BTS Services Informatiques aux Organisations

Option Solutions d'Infrastructure, Systèmes et Réseaux

OPTION SISR

Épreuve E5 – Administration des systèmes et des réseaux

Fiche technique

Projet 2 :

Mise en place d'un contrôleur de domaine sous Windows Server 2022 avec les services AD DS, DHCP, DNS, différentes GPO déployées, un serveur de fichiers, un firewall pfsense

ELAMRANI Iliane

Session 2024

Table des matières :

Table des figures :

1 *Introduction :*

Afin de répondre aux demandes de l'instep de Ales, nous devons mettre en place :

Un contrôleur de domaine sous Windows Server 2022 avec les rôles et services suivants :

- **Un AD DS** : pour les fonctions d'Active Directory pour la gestion des utilisateurs par exemple.
- **Un DNS** : attribue un nom compréhensible, à une adresse IP et inversement.
- **Un DHCP** : Permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP.

2 *Installation Windows Server 2022 :*

Je possédais une clé USB contenant Windows Server 2022. Je l'ai donc simplement installé sur ma machine.

Suite à cela, les choix suivant ce présentent à nous :

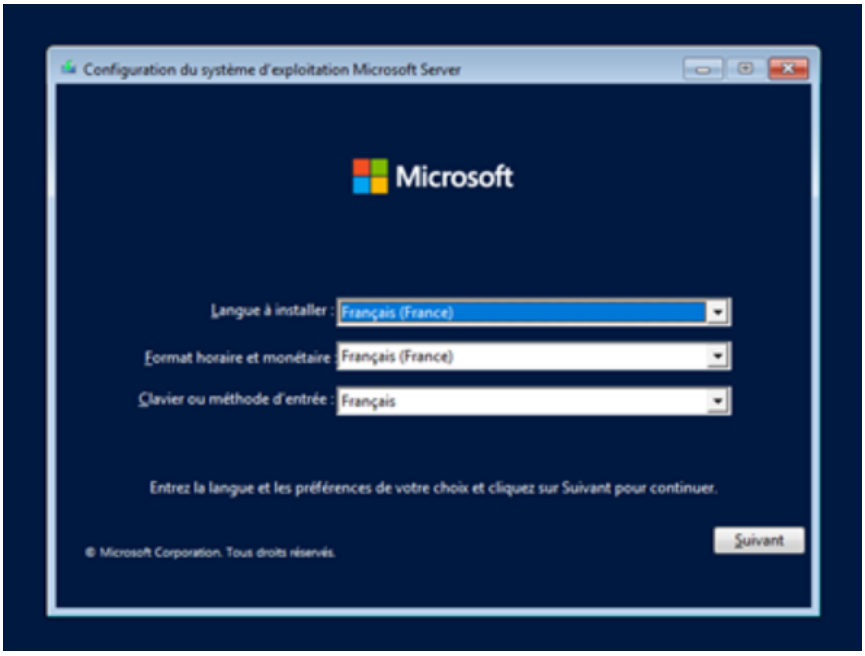


Figure 1 : Windows Server 2016 / langue

Cliquer sur **« Installer maintenant »**

Figure 2 : Windows Server 2016 / Installer maintenant

Nous avons besoin d'une interface graphique pour plus tard, le choix de **Windows Serveur 2022 Standard (expérience utilisateur)** est donc essentiel.

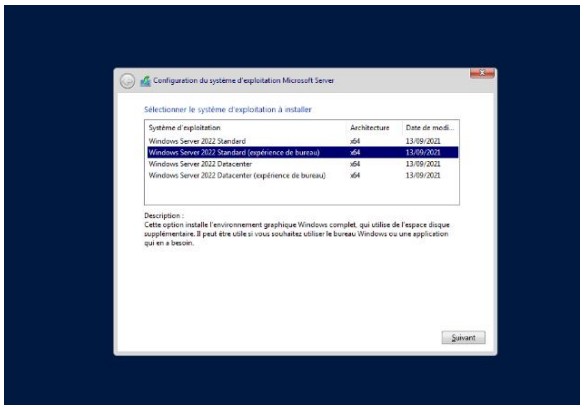


Figure 3 : Windows Server 2016 / Standard Evaluation (Expérience utilisateur)

Choisissons l'installation **mise à niveau**

Figure 4 : Windows Server 2022 / Mise à niveau

Maintenant l'installation démarre :

Figure 5 : Windows Server 2016 / Installation de Windows

Après cette étape, nous allons créer un mot de passe afin de se connecter à l'interface graphique du Windows Server 2022.

3 *Contrôleur de domaine :*

Avant toutes choses, nous allons communiquer des informations sur le protocole internet TCP/IPv4 du serveur Windows Server 2022 avant d'installer le contrôleur de domaine

Pour cela, il faut ouvrir le terminal cmd et rentrer la commande **« ipconfig »** pour consulter les données dont nous avons besoins.

Maintenant, Rendez-vous sur le Centre Réseau et partage puis dans les propriétés Ethernet.

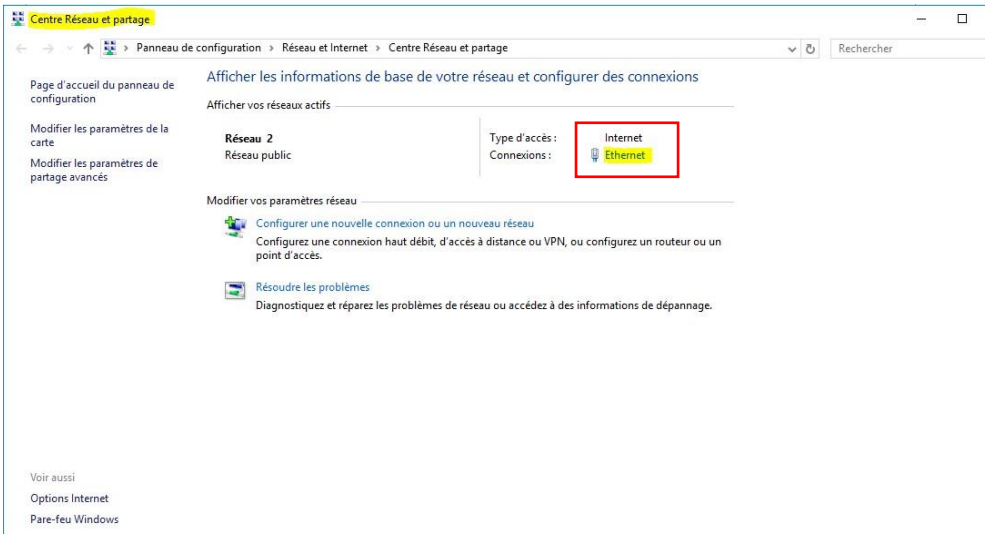


Figure 6 : Centre Réseau et partage / propriétés Ethernet

Aller sur **Protocole Internet version 4 (TCP/IPv4)**.

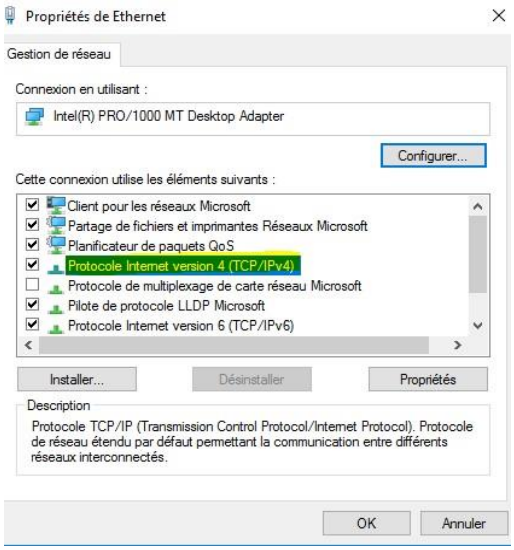
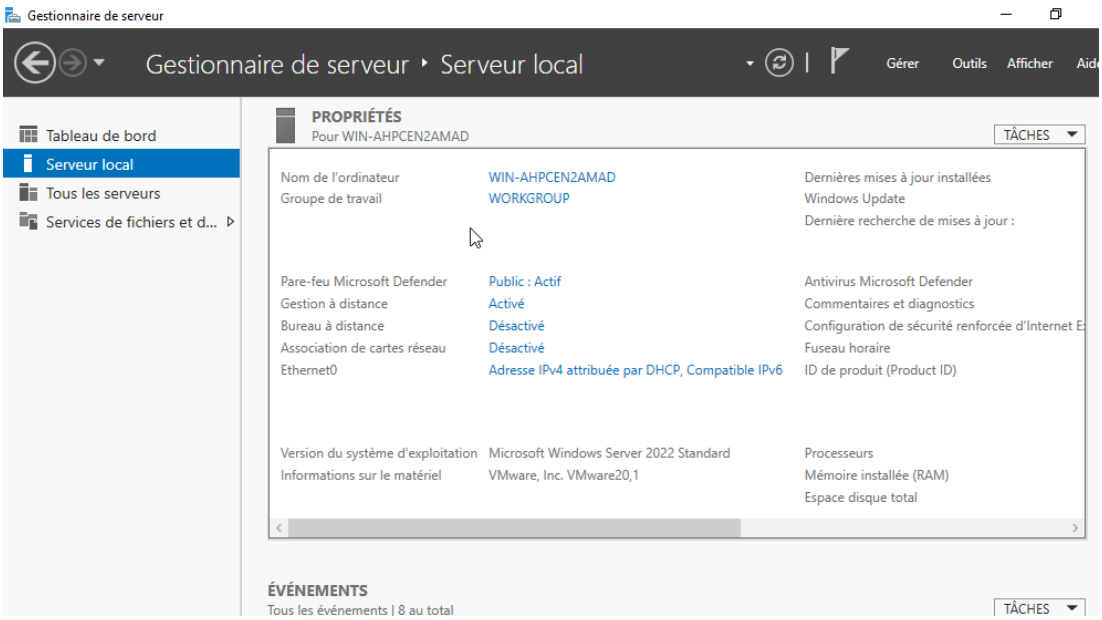


Figure 7 : Gestion de réseau Protocole TCP/IPv4

Maintenant rentrons les informations associées à notre serveur. Notamment l'adresse IP et le masque de sous-réseau.

Figure 8 : Paramètres IP Protocole TCP/IPv4

Après cela, nous ouvrons **le gestionnaire de serveur** puis **Serveur local** à gauche de la fenêtre. Le but étant de modifier le nom de la machine



Modifier le nom, puis cliquer sur OK :

Figure 10 : Propriétés système / modification du nom du PC

Redémarrer la machine afin d'appliquer le changement de nom.

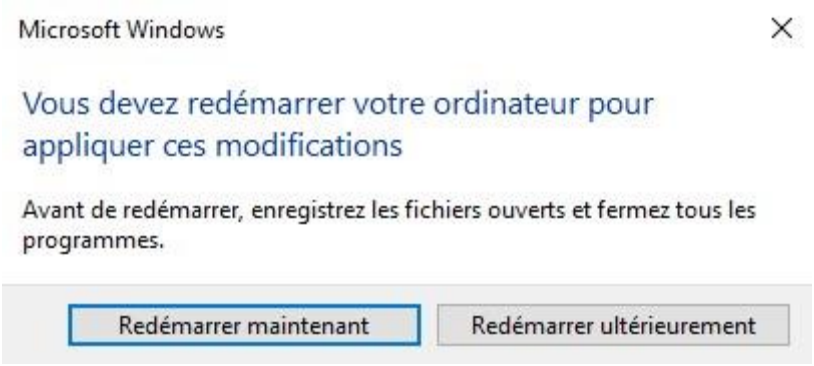


Figure 11 : « Redémarrer maintenant »

4 Rôles et fonctionnalités :

Encore sur le gestionnaire de serveur pour **ajouter des rôles et fonctionnalités**. Il faudra aller sur **Gérer** puis **Ajouter des rôles et fonctionnalités** placé à côté du drapeau.

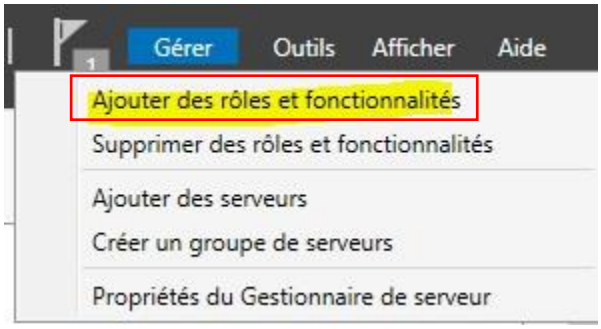


Figure 12 : Gérer / ajout des rôles et fonctionnalités

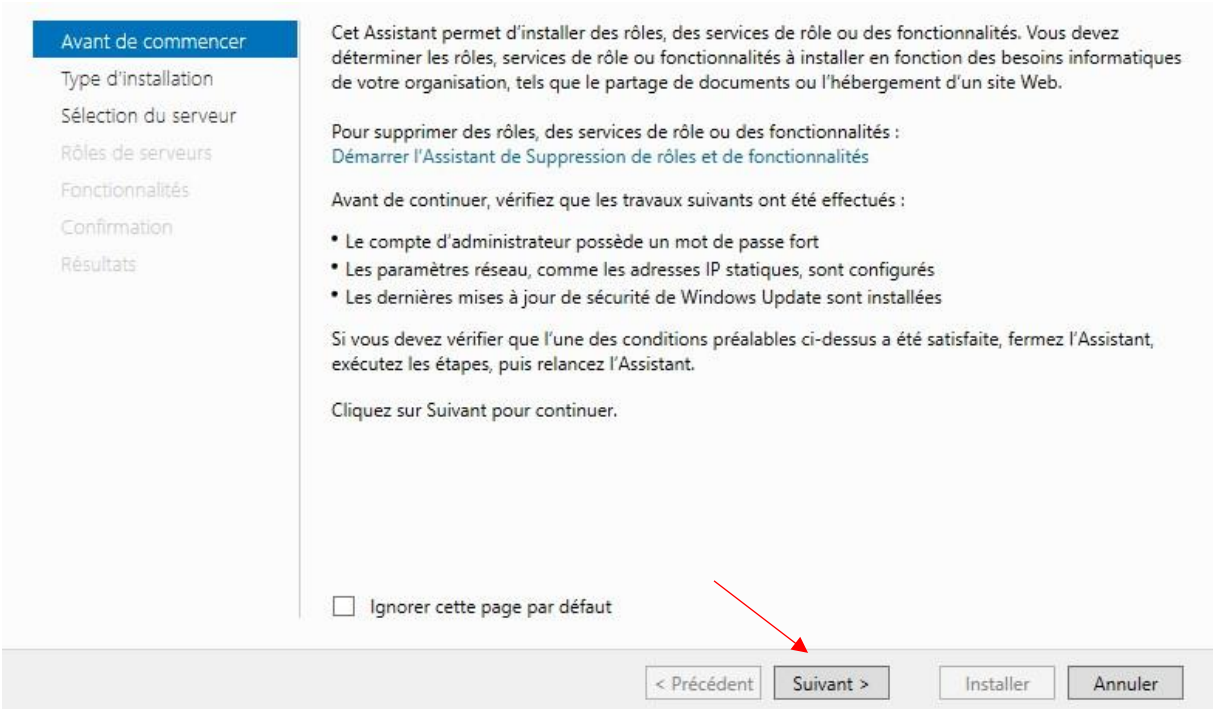


Figure 13 : Assistant / Avant de commencer

Installation basée sur un rôle ou une fonctionnalité.

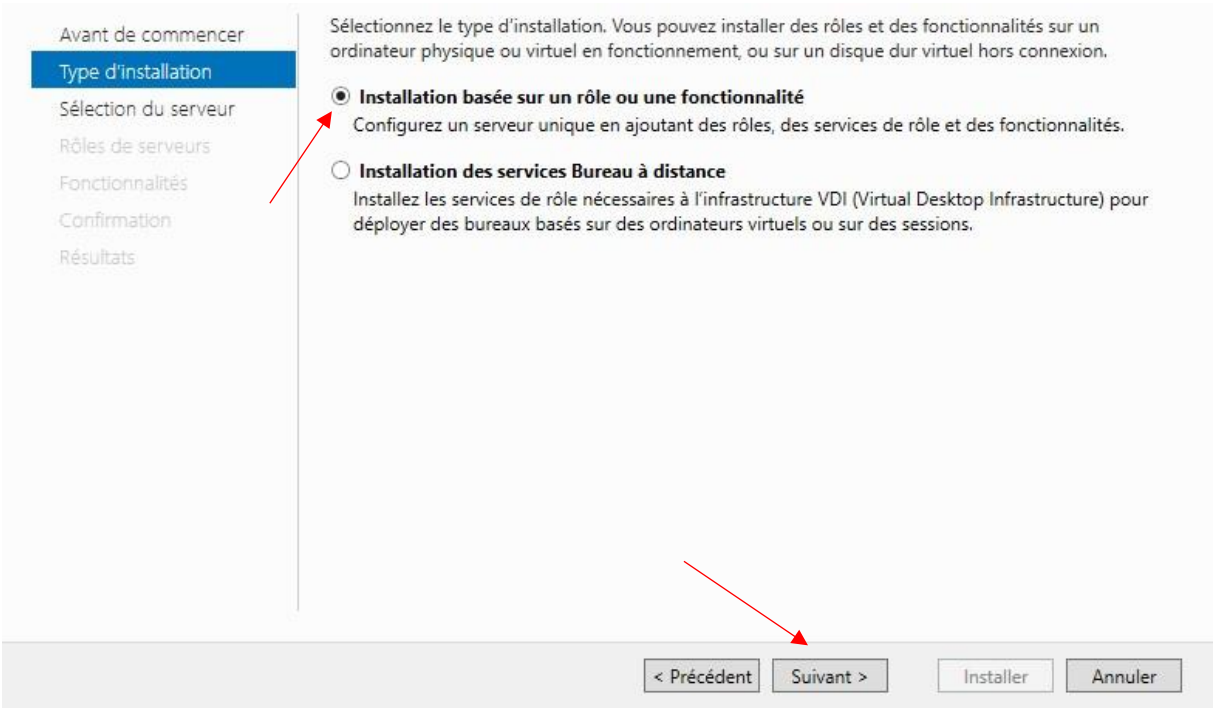


Figure 14 : Assistant / Type d'installation

Sélectionner un serveur du pool de serveurs :

Choisissons les rôles de serveur de base, **DHCP / DNS / AD DS** comme expliqué dans L'introduction :

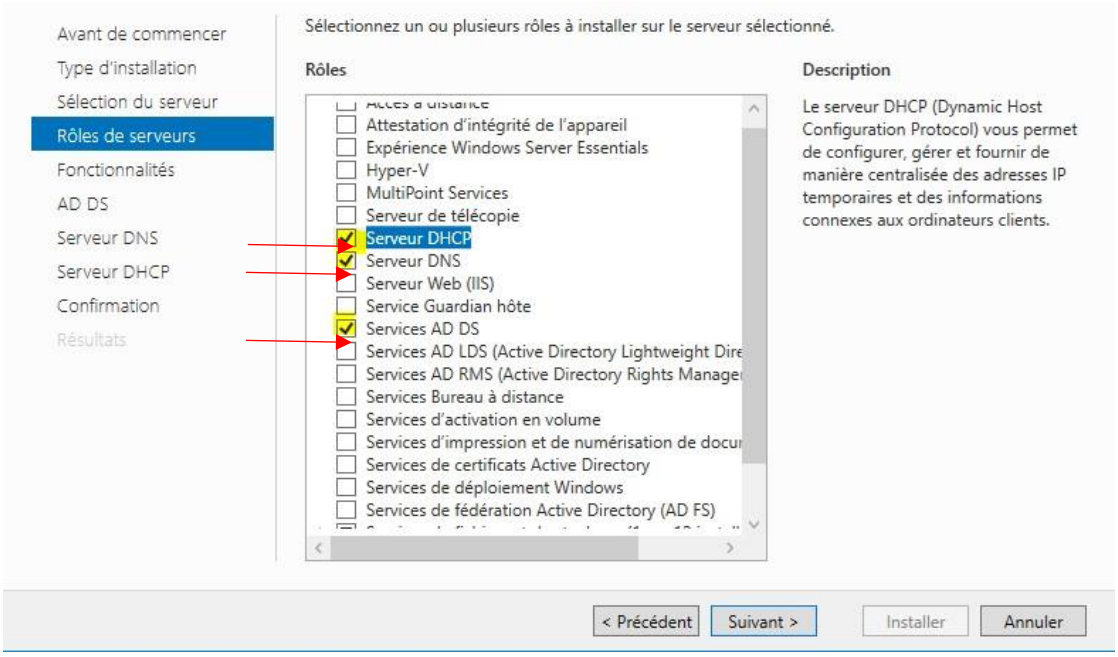


Figure 16 : Assistant / Rôles de serveurs

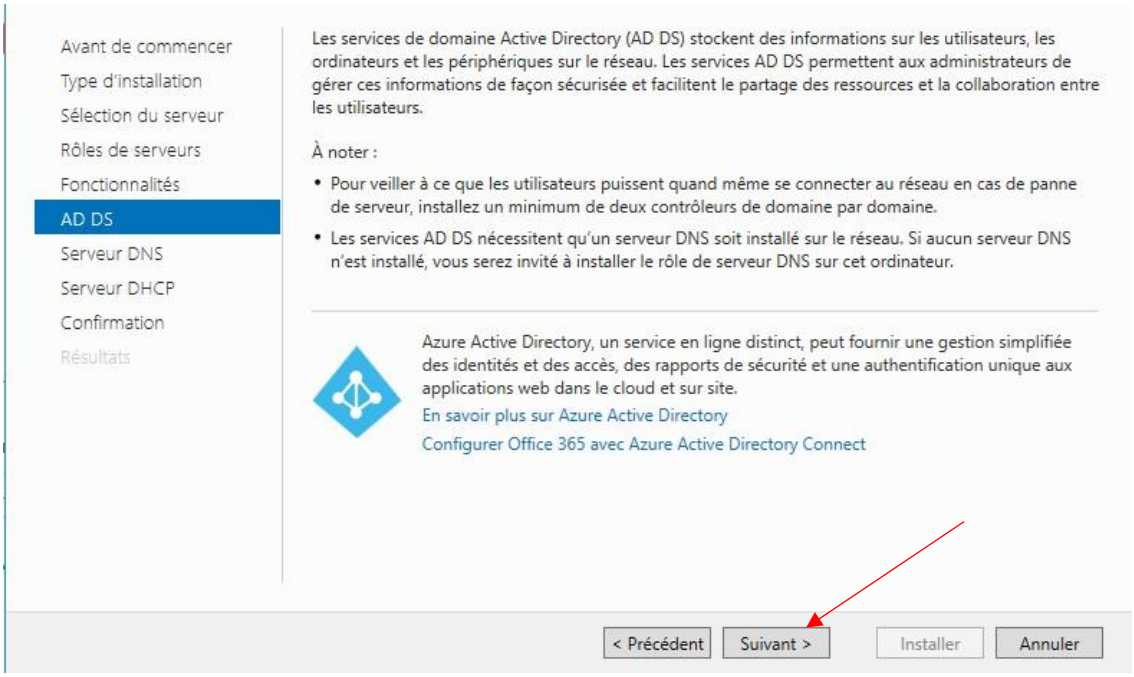


Figure 17 : Assistant / (AD DS) Services de domaine Active Directory

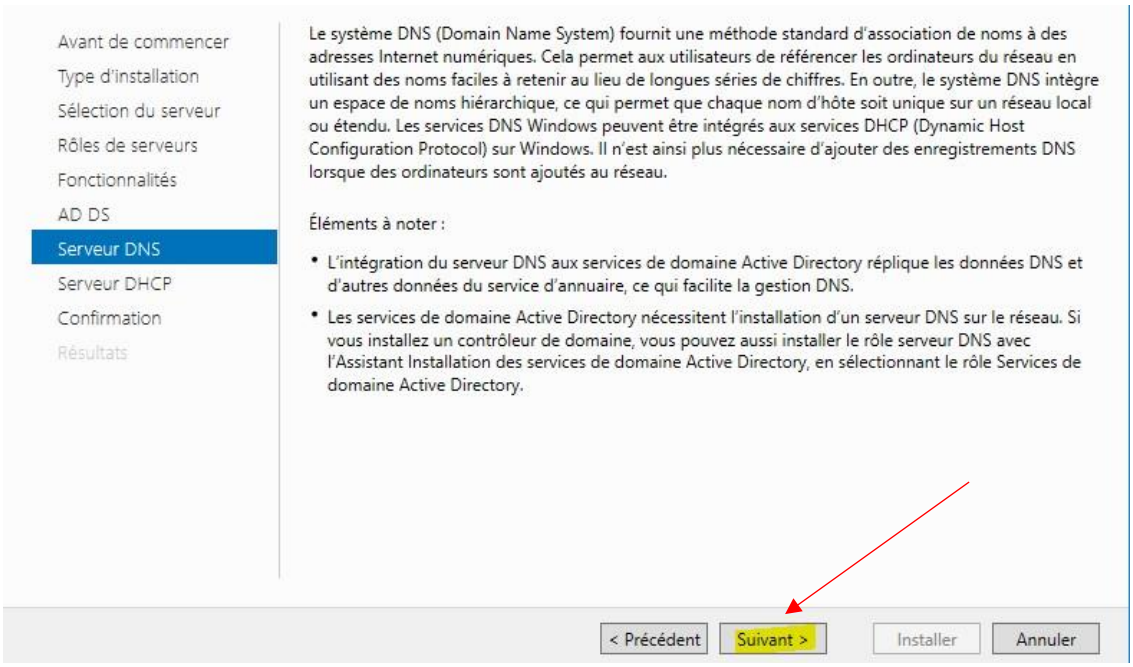


Figure 18 : Assistant / Serveur (DNS) Domain name system

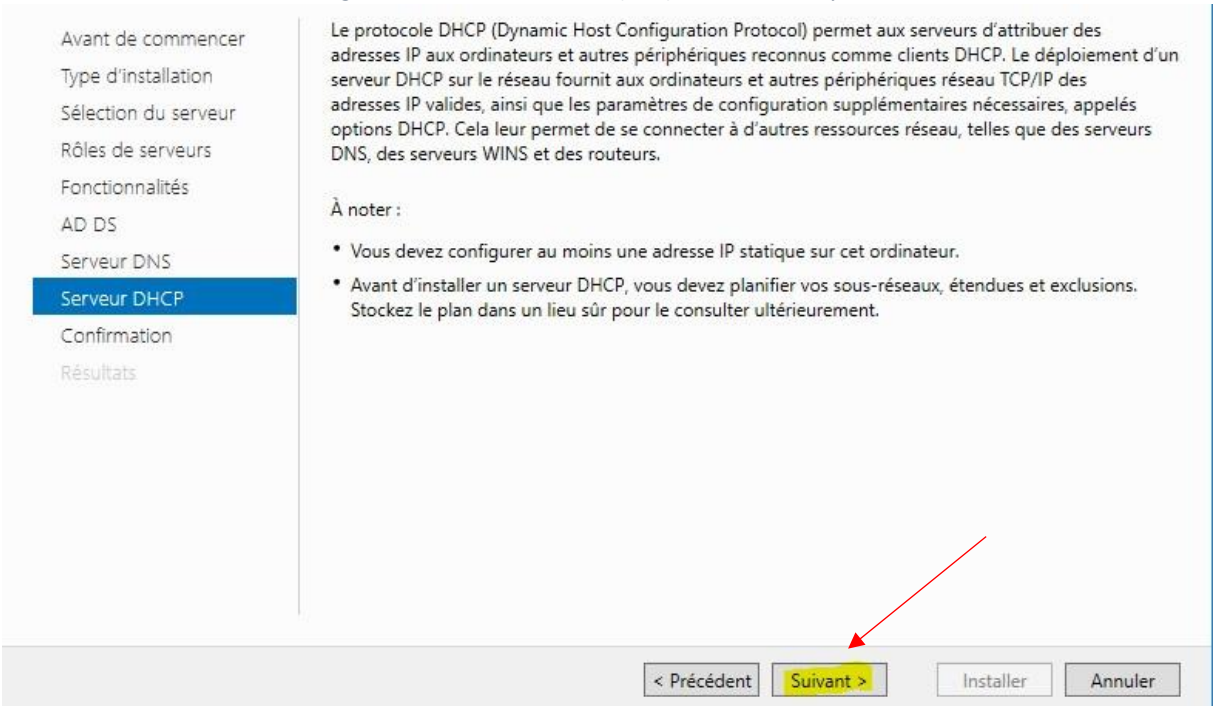


Figure 19 : Assistant / Serveur (DHCP) Dynamic host configuration protocol

L’installation est à présent en cours de chargement…

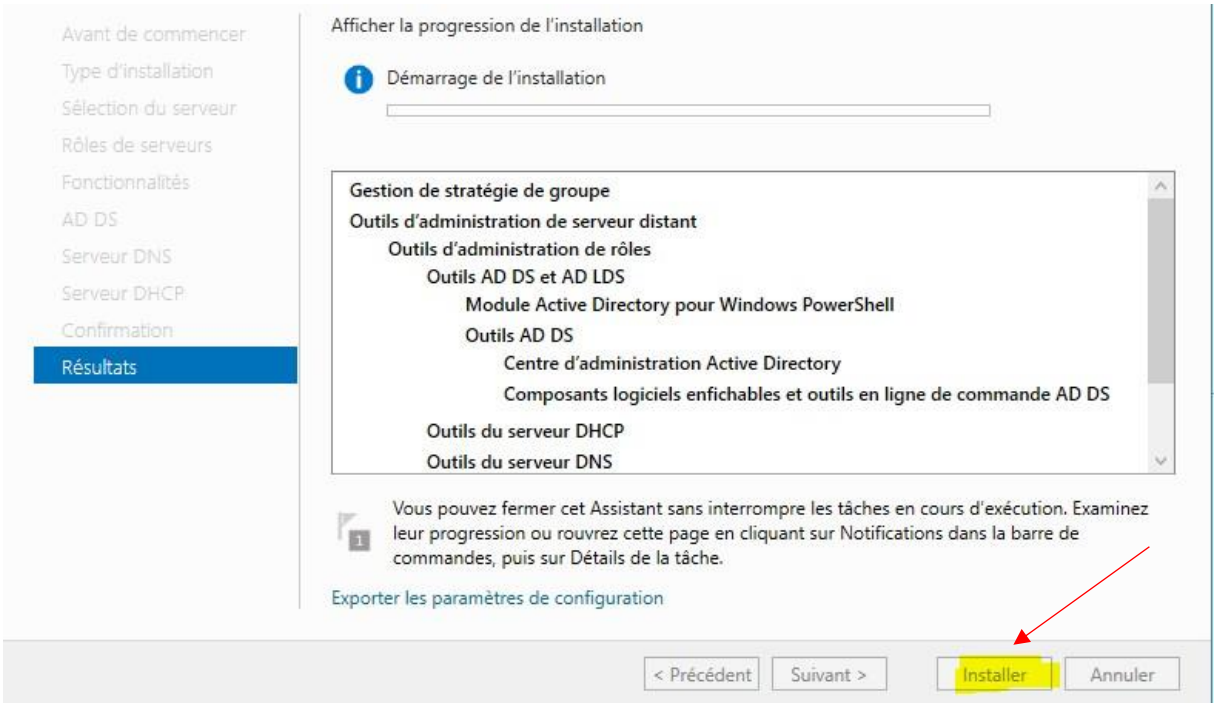
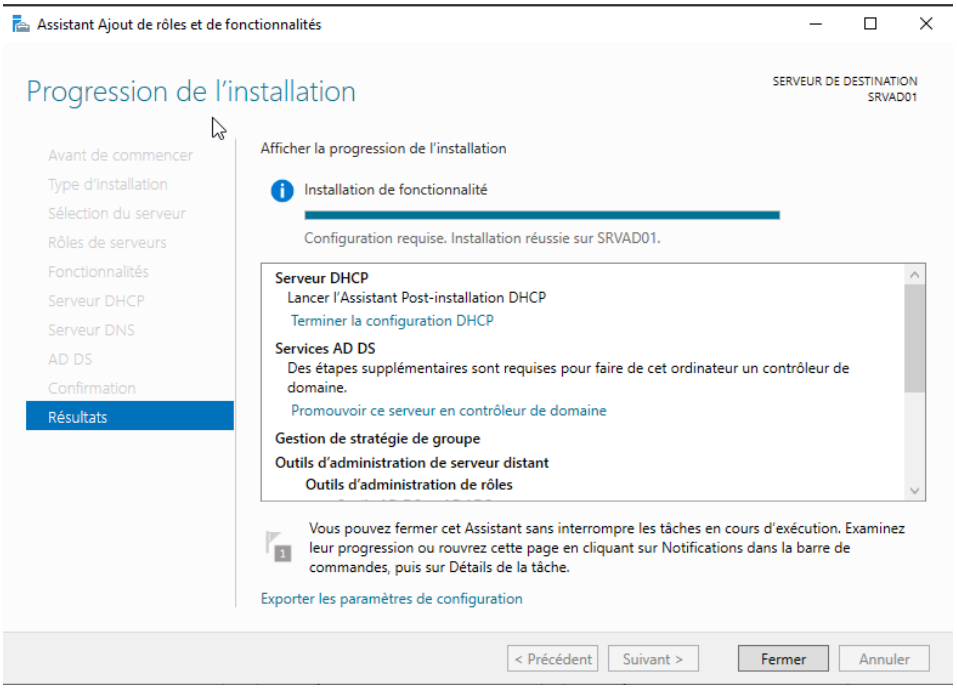


Figure 20 : Assistant / Démarrage de l’installation

Après l’installation, allons sur **Promouvoir ce serveur en contrôleur de domaine**.



5 *Configuration Active Directory :*

Dans **configuration de déploiement**, Prenez l'option **ajouter une nouvelle forêt**. Avec le contexte Keyse sous la forme de : Keyse.local

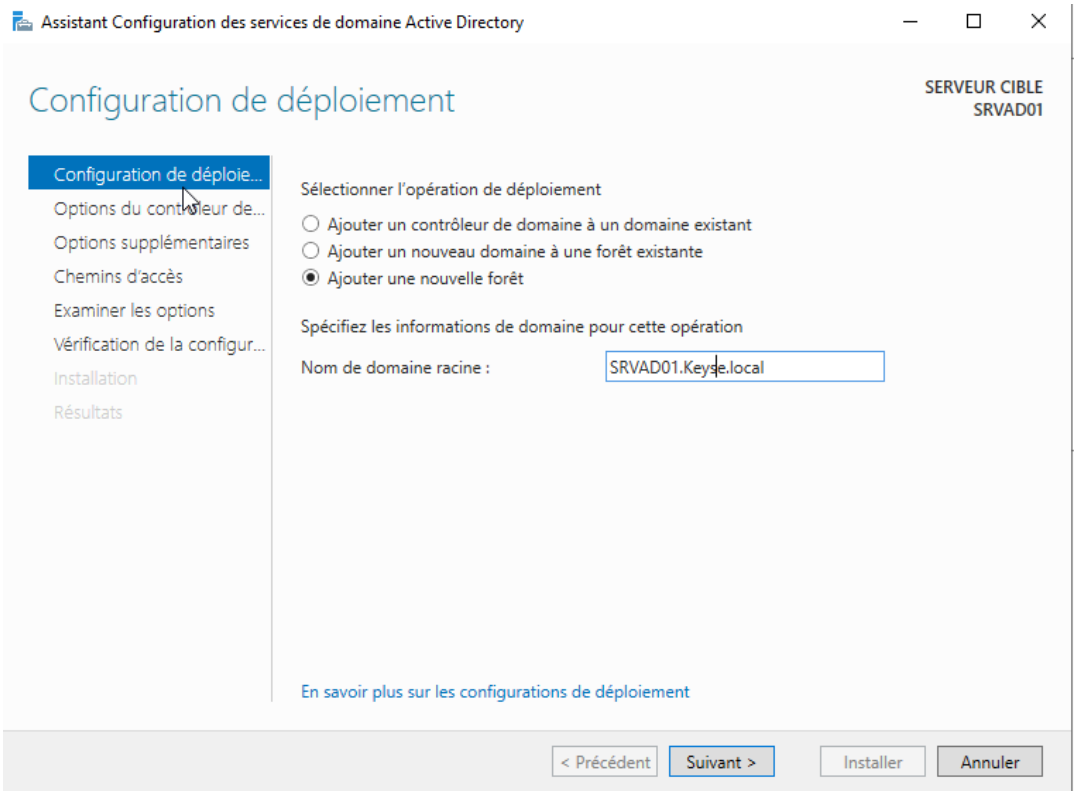


Figure 22 : Active Directory / Configuration de déploiement

Mettre un nouveau mot de passe comme indiqué sur la capture d'écran :

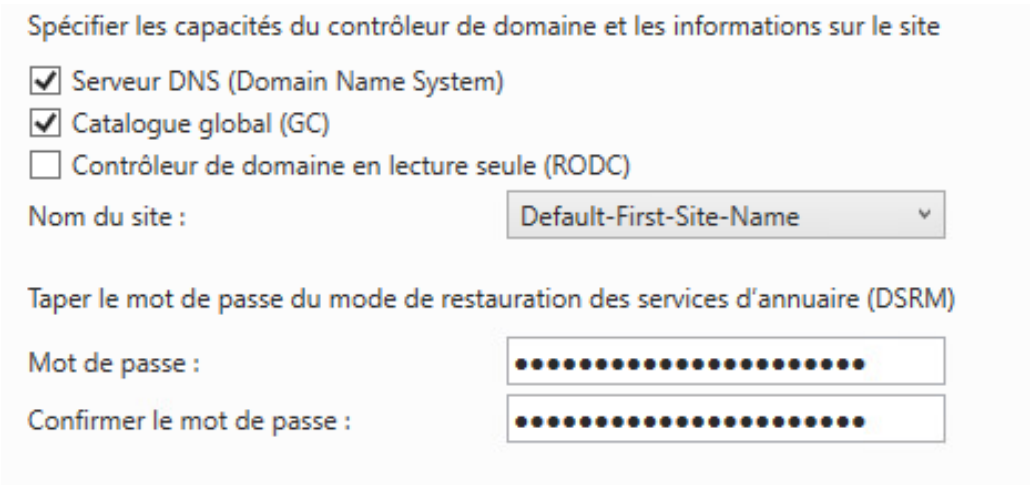


Figure 23 : Active Directory / Option du contrôleur de domaine

Pas de création de délégation DNS.

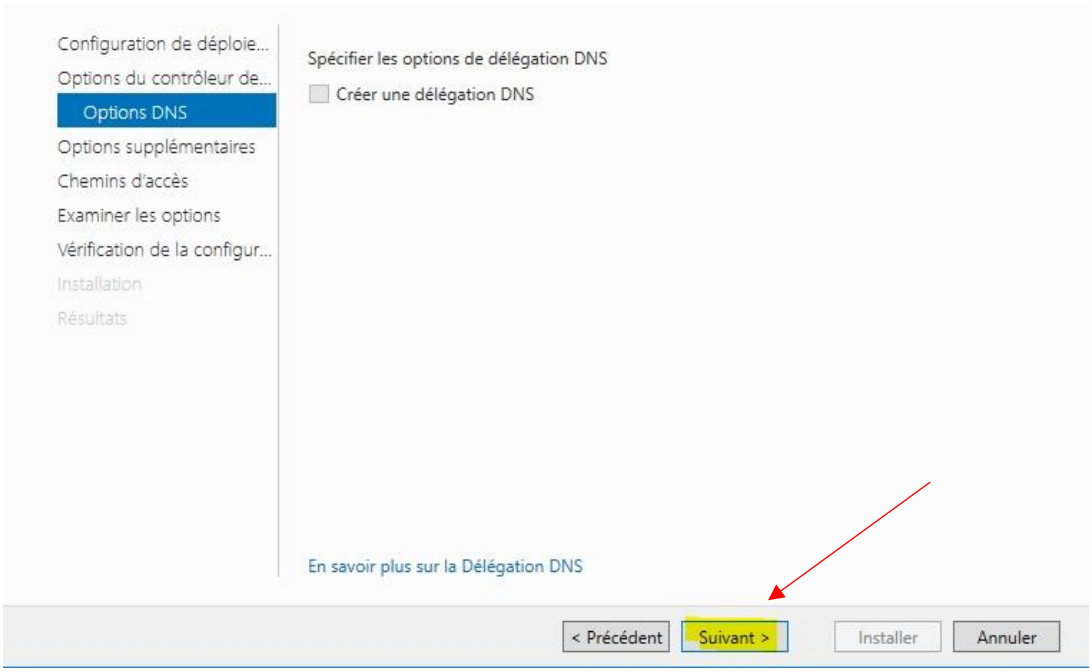


Figure 24 : Active Directory / Option DNS

Aucune modification pour les chemins d'accès :

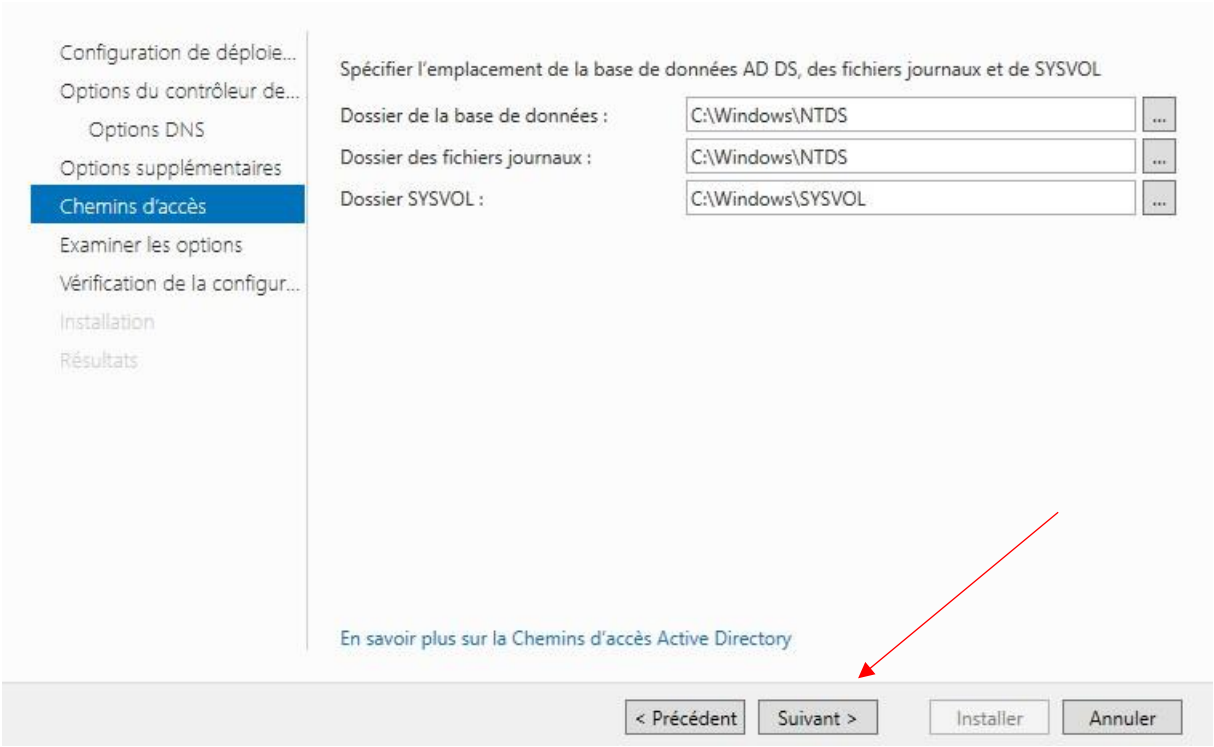


Figure 26 : Active Directory / Chemin d'accès

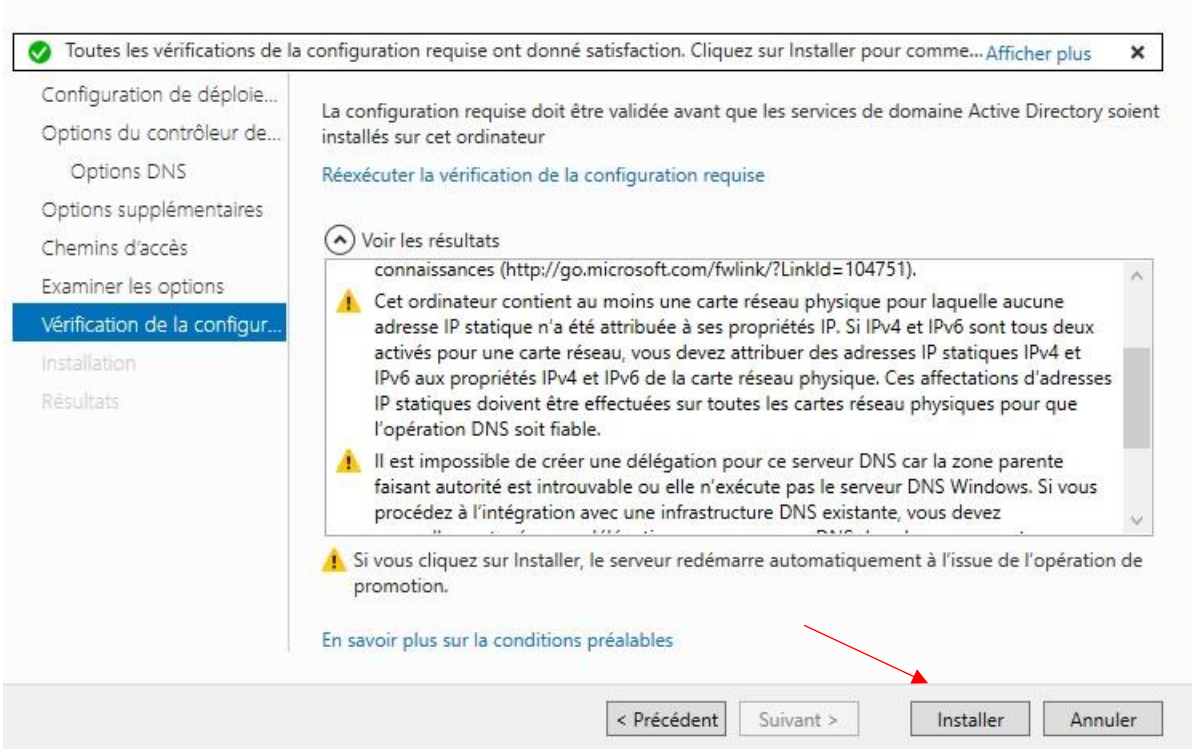


Figure 28 : Active Directory / Vérification de la configuration requise

Après l'installation, le redémarrage se fera automatiquement.

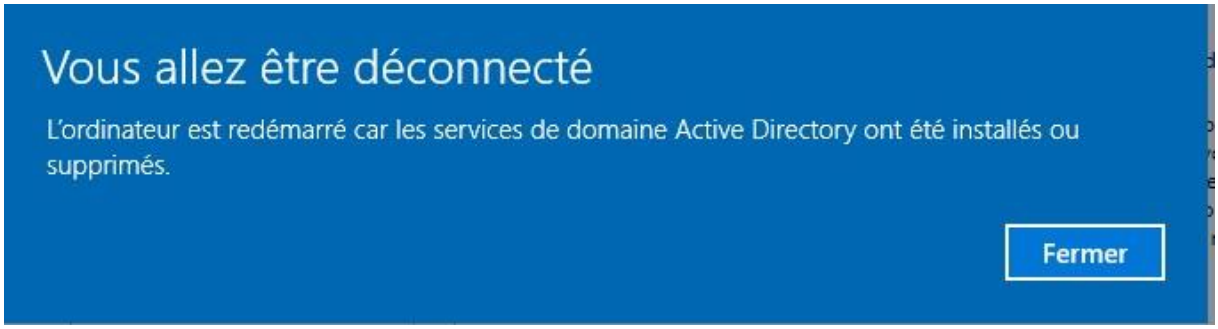


Figure 29 : Installer puis redémarrer

Un nouveau mot de passe vous sera demandé à la prochaine connexion, Il doit être différent du précédent.

Maintenant que vous êtes sur la session, dirigez-vous sur **le gestionnaire de serveur** puis sur le **drapeau** en haut de la fenêtre. Ce drapeau permet d'afficher les notifications.

Ici nous avons l'état de l'avancement de la configuration du post-déploiement :

Figure 30 : Notification / Avancement de la configuration

5.1 Paramétrage DHCP :

Du coup, nous allons procéder à la configuration du DHCP, pour cela, cliquez sur Terminer la configuration DHCP :

Figure 31 : DHCP / « Terminer la configuration DHCP »

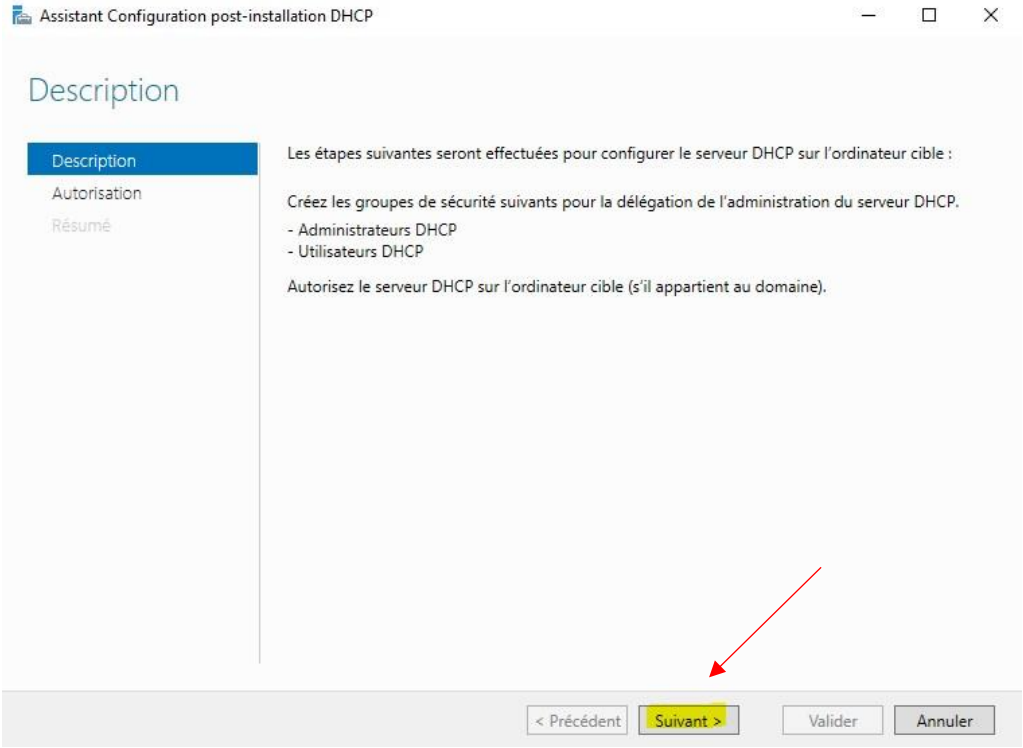


Figure 32 : DHCP / Description

Sélectionner "utiliser les informations d'identifications de l'utilisateur suivant :"

Vous devriez retrouver : "**NOMDEVOTREMACHINE\Administrateur**"

Figure 33 : DHCP / Autorisation

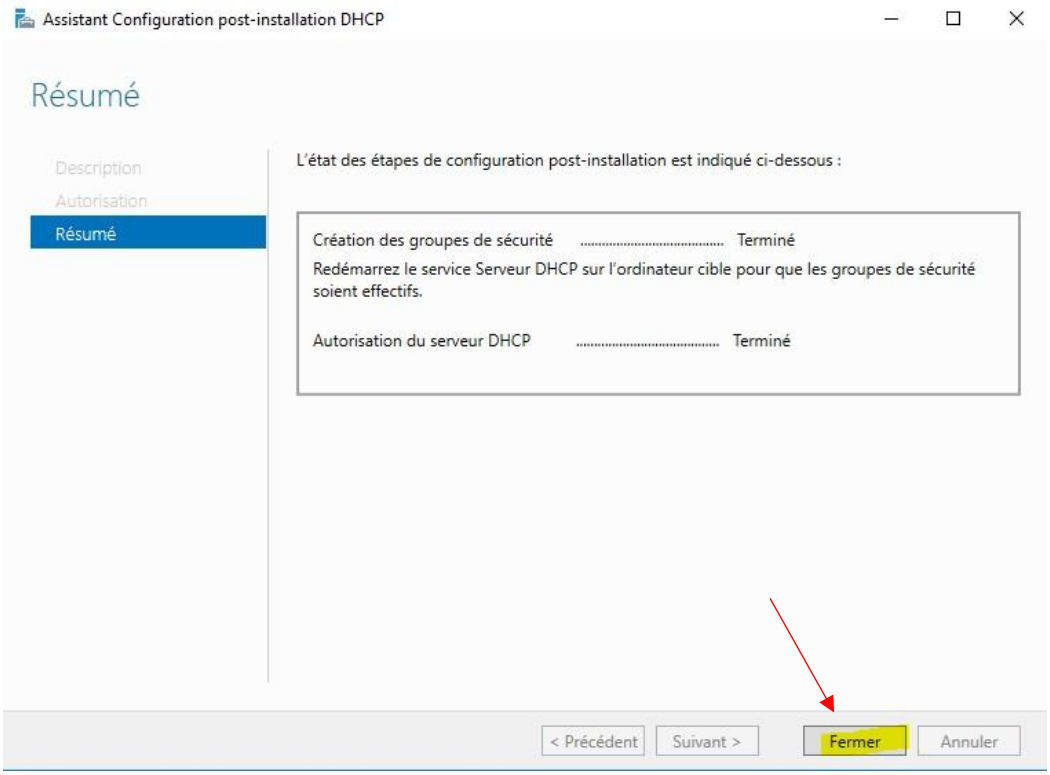


Figure 34 : DHCP / Résumé

Maintenant, redémarrez l'ordinateur.

Figure 35 : Fermer puis redémarrer

Nous allons Configurer le rôle DHCP.

Je me dirige donc vers **le gestionnaire de serveur** puis **Outils** et **DHCP**.

Nous allons créer une étendue, en réduisant l'adresse du DHCP faire **clic droit** et **Nouvelle étendue**.

L’assistant demandera de renseigner une adresse IP de début et de fin, une longueur et pour finir, un masque de sous réseau.

Voici un exemple de configuration pour ma première étendue.

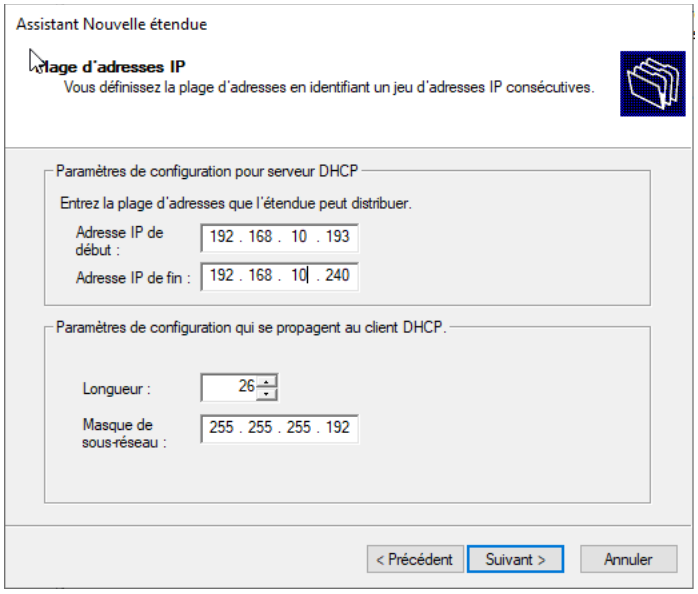


Figure 36 : Paramétrage adresse IP / VLAN 22

La passerelle par défaut correspond à l’adresse IP du routeur.

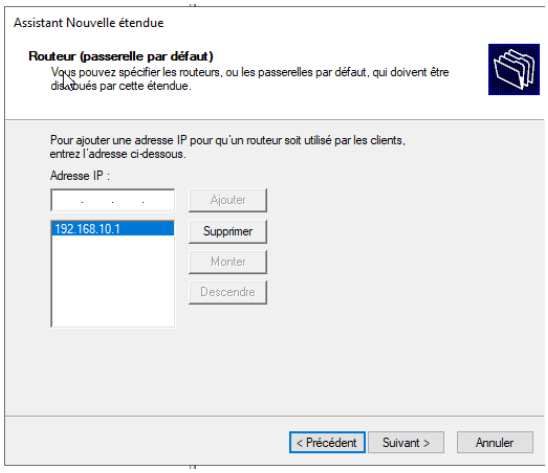


Figure 37 : Routeur / Passerelle par défaut

Pour cette étape vérifier simplement que les informations préremplies sont bonnes, puis faite suivant :

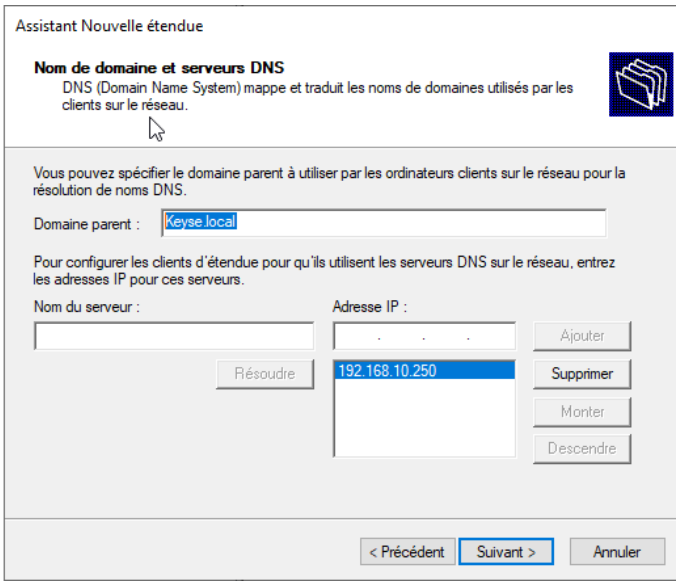


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

5.2 Paramétrage DNS :

Passons à la configuration du DNS, il nous faut avant tout créer une zone inversée.

Aller sur le gestionnaire de serveur, puis **Outils** et **DNS**.

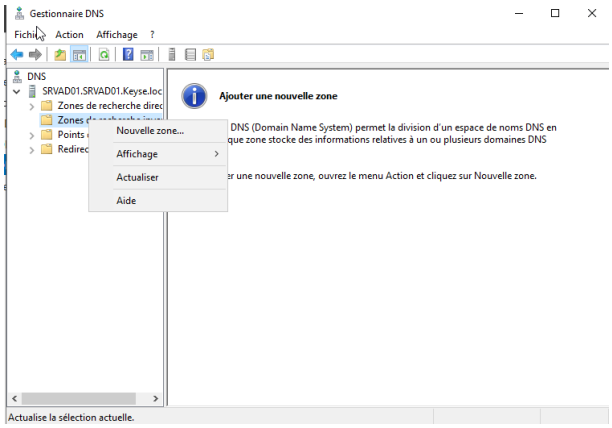
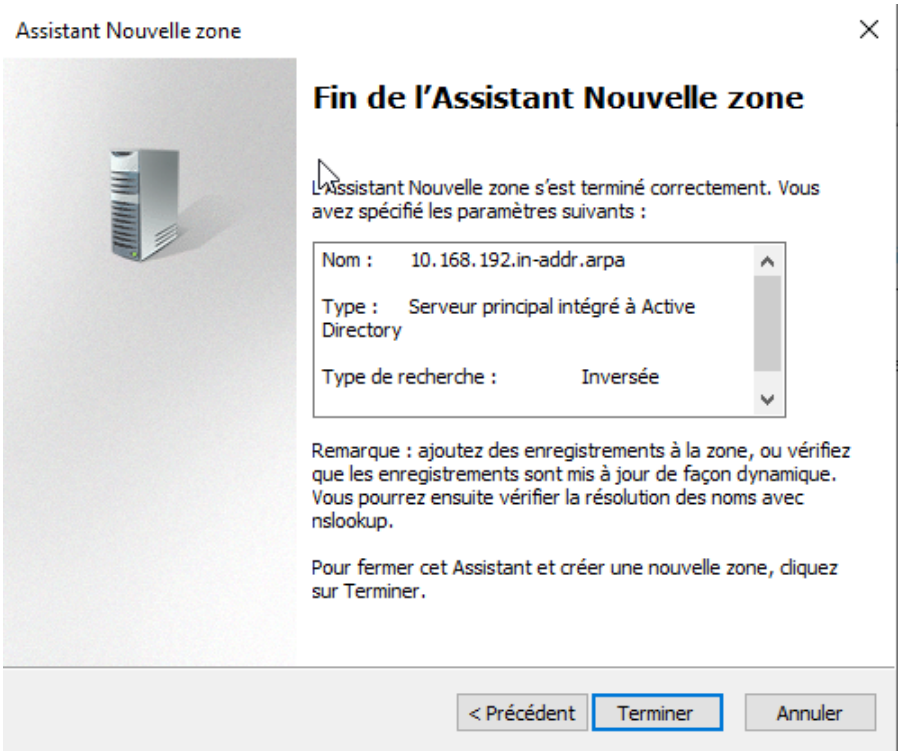


Figure 41 : DNS / Nouvelle zone de recherche inversée

Ensuite, je laisse la configuration par défaut que l'assistant me donne.

Puis comme ID réseau je renseigne : **192.168.10.250** (qui correspond à mon serveur).



Le DNS est maintenant configuré.

Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Vérifions tout de même que la zone est bien dans le dossier **Zones de recherche inversée**.

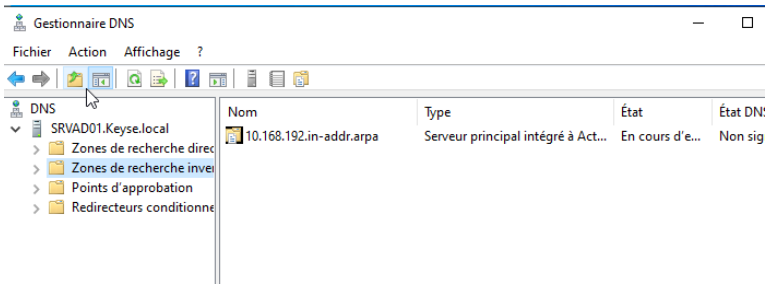


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

6 Utilisateurs :

Pour ce qui est de la création des utilisateurs dans l'AD, aller dans **Outils** puis **Utilisateurs et ordinateurs Active Directory**.

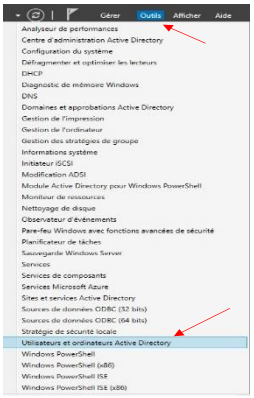


Figure 44 : Active Directory / Utilisateurs et ordinateurs

Voici ma liste d'utilisateur que je vais créer :

Prénom	***Nom***	***Groupe***	***Mot de passe***
Brice	Wilems	Formateurs	Yh! D0kNYsxHkO"mEaq.W
Jean	maltra	Formateurs	%'f1@Nqr1If+PgMj!DSw
Mathilde	Brunier	Administratif	Keh=e'lxl":~J60nR&#I
Anna	Delfort	Administratif	W+A3hCKe@mGvce9S!p$d
Nicolas	Benothmane	Elèves	77pk#57u:rJk4gdj~jpx
Claire	Malfra	Elèves	%'f1@N7eydHisjk
Marilou	Autain	Elèves	Gvce9SeW+A3hCKe
Marion	Marti	Elèves	W+A3hCfye4zTudh
Patrick	Lavier	Elèves	D0kNYsxHkO"mEaqedd78K
Malak	Angelle	Elèves	Gvce9SeW+A7fUshey
Magali	Lafros	Elèves	Gvce9SeEyhdiy595
Marie	Dupont	Elèves	@mGvce9SedghuY42edD

Pour leurs créations, dirigez-vous dans la rubrique **Users** puis faire un clic droit, **Nouveau** et enfin **Utilisateur**.

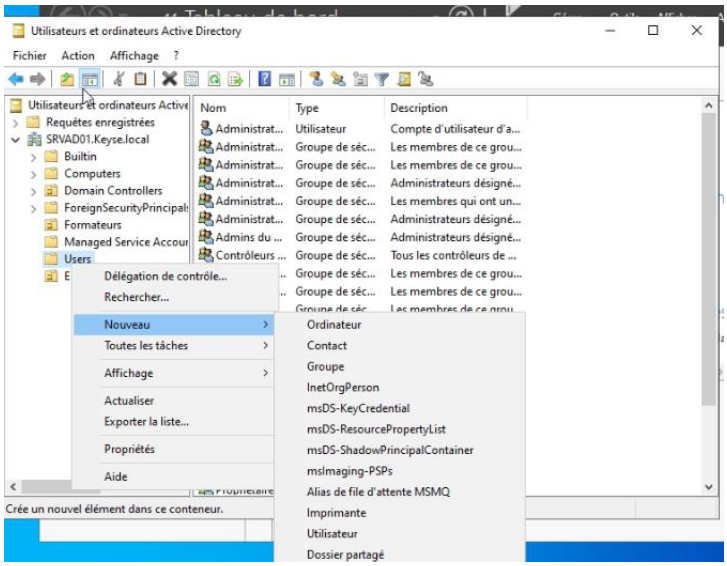


Figure 45 : Active Directory / création des utilisateurs

Voici un exemple de création pour le premier utilisateur, prénom, nom, nom d'utilisateur et mot de passe :

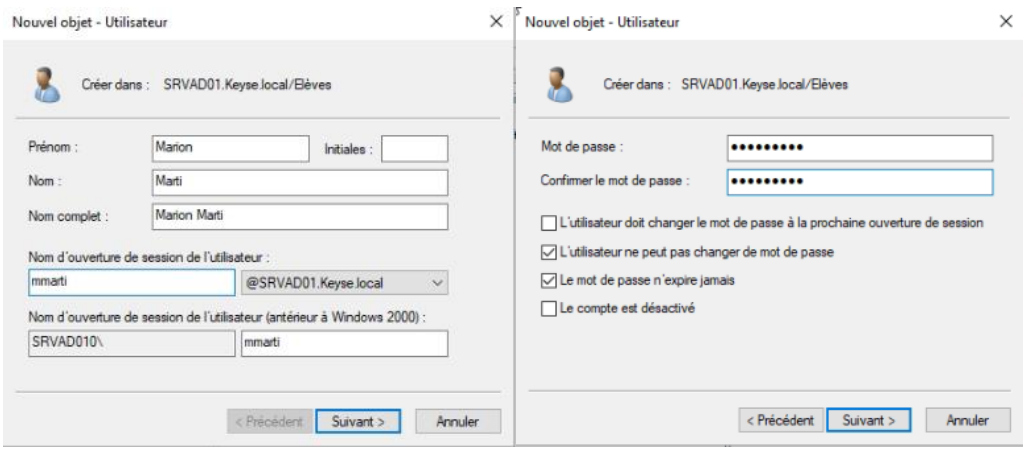


Figure 46 : Active Directory / création utilisateur Marion *Figure 47 : Active Directory / création utilisateur MDP*

Faire exactement la même manipulation pour les autres utilisateurs, je vais également créer des unités d'organisation et des groupes pour mieux les infogérer.

D'abord l'unité d'organisation, comme sur la capture d'écran, faite un clic droit, **nouveau** puis **unité d'organisation**.

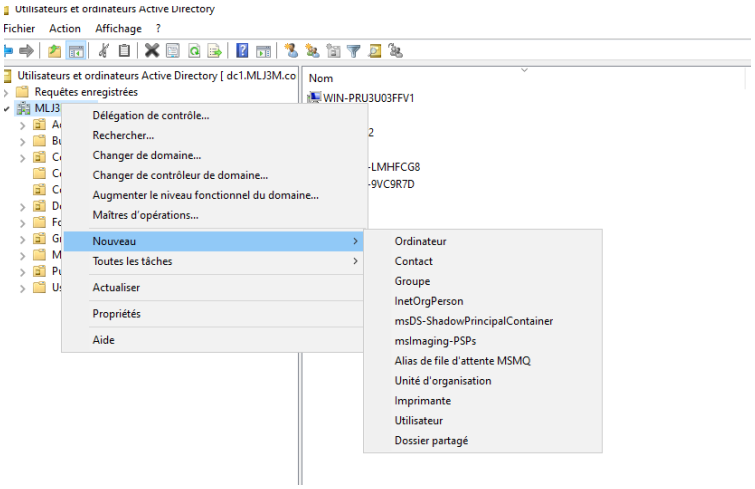


Figure 48 : Active Directory / création unité d'organisation

Nous créerons les UO « Elèves », « Formateurs » et enfin « Administratif »

Maintenant pour la création des groupes, faite aussi **clic droit** puis **Groupe**. Nous allons en créer trois

Groupe 1 : Formateurs/ **Groupe 2 :** Administratif/ **Groupe 3 :** Elèves

Puis enfin déplacer les utilisateurs dans les groupes que vous souhaitez :

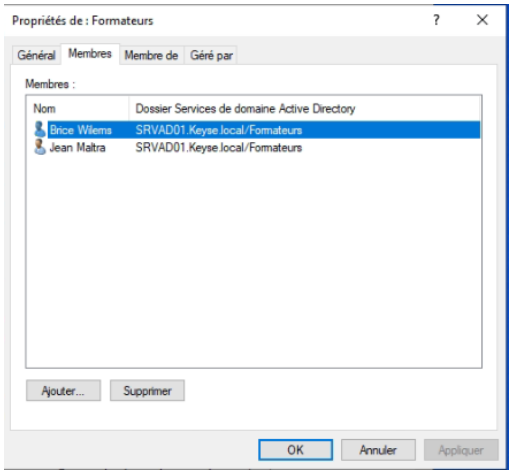


Figure 49 : Active Directory / Groupe Formateurs avec utilisateurs

Figure 50 : Active Directory / Groupe Administratif

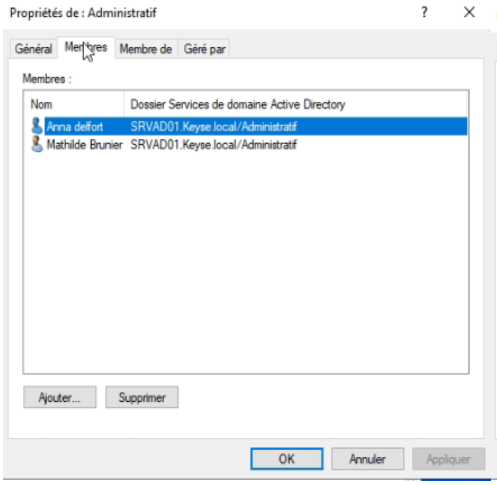
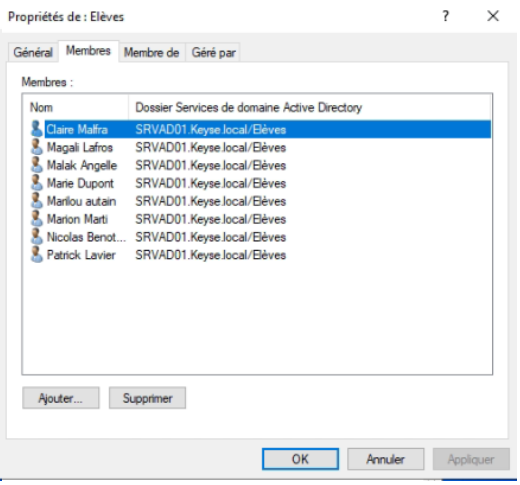


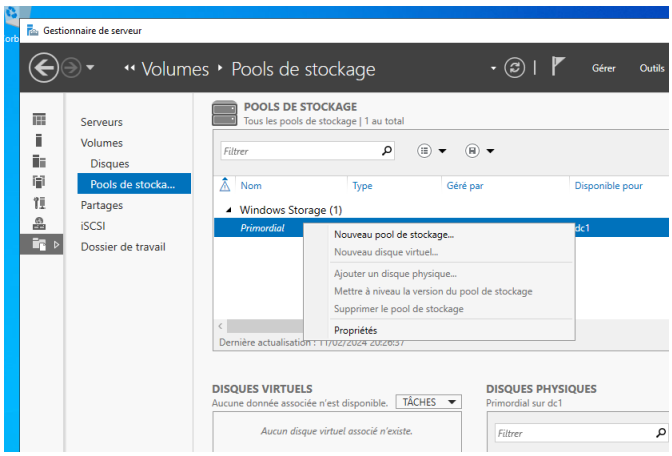
Figure 51 : Active Directory / Groupe Elèves



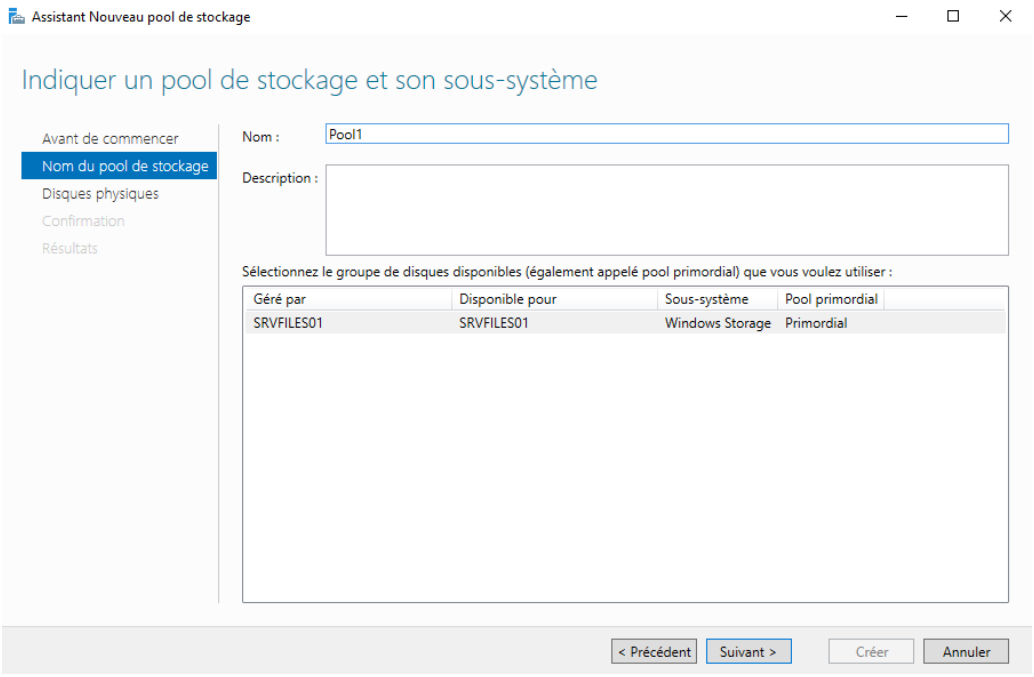
7 *Serveur de fichiers :*

À la suite d'une installation d'un Windows Serveur 2022 sur un serveur,
avec dessus un disque monter de 400Go.
Nous allons maintenant configurer notre serveur de fichier.

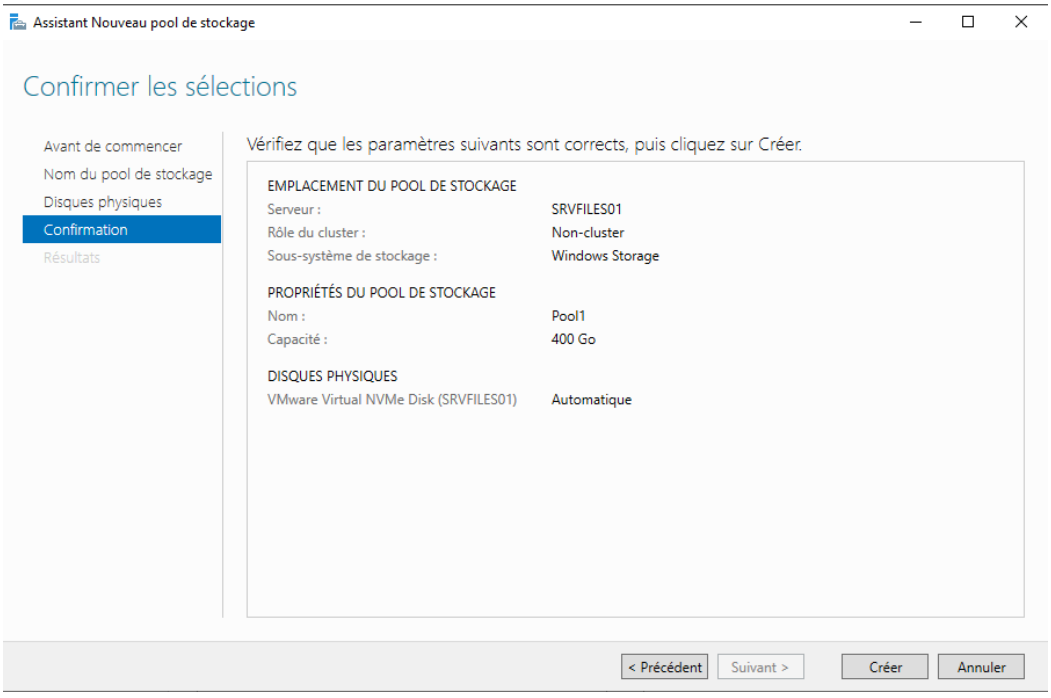
Un serveur de fichiers permet de partager des données à travers un réseau. Le terme désigne souvent l'ordinateur hébergeant le service applicatif.
Création d'un nouveau pool de stockage :



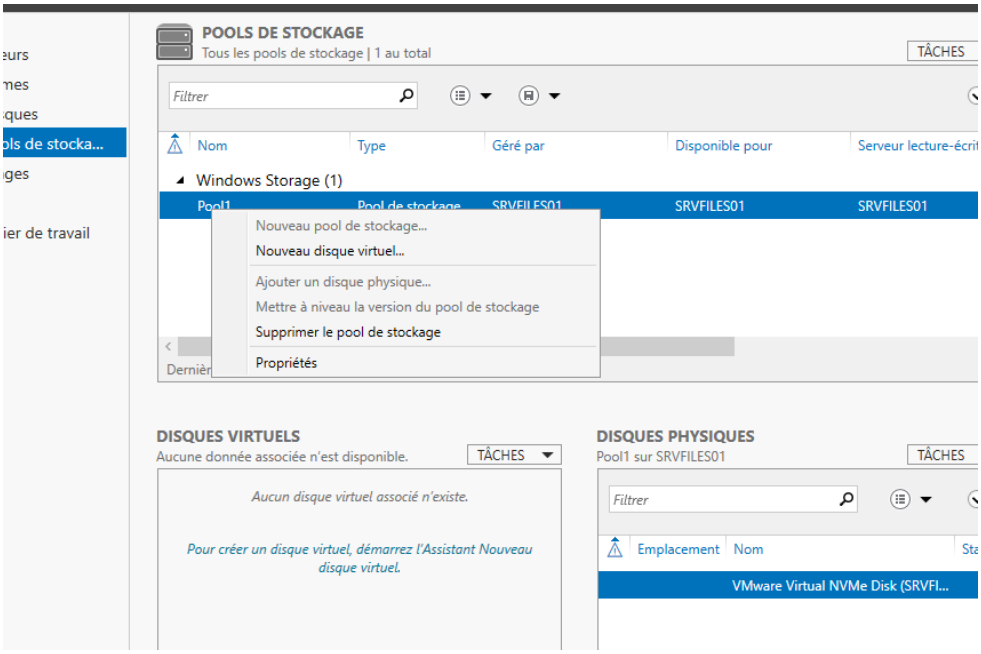
Nommage du Pool de stockage :



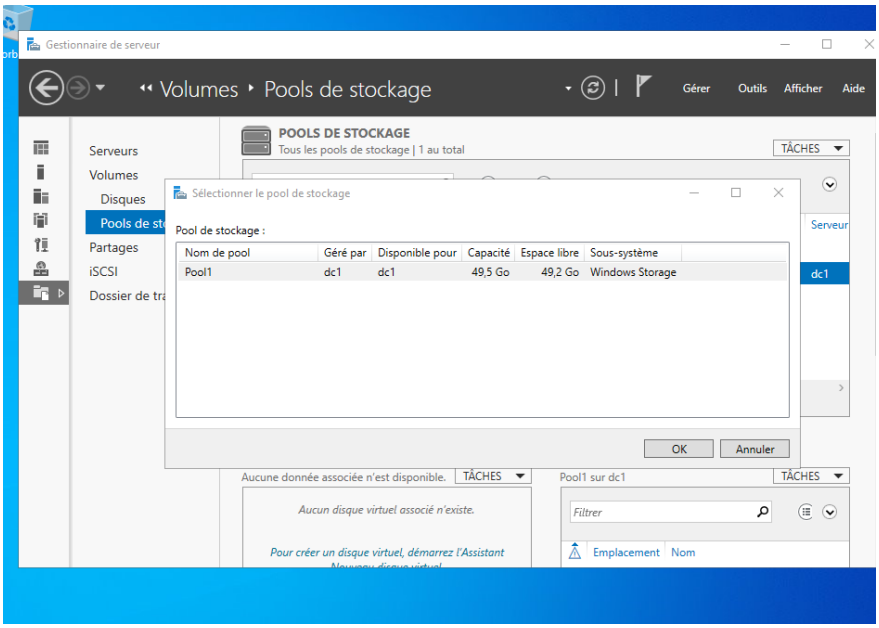
Confirmation des différentes configurations :



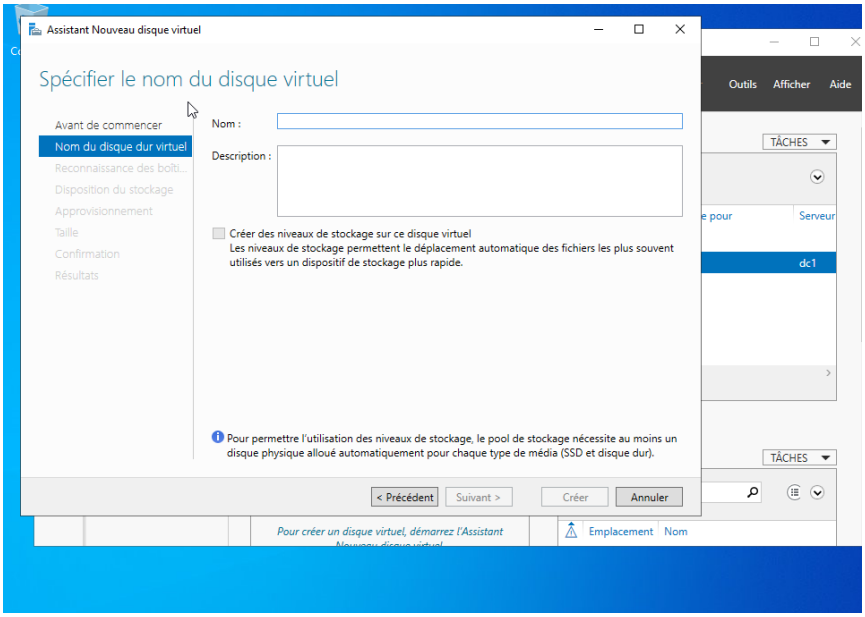
Création d’un nouveau disque virtuel :



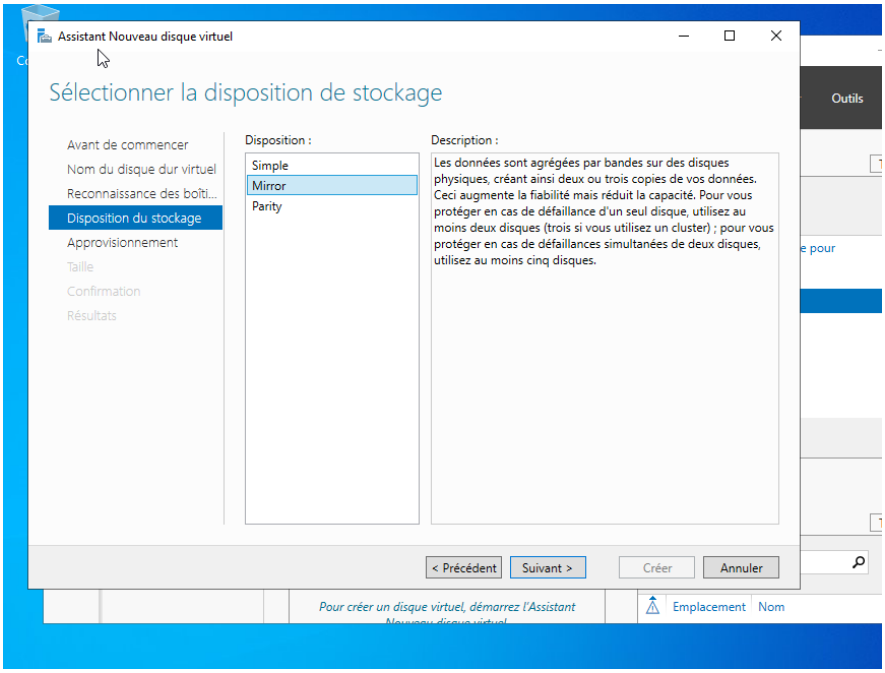
Sélection du Pool de stockage :



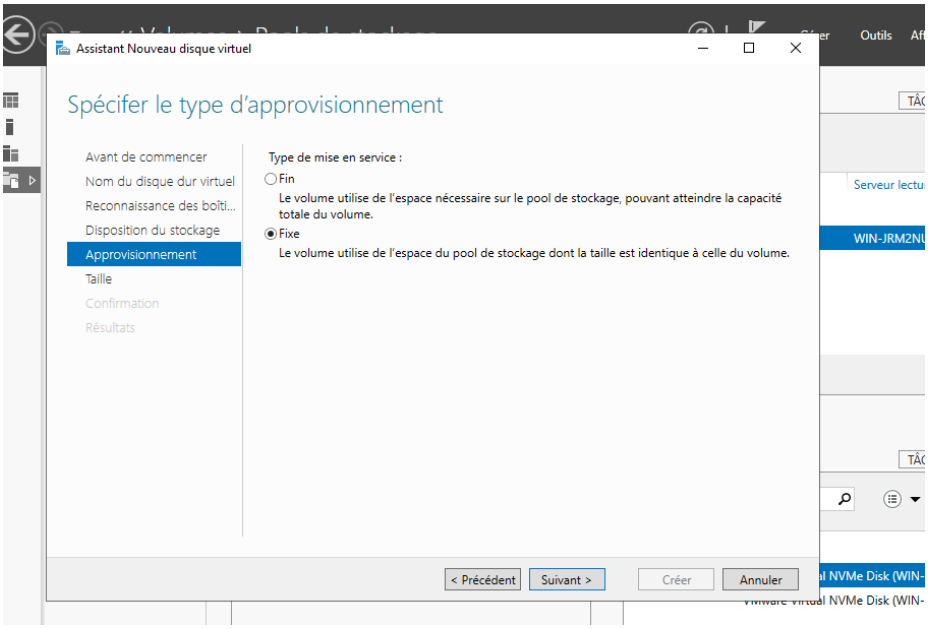
Nommage du disque virtuel :



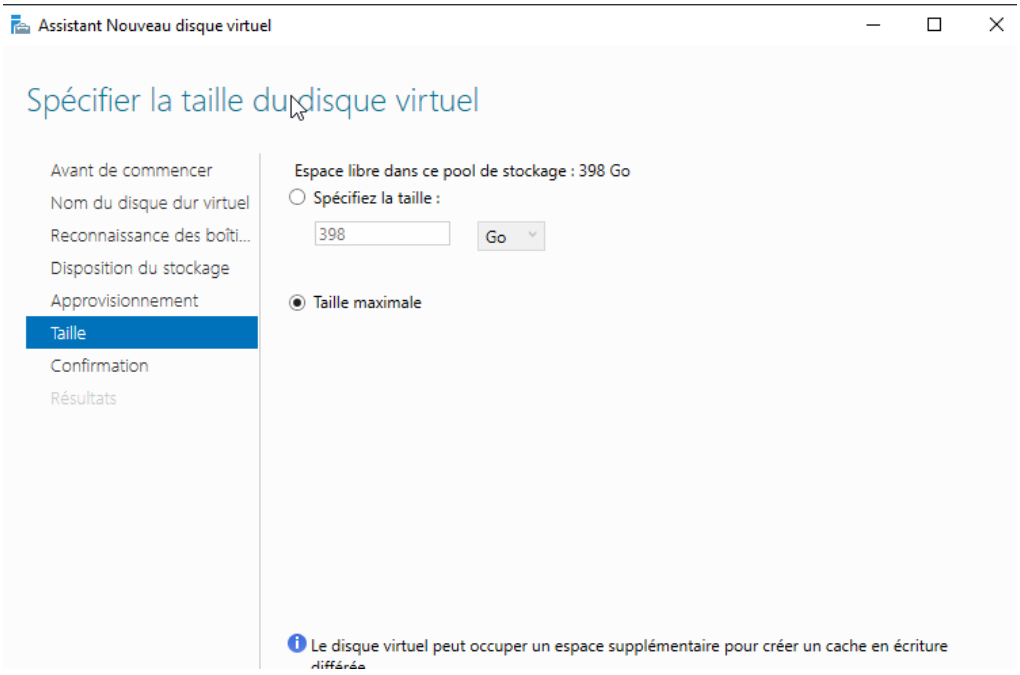
Sélection de la disposition de stockage :



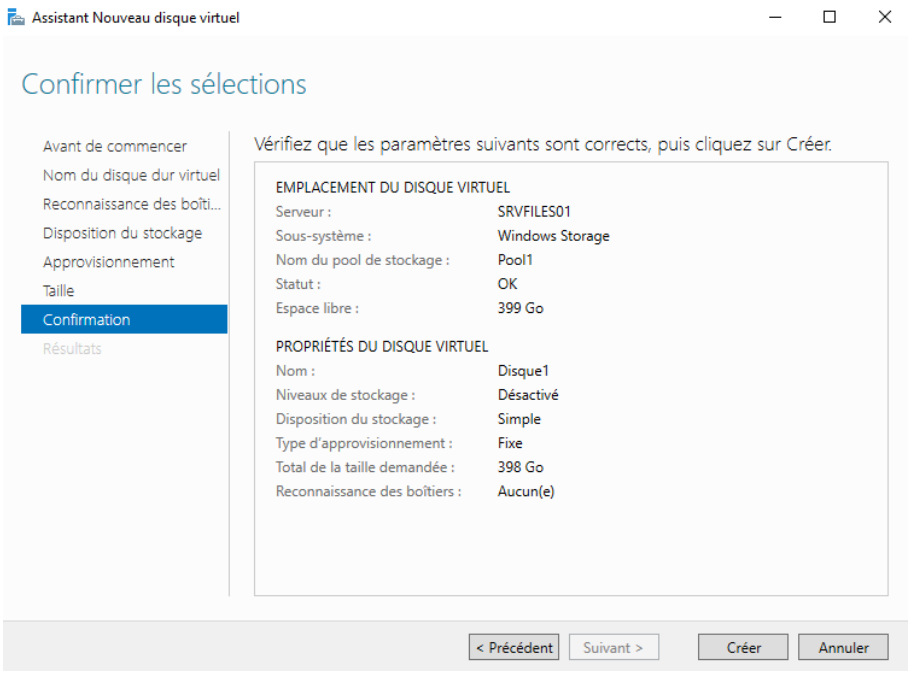
Sélection du type d'approvisionnement :



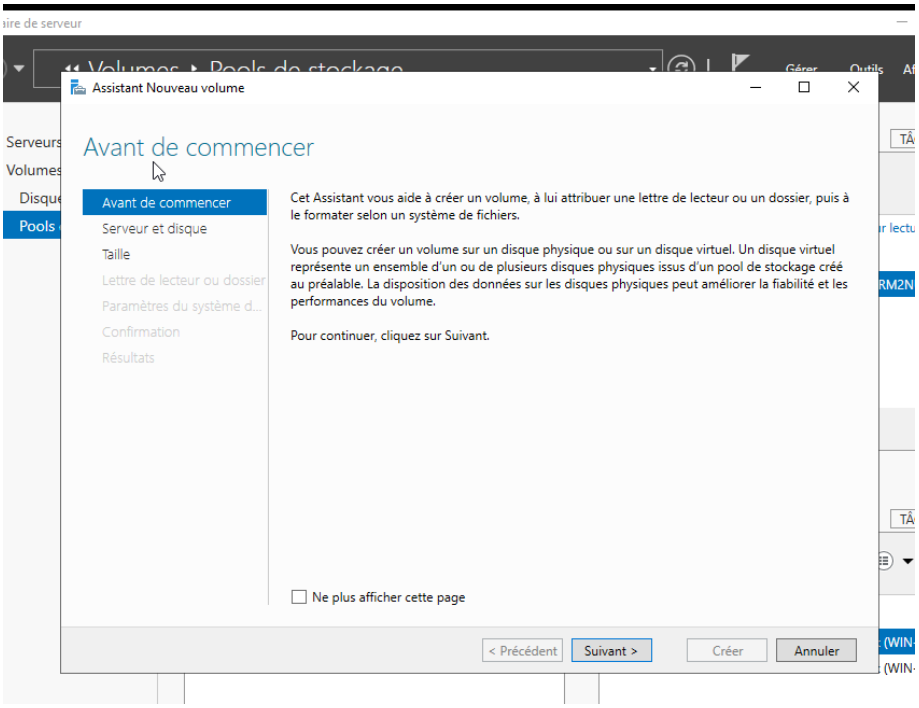
Sélection de la taille du disque virtuel :



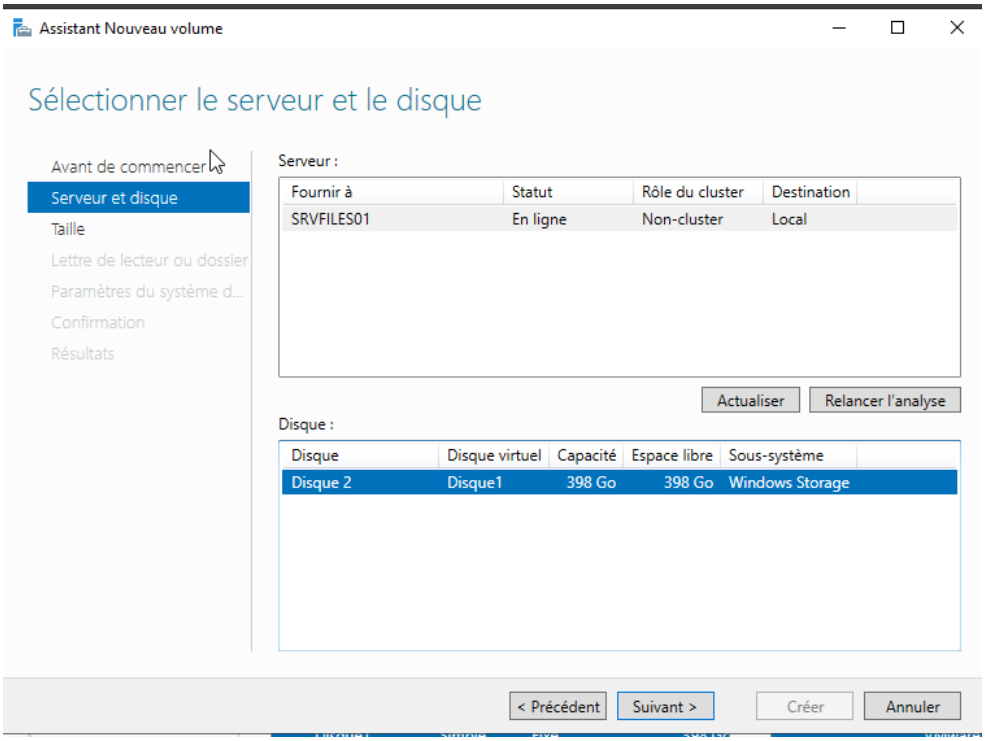
Confirmations des différentes configurations :



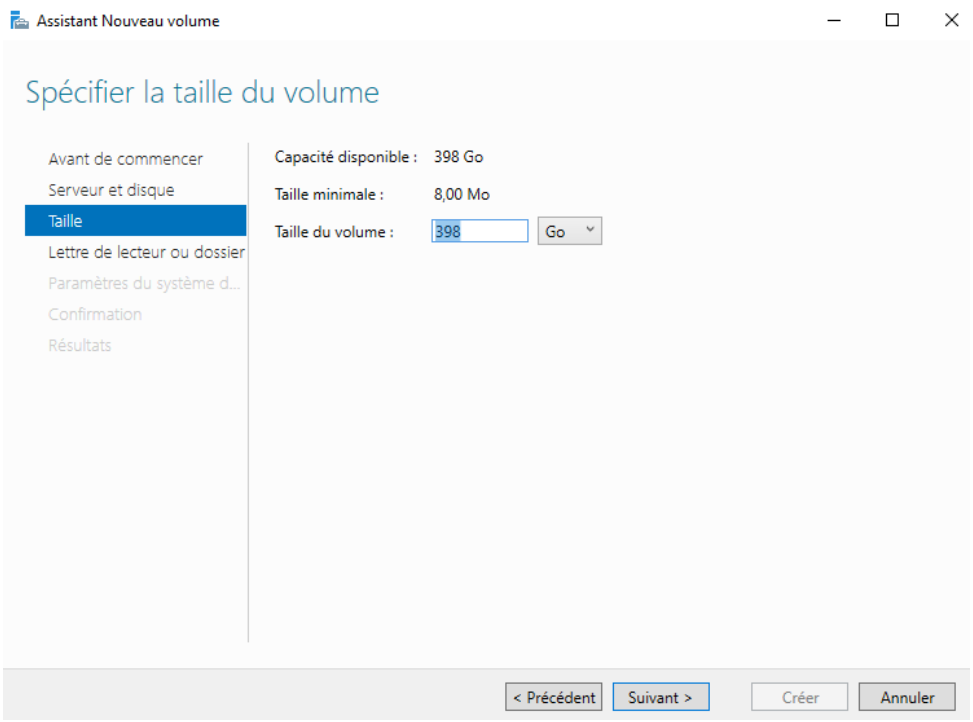
Création d'un nouveau volume :



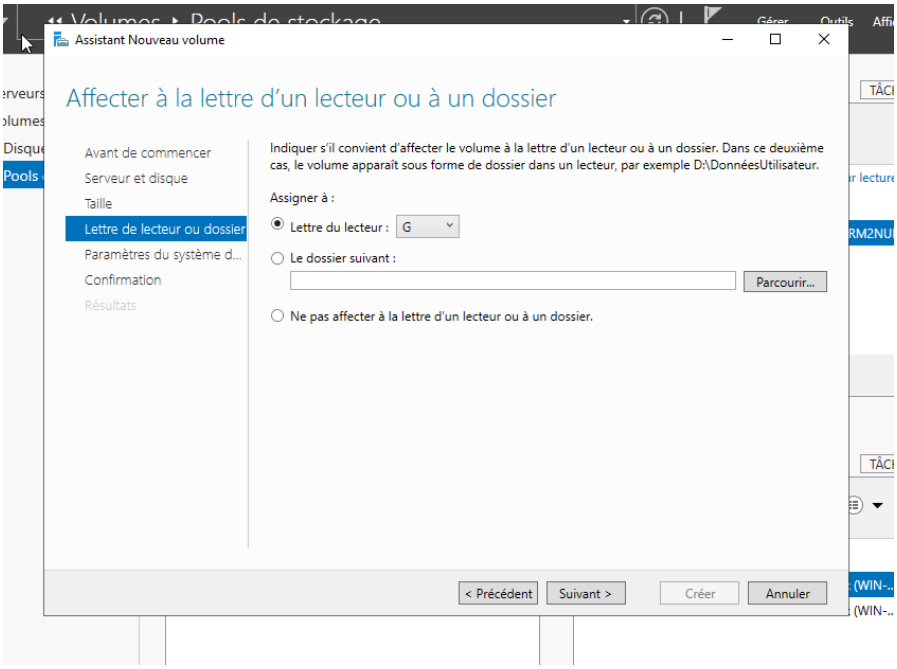
Sélection du serveur et du disque :



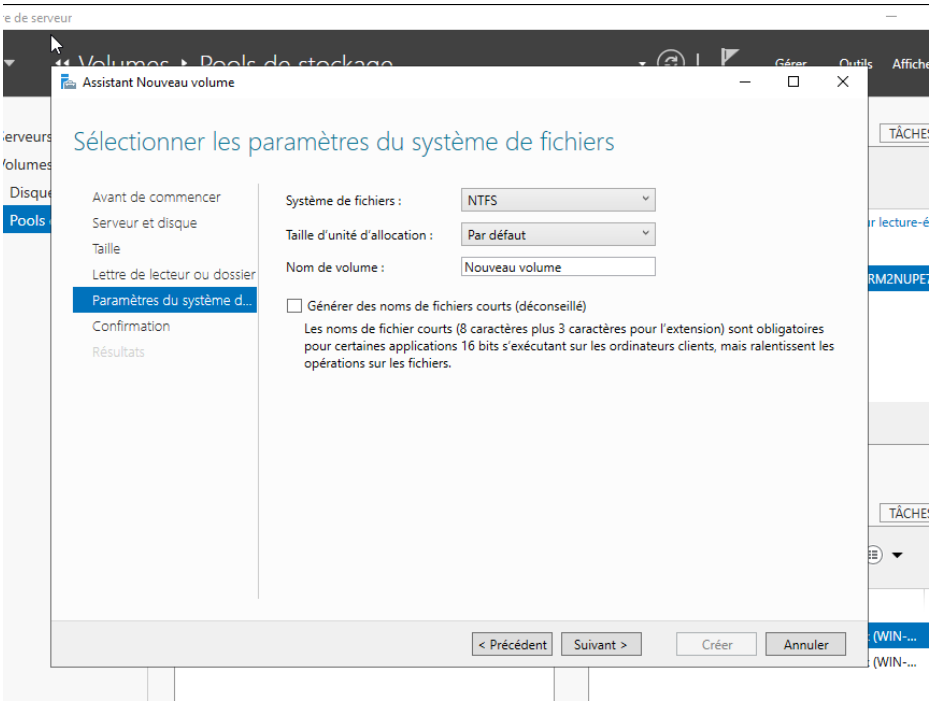
Sélection du la taille du volume :



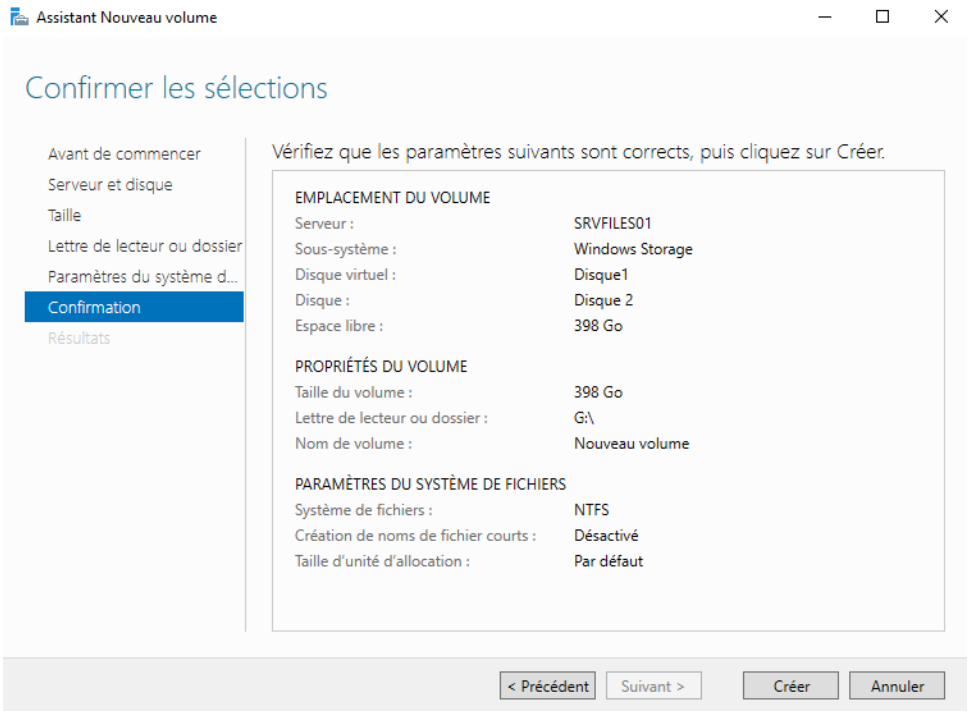
Affectation de la lettre du lecteur :



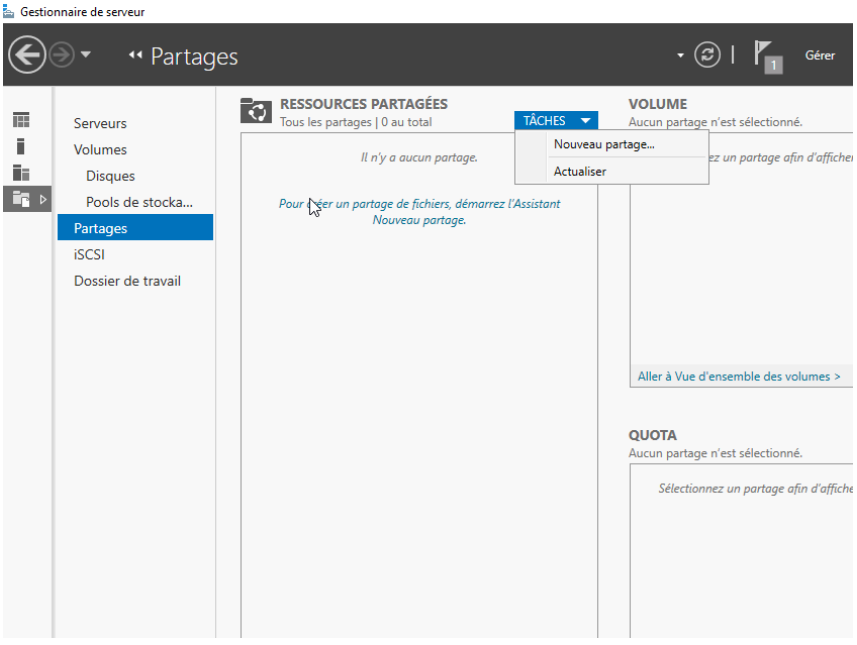
Sélection des paramètres du système de fichier :



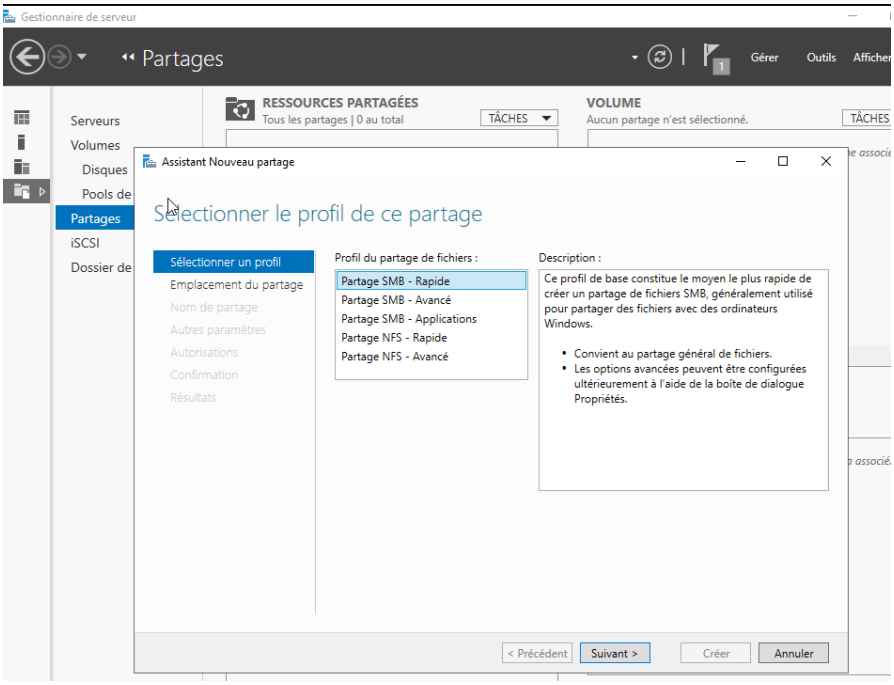
Confirmer différentes les configurations :



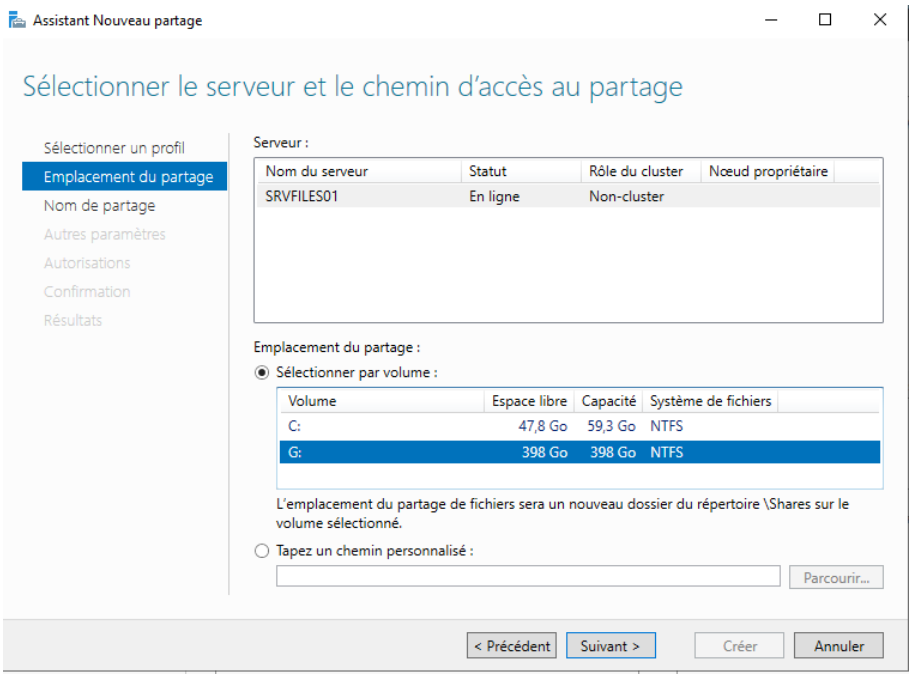
Création d'un nouveau partage :



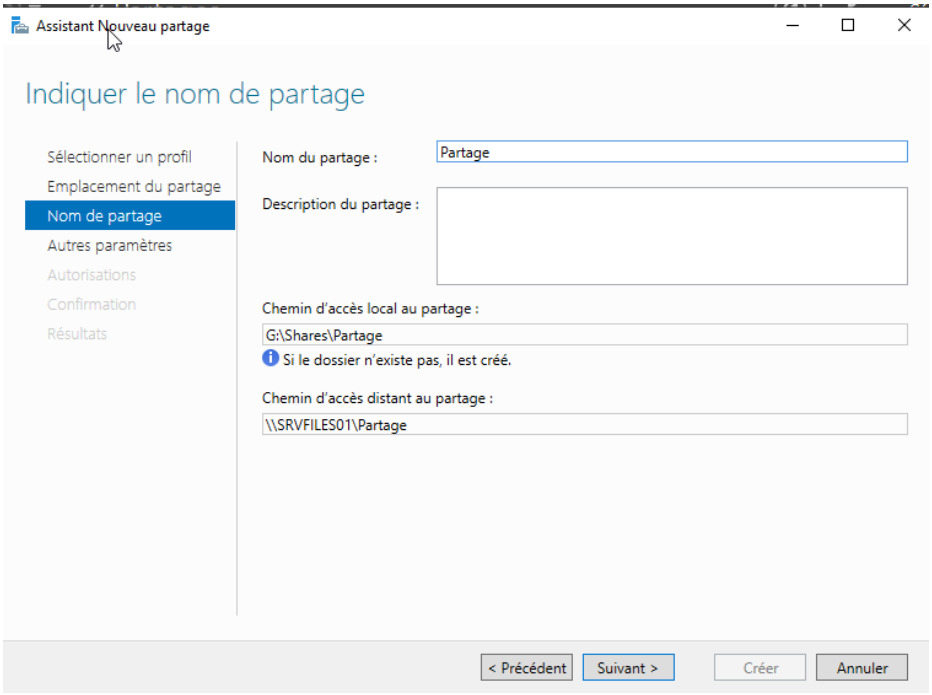
Sélection du profil de ce partage :



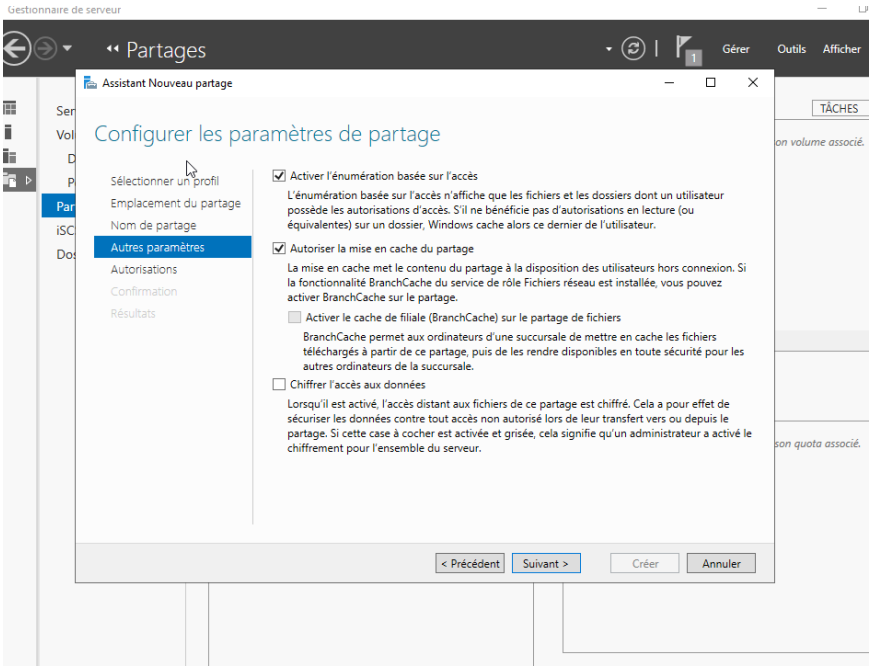
Sélectionner le serveur et le chemin d'accès au partage :



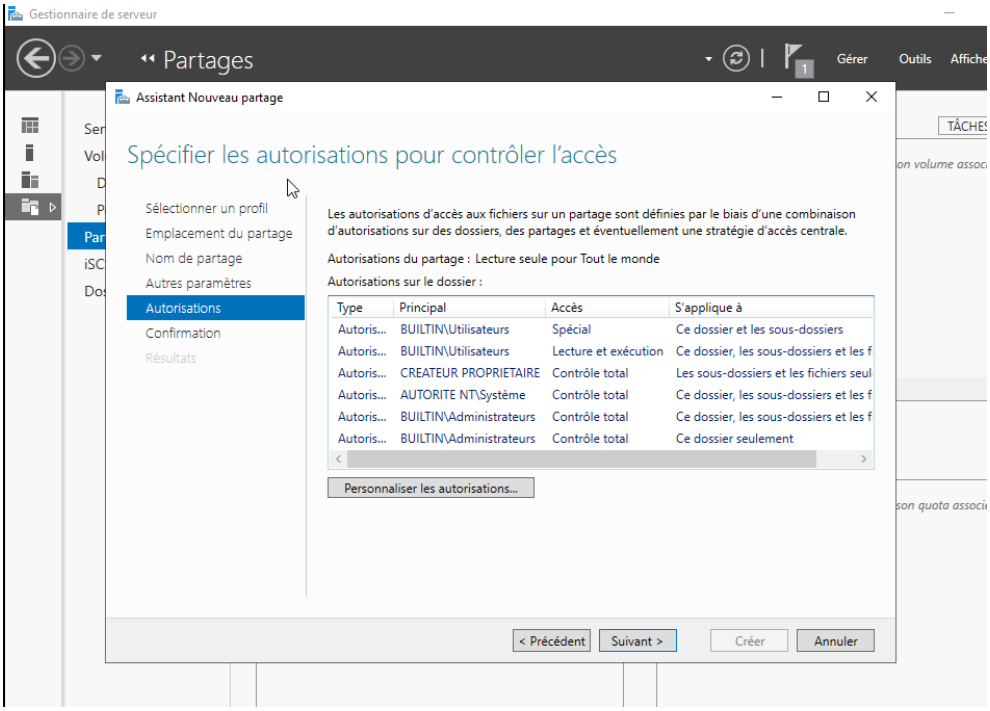
Indiquer le nom du partage :



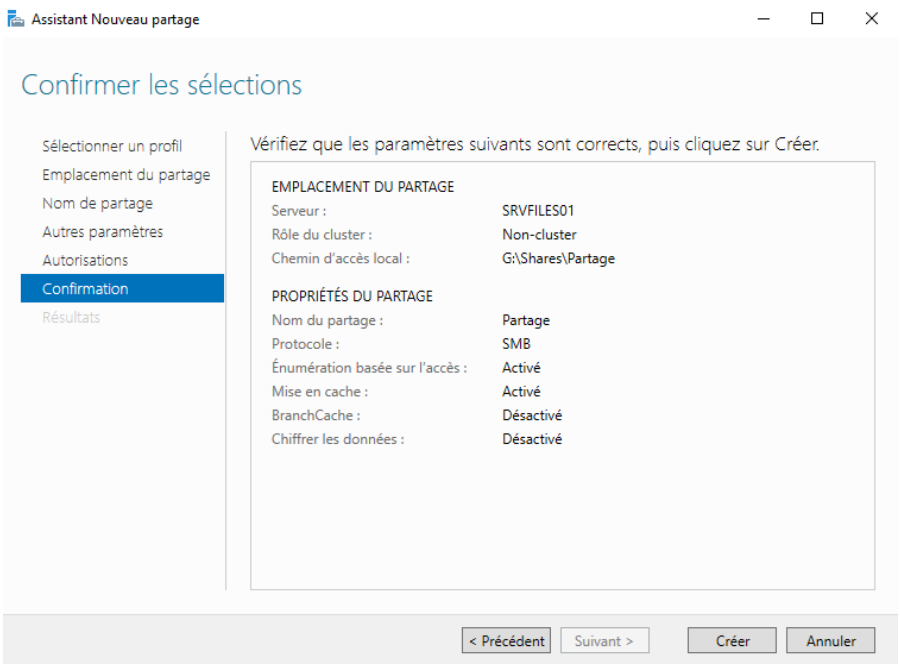
Configurer les paramètres de partage :



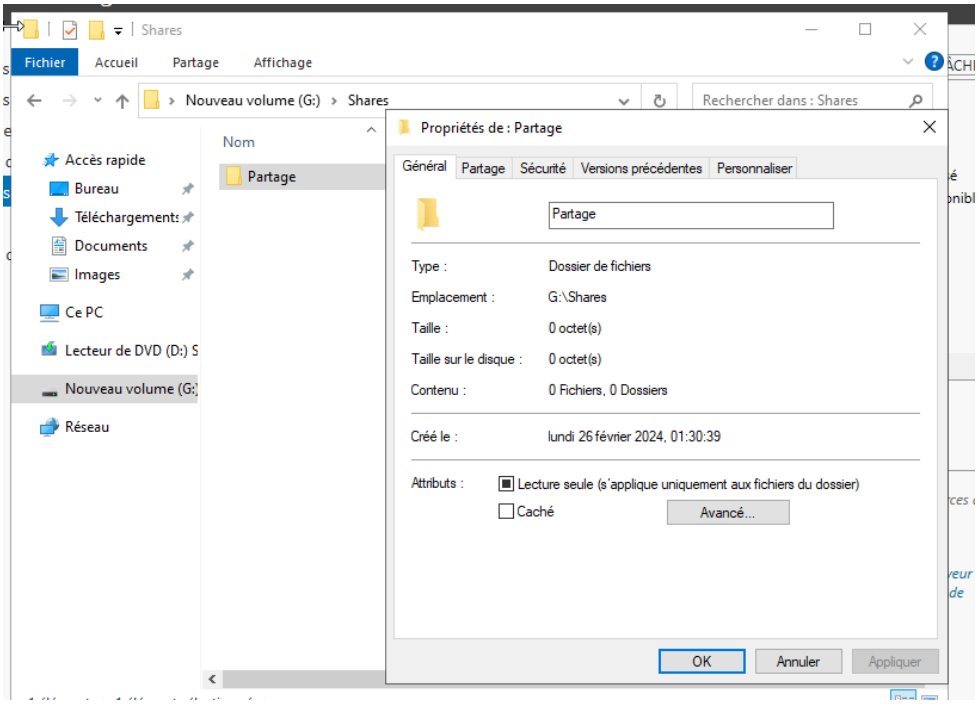
Spécification des autorisations pour contrôler l'accès :



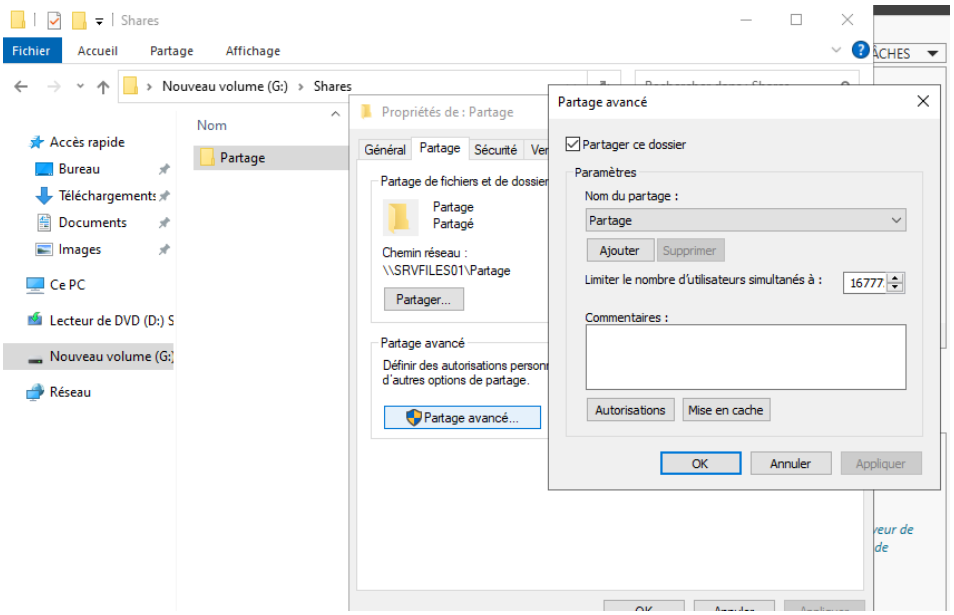
Confirmer les différentes configurations :



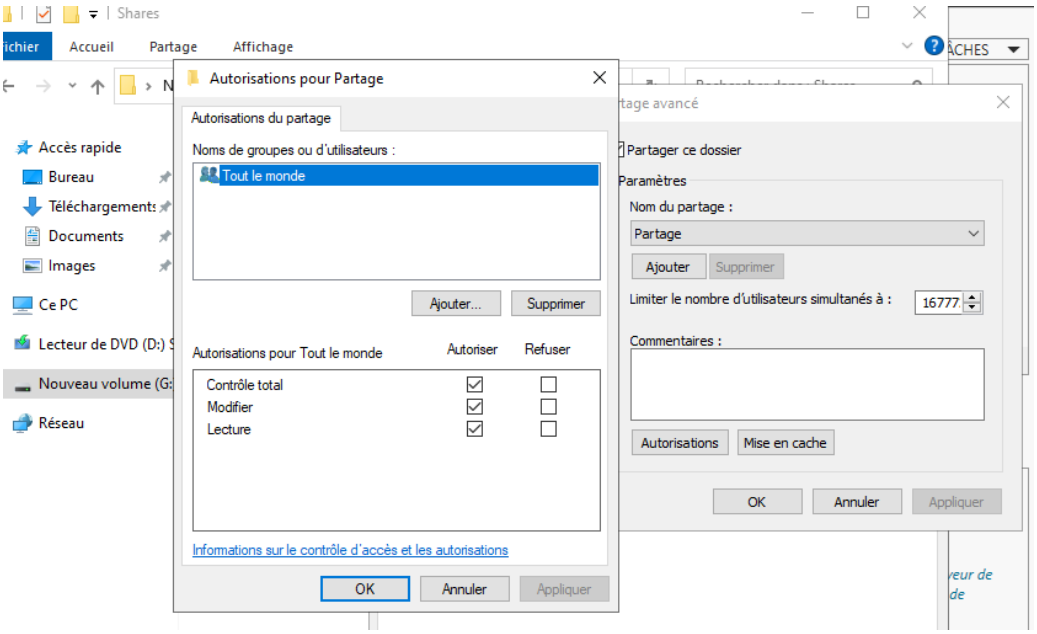
Propriétés du partage créé :



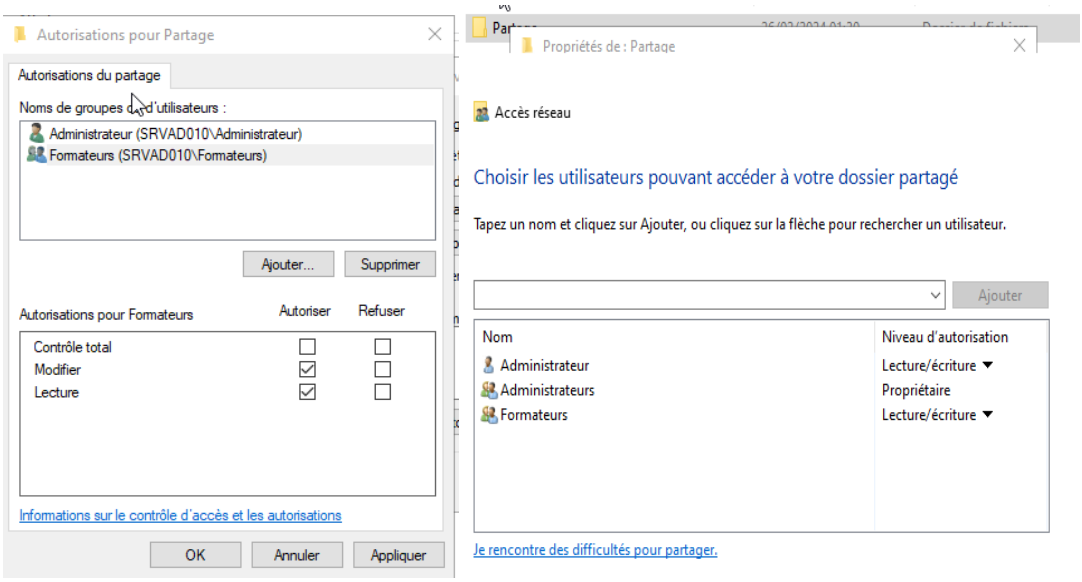
Paramétrage de partage avancé sur le partage créé :



Sélections des différentes autorisations sur ce partage :



Sélection du groupe « formateurs » avec les droits de modification :



8 GPO :

La stratégie de groupe, permet d'avoir une configuration homogène entre les différentes machines du votre parc informatique, mais aussi au niveau de l'environnement utilisateur.

En effet, une stratégie de groupe peut servir à appliquer des paramètres sur Windows en lui-même, mais aussi à l'utilisateur directement (à son environnement, sa session), ou les deux.

Chaque stratégie dispose de ses propres paramètres, définis par l'administrateur système, et qui seront appliqués ensuite à des postes de travail, des serveurs ou des utilisateurs.

Voici les différentes GPO que je vais utiliser :

-Mappage d'un lecteur réseau personnelle pour **chaque utilisateur du groupe Formateurs**

Figure 62 : GPO /Mappage d'un lecteur réseau d'un espace personnel pour chaque Utilisateurs du groupe Conseiller

Nous recréerons une GPO de la même façon : « crée un objet GPO dans ce domaine, et le lier ici »
Nous nommerons notre GPO « Mappage lecteur perso Conseiller »

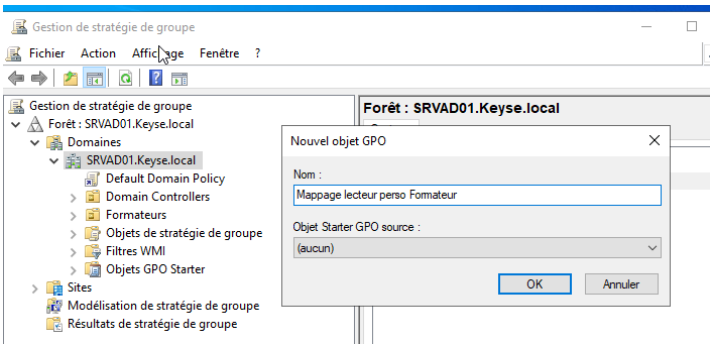


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Puis une fois dans la GPO créé, nous nous rendrons dans :
Configuration utilisateur -> Préférences -> Mappages de lecteurs
Clique droite puis Nouveau et « Lecteur mappé

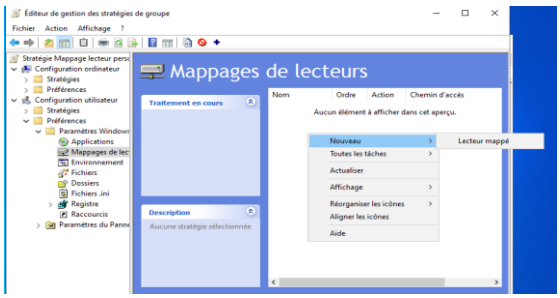


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Une fois dans le menu du lecteur mappé, nous configurerons donc l'action « Mettre à jour », L'emplacement du partage «\\srvfiles01\partage\Espace Perso$\%LongonUser%» crée au préalable, attention a bien coché la case « Reconnecter » et attribuer un nom au Lecteur et enfin, nous choisirons une lettre pour le lecteur.

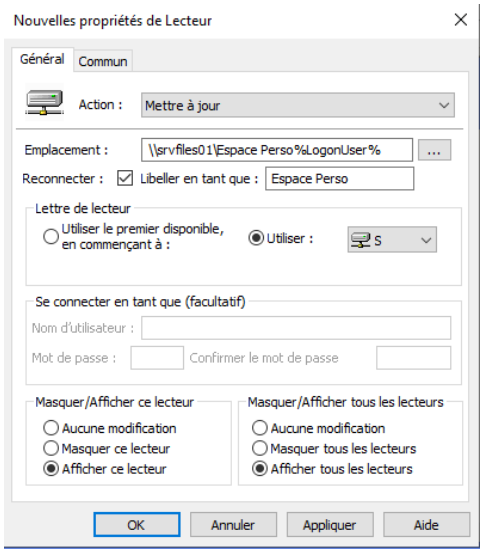


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous nous rendrons ensuite dans « commun » et nous cocherons la case « Exécuter dans le contexte de sécurité de l'utilisateur connecté » et la case « Ciblage au niveau de l'élément » afin d'attribuer cette GPO a un groupe sélectionné.

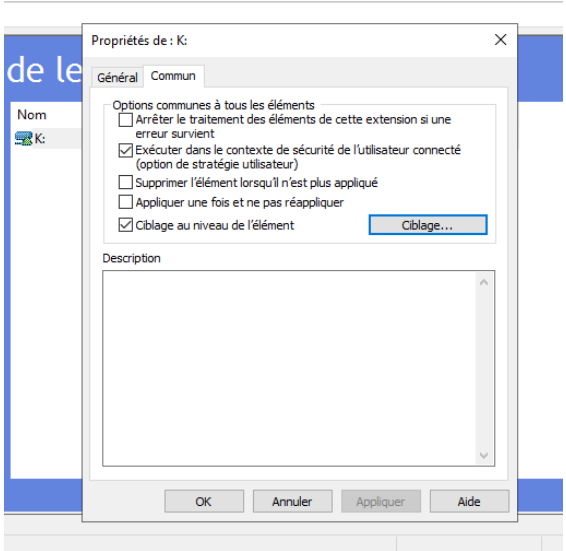


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous nous rendrons dans « Nouvel élément » puis sélectionner « Groupe de sécurité »

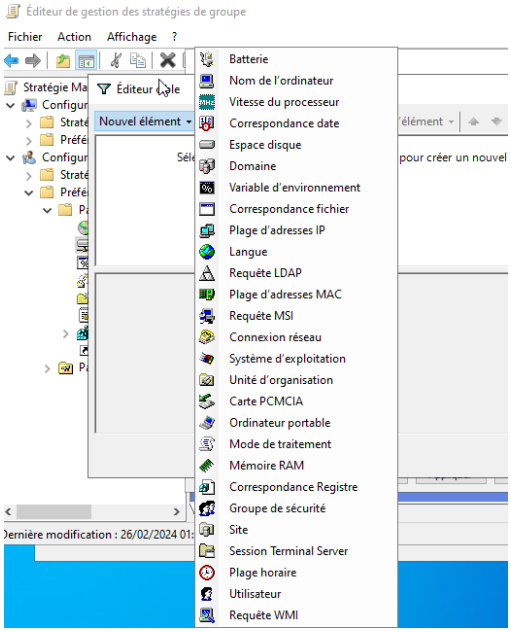


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous ajouterons notre groupe pour lequel nous souhaitons activé la GPO, puis «OK »

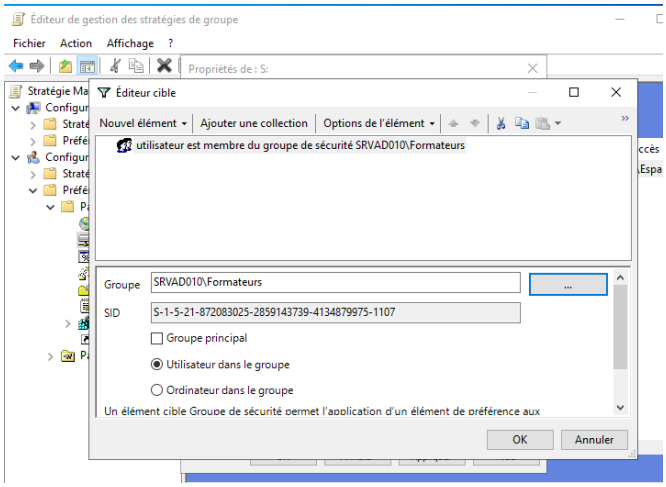


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Par la suite, nous nous rendrons dans :
Configuration utilisateur -> Préférences -> Dossier

Clique droit puis Nouveau et « Dossier »

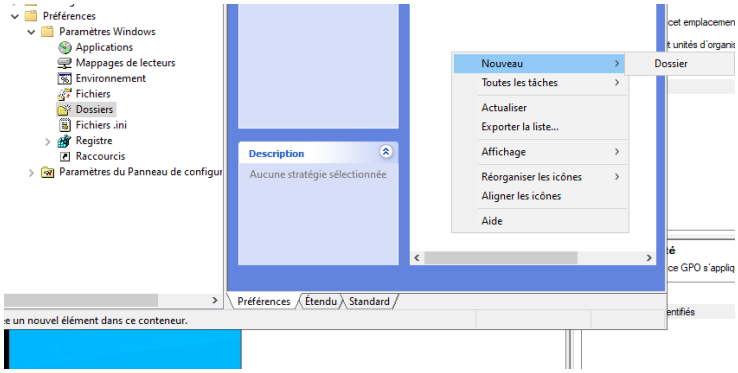


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Une fois dans le menu du Dossier, nous configurerons donc l'action « Remplacer »,
L'emplacement du partage «\\srvfiles01\partage\Espace Perso$\%LongonUser%» crée au préalable.

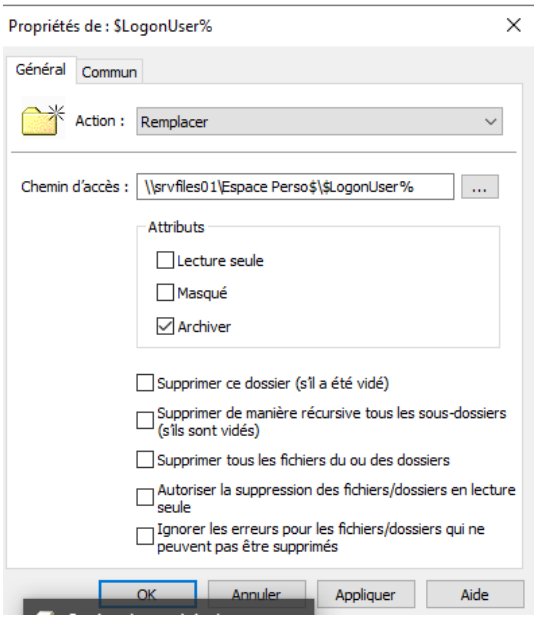


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous nous rendrons ensuite dans « commun » et nous cocherons la case « Exécuter dans le contexte de sécurité de l'utilisateur connecté » et la case « Ciblage au niveau de l'élément » afin d'attribuer cette GPO a un groupe sélectionné.

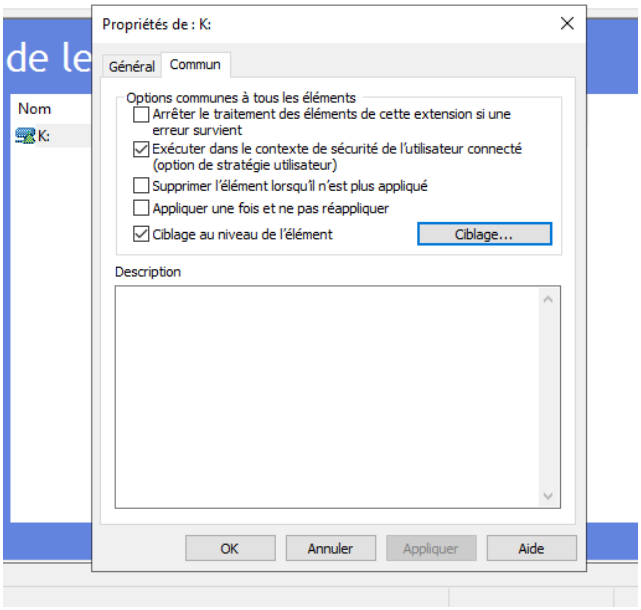


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25

Nous nous rendrons dans « Nouvel élément » puis sélectionner « Groupe de sécurité »

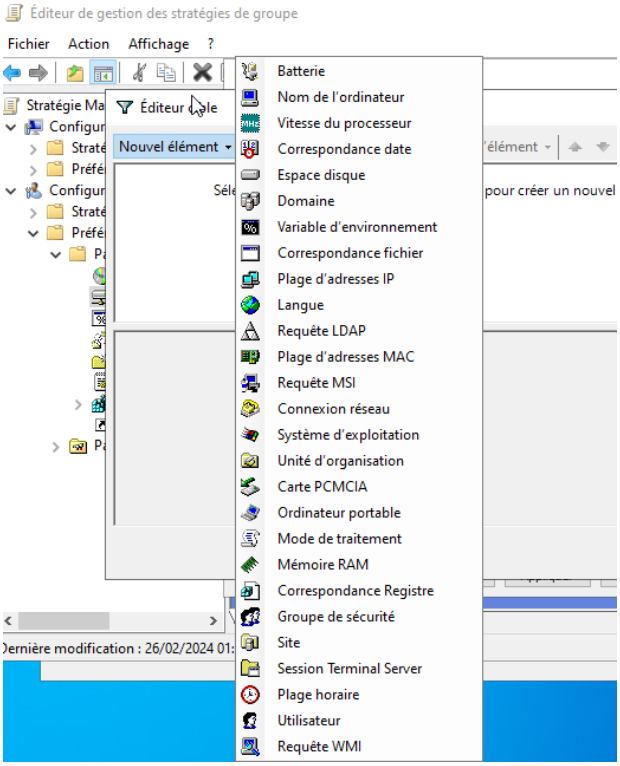


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous ajouterons notre groupe pour lequel nous souhaitons activer la GPO, puis « OK »

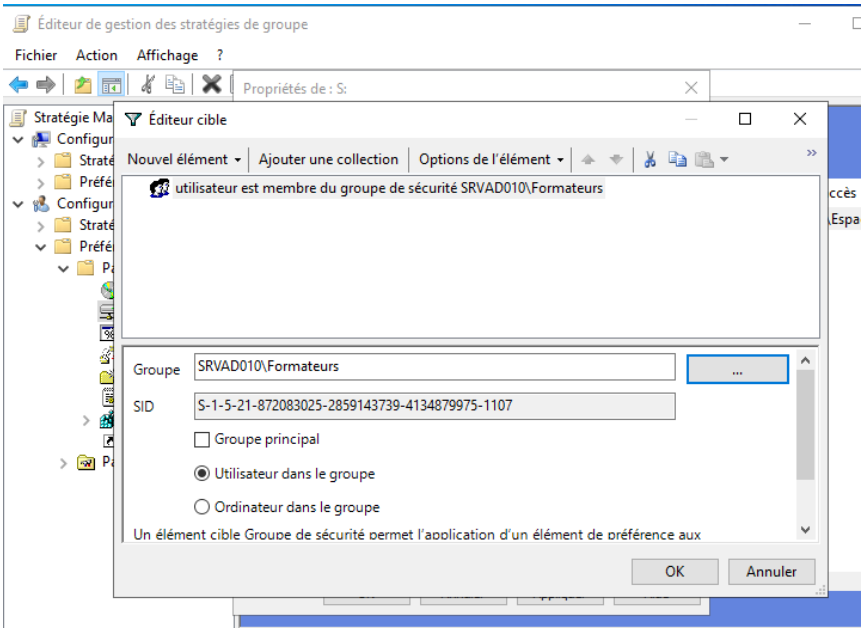


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Par la suite, nous nous rendrons dans :
Configuration utilisateur -> Préférences -> Raccourci
Clique droite puis Nouveau et « Raccourci »

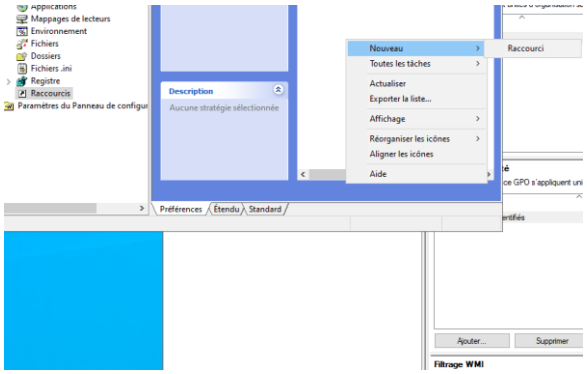


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Une fois dans le menu du Raccourci, nous configurerons donc l'action « Mettre à jour », L'emplacement du partage «\\srvfiles01\Espace Perso$\%LongonUser%» crée au préalable.

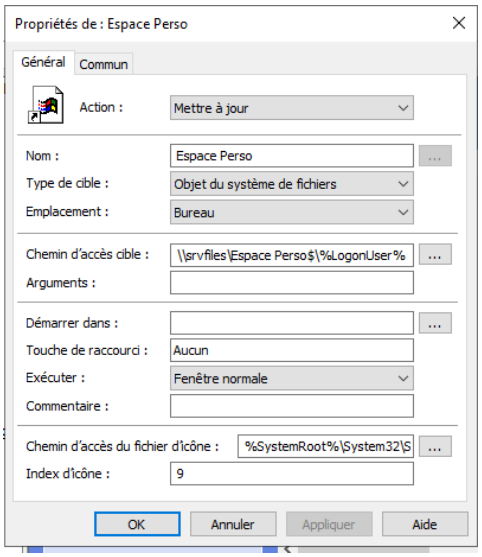


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous nous rendrons ensuite dans « commun » et nous cocherons la case « Exécuter dans le contexte de sécurité de l'utilisateur connecté » et la case « Ciblage au niveau de l'élément » afin d'attribuer cette GPO a un groupe sélectionné.

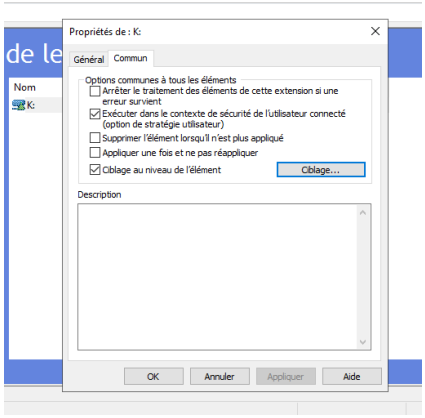


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous nous rendrons dans « Nouvel élément » puis sélectionner « Groupe de sécurité »

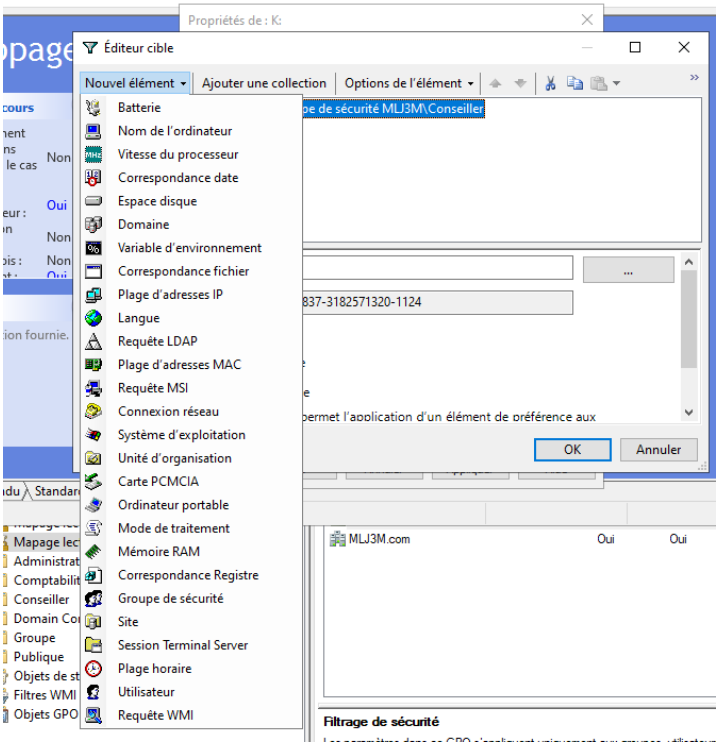


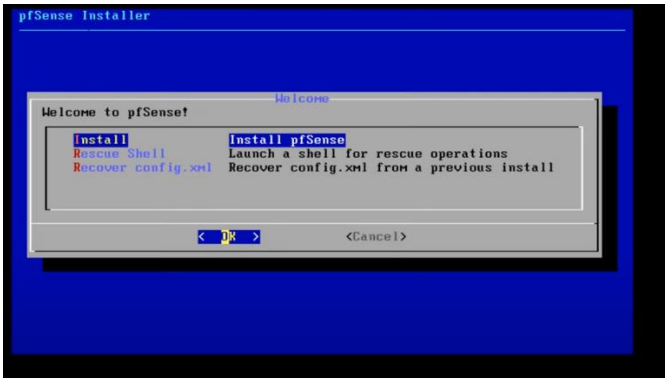
Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous ajouterons notre groupe pour lequel nous souhaitons activer la GPO, puis « OK »

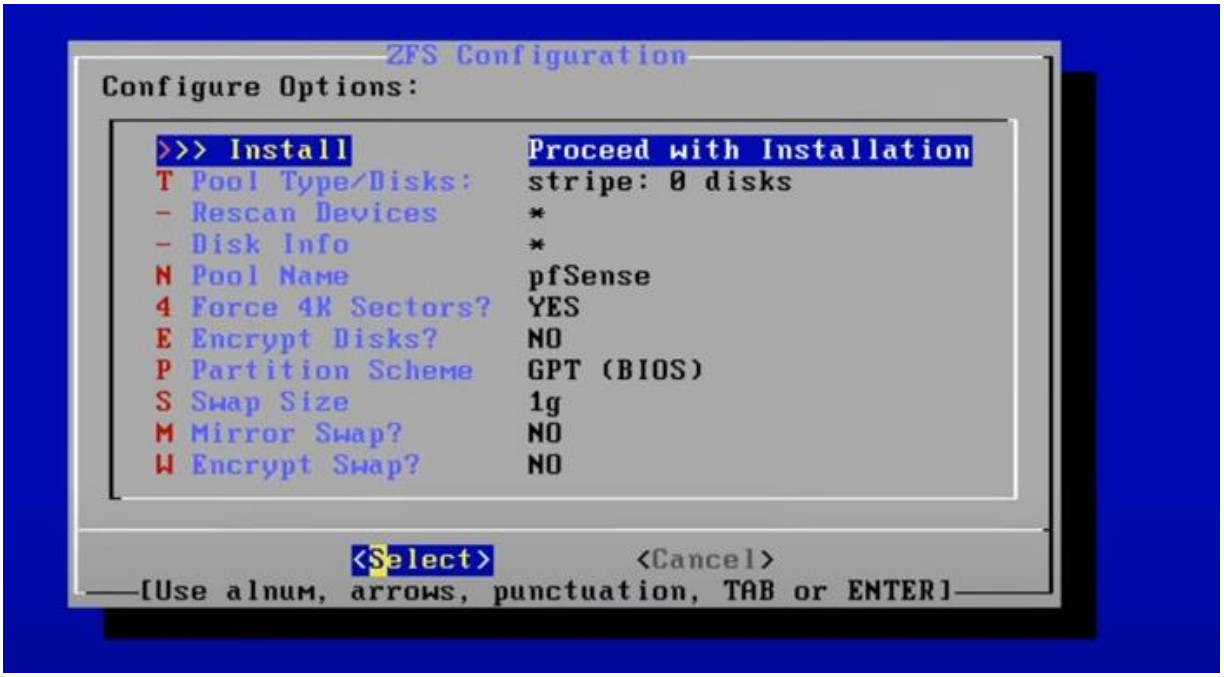
8 *Firewall PFSense :*

Installation de PFSense :

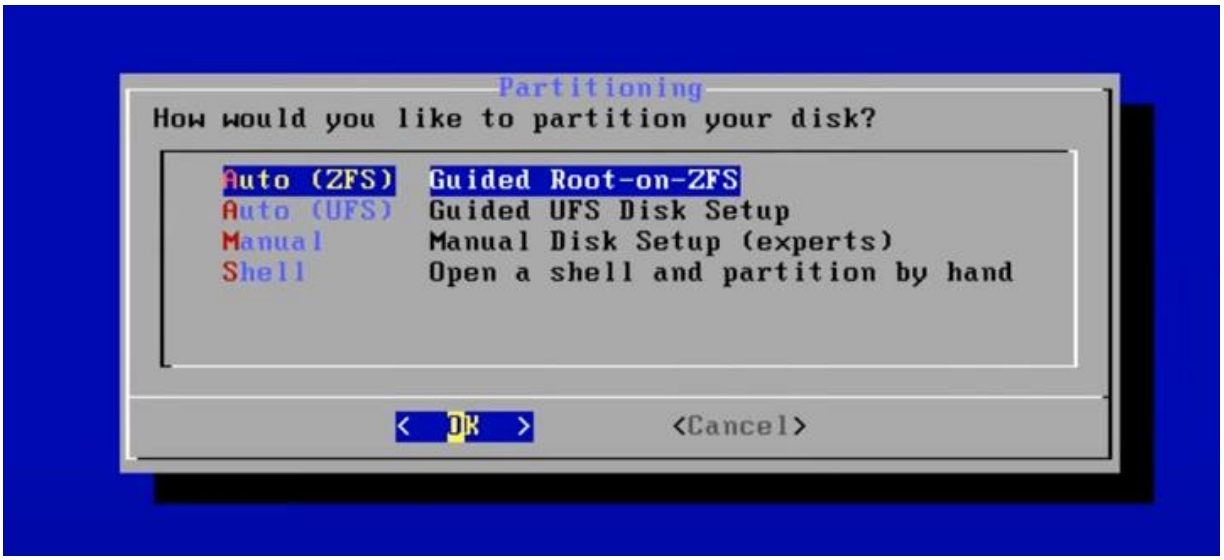
Install pfSense : **OK**



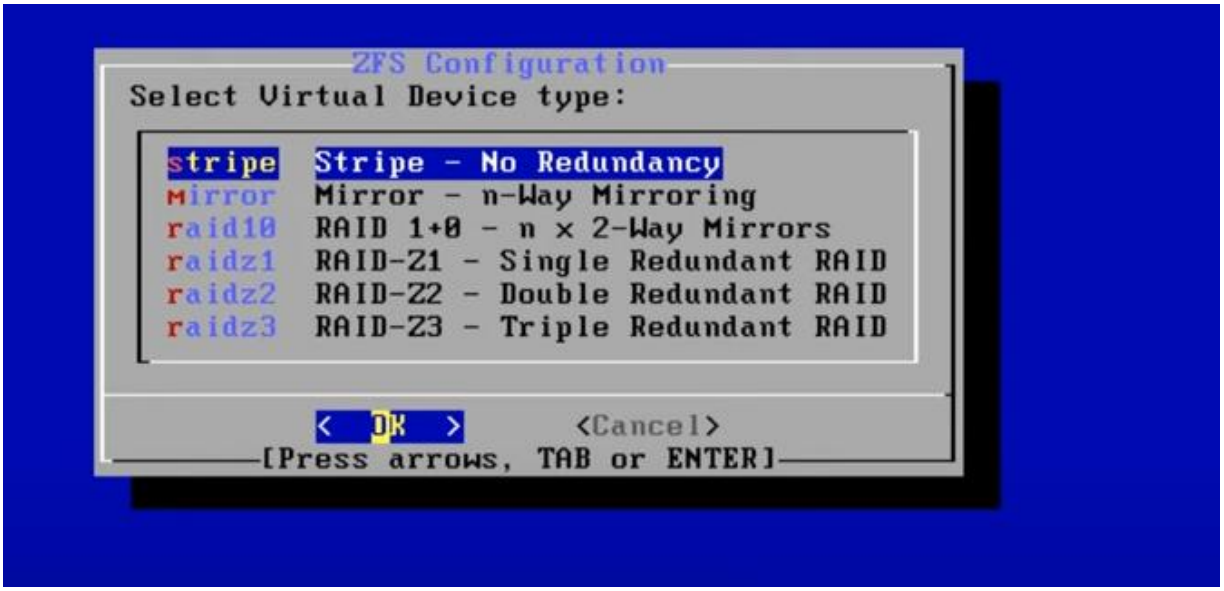
Proceed with installation : « Select »



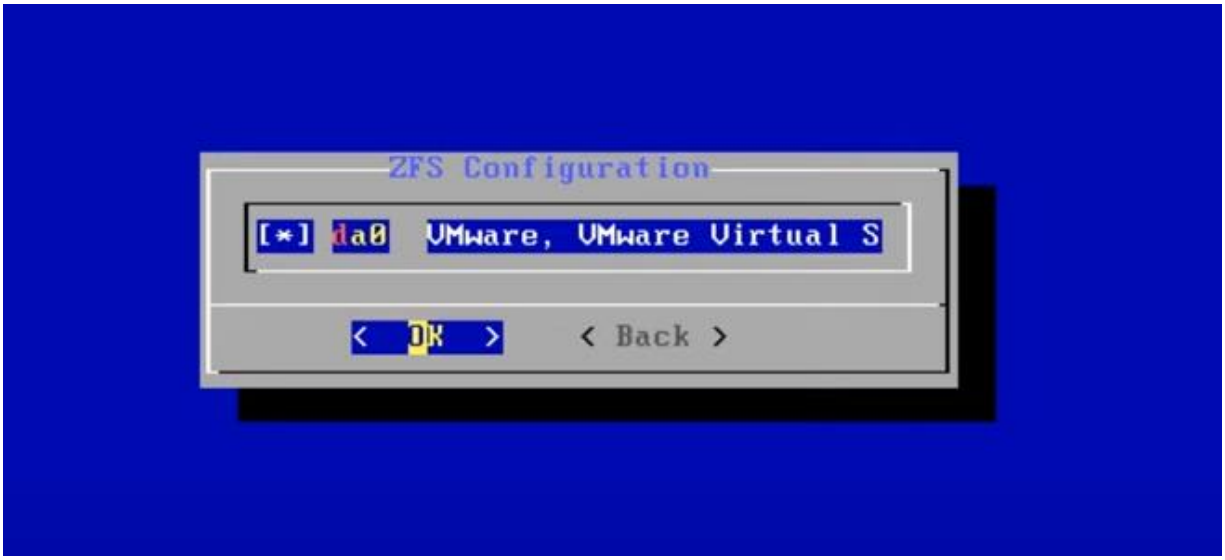
Auto (ZFS) pour pfSense version 2.6 et ultérieure ou **Auto (UFS) BIOS** pour version inferieure



Sélectionner : sans redondance

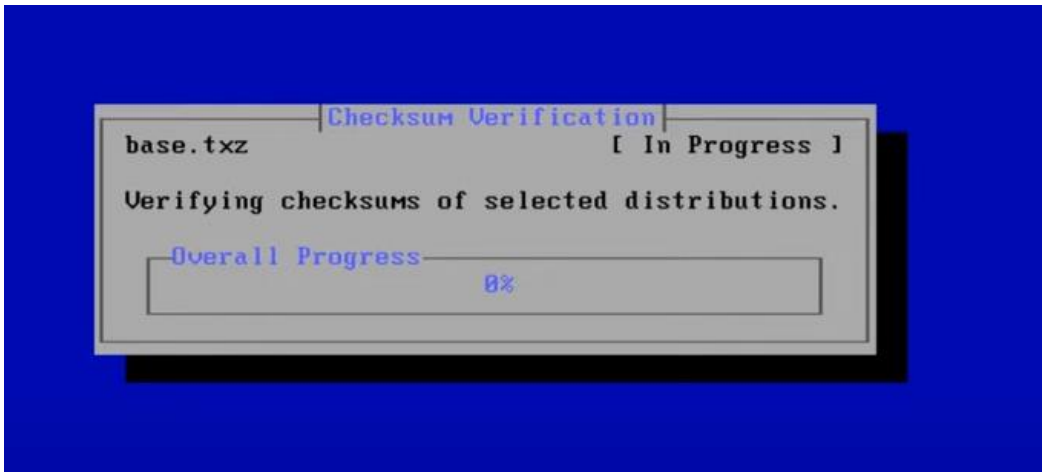


Sélectionner le disque virtuel

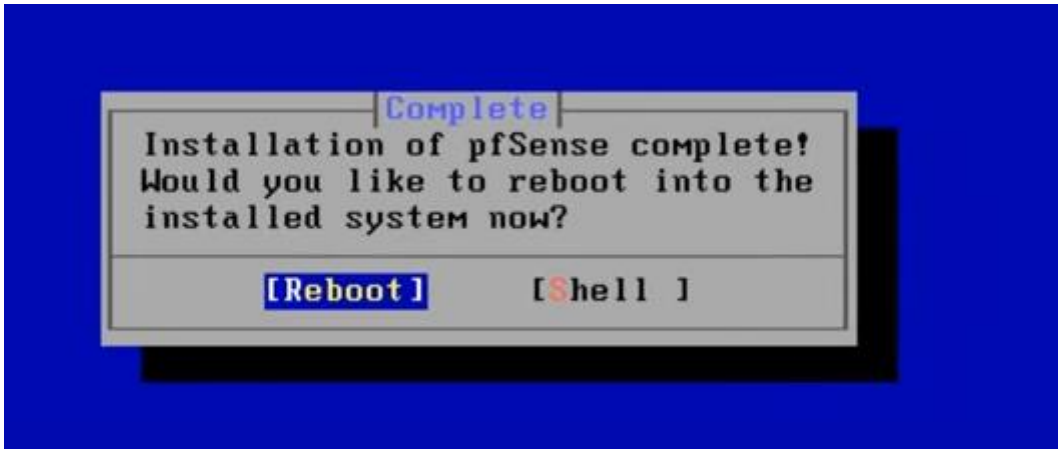


Confirmer par « yes » que vous souhaitez formateur le disque

Patientez pendant l'installation

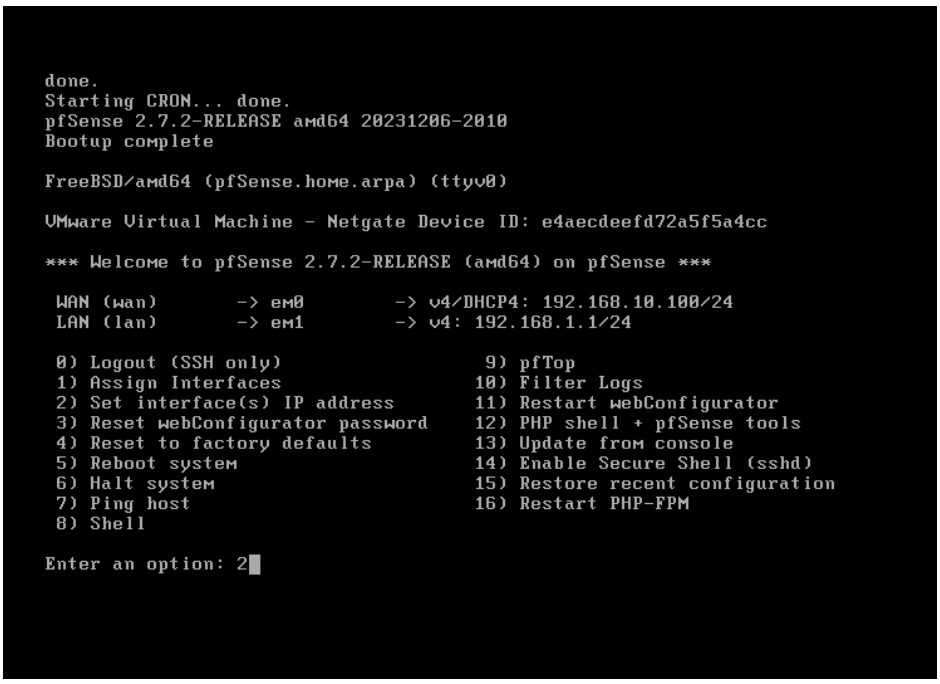


Sélectionner : **Reboot** (Ne pas oublier d'éjecter le CD)

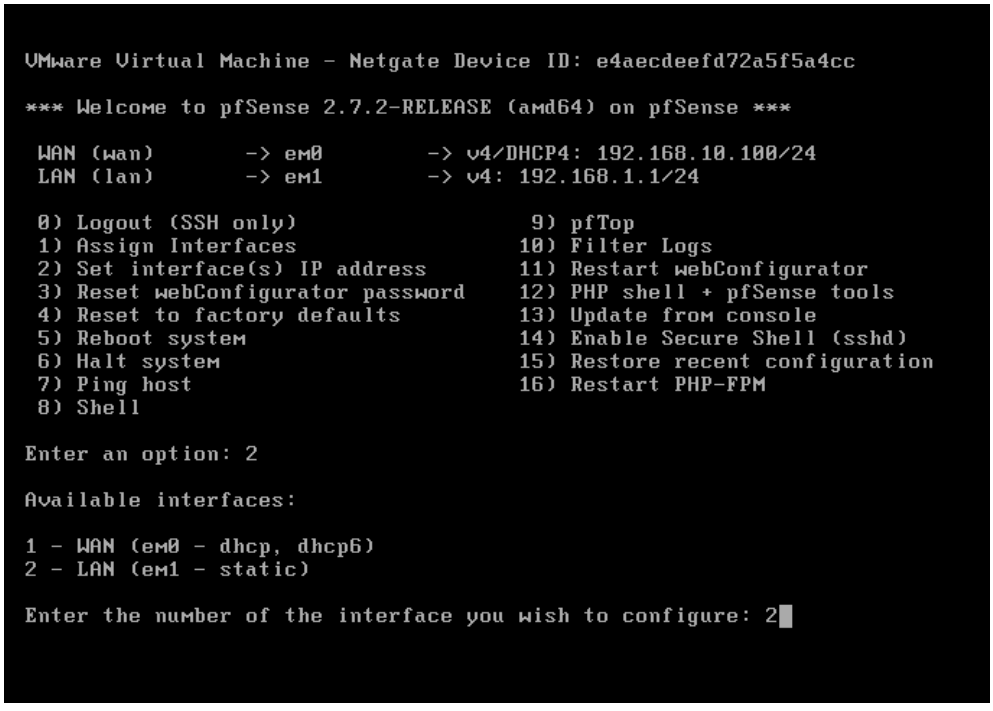


Configuration de l'adresse IP de la carte réseau local LAN **Sélectionner** : 2 (Set interface IP address)

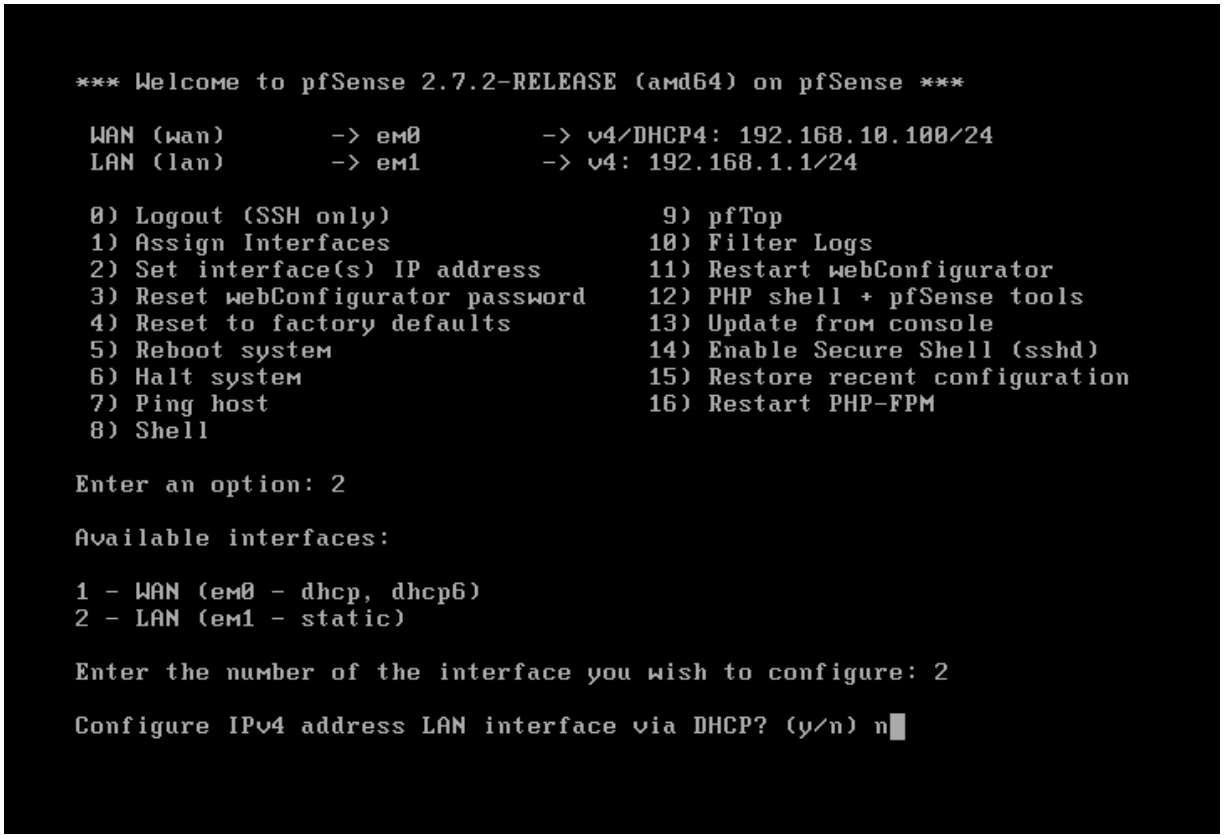
Figure 60 : PFSense /Installation de PFSENSE



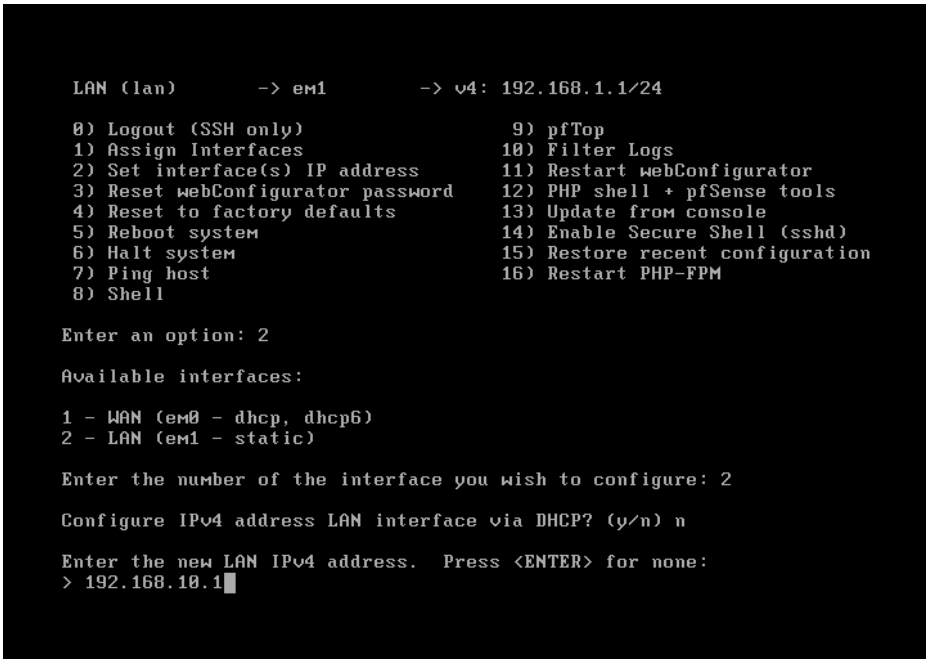
Sélectionner la carte réseau local LAN : **2**



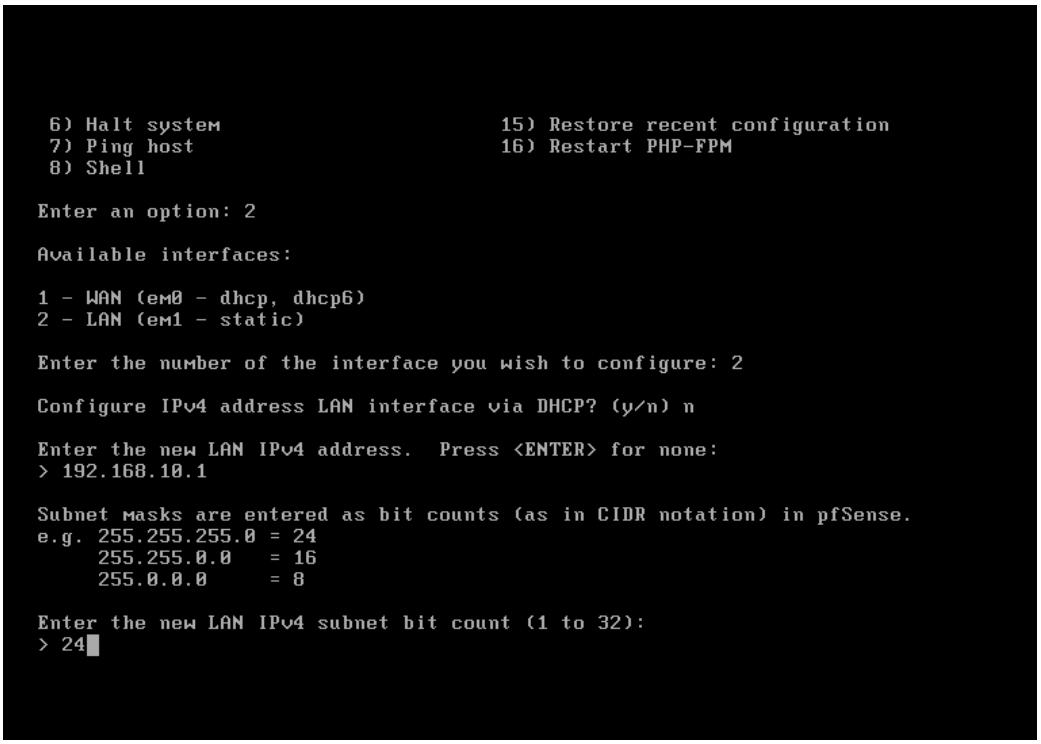
Ne pas configurer les adresses IPV4 du lan automatiquement via DHCP



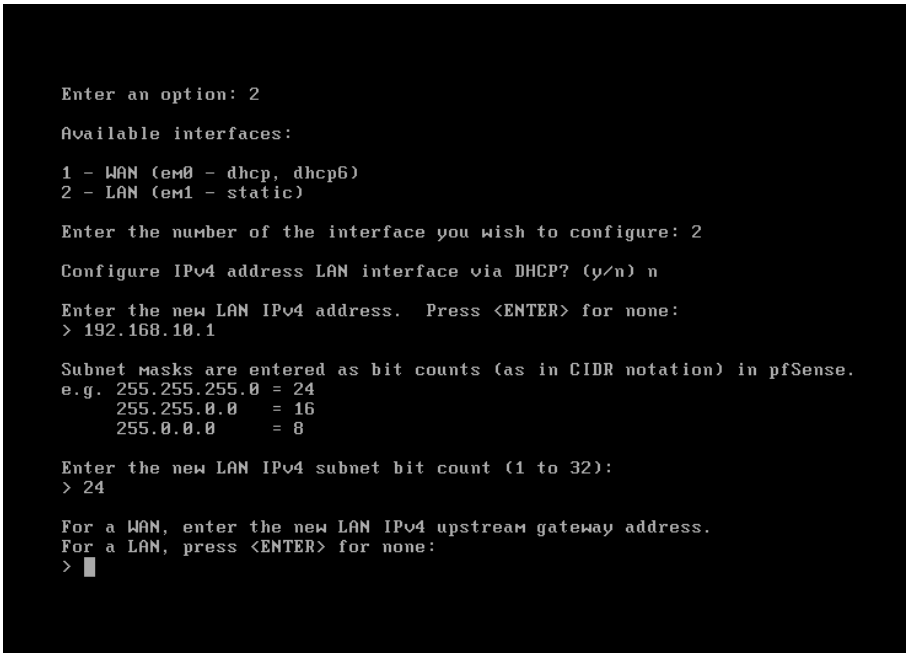
Saisissez l'adresse **IP** souhaitée : 192.168.10.1 (pour notre exemple)



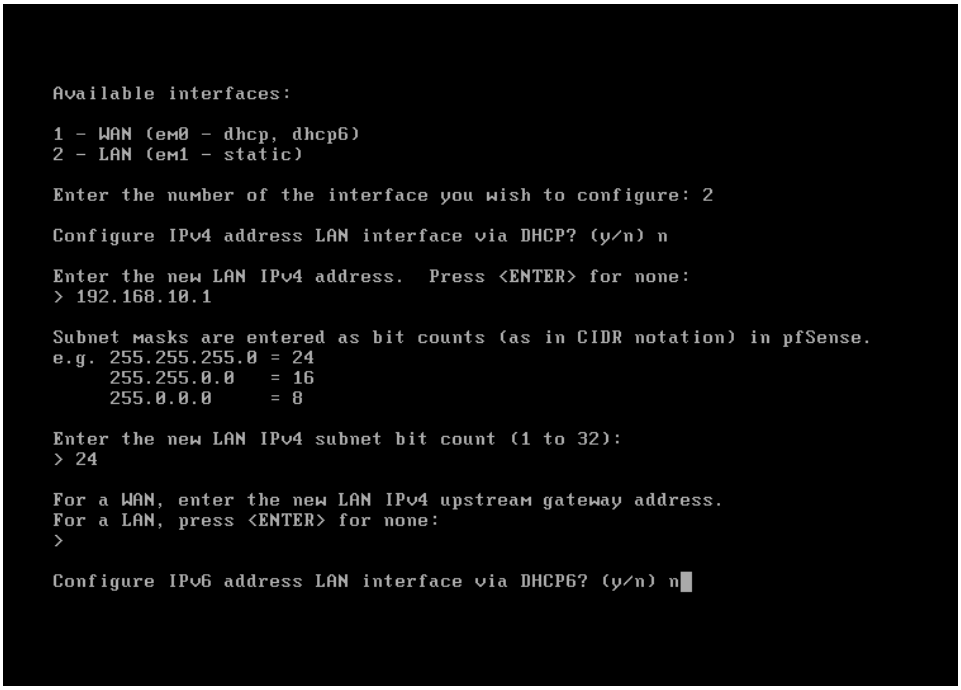
Saisissez le masque sous réseau au format CIDR : **24**



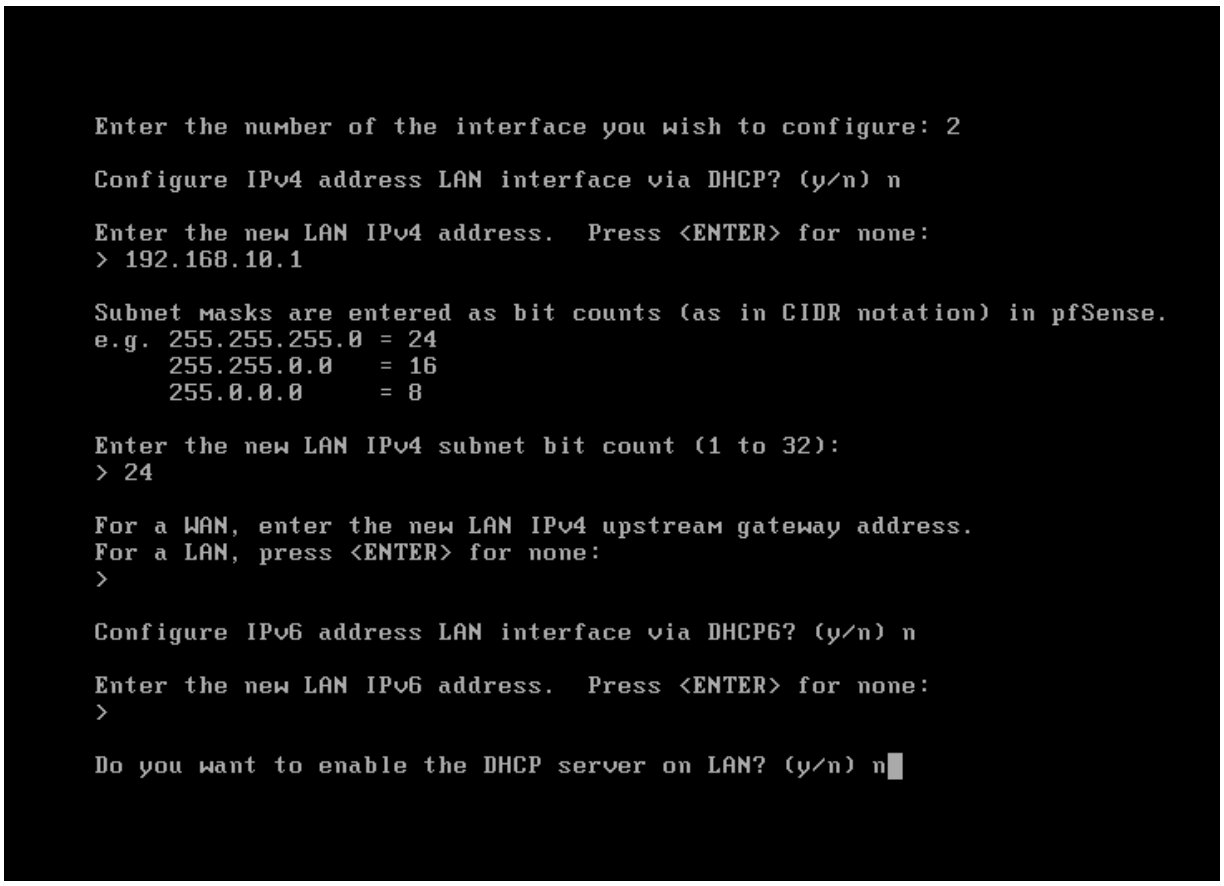
Laissez vide pour ne pas définir la passerelle : Tapez **ENTREE**



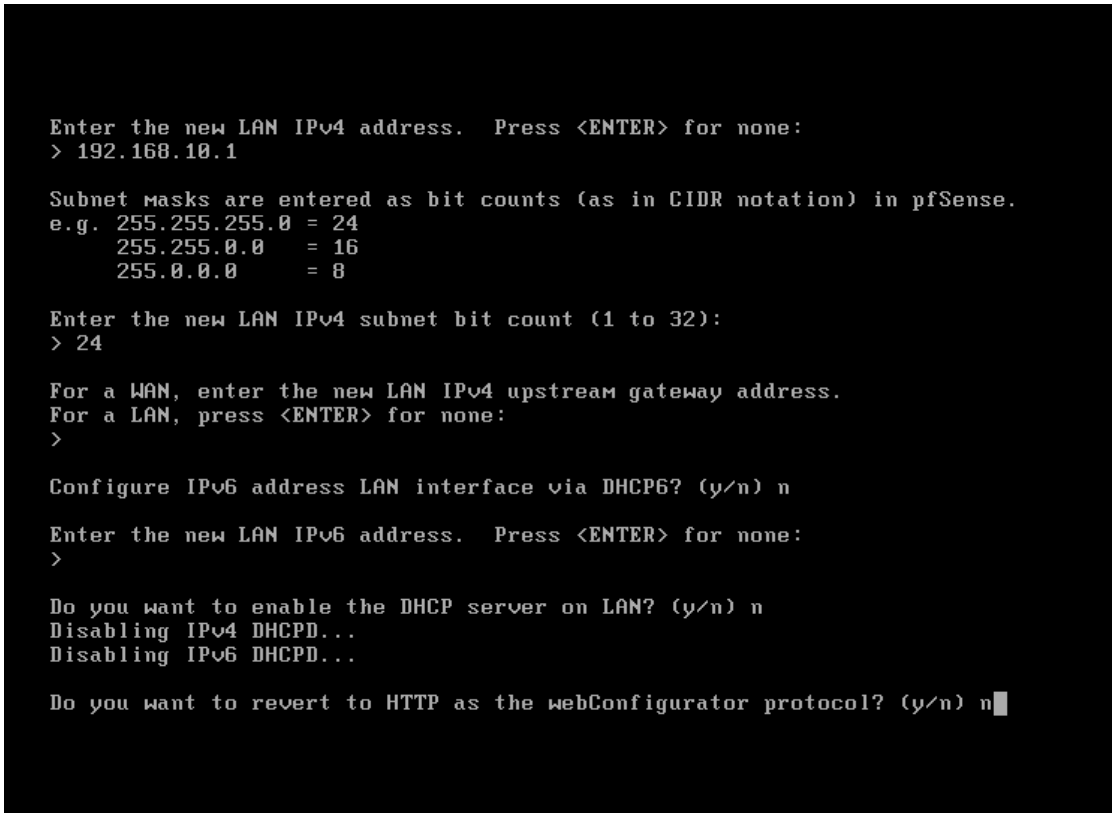
Saisir « n » pour ne pas configure d'ipv6 via DHCP6



Ne pas activer le Serveur DHCP : « **n** » pour « no »



Ne pas activez le retour à http en tant que protocole de configuration Web. Entrez : « **n**” pour “no”



Retour au Menu. L’adresse **IP** de pfSense est notée dans la partie **LAN** : 192.168.10.1

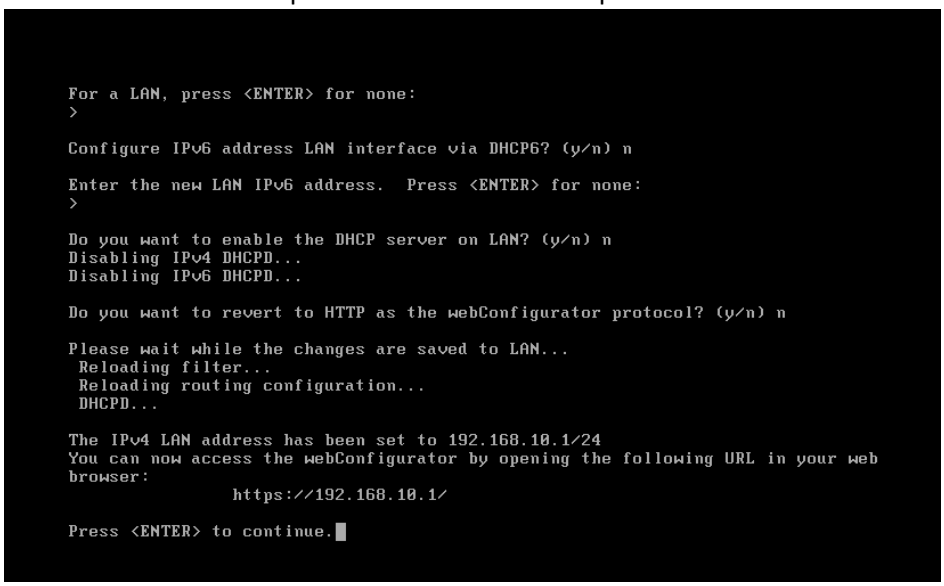
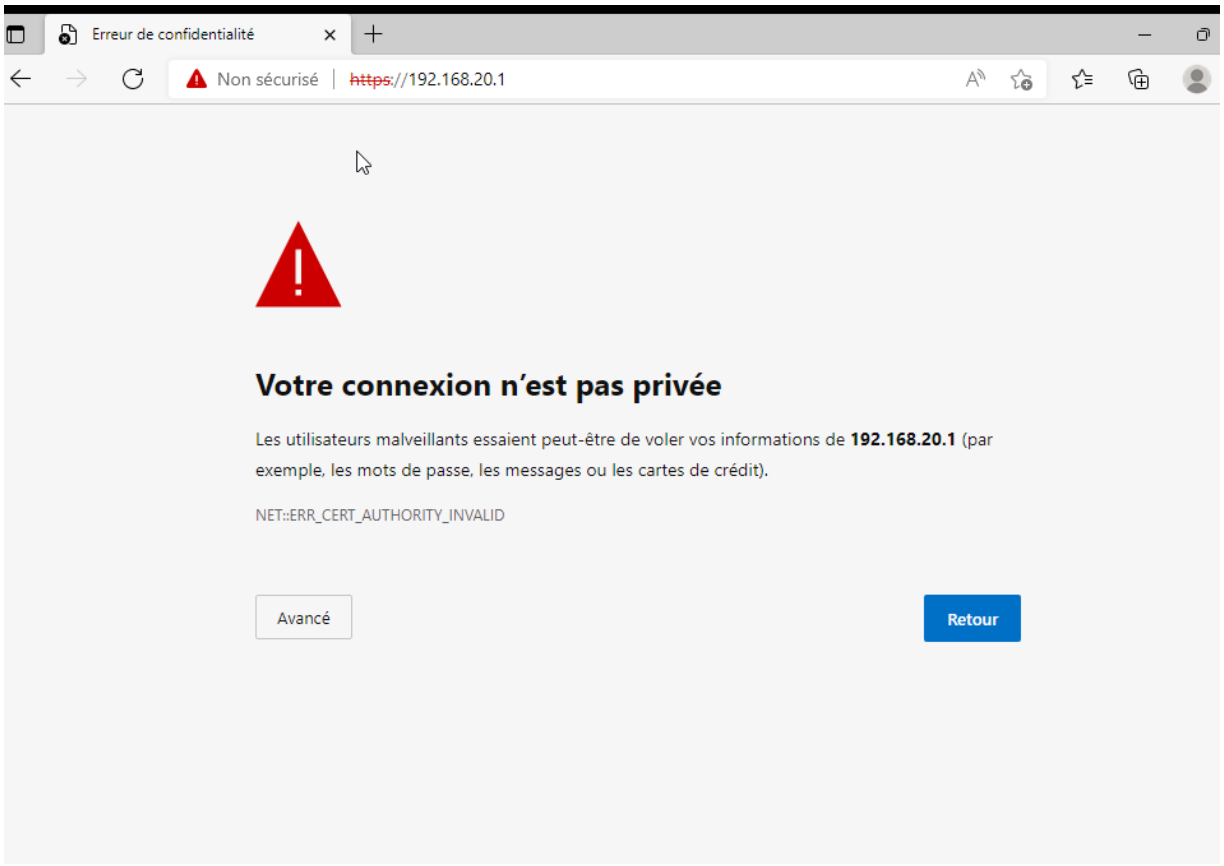


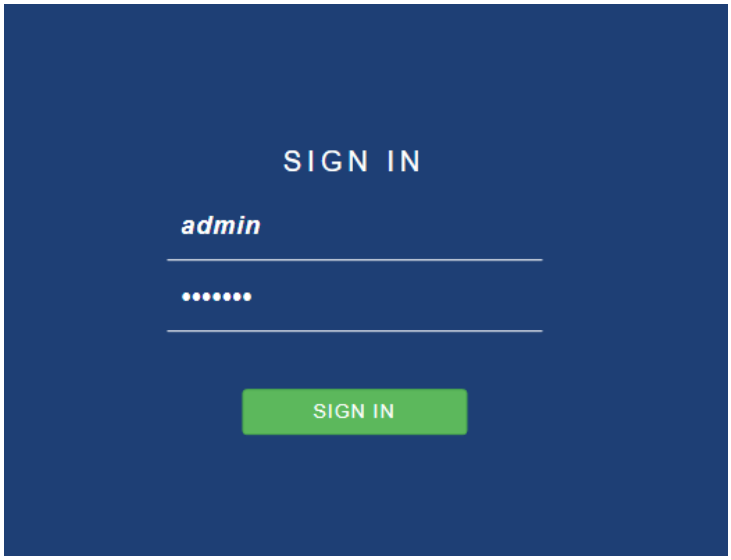
Figure 61 : PFSense /Configuration de l’interface Lan de PFSense

Cliqué sur Avancé puis « accéder au site »

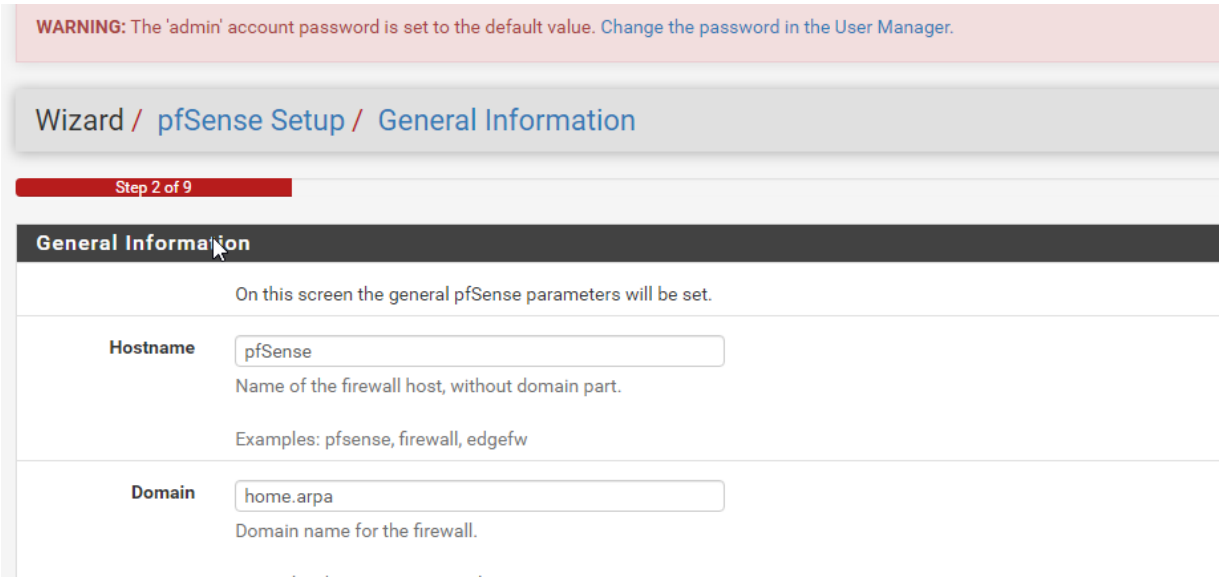


Configuration de l'installation de Base de pfSense

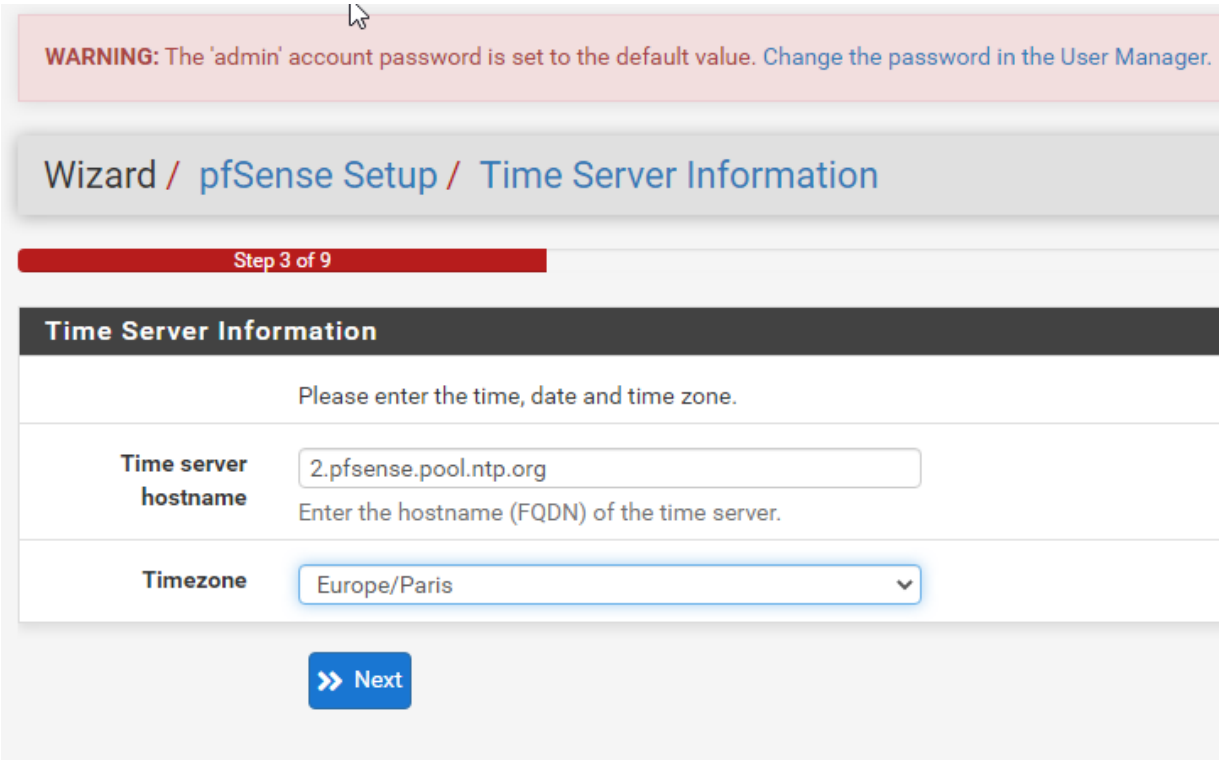
Tapez L'adresse **IP** dans le navigateur : 192.168.2.1 – Username : **admin** – Password : **pfsense**



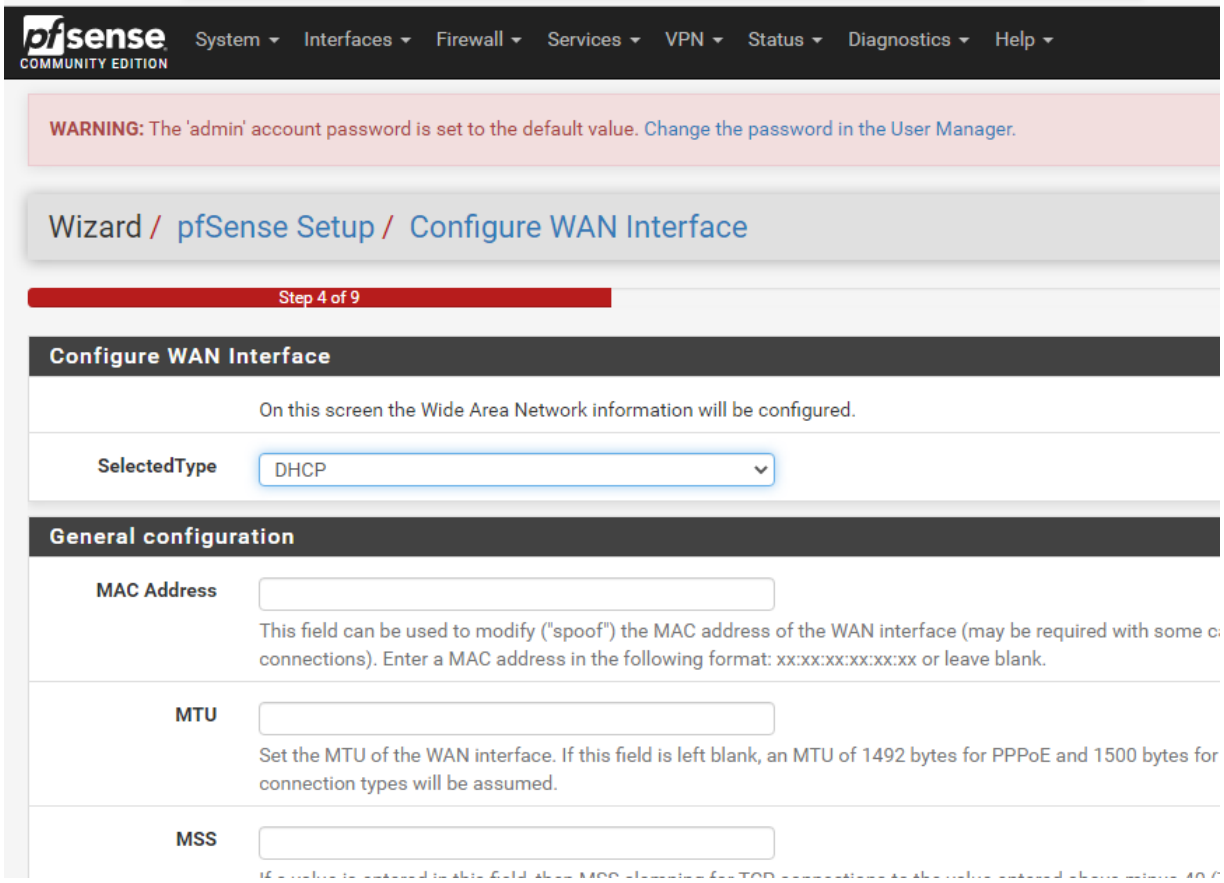
Renseigner : **Hostname , Domain**



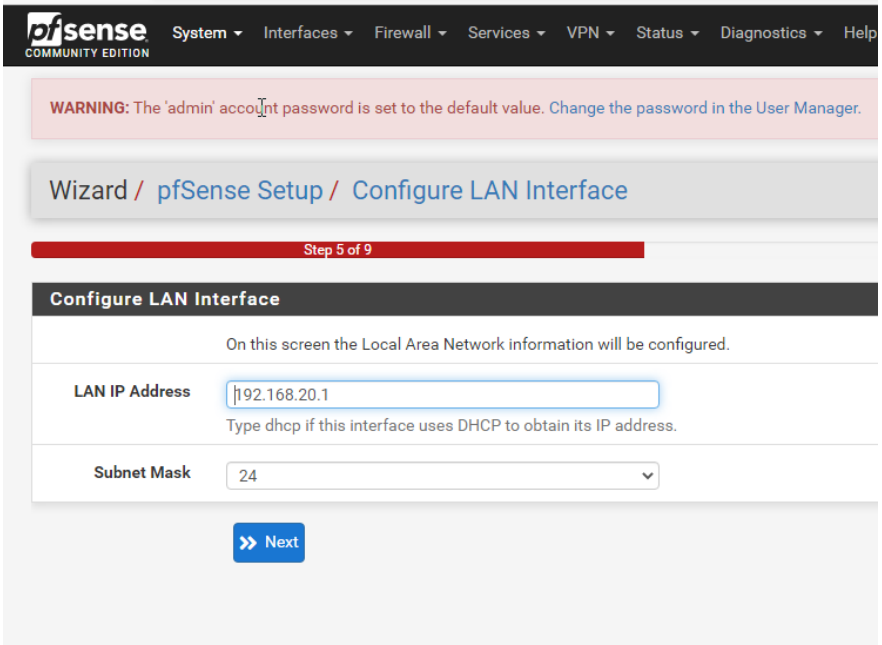
Sélectionner la **Timezone Europe**



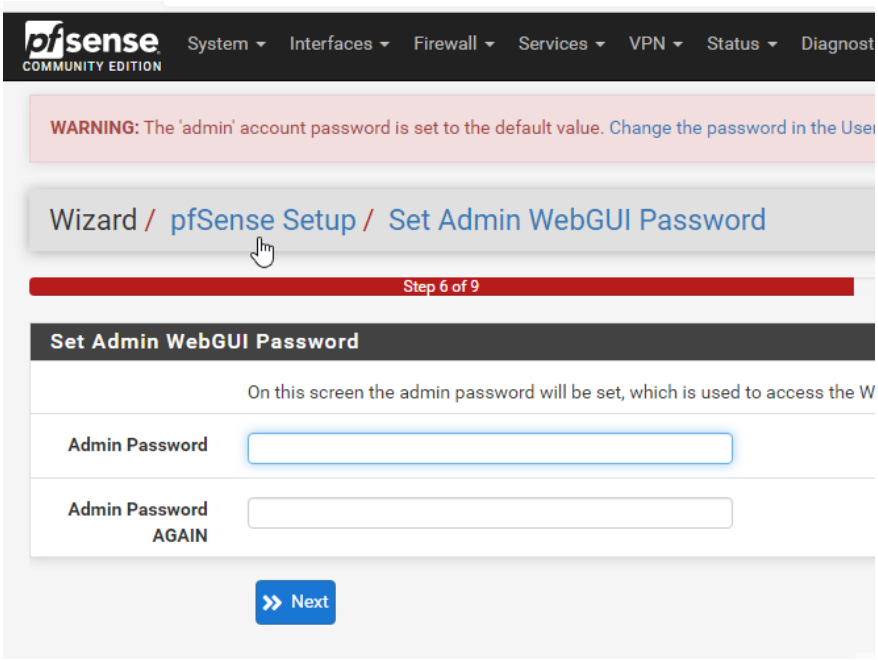
Configuration de la carte réseau internet **WAN : « DHCP »**



Vérification de la configuration de la carte réseau local **LAN**



Modifier le **mot de passe admin**



Cliquer sur : **Reload**

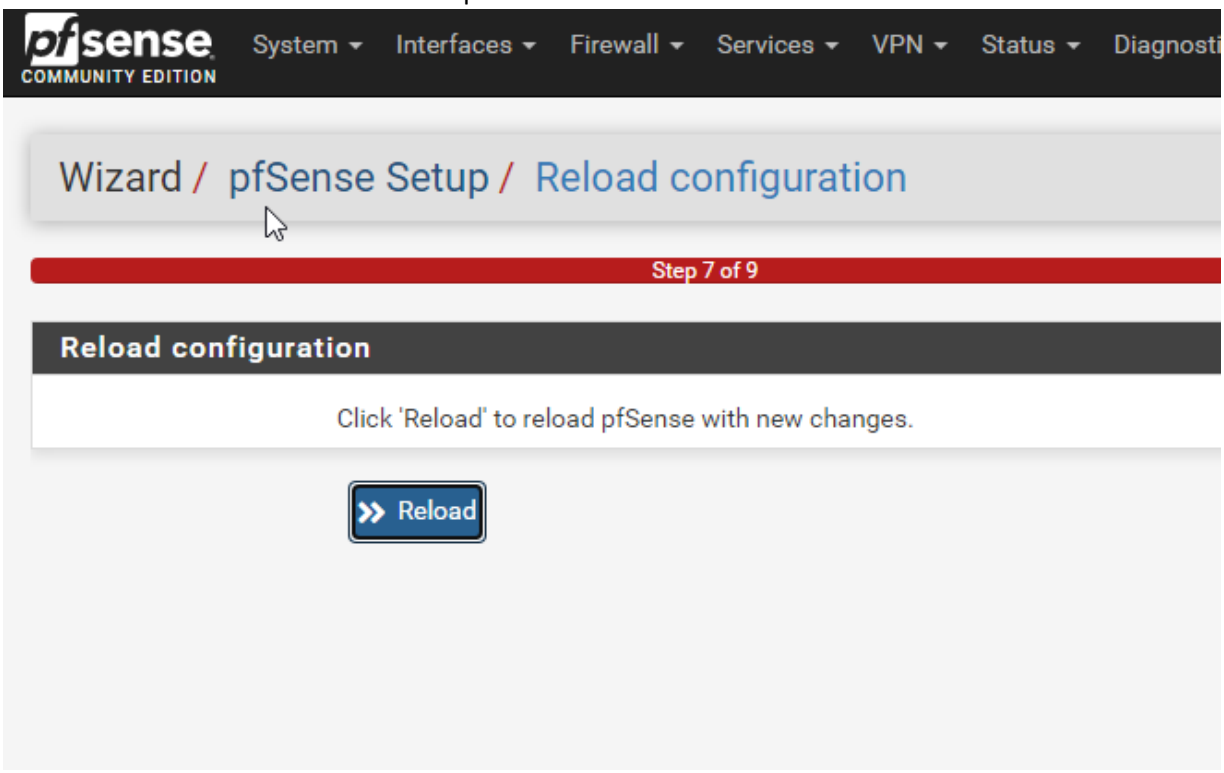
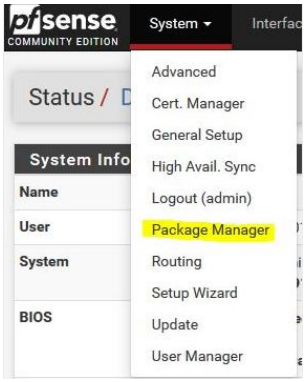


Figure 62 : PFSense /Configuration de PFSENSE

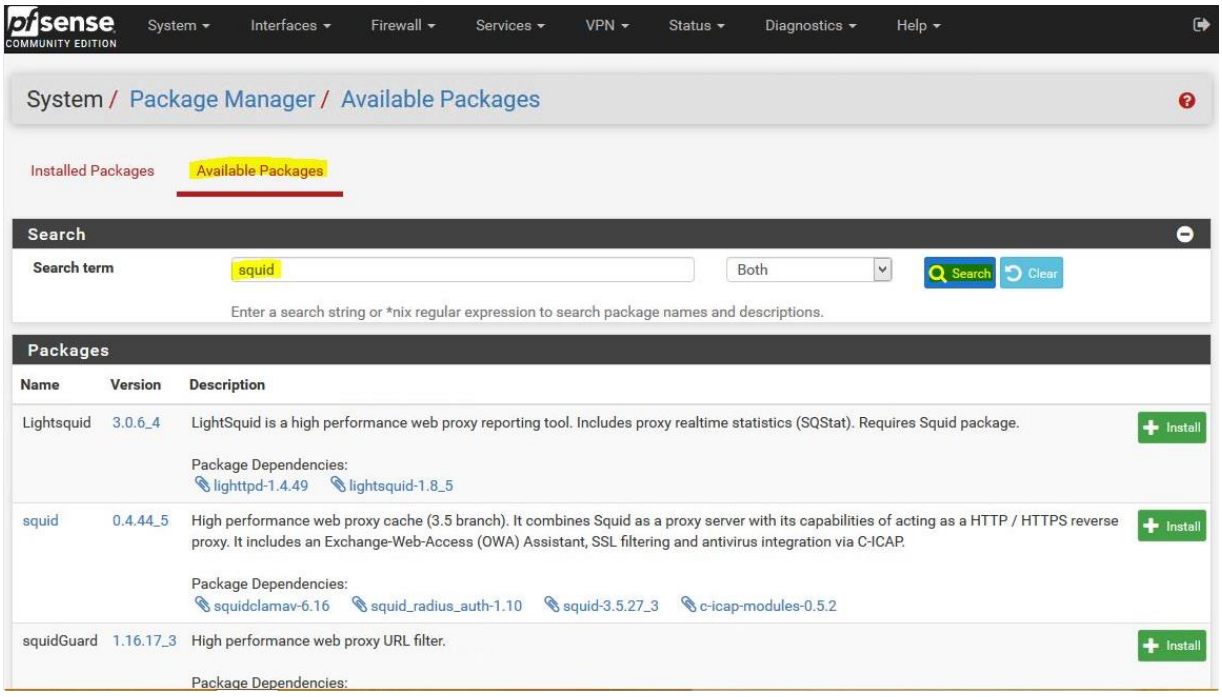
9.1 *Mise en place d'un proxy transparent **Squid** avec filtrage d'URL*

Sélectionner : System, Package Manager

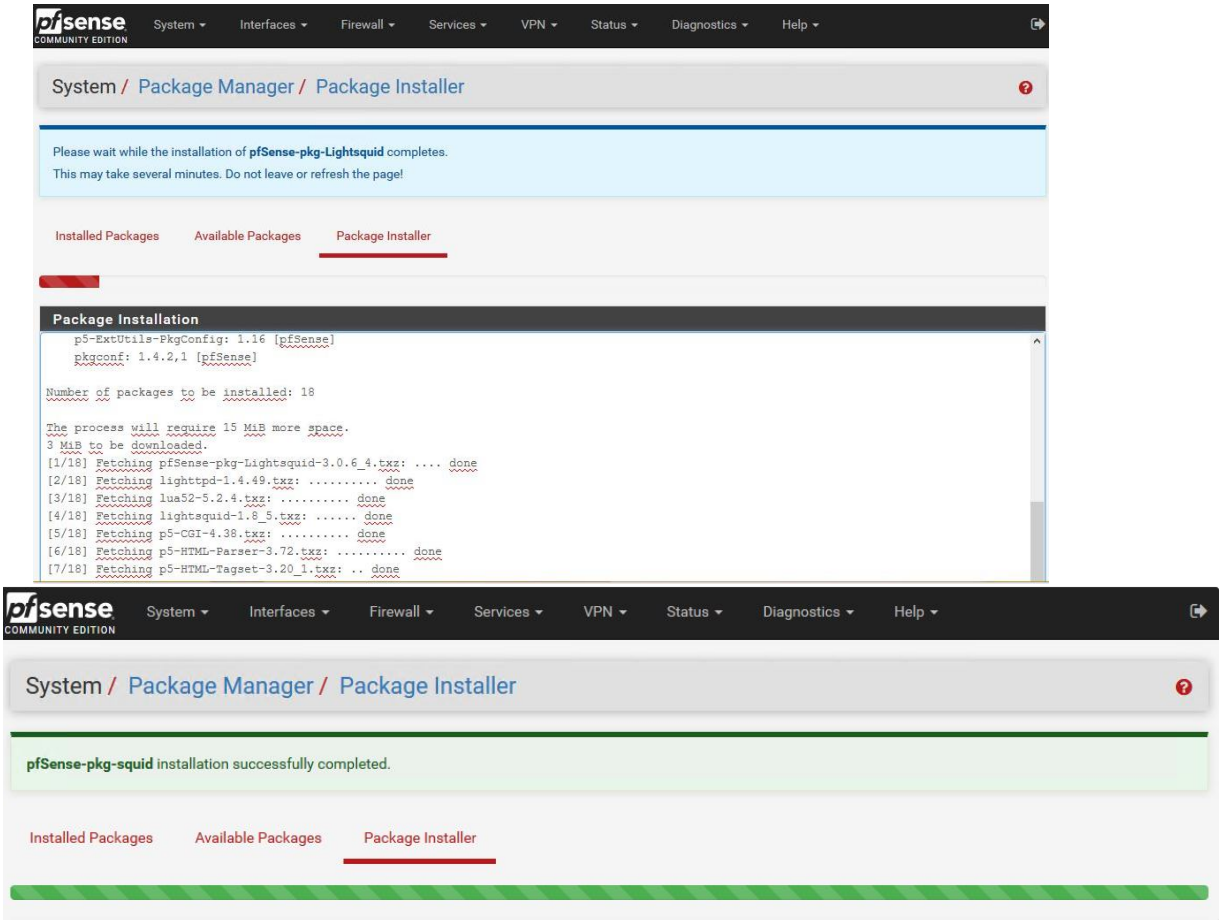


Sélectionner « **Available Packages** », dans la recherche taper « **squid** » puis cliquez sur « **Search** »

Installer les 3 packages un par un : **Squid , SquidGuard, LightSquid**



Installation des Packages



Les 3 Packages sont installés

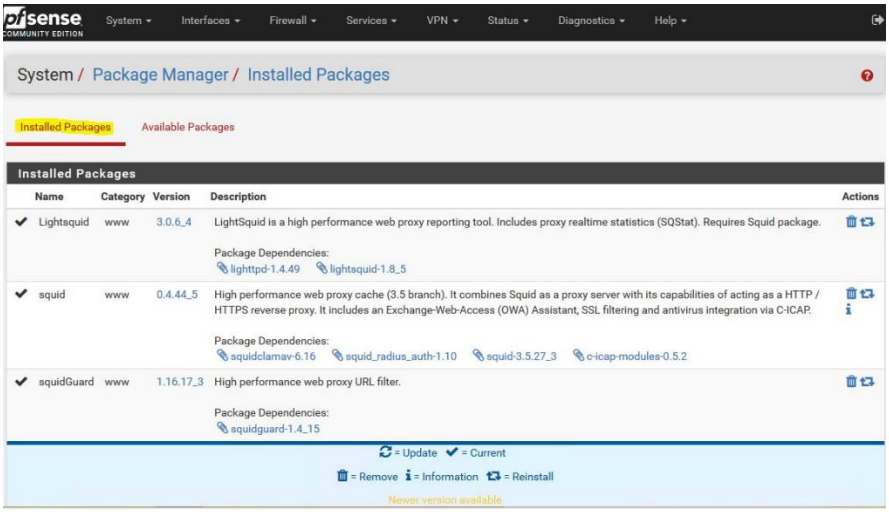
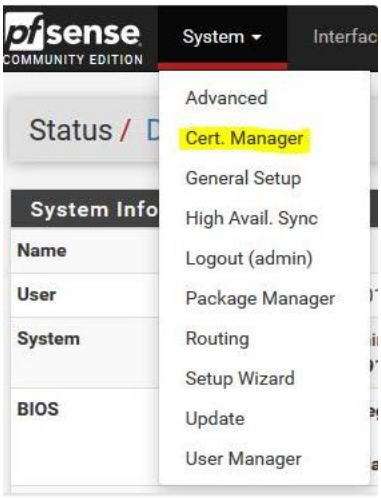


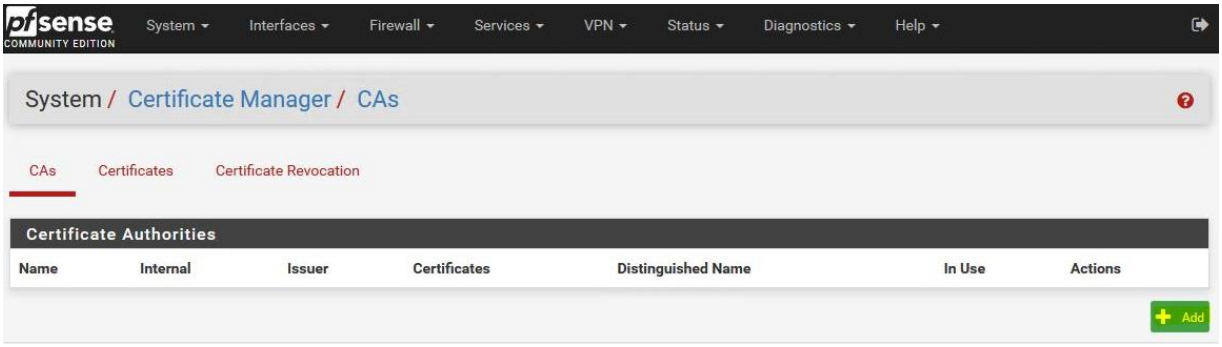
Figure 63 : PFSense Filtrage /Installation des packages

Création du Certificat pour le filtrage en HTTPS

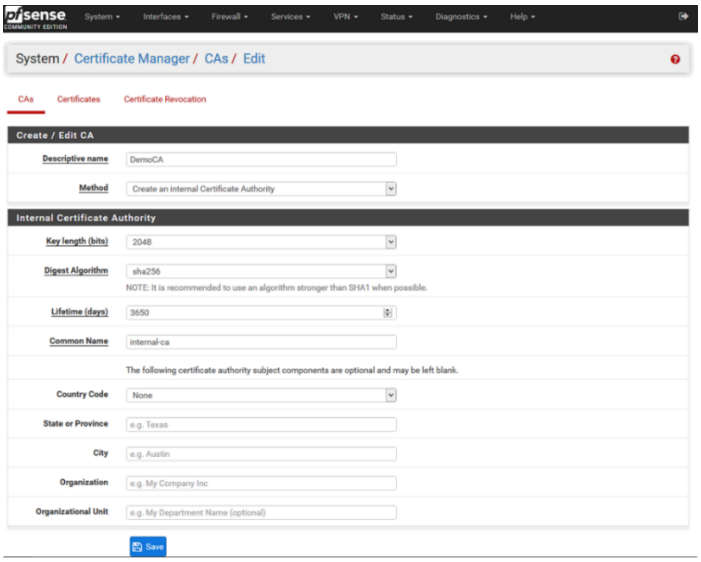
Sélectionner : System , Cert. Manager



Cliquer sur « **Add** »



Donner un « **Nom**« , sans espace. Exemple : « **DemoCA** » , laisser le reste par défaut et cliquez sur « **Save** »



Le Certificat est créé

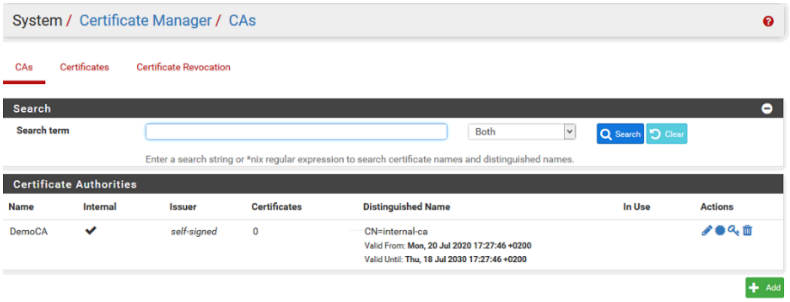
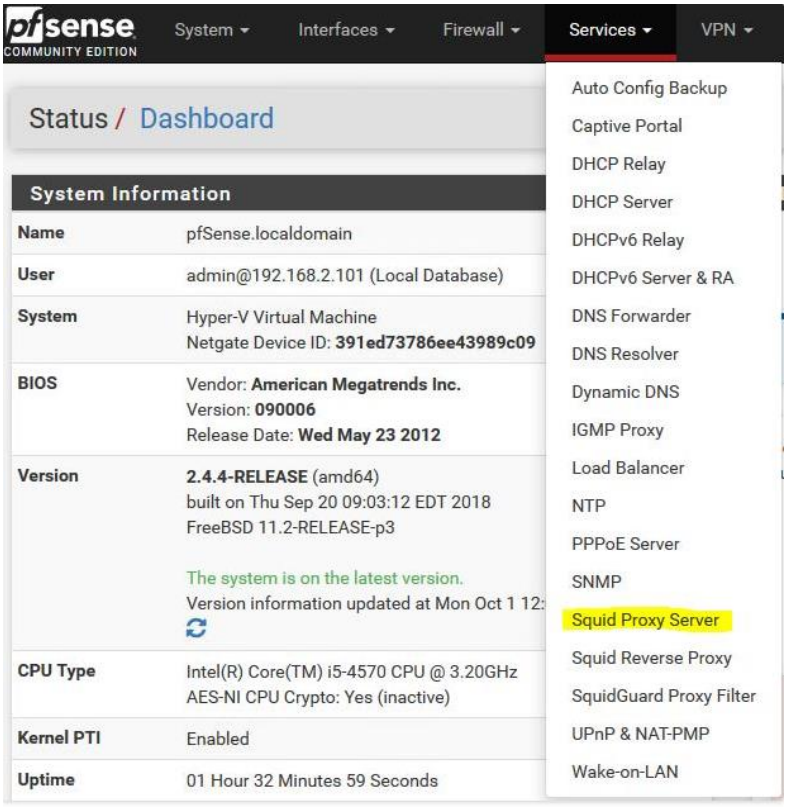


Figure 64 : PFSense Filtrage /Configuration du certificat

Configuration de Squid

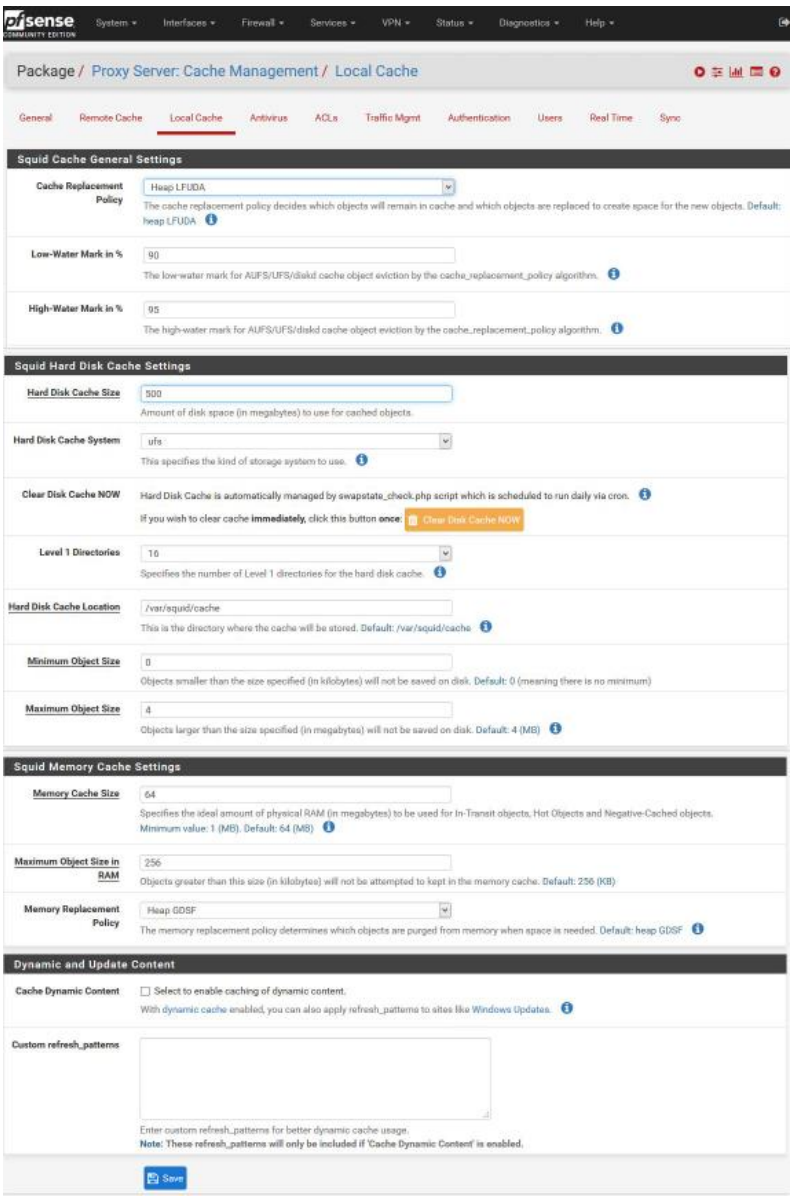
Sélectionner « Services » et « Squid Proxy Server »



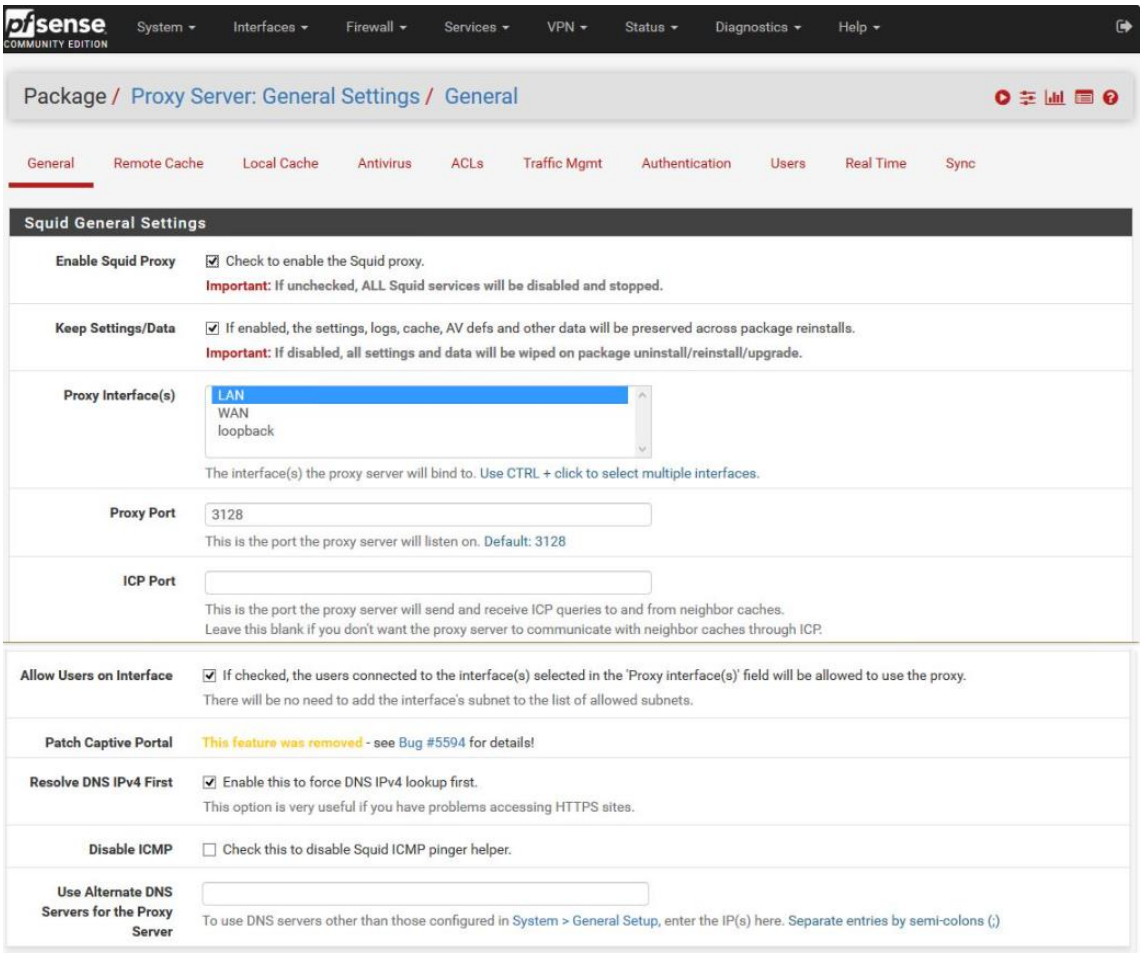
Sélectionner « **Local Cache** » et paramétrer :

- « **Hard Disk Cache Size** » : **500 Mo**, mais **<u>3000 Mo</u>** est préférable en production
    - « **Memory Cache Size** » : 50% de la RAM installée > **1000 MB**

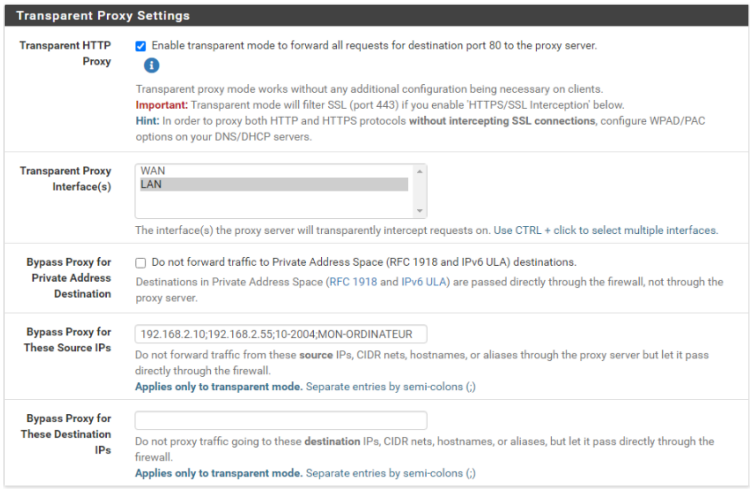
Cliquer sur « **Save** »



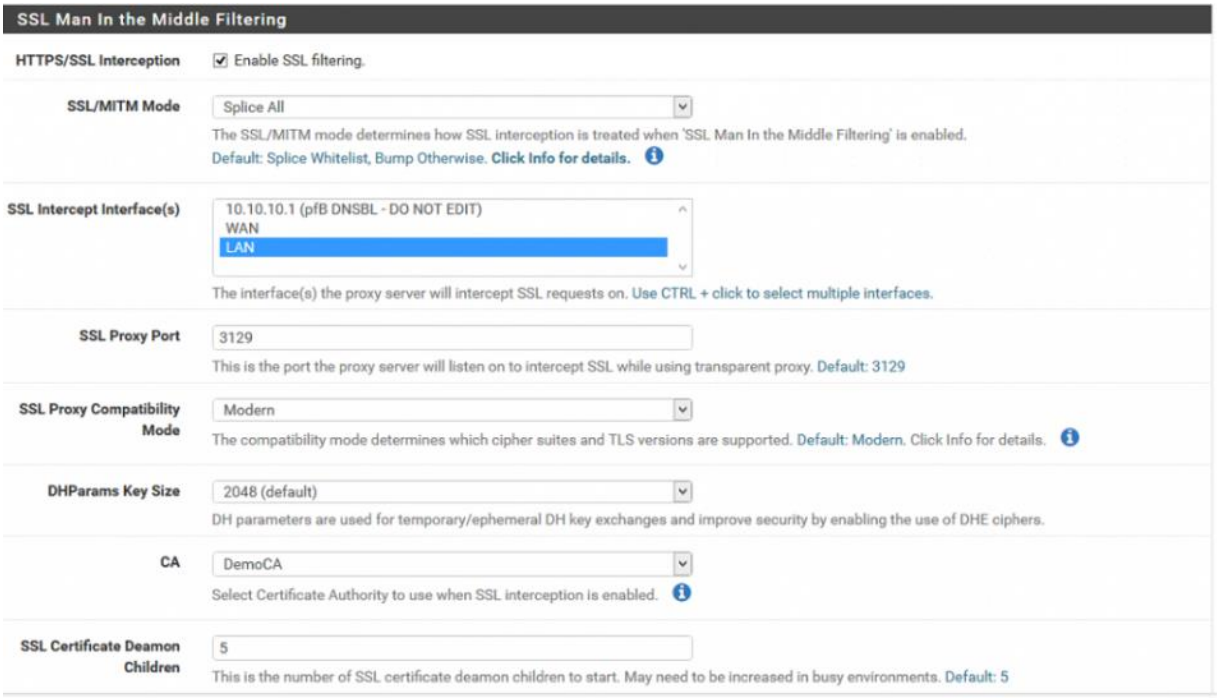
Onglet « **General** » : **Activer** « **Enable Squid Proxy**« , sélectionner l'interface réseau « **LAN**« et « **Resolve DNS IPv4 First** »



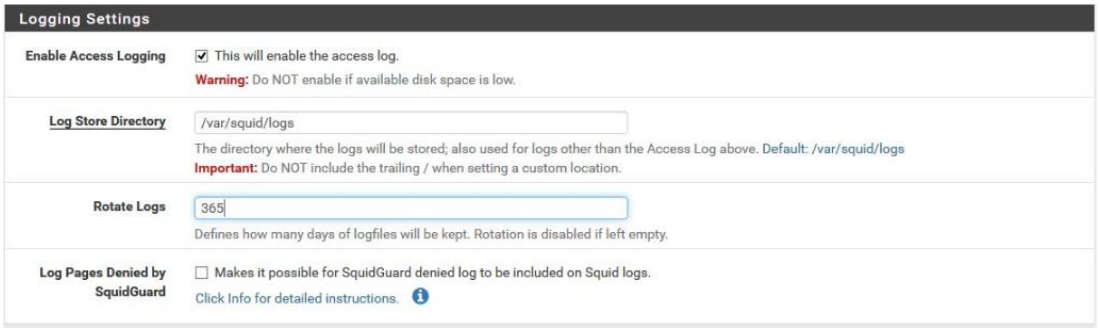
Activer « **Transparent HTTP Proxy** » et sélectionner l'interface réseau « **LAN** »



Activer « **HTTPS/SSL Interception SSL filtering** » , sélectionner « **Splice All**« , l'interface « **LAN** » et le Certificat précédemment créé « **DemoCA** »



Activer « **Enable Access Logging** » et définir combien de jours les logs seront conservés : **365** (un an)



Sélectionner « **fr** » pour « **Error language** » et Activer « **Suppress Squid Version** »

Puis Cliquer sur « **Save** » pour enregistrer toutes les modifications effectuées dans Squid

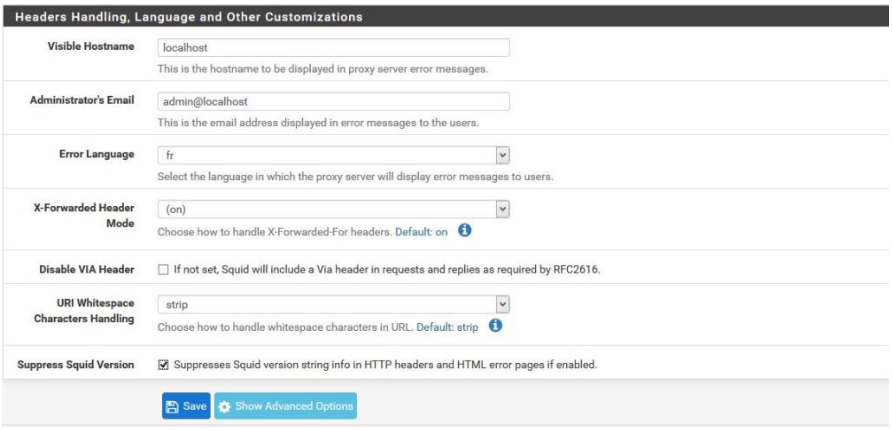
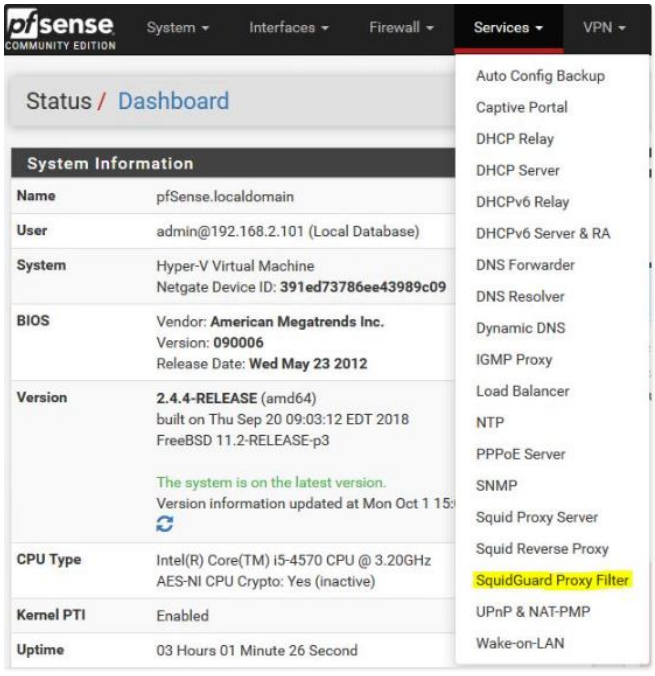


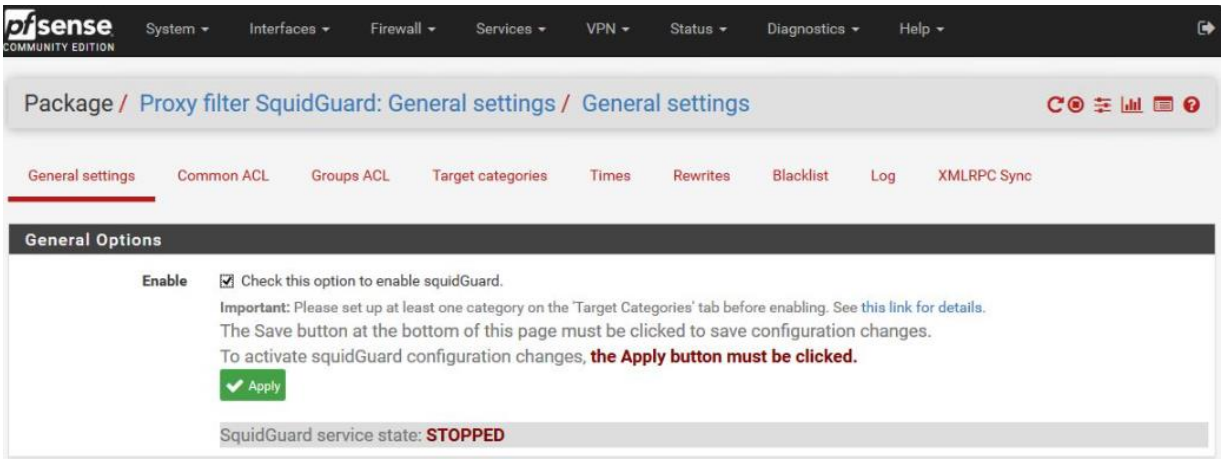
Figure 65 : PFSense Filtrage /Configuration de Squid

Configuration de SquidGuard

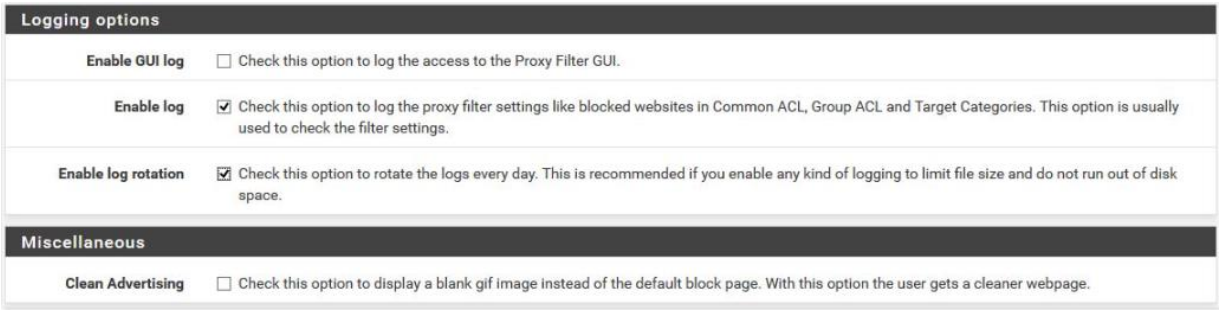
Sélectionner « Services » et « SquidGuard Proxy Filter »



Activer SquidGuard « **Enable** »

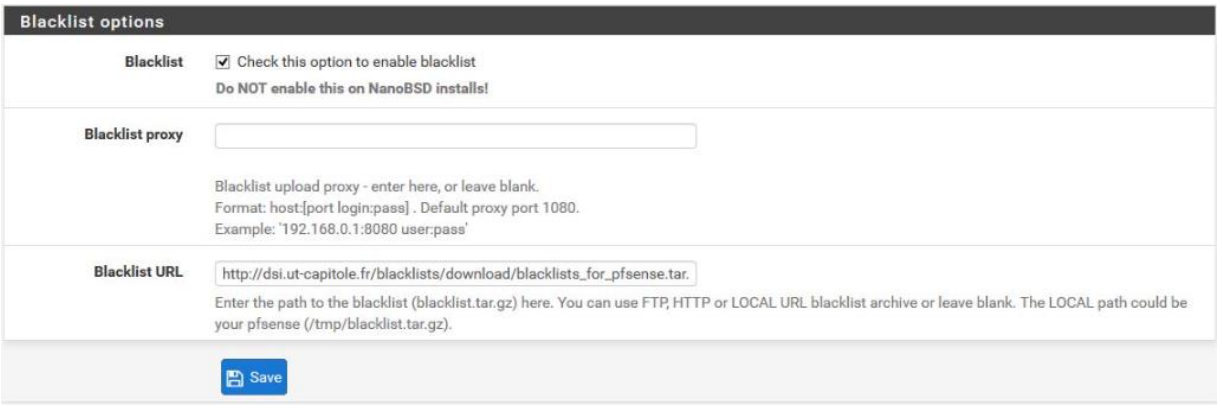


Activer « **Enable Log** » et « **Enable log rotation** »

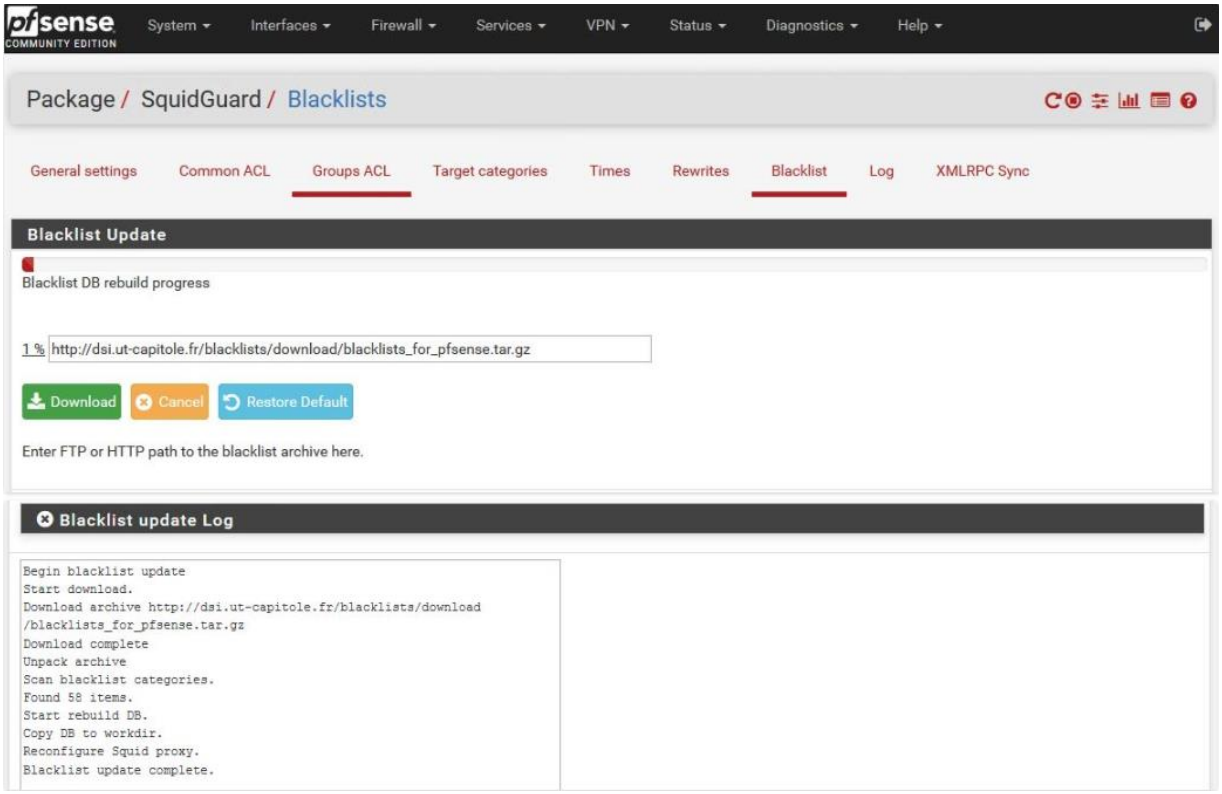


Activer « **Enable Blacklist** » et inserer dans **Blacklist URL** : http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

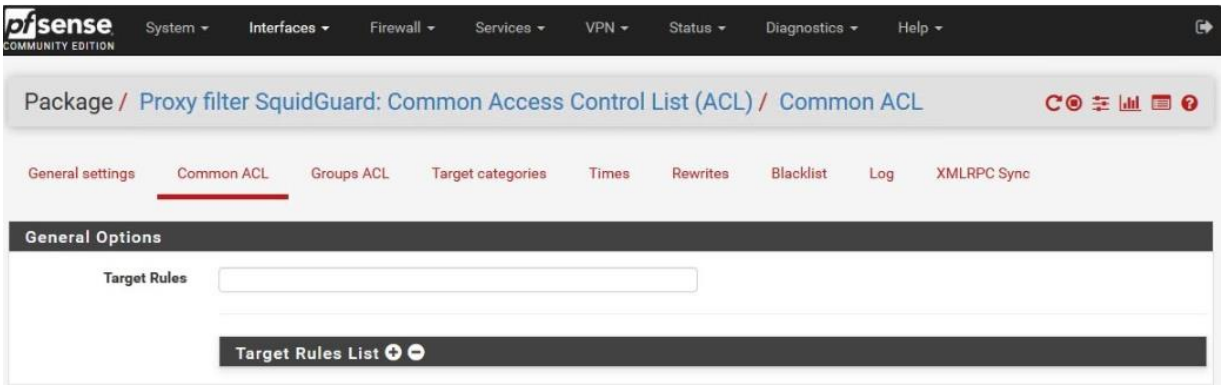
Puis cliquez sur « **Save** »



Onglet « **Blacklist** » : Cliquer sur « **Download** » pour télécharger les listes de filtrage

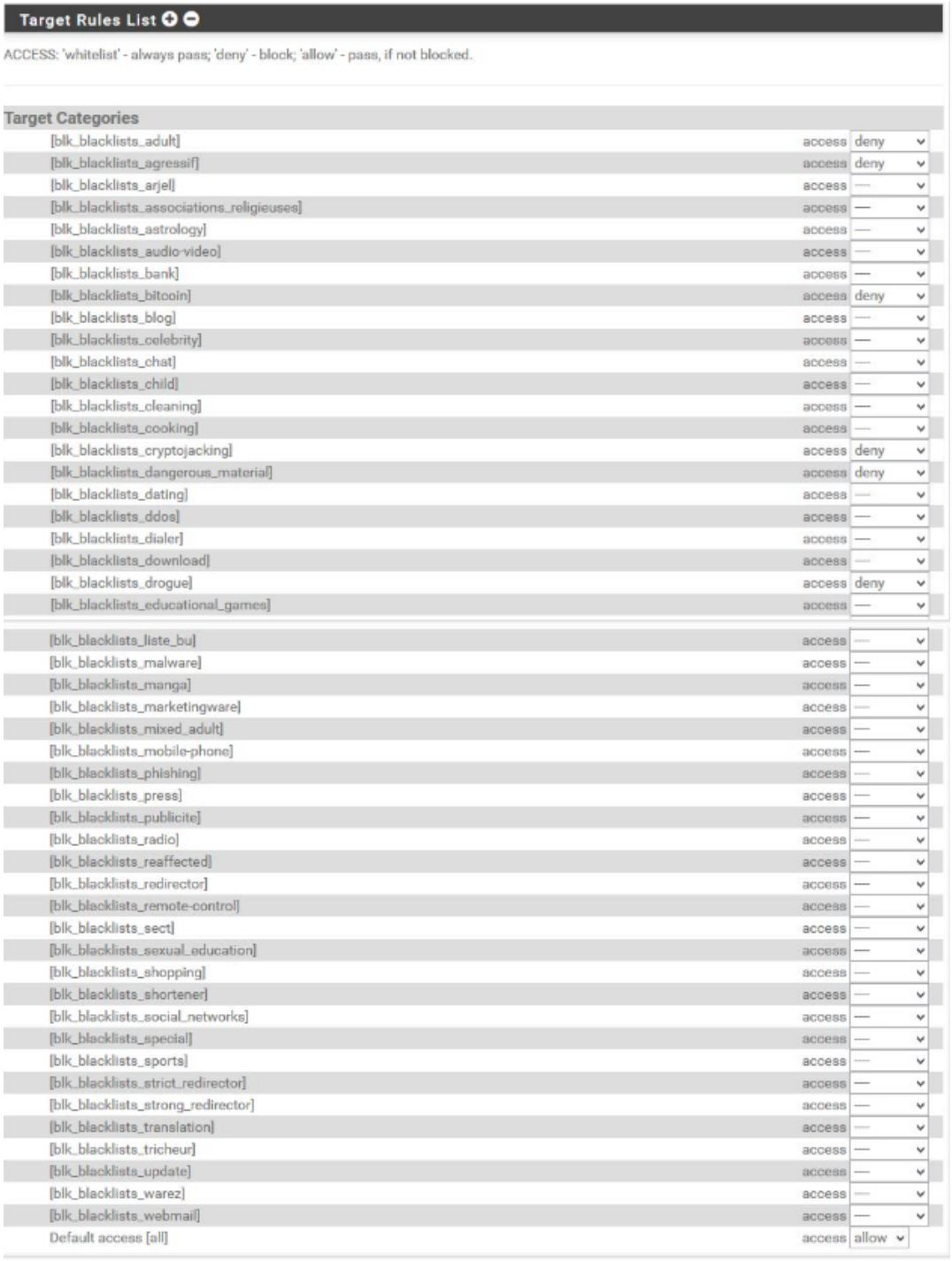


Onglet « **Common ACL** » , Cliquez, dans « **Target Rules List** » sur le » **+** »

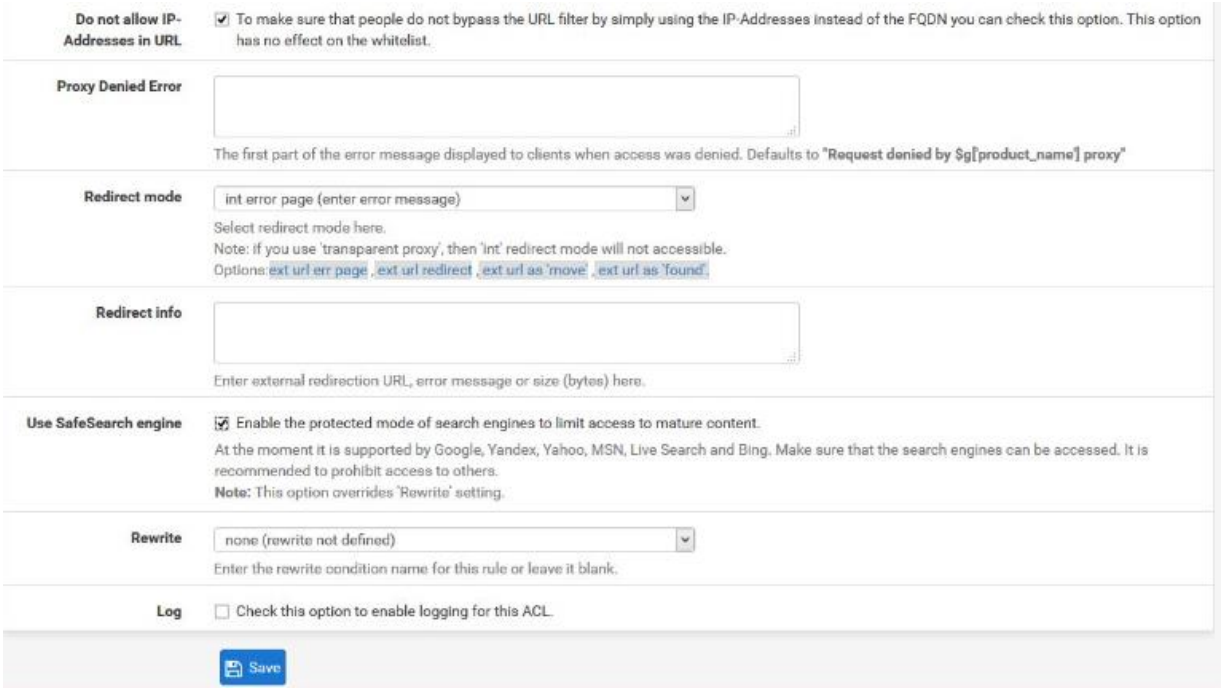


Sélectionner les catégories a bloquer (ou a autoriser)

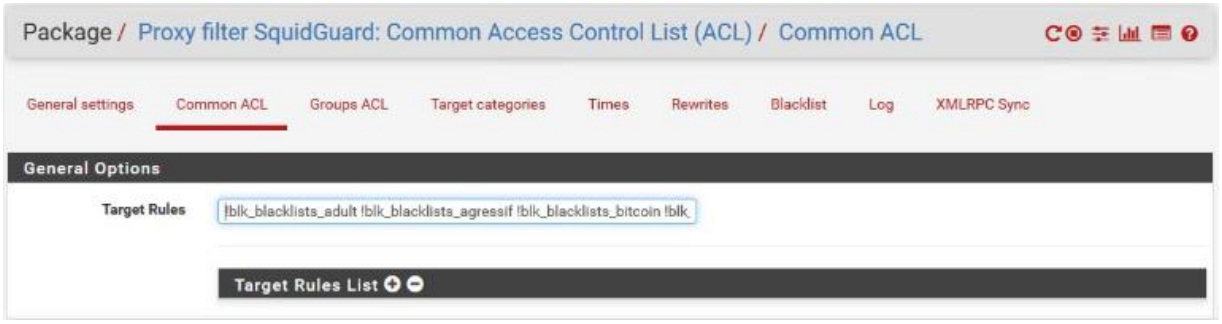
<u>Important</u> : Sélectionner »**Allow** » pour « **Default access [all]** »



Cocher « **Do not allow IP addresses in URL** » et « **Use SafeSearch engine** »



Les catégories de filtrages sont bien enregistrées dans « **Target Rules** »



Pour valider les paramétrages, retournez sur l'onglet « **General settings** » et cliquez sur « **Apply** »

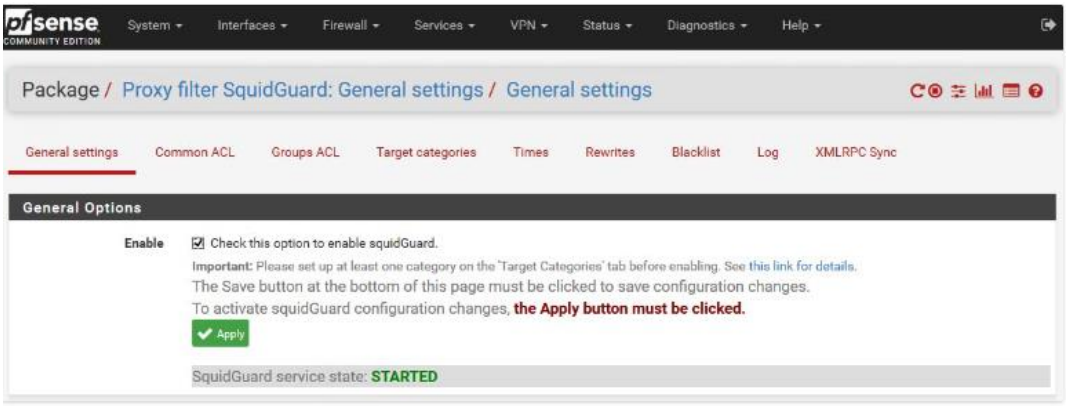
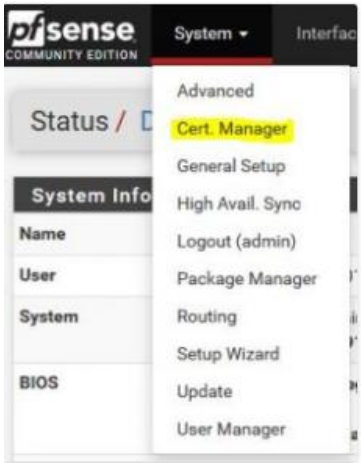


Figure 66 : PFSense Filtrage /Configuration de Squidguard

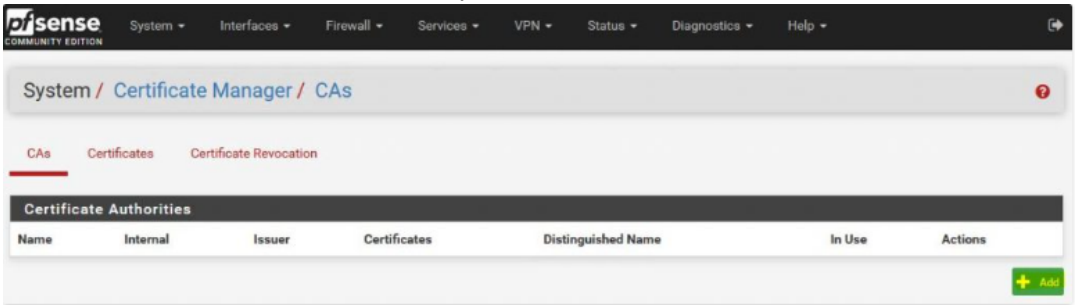
9.2 *Configuration d'un tunnel VPN avec OpenVPN*

Création de l'Autorité de Certification – CA

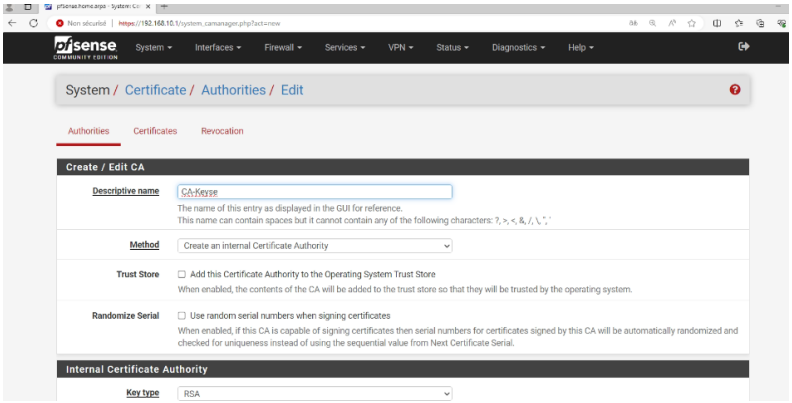
Sélectionner : System > **Cert. Manager**



Cliquer sur "**+ Add**"



Donner un “**Nom**“, sans espace. Exemple : “**CA-Keyse**” , laisser le reste par défaut et cliquez sur “**Save**”



Le Certificat est créé

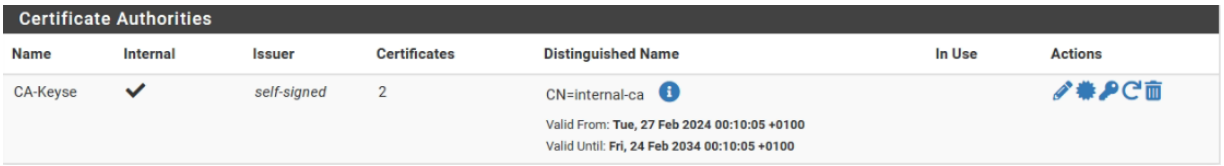
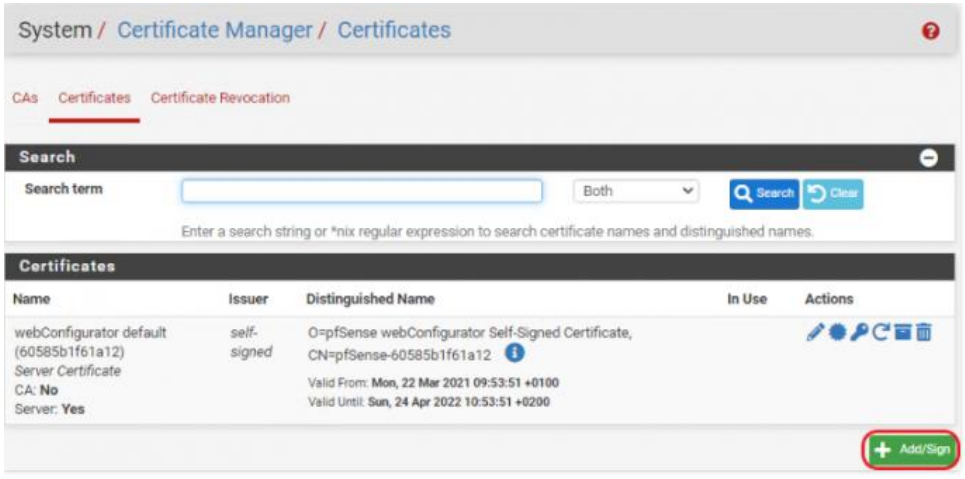
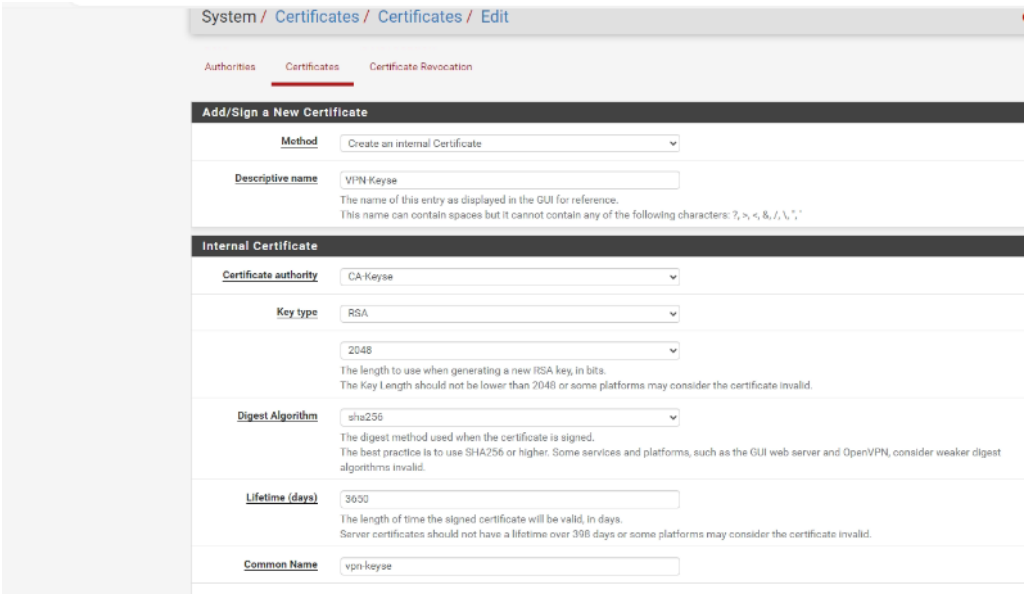


Figure 67 : PFSense VPN /Création de l’autorité de certification

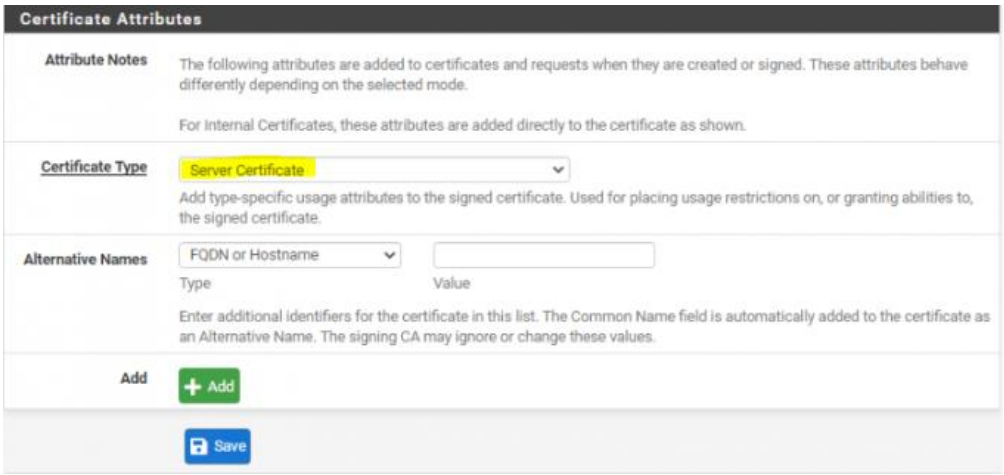
Sélectionner : « **Certificates** » et cliquer sur « **+ Add/Sign** »



Définir « **Method** » sur « **Create an Internal Certificate**« , donner un Nom « **VPN-Keyse**» et sélectionner l'autorité de certification « **Certificate authority** » créée précédemment « **CA-Keyse** »



Sélectionner le type de certificat (Certificate Type) : « **Server Certificate** » puis cliquer sur « **Save** »



Le Certificat est créé.

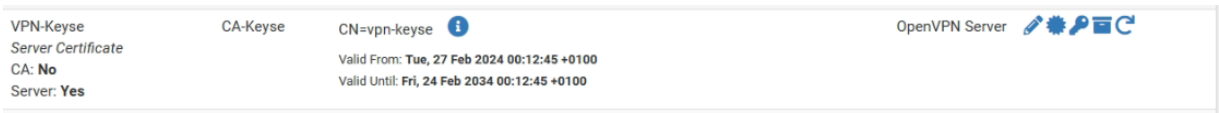
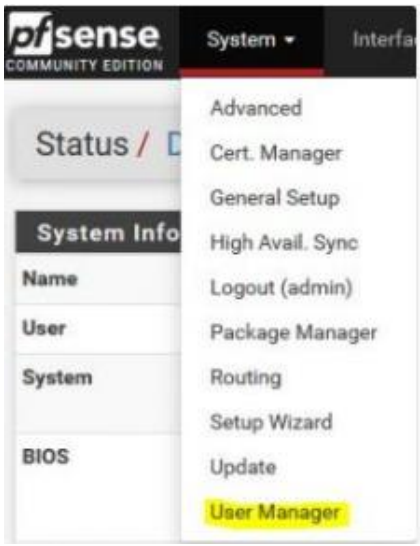


Figure 68 : PFSense VPN /Création du certificat serveur

Création des Utilisateurs du VPN

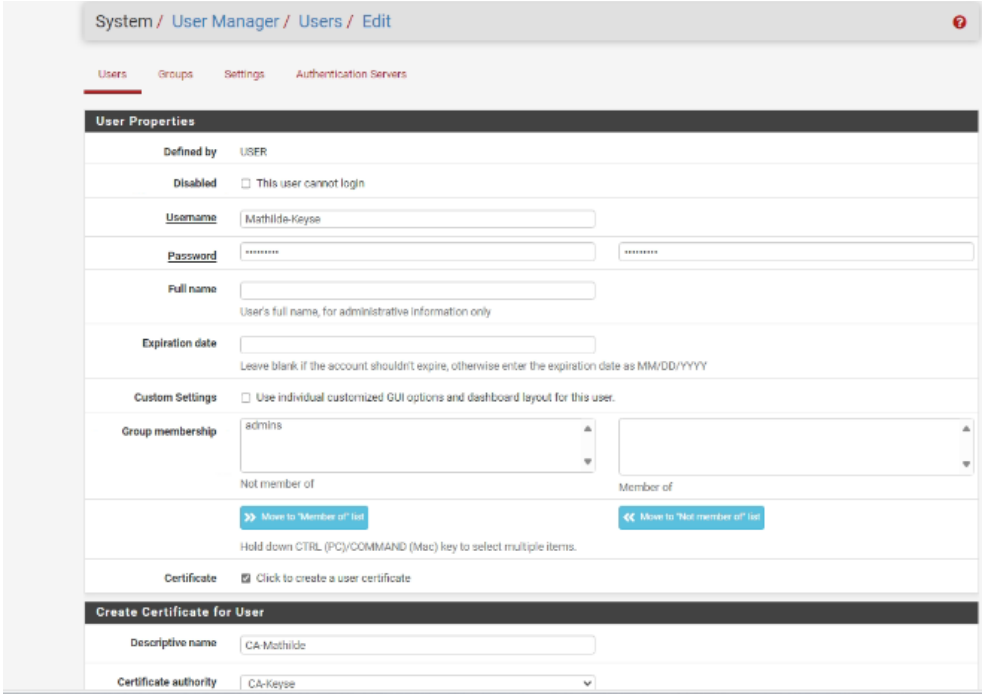
Sélectionner : System > **User Manager**



Cliquer sur "**+ Add**"

Entrer un **Nom d'Utilisateu**r "Mathilde-Keyse" et son **mot de passe**.
> **Cocher « Click to create a user certificate »**

En bas, entrer le **Nom du Certificat de l'Utilisateur** « CA-Bubu » et sélectionner le « Certificate authority » « CA-PC2S » puis cliquer sur « **Save** »



L'Utilisateur du VPN est créé.

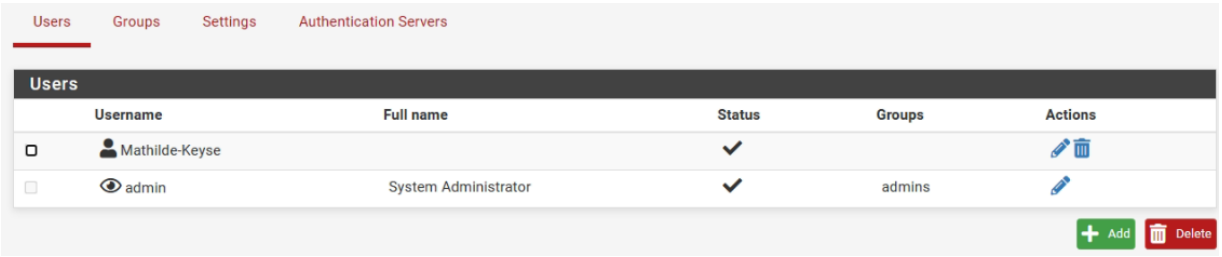
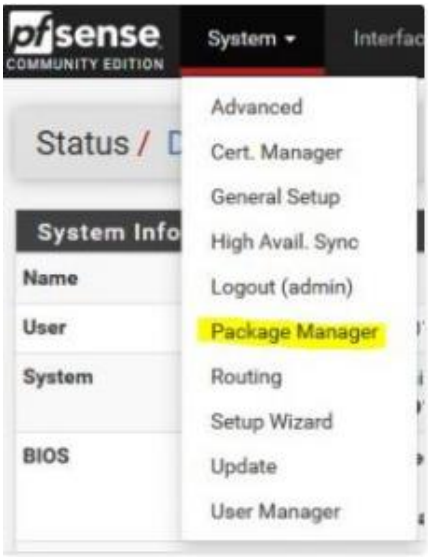


Figure 69 : PFSense VPN /Création des utilisateurs

Installation du package « OpenVPN-Client-Export » *(Utilitaire pour exporter la configuration Client au format .ovpn)*

Sélectionner : System > Package Manager



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

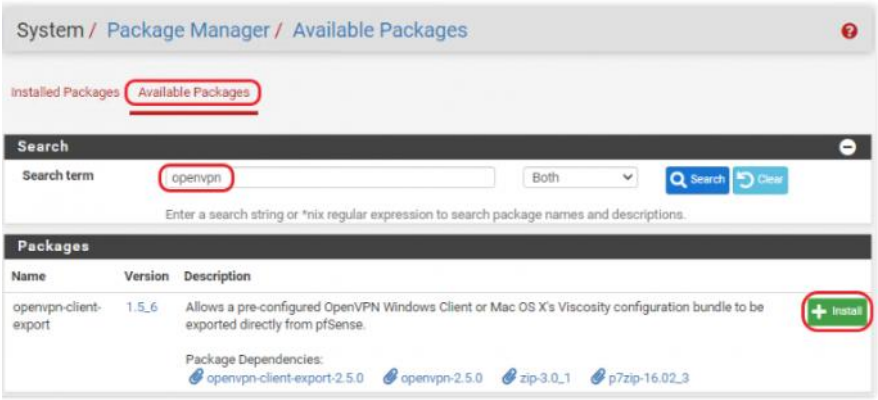
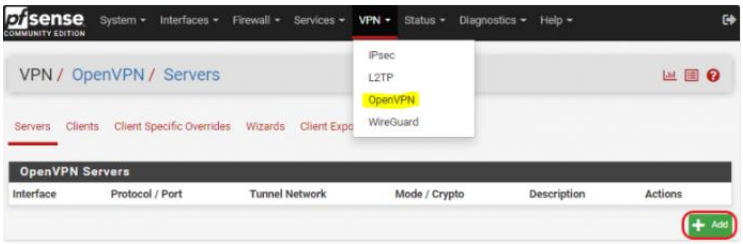


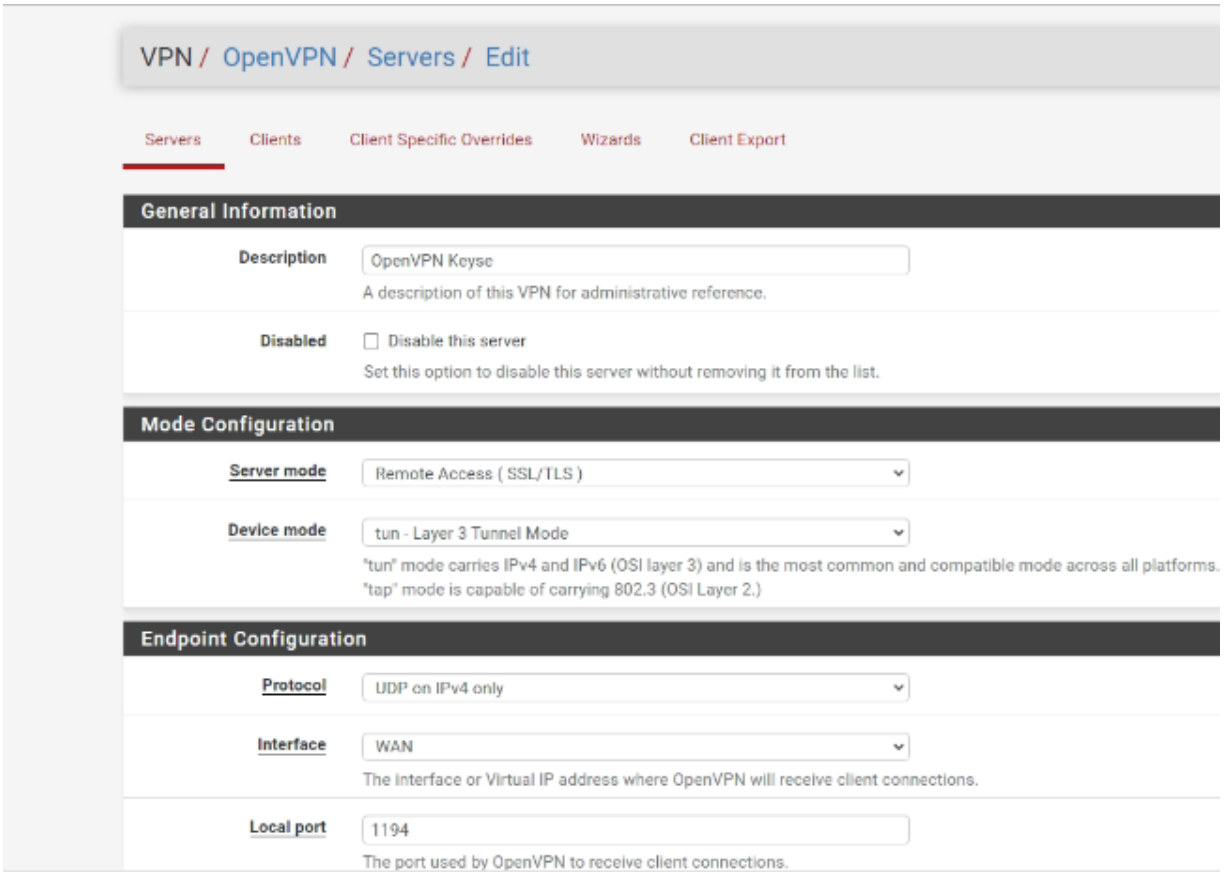
Figure 70 : PFSense VPN /Installation du package OpenVPN-client-export

Configurer OpenVPN

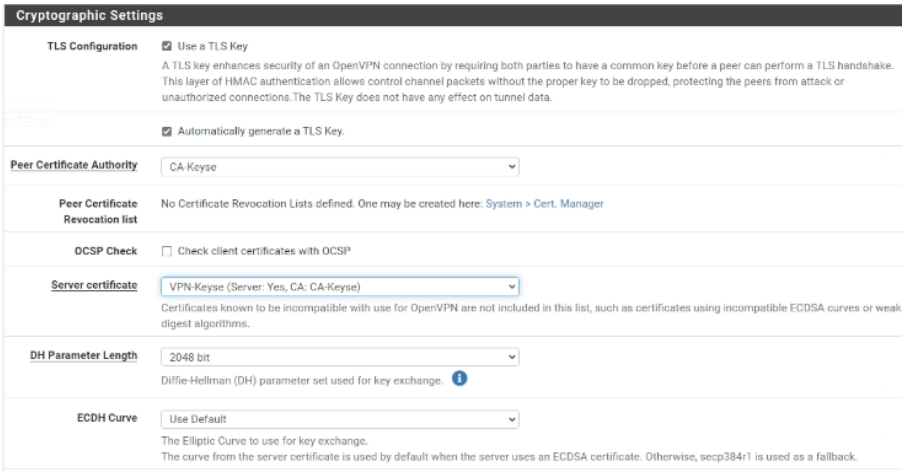
Sélectionner « VPN » > « **OpenVPN** » et cliquer sur « **+ Add** »



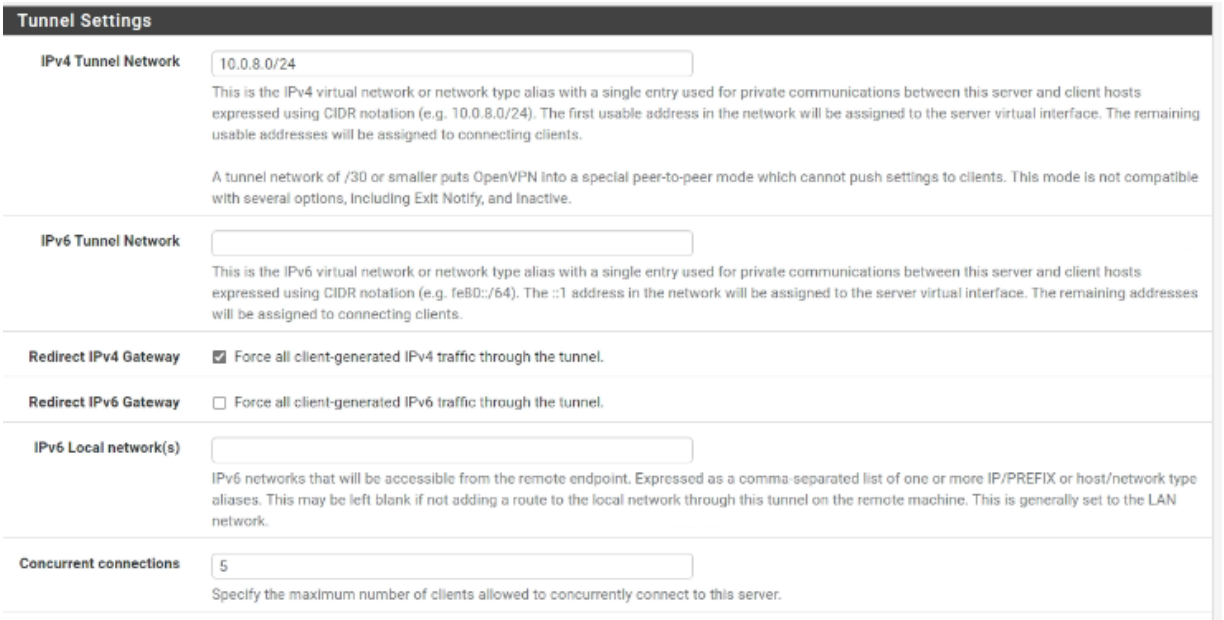
- Server mode : « **Remote Access (SSL/TLS)**«
- Local port : **1194** (Port par Défaut)
- Description : « **OpenVPN PC2S** » (Nom du Tunnel VPN)



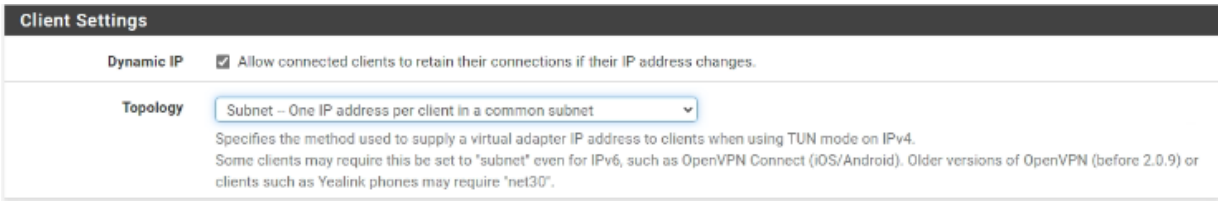
Sélectionner votre autorité de certification « **CA-Keyse** » dans « Peer Certificate Authority » et le certificat Server « **VPN-Keyse** » dans « Server certificate ».



- IPv4 Tunnel Network : **10.210.10.0/24** (Adresse du réseau VPN au format CIDR)
- **Cocher** « **Redirect IPv4 Gateway** » pour passer en mode full tunnel
- **Concurrent connections** : Nombre de connexions VPN simultanées

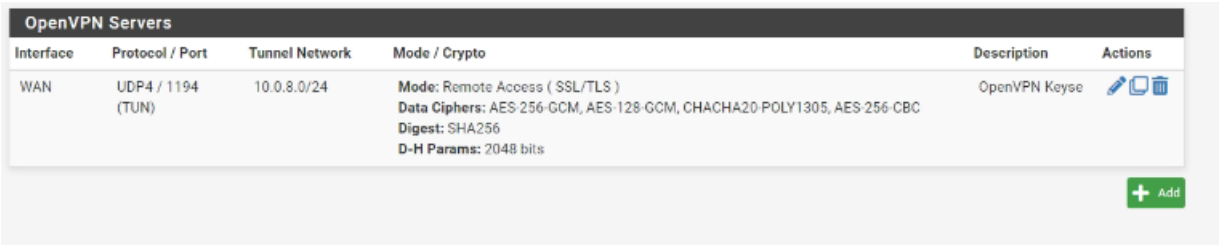


Cocher « **Dynamic IP** » et laisser « Topology » sur « Subnet – One IP address per client… »



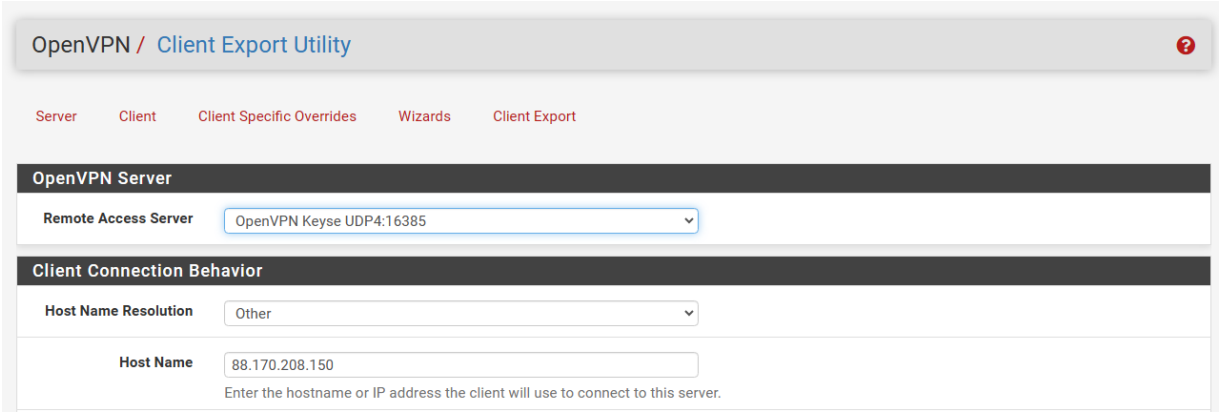
Indiquez « **auth-nocache** » dans « **Custom options**« . (Pas de mise en cache des identifiants)

Cliquer sur « **Save**« . Le Serveur VPN est créé.



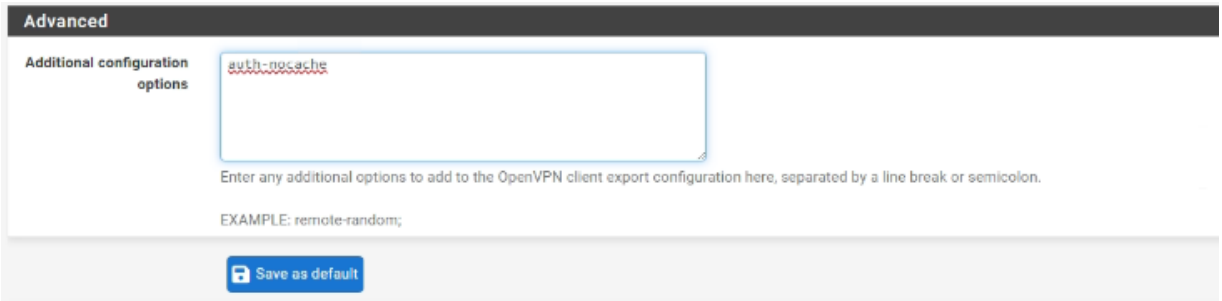
Exporter la configuration VPN pour un Client

Menu « **Client Export**« , Sélectionner « **Other** » pour « Host Name Resolution » et renseigner **votre IP WAN Publique** dans « Host Name »



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

Cliquer sur « **Save as default** »



Toujours dans le Menu « **Client Export**« , en bas de page, « **OpenVPN Clients** » > 2 Solutions pour l'installation des postes Clients :

- **1ère** solution : **Cliquer** sur « **Most Clients** » pour télécharger uniquement la configuration du Client à importer sur son ordinateur
- **2ème** solution : **Sélectionner** « **64-bit** » pour télécharger le **Package OpenVPN** (Logiciel + fichiers de configuration)

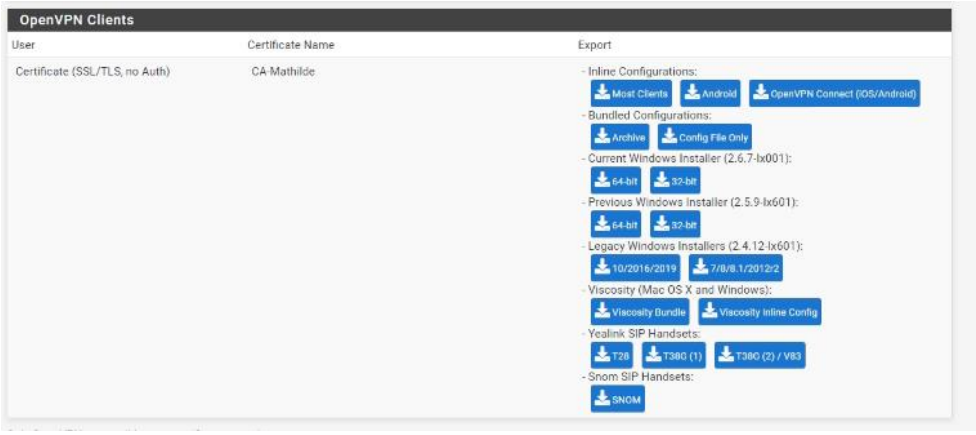
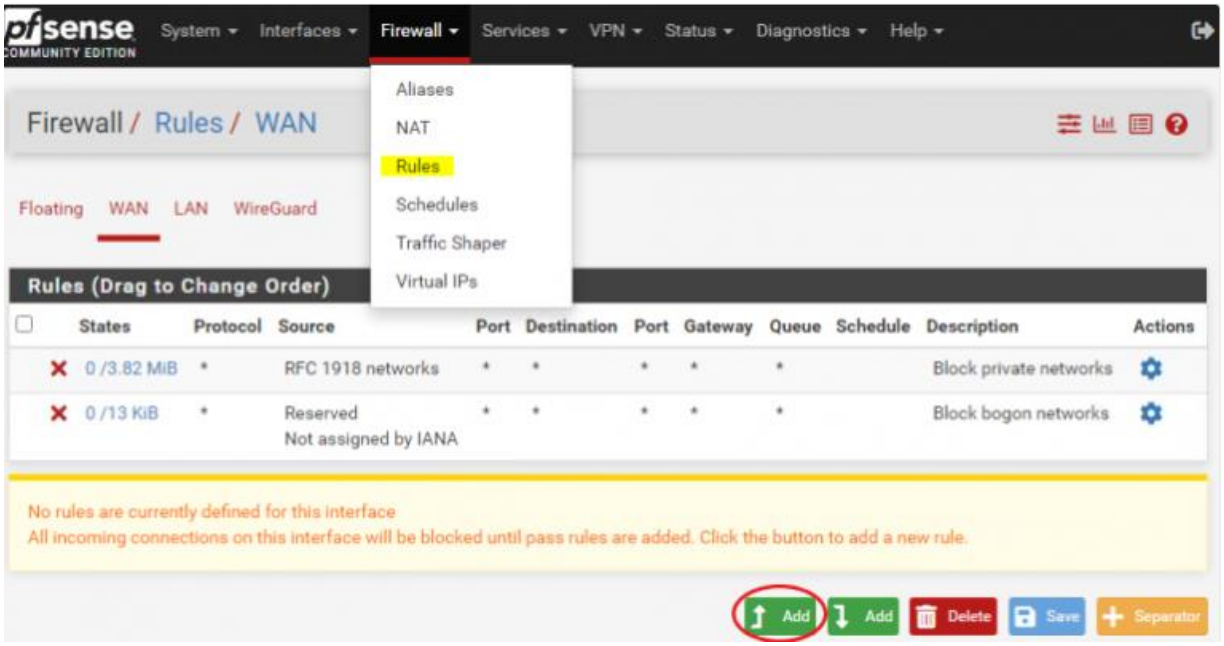


Figure 71 : PFSense VPN /Configuration du serveur OpenVPN

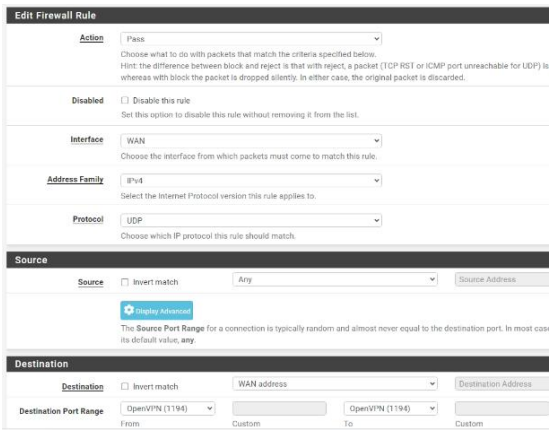
Configurer les règles du Pare-Feu pfSense

Firewall > Rules > WAN : cliquer sur "**+ Add**"



- Action : **Pass**
- Interface : **WAN**
- Protocol : **UDP**
- Source : **any**
- Destination : **WAN address**
- Destination Port Range : **OpenVPN (1194)**

Cliquer sur "**Save**" et valider "**Apply Changes**"



Firewall > Rules > OpenVPN : cliquer sur "**+ Add**"

- Action : **Pass**
- Interface : **OpenVPN**
- Protocol : **Any**
- Source : **any**
- Destination : **any**

Cliquer sur "**Save**" et valider "**Apply Changes**"

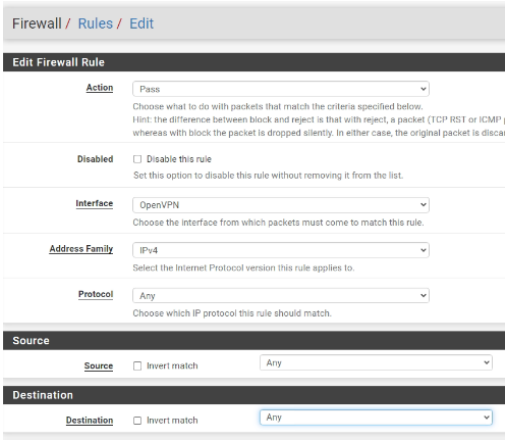


Figure 72 : PFSense VPN /Configuration des règles firewall pour OpenVPN

Redirection de port sur la Box, Routeur, Modem

Rediriger le port "**UDP 1194**" (dans mon cas le port « 16385 » car je ne peux utiliser seulement les ports au-dessus de 16384) arrivant de l'IP WAN Publique vers pfSense pour autoriser le VPN client.

Exemple sur Freebox OS 4.7 :

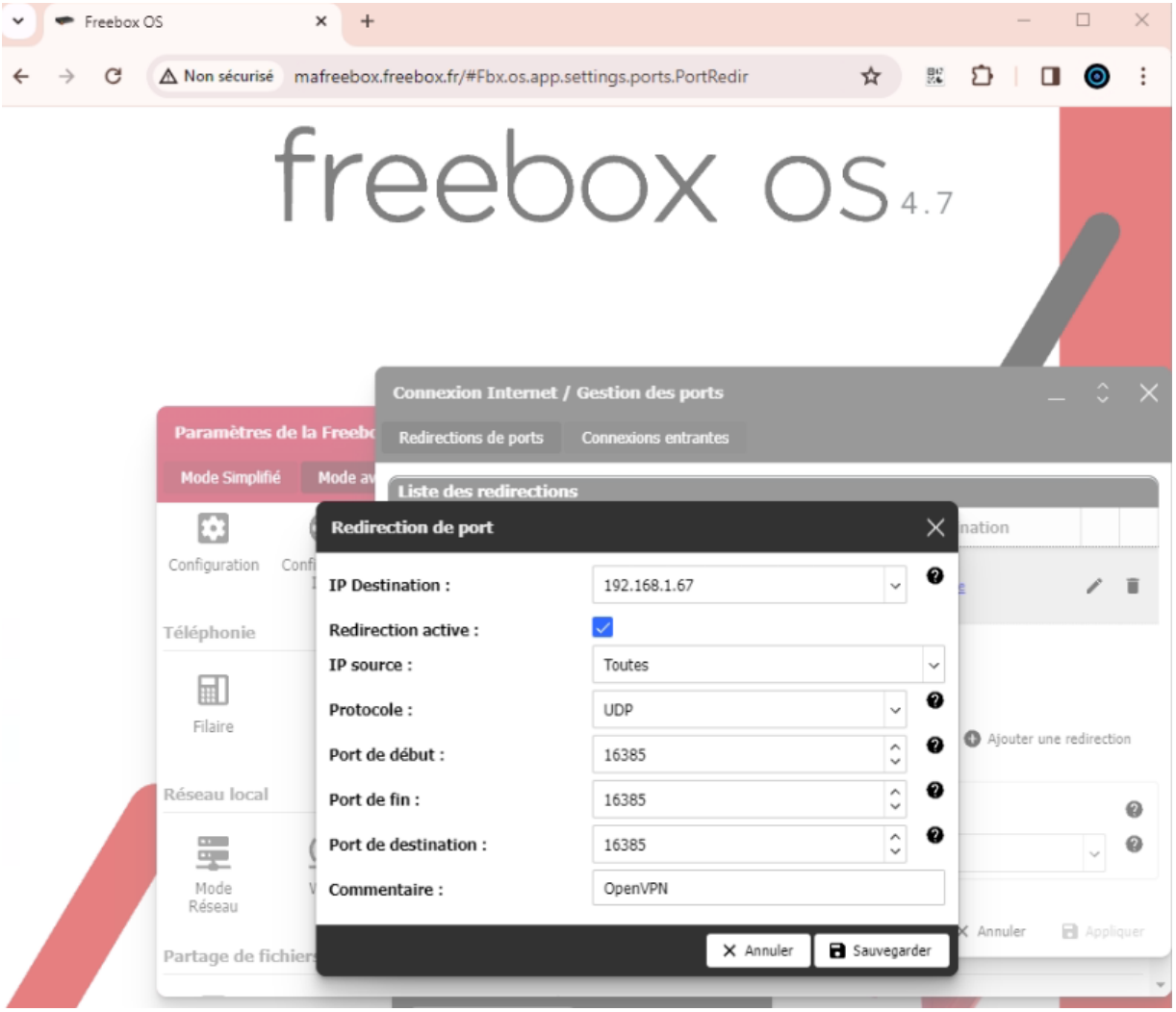


Figure 73 : PFSense VPN /Création de la redirection de port sur la boxe

10 *Configuration d'une sauvegarde des serveurs avec Veeam Backup*

Sélectionner le type «**Serveur** » car nous sauvegardons seulement nos 2 machines serveurs.
Sélectionner le mode **« Managed by backup serveur** » car nous souhaitons sauvegarder nos serveur depuis notre serveur Veeam.

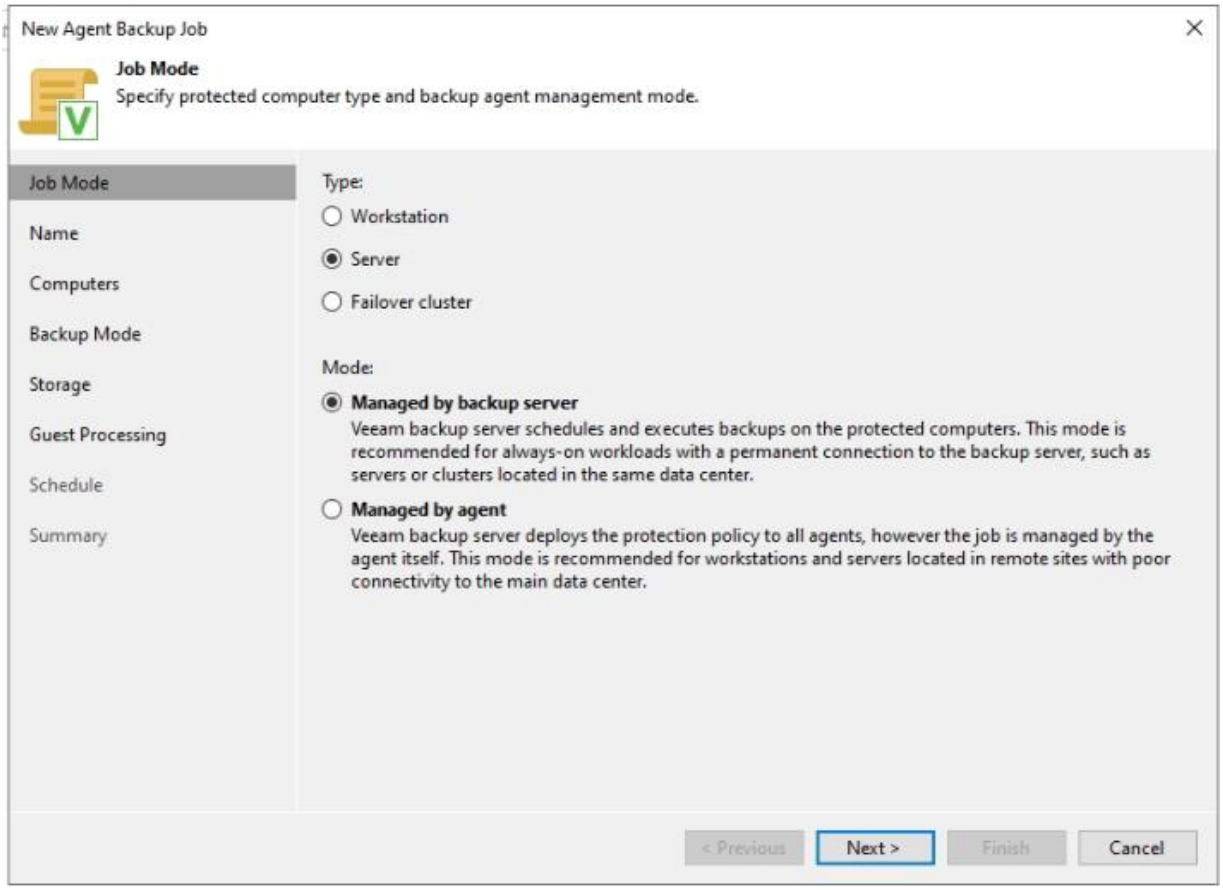


Figure 74 : Veeam / Création du job et configuration du mode

Attribuer un nom au job Créé.

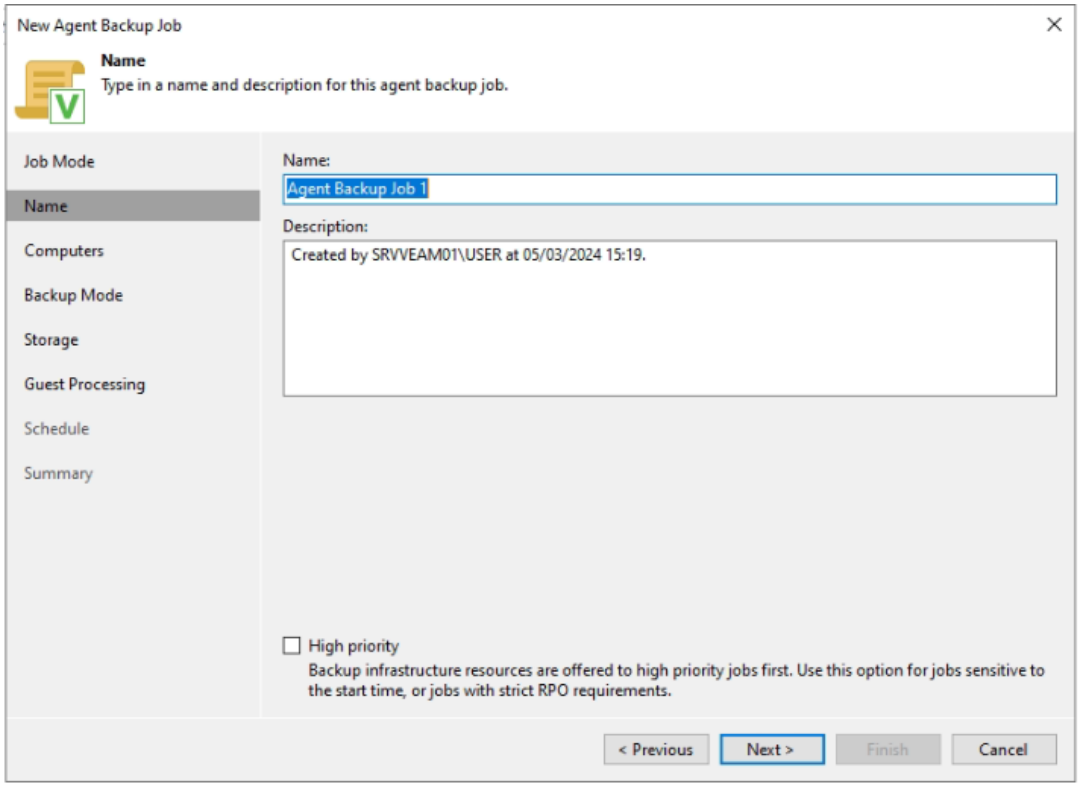


Figure 75 : Veeam / Nommage du Job

Sélectionner votre groupe de machines serveur ou vos machines serveurs.

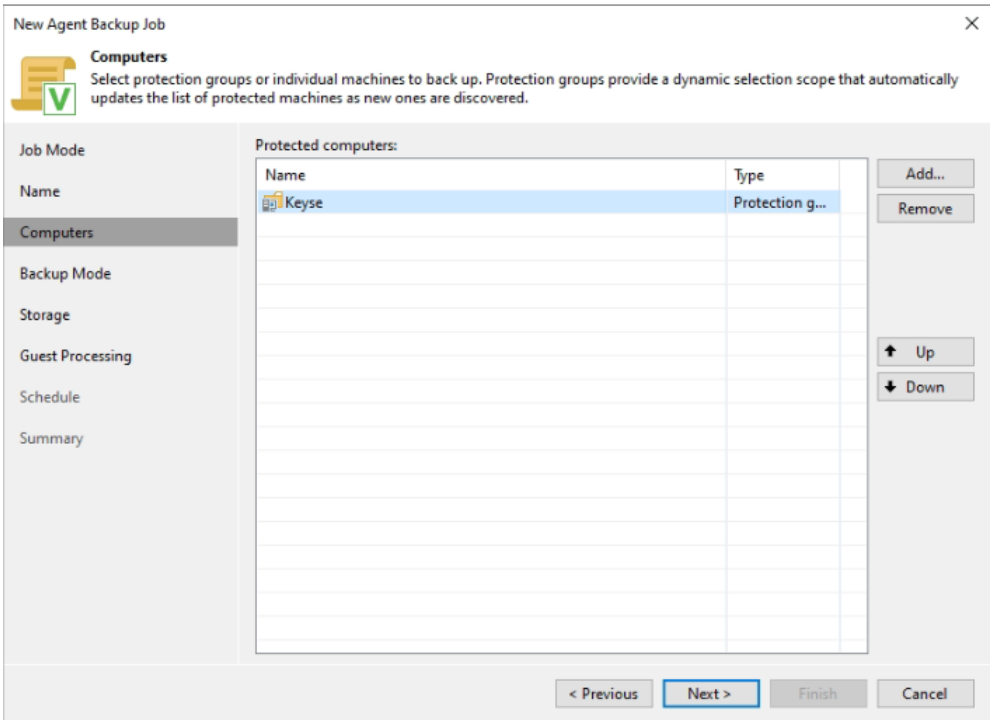


Figure 76 : Veeam / Sélections du groupe de machines serveur

Définir le mode de sauvegarde a utilisé (dans mon cas, une sauvegarde complète de la machine)

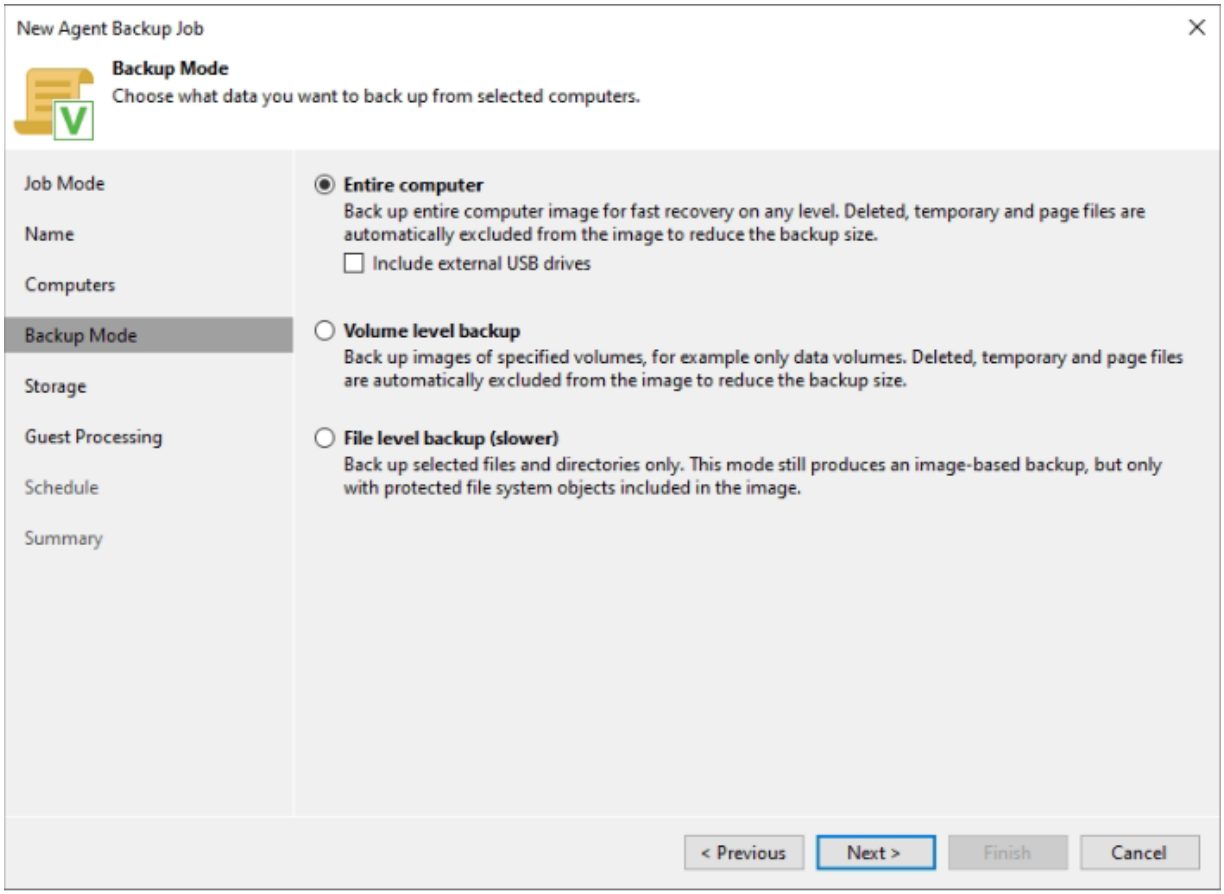


Figure 77 : Veeam / Sélections du type de sauvegarde

Cliqué sur « next », votre volume de stockage de la sauvegarde est sélectionné (dans mon cas un disque de 50Gb)

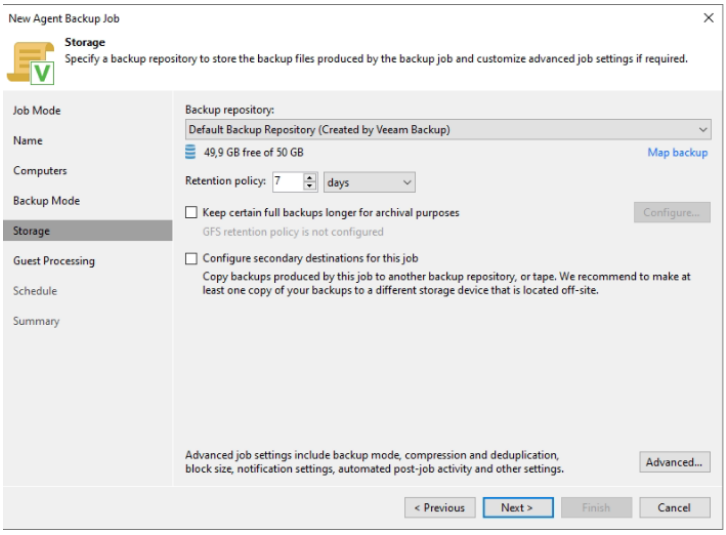


Figure 78 : Veeam / Sélections du volume de stockage de sauvegarde

Cliqué sur « next »

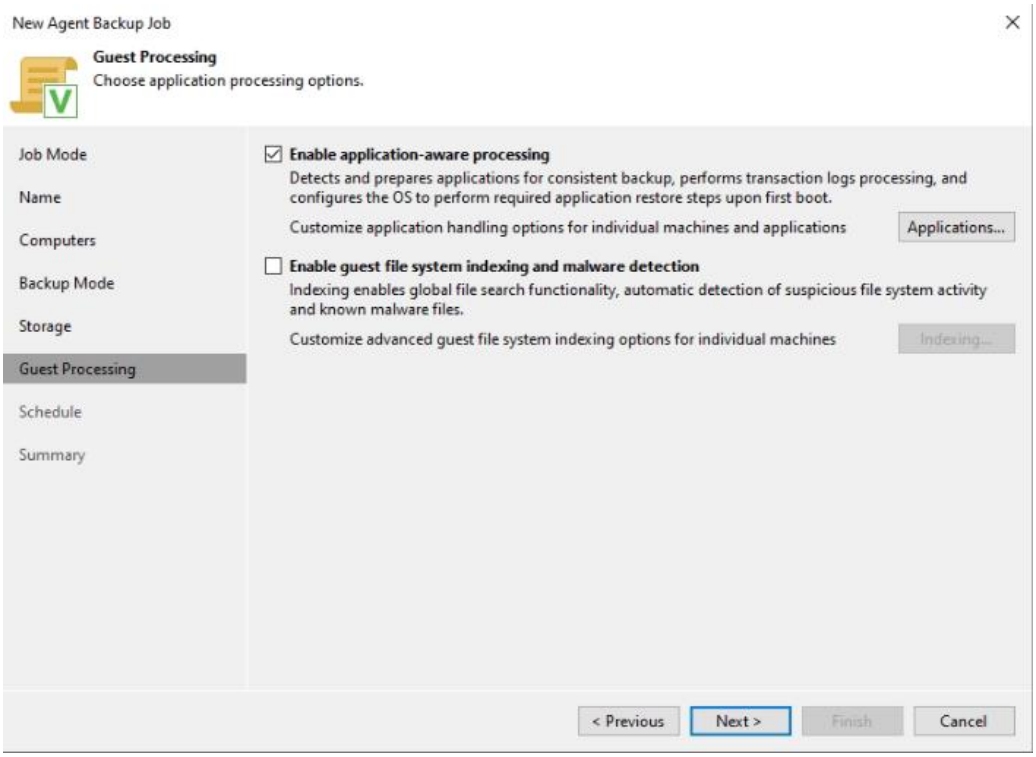


Figure 79 : Veeam / Guest Processing

Nous planifierons ensuite l'exécution du job de sauvegarde (dans mon cas : tout les jours a 22h00)

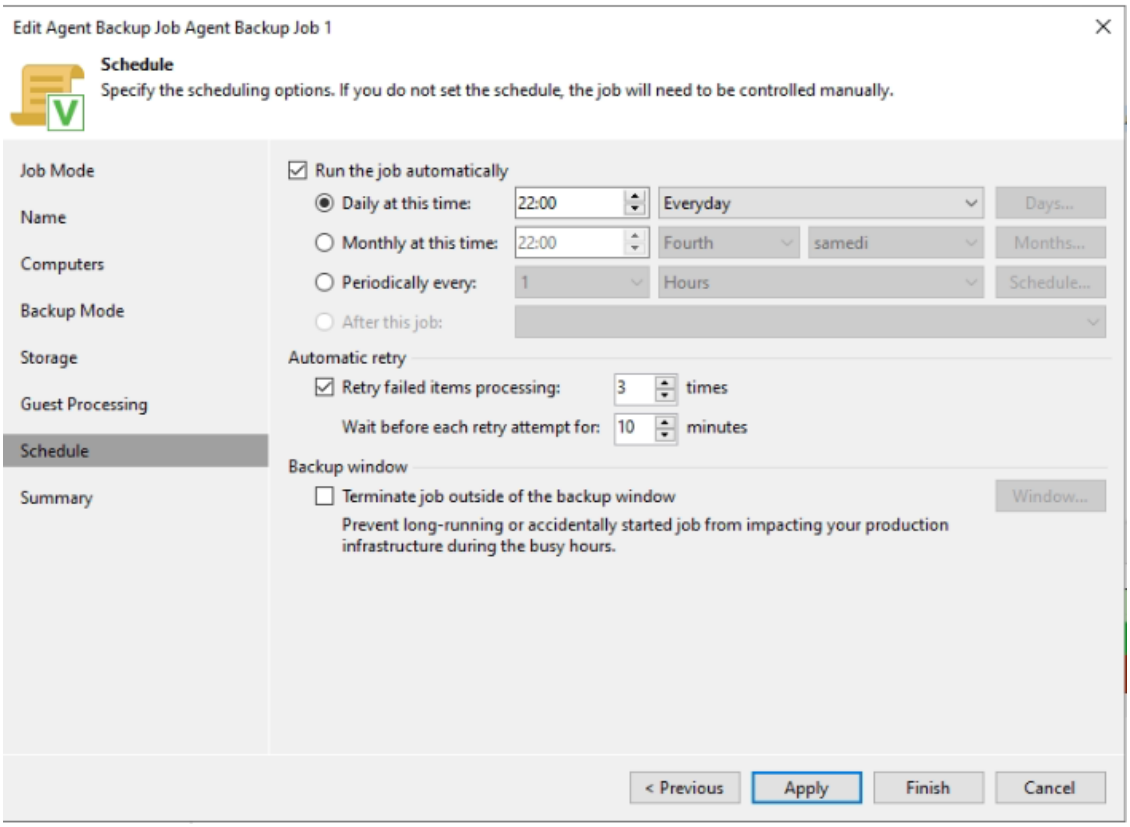


Figure 80 : Veeam / Planification du job de sauvegarde

Voici le résumé des paramètres du Job créé.

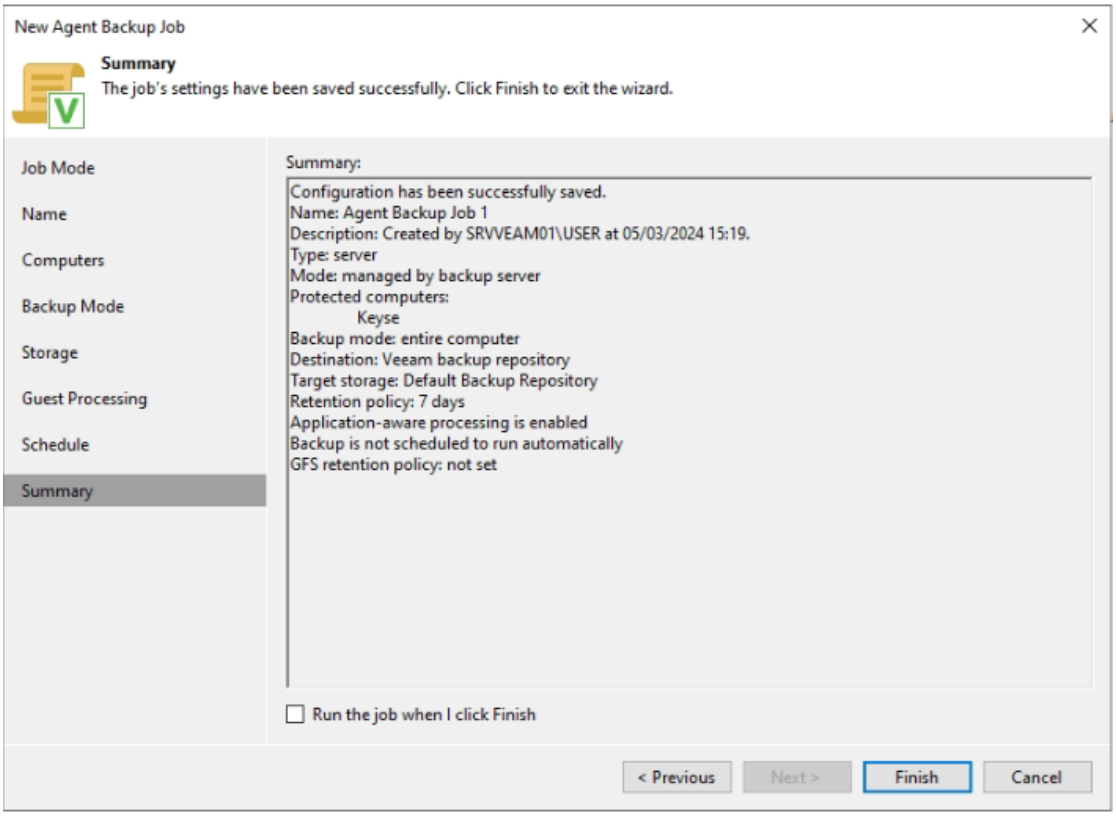


Figure 81 : Veeam / Résumé du Job

Nos serveurs ont été sauvegardé avec succès.

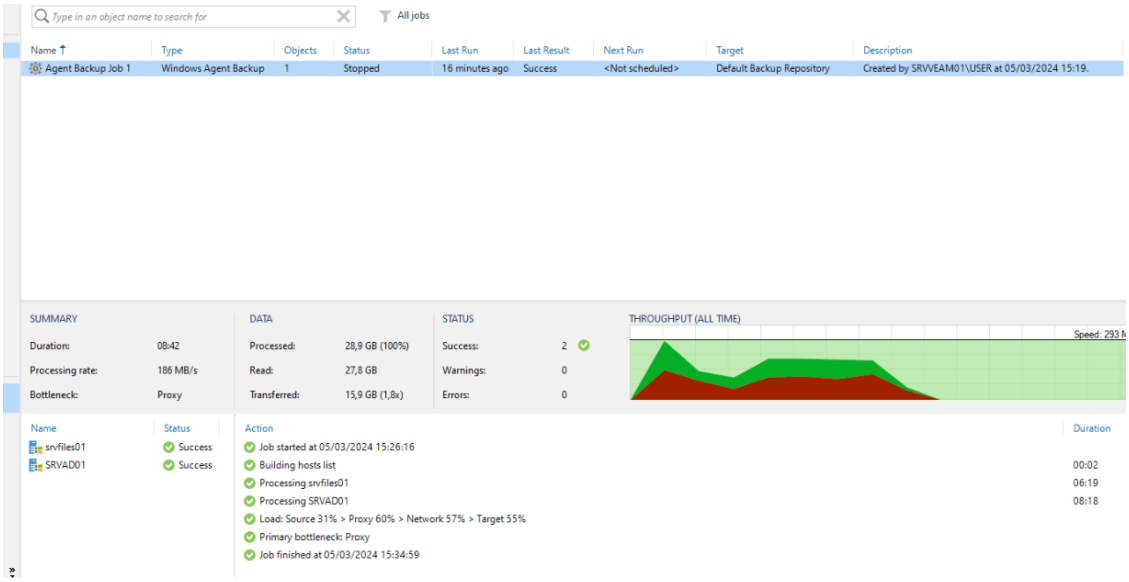


Figure 82 : Veeam / Sauvegarde effectuée