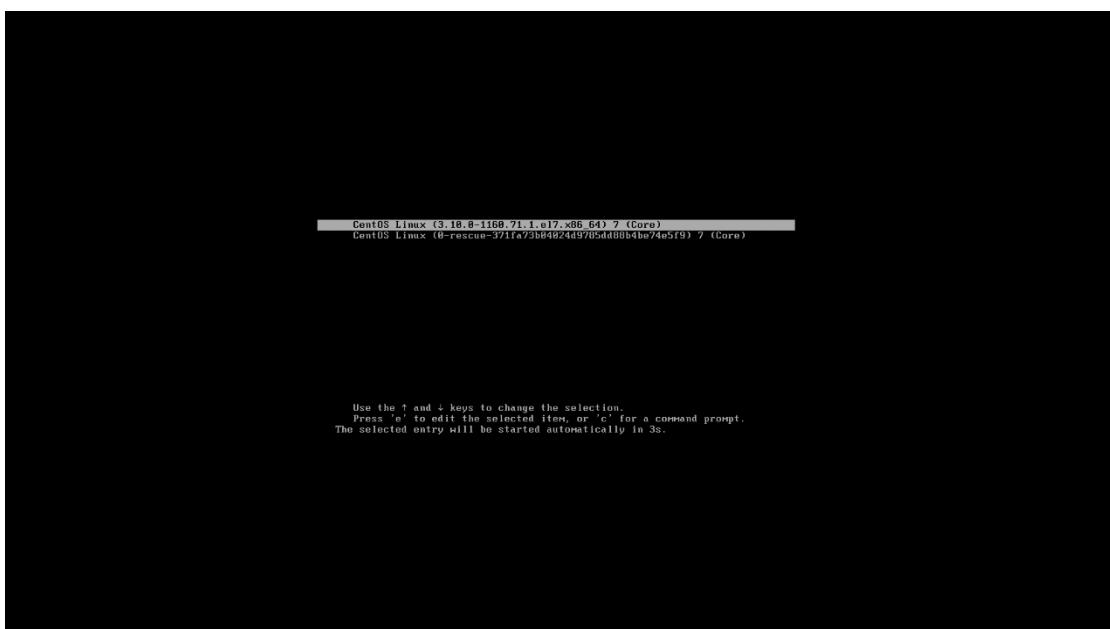
Après avoir enregistré, on clique sur « Démarrer ».



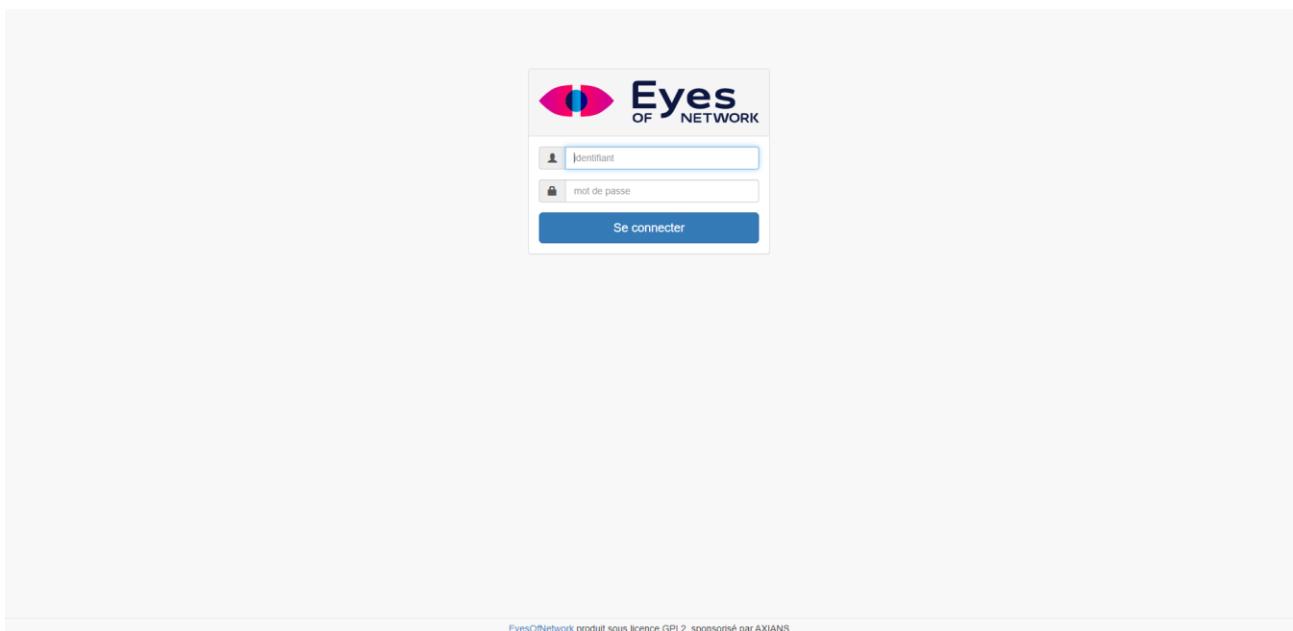
On définit un mot de passe administrateur puis on patiente jusqu'as la fin de l'installation.



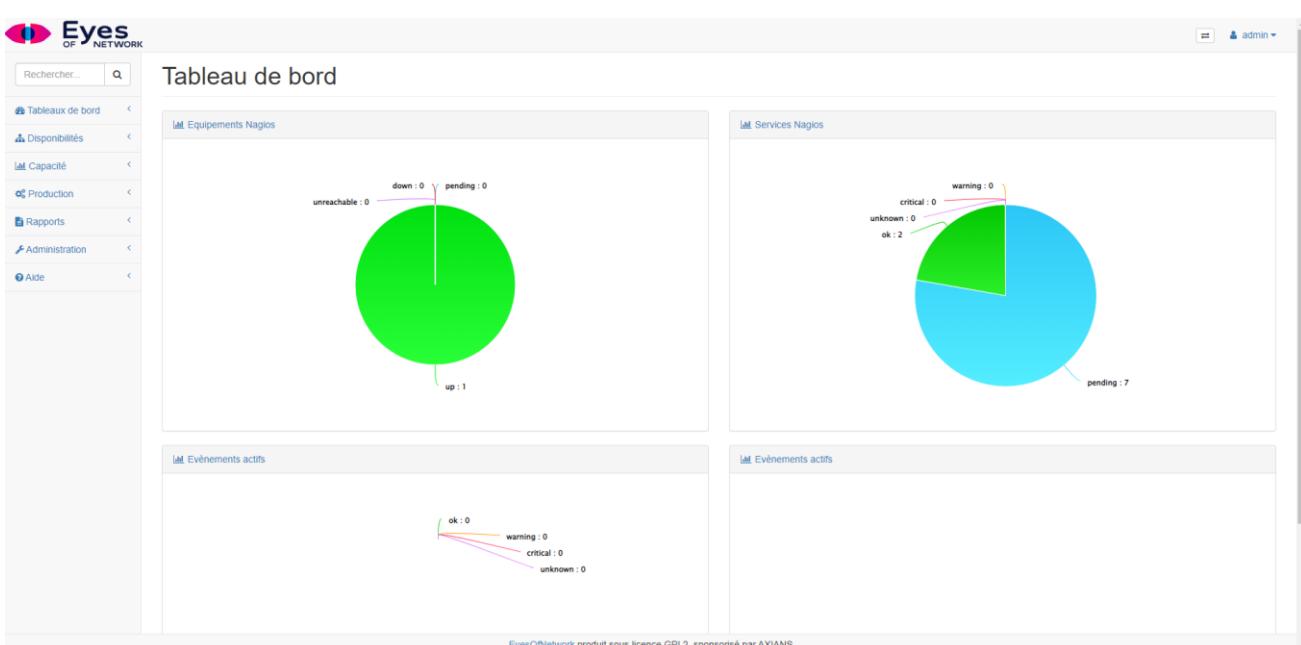
Après l'installation, on redémarre notre machine et on arrive sur cette page, on sélectionne la première option.



Ensuite, on accède à notre interface web en allant sur notre navigateur web et en y rentrant l'adresse IP précédemment défini. On arrive alors sur cette page.



On rentre les identifiants admin par défaut « admin » avec comme mot de passe « admin » puis on arrive sur notre tableau de bord.



Pour ajouter l'hôte que nous voulons superviser, on va dans Administration > Configuration Nagios.

The screenshot shows the Eonweb Configurator interface. In the top navigation bar, there are links for 'Paramètres', 'Equipements', 'Modèles', 'Outils', and 'admin'. On the left, a sidebar menu includes 'Tableaux de bord', 'Disponibilités', 'Capacité', 'Production', 'Rapports', 'Administration' (selected), 'Configuration Nagios' (selected), 'Applications', 'Appliquer la configuration', 'Généralités', 'Nagios', 'Cartographies', 'Liens externes', and 'Aide'. The main content area is titled 'GENERAL CONFIGURATION' and contains several configuration items: 'Nagios Daemon Configuration', 'Nagios Web Interface Configuration', 'Nagios Resources', 'Nagios Commands', 'Contact Groups', 'Host Groups', 'Service Groups', and 'Time Periods'. A search bar at the top right says 'Search:'. At the bottom, it says 'Eonweb Configurator produit sous licence GPL2, sponsorisé par AXIANS'.

On clique sur Equipements > Ajouter

This screenshot is similar to the previous one, showing the Eonweb Configurator interface. The 'Administration' and 'Configuration Nagios' items are still selected in the sidebar. The main content area shows the same 'GENERAL CONFIGURATION' section with its various configuration items. In the top right, there are buttons for 'Lister' and 'Ajouter'. A search bar is also present. The bottom status bar shows the URL 'https://192.168.6.211/module/module\_frame/index.php?url=%2Fae%2Fadd\_host.php' and the text 'Eonweb Configurator produit sous licence GPL2, sponsorisé par AXIANS'.

On rentre les informations concernant notre hôte (Nom et IP)

The screenshot shows the 'Add New Host' page of the EyesOfNetwork web interface. The left sidebar contains navigation links for 'Tableaux de bord', 'Disponibilités', 'Capacité', 'Production', 'Rapports', 'Administration', and 'Aide'. The main form area has a header 'ADD A TOP-LEVEL HOST'. It includes fields for 'Host Name' (with a placeholder 'host1'), 'Host Description' (empty), 'Address' (empty), and 'Display Name (Optional)' (empty). Below these is a section for 'Host Templates To Inherit From (Top to Bottom)'. A dropdown menu shows 'AIX4' selected, and a button 'Add Template' is visible. At the bottom are 'Add Host' and 'Cancel' buttons. The top right corner shows 'Paramètres', 'Equipements', 'Modèles', 'Outils', and 'admin'. A search bar 'Search:' is also present.

Après l'avoir enregistré, on clique sur Outils > Appliquer la configuration.

The screenshot shows the 'Eonweb Configurator' page of the EyesOfNetwork web interface. The left sidebar contains navigation links for 'Tableaux de bord', 'Disponibilités', 'Capacité', 'Production', 'Rapports', 'Administration', and 'Configuration Nagios'. Under 'Configuration Nagios', there is a link 'Appliquer la configuration'. The main content area is titled 'GENERAL CONFIGURATION' and lists several configuration items: 'Nagios Daemon Configuration', 'Nagios Web Interface Configuration', 'Nagios Resources', 'Nagios Commands', 'Contact Groups', 'Host Groups', 'Service Groups', and 'Time Periods'. Each item has a brief description. On the right side of the main content area, there is a button 'Appliquer la configuration'. The top right corner shows 'Paramètres', 'Equipements', 'Modèles', 'Outils', and 'admin'. A search bar 'Import XML' and 'Appliquer la configuration' is also present.

On clique sur « Restart ».

Rechercher...

Paramètres    Équipements    Modèles    Outils    admin

Exporter

Search:

EXISTING EXPORT JOBS

There appears to be existing export jobs. There should only be one running. If there are multiple showing as running, you should cancel them or purge them. Click on a job to view its progress and its log.

| Name   | Description | Start Time          | Status   | Actions  |
|--------|-------------|---------------------|----------|--|
| nagios |             | 2023-04-02 15:50:28 | Complete | <a href="#">View Job</a> <a href="#">Restart</a> |

CREATE NEW EXPORT JOB

To begin an export of your configuration, an Export Job must be defined. Configure your export job below. Once created, your export job will begin in the background. You will be able to check on the status of your export and view its log as it continues running. You are advised to NOT edit anything in Lilac while your export is running.

**Job Definition ID : 2**

Job Name:

Job Description:

Export Engine To Use:

Choose an Engine to use for your Import Job from Above.

EyesOfNetwork produit sous licence GPL2, sponsorisé par AXIANS

On attend la fin de la configuration pour que celle-ci soit effective.

Rechercher...

Paramètres    Équipements    Modèles    Outils    admin

Exporter

Search:

JOB DETAILS

Job Name: nagios  
Job Id: 1  
Start Time: 2023-04-03 12:52:31  
Elapsed Time: 0 Hours 0 Minutes 5 Seconds  
Current Status: Complete

Job Supplemental:  
Performing Preflight Check With Command: /usr/eyesofnetwork/nagios/bin/nagios -v /tmp/lilac-export-1/nagios.cfg  
Performing Nagios Restart With Command: /usr/bin/sudo /bin/systemctl restart nagios

Export Job Complete. Content Exported Successfully.

[Restart Job](#) [Stop Job](#) [Remove Job](#) [Return To Exporter](#)

JOB LOG

| Time               | Type   | Text                                   |
|--------------------|--------|--|
| 2023-04-03 12:52:1 | NOTICE | NagiosExportEngine beginning export... |
| 2023-04-03 12:52:1 | NOTICE | NagiosExportEngine Starting...         |

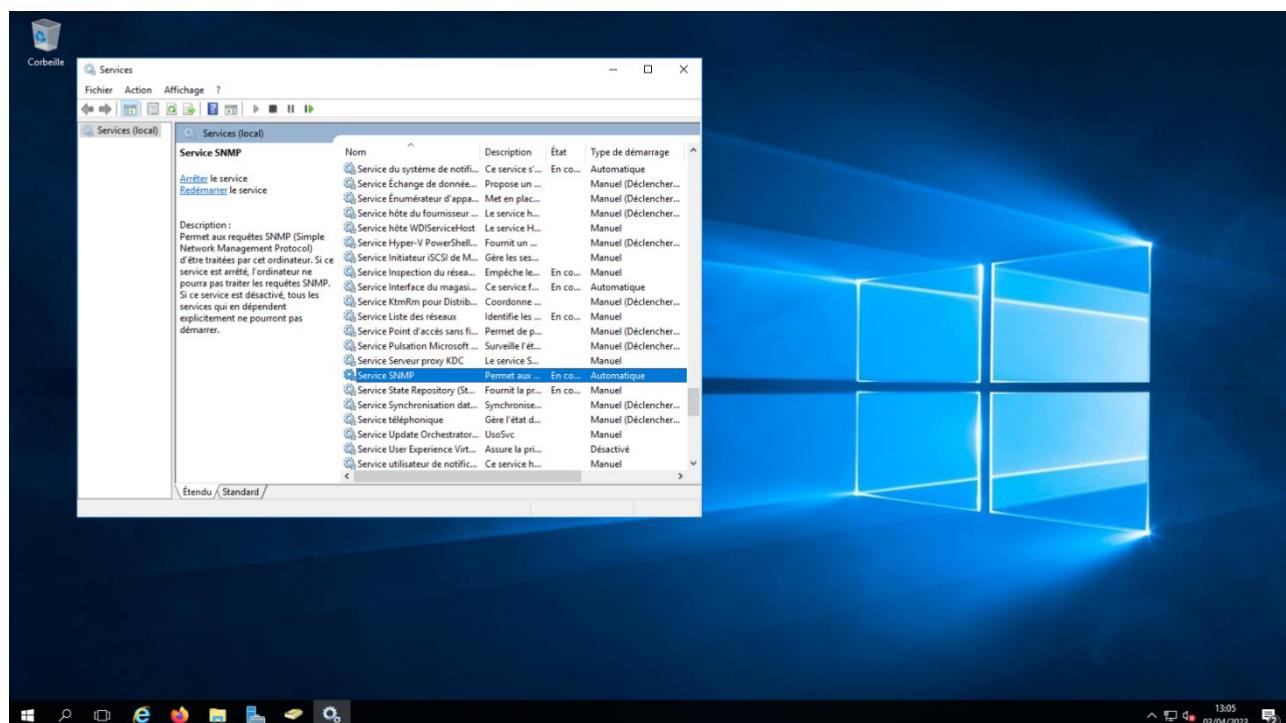
20   Page 1 of 1   Displaying 1 to 2 of 2 items

EyesOfNetwork produit sous licence GPL2, sponsorisé par AXIANS

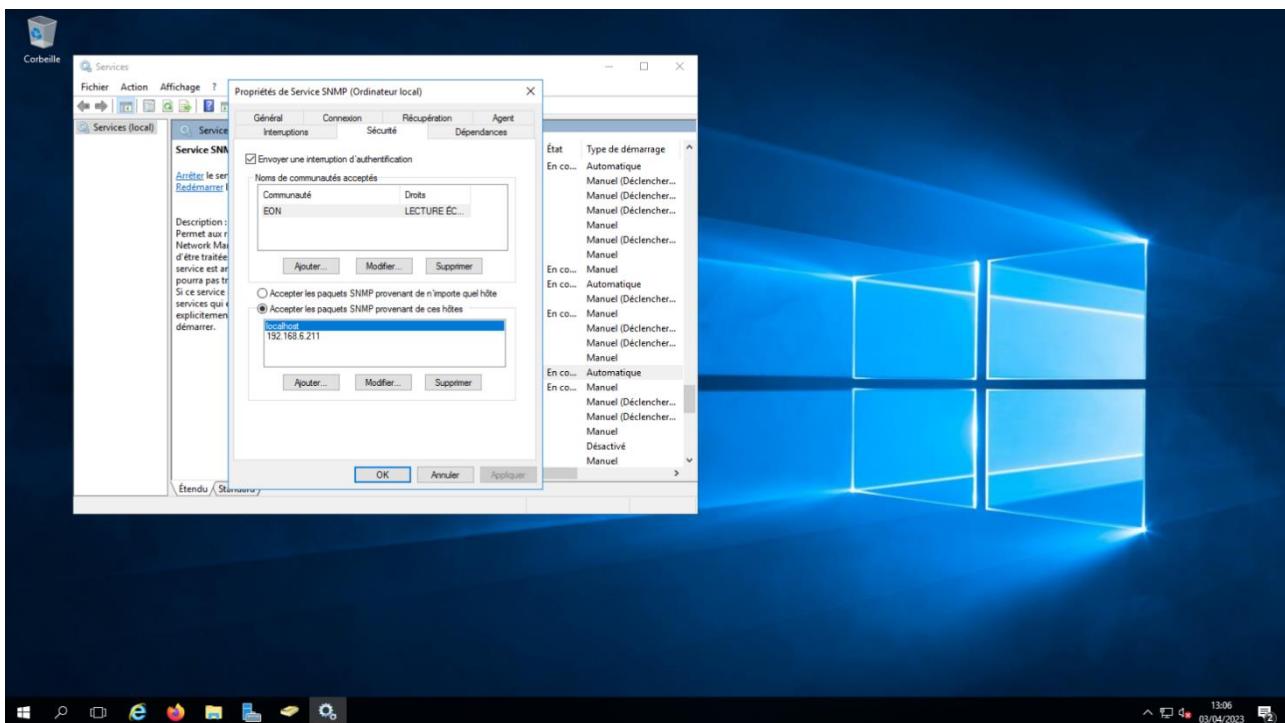
Maintenant pour que notre hôte Windows Server 2016 puisse communiquer avec notre Eyes of Network, nous devons configurer quelques éléments.

On se rend dans « Nagios Ressources » dans notre onglet « Configuration Nagios » et on nomme la case \$USER2\$.

On se rend ensuite dans les services sur notre Windows Server 2016 puis on fait un clic droit > propriété.



On va dans l'onglet sécurité, et on y ajoute le nom que nous avons donnée dans notre case puis son adresse IP.



On retourne sur notre tableau de bord et on y constate que nos deux machines sont correctement liées.

| Host ..   | Service .. | Status .. | Last Check .. | Duration ..    | Attempt .. | Status Information ..   |
|-----------|------------|-----------|---------------|----------------|------------|---|
| localhost | interfaces | OK        | 13:03:10      | 0d 0h 1m 35s   | 1/4        | OK, Intel(R) Dual Band Wireless-AC 7265, Gigabit Network Connection up  |
|           | memory     | OK        | 13:03:44      | 0d 0h 1m 1s    | 1/4        | Physical Memory: 360Used(1466MB/40995MB) Virtual Memory: 32%Used(1551MB/4799MB) (<0%) : OK                          |
|           | partitions | OK        | 13:04:18      | 0d 0h 0m 27s   | 1/4        | All selected storages (>95%): OK  |
|           | processor  | OK        | 13:00:53      | 0d 0h 3m 52s   | 1/4        | 2 CPU, average load 5.0%, >80%: OK  |
|           | system     | OK        | 13:01:27      | 0d 0h 3m 18s   | 1/4        | System Time OK - 04-03-2023, 13:01:27   |
|           | mysql      | OK        | 13:03:33      | 2d 20h 59m 46s | 1/4        | UpTime: 999 Threads: 12 Questions: 10244 Slow queries: 0 Opens: 115 Open tables: 100 Queries per second avg: 11.239 |
|           | ssh        | OK        | 13:01:50      | 2d 20h 58m 0s  | 1/4        | SSH OK - OpenSSH_7.4 protocol 2.0   |

Notre Eyes of Network est désormais correctement configuré et peut superviser notre Windows Server 2016.

## Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 8-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate

## CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

En référence à l'annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

|                             |                                |      |
|-----------------------------|--------------------------------|------|
| Identification <sup>1</sup> | GUELLUY, Pascal<br>02246218463 | SISR |
|-----------------------------|--------------------------------|------|

## 1. Environnement commun aux deux options

## 1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

| Éléments  | Description de l'implantation dans le centre d'examen<br>(nom du service ou de l'outil et caractéristiques techniques) | Remarques de la commission<br>d'interrogation |
|---|--|---|
| Un service d'authentification   | Active Directory   |   |
| Un SGBD   |  |   |
| Un accès sécurisé à internet  | FireWall, Antivirus  |   |
| Un environnement de travail collaboratif  |  |   |
| Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre ( <i>open source</i> ) | Windows, CentOs  |   |

<sup>1</sup> Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

**ANNEXE 8-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel**  
**Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**

| <b>Éléments</b>  | <b>Description de l'implantation dans le centre d'examen<br/>(nom du service ou de l'outil et caractéristiques techniques)</b> | <b>Remarques de la commission<br/>d'interrogation</b> |
|--|--|---|
| Une solution de sauvegarde   | Dossier partagé  |   |
| Des ressources dont l'accès est sécurisé et soumis à habilitation                  | Groupes active directory, GPO  |   |
| Deux types de terminaux dont un mobile (type <i>smartphone</i> ou encore tablette) |  |   |

**1.2 Des outils sont mobilisés pour la gestion de la sécurité :**

| <b>Éléments</b>                        | <b>Description de l'implantation dans le centre d'examen<br/>(nom du service ou de l'outil et caractéristiques techniques)</b> | <b>Remarques de la commission<br/>d'interrogation</b> |
|--|--|---|
| Gestion des incidents                  |  |   |
| Détection et prévention des intrusions | Pfsense  |   |
| Chiffrement                            |  |   |
| Analyse de trafic                      | Eyes of Network  |   |

**Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.**

## Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 8-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel

### 2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »

#### 2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

| Éléments  | Description de l'implantation dans le centre d'examen<br>(nom du service ou de l'outil et caractéristiques techniques) | Remarques de la commission<br>d'interrogation |
|---|--|---|
| Un réseau comportant plusieurs périmètres de sécurité   |  |   |
| Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité                                    |  |   |
| Un logiciel d'analyse de trames   |  |   |
| Un logiciel de gestion des configurations   | Tableau de bord Windows Server   |   |
| Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès  | RSAT   |   |
| Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes | Pfsense  |   |
| Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)               |  |   |

| <b>Éléments</b>   | <b>Description de l'implantation dans le centre d'examen<br/>(nom du service ou de l'outil et caractéristiques techniques)</b> | <b>Remarques de la commission<br/>d'interrogation</b> |
|---|--|---|
| Une solution garantissant la continuité d'un service  |  |   |
| Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion     | Redondance de serveur  |   |
| Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion |  |   |

**2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :**

| <b>Éléments</b>  | <b>Description de l'implantation dans le centre d'examen<br/>(nom du service ou de l'outil et caractéristiques techniques)</b> | <b>Remarques de la commission<br/>d'interrogation</b> |
|--|--|---|
| Une solution permettant la connexion sécurisée entre deux sites distants                           |  |   |
| Une solution permettant le déploiement des solutions techniques d'accès                            | WDS  |   |
| Une solution gérée à l'aide de procédures automatisées écrites avec un langage de <i>scripting</i> |  |   |
| Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau       |  |   |

- Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**
- Épreuve E5 - Conception et développement d'applications (option SLAM)**

**ANNEXE 7-2 : Modèle de fiche de contrôle de conformité pour l'épreuve****CONTRÔLE DE CONFORMITÉ****Nom et prénom :** GUELLUY, Pascal**N° candidat :** 02246218463

Conformément à l'arrêté du 22 juillet 2008 (B0 n° 32 du 28 août 2008) fixant définition et conditions de délivrance de certaines spécialités de brevet de technicien supérieur dont l'*annexe I* définissant le contrôle de conformité du dossier support d'épreuve, une commission de contrôle a été chargée d'apprécier la conformité des dossiers des candidats.

Après vérification, votre candidature ne peut être retenue pour le(s) motif(s) ci-dessous :

- absence de dossier ;
- dépôt du dossier au-delà de la date fixée par les autorités académiques.

Vous ne pourrez pas être interrogé(e), la note « non valide » (NV) vous sera attribuée pour l'épreuve, et le diplôme ne pourra vous être délivré.

**Date du contrôle :****Visa :**

- Épreuve E5 - Administration des systèmes et des réseaux (option SISR)  
 Épreuve E5 - Conception et développement d'applications (option SLAM)

**ANNEXE 7-3 : Document de préparation au déroulement de l'épreuve (recto)**

|  |   |   |
|--|---|---|
| <b>EXPRESSION DES BESOINS</b>  |   | N° commission :                                       |
| Épreuve ponctuelle   | <input type="checkbox"/> Contrôle en cours de formation | <input type="checkbox"/> Date : ..... / ..... / ..... |
| NOM, prénom : GUELLUY, Pascal  |   | N° candidat : 02246218463                             |
| Réalisation professionnelle retenue :  |   | N° réalisation :                                      |
| Circonstances de l'expression des besoins  |   |   |
| Spécifications fonctionnelles de la production attendue  |   |   |
| Si besoin liste des documents fournis (notamment schémas, diagrammes, ou encore images écran)  |   |   |
| Production attendue  |   |   |
| <b>Nature de la documentation professionnelle à présenter en appui de la solution</b>  |   |   |
| <input type="checkbox"/> Rapport de test<br><input type="checkbox"/> Documentation technique<br><input type="checkbox"/> Rapport d'incident<br><input type="checkbox"/> Documentation utilisateur                                |   | <input type="checkbox"/> Autre                        |
| Au cours de l'épreuve, la personne candidate est autorisée à utiliser les ressources électroniques mises à disposition par le centre d'examen, à l'exception de tout service d'échanges synchrones ou asynchrones avec un tiers. |   |   |
| La personne candidate est informée que l'ensemble des connexions réalisées peuvent faire l'objet d'un contrôle par la commission d'interrogation.  |   |   |

- Épreuve E5 - Administration des systèmes et des réseaux (option SISR)**
- Épreuve E5 - Conception et développement d'applications (option SLAM)**

**ANNEXE 7-3 : Document de préparation au déroulement de l'épreuve (verso)**

**Ajustements éventuellement demandés après le premier entretien d'explicitation (*pouvant être indiqués de façon manuscrite*)**

## Épreuve E5 - Administration des systèmes et des réseaux (option SISR)

## ANNEXE 7-5-A : Grille d'aide à l'évaluation (recto)

|  |   |                           |
|--|---|---------------------------|
| Nom, prénom : GUELLUY, Pascal                              | Date : ..... / ..... / .....                            | N° candidat : 02246218463 |
| Épreuve ponctuelle <input type="checkbox"/>                | Contrôle en cours de formation <input type="checkbox"/> | N° commission :           |
| Noms des membres de la commission d'interrogation<br>..... |   |                           |

**Proposition de note suite à l'évaluation du profil de la personne candidate**

Le tableau d'aide à l'appréciation des niveaux de maîtrise des compétences doit être complété de façon à évaluer le profil de la personne candidate (voir au verso). Une grille proposant des éléments d'appréciation des niveaux de maîtrise des compétences est proposée en bas de page.

La commission sera vigilante, lors de l'établissement de la note, sur la couverture des compétences du bloc exigée dans la définition de l'épreuve. Le cas échéant, l'appréciation littérale fera apparaître ce défaut de couverture dans la fiche communicable à la personne candidate.

NOTE   / 20**Liste des pénalités retenues**

Les pénalités ci-dessous doivent être appliquées de façon à ce que la note finale de la personne candidate (**annexe 7-6**) en tienne compte.

L'outil d'aide à l'appréciation de l'environnement technologique (**annexe 8**) permettra de préciser les éléments fondant la pénalité attribuée.

- |  |  |
|--|--|
| <input type="checkbox"/> Absence d'une réalisation professionnelle (10 points de pénalité)                                     |  |
| <input type="checkbox"/> Absence des deux réalisations professionnelles (20 points de pénalité)                                |  |
| <input type="checkbox"/> Environnement technologique mis en œuvre non conforme à l'annexe II.E (jusqu'à 15 points de pénalité) |  |

NOTE FINALE   / 20

Note à reporter sur la fiche d'appréciation destinée à la personne candidate

**Tableau d'aide à l'appréciation des niveaux de maîtrise des compétences du bloc au verso**

| Non évalué   | Non maitrisé  | Maitrise partielle   | Bonne maitrise  | Excellent maitrise  |
|--|---|--|---|---|
| Sous-compétence non évaluée au travers de la situation retenue | N'identifie pas, n'exploite pas ou n'intègre pas les informations, indicateurs, besoins ou contraintes              | Identifie, exploite ou intègre partiellement les informations, indicateurs, besoins ou contraintes | Identifie, exploite ou intègre les informations, indicateurs, besoins ou contraintes                      | Analyse de façon pertinente les informations, indicateurs, besoins ou contraintes, en mobilisant des outils     |
|  | Ne répond pas ou n'apporte pas de solution aux besoins exprimés   | Répond de façon peu adaptée au besoin exprimé, propose des solutions peu pertinentes               | Atteint les objectifs demandés, répond globalement aux besoins exprimés ou donne des éléments de solution | Propose des solutions pertinentes, permettant des améliorations/gains notables et en anticipant les contraintes |
|  | Ne s'implique pas ou ne mobilise pas les technologies et démarches adéquates dans la production du résultat attendu | Ne structure pas sa démarche ou mobilise de façon parcellaire les technologies et démarches        | Réalisation rigoureuse mobilisant les technologies et démarches appropriées                               | Mobilise une démarche agile et réactive, envisageant diverses technologies et solutions possibles               |
|  | Ne traite pas les erreurs   | Identifie les erreurs sans les résoudre  | Identifie et résout les erreurs   | Identifie et résout les erreurs et les documente  |
|  | Ne communique pas de façon appropriée, ni à l'écrit, ni à l'oral  | Communique à l'écrit et/ou l'oral sans apporter d'argumentation                                    | Communique à l'écrit et/ou l'oral de façon claire et explicite  | Communique à l'écrit et/ou l'oral de façon adaptée aux interlocuteurs, argumente de façon étayée                |

| Niveaux de maîtrise   |  |                          |                          |                          |                          |                          | ANNEXE 7-5-A : E5 - (option SISR) - Grille d'aide à l'évaluation (verso)  |
|---|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|---|
| Compétences   |  | Non évalué               | Non maîtrisé             | Maîtrise partielle       | Bonne maîtrise           | Excellent maîtrise       | Indicateurs de performance  |
| <b>Concevoir une solution d'infrastructure réseau</b>   |  | <input type="checkbox"/> | Les fonctionnalités et les exigences liées à la qualité attendue de la solution d'infrastructure sont identifiées.<br>Les contextes d'utilisation, les processus et les acteurs sur lesquels la solution d'infrastructure à produire aura un impact sont décrits.   |
| Analyser un besoin exprimé et son contexte juridique  |  | <input type="checkbox"/> | Les composants de l'architecture technique sur lesquels la solution d'infrastructure à produire aura un impact sont recensés.<br>Les risques liés à une mauvaise utilisation ou à un dysfonctionnement de la solution d'infrastructure sont identifiés.   |
| Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique                  |  | <input type="checkbox"/> | Les choix de solutions répondant au besoin exprimé (adaptation d'une solution existante ou réalisation d'une nouvelle) sont décrits et justifiés en termes de coût, de délai et de qualité.<br>La solution proposée tient compte des limites de responsabilité du prestataire informatique vis-à-vis de son métier et de son environnement.   |
| Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques       |  | <input type="checkbox"/> | Le dossier de choix et l'argumentaire technique sont rédigés et prennent en compte des préoccupations éthiques et environnementales.  |
| Choisir les éléments nécessaires pour assurer la qualité et la disponibilité d'un service                   |  | <input type="checkbox"/> | Les éléments permettant d'assurer la qualité et la continuité des services sont justifiés et caractérisés :<br>- les éléments à sauvegarder et à journaliser pour assurer la continuité du service et la traçabilité des transactions sont identifiés ;<br>- les procédures d'alerte associées au service sont spécifiées ;<br>- les solutions de fonctionnement en mode dégradé et les procédures de reprise du service sont décrites. |
| Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue |  | <input type="checkbox"/> | La maquette et le prototype sont conformes au besoin exprimé.   |
| Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue        |  | <input type="checkbox"/> | Les tests d'acceptation nécessaires à la validation de la solution d'infrastructure sont recensés.<br>Les jeux d'essai pertinents et les procédures pour la réalisation des tests sont préparés.  |
| <b>Installer, tester et déployer une solution d'infrastructure réseau</b>                                   |  | <input type="checkbox"/> | Des éléments d'infrastructure (élément d'interconnexion, service, serveur, équipement utilisateur) sont installés et configurés.<br>Les éléments d'infrastructure permettant d'assurer la continuité de service sont installés et configurés.<br>Le service fonctionne avec la disponibilité attendue.  |
| Installer et configurer des éléments d'infrastructure   |  | <input type="checkbox"/> | Une procédure de remplacement ou de migration d'un élément d'infrastructure est élaborée et mise en œuvre en respectant la continuité d'un service.   |
| Installer et configurer des éléments nécessaires pour assurer la continuité des services                    |  | <input type="checkbox"/> | Les éléments d'infrastructure permettant d'assurer la qualité de service sont installés et configurés.<br>Le service fonctionne avec la qualité attendue.   |
| Installer et configurer des éléments nécessaires pour assurer la qualité de service                         |  | <input type="checkbox"/> | La solution d'infrastructure est installée et configurée dans les règles de l'art :<br>- l'environnement de test est mis en place ;<br>- les tests pertinents d'intégration et d'acceptation sont effectués ;<br>- le rapport de tests est rédigé ;<br>- la documentation est à jour et disponible ;<br>- la solution d'infrastructure tient compte des préoccupations de développement durable.  |
| Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure          |  | <input type="checkbox"/> | L'intégration de la solution ne génère pas de dysfonctionnement du réseau ou dans le réseau.<br>Une procédure claire de déploiement de la solution est rédigée.   |
| Tester l'intégration et l'acceptation d'une solution d'infrastructure                                       |  | <input type="checkbox"/> | La solution d'infrastructure est déployée selon la procédure et la planification définies.  |
| <b>Exploiter, dépanner et superviser une solution d'infrastructure réseau</b>                               |  | <input type="checkbox"/> | Un dispositif d'administration sur site et à distance est configuré et exploité.<br>Les conditions d'administration des éléments d'infrastructure sont maîtrisées.<br>L'automatisation des tâches d'administration répond au besoin exprimé.  |
| Administrer sur site et à distance des éléments d'une infrastructure  |  | <input type="checkbox"/> | Les outils nécessaires à la production d'indicateurs d'activité et à l'exploitation de fichiers d'activité sont installés et configurés.<br>Les dysfonctionnements récurrents dans une solution d'infrastructure sont repérés et leurs causes identifiées.<br>Le degré d'urgence et le niveau d'intervention sont définis.<br>Les conséquences techniques du problème sont évaluées.  |
| Automatiser des tâches d'administration   |  | <input type="checkbox"/> | L'incident est résolu ou escaladé de manière efficiente, en tenant compte des délais et procédures en vigueur.<br>Le problème est résolu ou escaladé de manière efficiente, en tenant compte des délais et procédures en vigueur.   |
| Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure                          |  | <input type="checkbox"/> | Les rapports d'incidents et les comptes rendus de problèmes sont rédigés et adaptés à chaque destinataire tant par leur contenu que par leur présentation.<br>Des mesures correctives sont proposées ou mises en œuvre pour maintenir ou améliorer la qualité d'un service.   |
| Identifier, qualifier, évaluer et réagir face à un incident ou à un problème                                |  | <input type="checkbox"/> | Les éléments d'une solution d'infrastructure et leur utilisation sont supervisés.<br>Les indicateurs et les fichiers d'audit sont analysés et exploités.<br>Des alertes adaptées à la criticité du service sont générées.   |
| Évaluer, maintenir et améliorer la qualité d'un service   |  | <input type="checkbox"/> | Les procédures d'alerte destinées à rétablir la qualité du service sont appliquées.<br>Le fonctionnement du service en mode dégradé et la disponibilité des éléments d'infrastructure permettant une reprise du service sont périodiquement vérifiés.<br>Le rétablissement de la qualité du service est assuré dans les délais prévus.  |

**Épreuve E5 - Administration des systèmes et des réseaux (option SISR)****Épreuve E5 - Conception et développement d'applications (option SLAM)****ANNEXE 7-6 : Fiche d'appréciation destinée à la personne candidate**

|   |                          |                                       |  |                                     |
|---|--------------------------|---------------------------------------|--|-------------------------------------|
| <b>Nom, prénom : GUELLUY, Pascal</b>  |                          | <b>N° candidat : 02246218463</b>      |  |                                     |
| <b>Épreuve ponctuelle</b>   | <input type="checkbox"/> | <b>Contrôle en cours de formation</b> | <input type="checkbox"/>                     | <b>N° commission :</b>              |
| <b>OPTION SISR</b>  | <input type="checkbox"/> | <b>OPTION SLAM</b>                    | <input type="checkbox"/>                     | <b>Date : ..... / ..... / .....</b> |
| <b>Phase 1 : Entretien d'explicitation (20 minutes maximum)</b>   |                          |                                       |  |                                     |
| <b>Observations</b>   |                          |                                       |  |                                     |
| <b>Phase 2 : Recette de la solution (20 minutes maximum)</b>  |                          |                                       |  |                                     |
| <b>Observations</b>   |                          |                                       |  |                                     |
| <b>Appréciation sur les niveaux de maîtrise des compétences, sur la mobilisation de toutes les compétences du bloc et sur la conformité de l'environnement technologique des réalisations professionnelles présentées</b> |                          |                                       |  |                                     |
| Une réalisation professionnelle absente   |                          | <input type="checkbox"/>              | Aucune réalisation professionnelle présentée | <input type="checkbox"/>            |
|   |                          |                                       | <b>NOTE</b>                                  | <input type="text"/> / 20           |
| <b>Visa des membres de la commission d'interrogation</b>  |                          |                                       |  |                                     |