

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

Table des matières :

1 Introduction :	4
2 Installation Windows Server 2022 :	4
3 Contrôleur de domaine :	6
4 Rôles et fonctionnalités :	8
5 Configuration Active Directory :	13
5.1 Paramétrage DHCP :	16
5.2 Paramétrage DNS :	19
6 Utilisateurs :	21
7 Serveur de fichier :	38
8 GPO :	
9 Firewall PFSense :	
9.1 Mise en place d'un proxy transparent Squid avec filtrage d'URL :	
9.2 Configuration d'un tunnel VPN avec OpenVPN :	
10 Mise en place d'une sauvegarde des Serveurs avec Veeam	

Table des figures :

Figure 1 : Windows Server 2022 / langue	4
Figure 2 : Windows Server 2022 / Installer maintenant	4
Figure 3 : Windows Server 2022 / Standard Evaluation (Expérience utilisateur)	5
Figure 4 : Windows Server 2022 / Mise à niveau	5
Figure 5 : Windows Server 2022 / Installation de Windows	5
Figure 6 : Centre Réseau et partage / propriétés Ethernet	6
Figure 7 : Gestion de réseau Protocole TCP/IPv4	6
Figure 8 : Paramètres IP Protocole TCP/IPv4	7
Figure 9 : Gestionnaire de serveur / Serveur local	7
Figure 10 : Propriétés système / modification du nom du PC	8
Figure 11 : « Redémarrer maintenant »	8
Figure 12 : Gérer / ajout des rôles et fonctionnalités	8
Figure 13 : Assistant / Avant de commencer	9
Figure 14 : Assistant / Type d'installation	9
Figure 15 : Assistant / Sélection du serveur	10
Figure 16 : Assistant / Rôles de serveurs	10
Figure 17 : Assistant / (AD DS) Services de domaine Active Directory	11
Figure 18 : Assistant / Serveur (DNS) Domain Name system	11
Figure 19 : Assistant / Serveur (DHCP) Dynamic host configuration Protocol	12
Figure 20 : Assistant / Démarrage de l'installation	12
Figure 21 : Assistant / Installation terminée	13
Figure 22 : Active Directory / Configuration de déploiement	13
Figure 23 : Active Directory / Option du contrôleur de domaine	14
Figure 24 : Active Directory / Option DNS	14
Figure 25 : Active Directory / Options supplémentaires	15
Figure 26 : Active Directory / Chemin d'accès	15
Figure 27 : Active Directory / Examiner les options	16
Figure 28 : Active Directory / Vérification de la configuration requise	16
Figure 29 : Installer puis redémarrer	17
Figure 30 : Notification / Avancement de la configuration	17
Figure 31 : DHCP / « Terminer la configuration DHCP »	17
Figure 32 : DHCP / Description	18
Figure 33 : DHCP / Autorisation	18
Figure 34 : DHCP / Résumé.....	19
Figure 35 : Fermer puis redémarrer	19
Figure 36 : Paramétrage adresse IP / VLAN 22	20
Figure 37 : Routeur / Passerelle par défaut	20
Figure 38 : Nom de domaine / serveur DNS	21
Figure 40 : Contenu serveur DHCP / Etendues créées	22
Figure 41 : DNS / Nouvelle zone de recherche inversée	22
Figure 42 : Assistant nouvelle zone terminée	23
Figure 43 : Vérification / Zone de recherche inversée	23
Figure 44 : Active Directory / Utilisateurs et ordinateurs	24
Figure 45 : Active Directory / création des utilisateurs	25

Figure 46 : Active Directory / création utilisateur Lucas	25
Figure 47 : Active Directory / création utilisateur MDP	25
Figure 48 : Active Directory / création unité d'organisation	26
Figure 49 : Active Directory / Groupe Administration avec utilisateurs	26
Figure 50 : Active Directory / Groupe électronique avec utilisateurs	26
Figure 51 : Active Directory / Groupe mécanique avec utilisateurs	27
Figure 52 : Serveur de fichier /Configuration du Pool de stockage	
Figure 53 : Serveur de fichier /Configuration du Disque virtuel	
Figure 54 : Serveur de fichier /Configuration du Volume	
Figure 55 : Serveur de fichier /Configuration du Partage	
Figure 56 : Serveur de fichier /Configuration des autorisations	
Figure 57 : GPO /Mappage des lecteurs pour les groupe Administratif, Comptabilité et Conseiller	
Figure 58 : GPO /Mappage d'un lecteur réseau d'un espace personnel pour chaque Utilisateur du groupe Conseiller	
Figure 59 : GPO /Mappage d'un Fond d'écran sur les postes	
Figure 60 : PFSense /Installation de PFSense	
Figure 61 : PFSense /Configuration de l'interface Lan de PFSense	
Figure 62 : PFSense /Configuration de PFSense	
Figure 63 : PFSense Filtrage /Installation des packages	
Figure 64 : PFSense Filtrage /Configuration du certificat	
Figure 65 : PFSense Filtrage /Configuration de Squid	
Figure 66 : PFSense Filtrage /Configuration de Squidguard	
Figure 67 : PFSense VPN /Création de l'autorité de certification	
Figure 68 : PFSense VPN /Création du certificat serveur	
Figure 69 : PFSense VPN /Création des utilisateurs	
Figure 70 : PFSense VPN /Installation du package OpenVPN-client-export	
Figure 71 : PFSense VPN /Configuration du serveur OpenVPN	
Figure 72 : PFSense VPN /Configuration des règles firewall pour OpenVPN	
Figure 73 : PFSense VPN /Création de la redirection de port sur la boxe	
Figure 74 : Veeam / Création du job et configuration du mode	
Figure 75 : Veeam / Nommage du Job	
Figure 76 : Veeam / Sélections du groupe de machines serveur	
Figure 77 : Veeam / Sélections du type de sauvegarde	
Figure 78 : Veeam / Sélections du volume de stockage de sauvegarde	
Figure 79 : Veeam /	
Figure 80 : Veeam / Planification du job de sauvegarde	
Figure 81 : Veeam / Résumé du Job	
Figure 82 : Veeam / Sauvegarde effectuée	

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 :

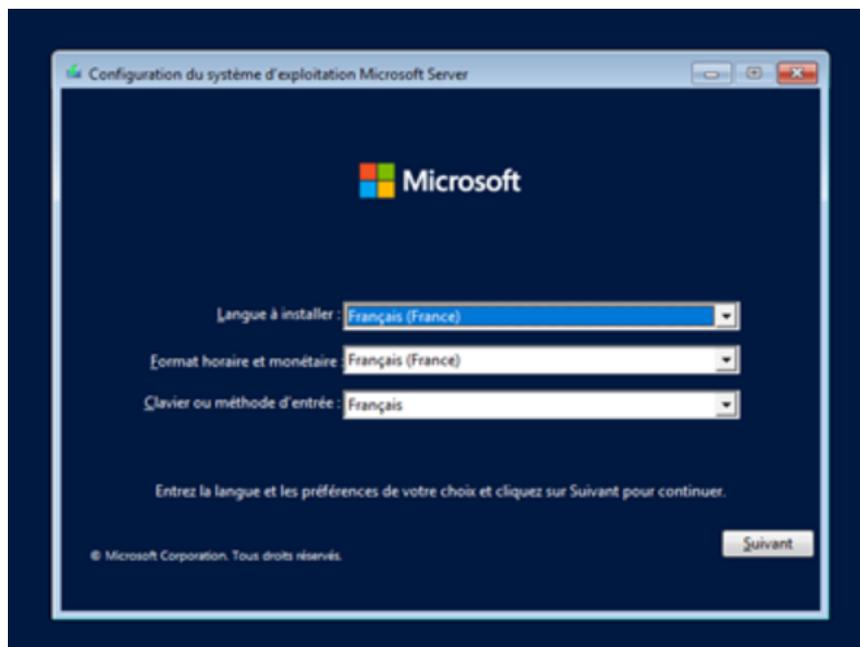


Figure 1 : Windows Server 2016 / langue

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.

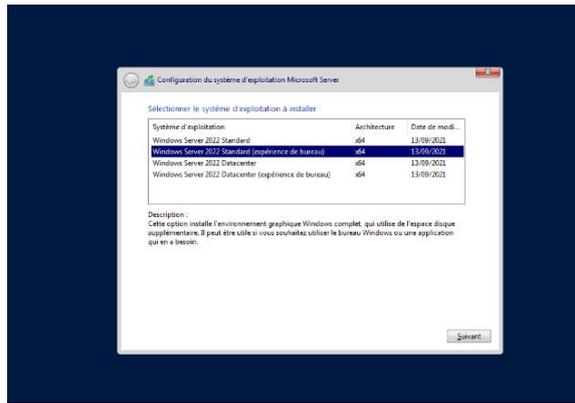


Figure 3 : Windows Server 2016 / Standard Evaluation (Expérience utilisateur)

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)**.

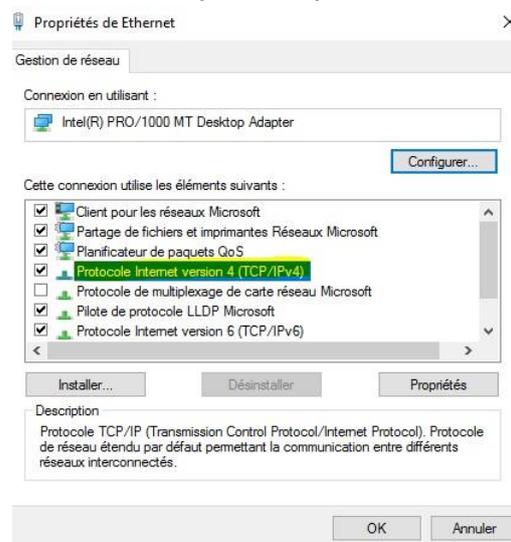
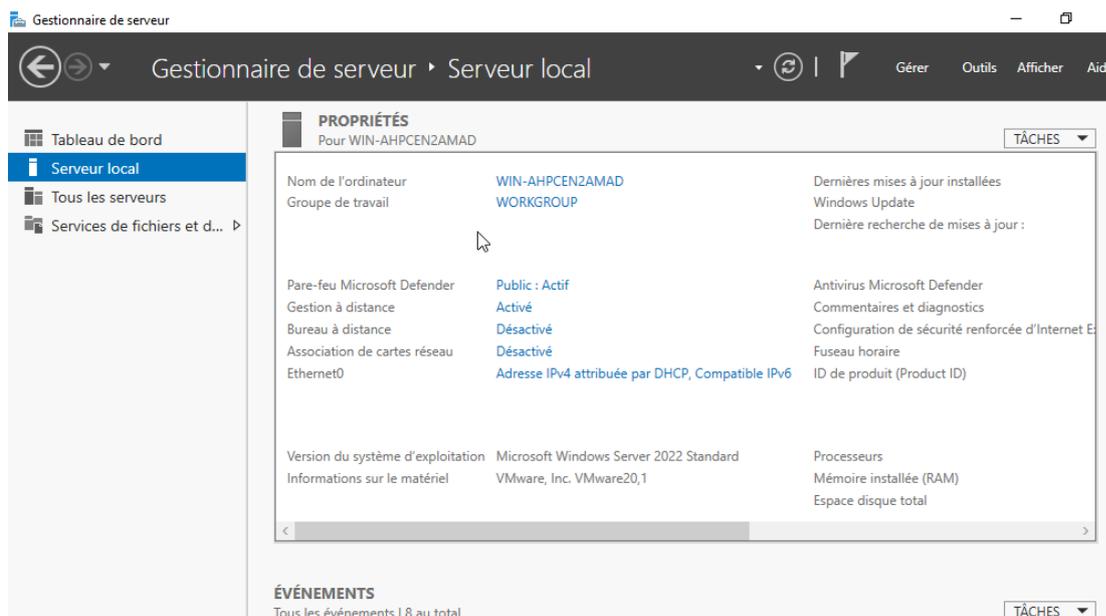


Figure 7 : Gestion de réseau Protocole TCP/IPv4

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.

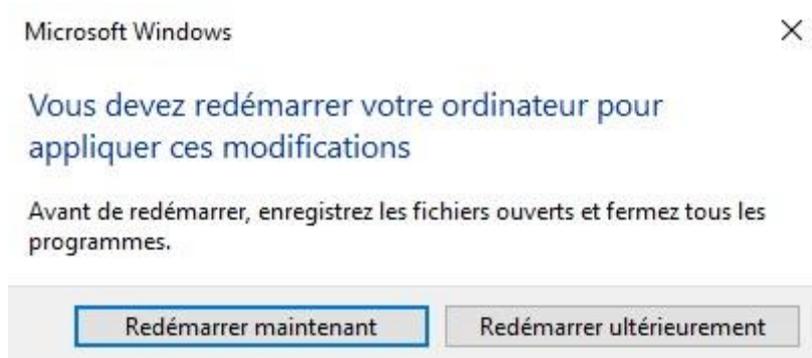


Figure 11 : « Redémarrer maintenant »

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.

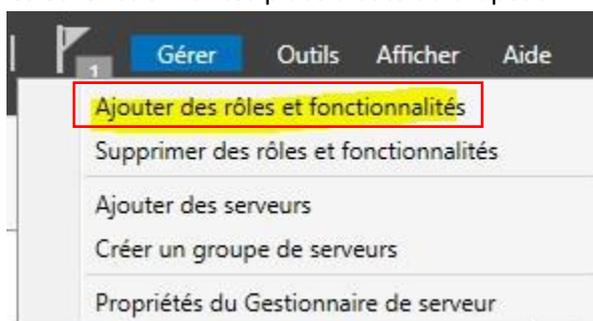


Figure 12 : Gérer / ajout des rôles et fonctionnalités

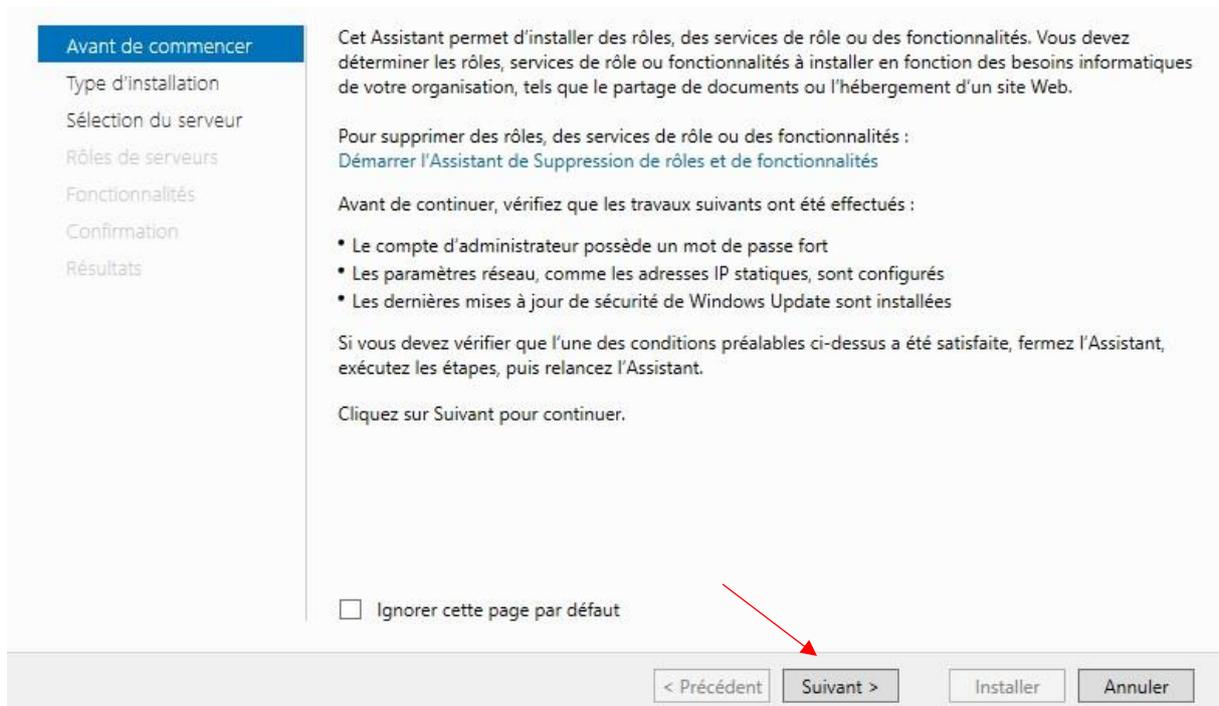


Figure 13 : Assistant / Avant de commencer

Installation basée sur un rôle ou une fonctionnalité.

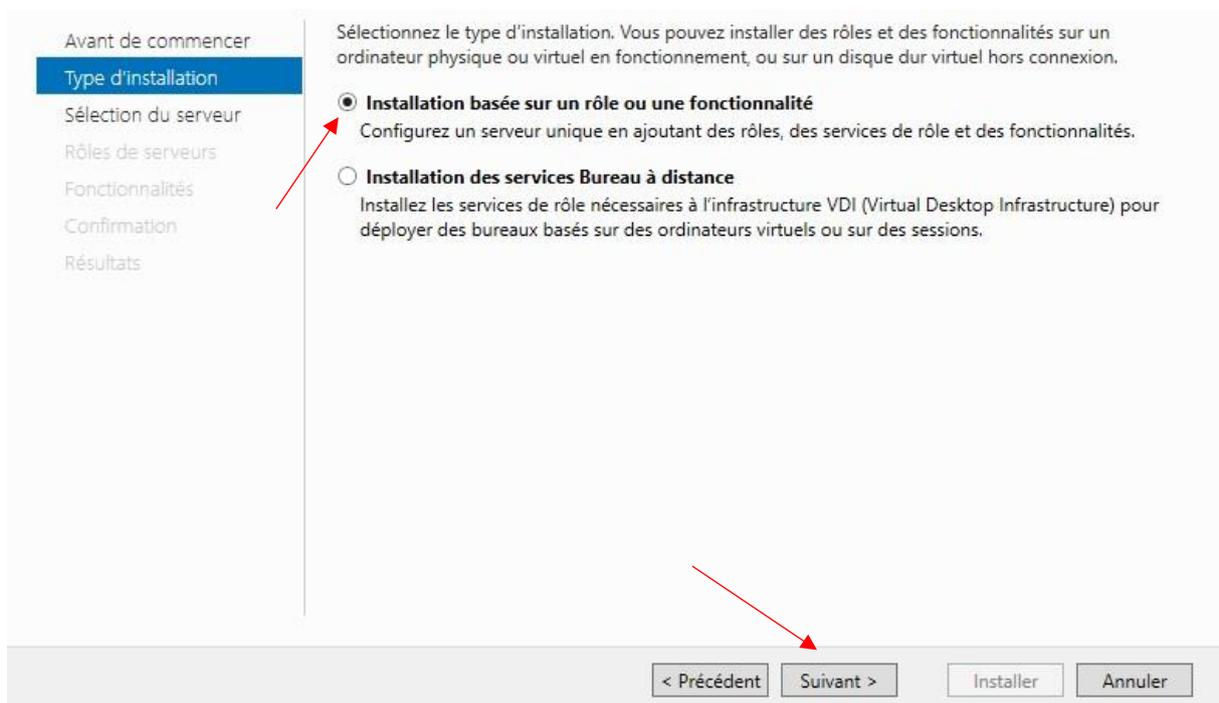


Figure 14 : Assistant / Type d'installation

Sélectionner un serveur du pool de serveurs :

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

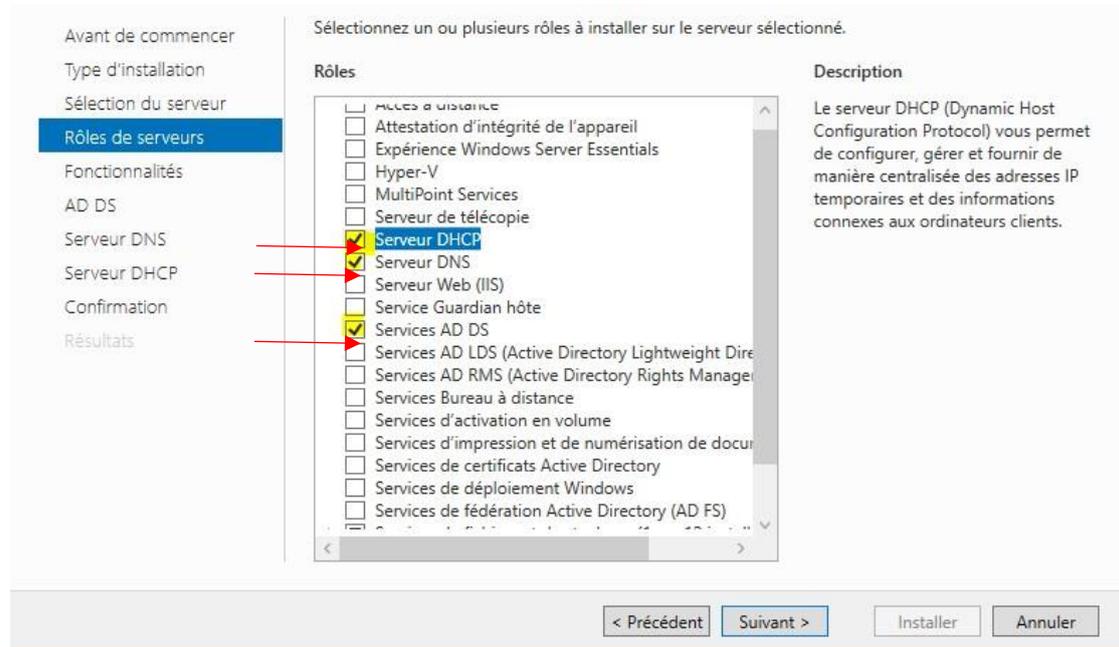


Figure 16 : Assistant / Rôles de serveurs

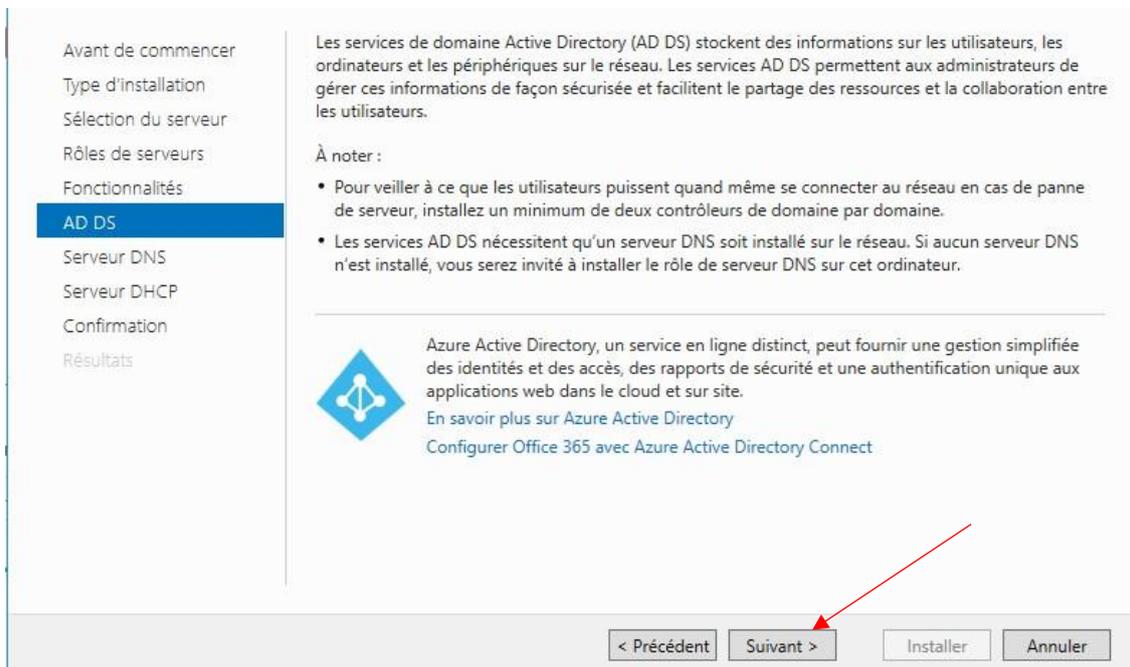


Figure 17 : Assistant / (AD DS) Services de domaine Active Directory

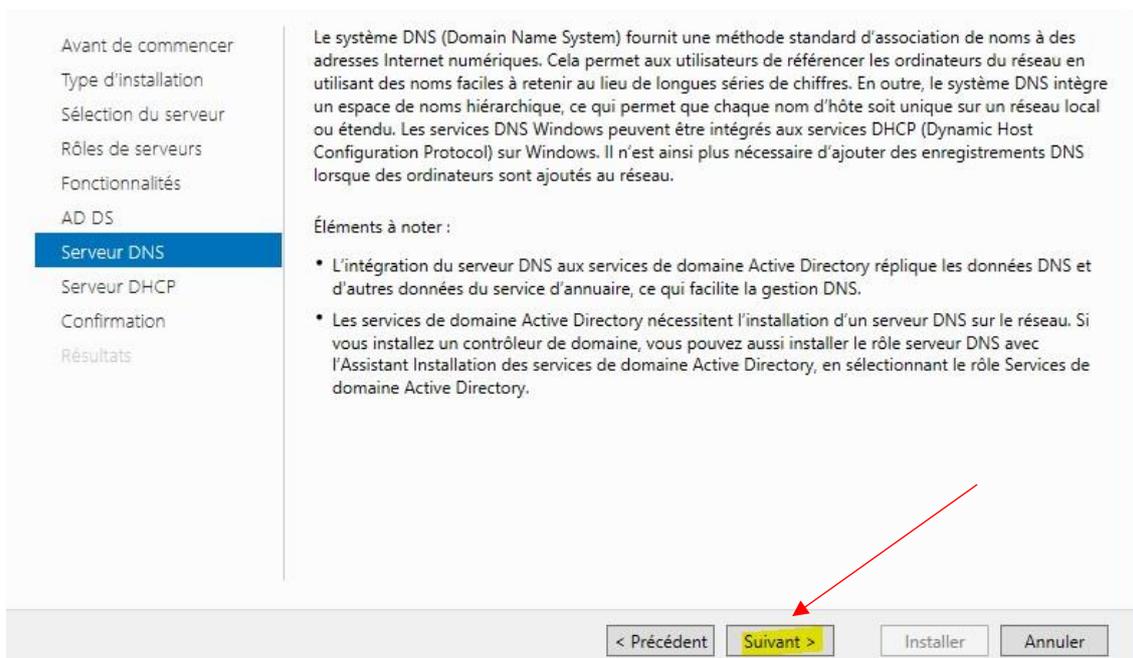


Figure 18 : Assistant / Serveur (DNS) Domain name system

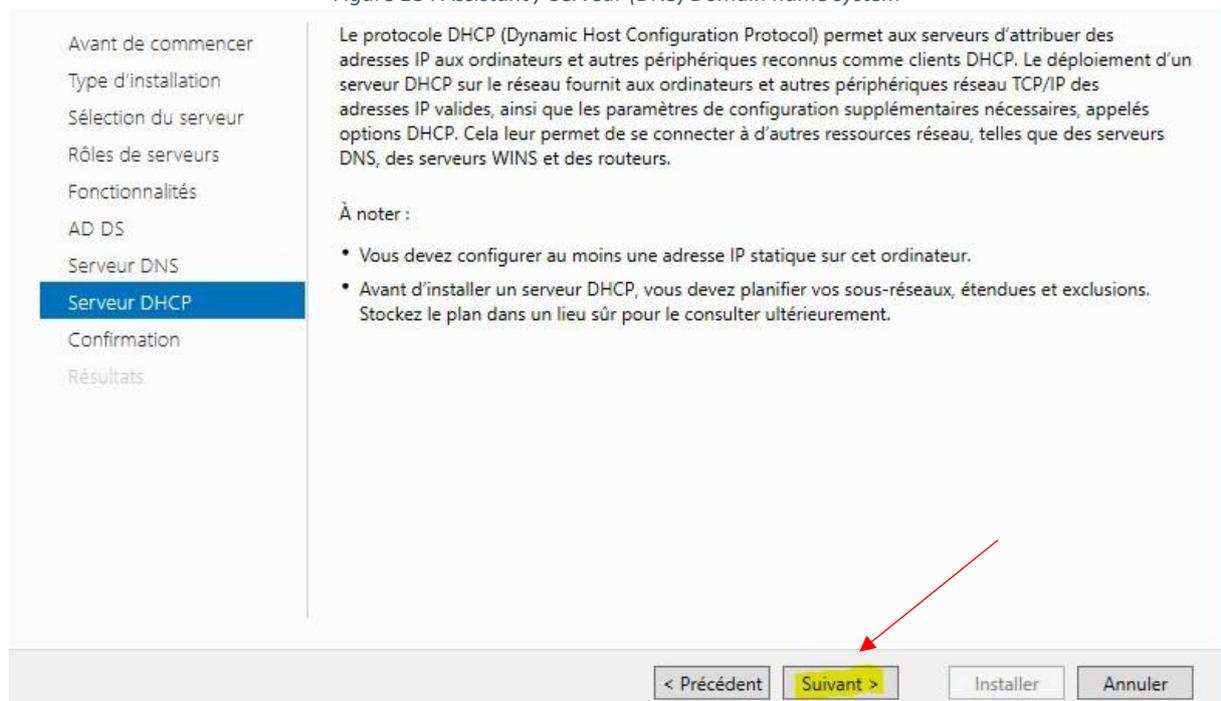


Figure 19 : Assistant / Serveur (DHCP) Dynamic host configuration protocol

L'installation est à présent en cours de chargement...

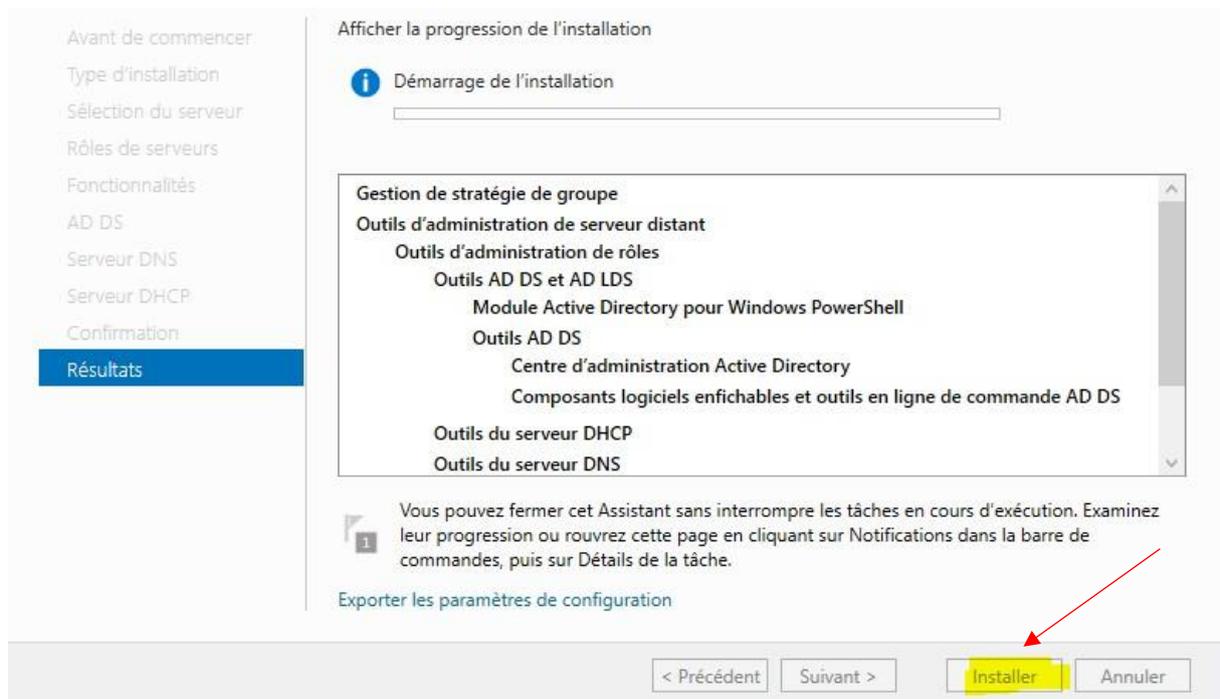
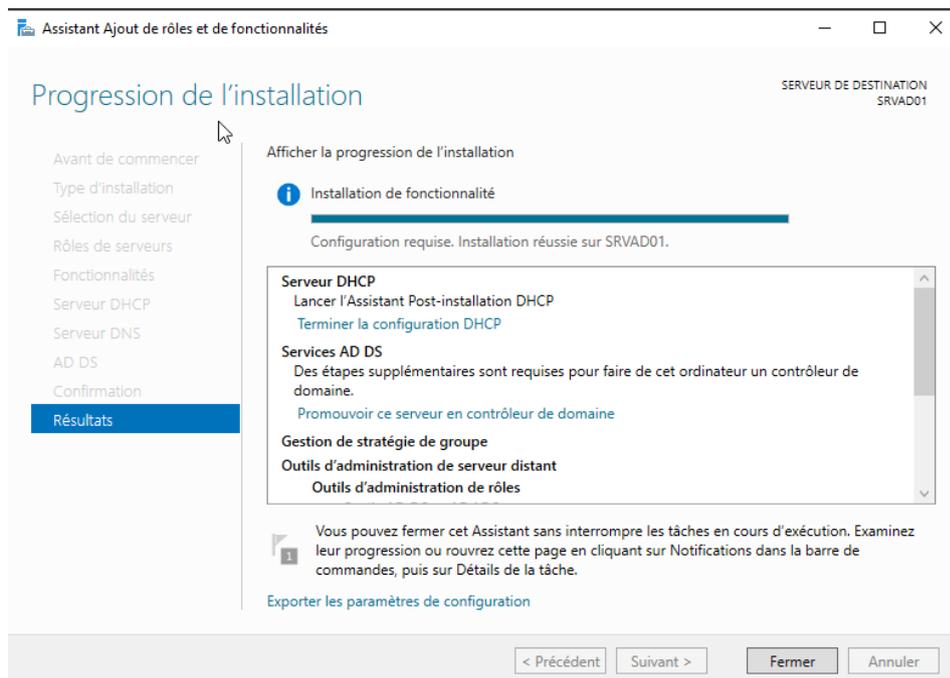


Figure 20 : Assistant / Démarrage de l'installation

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

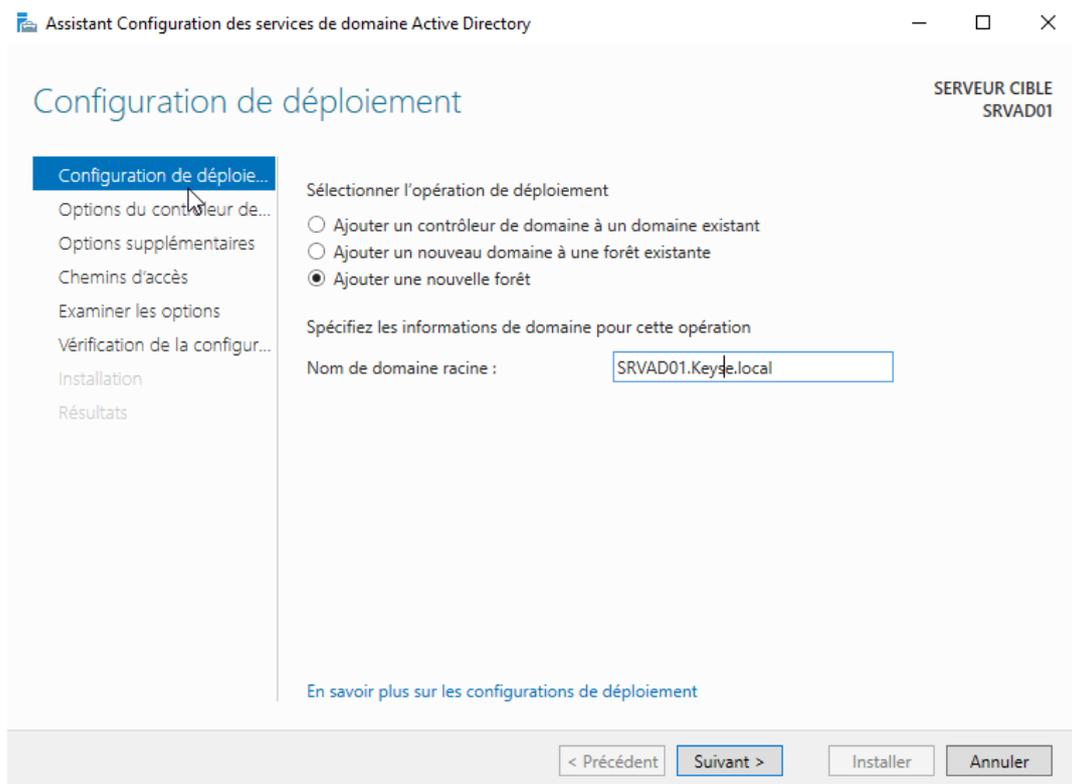


Figure 22 : Active Directory / Configuration de déploiement

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

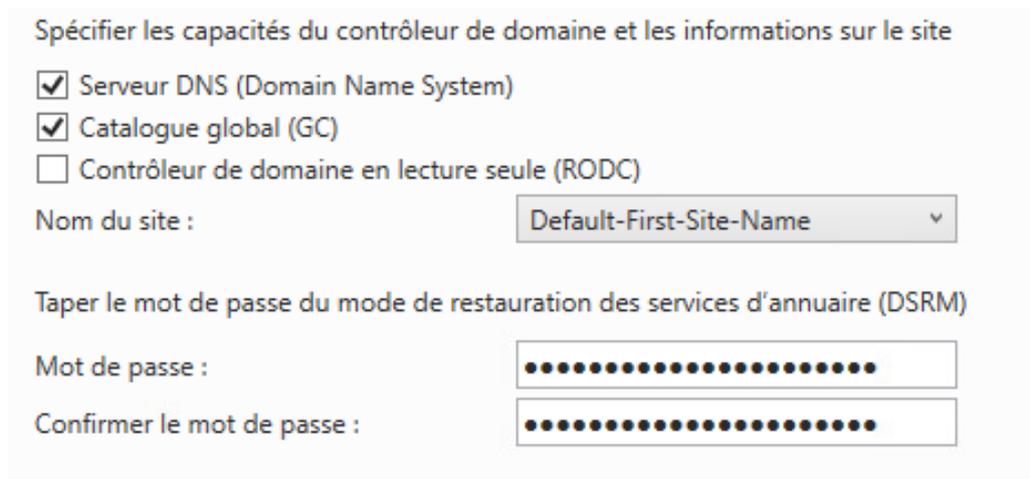


Figure 23 : Active Directory / Option du contrôleur de domaine

Pas de création de délégation DNS.

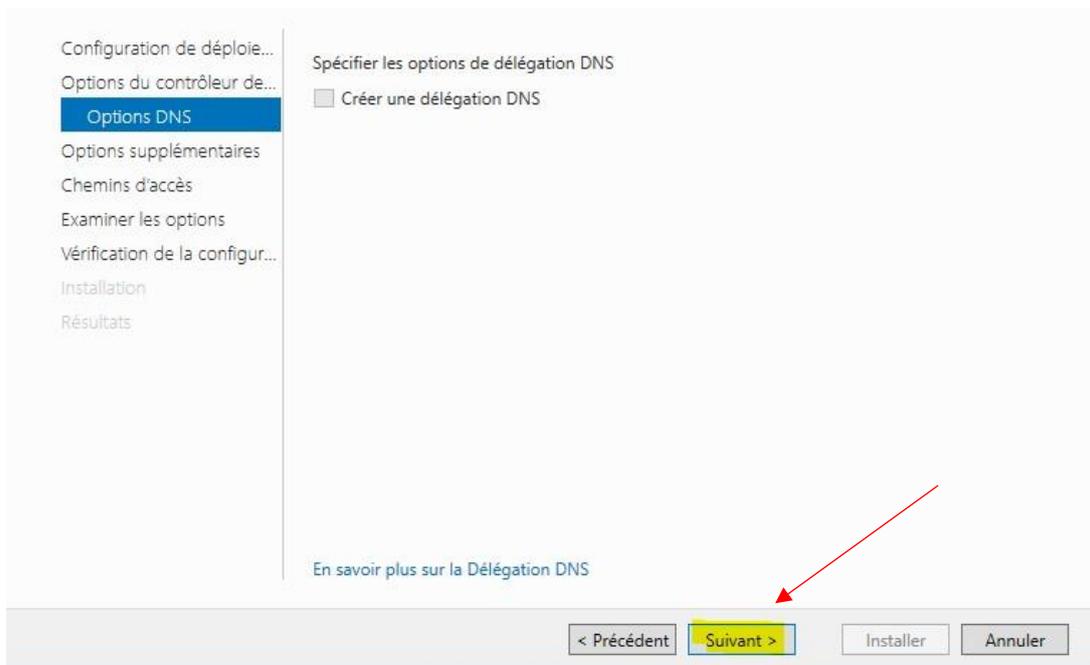


Figure 24 : Active Directory / Option DNS

Aucune modification pour les chemins d'accès :

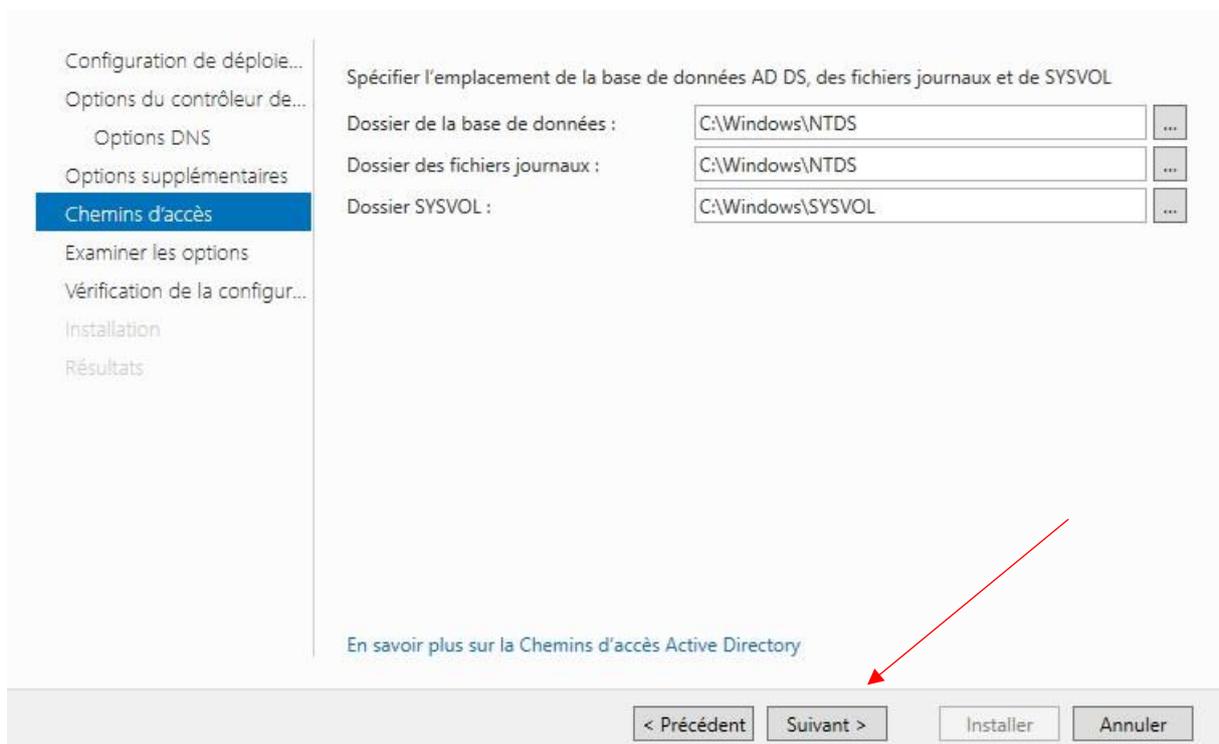


Figure 26 : Active Directory / Chemin d'accès

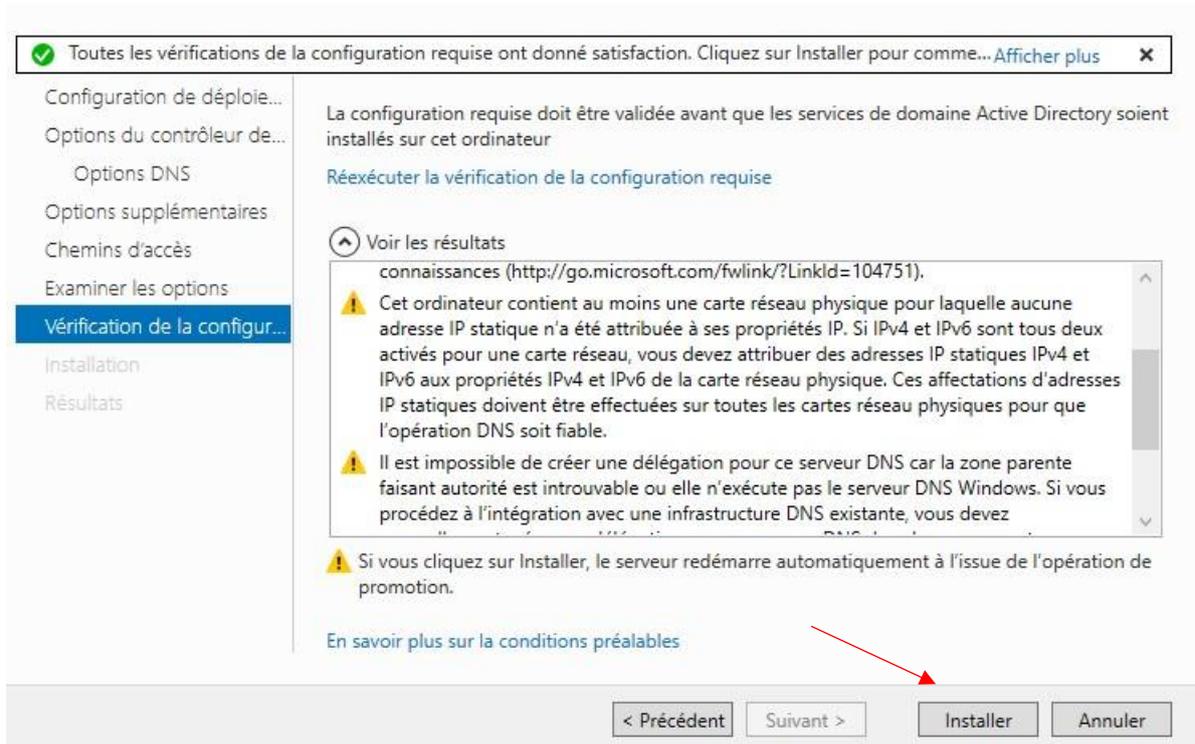


Figure 28 : Active Directory / Vérification de la configuration requise

Après l'installation, le redémarrage se fera automatiquement.

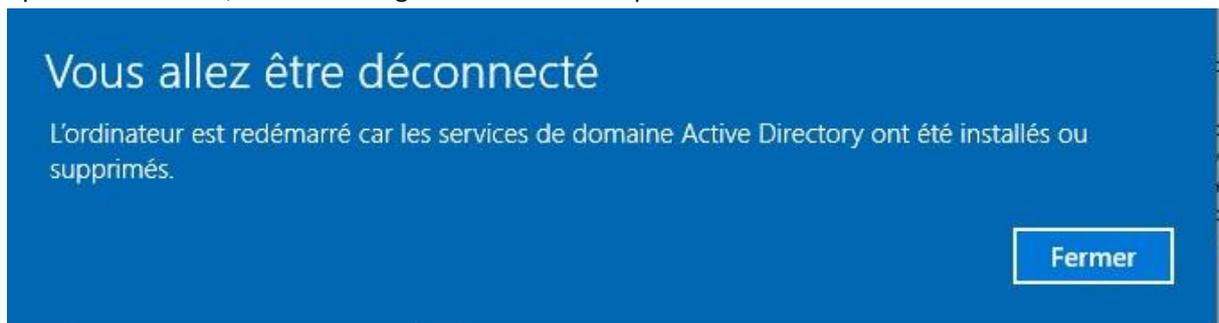


Figure 29 : Installer puis redémarrer

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 :

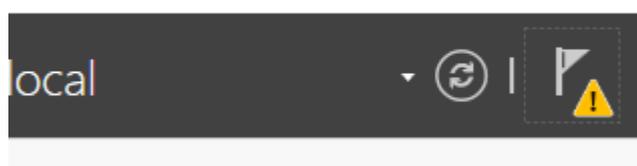


Figure 30 : Notification / Avancement de la configuration

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 »

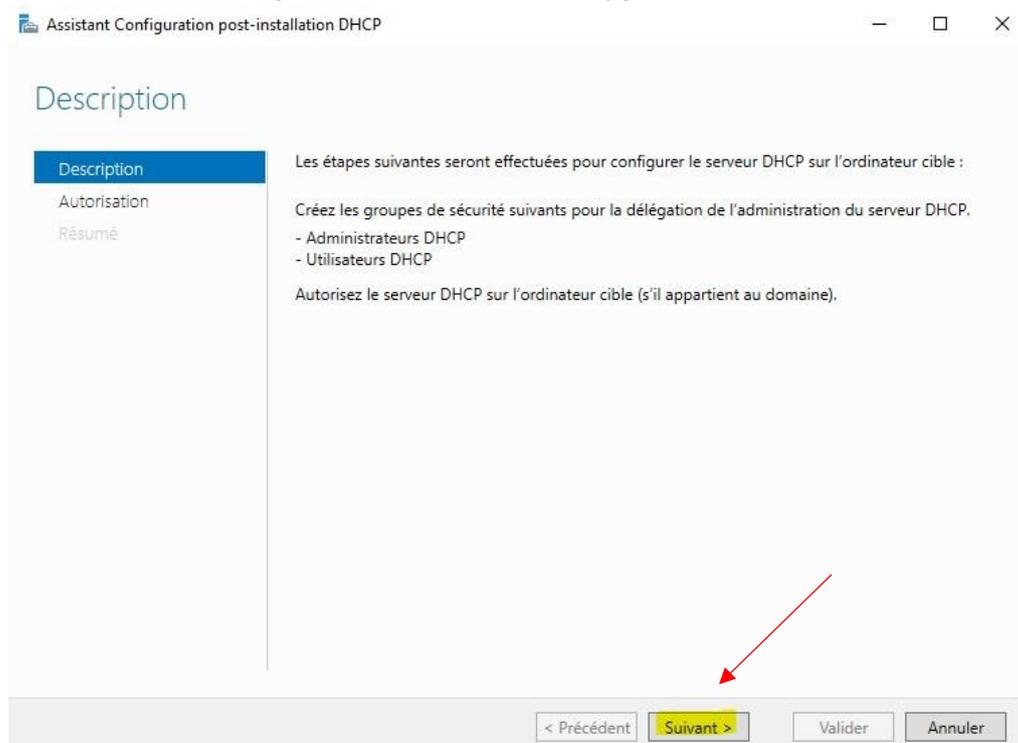


Figure 32 : DHCP / Description

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

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

Figure 33 : DHCP / Autorisation

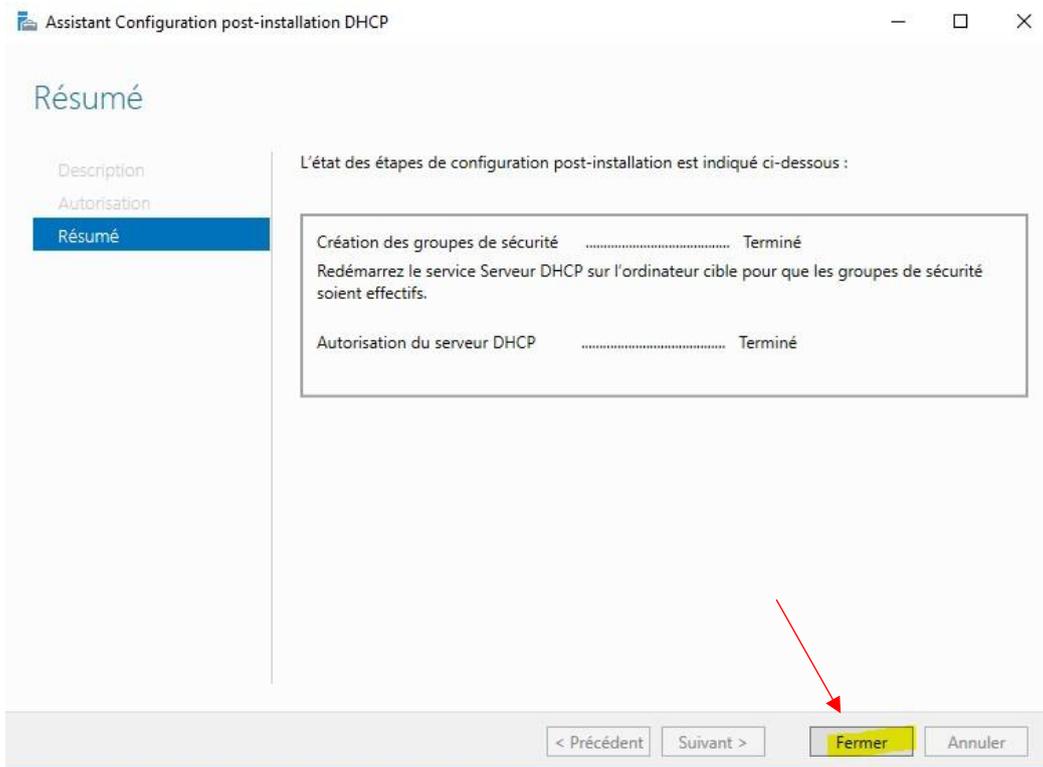


Figure 34 : DHCP / Résumé

Maintenant, redémarrez l'ordinateur.

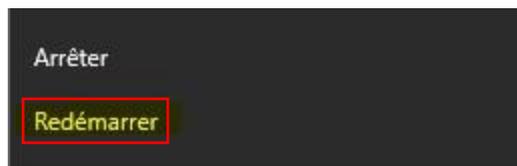


Figure 35 : Fermer puis redémarrer

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.

The screenshot shows the 'Assistant Nouvelle étendue' window at the 'Plage d'adresses IP' step. The title bar reads 'Assistant Nouvelle étendue'. Below the title, the step is titled 'Plage d'adresses IP' with a sub-instruction: 'Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.' To the right is a folder icon. The main area is divided into two sections: 'Paramètres de configuration pour serveur DHCP' and 'Paramètres de configuration qui se propagent au client DHCP'. In the DHCP server section, 'Adresse IP de début' is '192.168.10.193' and 'Adresse IP de fin' is '192.168.10.240'. In the DHCP client section, 'Longueur' is '26' and 'Masque de sous-réseau' is '255.255.255.192'. At the bottom are buttons for '< Précédent', 'Suivant >', and 'Annuler'.

Figure 36 : Paramétrage adresse IP / VLAN 22

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

The screenshot shows the 'Assistant Nouvelle étendue' window at the 'Routeur (passerelle par défaut)' step. The title bar reads 'Assistant Nouvelle étendue'. Below the title, the step is titled 'Routeur (passerelle par défaut)' with a sub-instruction: 'Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.' To the right is a folder icon. The main area contains the instruction: 'Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.' Below this is an 'Adresse IP' input field with a list of IP addresses. The first entry is '192.168.10.1', which is highlighted. To the right of the list are buttons for 'Ajouter', 'Supprimer', 'Monter', and 'Descendre'. At the bottom are buttons for '< Précédent', 'Suivant >', and 'Annuler'.

Figure 37 : Routeur / Passerelle par défaut

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

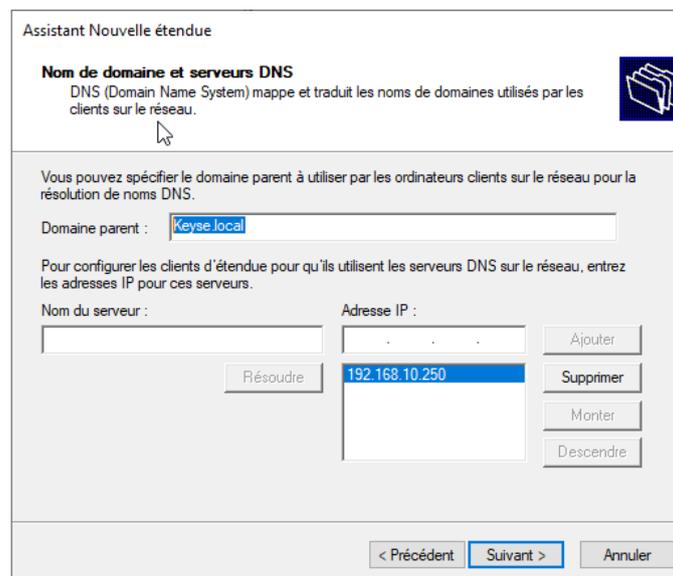


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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**.

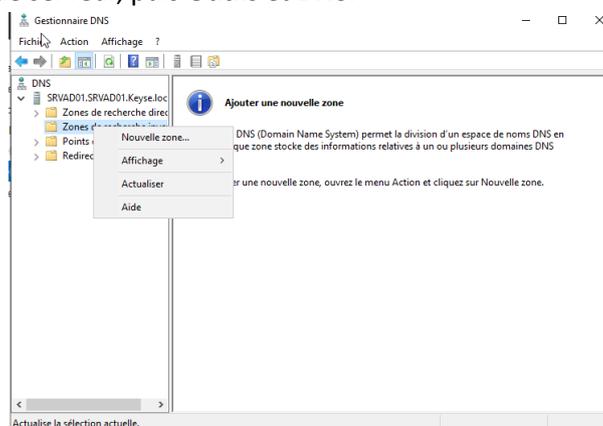
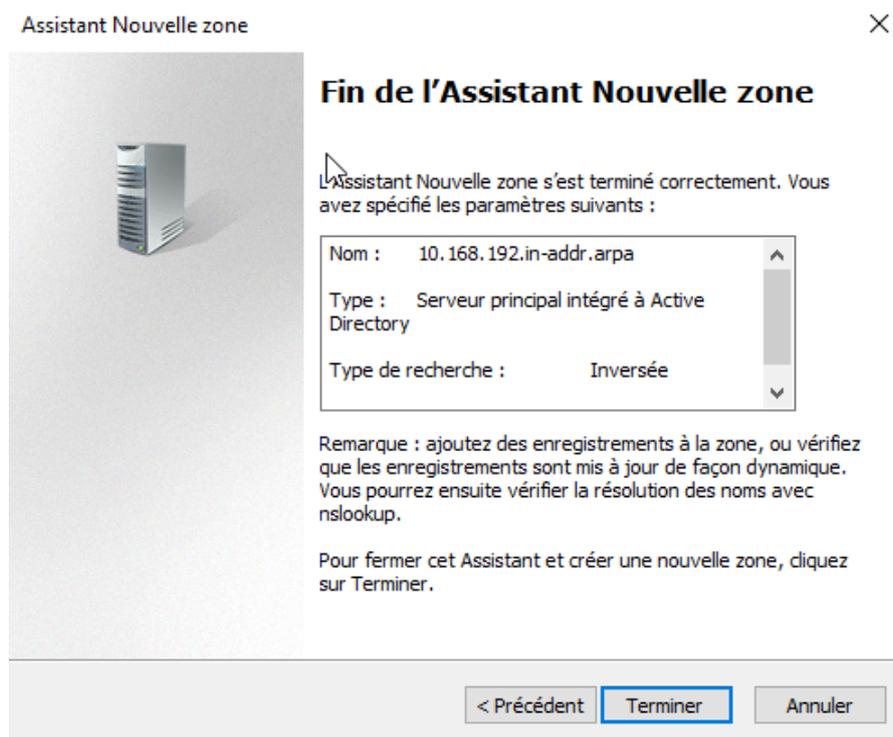


Figure 41 : DNS / Nouvelle zone de recherche inversée

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**.

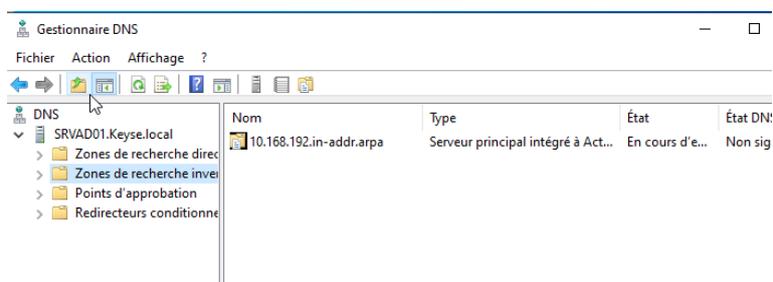


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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 :

<u>Prénom</u>	<u>Nom</u>	<u>Groupe</u>	<u>Mot de passe</u>
Brice	Wilems	Formateurs	Yh! D0kNYsxHkO"mEaq.W
Jean	maltra	Formateurs	%'f1@Nqr1lf+PgMj!DSw
Mathilde	Brunier	Administratif	Keh=e'lxl":~J60nR&#l
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**.

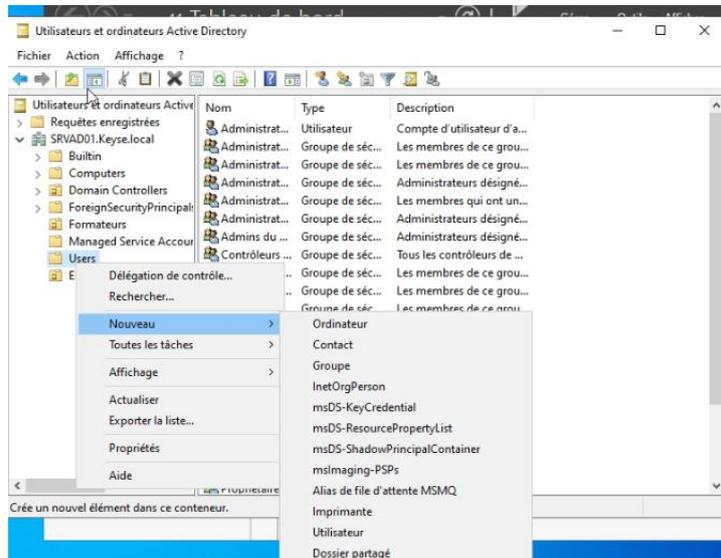


Figure 45 : Active Directory / création des utilisateurs

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

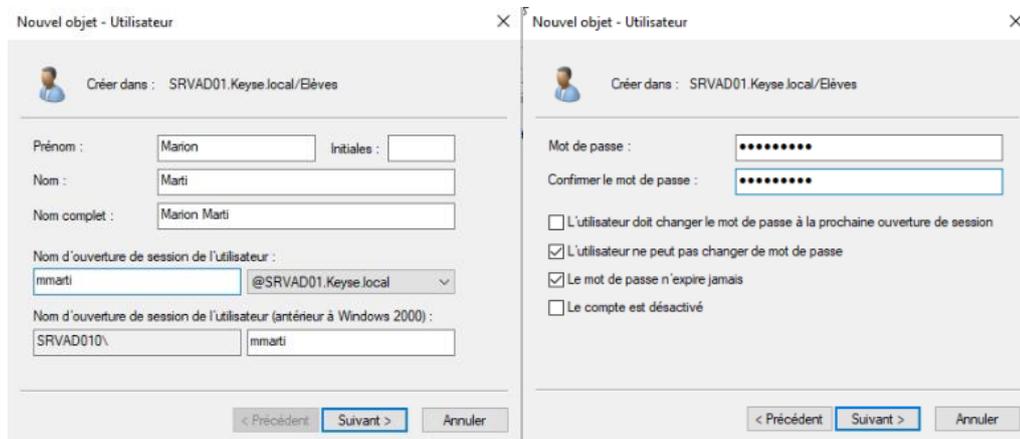


Figure 46 : Active Directory / création utilisateur Marion Figure 47 : Active Directory / création utilisateur MDP

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**.

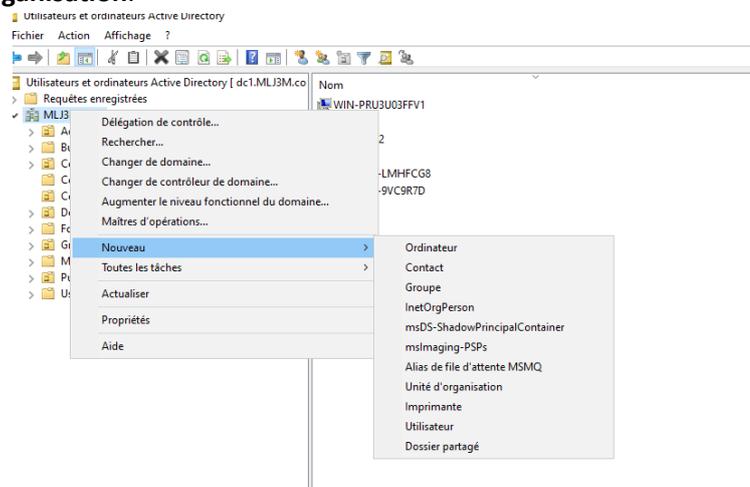


Figure 48 : Active Directory / création unité d'organisation

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 :

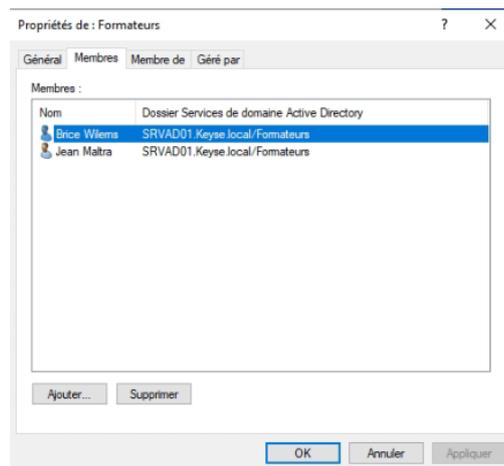


Figure 49 : Active Directory / Groupe Formateurs avec utilisateurs

Figure 50 : Active Directory / Groupe Administratif

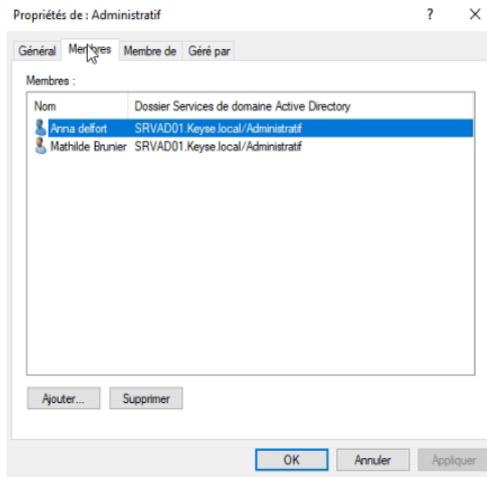
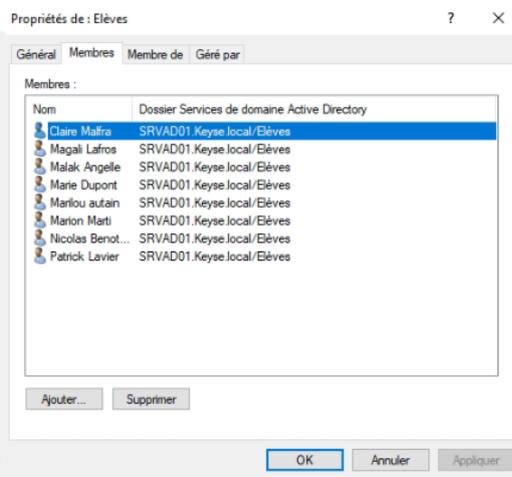


Figure 51 : Active Directory / Groupe Elèves



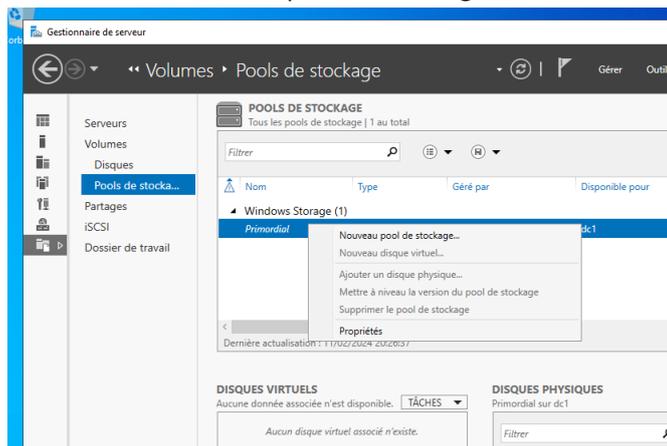
7 Serveur de fichiers :

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 :

Assistant Nouveau pool de stockage

Indiquer un pool de stockage et son sous-système

Avant de commencer
Nom du pool de stockage
Disques physiques
Confirmation
Résultats

Nom :

Description :

Sélectionnez le groupe de disques disponibles (également appelé pool primordial) que vous voulez utiliser :

Géré par	Disponible pour	Sous-système	Pool primordial
SRVFILES01	SRVFILES01	Windows Storage	Primordial

< Précédent Suivant > Créer Annuler

Confirmation des différentes configurations :

Assistant Nouveau pool de stockage

Confirmer les sélections

Avant de commencer
Nom du pool de stockage
Disques physiques
Confirmation
Résultats

Vérifiez que les paramètres suivants sont corrects, puis cliquez sur Créer.

EMPLACEMENT DU POOL DE STOCKAGE

Serveur : SRVFILES01
Rôle du cluster : Non-cluster
Sous-système de stockage : Windows Storage

PROPRIÉTÉS DU POOL DE STOCKAGE

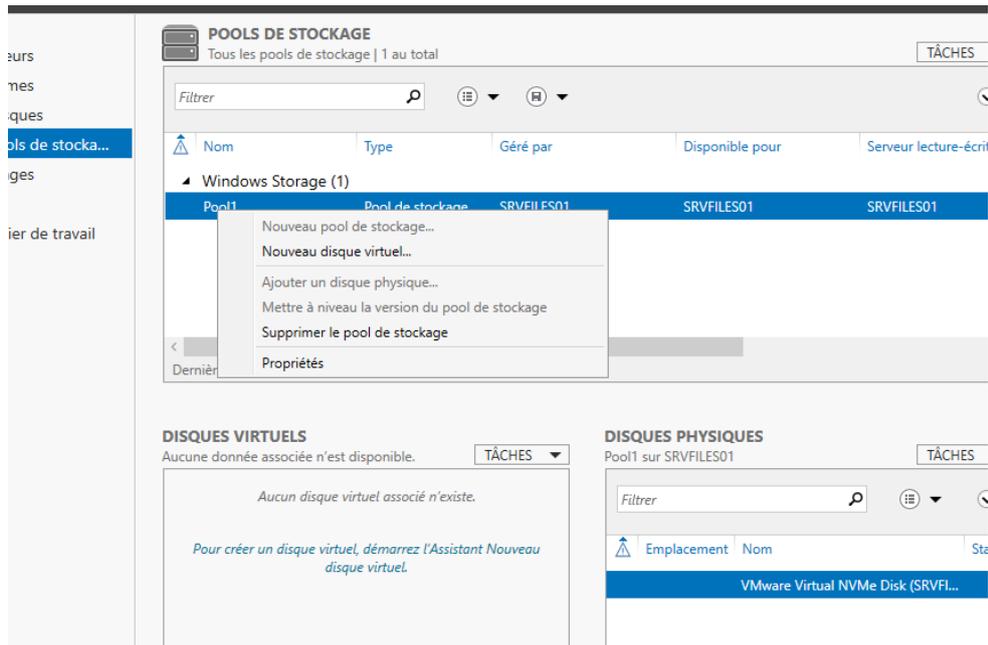
Nom : Pool1
Capacité : 400 Go

DISQUES PHYSIQUES

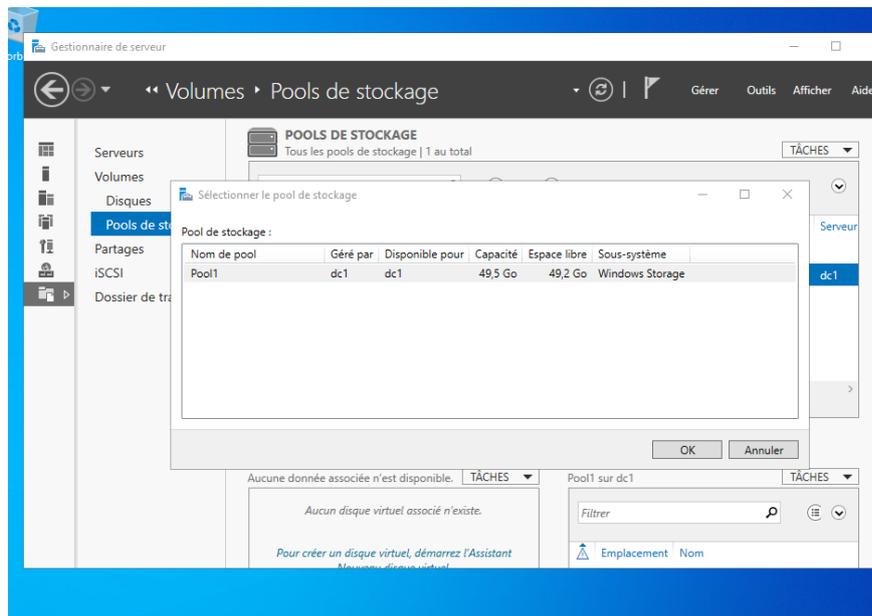
VMware Virtual NVMe Disk (SRVFILES01) Automatique

< Précédent Suivant > Créer Annuler

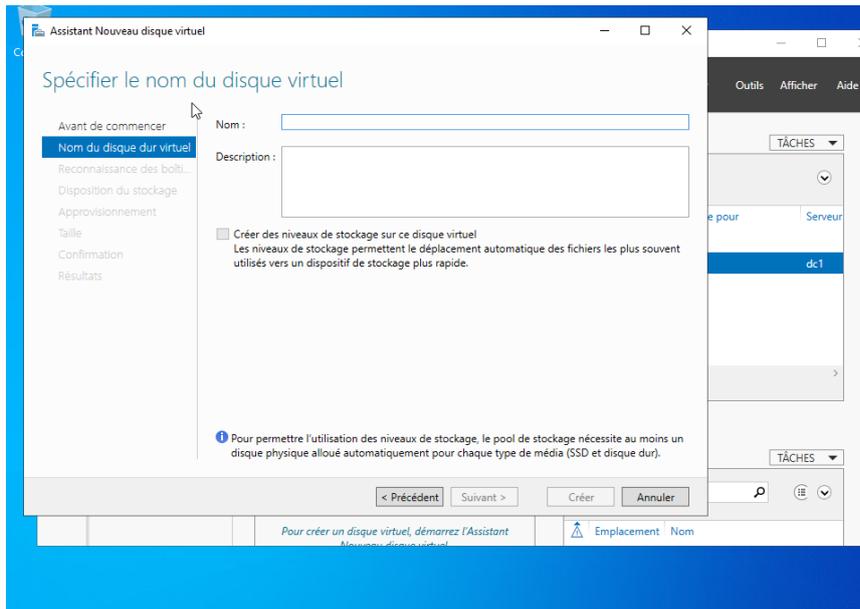
Création d'un nouveau disque virtuel :



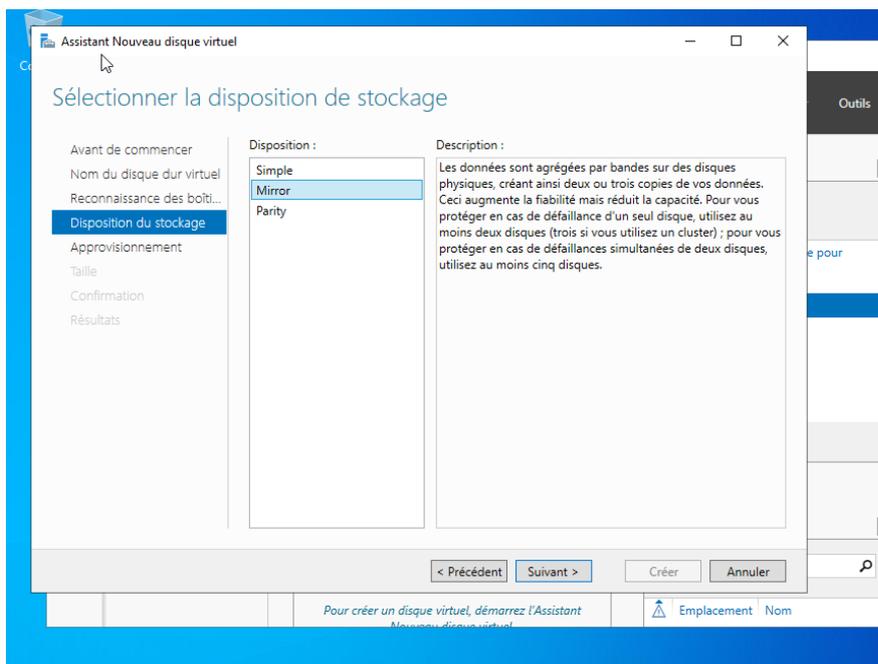
Sélection du Pool de stockage :



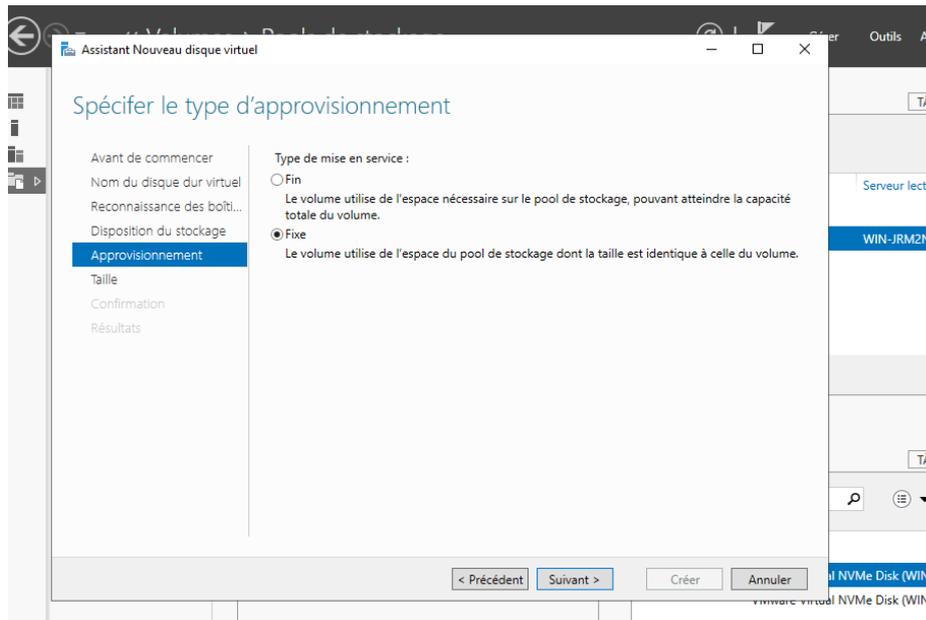
Nommage du disque virtuel :



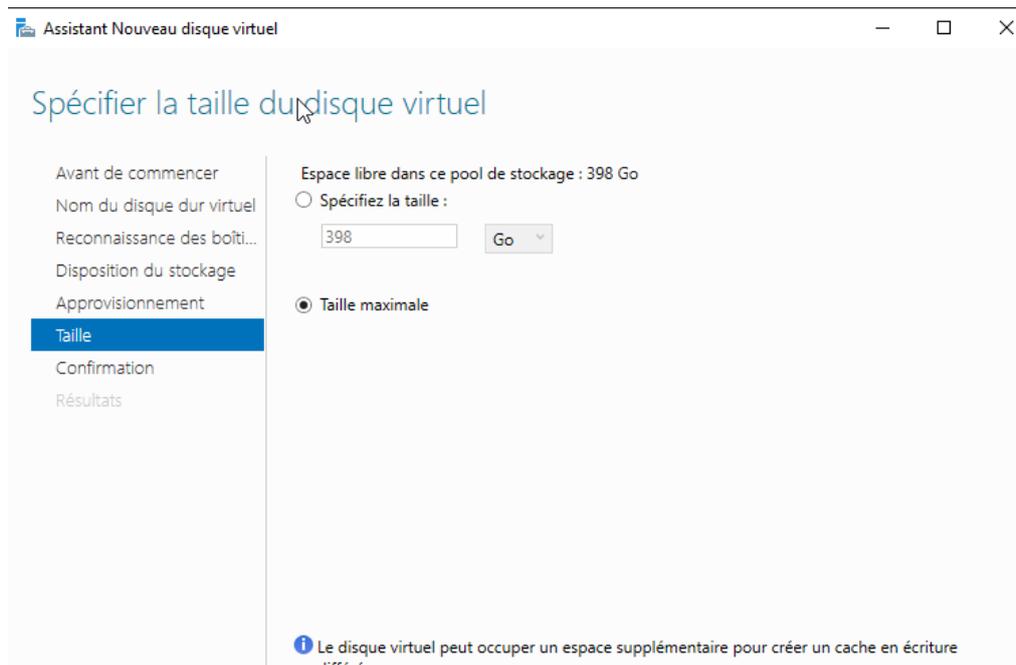
Sélection de la disposition de stockage :



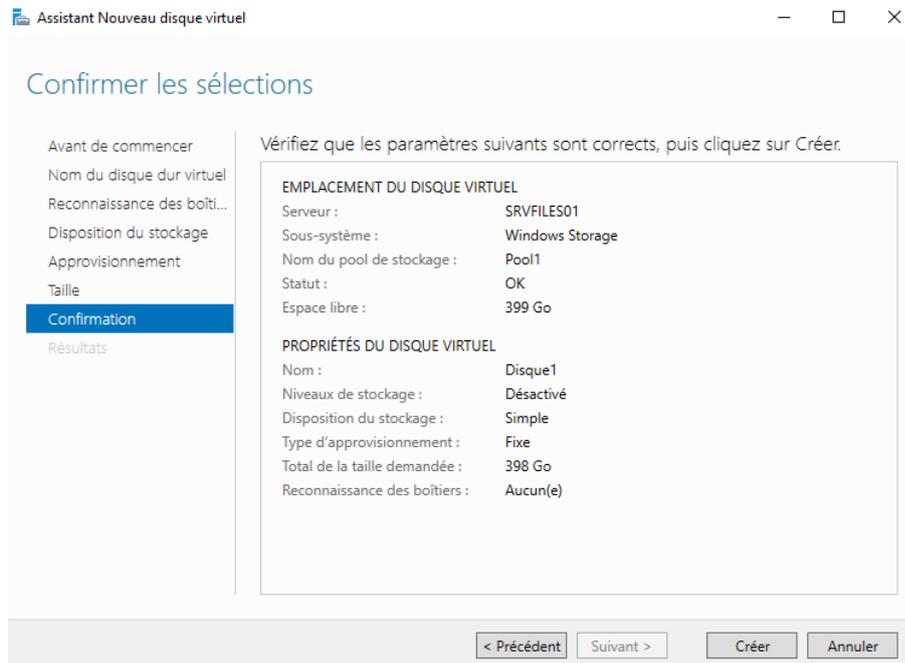
Sélection du type d'approvisionnement :



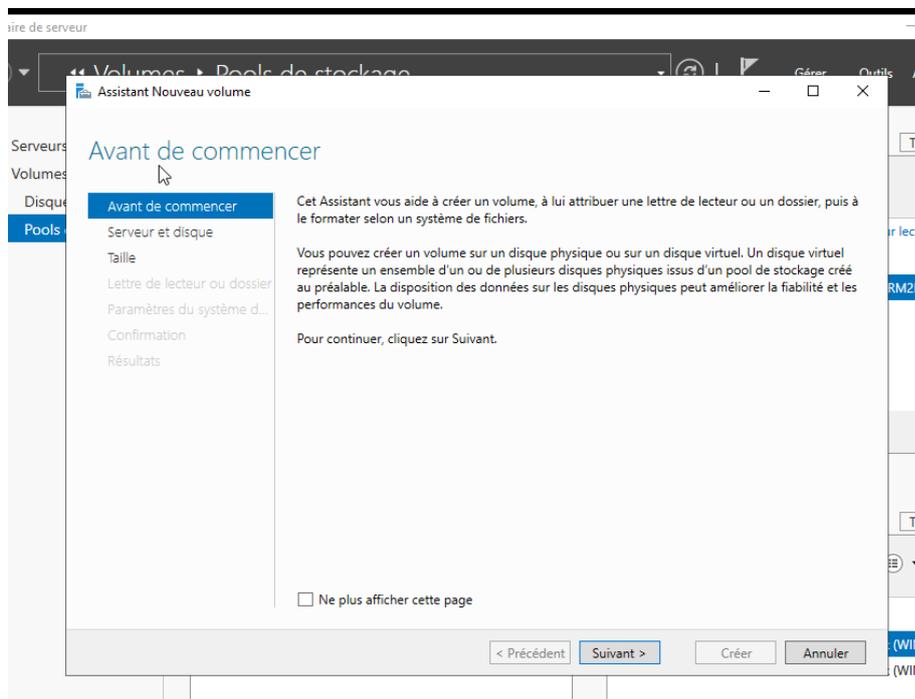
Sélection de la taille du disque virtuel :



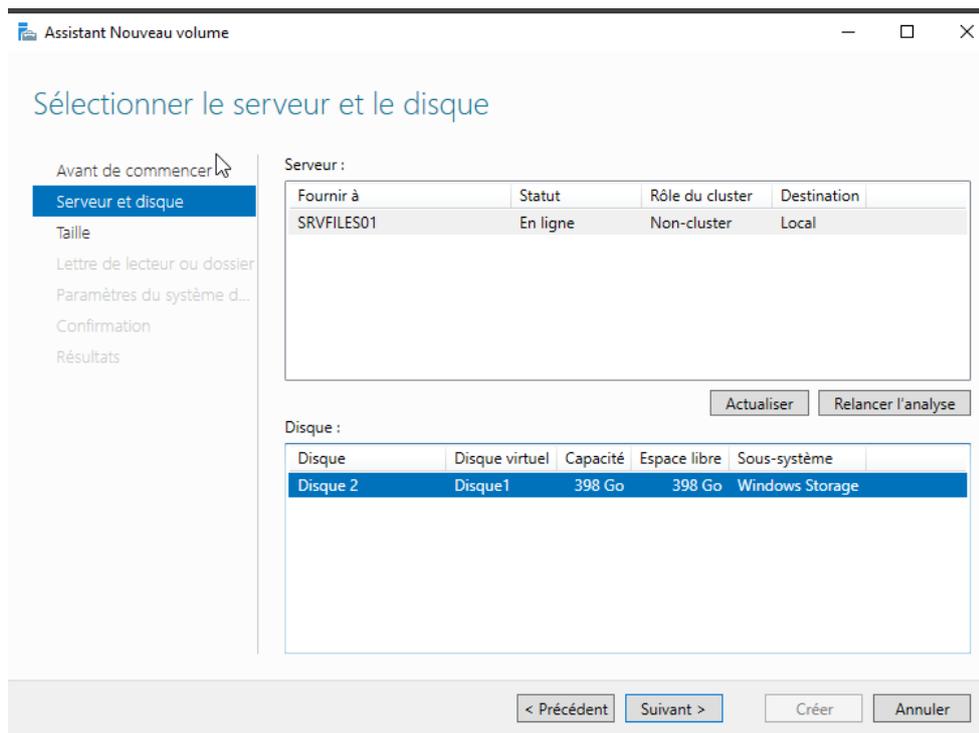
Confirmations des différentes configurations :



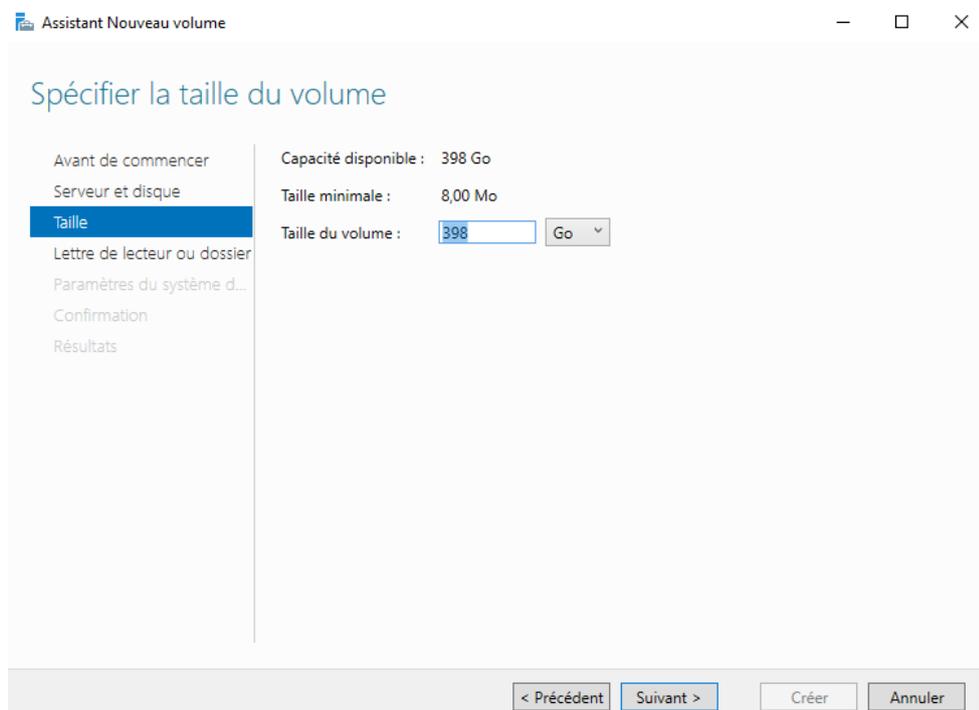
Création d'un nouveau volume :



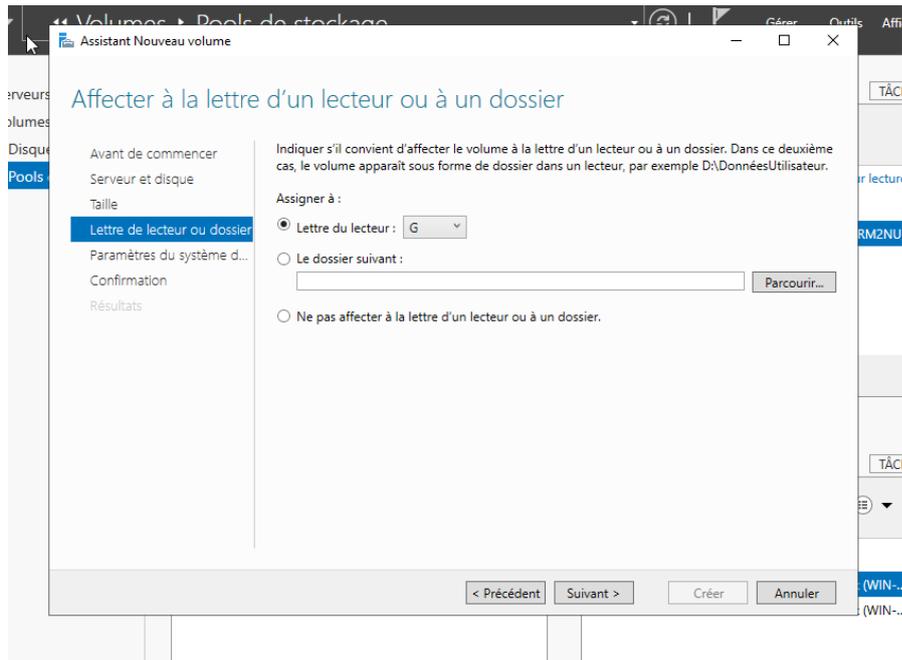
Sélection du serveur et du disque :



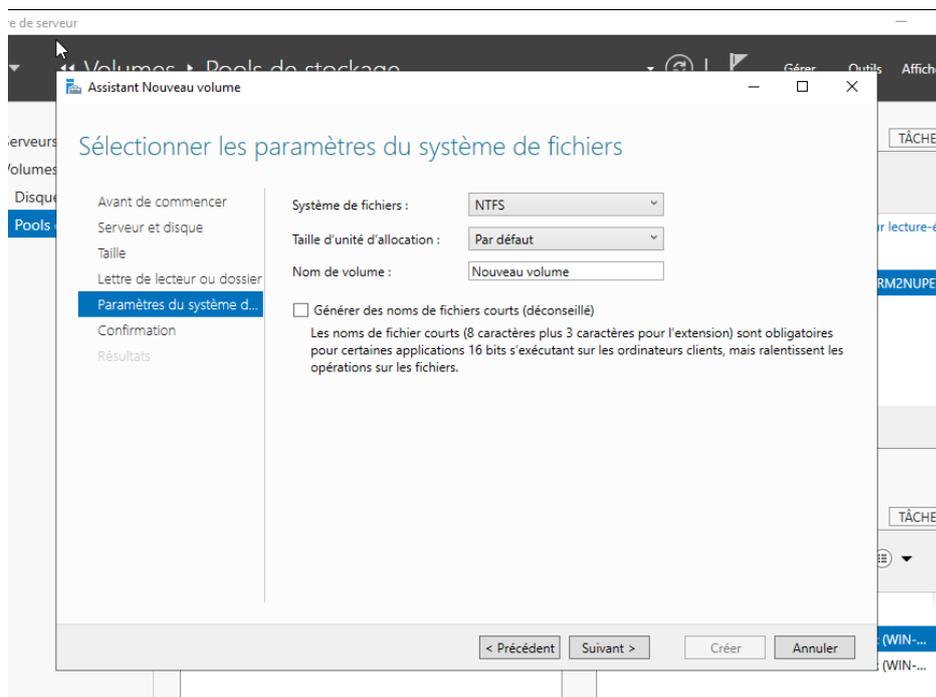
Sélection de la taille du volume :



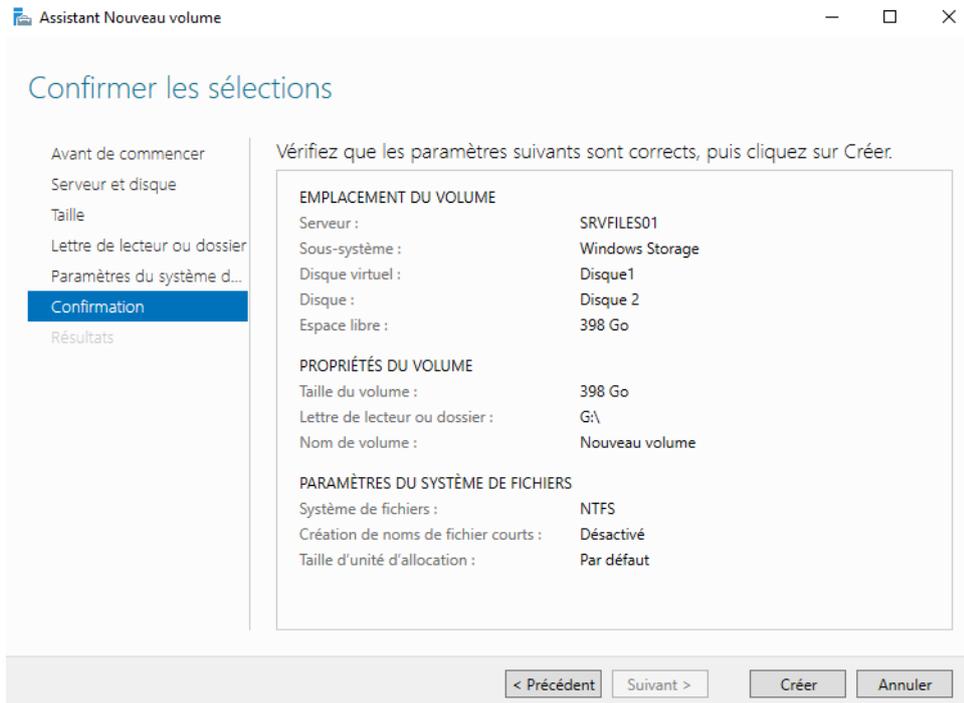
Affectation de la lettre du lecteur :



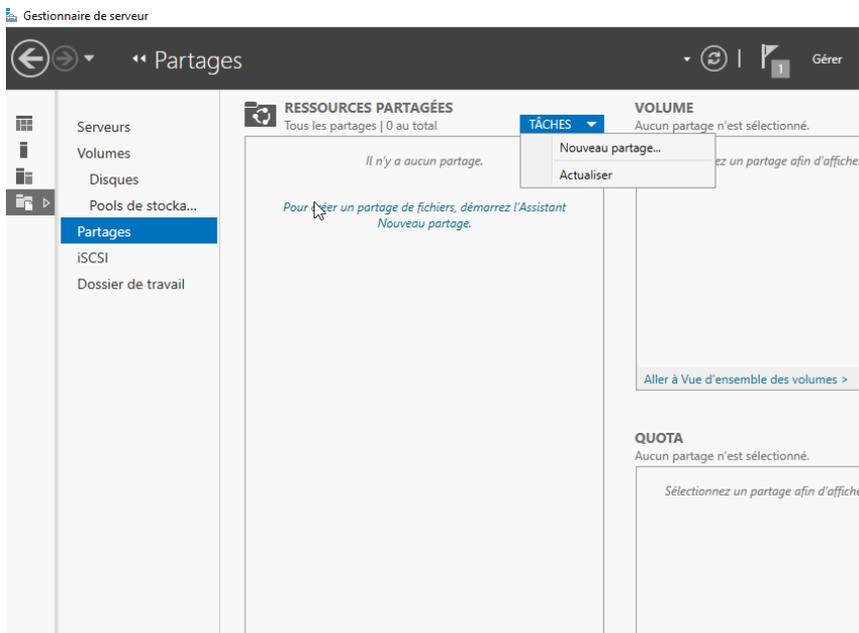
Sélection des paramètres du système de fichier :



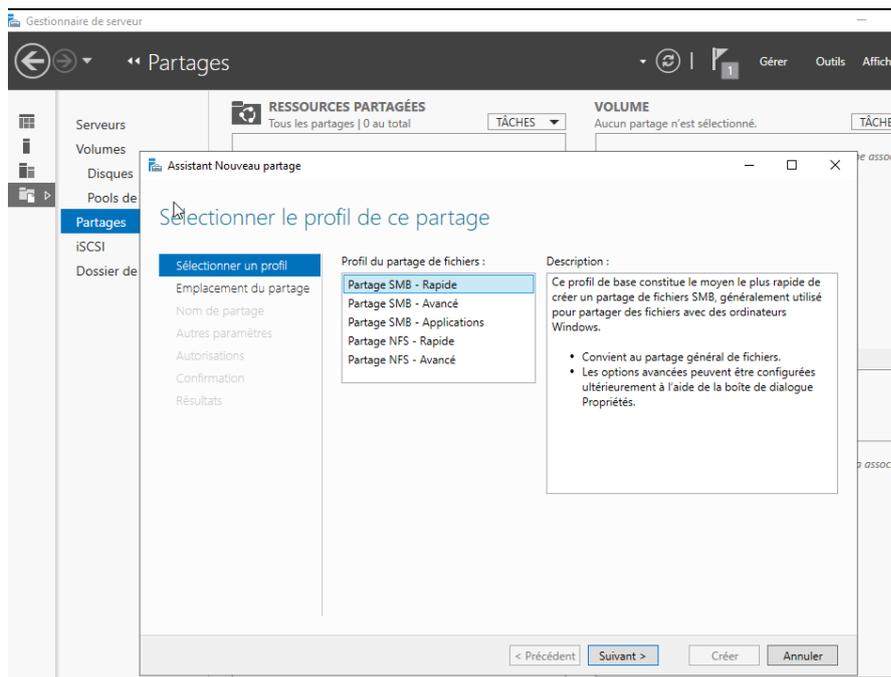
Confirmer différentes les configurations :



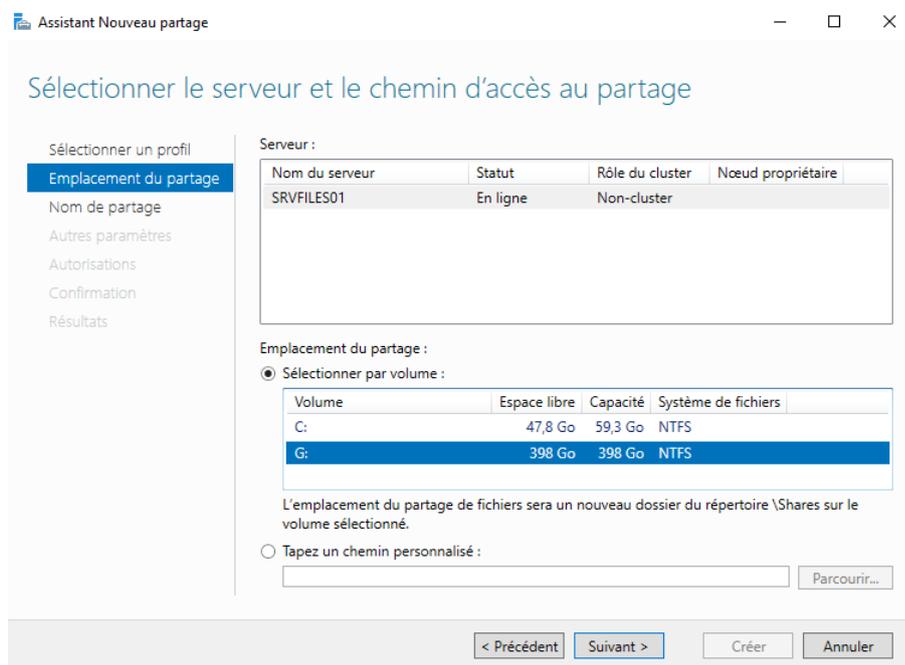
Création d'un nouveau partage :



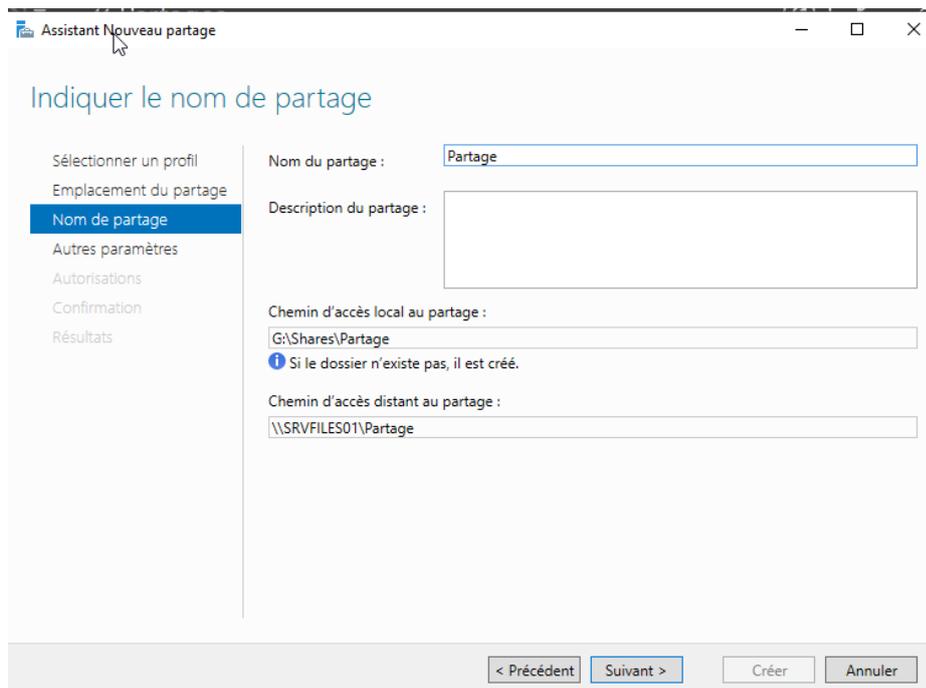
Sélection du profil de ce partage :



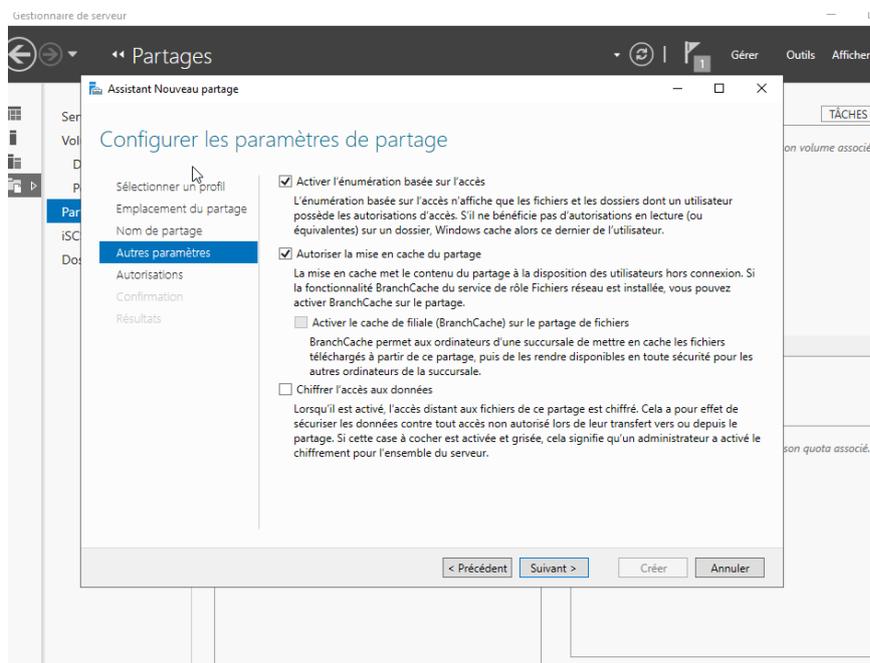
Sélectionner le serveur et le chemin d'accès au partage :



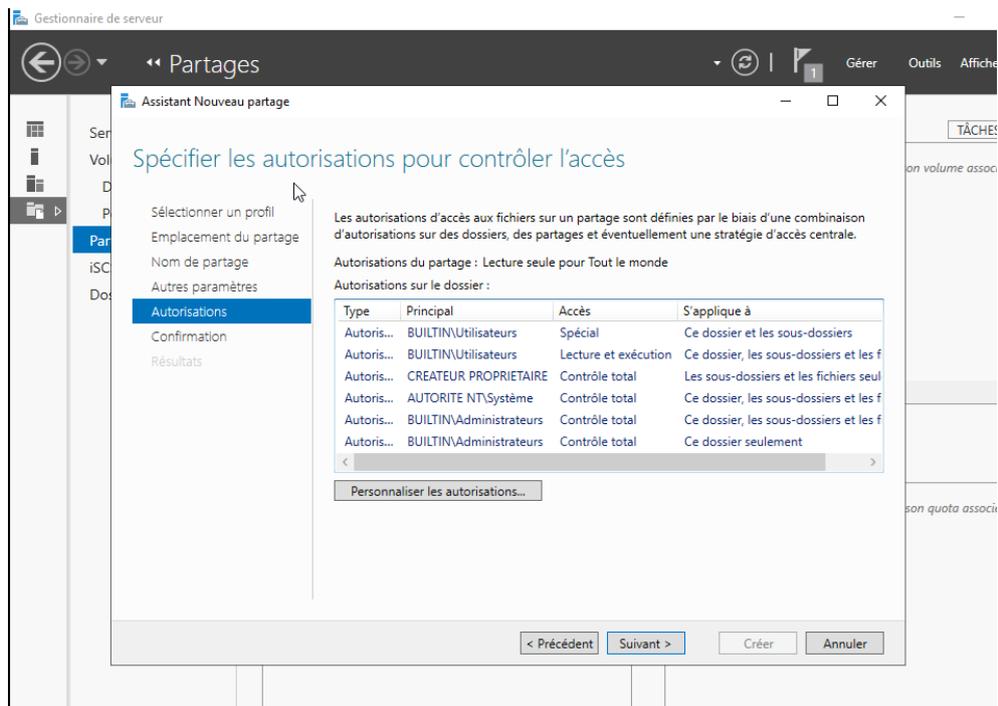
Indiquer le nom du partage :



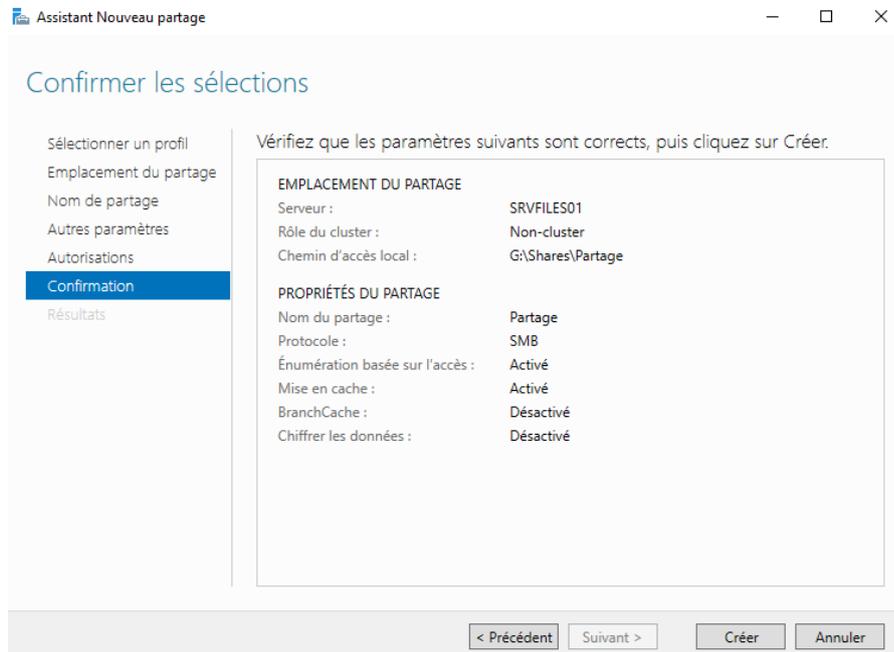
Configurer les paramètres de partage :



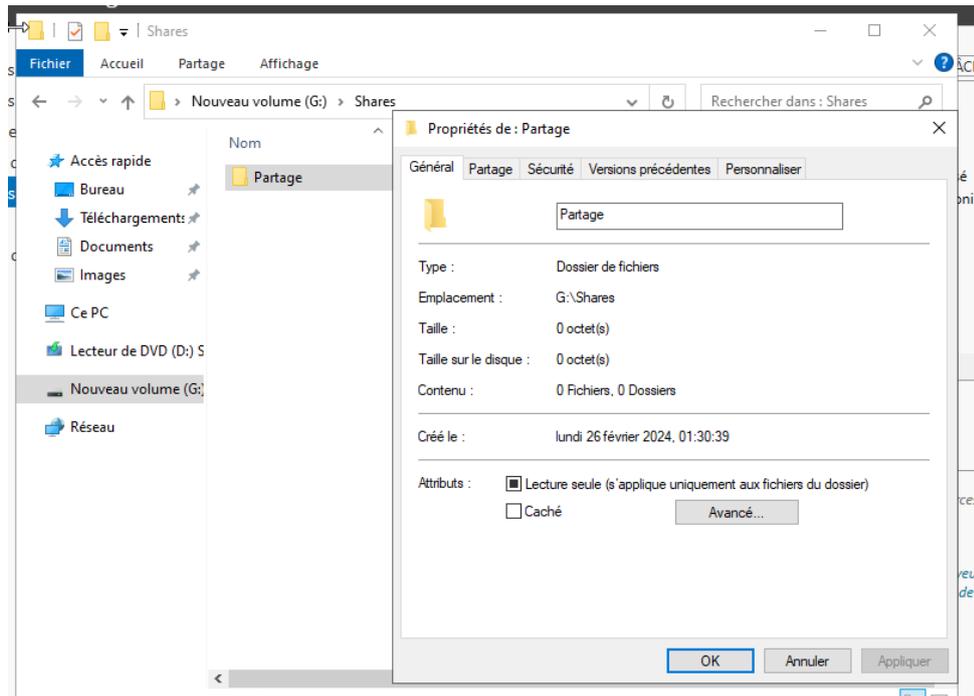
Spécification des autorisations pour contrôler l'accès :



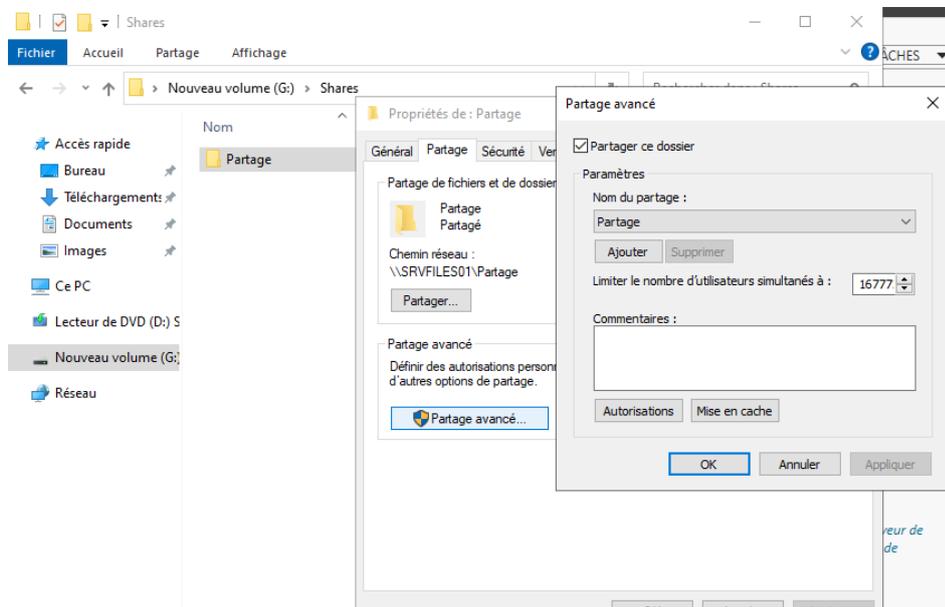
Confirmer les différentes configurations :



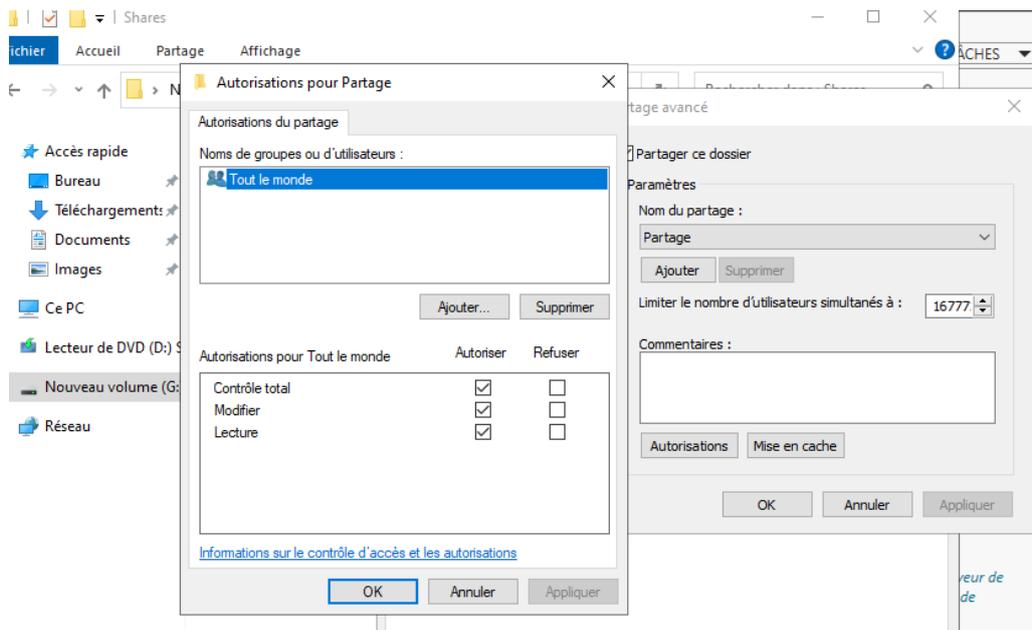
Propriétés du partage créé :



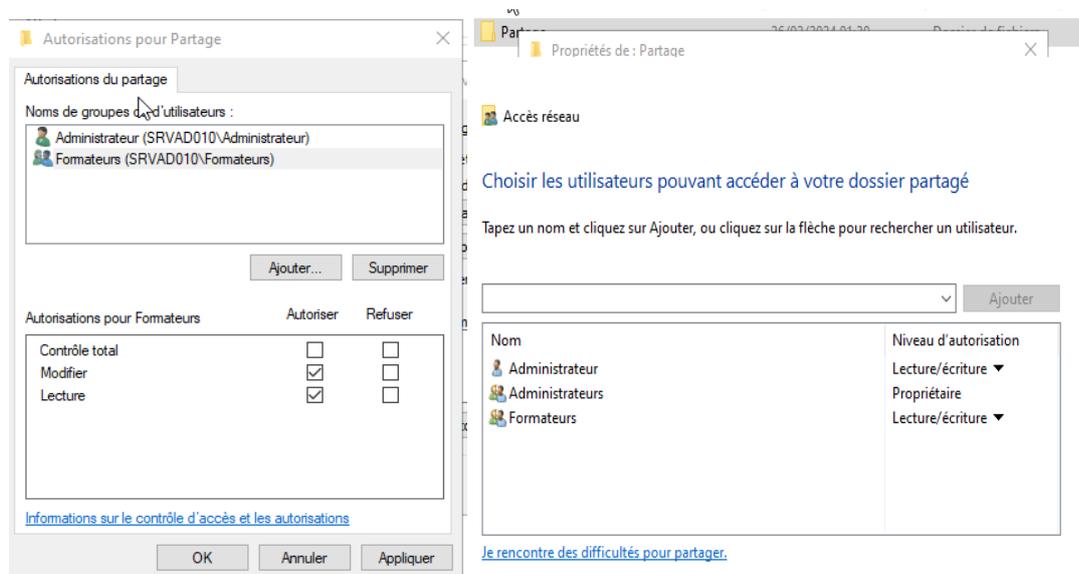
Paramétrage de partage avancé sur le partage créé :



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 »

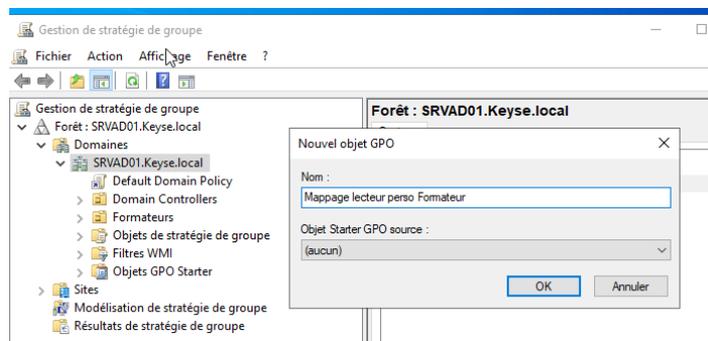


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

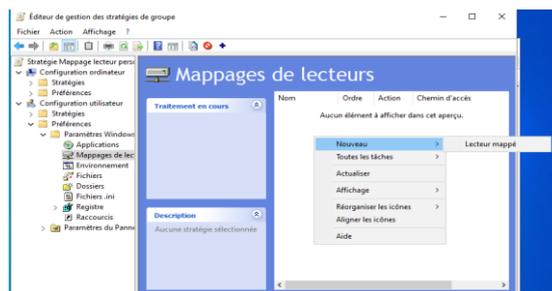


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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%» créée au préalable, attention a bien coché la case « Reconnecter » et attribuer un nom au Lecteur et enfin, nous choisirons une lettre pour le lecteur.

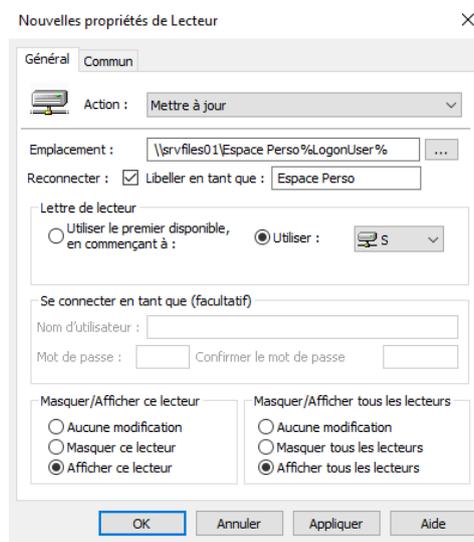


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous nous rendons 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 à un groupe sélectionné.

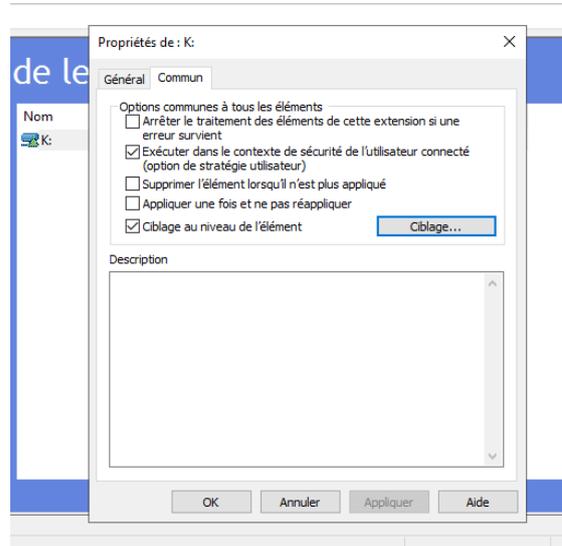


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

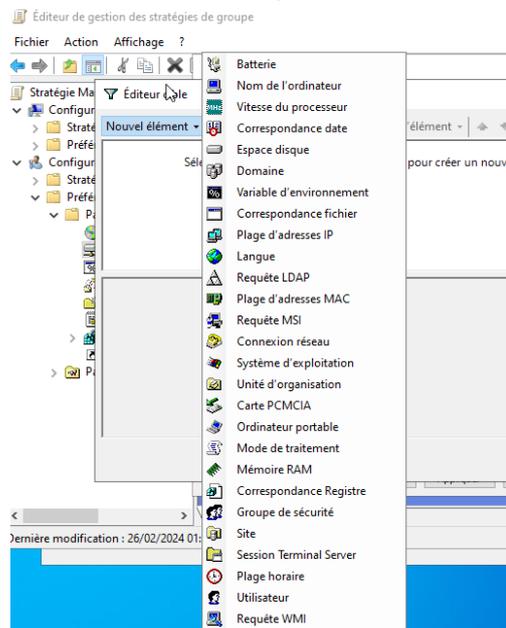


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

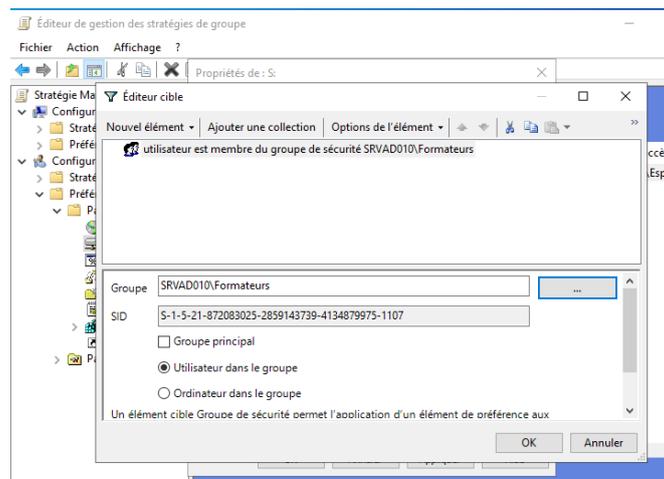


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

Clique droit puis Nouveau et « Dossier »

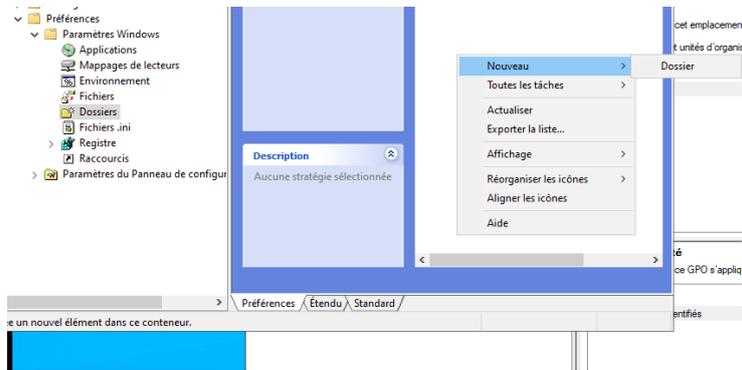


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

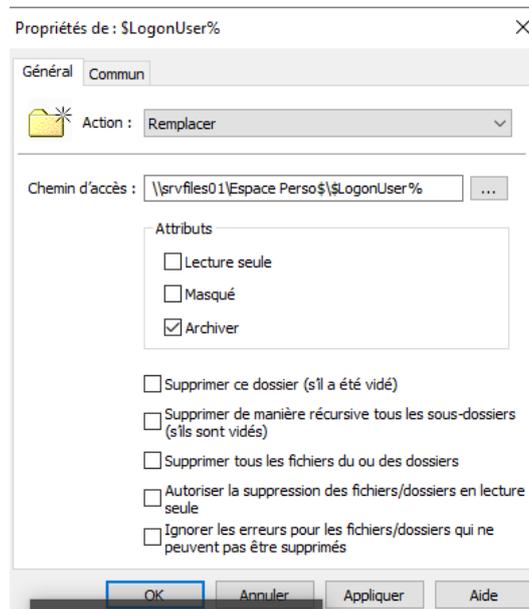


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous nous rendons 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 à un groupe sélectionné.

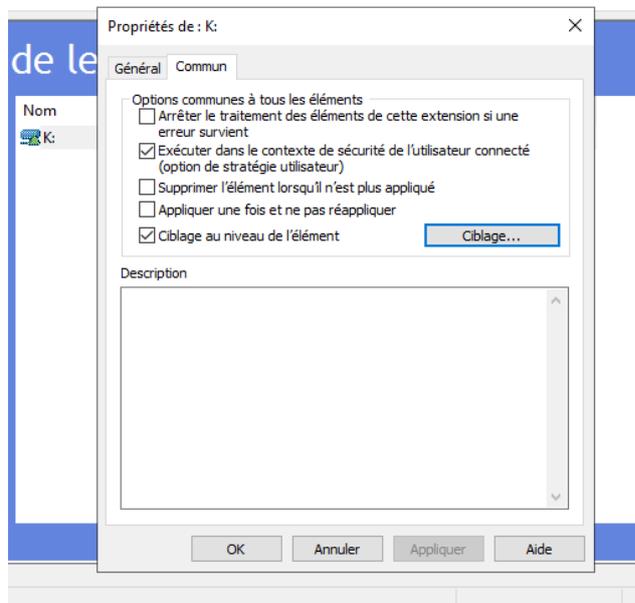


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25

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

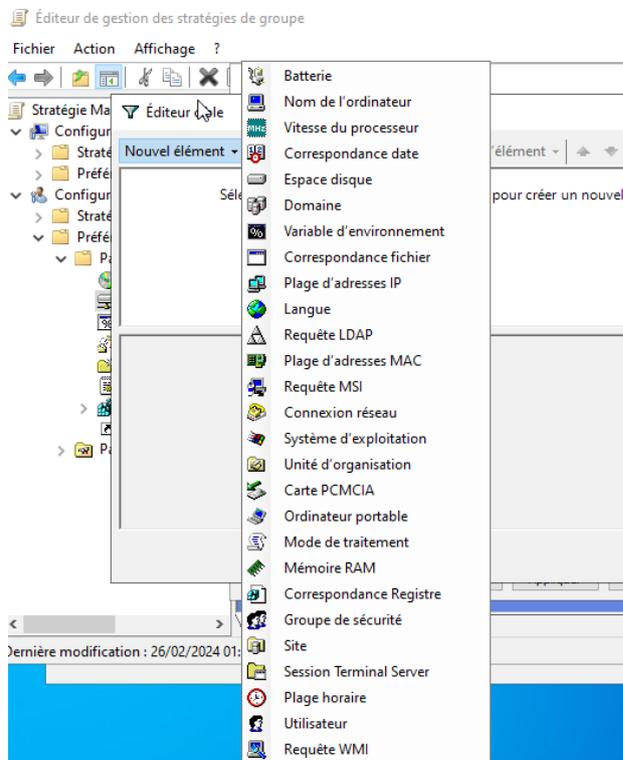


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

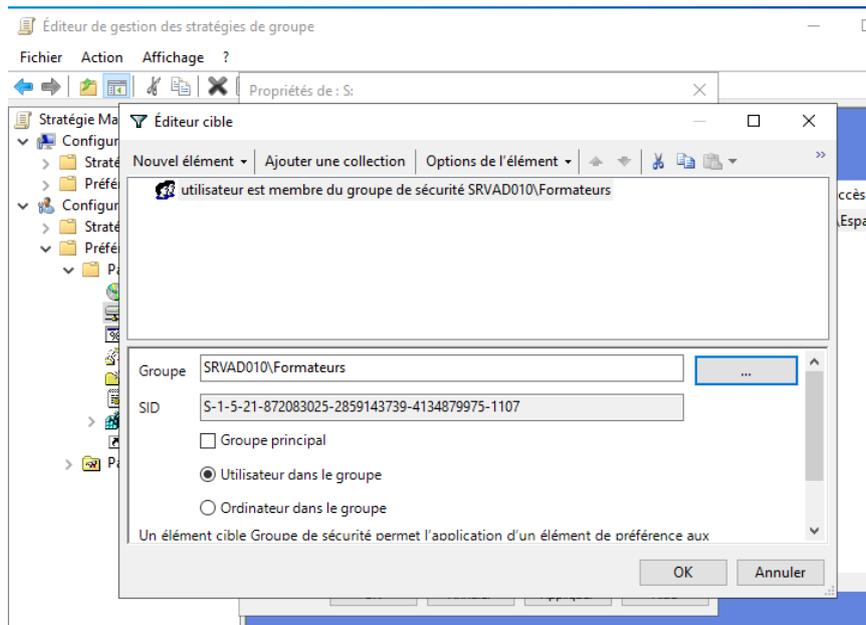


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

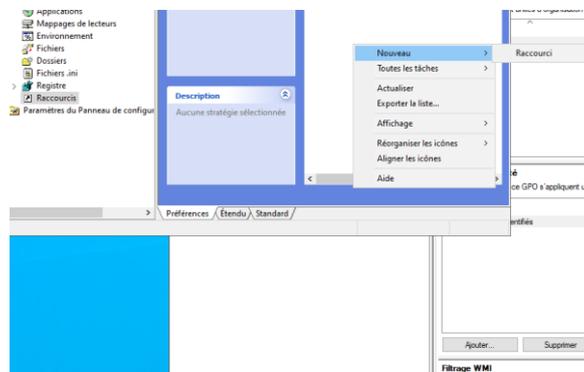


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

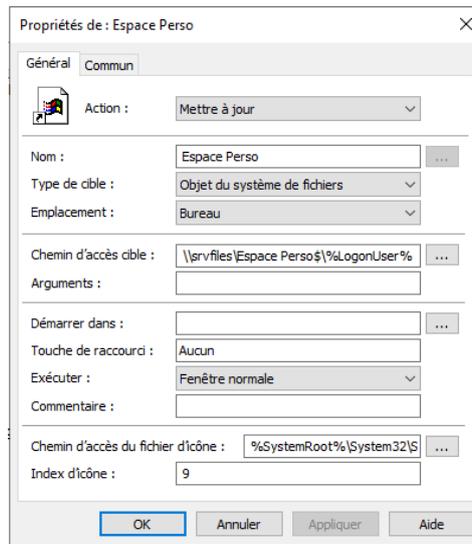


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

Nous nous rendons 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 à un groupe sélectionné.

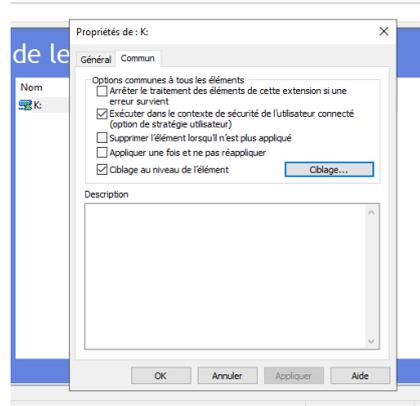


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

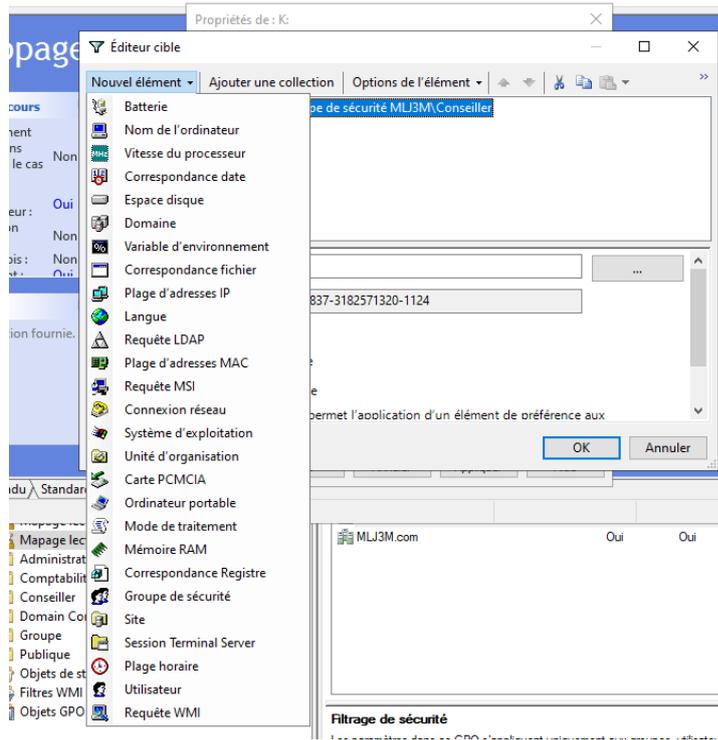


Figure 39 : Paramétrage adresse IP / VLAN 23-24-25-1

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

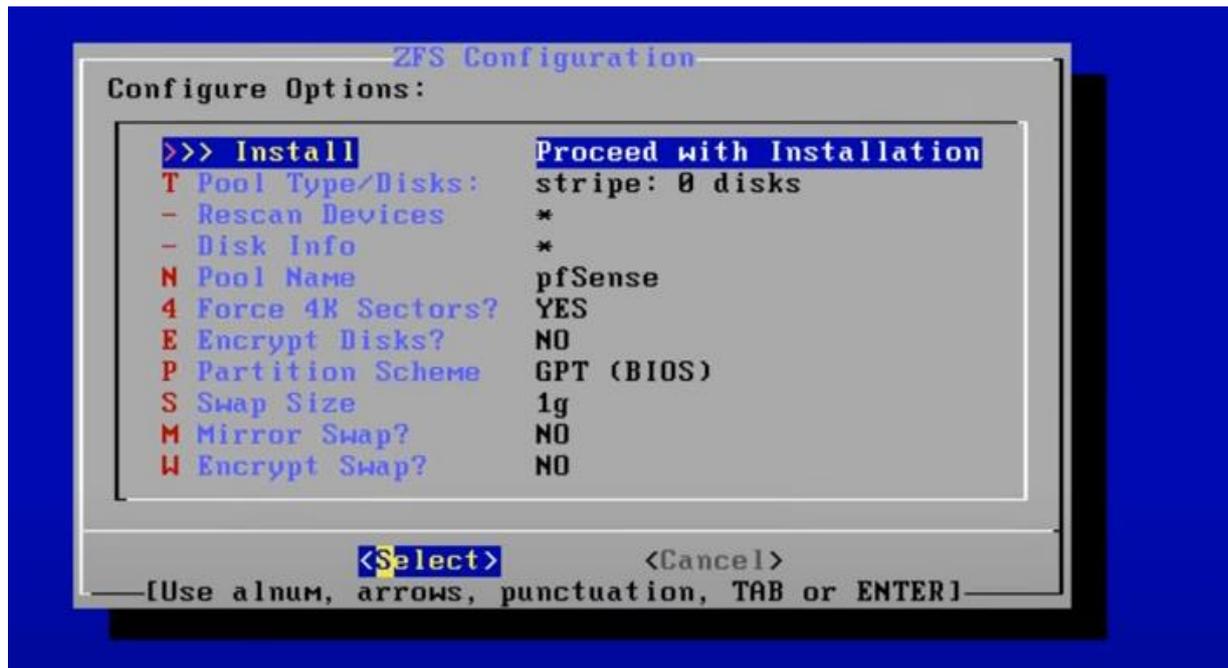
8 Firewall PFSense :

Installation de PFSense :

Install pfSense : **OK**



Proceed with installation : « Select »



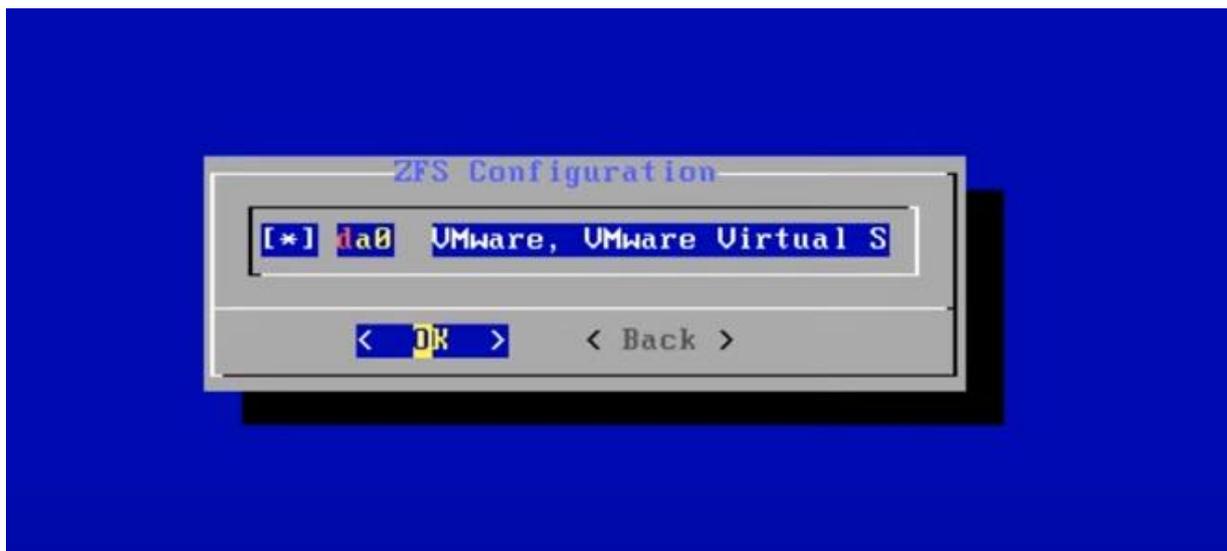
Auto (ZFS) pour pfSense version 2.6 et ultérieure ou Auto (UFS) BIOS pour version inférieure



Sélectionner : sans redondance



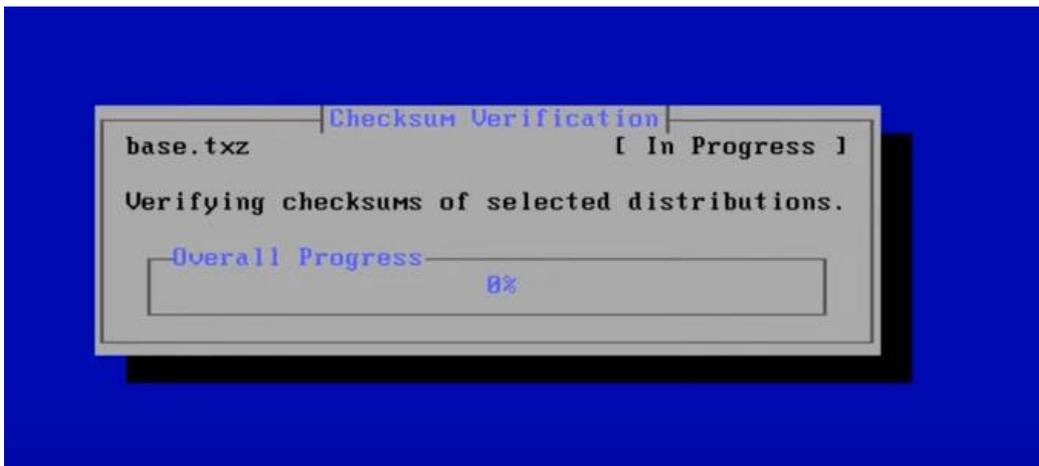
Sélectionner le disque virtuel



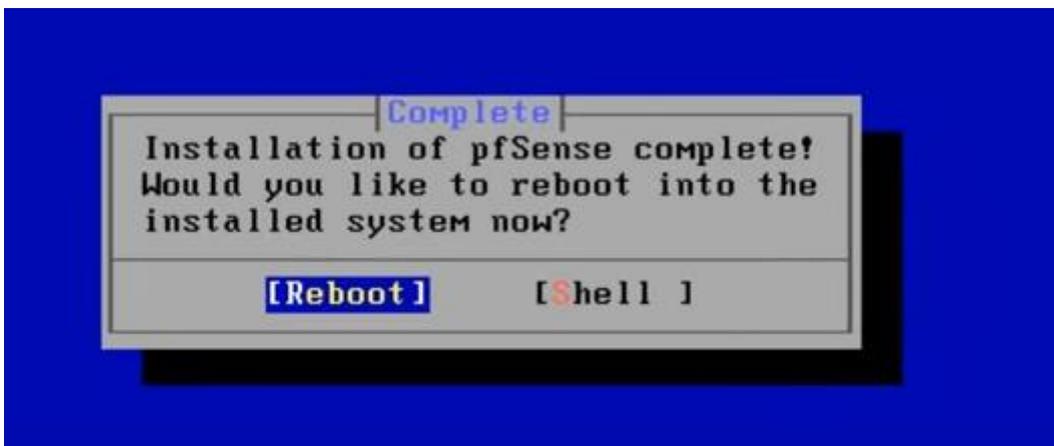
Confirmer par « yes » que vous souhaitez formater le disque



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

```
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

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

UMware Virtual Machine - Netgate Device ID: e4aecdeefd72a5f5a4cc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.10.100/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

Enter an option: 2
```

Sélectionner la carte réseau local LAN : 2

```
UMware Virtual Machine - Netgate Device ID: e4aecdeefd72a5f5a4cc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.10.100/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

Enter an option: 2

Available interfaces:

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

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

Ne pas configurer les adresses IPV4 du lan automatiquement via DHCP

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.10.100/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

Enter an option: 2

Available interfaces:

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

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

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

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

```
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

Enter an option: 2

Available interfaces:

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

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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1
```

Saisissez le masque sous réseau au format CIDR : 24

```
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 - static)

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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

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
```

Laissez vide pour ne pas définir la passerelle : Tapez ENTREE

```
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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

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:
>
```

Saisir « n » pour ne pas configurer d'IPv6 via DHCP6

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

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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

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:
>

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

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

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

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

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:
>

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

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

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

Ne pas activer le retour à http en tant que protocole de configuration Web. Entrez : « n »
pour "no"

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

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:
>

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

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 DHCPD...
Disabling IPv6 DHCPD...

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

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

```
For a LAN, press <ENTER> for none:
>

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

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 DHCPD...
Disabling IPv6 DHCPD...

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

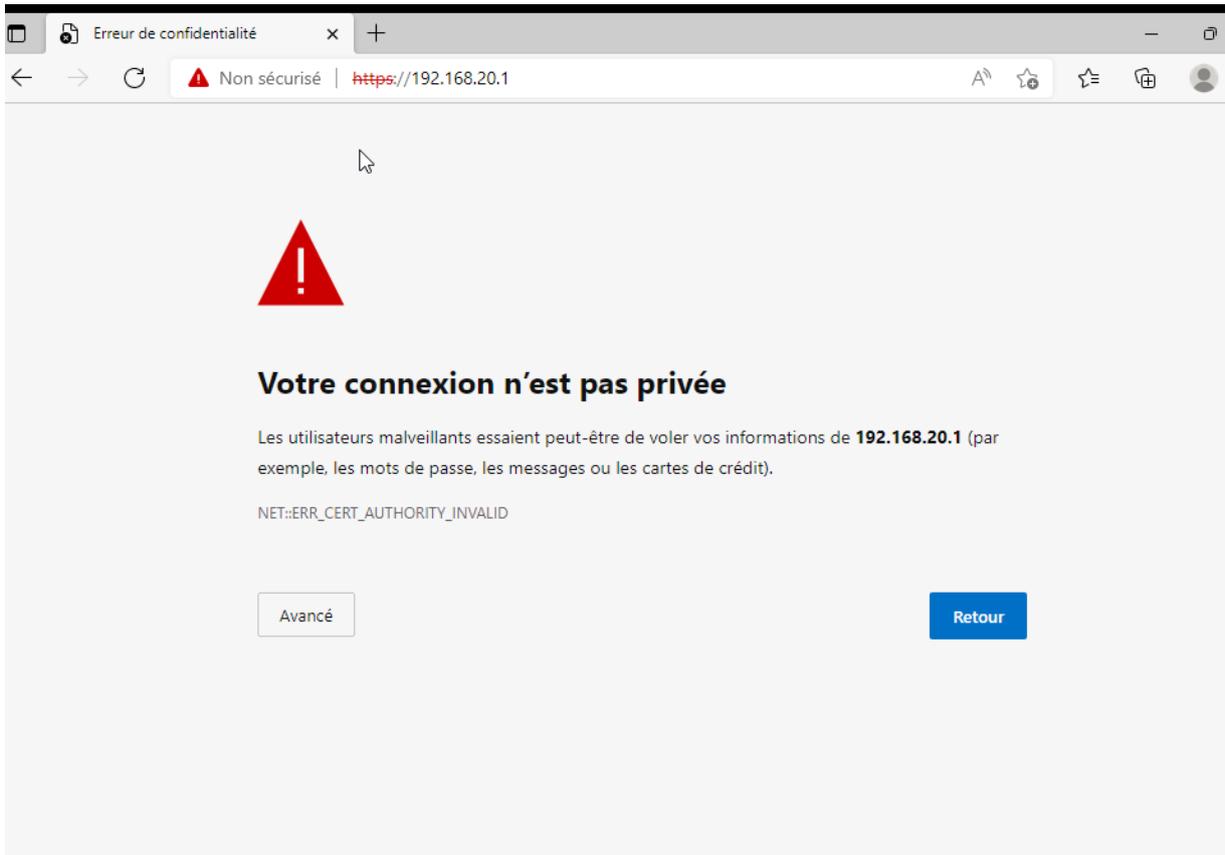
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

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

Press <ENTER> to continue. █
```

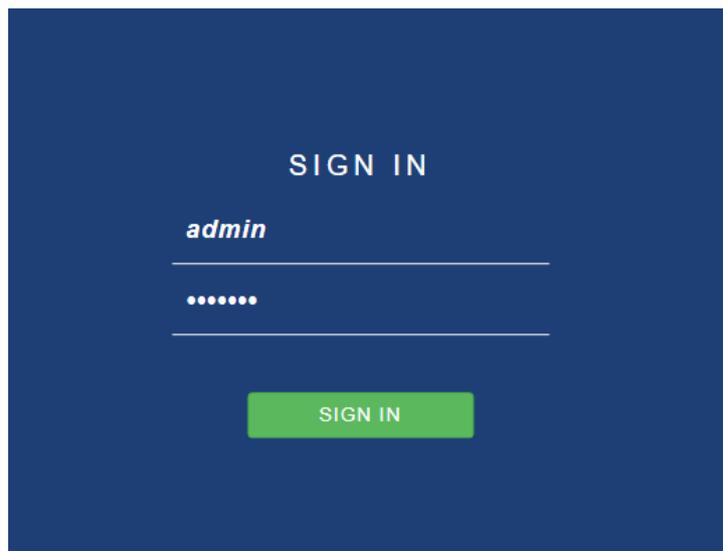
Figure 61 : PFSense /Configuration de l'interface Lan de PFSense

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

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall.

Sélectionner la Timezone Europe

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

[» Next](#)

Configuration de la carte réseau internet WAN : « DHCP »

The screenshot shows the pfSense web interface for configuring a WAN interface. At the top, there is a navigation menu with items like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb trail reads "Wizard / pfSense Setup / Configure WAN Interface". A progress bar indicates "Step 4 of 9". The main heading is "Configure WAN Interface", followed by the instruction: "On this screen the Wide Area Network information will be configured." The "SelectedType" dropdown menu is set to "DHCP". Under the "General configuration" section, there are three input fields: "MAC Address" (empty), "MTU" (empty), and "MSS" (empty). Each field has a descriptive text below it explaining its purpose and format.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Configure WAN Interface

Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType:

General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for connection types will be assumed.

MSS

If a value is entered in this field, the MSS (maximum segment size) for TCP connections to the value entered above minus 40 bytes will be used.

Vérification de la configuration de la carte réseau local LAN

The screenshot shows the pfSense web interface for configuring a LAN interface. It features the same navigation menu and warning message as the previous page. The breadcrumb trail is "Wizard / pfSense Setup / Configure LAN Interface". The progress bar shows "Step 5 of 9". The heading is "Configure LAN Interface" with the instruction: "On this screen the Local Area Network information will be configured." The "LAN IP Address" field contains "192.168.20.1" and has a note below it: "Type dhcp if this interface uses DHCP to obtain its IP address." The "Subnet Mask" dropdown menu is set to "24". At the bottom, there is a blue "Next" button with a double arrow icon.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

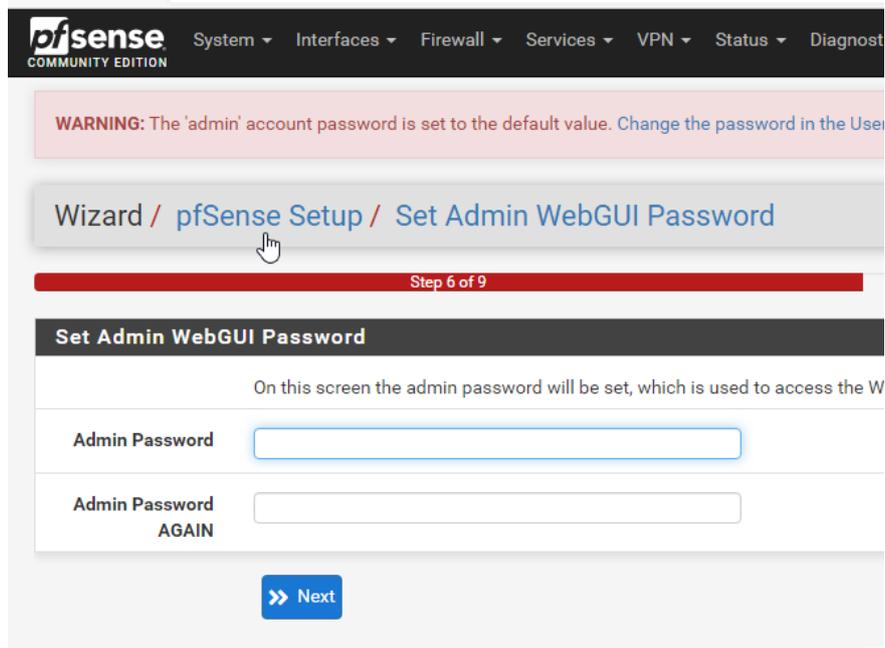
LAN IP Address:

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask:

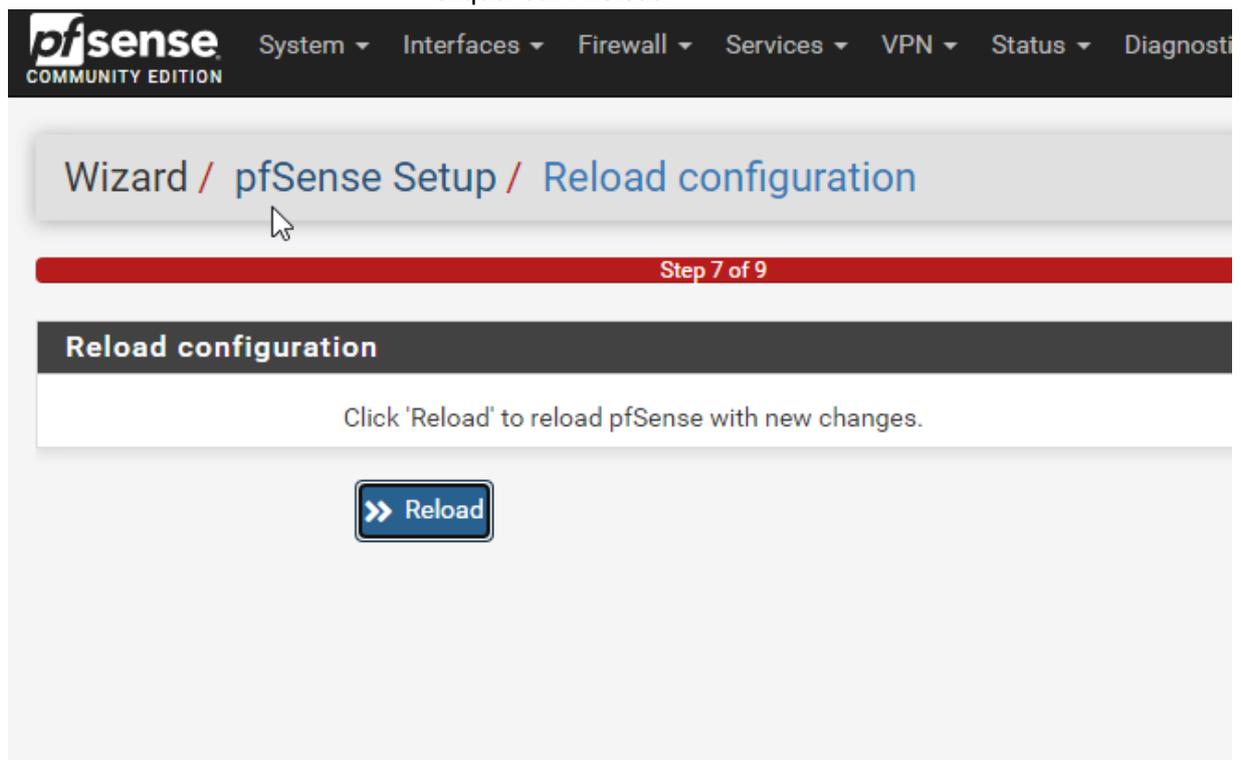
[Next](#)

Modifier le mot de passe admin



The screenshot shows the pfSense web interface. At the top, there is a navigation menu with the pfSense logo and the text 'COMMUNITY EDITION'. Below the menu, there is a warning message: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The breadcrumb trail is 'Wizard / pfSense Setup / Set Admin WebGUI Password'. A progress bar indicates 'Step 6 of 9'. The main heading is 'Set Admin WebGUI Password'. Below this, there is a text box that says 'On this screen the admin password will be set, which is used to access the WebGUI.' There are two input fields: 'Admin Password' and 'Admin Password AGAIN'. A blue button with a double arrow and the text 'Next' is at the bottom.

Cliquer sur : Reload



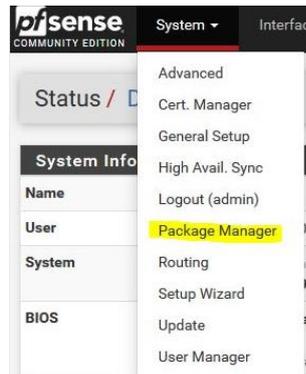
The screenshot shows the pfSense web interface. At the top, there is a navigation menu with the pfSense logo and the text 'COMMUNITY EDITION'. Below the menu, there is a breadcrumb trail: 'Wizard / pfSense Setup / Reload configuration'. A progress bar indicates 'Step 7 of 9'. The main heading is 'Reload configuration'. Below this, there is a text box that says 'Click 'Reload' to reload pfSense with new changes.' A blue button with a double arrow and the text 'Reload' is at the bottom.

Figure 62 : PFSense /Configuration de PFSENSE

9.1

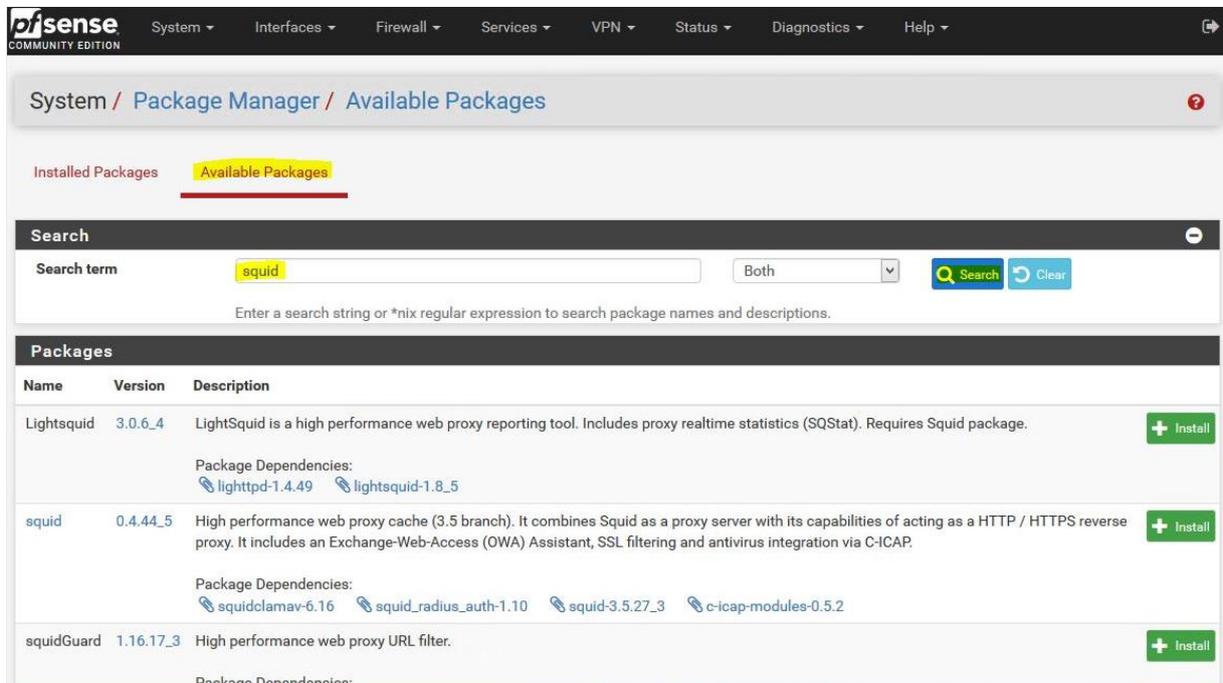
Mise en place d'un proxy transparent Squid avec filtrage d'URL

Sélectionner : System, Package Manager



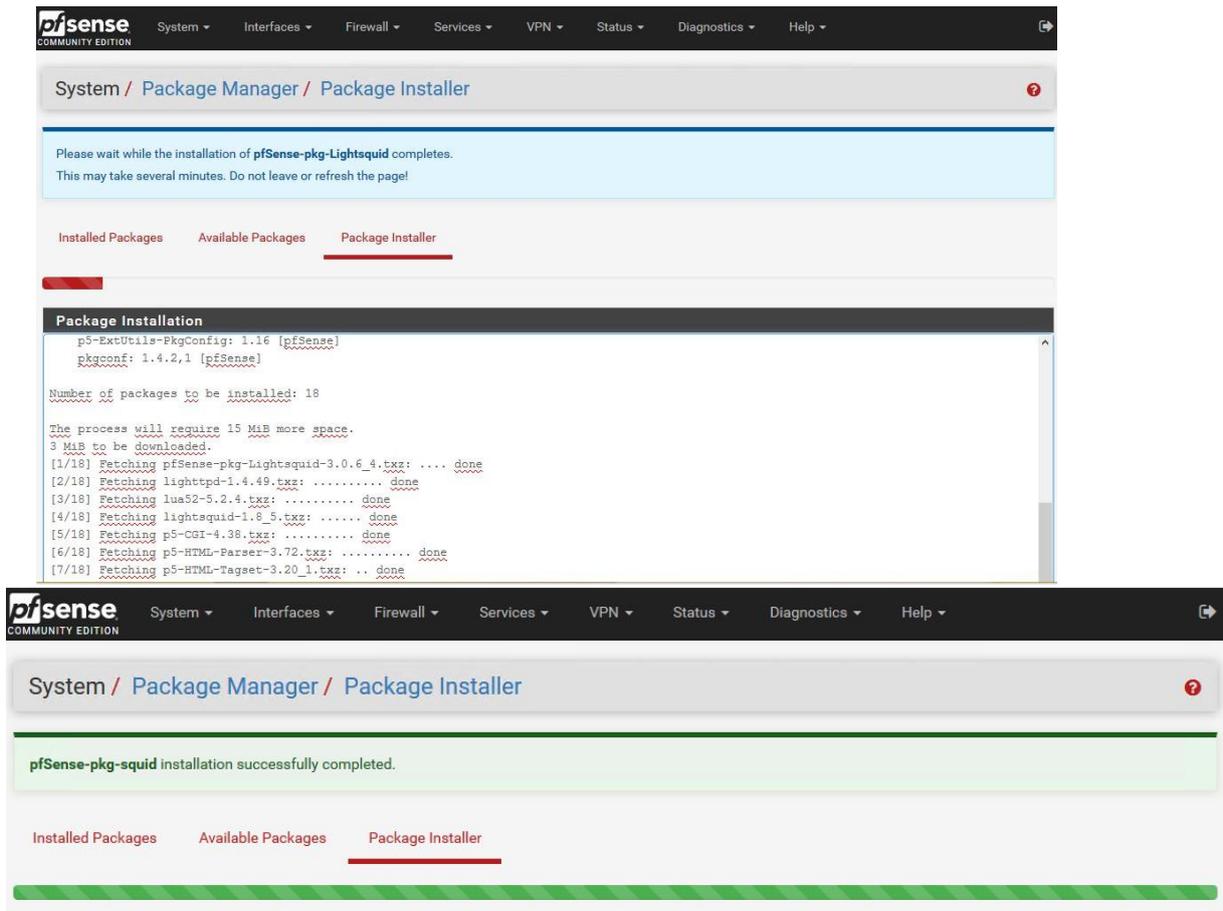
Sélectionner « Available Packages », dans la recherche taper « squid » puis cliquez sur « Search »

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

A screenshot of the pfSense web interface showing the 'Available Packages' page. The search term 'squid' is entered in the search box. The results table lists three packages: Lightsquid, squid, and squidGuard, each with an 'Install' button.

Name	Version	Description	Install
Lightsquid	3.0.6_4	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: lighttpd-1.4.49 lightsquid-1.8_5	+ Install
squid	0.4.44_5	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-6.16 squid_radius_auth-1.10 squid-3.5.27_3 c-icap-modules-0.5.2	+ Install
squidGuard	1.16.17_3	High performance web proxy URL filter. Package Dependencies:	+ Install

Installation des Packages



Les 3 Packages sont installés

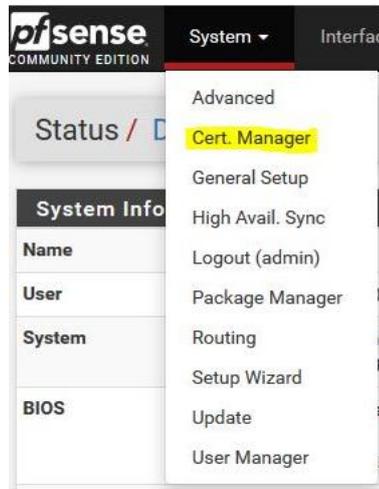
Name	Category	Version	Description	Actions
✓ Lightsquid	www	3.0.6_4	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	🗑️ ↻
Package Dependencies: lighttpd-1.4.49 lightsquid-1.8_5				
✓ squid	www	0.4.44_5	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	🗑️ ↻ ⓘ
Package Dependencies: squidclamav-6.16 squid_radius_auth-1.10 squid-3.5.27_3 c-icap-modules-0.5.2				
✓ squidGuard	www	1.16.17_3	High performance web proxy URL filter.	🗑️ ↻
Package Dependencies: squidguard-1.4_15				

🔄 = Update ✓ = Current
 🗑️ = Remove ⓘ = Information ↻ = Reinstall
Newer version available

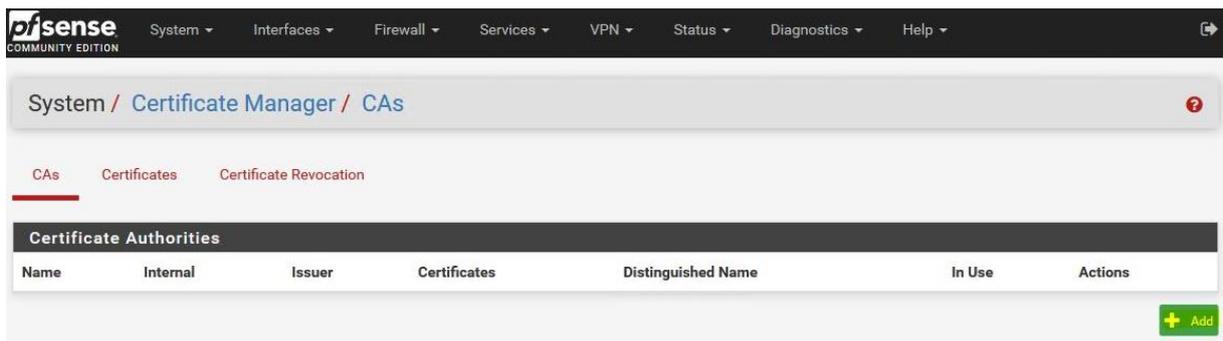
Figure 63 : PFsense Filtrage /Installation des packages

Création du Certificat pour le filtrage en HTTPS

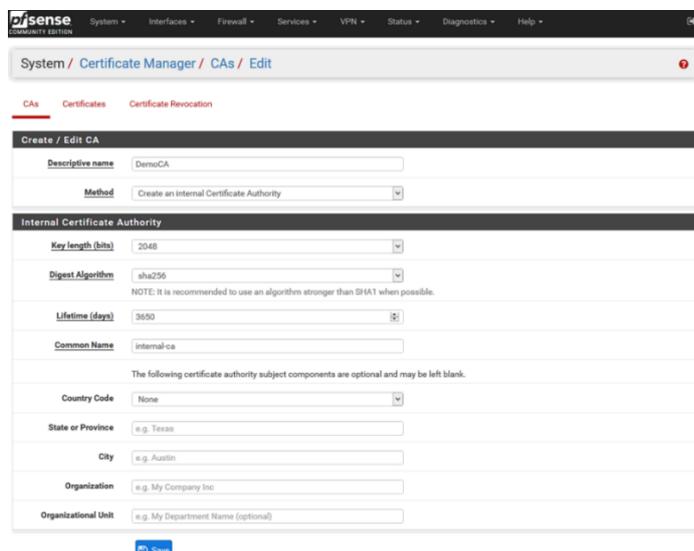
Sélectionner : System , Cert. Manager



Cliquer sur « Add »



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



Le Certificat est créé

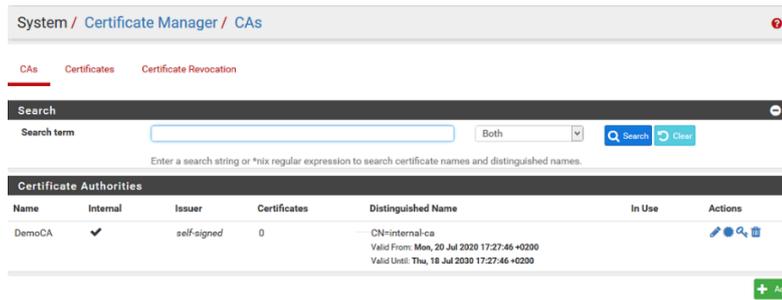
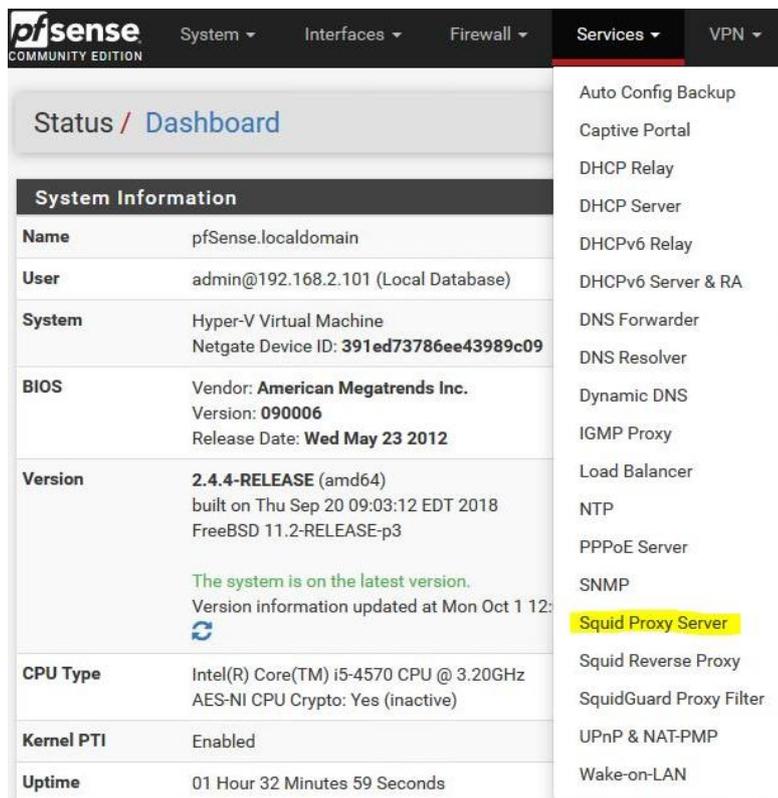


Figure 64 : PfSense Filtrage /Configuration du certificat

Configuration de Squid

Sélectionner « Services » et « Squid Proxy Server »



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

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

Cliquer sur « **Save** »

The screenshot shows the 'Local Cache' configuration page in the Palo Alto Networks Proxy Server. The page is divided into several sections:

- Squid Cache General Settings:**
 - Cache Replacement Policy: Heap LFUDA
 - Low-Water Mark in %: 90
 - High-Water Mark in %: 95
- Squid Hard Disk Cache Settings:**
 - Hard Disk Cache Size: 500
 - Hard Disk Cache System: ufs
 - Clear Disk Cache NOW: Button to clear the cache immediately.
 - Level 1 Directories: 16
 - Hard Disk Cache Location: /var/squid/cache
 - Minimum Object Size: 0
 - Maximum Object Size: 4
- Squid Memory Cache Settings:**
 - Memory Cache Size: 64
 - Maximum Object Size in RAM: 256
 - Memory Replacement Policy: Heap GDSP
- Dynamic and Update Content:**
 - Cache Dynamic Content: Select to enable caching of dynamic content.
 - Custom refresh_patterns: Text area for entering custom refresh patterns.

A 'Save' button is located at the bottom of the page.

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

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt Authentication Users Real Time Sync

Squid General Settings

Enable Squid Proxy Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Proxy Interface(s) LAN
WAN
loopback
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Proxy Port
This is the port the proxy server will listen on. Default: 3128

ICP Port
This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

Allow Users on Interface If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.

Patch Captive Portal **This feature was removed - see Bug #5594 for details!**

Resolve DNS IPv4 First Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.

Disable ICMP Check this to disable Squid ICMP pinger helper.

Use Alternate DNS Servers for the Proxy Server
To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)

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

Transparent Proxy Settings

Transparent HTTP Proxy Enable transparent mode to forward all requests for destination port 80 to the proxy server.
Transparent proxy mode works without any additional configuration being necessary on clients.
Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s) LAN
WAN
loopback
The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

Bypass Proxy for Private Address Destination Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.

Bypass Proxy for These Source IPs
Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.
Applies only to transparent mode. Separate entries by semi-colons (;)

Bypass Proxy for These Destination IPs
Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.
Applies only to transparent mode. Separate entries by semi-colons (;)

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

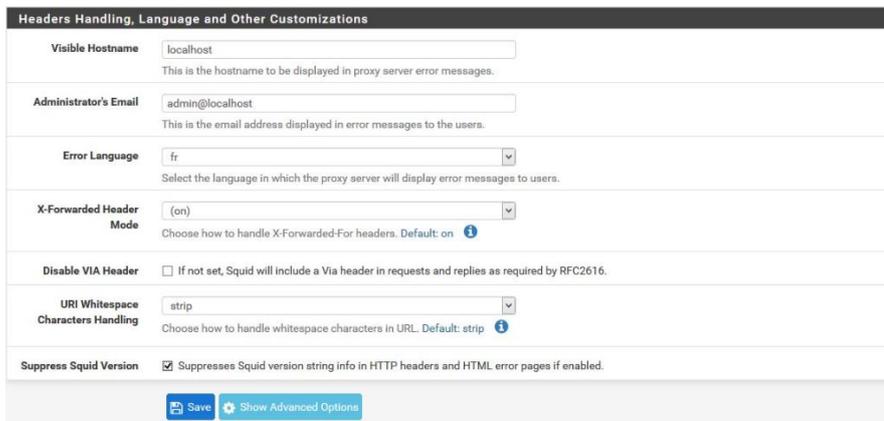
SSL Man in the Middle Filtering	
HTTPS/SSL Interception	<input checked="" type="checkbox"/> Enable SSL filtering.
SSL/MITM Mode	<input type="text" value="Splice All"/> <small>The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. Click Info for details. ⓘ</small>
SSL Intercept Interface(s)	<input type="text" value="10.10.10.1 (pfB DNSBL - DO NOT EDIT)"/> WAN LAN <small>The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.</small>
SSL Proxy Port	<input type="text" value="3129"/> <small>This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129</small>
SSL Proxy Compatibility Mode	<input type="text" value="Modern"/> <small>The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details. ⓘ</small>
DHParams Key Size	<input type="text" value="2048 (default)"/> <small>DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.</small>
CA	<input type="text" value="DemoCA"/> <small>Select Certificate Authority to use when SSL interception is enabled. ⓘ</small>
SSL Certificate Daemon Children	<input type="text" value="5"/> <small>This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5</small>

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

Logging Settings	
Enable Access Logging	<input checked="" type="checkbox"/> This will enable the access log. Warning: Do NOT enable if available disk space is low.
Log Store Directory	<input type="text" value="/var/squid/logs"/> <small>The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs Important: Do NOT include the trailing / when setting a custom location.</small>
Rotate Logs	<input type="text" value="365"/> <small>Defines how many days of logfiles will be kept. Rotation is disabled if left empty.</small>
Log Pages Denied by SquidGuard	<input type="checkbox"/> Makes it possible for SquidGuard denied log to be included on Squid logs. <small>Click Info for detailed instructions. ⓘ</small>

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

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



The screenshot shows the 'Headers Handling, Language and Other Customizations' section of the pfSense configuration interface. It contains several settings:

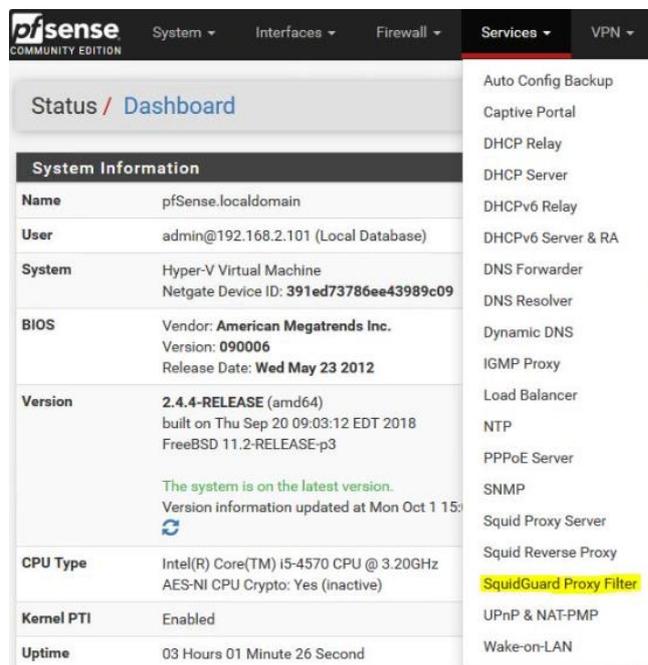
- Visible Hostname:** localhost
- Administrator's Email:** admin@localhost
- Error Language:** fr
- X-Forwarded Header Mode:** (on)
- Disable VIA Header:** If not set, Squid will include a Via header in requests and replies as required by RFC2616.
- URI Whitespace Characters Handling:** strip
- Suppress Squid Version:** Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

At the bottom, there are buttons for 'Save' and 'Show Advanced Options'.

Figure 65 : PFSense Filtrage /Configuration de Squid

Configuration de SquidGuard

Sélectionner « Services » et « SquidGuard Proxy Filter »



The screenshot shows the pfSense 'Services' menu. The 'SquidGuard Proxy Filter' option is highlighted in yellow. The menu also includes other services like Auto Config Backup, Captive Portal, DHCP Relay, etc.

Service
Auto Config Backup
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server & RA
DNS Forwarder
DNS Resolver
Dynamic DNS
IGMP Proxy
Load Balancer
NTP
PPPoE Server
SNMP
Squid Proxy Server
Squid Reverse Proxy
SquidGuard Proxy Filter
UPnP & NAT-PMP
Wake-on-LAN

Activer SquidGuard « Enable »

Package / Proxy filter SquidGuard: General settings / General settings

General settings | Common ACL | Groups ACL | Target categories | Times | Rewrites | Blacklist | Log | XMLRPC Sync

General Options

Enable Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked.**

SquidGuard service state: **STOPPED**

Activer « Enable Log » et « Enable log rotation »

Logging options

Enable GUI log Check this option to log the access to the Proxy Filter GUI.

Enable log Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

Enable log rotation Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

Miscellaneous

Clean Advertising Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

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

Puis cliquez sur « **Save** »

Blacklist options

Blacklist Check this option to enable blacklist
Do NOT enable this on NanoBSD installs!

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass]. Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

Blacklist URL

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfSense (/tmp/blacklist.tar.gz).

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

The screenshot shows the pfSense web interface for the SquidGuard Blacklists configuration. The breadcrumb trail is "Package / SquidGuard / Blacklists". The "Blacklist" tab is selected in the top navigation bar. The main section is titled "Blacklist Update" and contains a progress indicator for "Blacklist DB rebuild progress". A text input field shows the URL "http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz". Below the input are three buttons: "Download" (green), "Cancel" (orange), and "Restore Default" (blue). A note below the buttons says "Enter FTP or HTTP path to the blacklist archive here." Below this is a "Blacklist update Log" section with a scrollable log area containing the following text:

```
Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download
/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 58 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.
```

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

The screenshot shows the pfSense web interface for the Common ACL configuration. The breadcrumb trail is "Package / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL". The "Common ACL" tab is selected in the top navigation bar. The main section is titled "General Options" and contains a "Target Rules" text input field. Below the input field is a "Target Rules List" section with a plus sign icon to add new rules.

Sélectionner les catégories a bloquer (ou a autoriser)

Important : Sélectionner »Allow « pour « Default access [all] »

Target Rules List  		
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.		
Target Categories		
[blk_blacklists_adult]	access	deny ▼
[blk_blacklists_agresif]	access	deny ▼
[blk_blacklists_arjel]	access	— ▼
[blk_blacklists_associations_religieuses]	access	— ▼
[blk_blacklists_astrology]	access	— ▼
[blk_blacklists_audio-video]	access	— ▼
[blk_blacklists_bank]	access	— ▼
[blk_blacklists_bitcoin]	access	deny ▼
[blk_blacklists_blog]	access	— ▼
[blk_blacklists_celebrity]	access	— ▼
[blk_blacklists_chat]	access	— ▼
[blk_blacklists_child]	access	— ▼
[blk_blacklists_cleaning]	access	— ▼
[blk_blacklists_cooking]	access	— ▼
[blk_blacklists_cryptojacking]	access	deny ▼
[blk_blacklists_dangerous_material]	access	deny ▼
[blk_blacklists_dating]	access	— ▼
[blk_blacklists_ddos]	access	— ▼
[blk_blacklists_dialer]	access	— ▼
[blk_blacklists_download]	access	— ▼
[blk_blacklists_drogu]	access	deny ▼
[blk_blacklists_educational_games]	access	— ▼
[blk_blacklists_liste_bu]	access	— ▼
[blk_blacklists_malware]	access	— ▼
[blk_blacklists_manga]	access	— ▼
[blk_blacklists_marketingware]	access	— ▼
[blk_blacklists_mixed_adult]	access	— ▼
[blk_blacklists_mobile-phone]	access	— ▼
[blk_blacklists_phishing]	access	— ▼
[blk_blacklists_press]	access	— ▼
[blk_blacklists_publicite]	access	— ▼
[blk_blacklists_radio]	access	— ▼
[blk_blacklists_reaffected]	access	— ▼
[blk_blacklists_redirector]	access	— ▼
[blk_blacklists_remote-control]	access	— ▼
[blk_blacklists_sect]	access	— ▼
[blk_blacklists_sexual_education]	access	— ▼
[blk_blacklists_shopping]	access	— ▼
[blk_blacklists_shortener]	access	— ▼
[blk_blacklists_social_networks]	access	— ▼
[blk_blacklists_special]	access	— ▼
[blk_blacklists_sports]	access	— ▼
[blk_blacklists_strict_redirector]	access	— ▼
[blk_blacklists_strong_redirector]	access	— ▼
[blk_blacklists_translation]	access	— ▼
[blk_blacklists_tricheur]	access	— ▼
[blk_blacklists_update]	access	— ▼
[blk_blacklists_warez]	access	— ▼
[blk_blacklists_webmail]	access	— ▼
Default access [all]	access	allow ▼

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

Do not allow IP-Addresses in URL	<input checked="" type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.
Proxy Denied Error	<input type="text"/> The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by Sg[product_name] proxy"
Redirect mode	<input type="text" value="int error page (enter error message)"/> Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible. Options: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'
Redirect info	<input type="text"/> Enter external redirection URL, error message or size (bytes) here.
Use SafeSearch engine	<input checked="" type="checkbox"/> Enable the protected mode of search engines to limit access to mature content. At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search and Bing. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. Note: This option overrides 'Rewrite' setting.
Rewrite	<input type="text" value="none (rewrite not defined)"/> Enter the rewrite condition name for this rule or leave it blank.
Log	<input type="checkbox"/> Check this option to enable logging for this ACL.
<input type="button" value="Save"/>	

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

Package / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL ⊞ ⊞ ⊞ ⊞ ⊞

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Target Rules

Target Rules List ⊞ ⊞

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

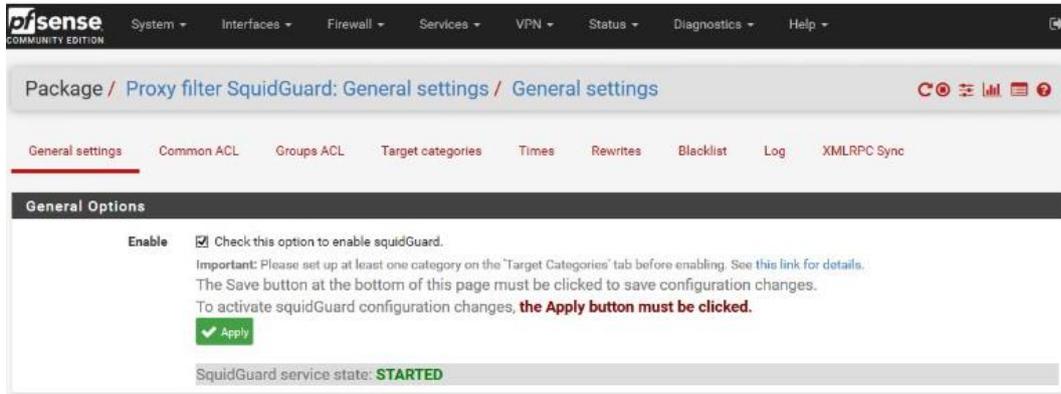
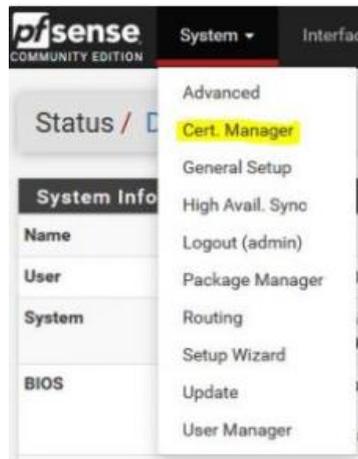


Figure 66 : PFSense Filtrage /Configuration de Squidguard

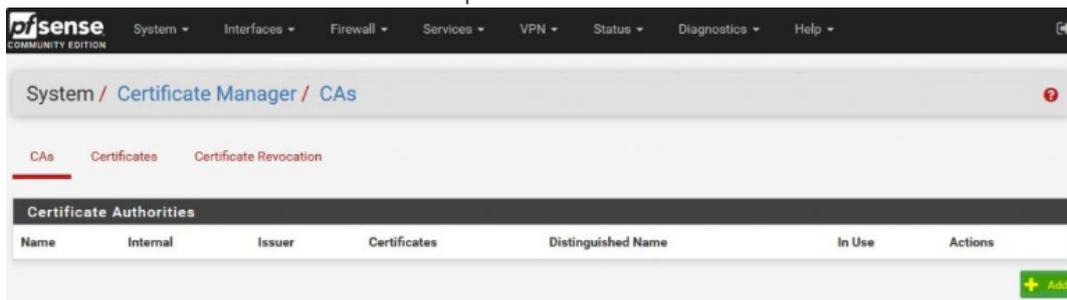
9.2 Configuration d'un tunnel VPN avec OpenVPN

Création de l'Autorité de Certification – CA

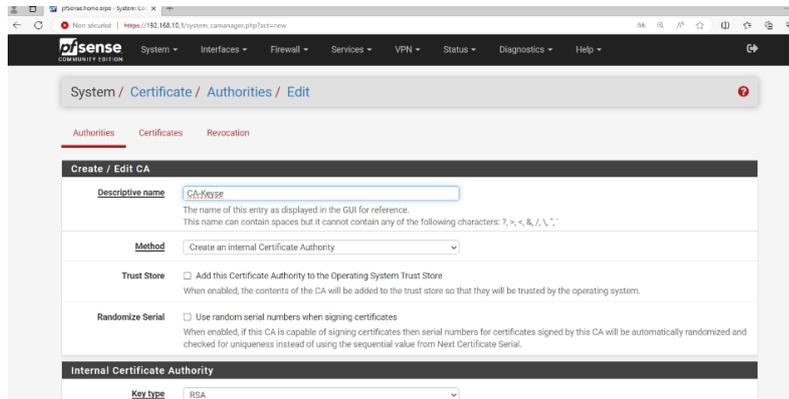
Sélectionner : System > **Cert. Manager**



Cliquer sur “+ Add”



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

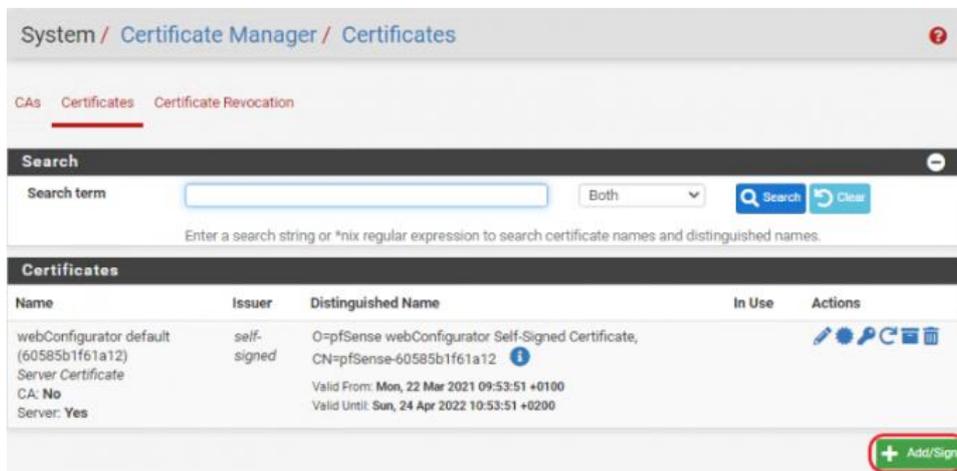


Le Certificat est créé

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-Keyse	✓	self-signed	2	CN=internal-ca Valid From: Tue, 27 Feb 2024 00:10:05 +0100 Valid Until: Fri, 24 Feb 2024 00:10:05 +0100		   

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** »

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name VPN Keyse
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ? , > , < , & , / , \ , * ,

Internal Certificate

Certificate authority CA-Keyse

Key type RSA

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

Digest Algorithm sha256
The digest method used when the certificate is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 306 days or some platforms may consider the certificate invalid.

Common Name vpn-keyse

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

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For internal Certificates, these attributes are added directly to the certificate as shown.

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

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

Add + Add

Save

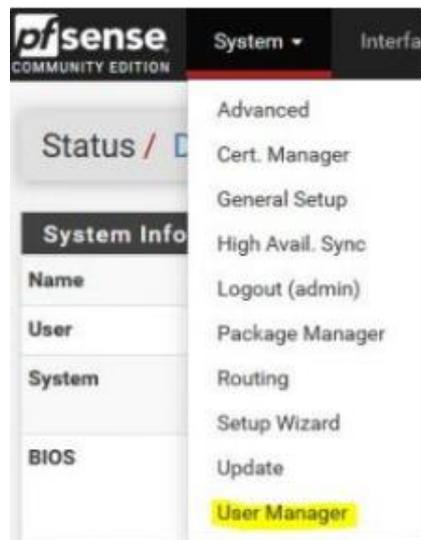
Le Certificat est créé.

VPN-Keyse Server Certificate CA: No Server: Yes	CA-Keyse	CN=vpn-keyse ⓘ Valid From: Tue, 27 Feb 2024 00:12:45 +0100 Valid Until: Fri, 24 Feb 2024 00:12:45 +0100	OpenVPN Server ⚙️ 🔑 🔄
--	----------	---	-----------------------

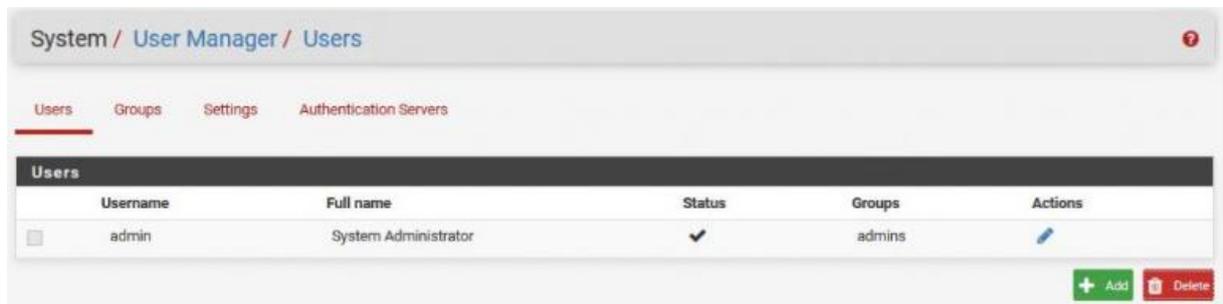
Figure 68 : PFSense VPN /Création du certificat serveur

Création des Utilisateurs du VPN

Sélectionner : System > **User Manager**



Cliquer sur "+ Add"



Entrer un **Nom d'Utilisateur** "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** »

The screenshot shows the 'Edit' page for a user in the PFSense User Manager. The breadcrumb trail is 'System / User Manager / Users / Edit'. The page has tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers'. The 'User Properties' section includes fields for 'Defined by' (USER), 'Disabled' (checkbox), 'Username' (Mathilde-Keyse), 'Password' (masked), 'Full name', 'Expiration date', 'Custom Settings', and 'Group membership' (admins). The 'Certificate' section has a checked checkbox for 'Click to create a user certificate'. Below this is the 'Create Certificate for User' section with 'Descriptive name' (CA Mathilde) and 'Certificate authority' (CA-Keyse).

L'Utilisateur du VPN est créé.

The screenshot shows the 'Users' list page in PFSense. The breadcrumb trail is 'Users / Groups / Settings / Authentication Servers'. The 'Users' section contains a table with the following data:

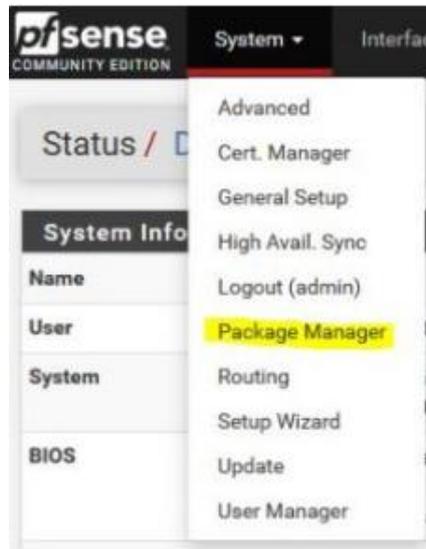
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	Mathilde-Keyse		✓		
<input type="checkbox"/>	admin	System Administrator	✓	admins	

At the bottom right, there are '+ Add' and 'Delete' buttons.

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 »

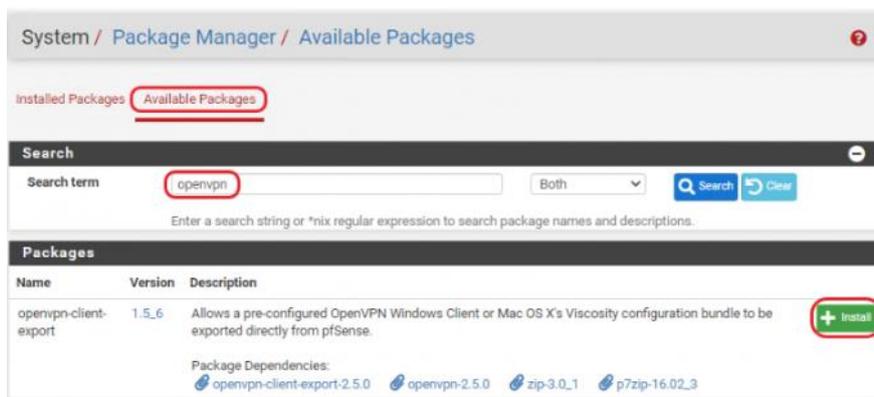
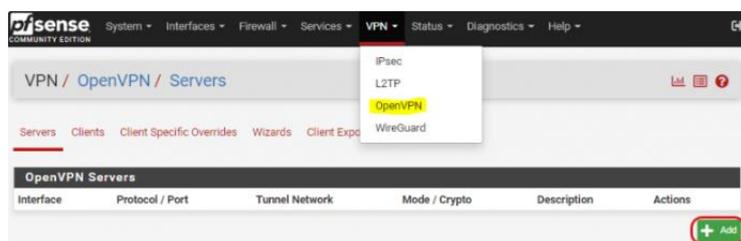


Figure 70 : PFSense VPN /Installation du package OpenVPN-client-export

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)

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export

General Information

Description
A description of this VPN for administrative reference.

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

Mode Configuration

Server mode

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

Endpoint Configuration

Protocol

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

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

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

Cryptographic Settings	
TLS Configuration	<input checked="" type="checkbox"/> Use a TLS Key <small>A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.</small>
	<input checked="" type="checkbox"/> Automatically generate a TLS Key
Peer Certificate Authority	CA-Keyse
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	<input type="checkbox"/> Check client certificates with OCSP
Server certificate	VPN-Keyse (Server: Yes, CA: CA-Keyse) <small>Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.</small>
DH Parameter Length	2048 bit <small>Diffie-Hellman (DH) parameter set used for key exchange. ⓘ</small>
ECDH Curve	Use Default <small>The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.</small>

- 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

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.0.8.0/24"/> <small>This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.</small> <small>A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Ext Notify, and Inactive.</small>
IPv6 Tunnel Network	<input type="text"/> <small>This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.</small>
Redirect IPv4 Gateway	<input checked="" type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv6 Local network(s)	<input type="text"/> <small>IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent connections	<input type="text" value="5"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>

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

Client Settings

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

Topology Subnet – One IP address per client in a common subnet

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

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

Advanced Configuration

Custom options

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

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

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	Mode: Remote Access (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	OpenVPN Keyse	  

[+ Add](#)

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 »

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

OpenVPN Server

Remote Access Server OpenVPN Keyse UDP4:16385

Client Connection Behavior

Host Name Resolution Other

Host Name 88.170.208.150
Enter the hostname or IP address the client will use to connect to this server.

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

Cliquer sur « **Save as default** »

Advanced

Additional configuration options auth-nocache

Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
EXAMPLE: remote-random;

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)

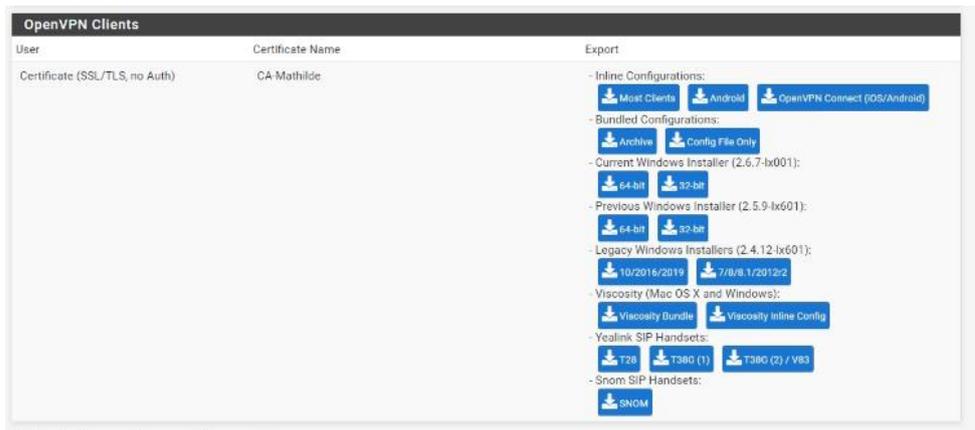
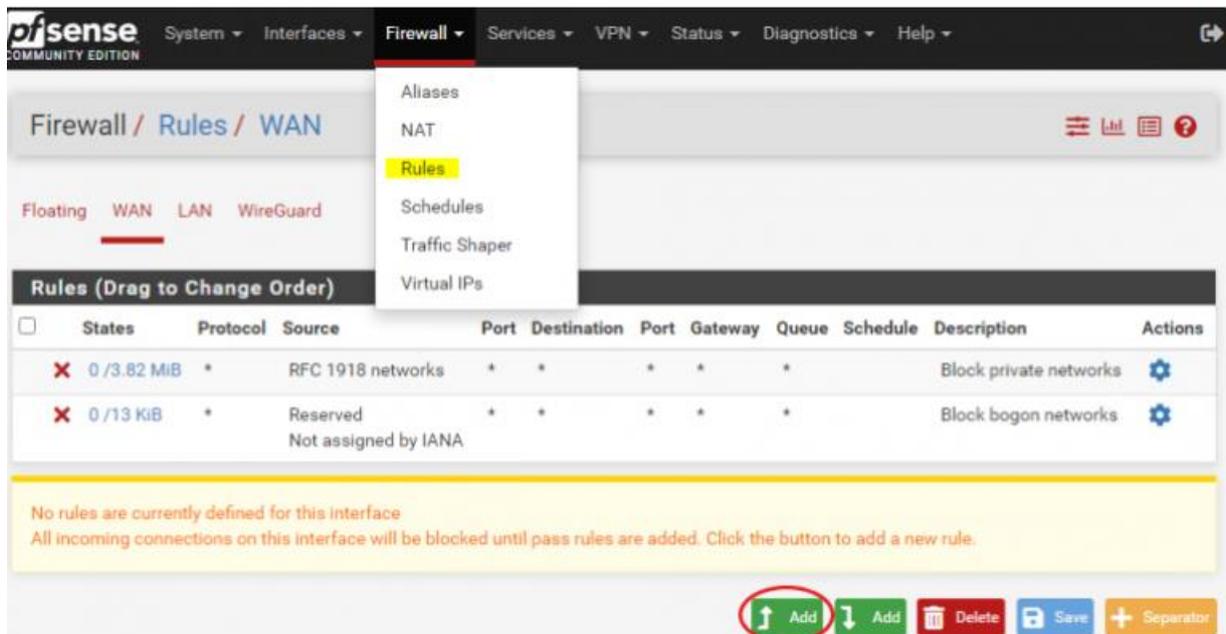


Figure 71 : PFsense VPN /Configuration du serveur OpenVPN

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**”

Edit Firewall Rule

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

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

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

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol UDP
Choose which IP protocol this rule should match.

Source

Source Invert match Any Source Address

Destination

Destination Invert match WAN address Destination Address

Destination Port Range OpenVPN (1194) OpenVPN (1194)
From Custom To Custom

Firewall > Rules > OpenVPN : cliquer sur “+ Add”

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

Cliquer sur “**Save**” et valider “**Apply Changes**”

Firewall / Rules / Edit

Edit Firewall Rule

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

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

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

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source

Source Invert match Any Source Address

Destination

Destination Invert match Any Destination Address

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 :

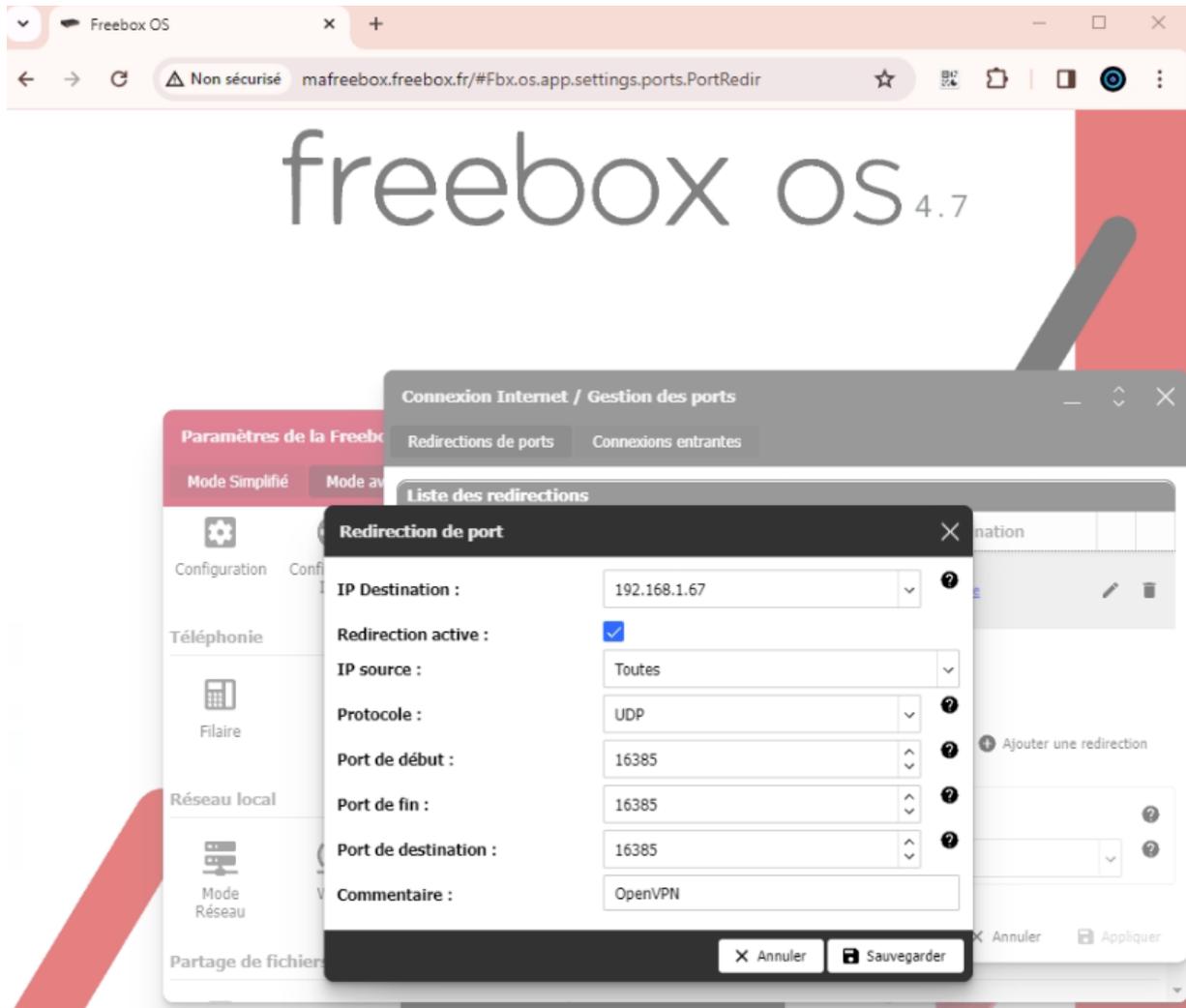
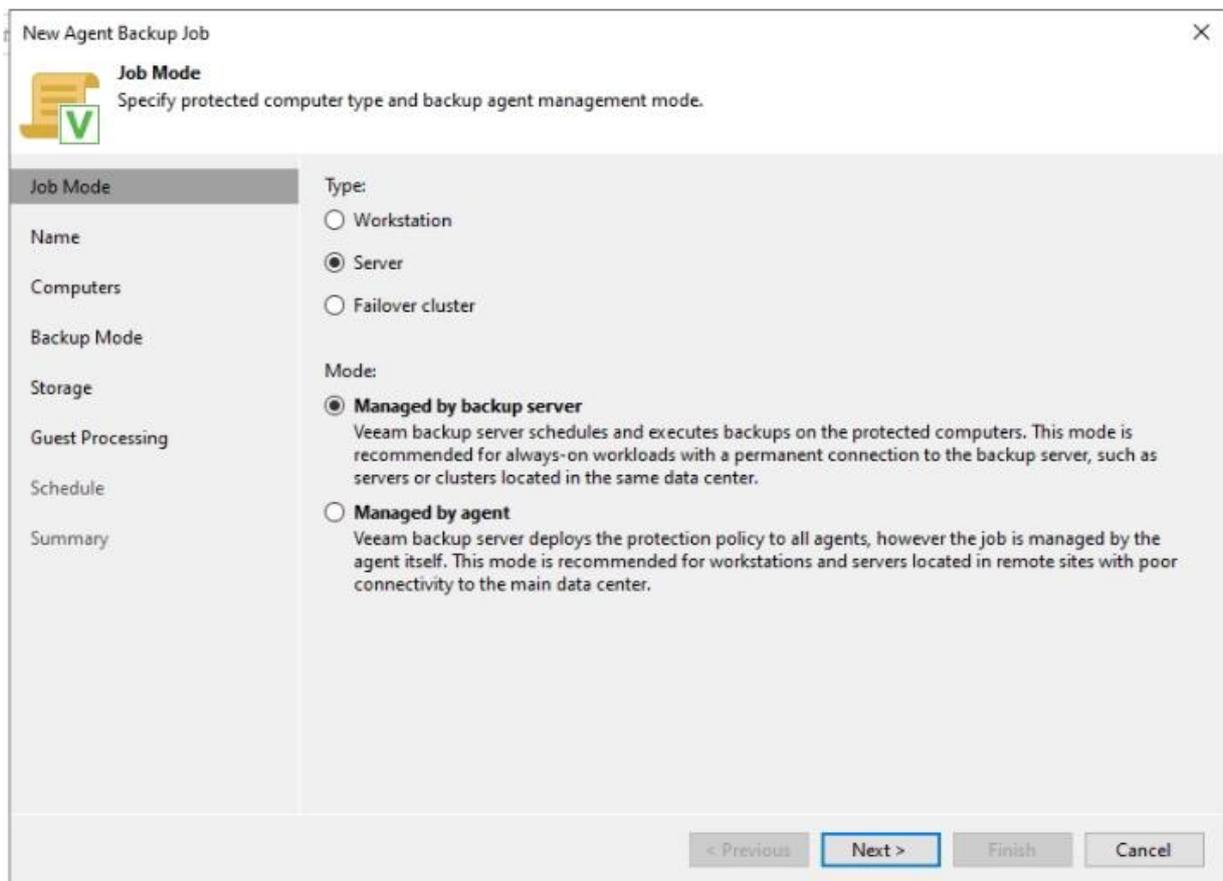


Figure 73 : PFSense VPN /Création de la redirection de port sur la box

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.



The screenshot shows the 'New Agent Backup Job' wizard window. The 'Job Mode' step is selected in the left-hand navigation pane. The main area displays the following configuration options:

- Job Mode:** Specify protected computer type and backup agent management mode.
- Type:**
 - Workstation
 - Server**
 - Failover cluster
- Mode:**
 - Managed by backup server**
Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.
 - Managed by agent**
Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

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

Attribuer un nom au job Créé.

New Agent Backup Job

Name
Type in a name and description for this agent backup job.

Job Mode

Name

Computers

Backup Mode

Storage

Guest Processing

Schedule

Summary

Name:
Agent Backup Job 1

Description:
Created by SRVVEAM01\USER at 05/03/2024 15:19.

High priority
Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

< Previous Next > Finish Cancel

Figure 75 : Veeam / Nommage du Job

Sélectionner votre groupe de machines serveur ou vos machines serveurs.

New Agent Backup Job

Computers
Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

Job Mode

Name

Computers

Backup Mode

Storage

Guest Processing

Schedule

Summary

Protected computers:

Name	Type
Keyse	Protection g...

Add...
Remove

Up
Down

< Previous Next > Finish Cancel

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)

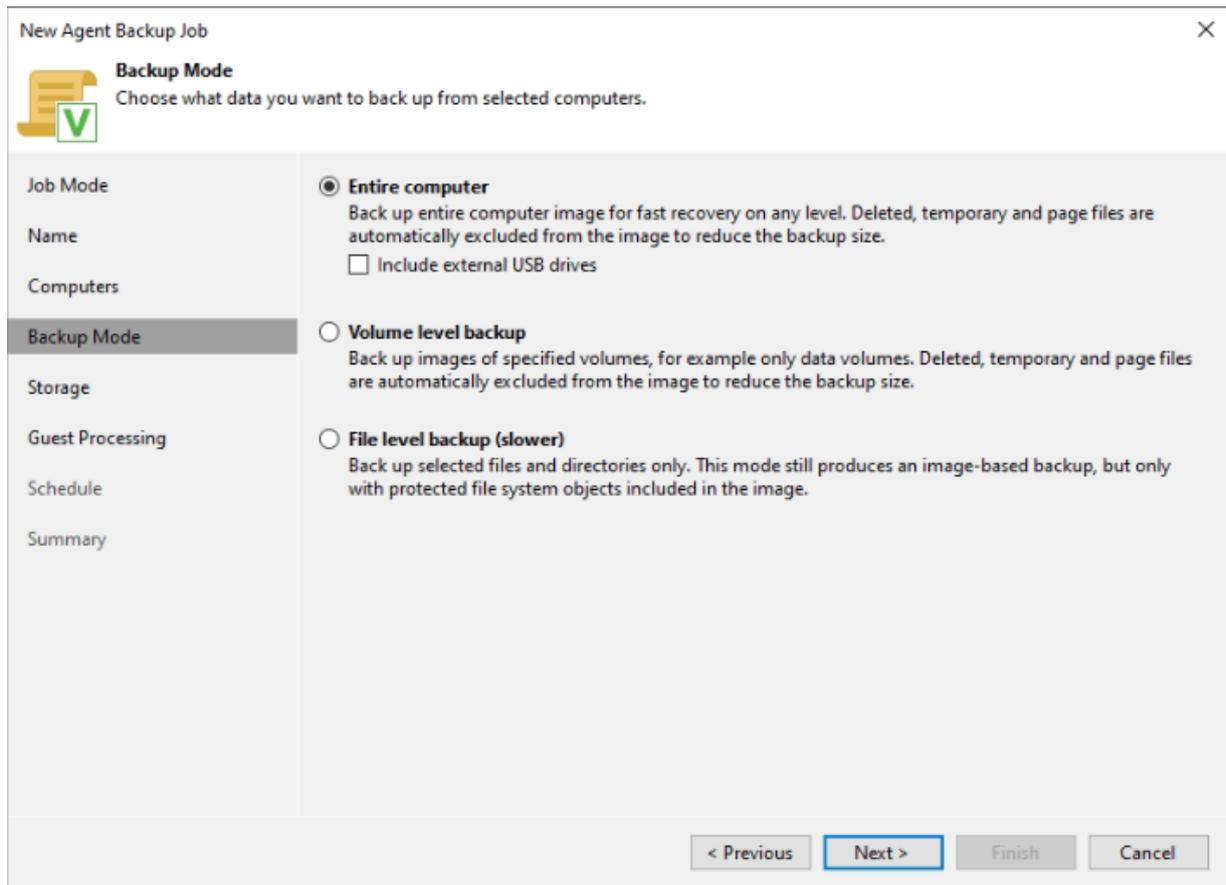


Figure 77 : Veeam / Sélections du type de sauvegarde

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

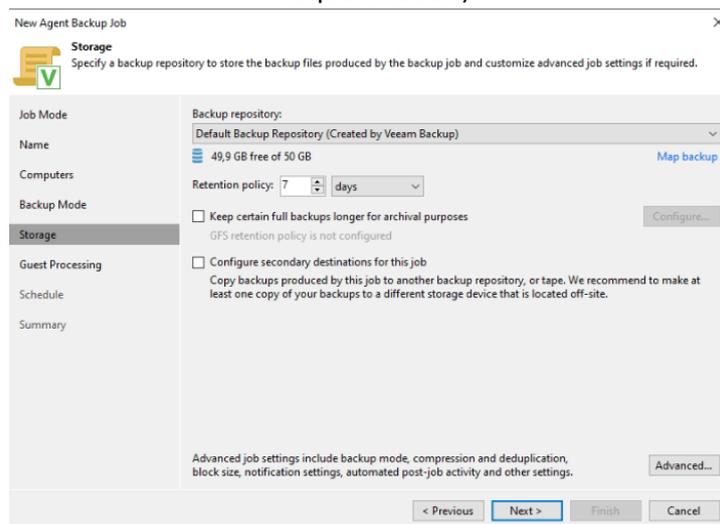


Figure 78 : Veeam / Sélections du volume de stockage de sauvegarde

Cliqué sur « next »

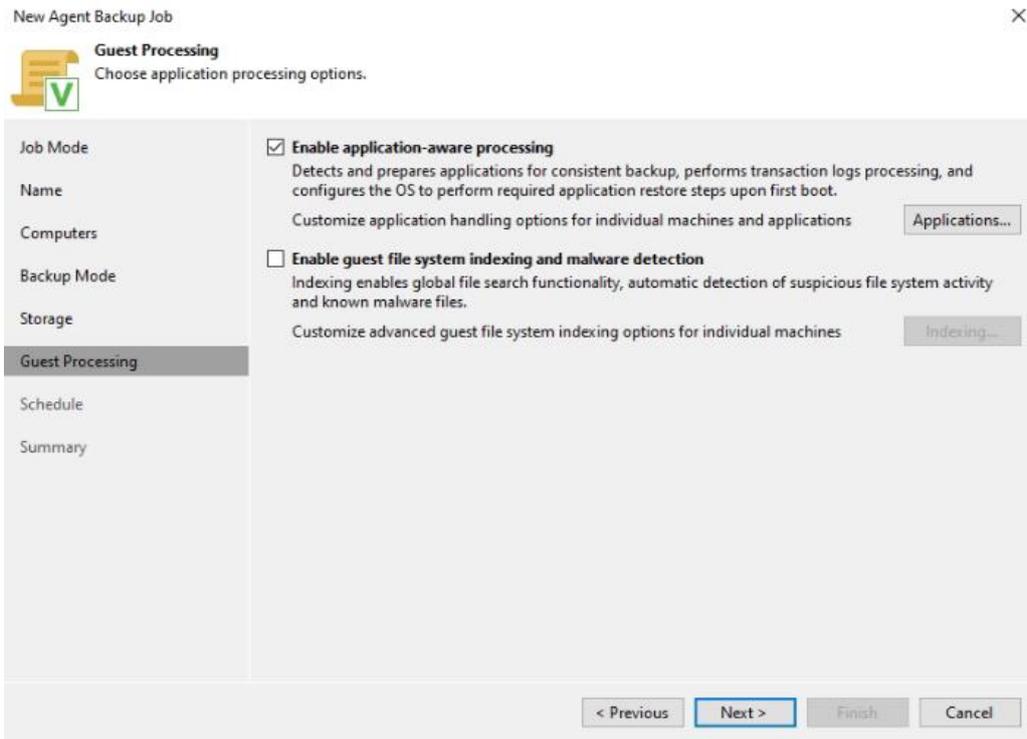


Figure 79 : Veeam / Guest Processing

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

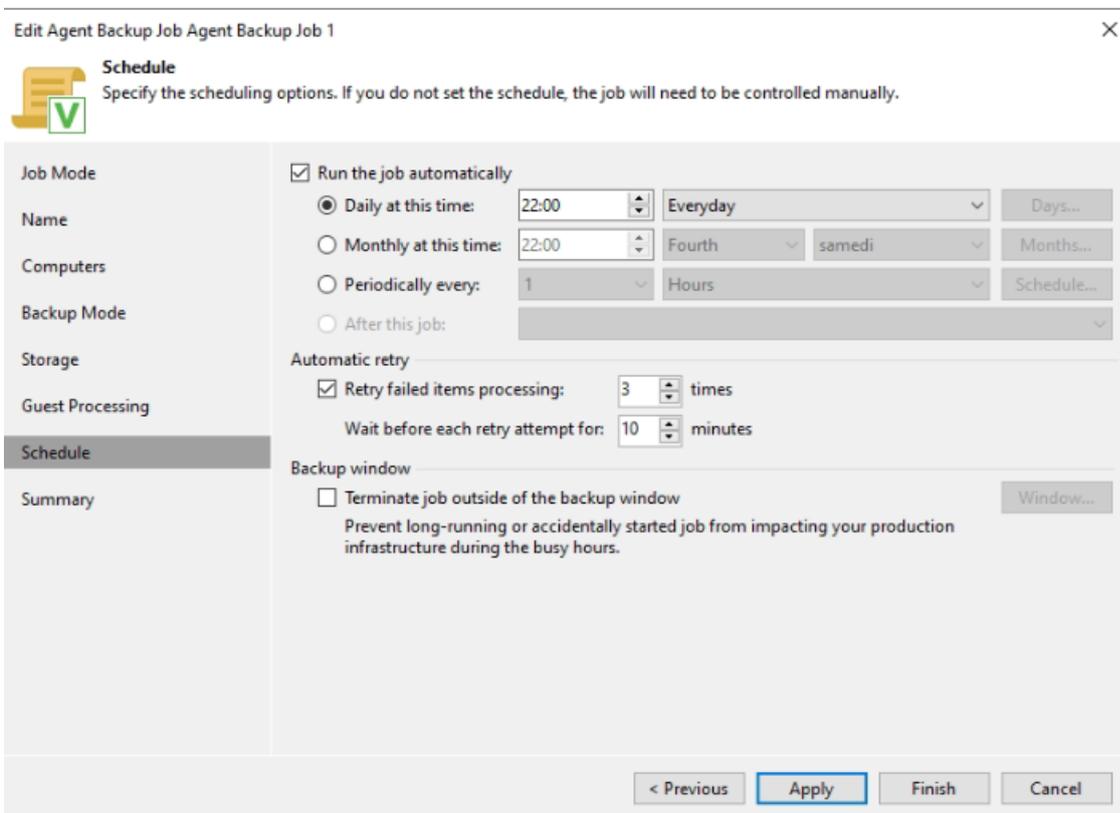


Figure 80 : Veeam / Planification du job de sauvegarde

Voici le résumé des paramètres du Job créé.

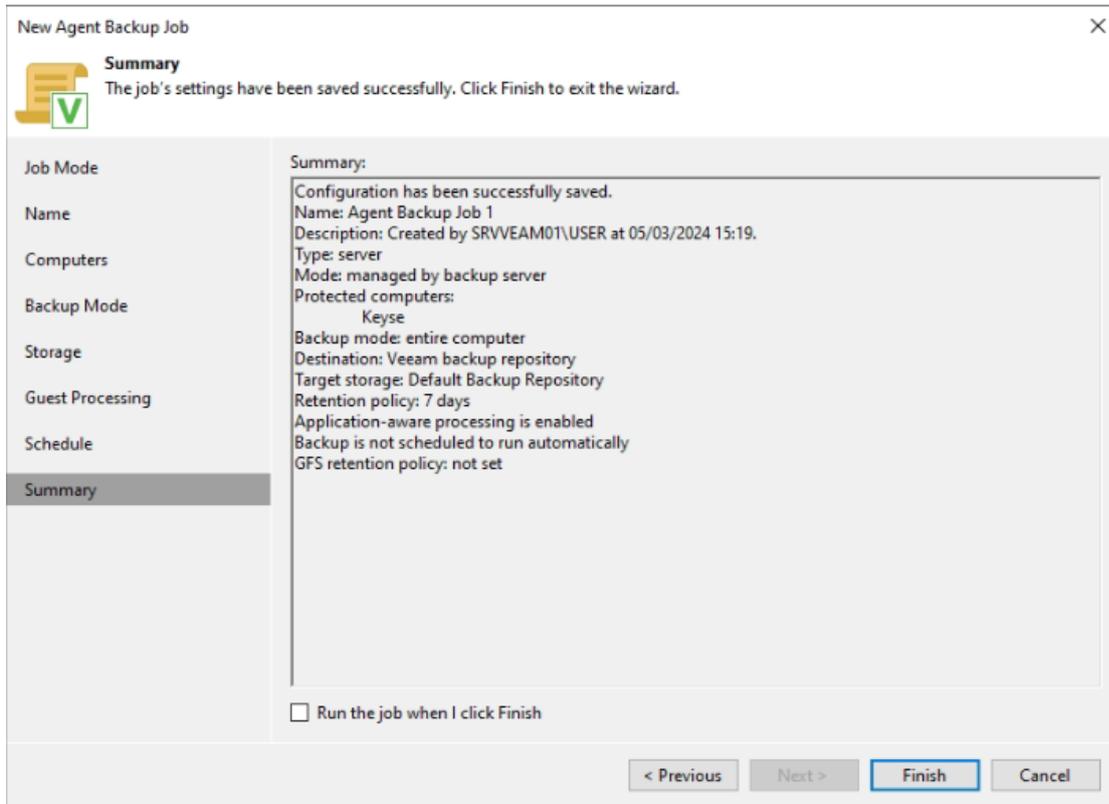


Figure 81 : Veeam / Résumé du Job

Nos serveurs ont été sauvegardé avec succès.

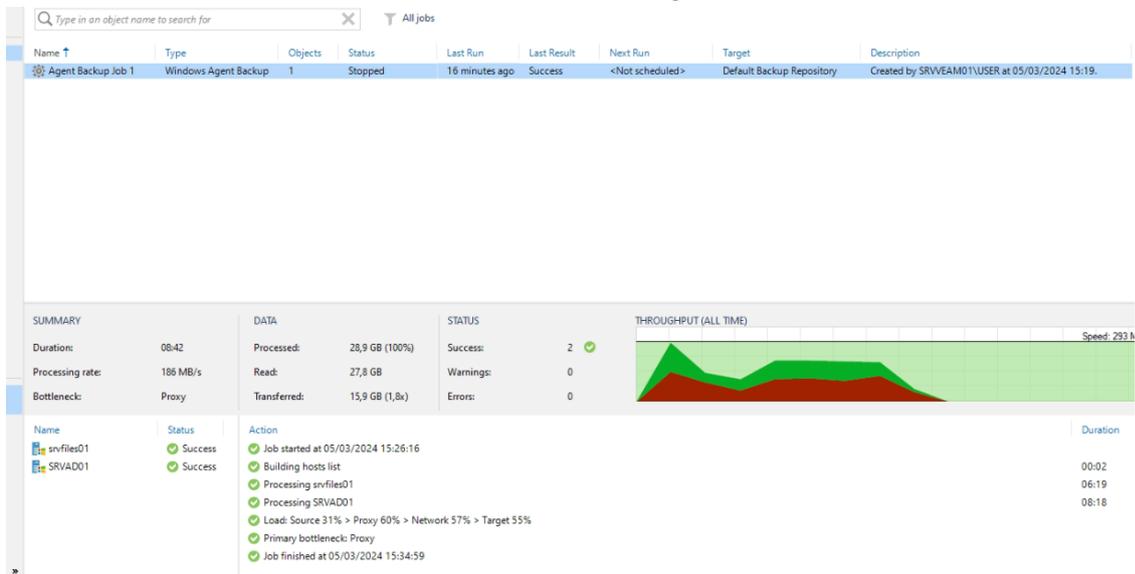


Figure 82 : Veeam / Sauvegarde effectuée