

Épreuve E5 – Administration des systèmes et des réseaux

Fiche technique



Projet 1 :

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, un serveur PRTG

Table des matières :

1 <i>Introduction :</i>	4
2 <i>Installation Windows Server 2022 :</i>	4
3 <i>Contrôleur de domaine :</i>	6
4 <i>Rôles et fonctionnalités :</i>	8
5 <i>Configuration Active Directory :</i>	12
5.1 <i>Paramétrage DHCP :</i>	15
5.2 <i>Paramétrage DNS :</i>	19
6 <i>Utilisateurs :</i>	20
7 <i>Serveur de fichier :</i>	38
8 <i>GPO :</i>	
9 <i>Firewall PFSense :</i>	
9.1 <i>Mise en place d'un proxy transparent Squid avec filtrage d'URL :</i>	
10 <i>PRTG</i>	

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 : PRTG / Prise en main de PRTG	
Figure 68 : PRTG / Utiliser PRTG	
Figure 69 : PRTG / Ping	
Figure 70 : PRTG / CPU	
Figure 71 : PRTG / Mémoire	
Figure 72 : PRTG / Espace disque	
Figure 73 : PRTG / Carte réseau	

1 Introduction :

Afin de répondre aux demandes de la Mission local de Montpellier, 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 :

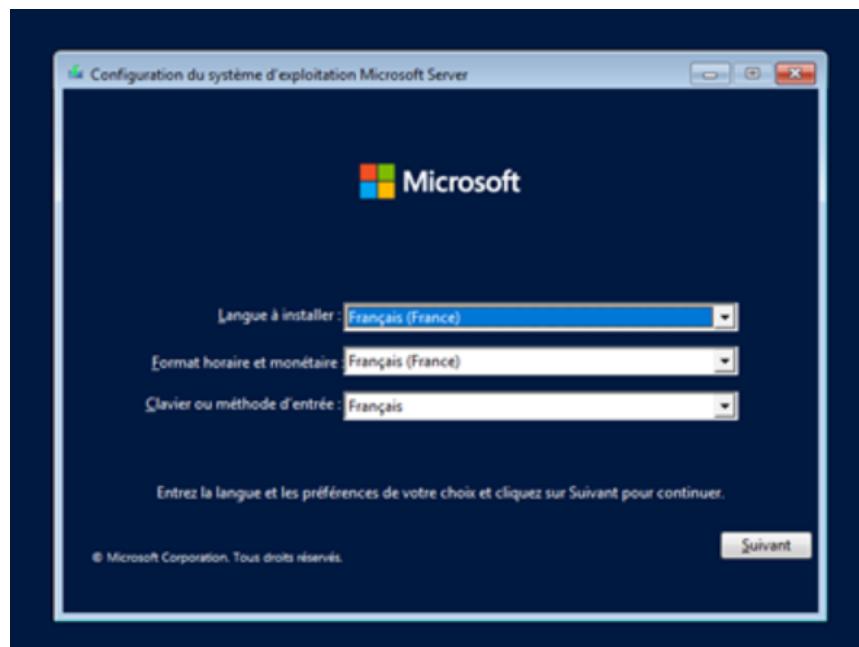


Figure 1 : Windows Server 2016 / langue

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.

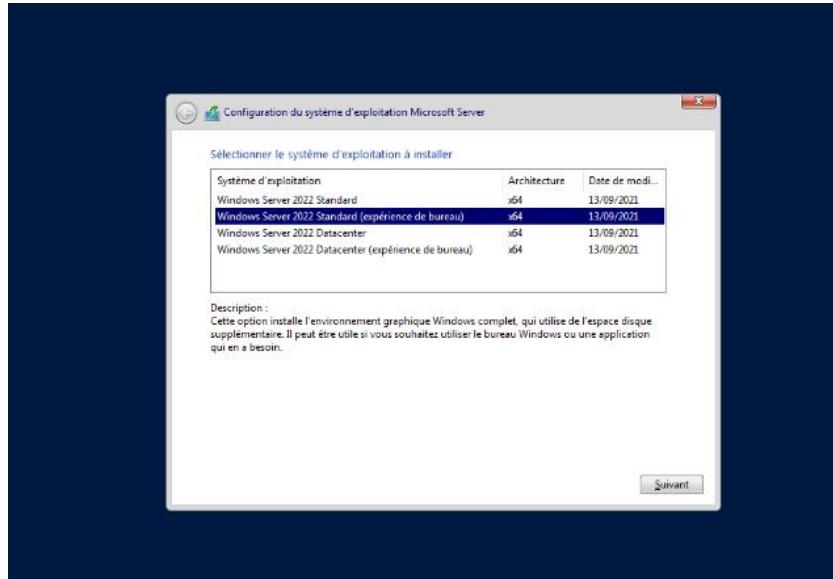


Figure 3 : Windows Server 2016 / Standard Evaluation (Expérience utilisateur)

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).

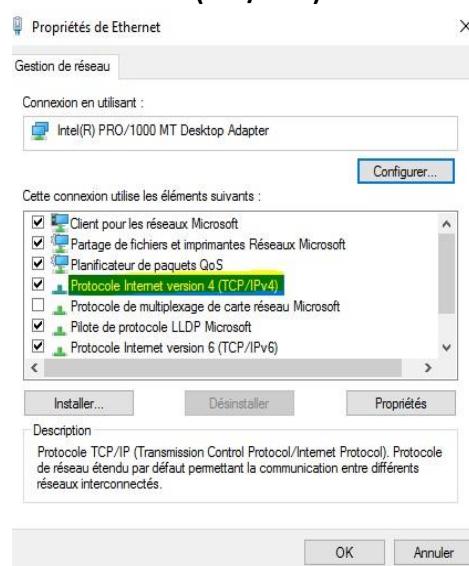


Figure 7 : Gestion de réseau Protocole TCP/IPv4

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

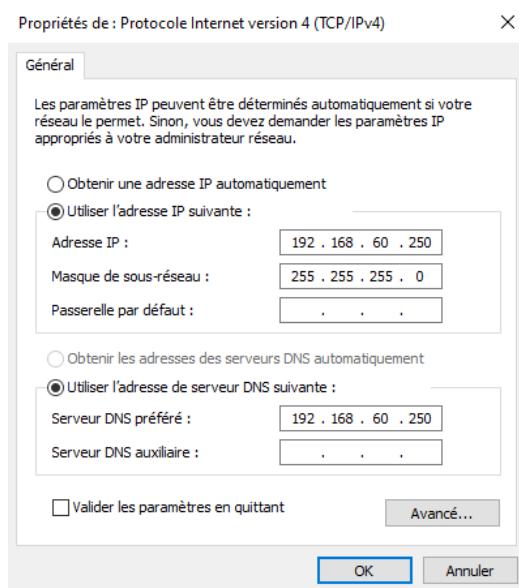


Figure 8 : Paramètres IP Protocole TCP/IPv4

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

Nom de l'ordinateur	dc1	Dernières mises à jour installées
Domaine	ML3M.com	Windows Update
Pare-feu Microsoft Defender	Public : Actif, Privé : Actif	Antivirus Microsoft Defender
Gestion à distance	Activé	Commentaires et diagnostics
Bureau à distance	Désactivé	Configuration de sécurité renforcée d'Internet Explore
Association de cartes réseau	Désactivé	Fuseau horaire
Ethernet0	Adresse IPv4 attribuée par DHCP, Compatible IPv6	ID de produit (Product ID)
Ethernet1	192.168.1.250, Compatible IPv6	
Gestion Azure Arc	Désactivé	
Version du système d'exploitation	Microsoft Windows Server 2022 Standard	Processeurs
Informations sur le matériel	VMware, Inc. VMware20,1	Mémoire installée (RAM)

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.

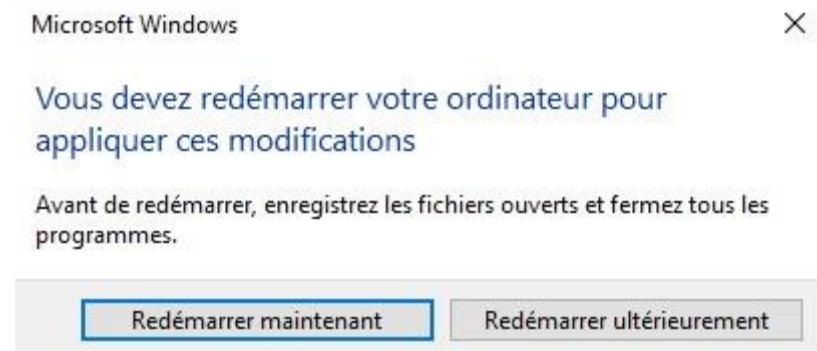


Figure 11 : « Redémarrer maintenant »

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.

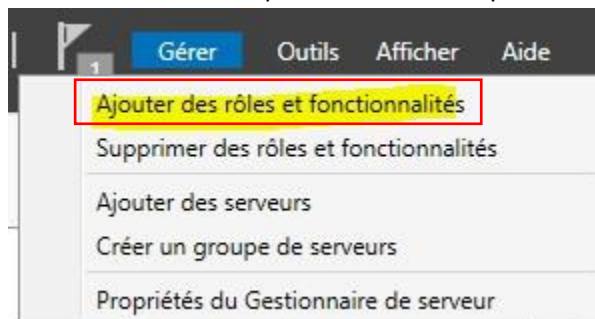


Figure 12 : Gérer / ajout des rôles et fonctionnalités

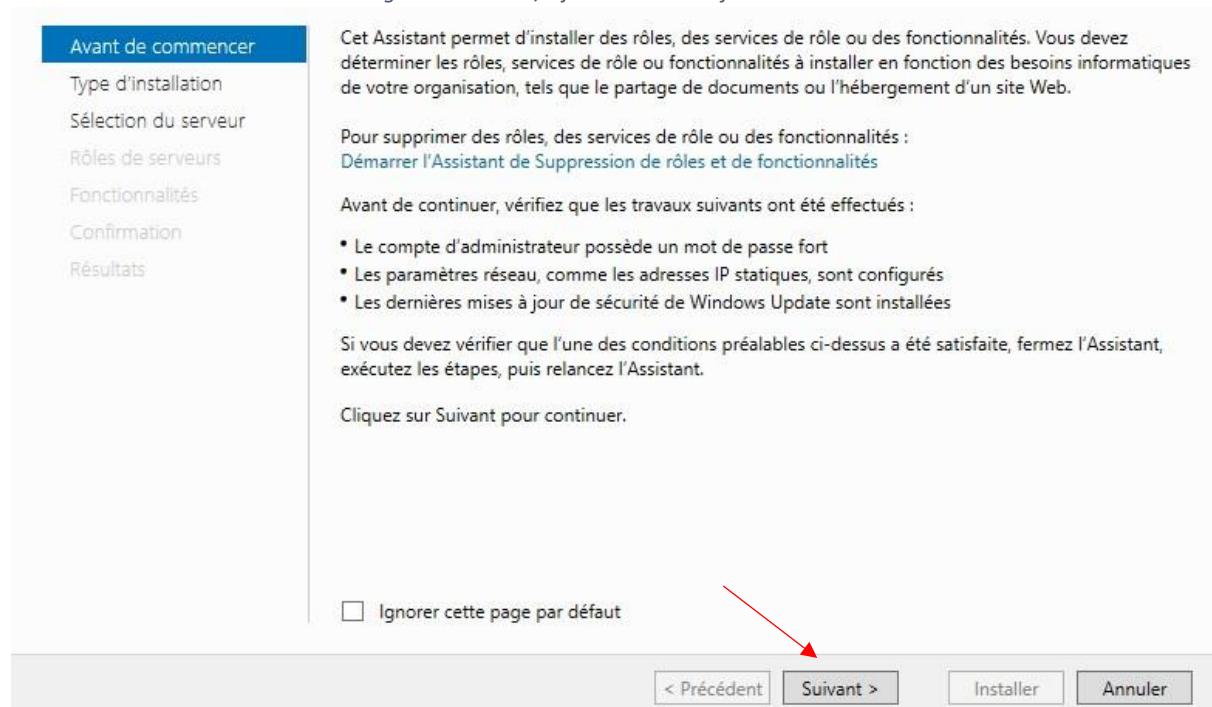


Figure 13 : Assistant / Avant de commencer

Installation basée sur un rôle ou une fonctionnalité.

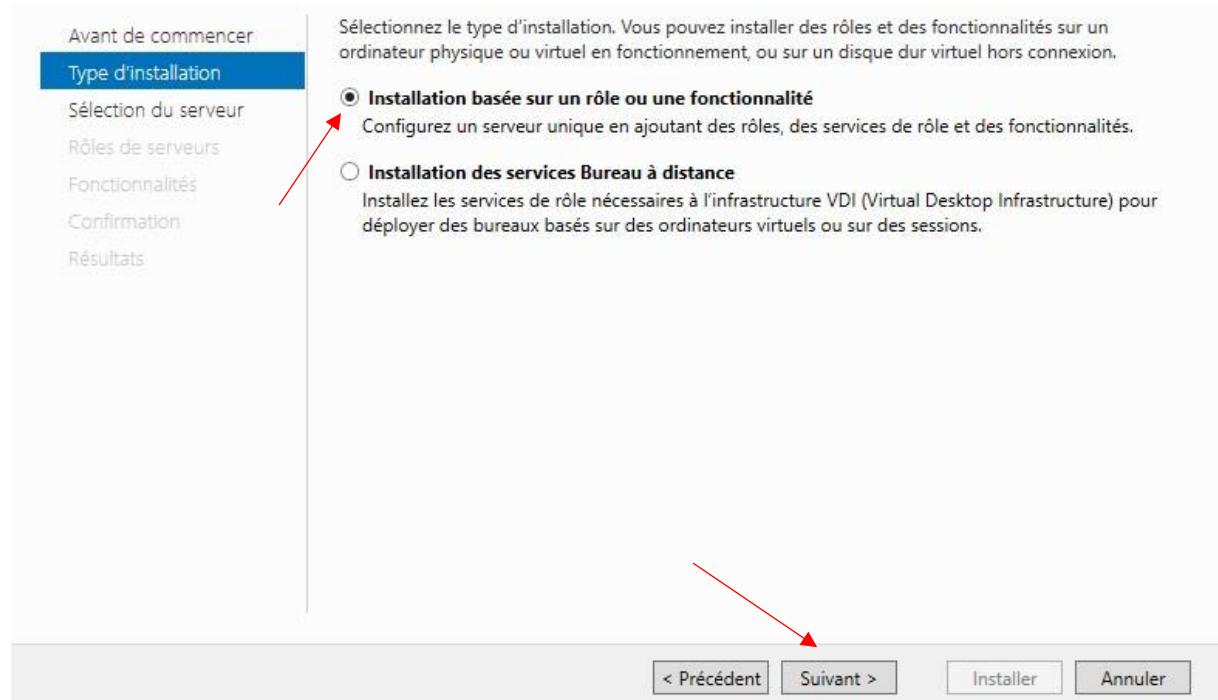


Figure 14 : Assistant / Type d'installation

Sélectionner un serveur du pool de serveurs :

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

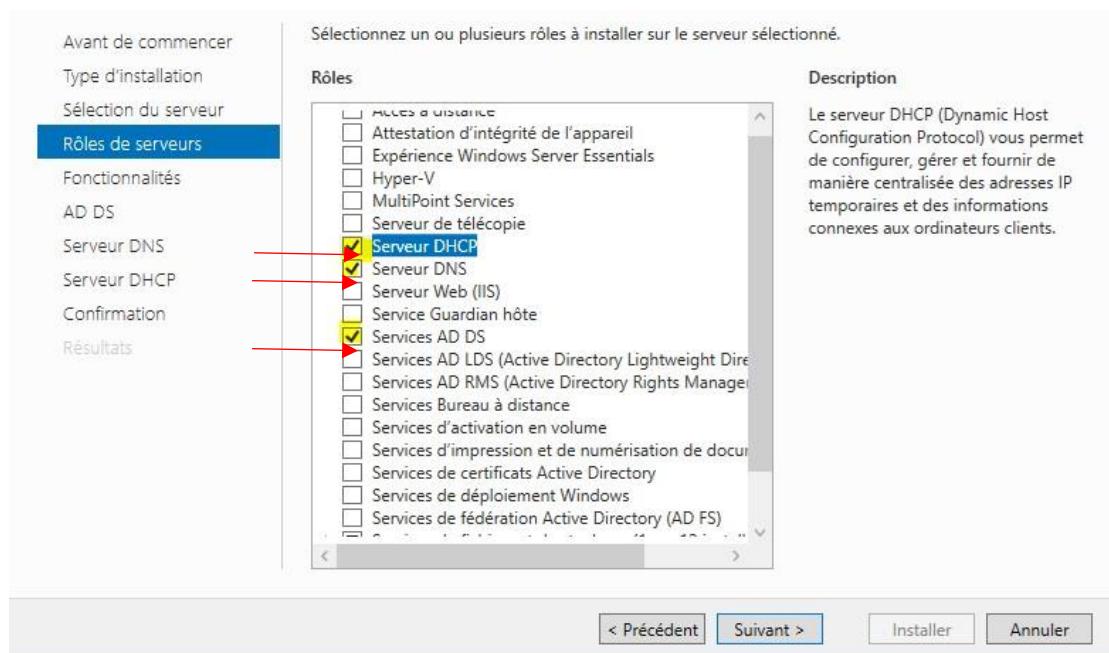


Figure 16 : Assistant / Rôles de serveurs

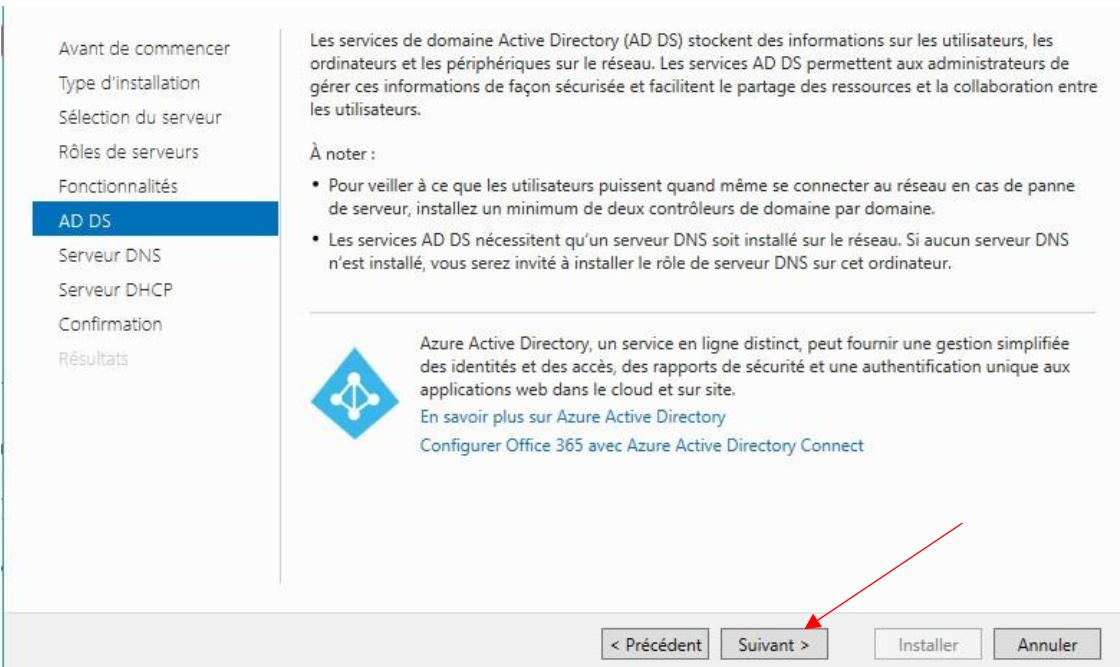


Figure 17 : Assistant / (AD DS) Services de domaine Active Directory

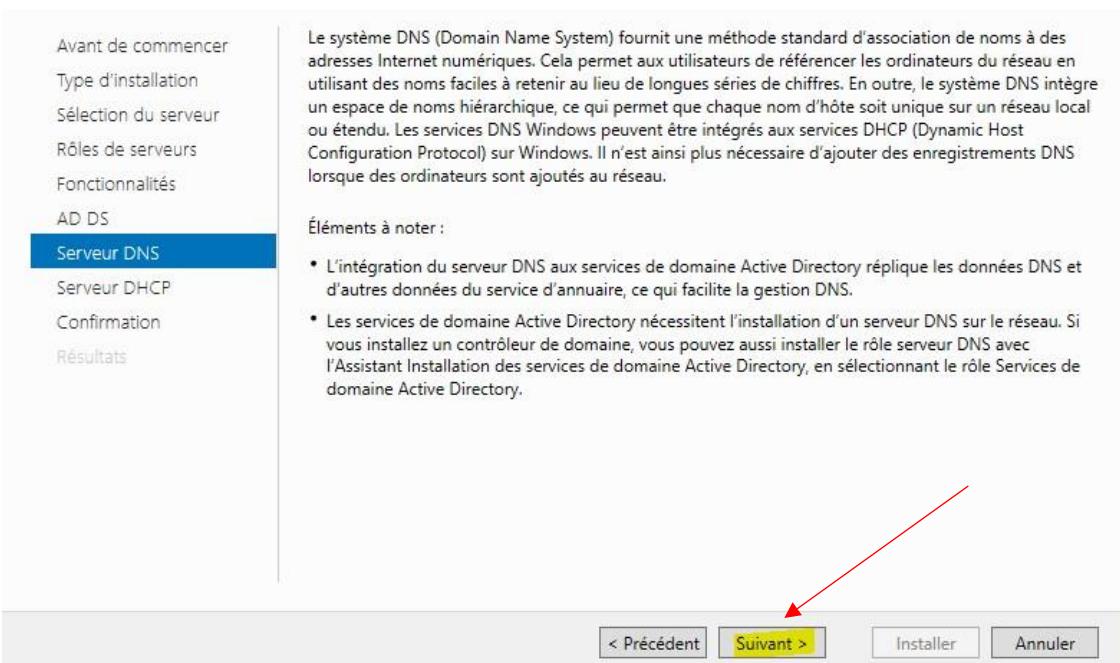


Figure 18 : Assistant / Serveur (DNS) Domain name system

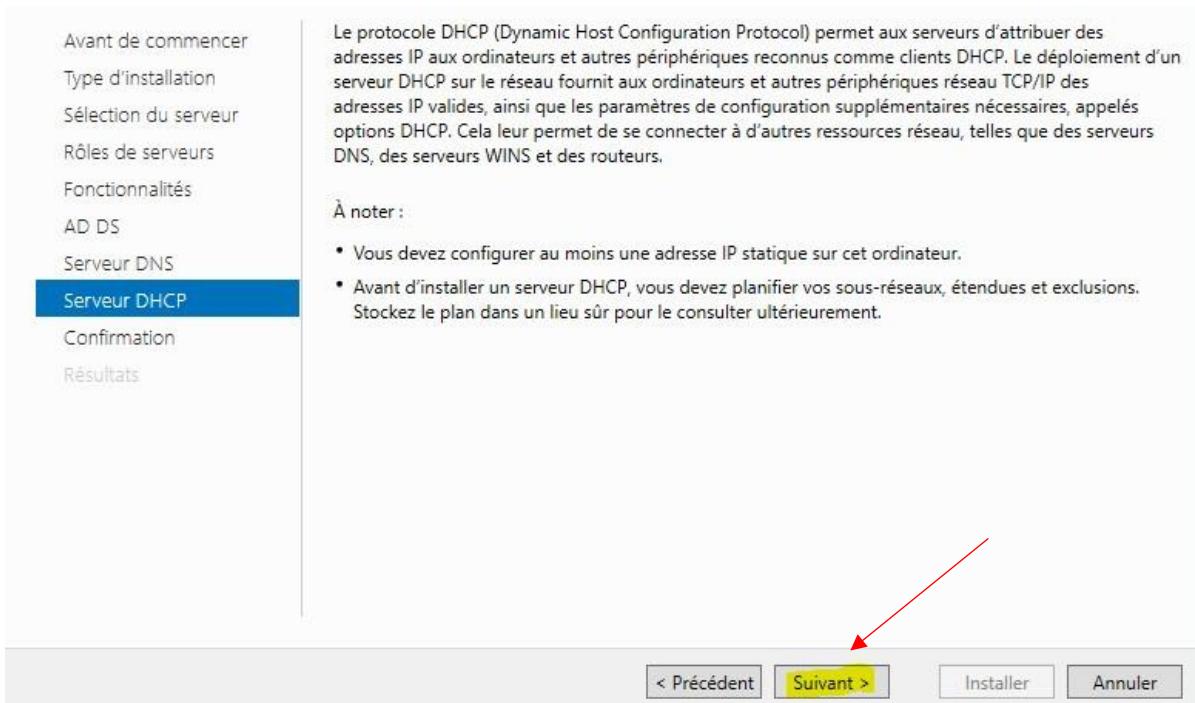


Figure 19 : Assistant / Serveur (DHCP) Dynamic host configuration protocol

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

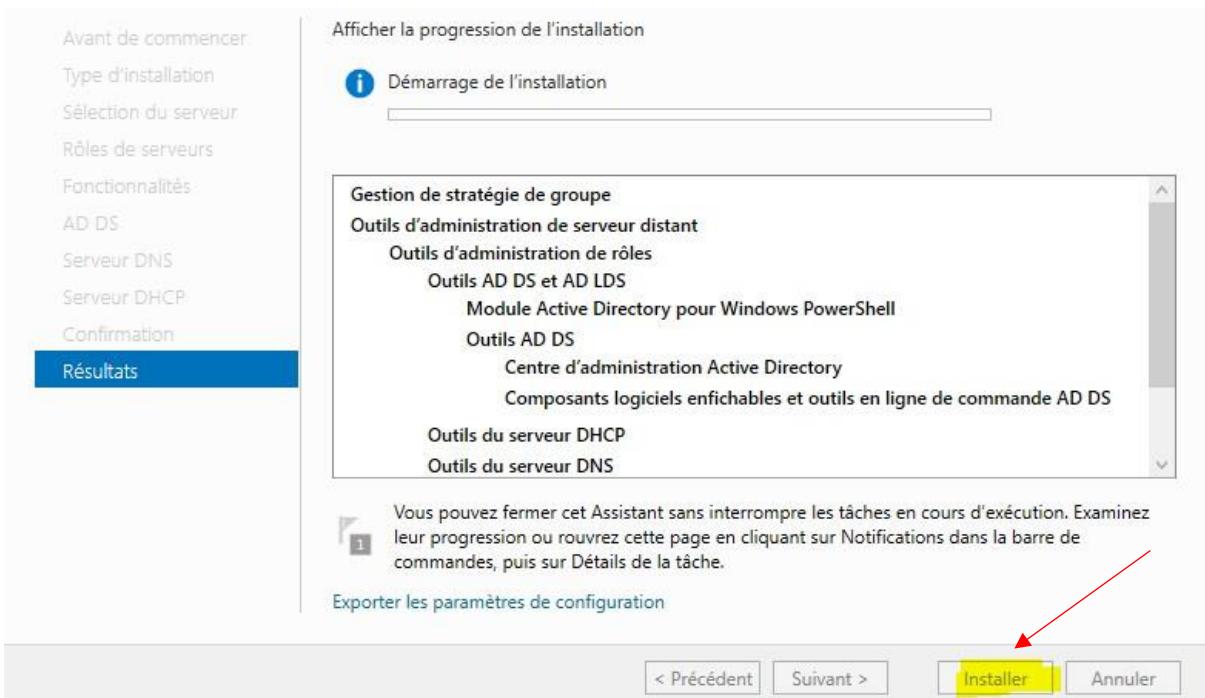


Figure 20 : Assistant / Démarrage de l'installation

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

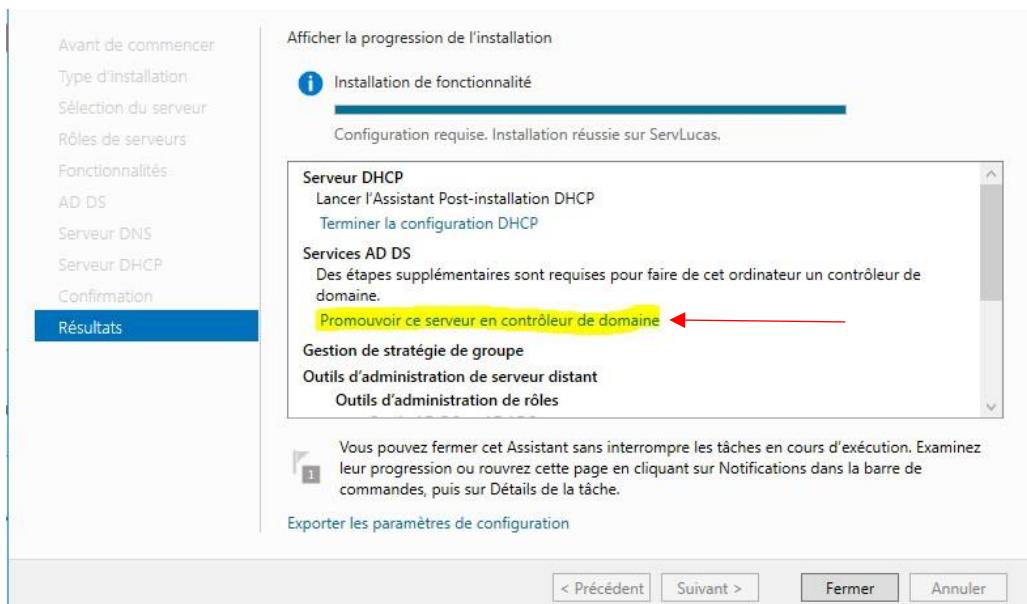


Figure 21 : Assistant / Installation terminée

5 Configuration Active Directory :

Dans **configuration de déploiement**, Prenez l'option **ajouter une nouvelle forêt**. Avec le contexte MLJ3M sous la forme de : MLJ3M.com

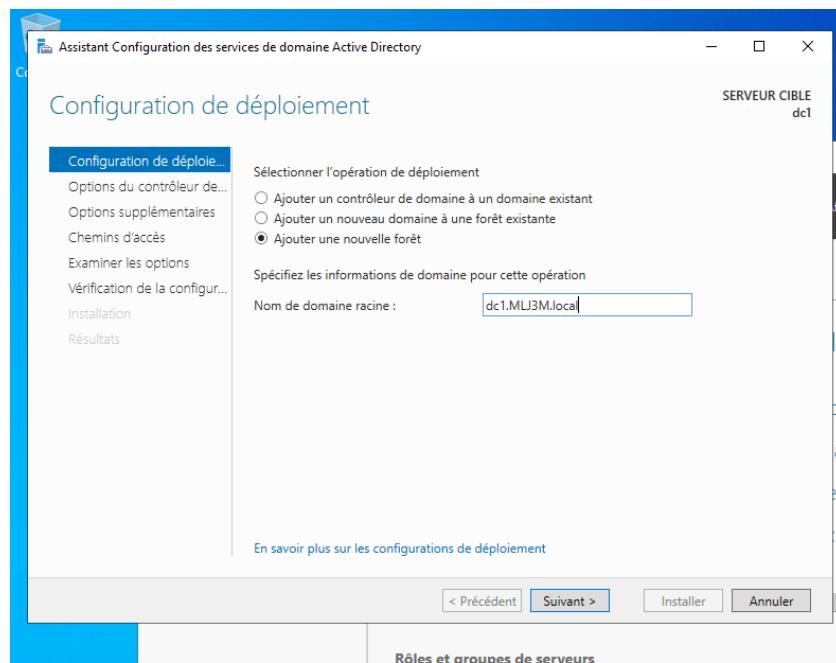


Figure 22 : Active Directory / Configuration de déploiement

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

Spécifier les capacités du contrôleur de domaine et les informations sur le site

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

Nom du site : Default-First-Site-Name

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

Mot de passe :

Confirmer le mot de passe :

Figure 23 : Active Directory / Option du contrôleur de domaine

Pas de création de délégation DNS.

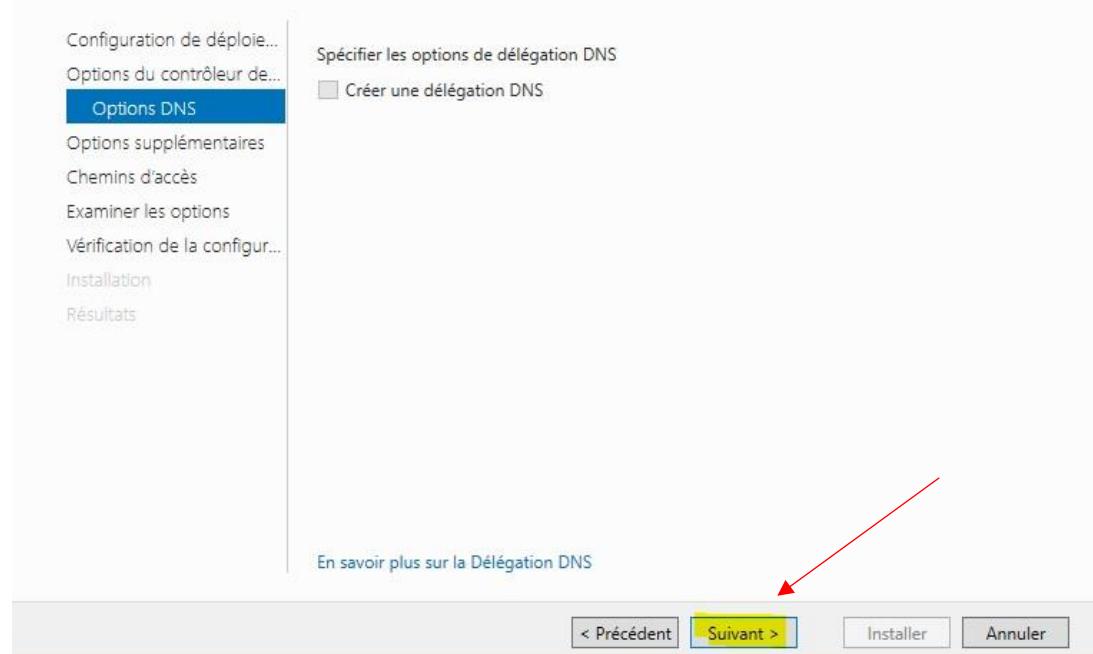


Figure 24 : Active Directory / Option DNS

Aucune modification pour les chemins d'accès :

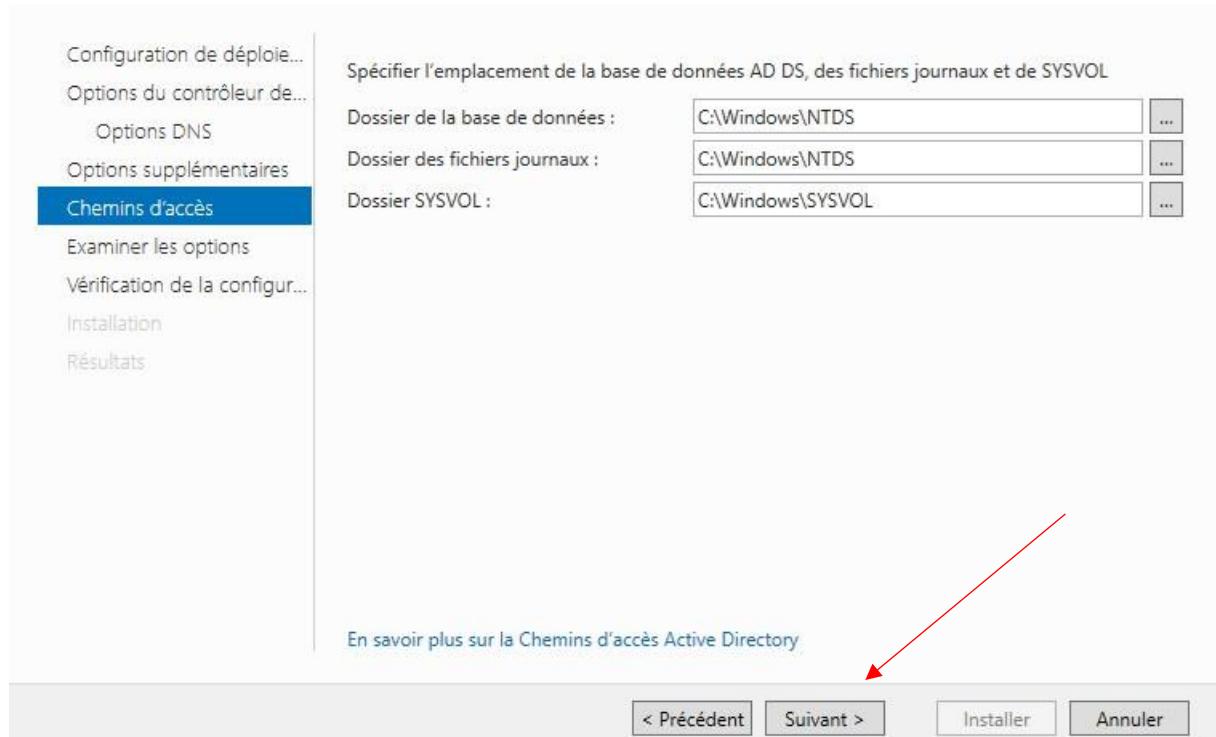


Figure 26 : Active Directory / Chemin d'accès

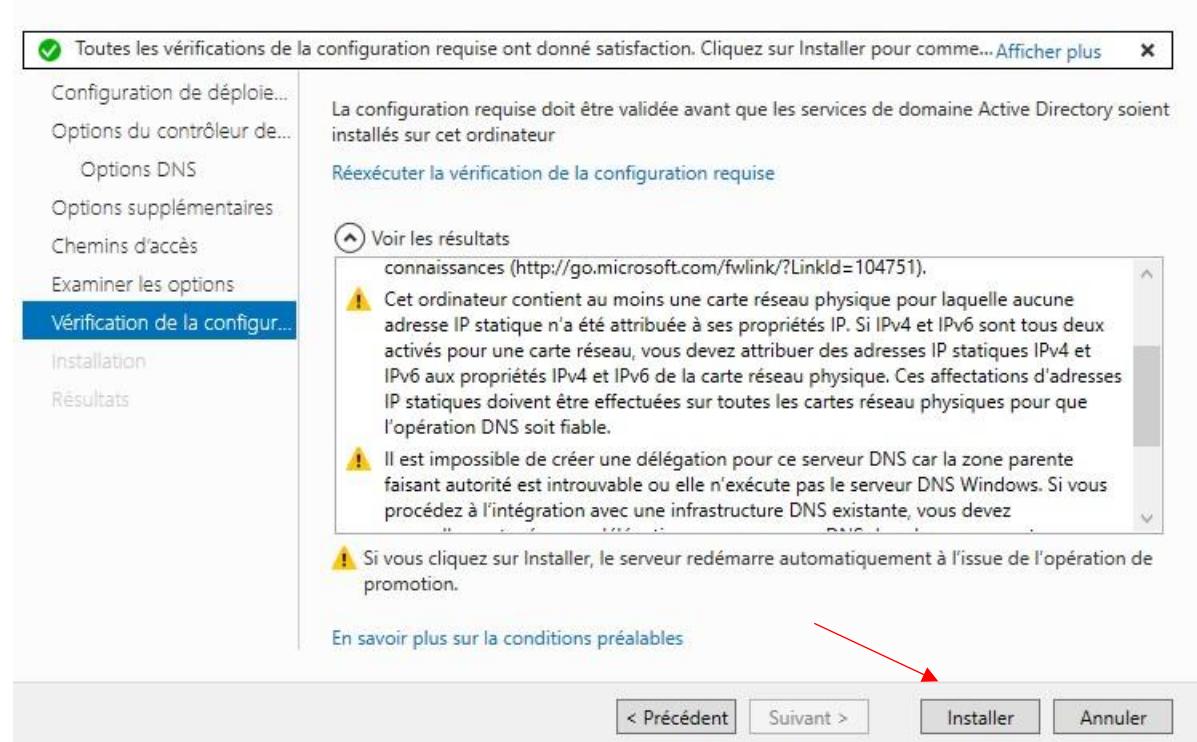


Figure 28 : Active Directory / Vérification de la configuration requise

Après l'installation, le redémarrage se fera automatiquement.

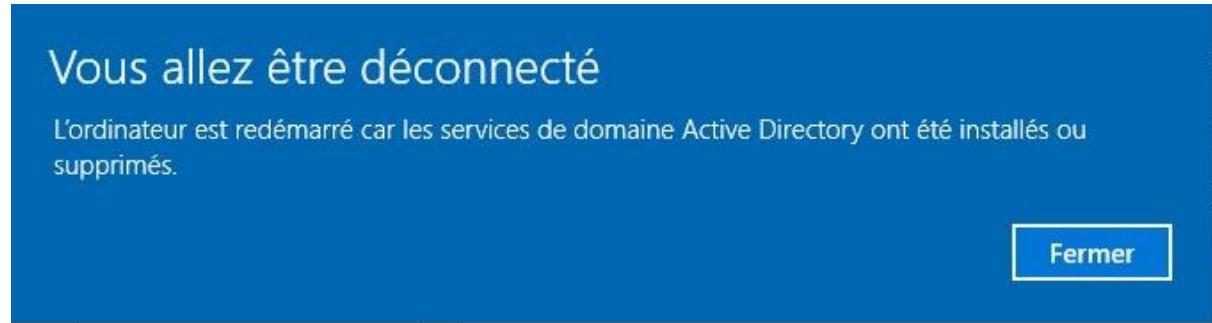


Figure 29 : Installer puis redémarrer

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 :

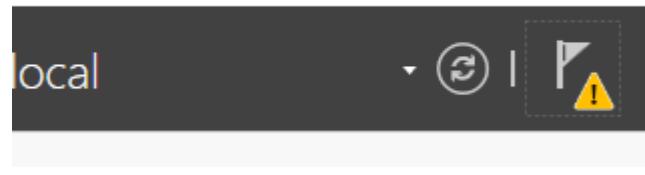


Figure 30 : Notification / Avancement de la configuration

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 »

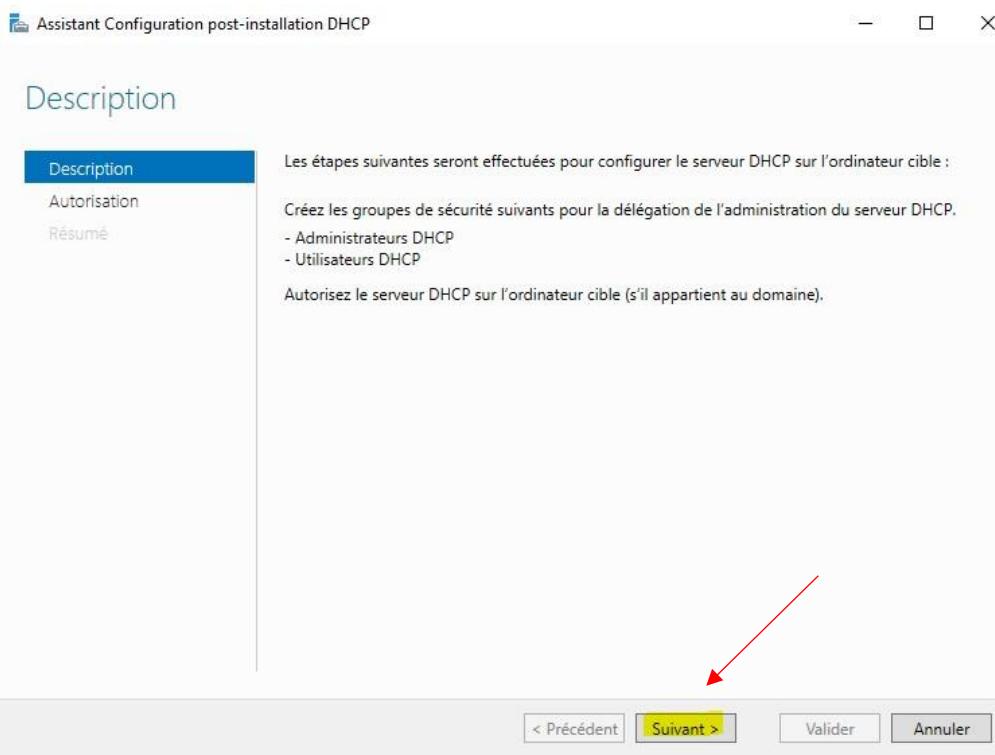


Figure 32 : DHCP / Description

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

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

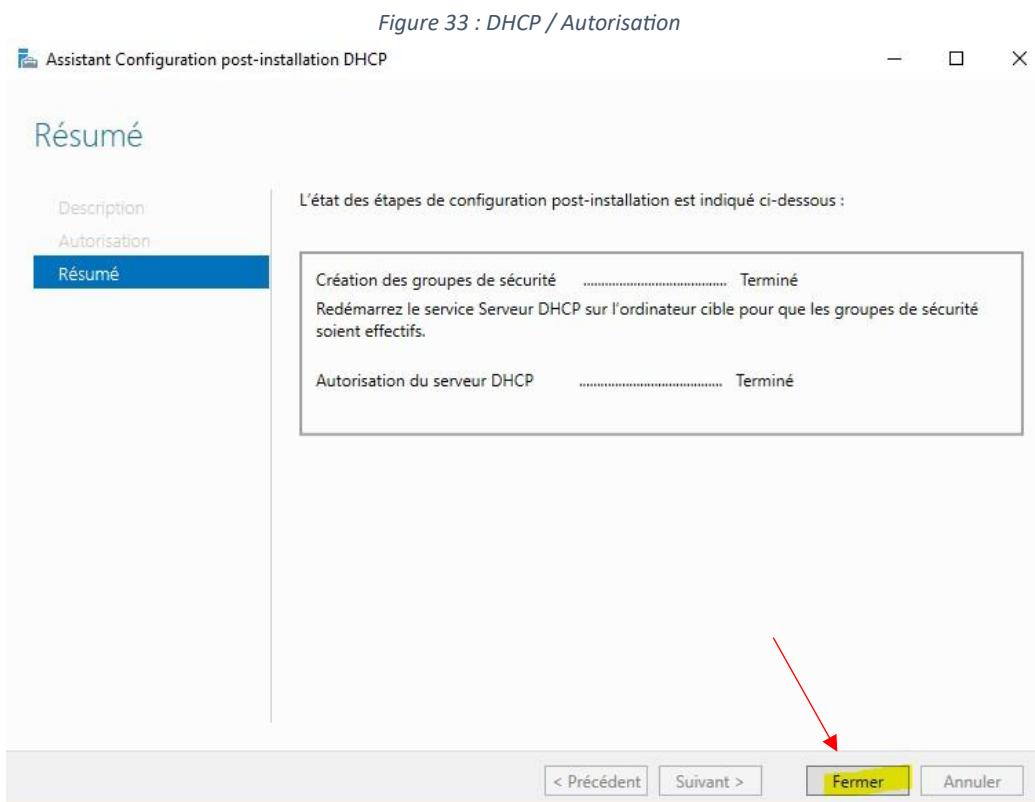


Figure 34 : DHCP / Résumé

Maintenant, redémarrez l'ordinateur.

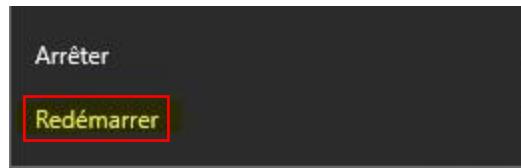


Figure 35 : Fermer puis redémarrer

Nous allons Configurer le rôle DHCP.

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

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

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

Voici un exemple de configuration pour ma première étendue.

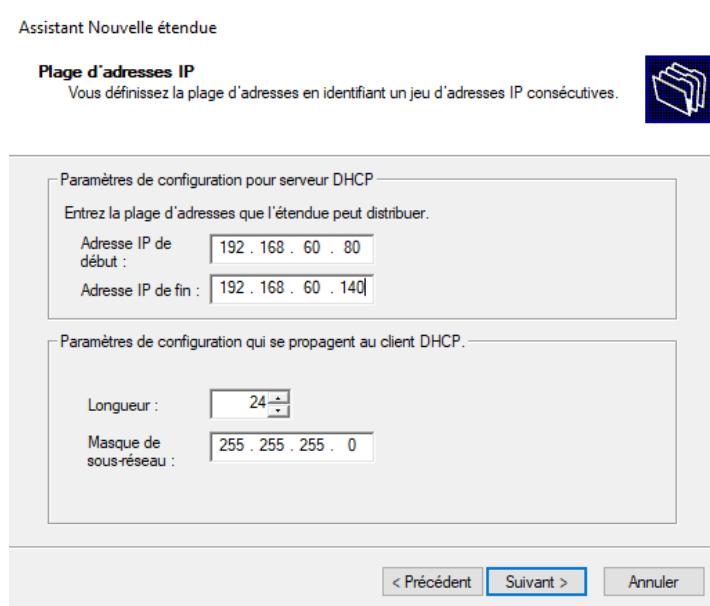


Figure 36 : DHCP / Paramétrage adresse IP

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

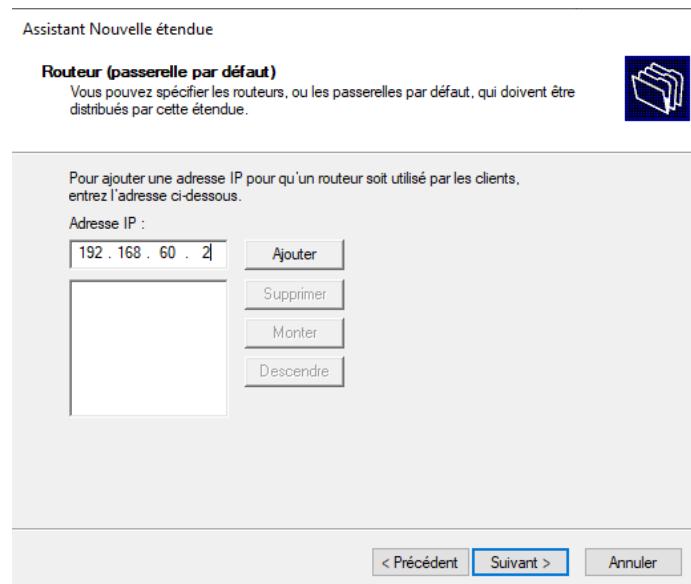


Figure 37 : Routeur / Passerelle par défaut

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

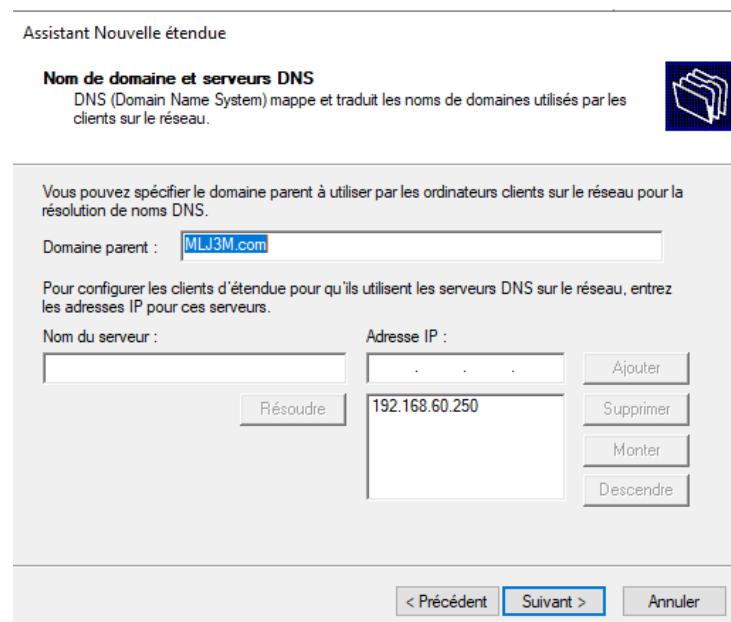
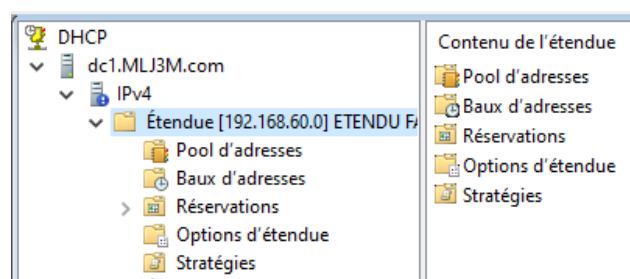


Figure 39 : Paramétrage adresse IP /

Une fois terminé, vous devriez avoir ce résultat :



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**.

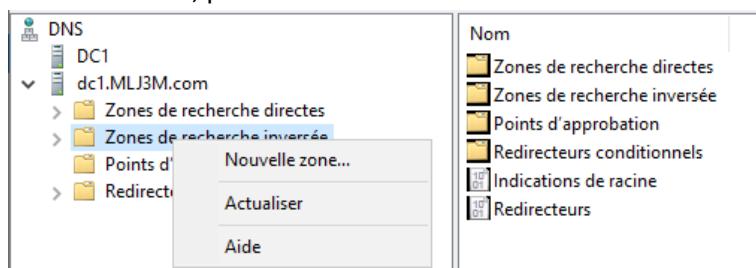
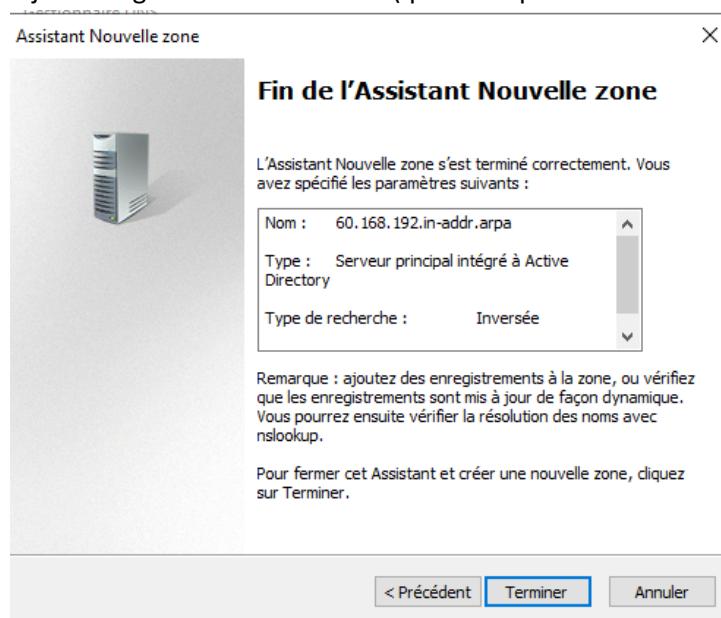


Figure 41 : DNS / Nouvelle zone de recherche inversée

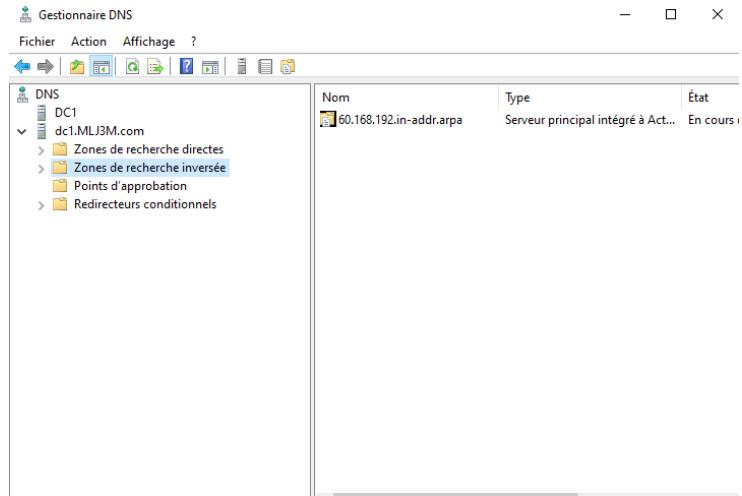
Ensuite, je laisse la configuration par défaut que l'assistant me donne.

Puis comme ID réseau je renseigne : **192.168.60.250** (qui correspond à mon serveur).



Le DNS est maintenant configuré.

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



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

Les utilisateurs seront les suivants, j'ai créé les mots de passe aléatoirement grâce à Keepass 2.0.

<u>Prénom</u>	<u>Nom</u>	<u>Groupe</u>	<u>Mot de passe</u>
Florent	Berneron	Conseiller	Yh! D0kNYsxHkO"mEaq.W
Jean	maltra	Conseiller	%'f1@Nqr1lf+PgMj!DSw
Magali	Lafros	Conseiller	Keh=e'lxl":~J60nR&#I
Marie	Dupont	Conseiller	W+A3hCKe@mGvce9S!p\$d
Nicolas	Benothmane	Conseiller	77pk#57u:rJk4gdj~jpx
Claire	Malfra	Administratif	%'f1@N7eydHisjk
Marilou	Autain	Administratif	Gvce9SeW+A3hCKe
Marion	Marti	Comptabilité	W+A3hCfyey4zTudh
Patrick	Lavier	Responsable	D0kNYsxHkO"mEaqedd78K

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

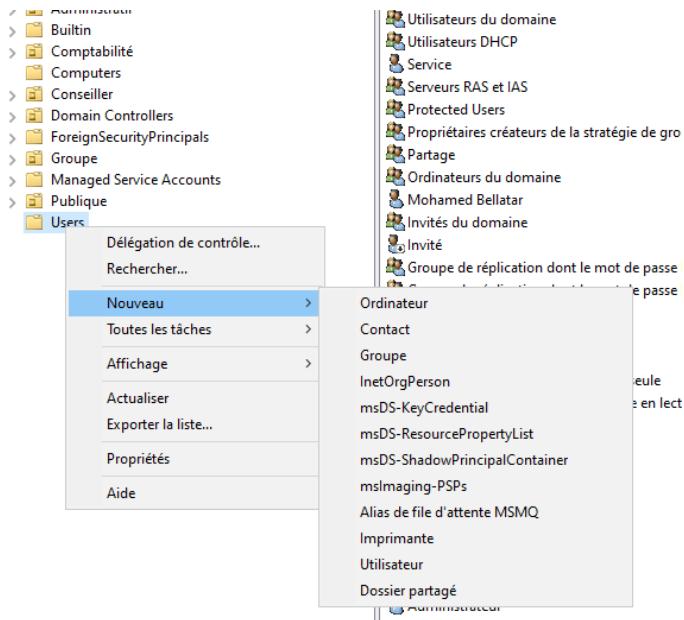


Figure 45 : Active Directory / création des utilisateurs

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

Nouvel objet - Utilisateur

Créer dans : MLJ3M.com/Users

Prénom :	Marion	Initials :	<input type="text"/>
Nom :	Moreno		
Nom complet : Marion Moreno			
Nom d'ouverture de session de l'utilisateur :			
mmoreno		@MLJ3M.com	
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :			
MLJ3M\		mmoreno	

< Précédent Suivant > Annuler

Figure 46 : Active Directory / création utilisateur Marion

Nouvel objet - Utilisateur

Créer dans : MLJ3M.com/Users

Mot de passe :	<input type="password"/> *****
Confirmer le mot de passe :	<input type="password"/> *****
<input type="checkbox"/> L'utilisateur doit changer le mot de passe à la prochaine ouverture de session <input checked="" type="checkbox"/> L'utilisateur ne peut pas changer de mot de passe <input checked="" type="checkbox"/> Le mot de passe n'expire jamais <input type="checkbox"/> Le compte est désactivé	

< Précédent Suivant > Annuler

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**.

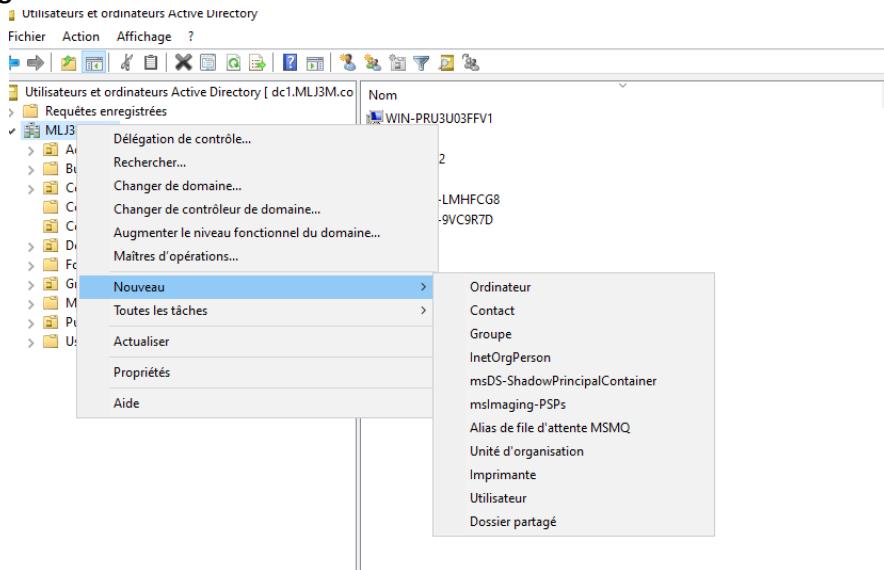


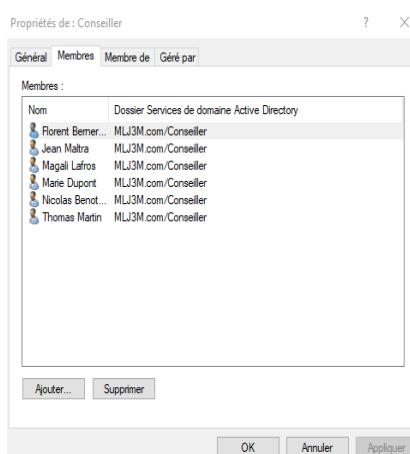
Figure 48 : Active Directory / création unité d'organisation

On lui donnera le nom : Publique

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

Groupe 1 : Administration / **Groupe 2 :** Conseillers / **Groupe 3 :** Comptabilité

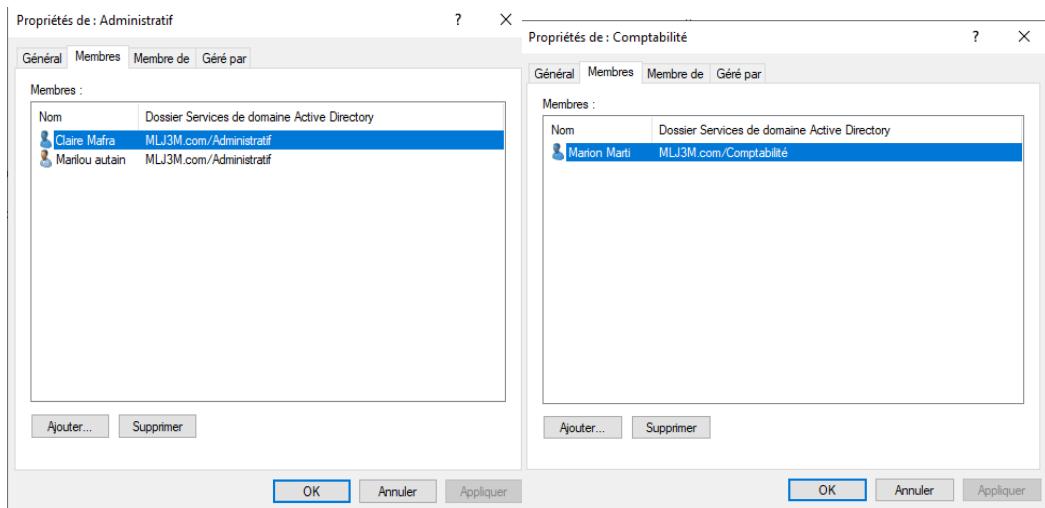
Puis enfin déplacer les utilisateurs dans les groupes que vous souhaitez :



26

Figure 49 : Active Directory / Groupe Conseiller avec utilisateurs

Figure 50 : Active Directory / Groupe Administration avec utilisateurs Figure 51 : Active Directory / Groupe comptabilité avec utilisateurs

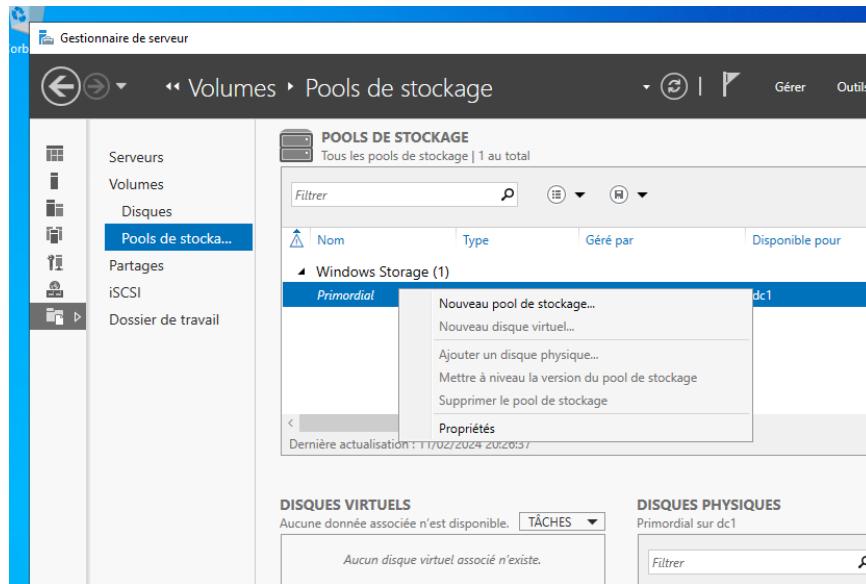


7 Serveur de fichiers :

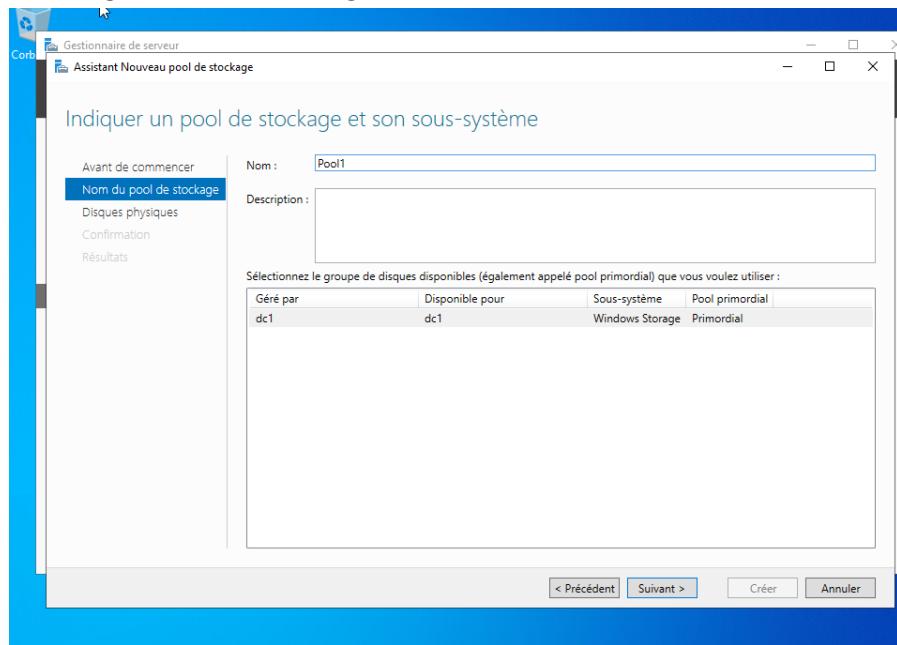
À la suite d'une installation d'un Windows Serveur 2022 sur un serveur,
 Avec dessus un disque monter de 400Go.
 Nous allons maintenant configurer notre serveur de fichier.

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

Création d'un nouveau pool de stockage :



Nommage du Pool de stockage :



Confirmation des différentes configurations :

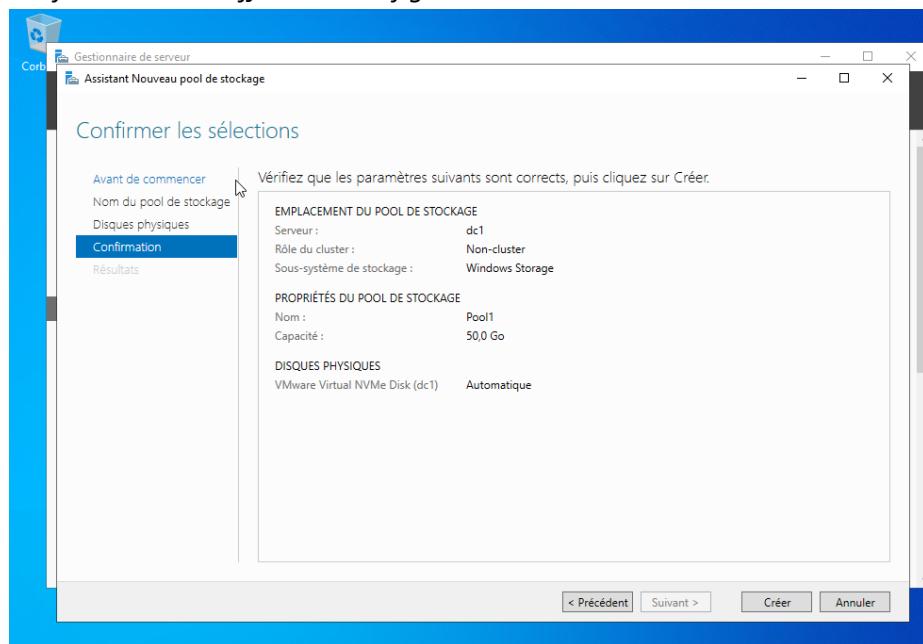
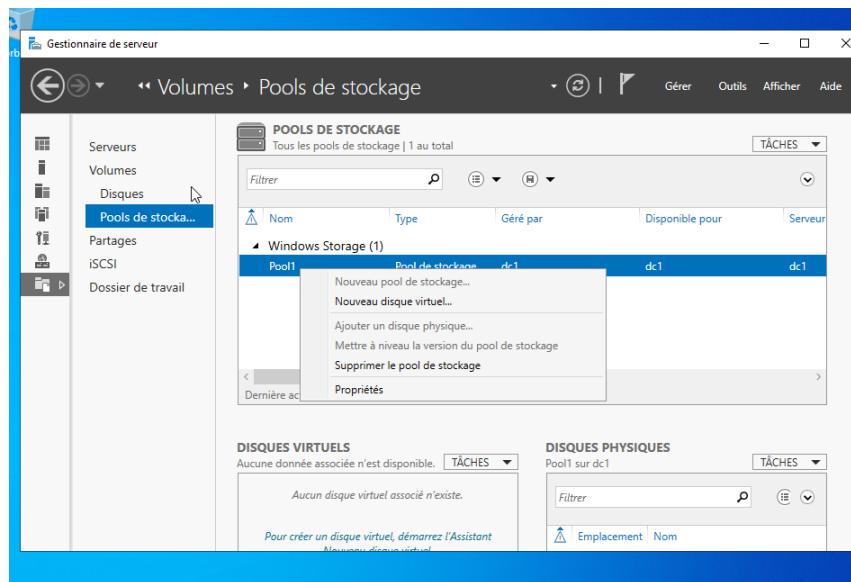
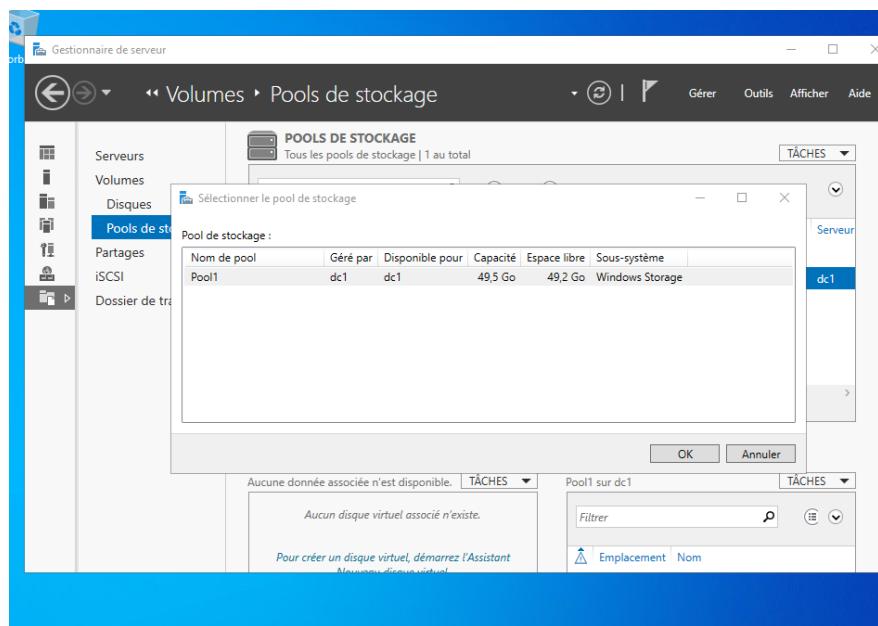


Figure 52 Serveur de fichier /Configuration du Pool de stockage

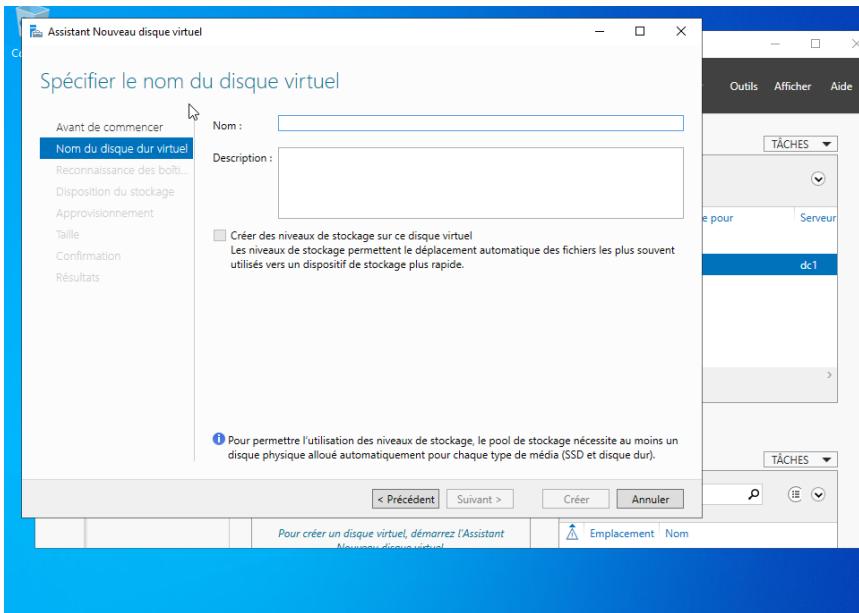
Création d'un nouveau disque virtuel :



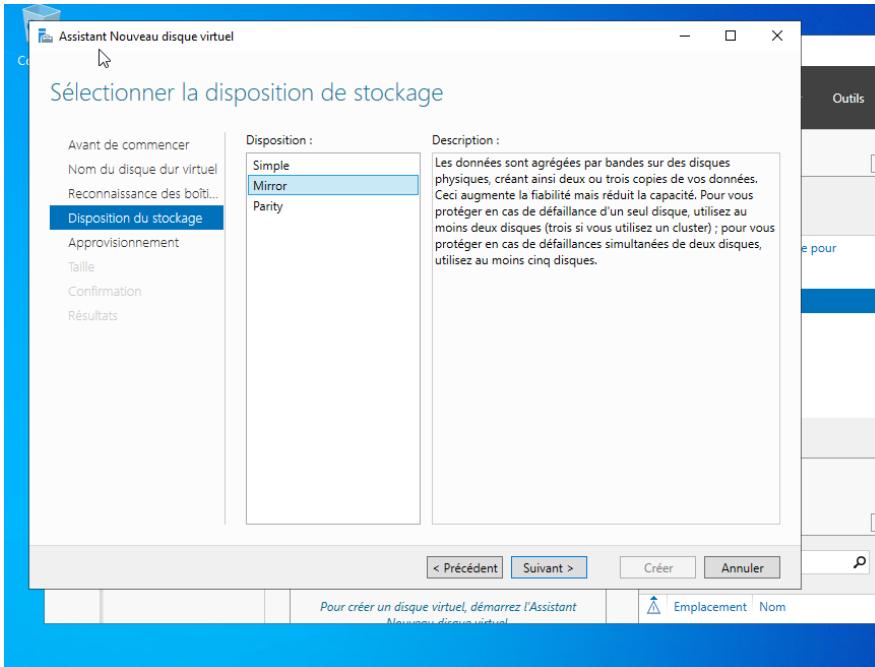
Sélection du Pool de stockage :



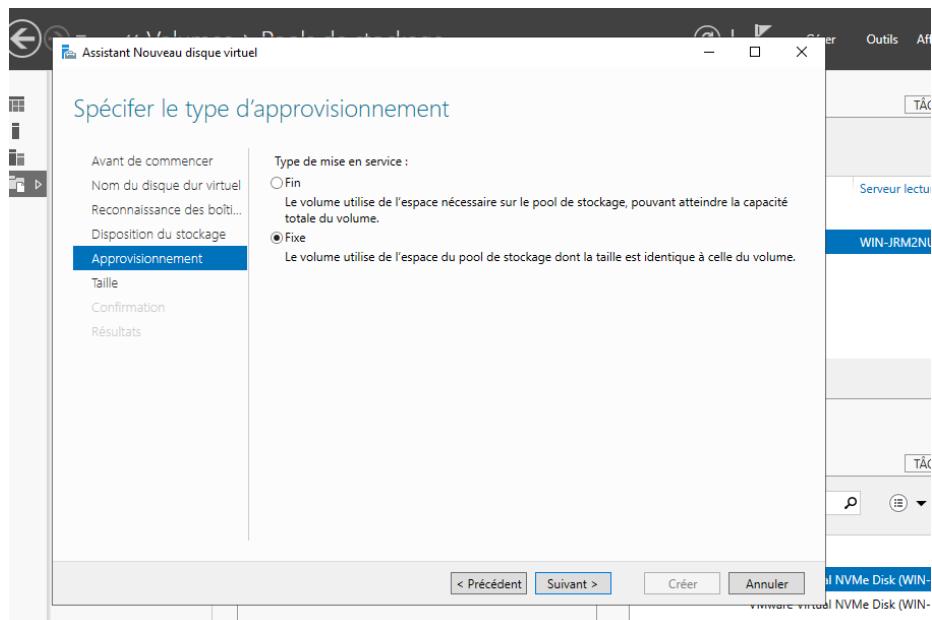
Nommage du disque virtuel :



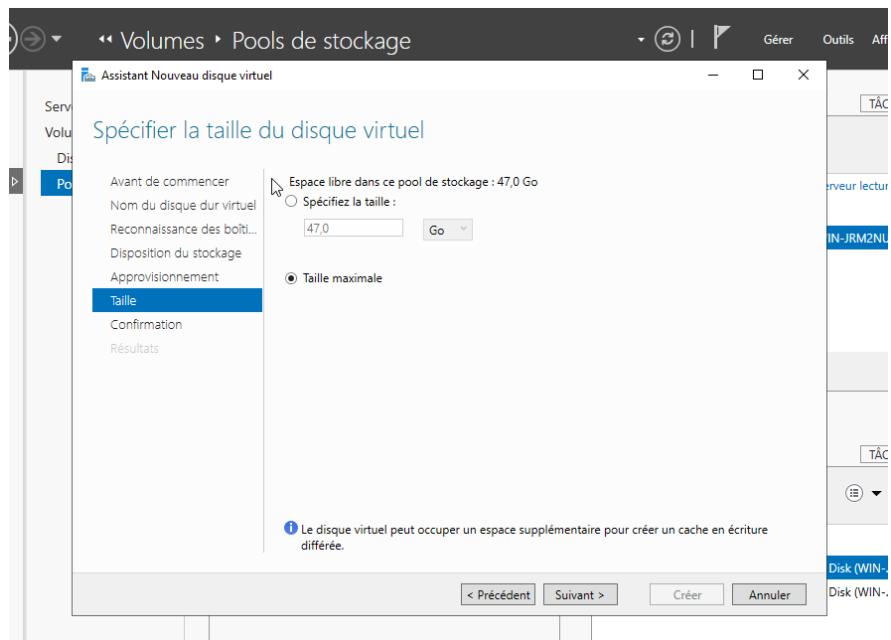
Sélection de la disposition de stockage :



Sélection du type d'approvisionnement :



Sélection de la taille du disque virtuel :



Confirmations des différentes configurations :

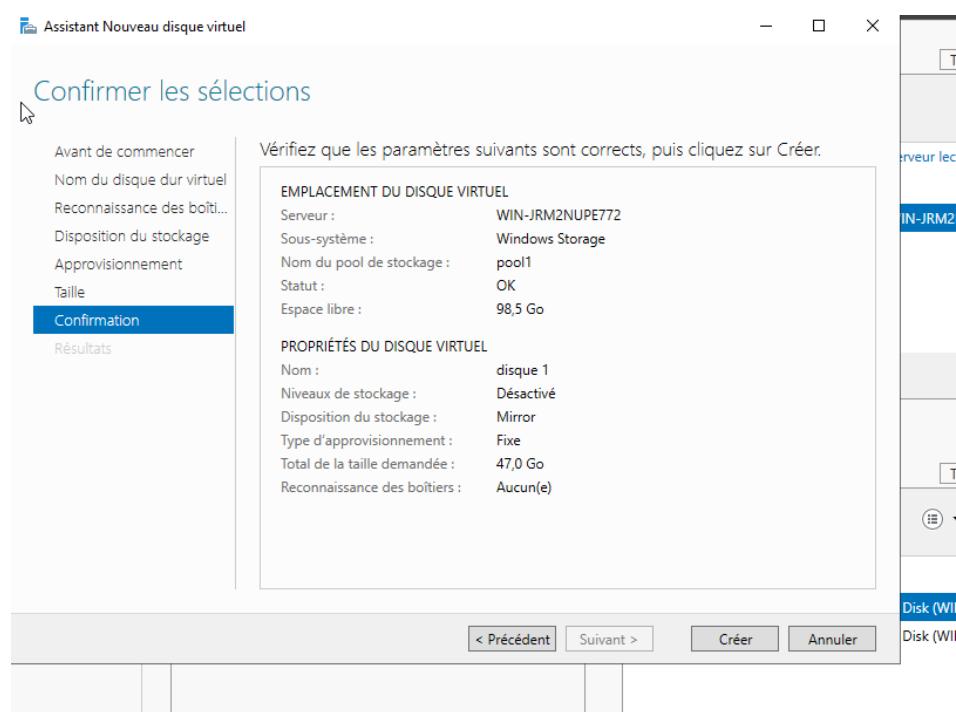
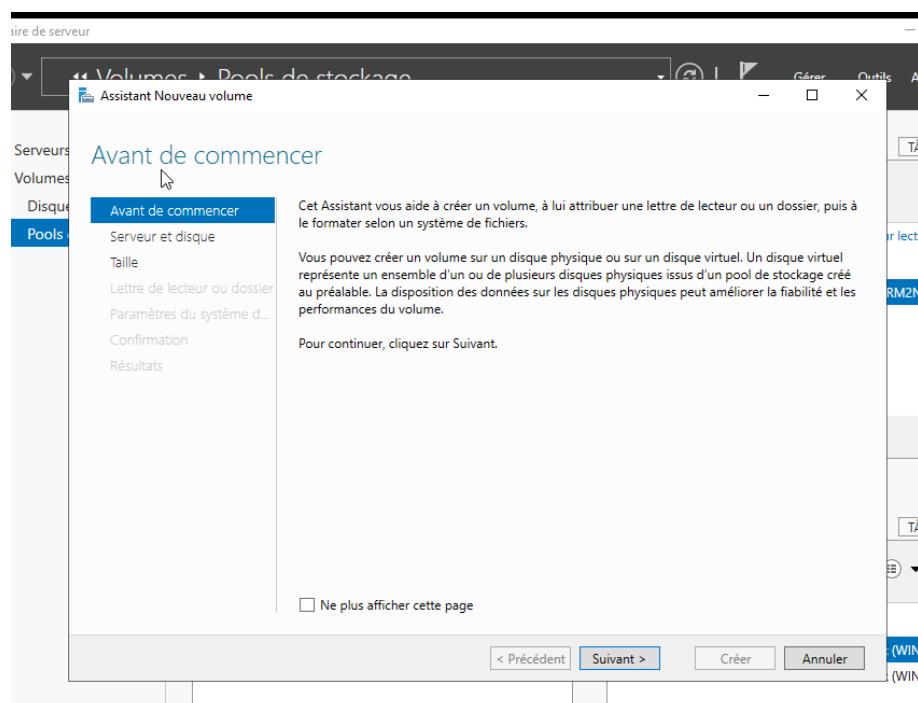
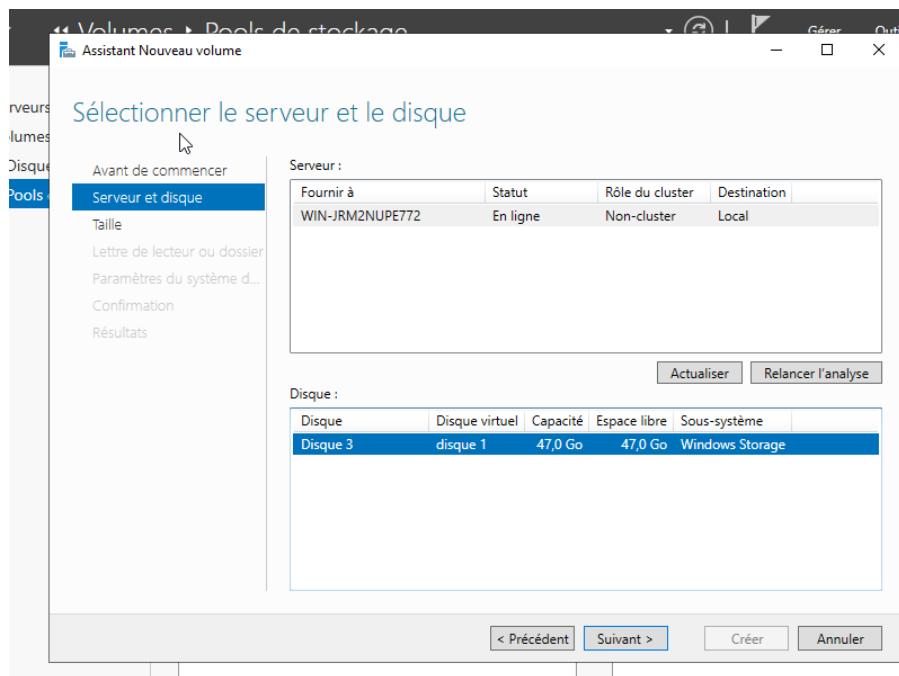


Figure 53 Serveur de fichier /Configuration du Disque virtuel

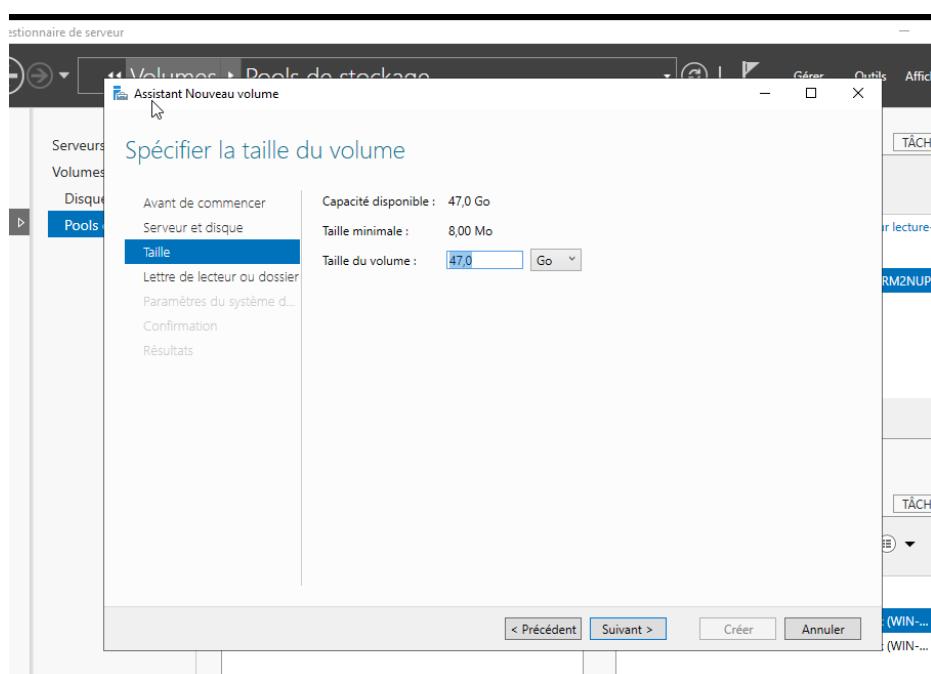
Création d'un nouveau volume :



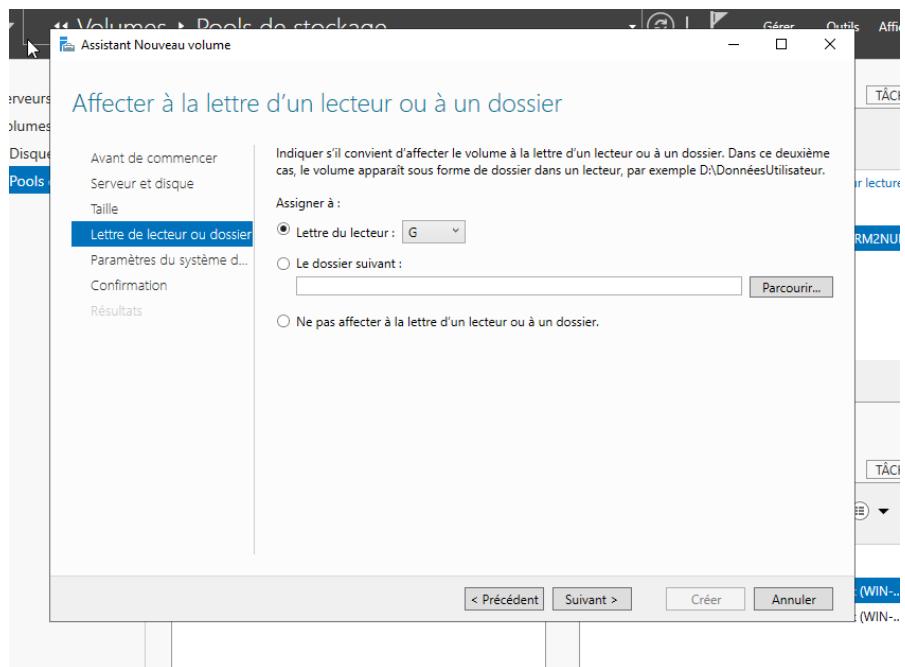
Sélection du serveur et du disque :



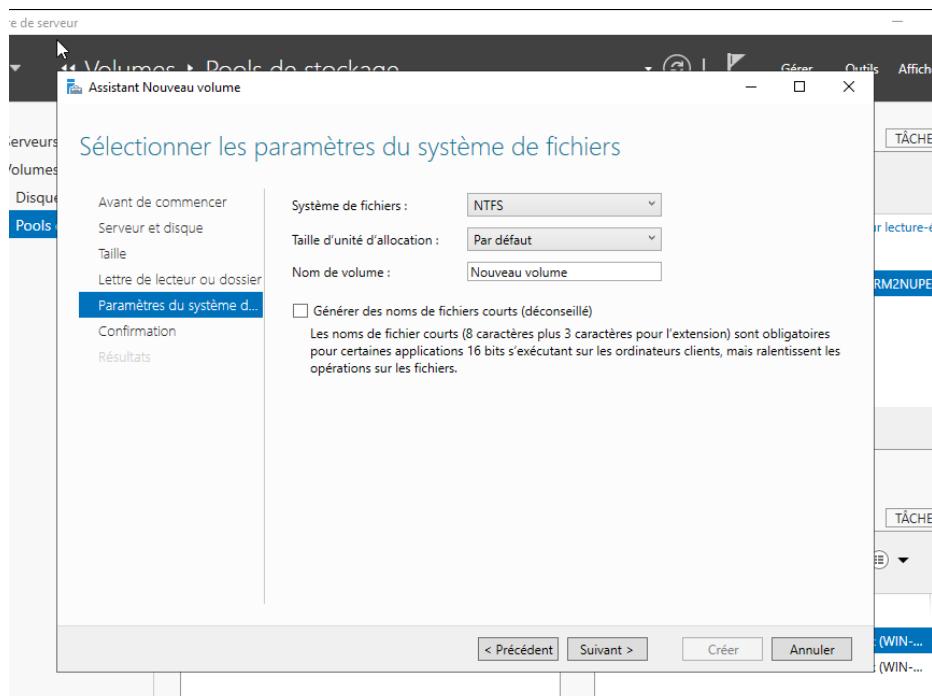
Sélection du la taille du volume :



Affectation de la lettre du lecteur :



Sélection des paramètres du système de fichier :



Confirmer différentes les configurations :

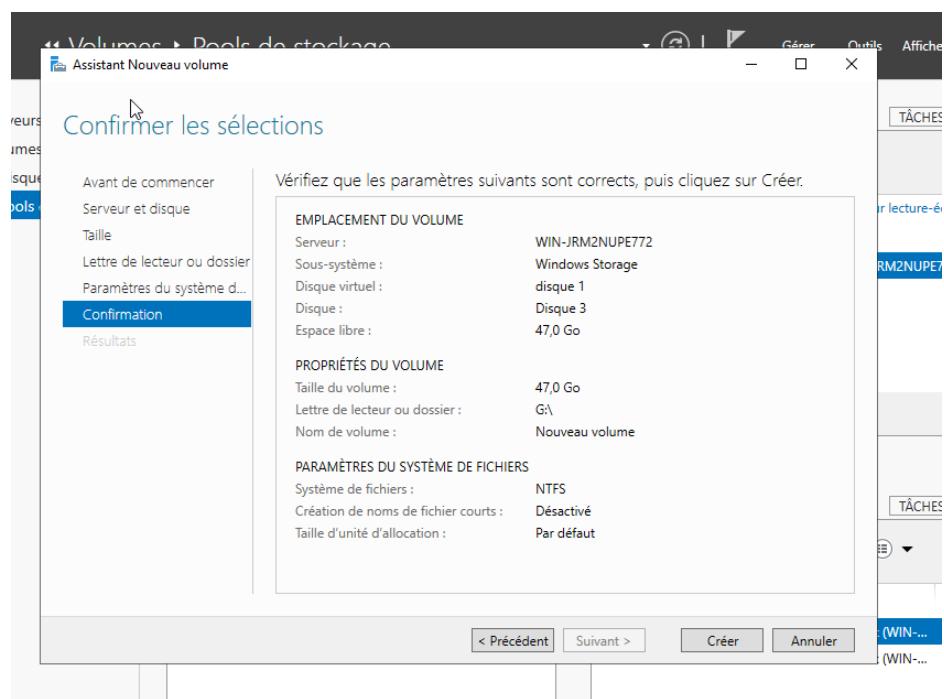
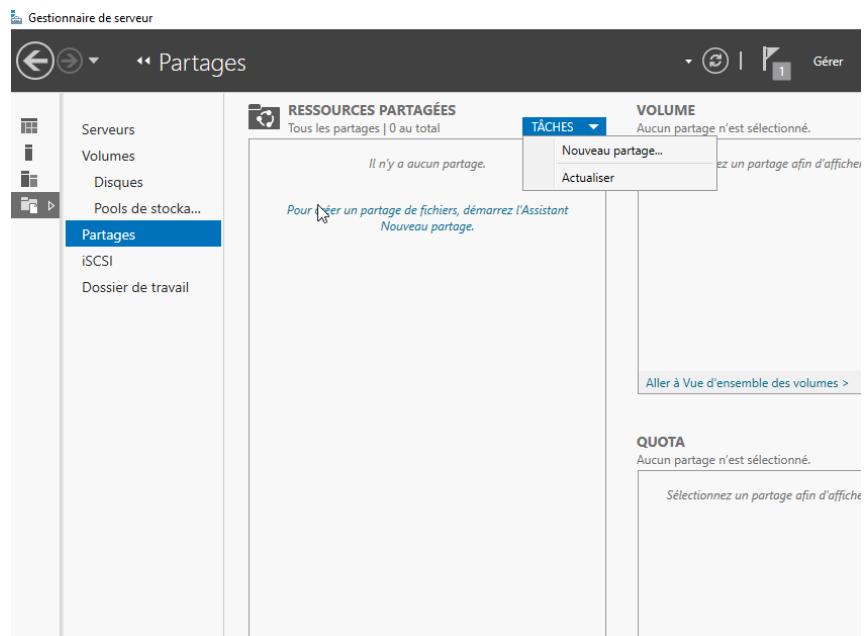
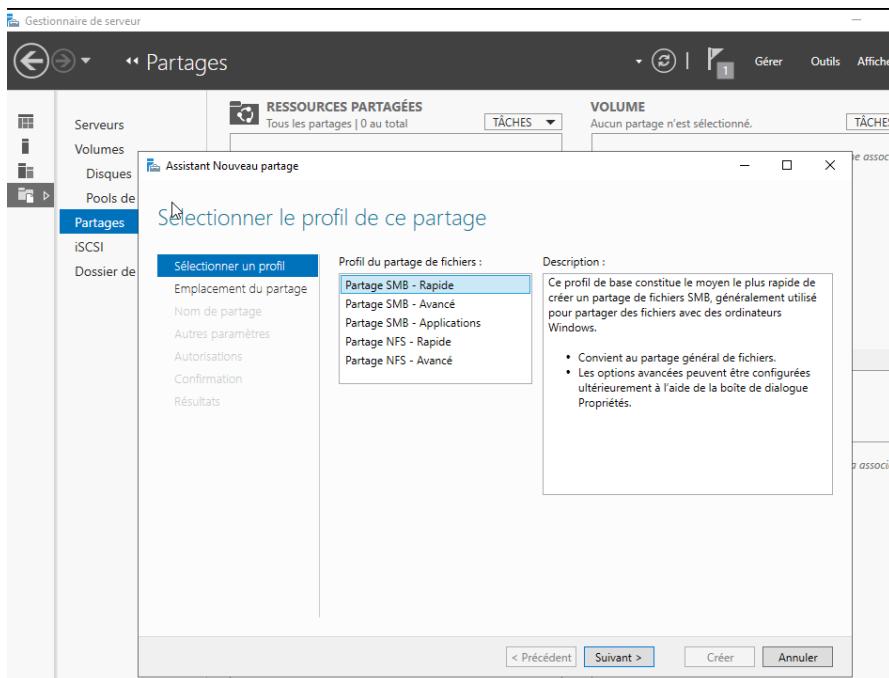


Figure 54 Serveur de fichier /Configuration du Volume

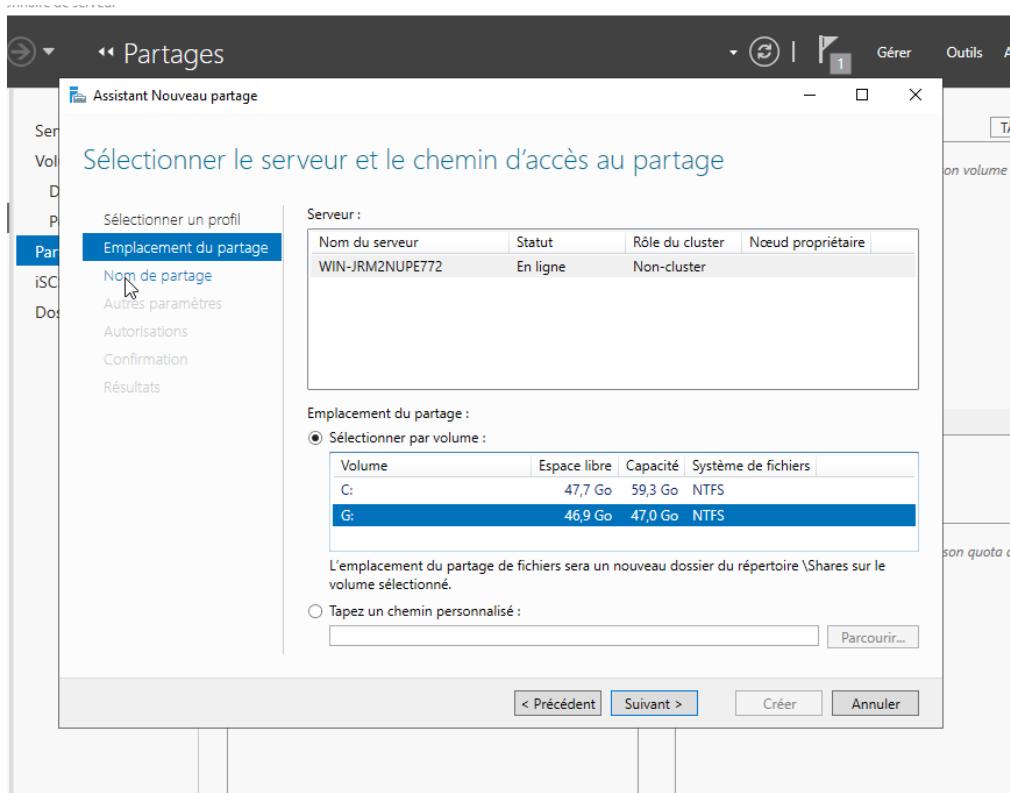
Création d'un nouveau partage :



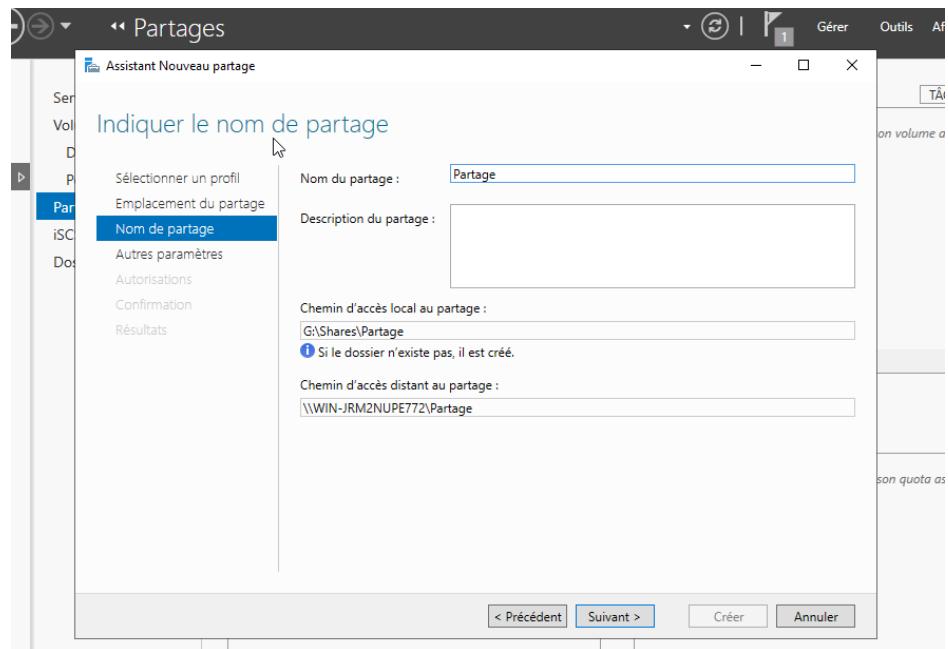
Sélection du profil de ce partage :



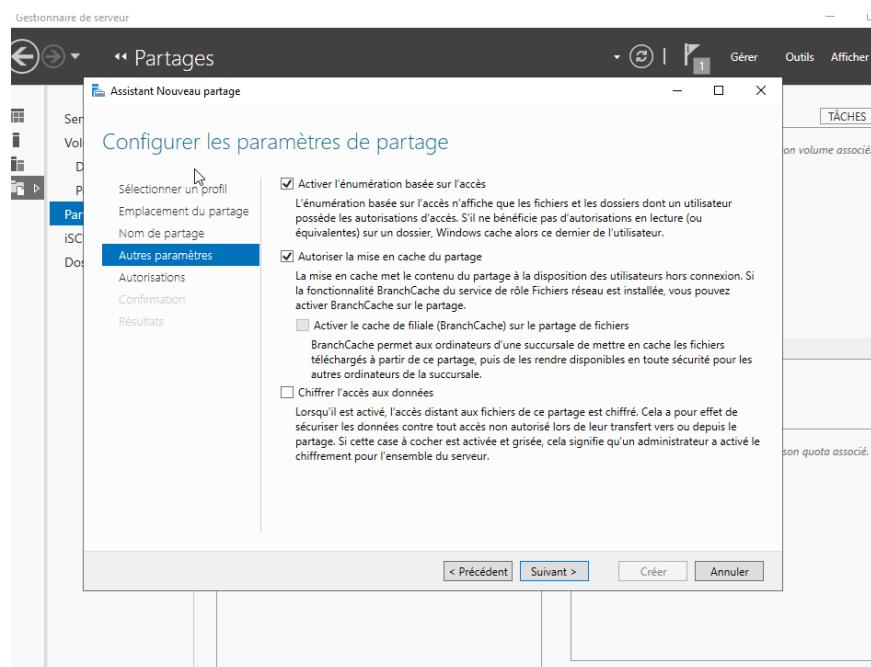
Sélectionner le serveur et le chemin d'accès au partage :



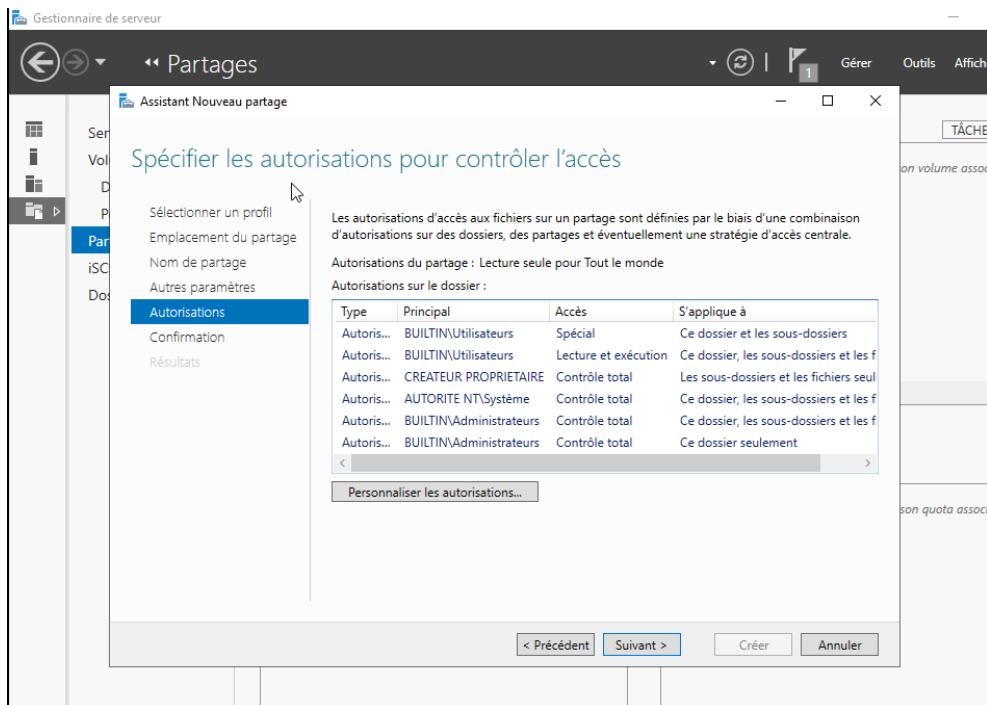
Indiquer le nom du partage :



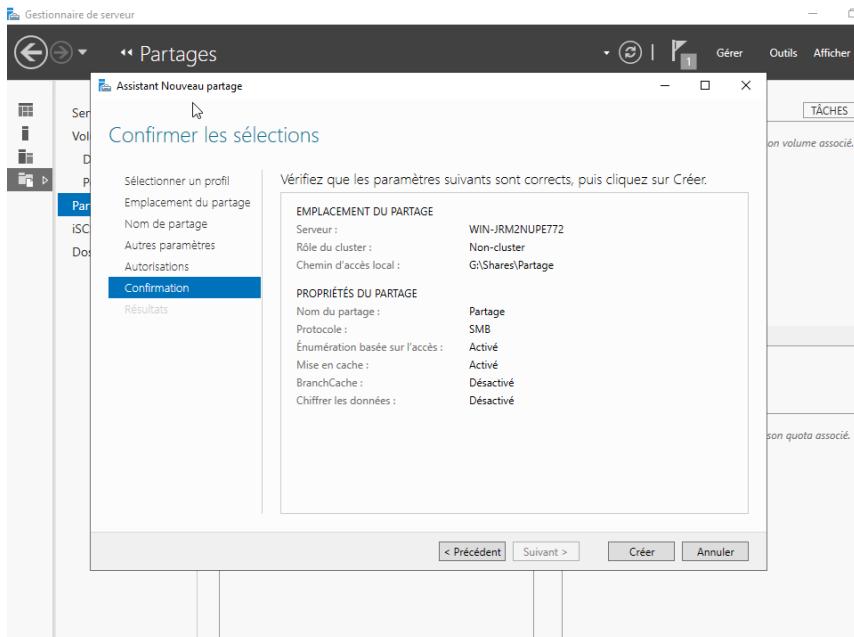
Configurer les paramètres de partage :



Spécification des autorisations pour contrôler l'accès :



Confirmer les différentes configurations :



Création d'un partage puis sélectionner le serveur et le chemin d'accès au partage et indication du nom du partage :

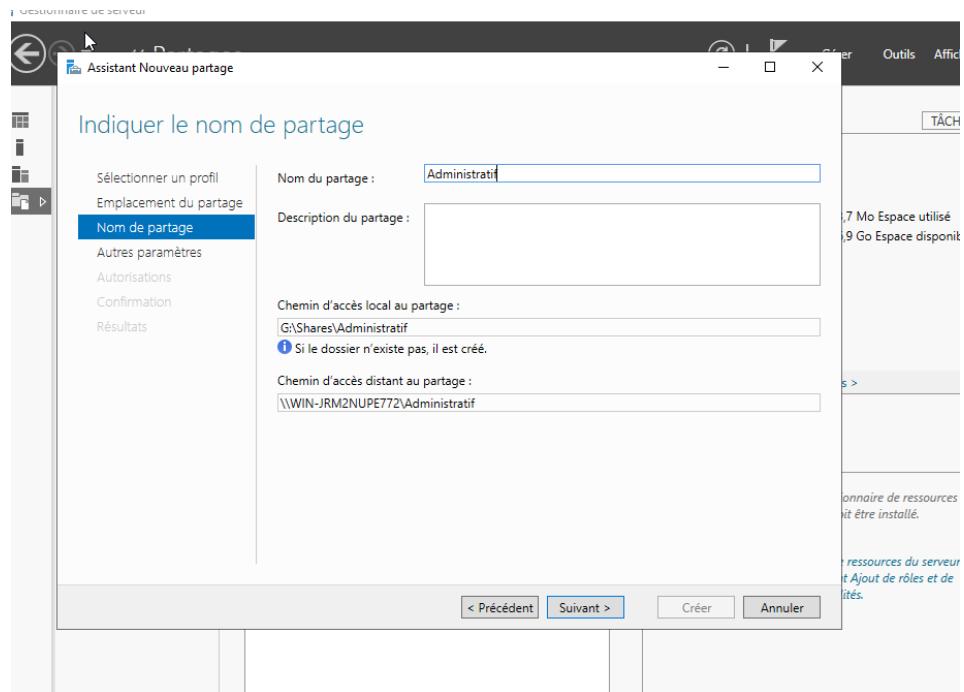
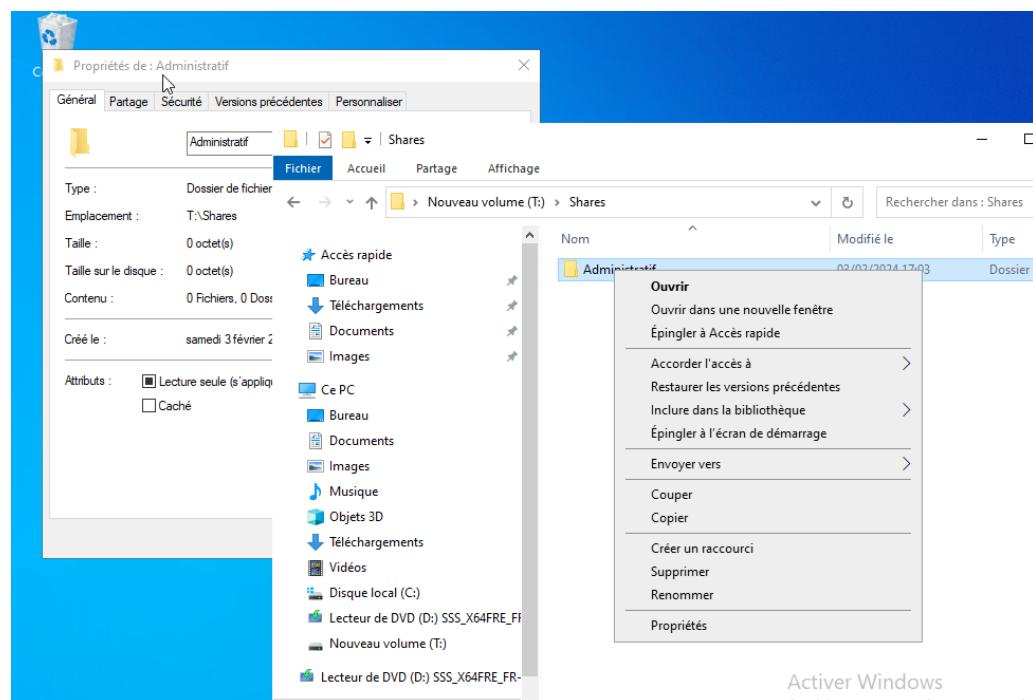
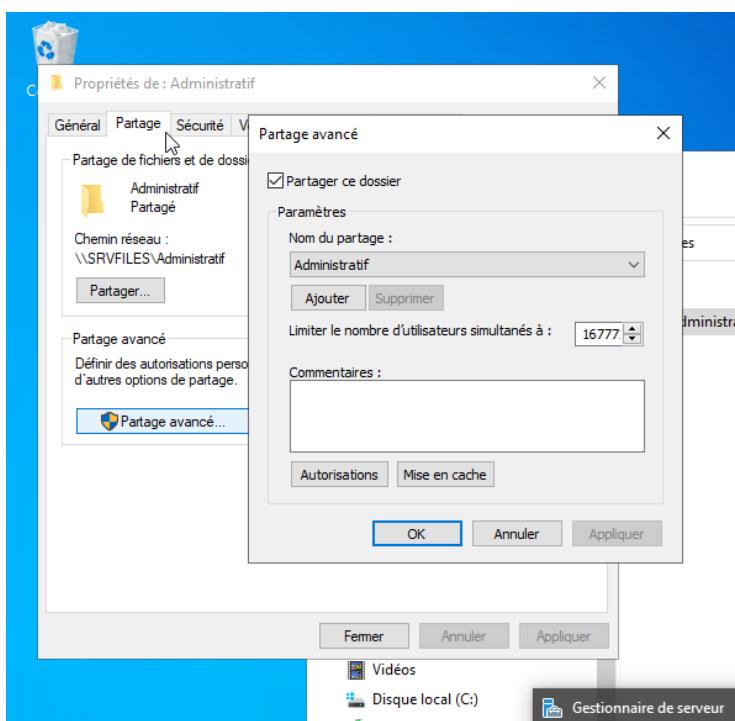


Figure 55 Serveur de fichier /Configuration du Partage

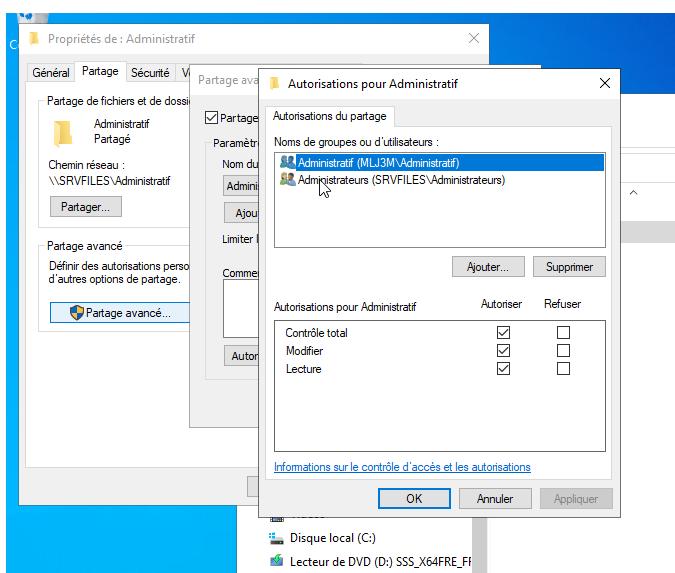
Propriétés du partage créé :



Paramétrage de partage avancé sur le partage créé :



Sélections des différentes autorisations sur ce partage :



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

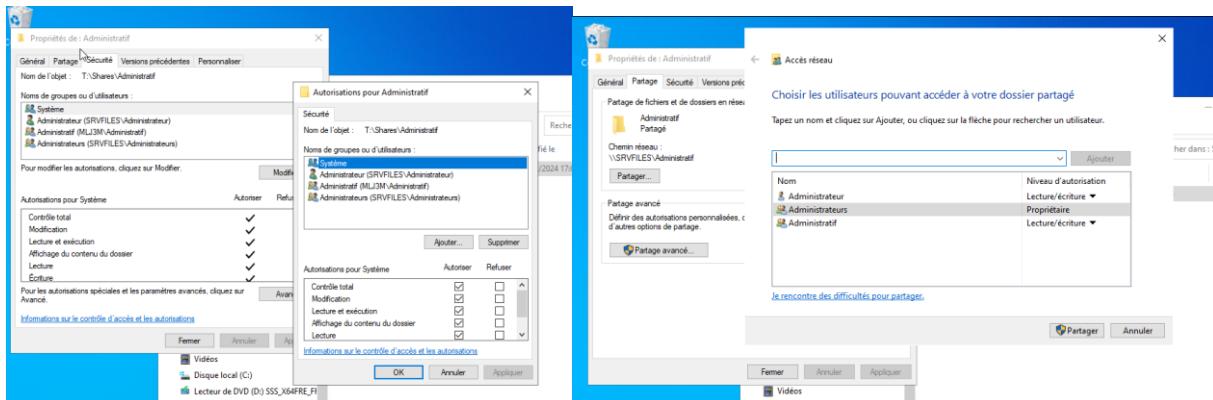


Figure 56 Serveur de fichier /Configuration des autorisations

Effectuer les différentes manipulations pour un partage « Conseiller », « Comptabilité » avec les groupes qui ont le même nom pour les autorisations.

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.

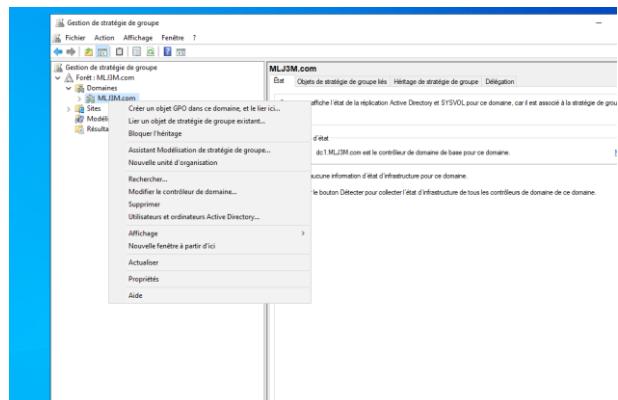
En effet, une stratégie de groupe peut servir à appliquer des paramètres sur Windows en lui-même, mais aussi à l'utilisateur directement (à son environnement, sa session), ou les deux.

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.

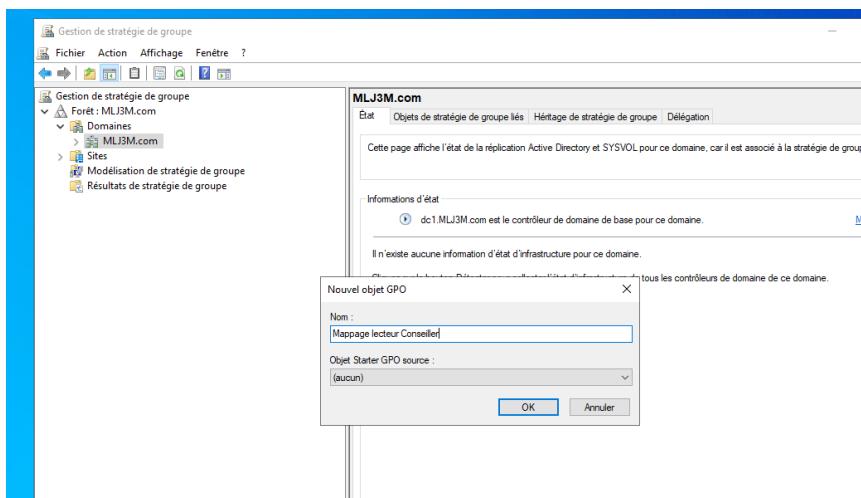
Voici les différentes GPO que je vais utiliser :

- Mappage d'un lecteur réseau pour le **groupe Administratif**
- Mappage d'un lecteur réseau pour le **groupe Comptabilité**
- Mappage d'un lecteur réseau pour le **groupe Conseiller**
- Mappage d'un lecteur réseau personnelle pour **chaque utilisateur du groupe Conseiller**

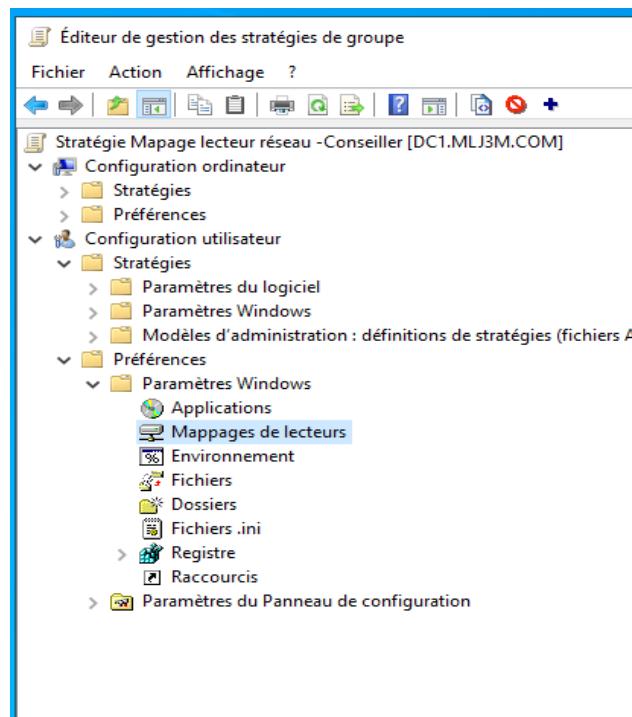
La première étape sera de vous rendre dans la gestion de stratégie de groupe, puis cliqué droit sur votre domaine et « crée un objet GPO dans ce domaine, et le lier ici »



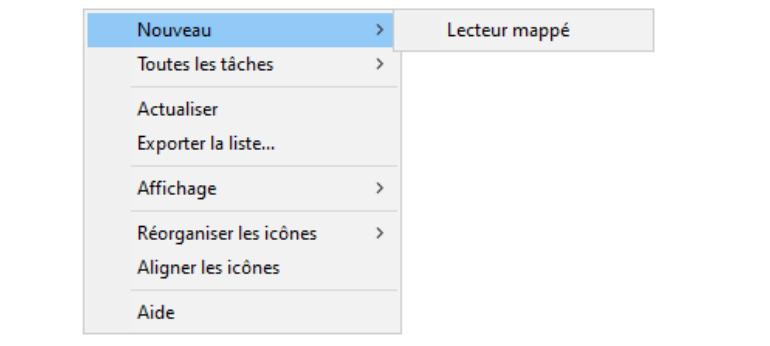
Nous nommerons notre GPO « Mappage lecteur Conseiller »



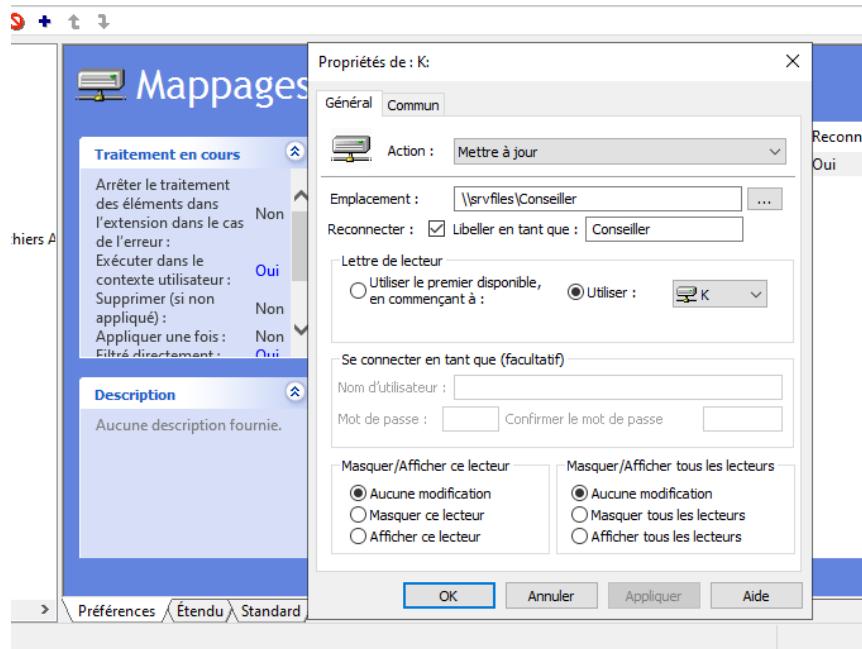
Puis une fois dans la GPO créée, nous nous rendrons dans :
Configuration utilisateur -> Préférences -> Mappages de lecteurs



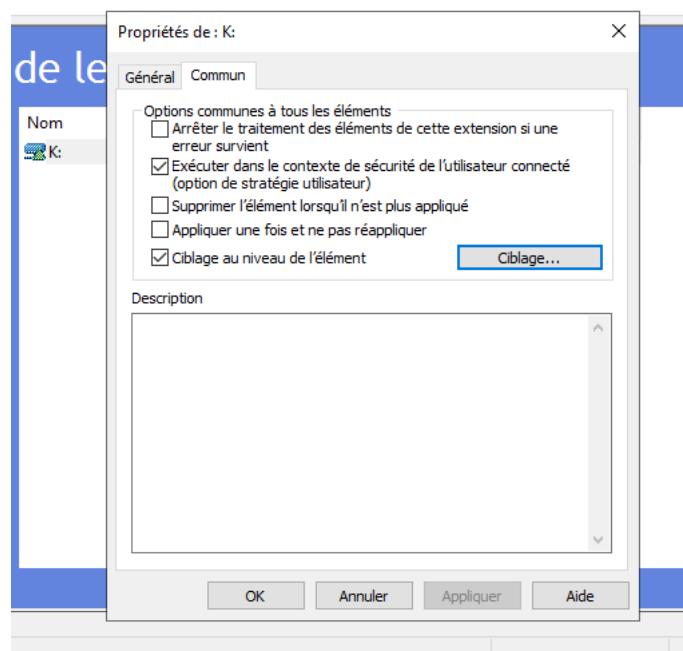
Clique droite puis Nouveau et « Lecteur mappé »



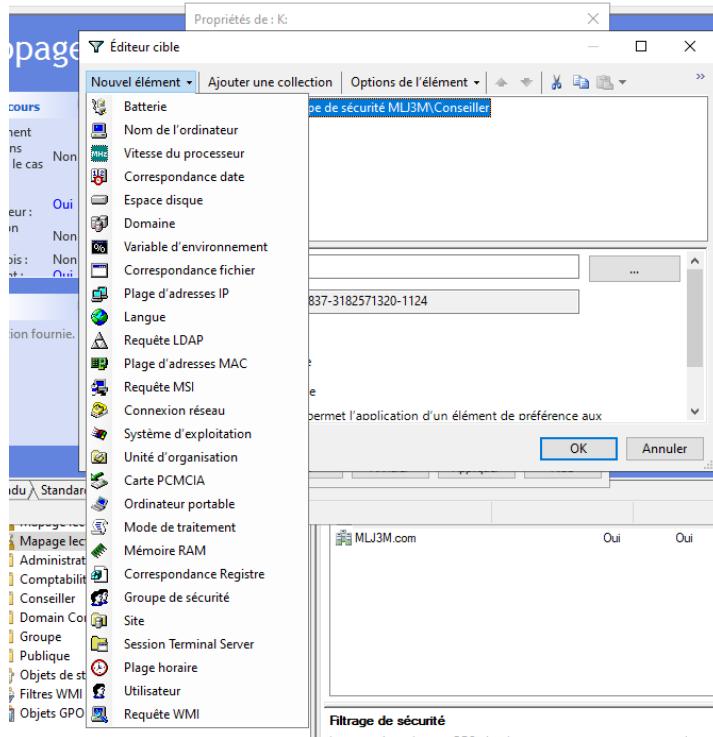
Une fois dans le menu du lecteur mappé, nous configurerons donc l'action « Mettre à jour », L'emplacement du partage « \\srvfiles\Conseiller » créé au préalable, attention a bien coché la case « Reconnecter » et attribuer un nom au Lecteur et enfin, nous choisirons une lettre pour le lecteur.



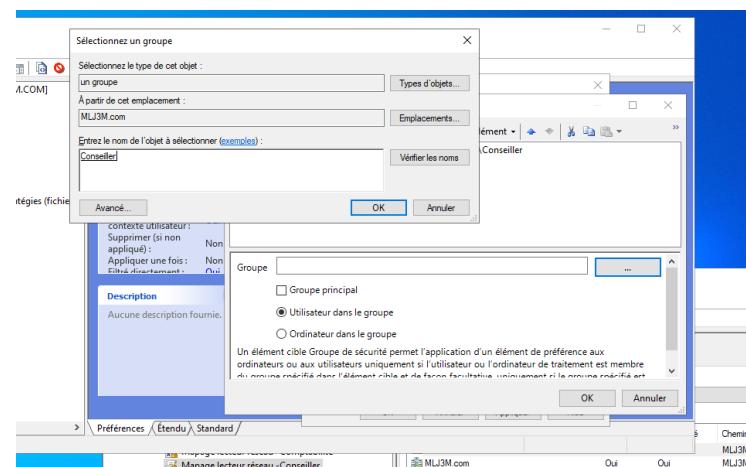
Nous nous rendrons ensuite dans « commun » et nous cocherons la case « Exécuter dans le contexte de sécurité de l'utilisateur connecté » et la case « Ciblage au niveau de l'élément » afin d'attribuer cette GPO à un groupe sélectionné.



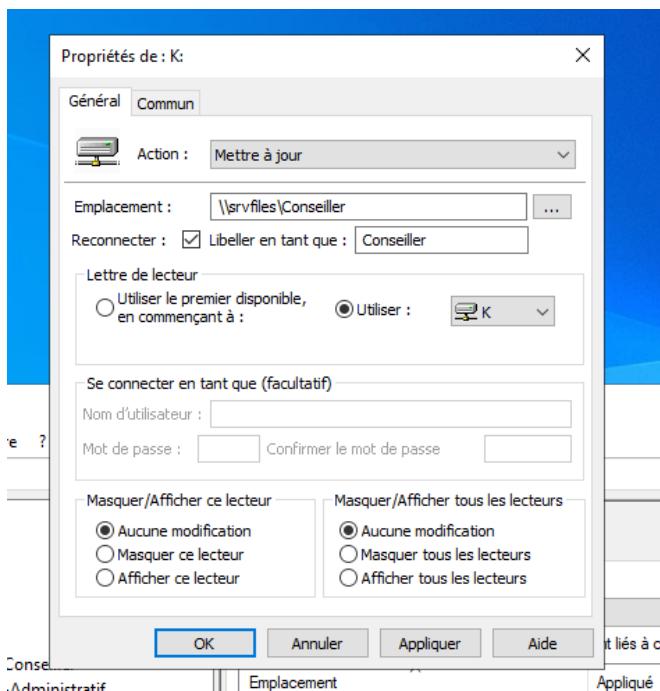
Nous nous rendrons dans « Nouvel élément » puis sélectionner « Groupe de sécurité »



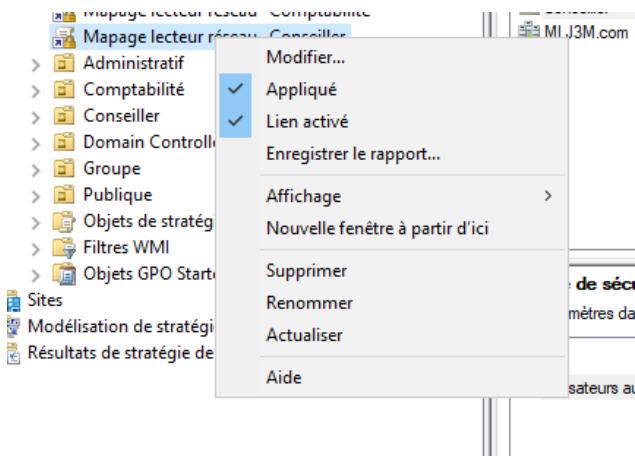
Nous ajouterons notre groupe pour lequel nous souhaitons activé la GPO, puis «OK »



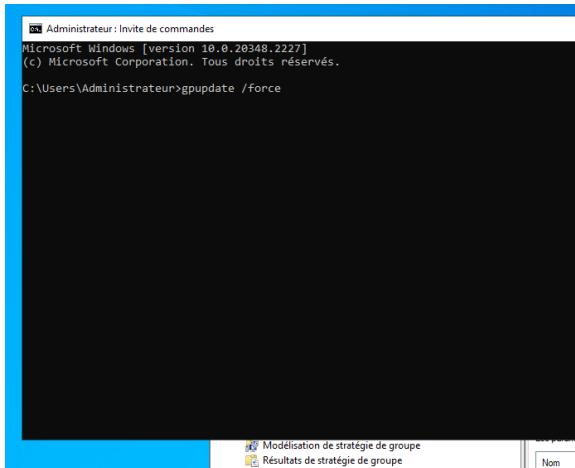
Vérifions toutes les informations et puis cliqué sur « appliquer »



N'oubliez pas d'appliquer la GPO en faisant clique droit sur celle-ci et « appliqué »



Pour forcer la GPO à s'activer, nous ouvrirons l'invite de commande (touche Windows puis tapé CMD), et nous utiliserons la commande « gpupdate /force »

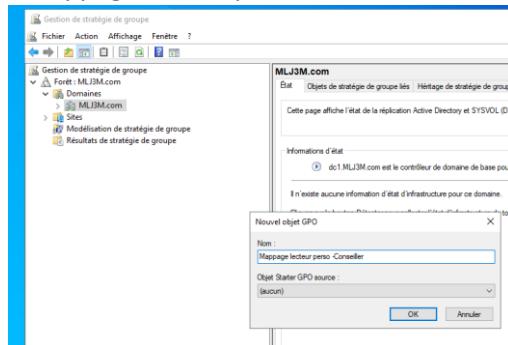


Nous répéterons les étapes pour le mappage du lecteur Administratif et le lecteur Comptabilité

Figure 57 : GPO /Mappage des lecteurs pour les groupes Administratif, Comptabilité et Conseiller

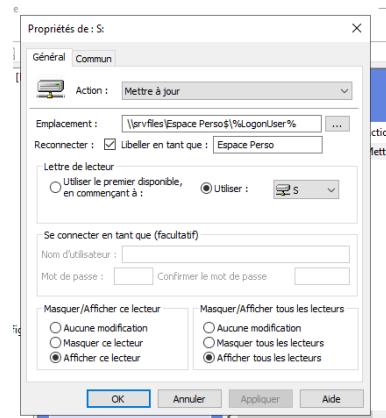
Nous recréerons une GPO de la même façon : « crée un objet GPO dans ce domaine, et le lier ici »

Nous nommerons notre GPO « Mappage lecteur perso Conseiller »

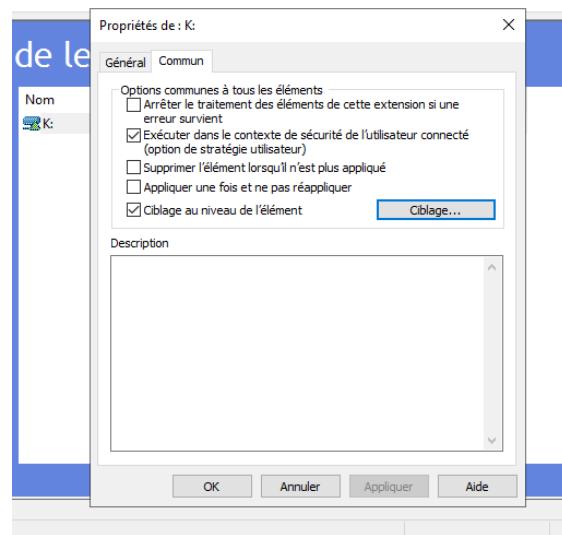


Puis une fois dans la GPO créée, nous nous rendrons dans :
Configuration utilisateur -> Préférences -> Mappages de lecteurs
Clique droit puis Nouveau et « Lecteur mappé »

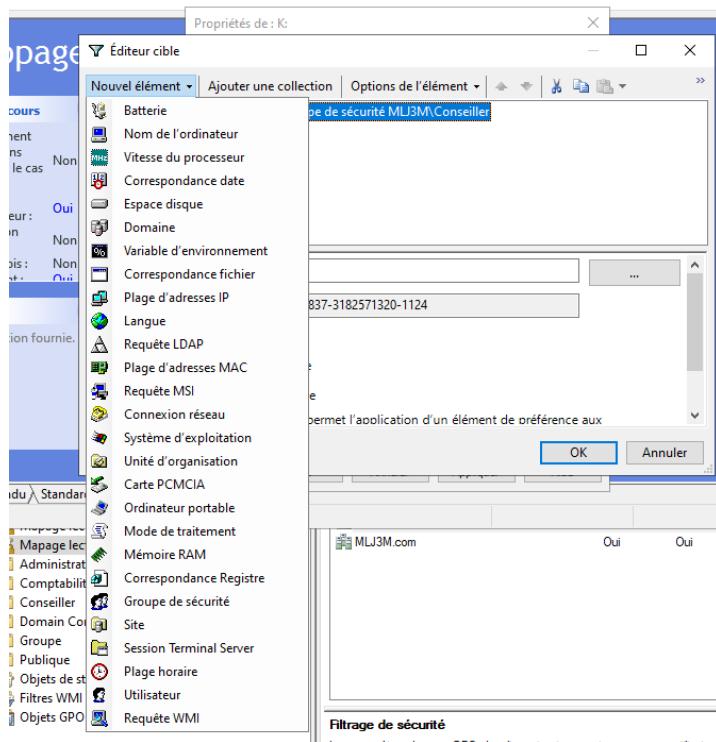
Une fois dans le menu du lecteur mappé, nous configurerons donc l'action « Mettre à jour »,
L'emplacement du partage « <\\srvfiles\Espace> Perso\$%\%LongonUser% » crée au préalable, attention à bien coché la case « Reconnecter » et attribuer un nom au Lecteur et enfin, nous choisirons une lettre pour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



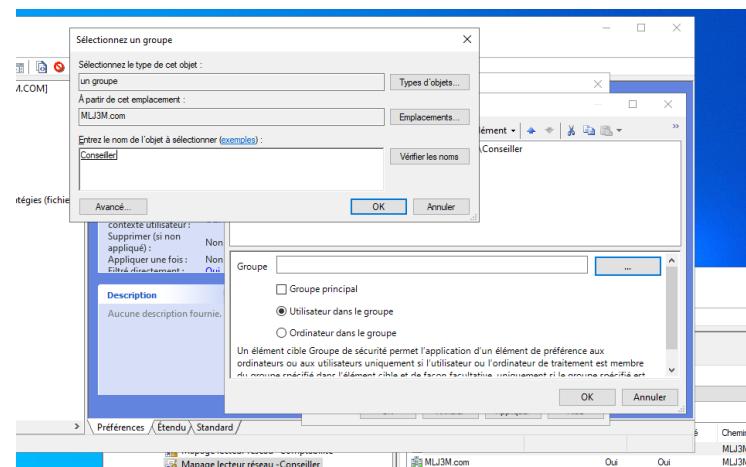
Nous nous rendrons ensuite dans « commun » et nous cocherons la case « Exécuter dans le contexte de sécurité de l'utilisateur connecté » et la case « Ciblage au niveau de l'élément » afin d'attribuer cette GPO à un groupe sélectionné.



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



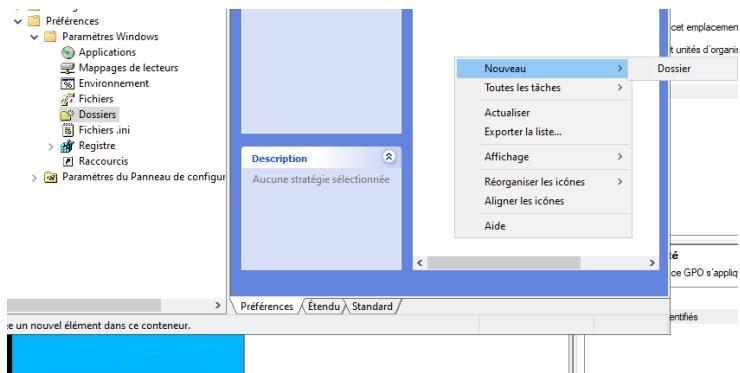
Nous ajouterons notre groupe pour lequel nous souhaitons activé la GPO, puis «OK »



Par la suite, nous nous rendrons dans :

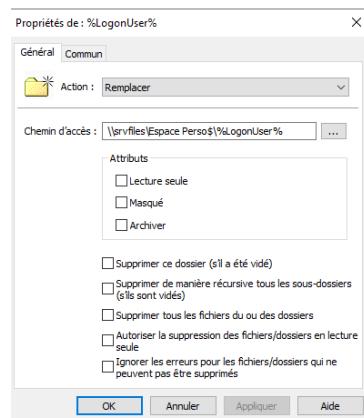
Configuration utilisateur -> Préférences -> Dossier

Clique droit puis Nouveau et « Dossier »

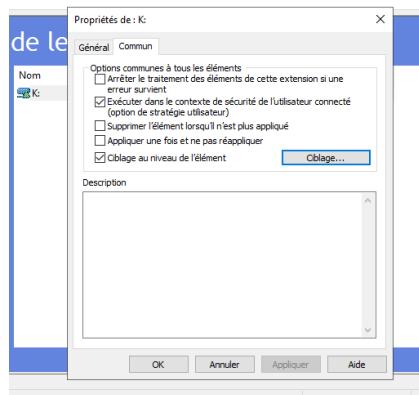


Une fois dans le menu du Dossier, nous configurerons donc l'action « Remplacer »,

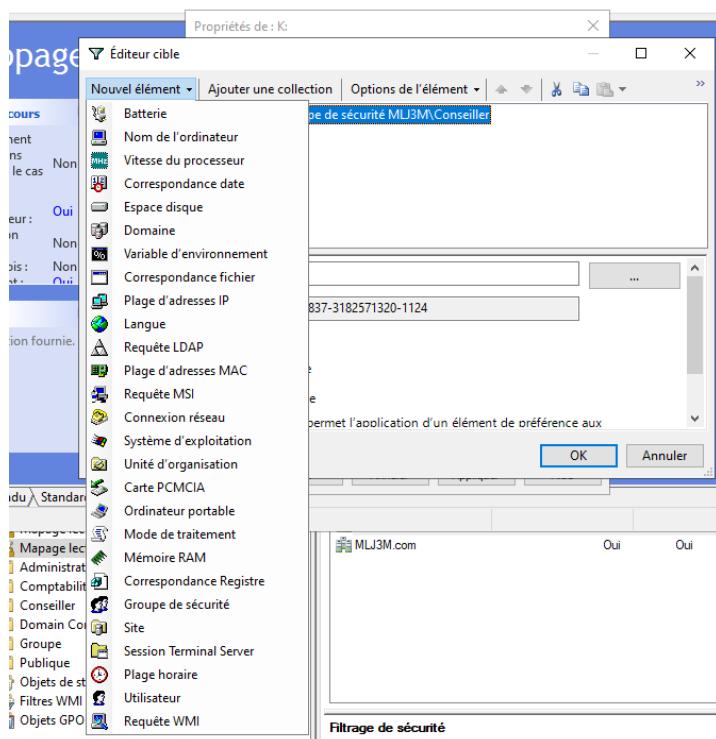
L'emplacement du partage « <\\srvfiles\Espace> Perso\$%\%LongonUser%» crée au préalable.



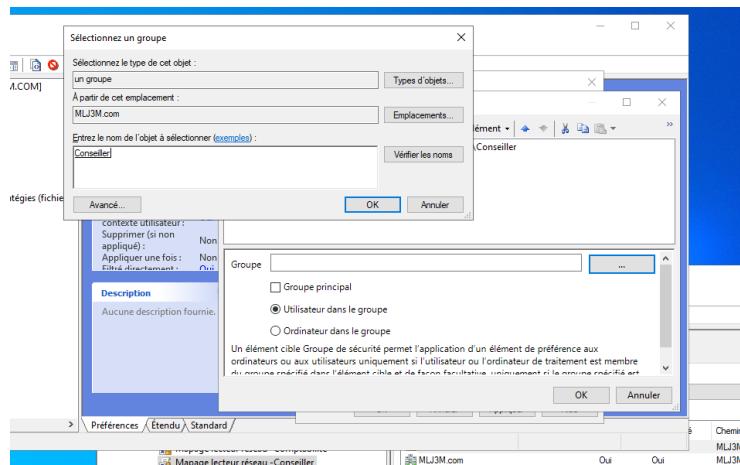
Nous nous rendrons ensuite dans « commun » et nous cocherons la case « Exécuter dans le contexte de sécurité de l'utilisateur connecté » et la case « Ciblage au niveau de l'élément » afin d'attribuer cette GPO à un groupe sélectionné.



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



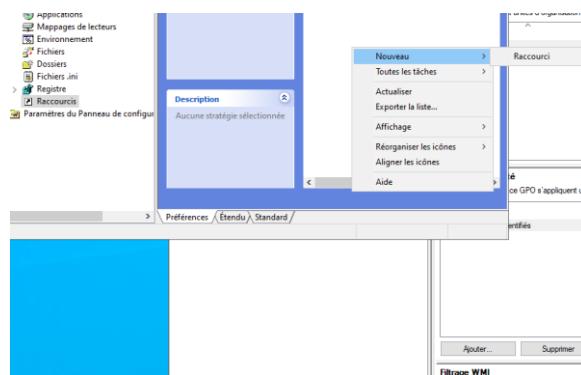
Nous ajouterons notre groupe pour lequel nous souhaitons activé la GPO, puis « OK »



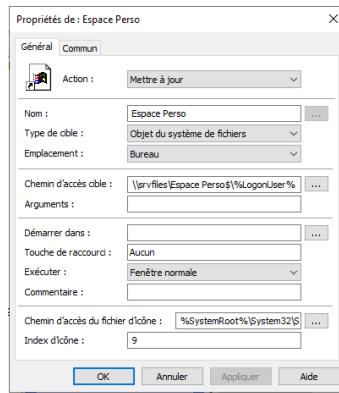
Par la suite, nous nous rendrons dans :

Configuration utilisateur -> Préférences -> Raccourci

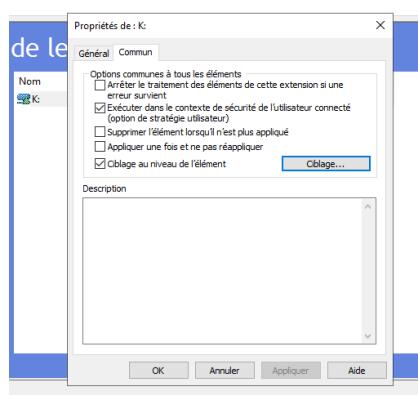
Clique droit puis Nouveau et « Raccourci »



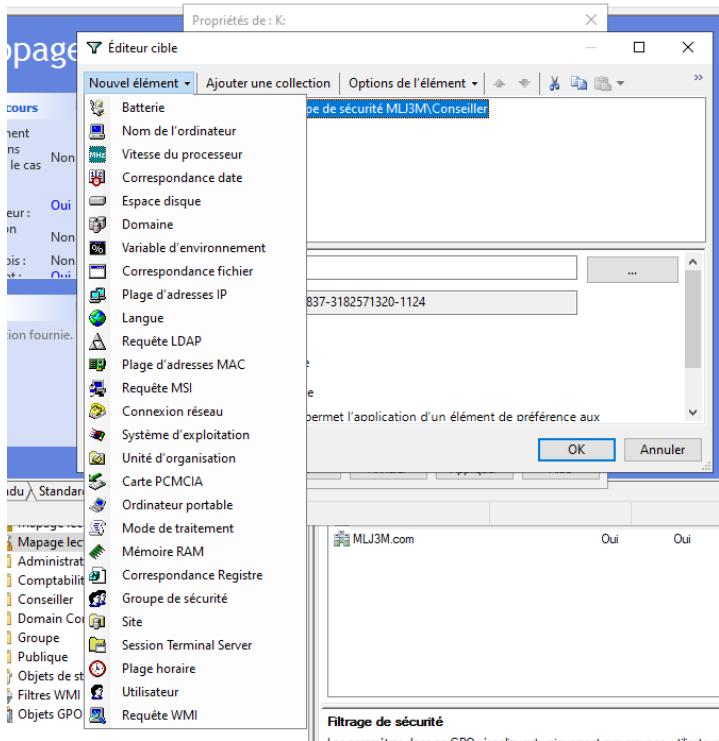
Une fois dans le menu du Raccourci, nous configurerons donc l'action « Mettre à jour »,
L'emplacement du partage « <\\srvfiles\Espace> Perso\$\%LongonUser% » crée au préalable.



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



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



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

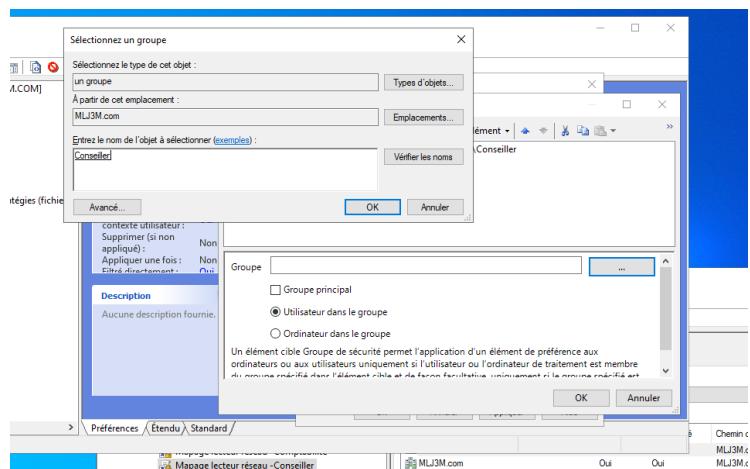
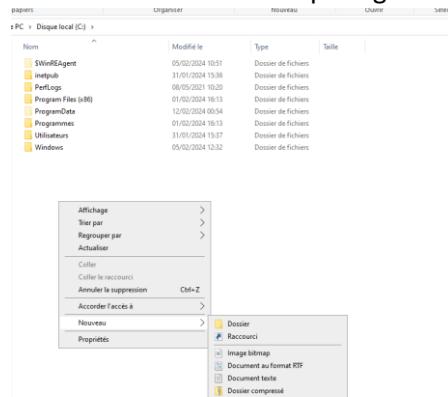
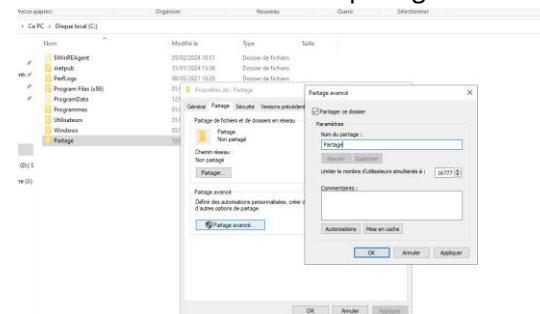


Figure 58 : GPO /Mappage d'un lecteur réseau d'un espace personnel pour chaque Utilisateurs du groupe Conseiller

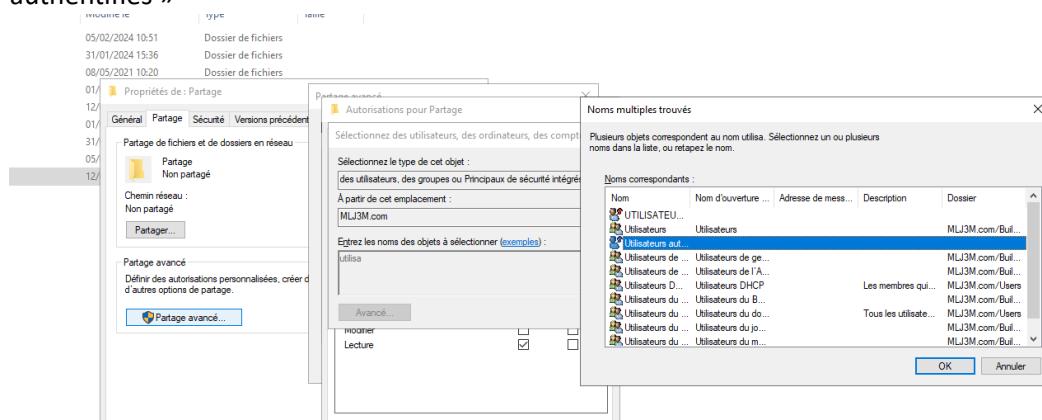
Dans un premier temps, nous créerons un nouveau dossier dans le « disque local C : »,
Nous le nommerons « partage »



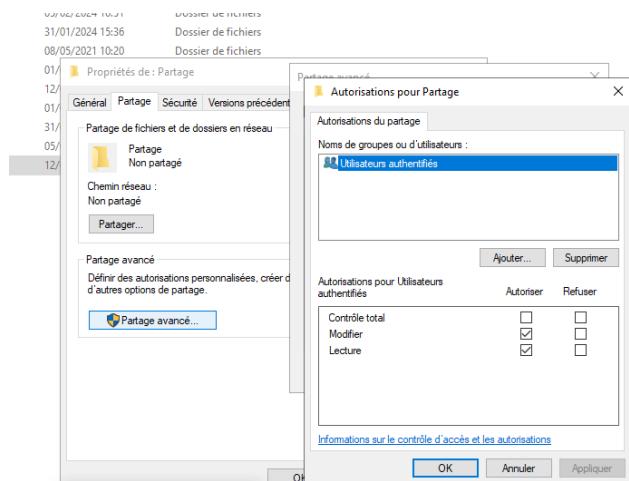
Ensuite, nous cloquerons droit dessus puis nous nous rendrons dans « partage »,
Une fois dans le menu partage, nous cocherons le « partage de ce dossier » et nous le
nommerons donc « partage »



Nous irons ensuite dans les « autorisations » et nous ajouterons le groupe « utilisateurs authentifiés »

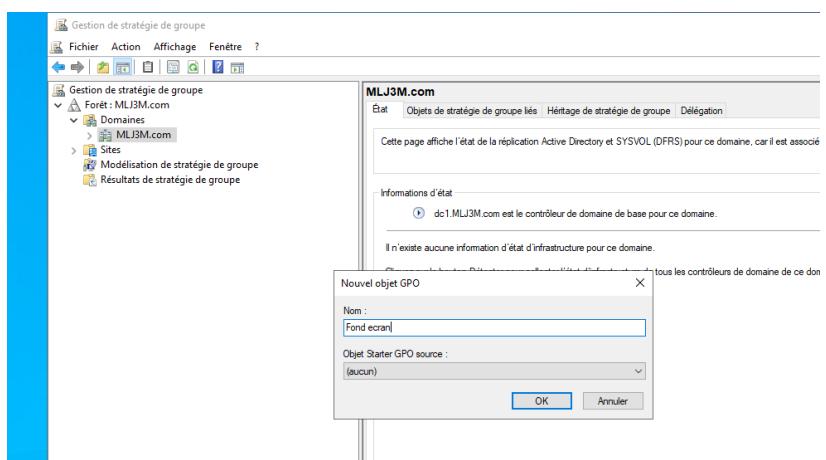


Vérifiez que le groupe a bien les deux cases « lecture » et « modifier » cocher.



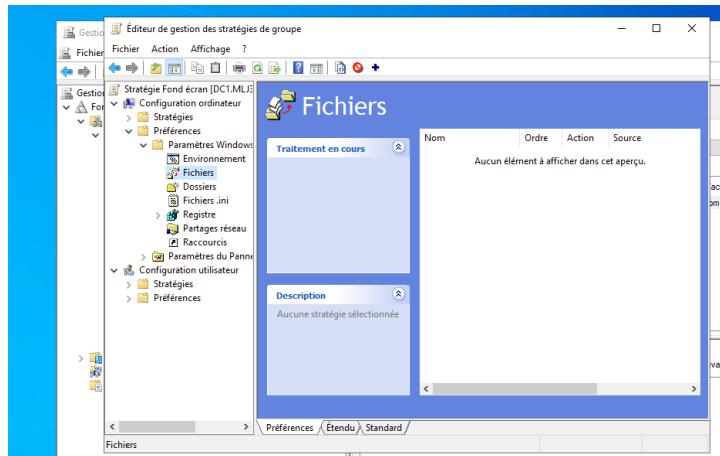
Nous créerons ensuite notre GPO, pour se faire nous nous rendrons dans la « gestion des stratégies de groupe » depuis le gestionnaire de serveur et nous ajouterons une nouvelle GPO en cliquant droit sur notre domaine puis « crée un objet GPO dans ce domaine, et le lier ici ».

Nous la nommerons « Fond écran »

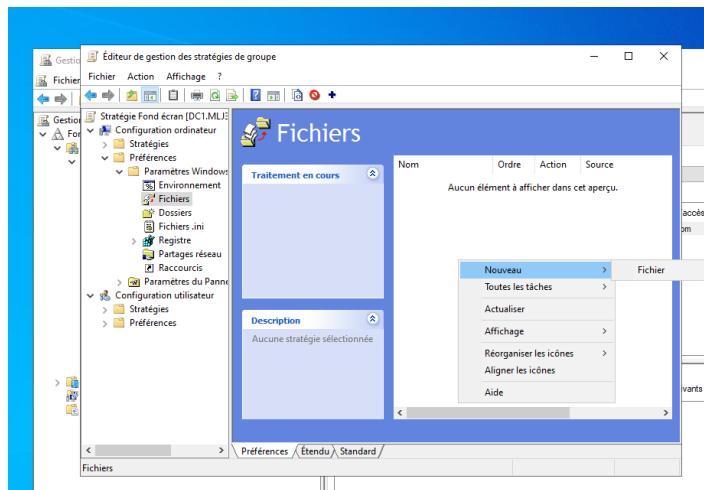


Par la suite, nous nous rendrons dans :

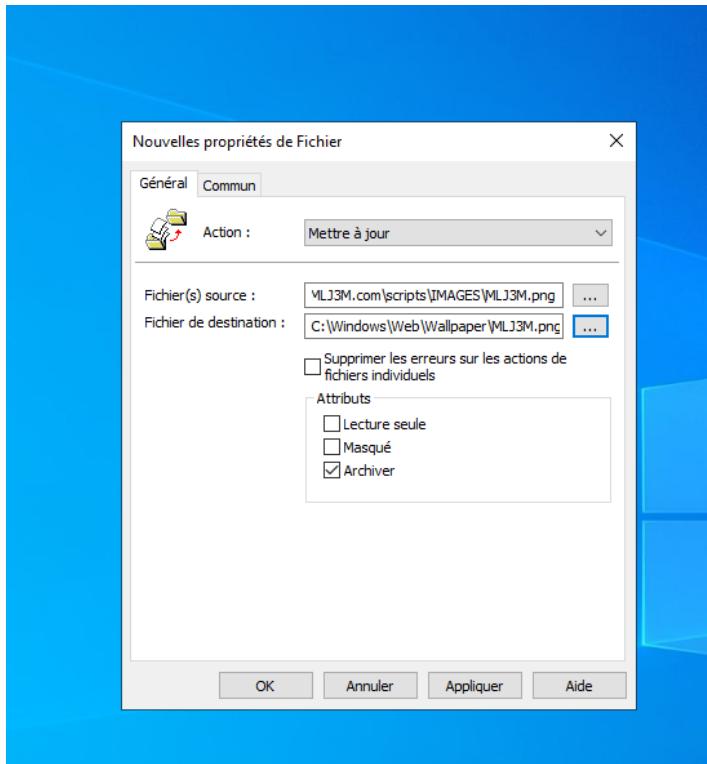
Configuration ordinateur -> Préférences -> paramètres Windows -> Fichier



Clique droit puis Nouveau et « Fichier »

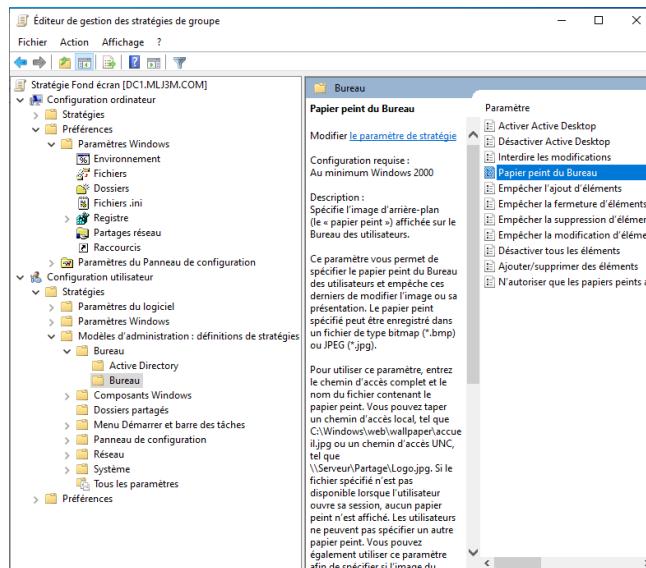


Une fois dans le menu du Fichier, nous configurerons donc l'action « Mettre à jour »,
l'emplacement du fichier sources, dans mon cas : « \\192.168.60.250\\partage\\MLJ3M.png »
l'emplacement du fichier de destination, dans mon cas : « C:\\Windows\\Web\\Wallpaper\\MLJ3M.png »

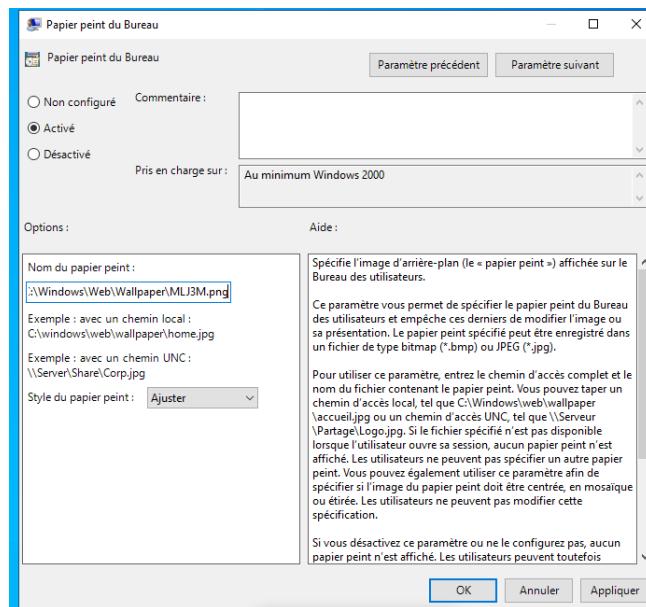


Ensuite, nous nous rendrons dans :

Configuration utilisateur -> Modèle d'administration -> Bureau -> Bureau -> Papier peint du Bureau



Dans les paramètres du papier peint du bureau, nous cocherons la case « activé » et nous vérifierons le bon chemin dans « nom du papier peint » (Chemin du fichier de destination)



Pour forcer la GPO à s'activer, nous ouvrirons l'invite de commande (touche Windows puis tapé CMD), et nous utiliserons la commande « gpupdate /force »

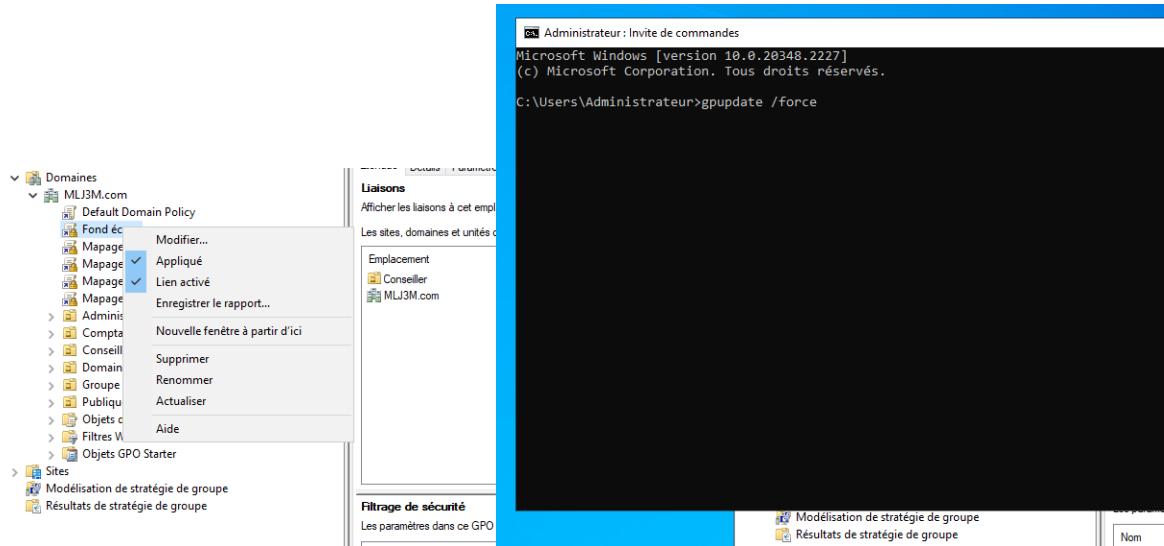
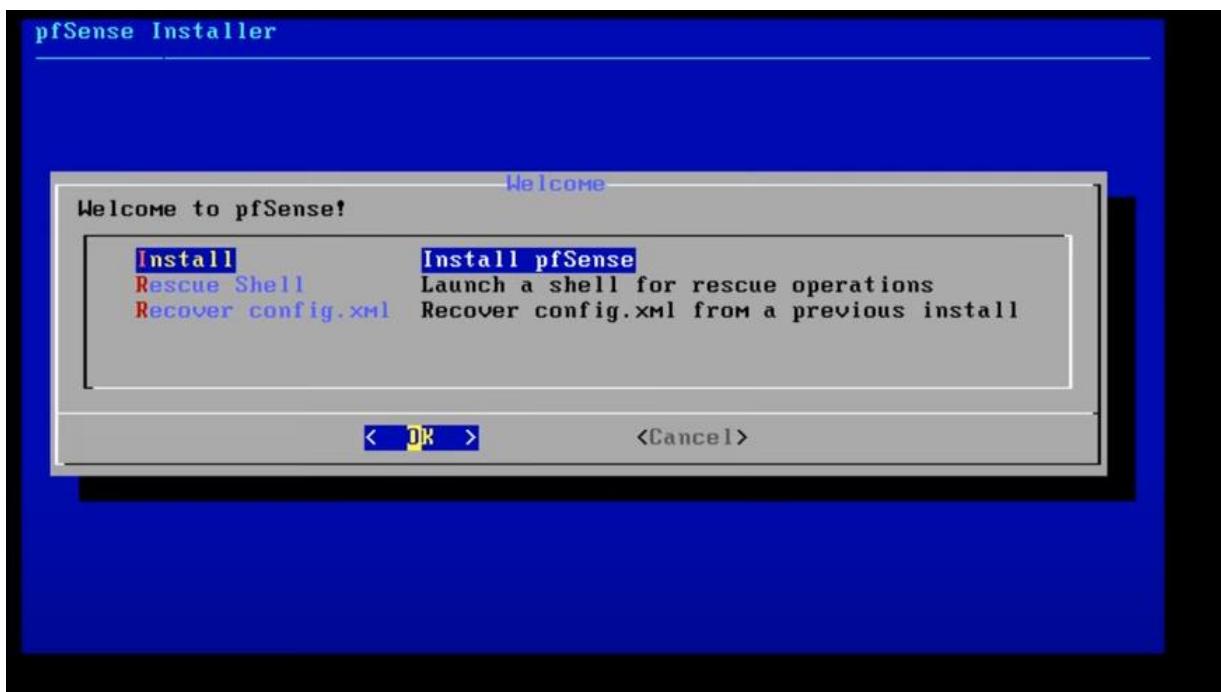


Figure 59 : GPO /Mappage d'un Fond d'écran sur les postes

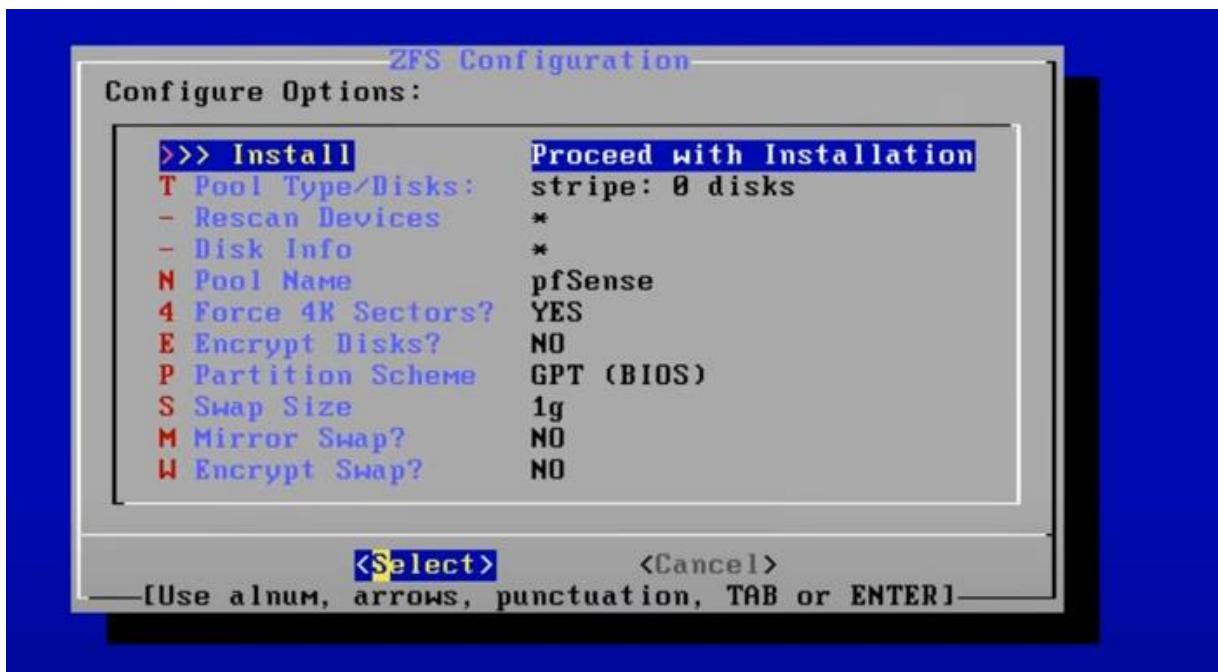
9 Firewall PFSense :

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



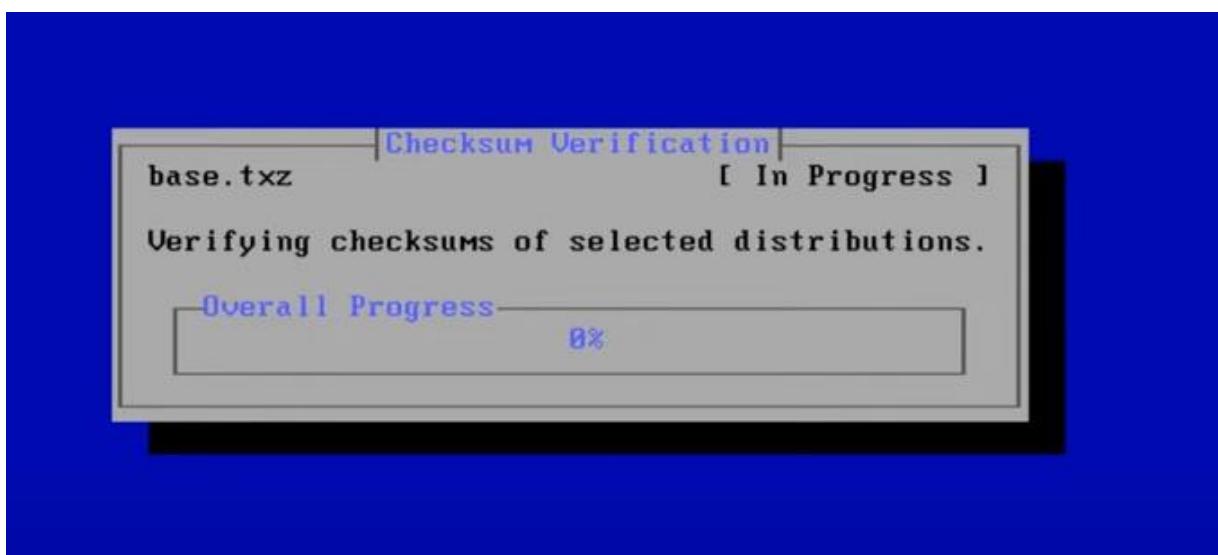
Sélectionner le disque virtuel



Confirmer par « yes » que vous souhaitez formater le disque



Patientez pendant l'installation



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

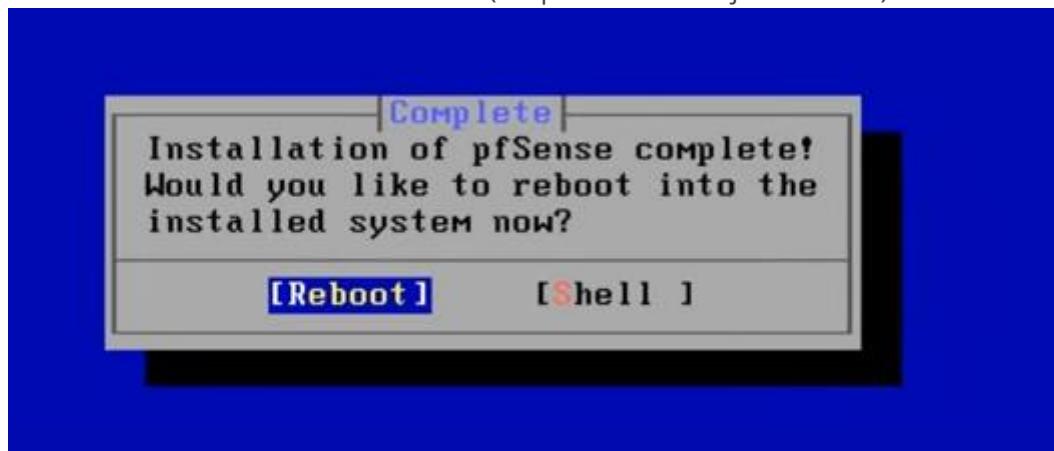


Figure 60 : PFSense /Installation de PFSENSE

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

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

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

VMware Virtual Machine - Netgate Device ID: e4aecdeef72a5f5a4cc

*** 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**

```
VMware Virtual Machine - Netgate Device ID: e4aecdeef72a5f5a4cc

*** 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 interfaces 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 : 192.168.60.1 (pour notre exemple)

```
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:
> 192,168,60,1
```

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

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 192.168.60.1  
  
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
```

```
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

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

```
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** :

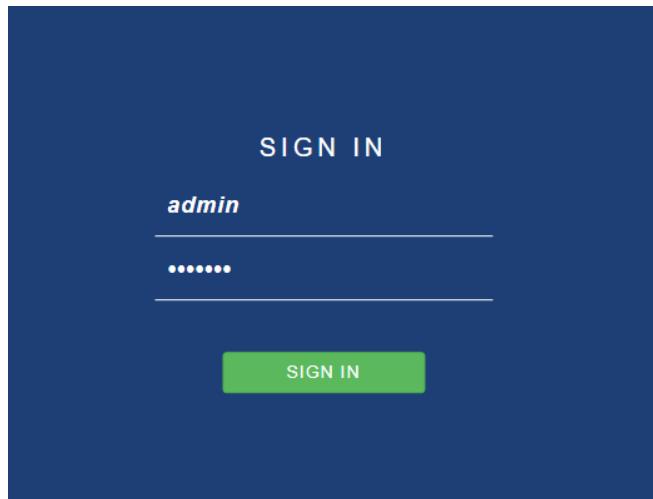
192.168.60.1

```
Do you want to enable the DHCP server on LAN? (y/n) n  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...  
  
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
  
The IPv4 LAN address has been set to 192.168.60.1/24  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
http://192.168.60.1/  
  
Press <ENTER> to continue.
```

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

Configuration de l'installation de Base de pfSense

Tapez L'adresse IP dans le navigateur : 192.168.60.1 – 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	<input type="text" value="pfSense"/>
Name of the firewall host, without domain part.	
Examples: pfsense, firewall, edgefw	
Domain	<input type="text" value="home.arpa"/>
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 »

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

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

Static IPv4 Configuration

IPv4 Address	192.168.60.1	/	24
IPv4 Upstream gateway	None	+ Add a new gateway	
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.			

Modifier le **mot de passe admin**

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnos

WARNING: The 'admin' account password is set to the default value. Change the password in the User Accounts section of the System menu.

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the Web-based configuration interface.

Admin Password:

Admin Password AGAIN:

>> Next

Cliquez sur : **Reload**

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnos

Wizard / pfSense Setup / Reload configuration

Step 7 of 9

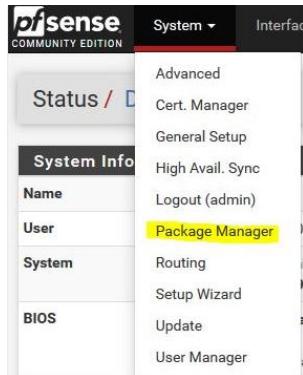
Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload

Figure 62 : PFSense /Configuration de PFSENSE

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 Package Manager. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', 'Help', and a question mark icon. The main title is 'System / Package Manager / Available Packages'. Below this, there are two tabs: 'Installed Packages' (red) and 'Available Packages' (yellow, highlighted). A search bar contains 'squid' in the 'Search term' field, with dropdown options 'Both' and 'Search' (with a magnifying glass icon) and a 'Clear' button. A note below says 'Enter a search string or *nix regular expression to search package names and descriptions.' The main table is titled 'Packages' and has columns 'Name', 'Version', and 'Description'. It lists three packages: 'Lightsquid 3.0.6_4', 'squid 0.4.44_5', and 'squidGuard 1.16.17_3'. Each row shows a brief description and a green 'Install' button with a plus sign. Under the 'Description' column for squid, it says 'Package Dependencies: squidclamav-6.16 squid_radius_auth-1.10 squid-3.5.27_3 c-icap-modules-0.5.2'.

Installation des Packages

The top screenshot shows the 'Package Installer' tab selected. A message at the top says: 'Please wait while the installation of pfSense-pkg-Lightsquid completes. This may take several minutes. Do not leave or refresh the page!'. Below the message, there are three tabs: 'Installed Packages', 'Available Packages', and 'Package Installer' (which is underlined). A progress bar is shown below the tabs. The main area displays the package installation log:

```

p5-ExtUtils-PkgConfig: 1.16 [pfSense]
pkcconf: 1.4.2.1 [pfSense]

Number of packages to be installed: 18

The process will require 15 MiB more space.
3 MiB to be downloaded.
[1/18] Fetching pfSense-pkg-Lightsquid-3.0.6_4.txz: ..... done
[2/18] Fetching lighttpd-1.4.49.txz: ..... done
[3/18] Fetching lua52-5.2.4.txz: ..... done
[4/18] Fetching lightsquid-1.8.5.txz: ..... done
[5/18] Fetching p5-CGI-4.38.txz: ..... done
[6/18] Fetching p5-HTML-Parser-3.72.txz: ..... done
[7/18] Fetching p5-HTML-Tagset-3.20_1.txz: .. done

```

The bottom screenshot shows the same interface after the installation is completed. A green success message at the top says: 'pfSense-pkg-squid installation successfully completed.' Below the message, the 'Installed Packages' tab is selected. The main area shows the installed packages:

- Lightsquid (version 3.0.6_4)
- squid (version 0.4.44_5)
- squidGuard (version 1.16.17_3)

Les 3 Packages sont installés

This screenshot shows the 'Installed Packages' tab selected. The main area displays a table of installed packages:

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.	
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.	
squidGuard	www	1.16.17_3	High performance web proxy URL filter.	

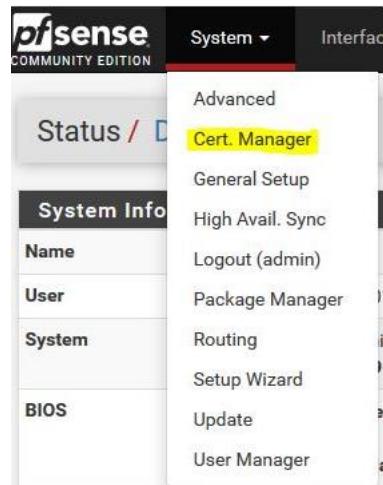
At the bottom of the table, there are notes about package dependencies and actions:

- Icons: = Update, = Current
- Buttons: = Remove, = Information, = Reinstall
- Text: 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 »

A screenshot of the pfSense Certificate Manager interface. The top navigation bar is identical to the main interface. The main area shows a breadcrumb path: System / Certificate Manager / CAs. Below this, there are three tabs: CAs (selected), Certificates, and Certificate Revocation. A table titled 'Certificate Authorities' is displayed with columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. At the bottom right of the table is a green button with a plus sign and the word 'Add'.

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

System / Certificate Manager / CAs / Edit

Create / Edit CA

Internal Certificate Authority

Descriptive name:	DemoCA
Method:	Create an internal Certificate Authority
Key length (bits):	2048
Digest Algorithm:	sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.	
Lifetime (days):	3650
Common Name:	internal-ca
The following certificate authority subject components are optional and may be left blank.	
Country Code:	None
State or Province:	e.g. Texas
City:	e.g. Austin
Organization:	e.g. My Company Inc
Organizational Unit:	e.g. My Department Name (optional)

Save

Le Certificat est créé

System / Certificate Manager / CAs

Certificates

Search

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
DemoCA	✓	self-signed	0	CN=internal-ca Valid From: Mon, 20 Jul 2020 17:27:46 +0200 Valid Until: Thu, 18 Jul 2030 17:27:46 +0200		

Add

Figure 64 : PFSense Filtrage /Configuration du certificat

Configuration de Squid

Sélectionner « Services » et « Squid Proxy Server »

The screenshot shows the pfSense web interface. At the top, there is a navigation bar with tabs: System, Interfaces, Firewall, Services (which is currently selected), and VPN. Below the navigation bar is a status dashboard with sections for System Information, Network, and Services. On the right side of the screen, a vertical sidebar displays a list of services. The 'Services' tab is highlighted in red, and the 'Squid Proxy Server' option is highlighted with a yellow box.

System Information	
Name	pfSense.localdomain
User	admin@192.168.2.101 (Local Database)
System	Hyper-V Virtual Machine Netgate Device ID: 391ed73786ee43989c09
BIOS	Vendor: American Megatrends Inc. Version: 090006 Release Date: Wed May 23 2012
Version	2.4.4-RELEASE (amd64) built on Thu Sep 20 09:03:12 EDT 2018 FreeBSD 11.2-RELEASE-p3 The system is on the latest version. Version information updated at Mon Oct 1 12:45:25 UTC 2018
CPU Type	Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	01 Hour 32 Minutes 59 Seconds

- 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

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 pfSense Local Cache Management interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a breadcrumb trail: Package / Proxy Server: Cache Management / Local Cache. The main content area has tabs for General, Remote Cache, Local Cache, Antivirus, ACLs, Traffic Mgmt, Authentication, Users, Real Time, and Sync. The Local Cache tab is selected. The configuration is divided into several sections:

- Squid Cache General Settings:** Cache Replacement Policy is set to "Heap LFUDA". Low-Water Mark in % is 90, and High-Water Mark in % is 95.
- Squid Hard Disk Cache Settings:** Hard Disk Cache Size is 500 MB, using the ufs storage system. Clear Disk Cache NOW is enabled. Level 1 Directories is 10. Hard Disk Cache Location is /var/squid/cache. Minimum Object Size is 0, and Maximum Object Size is 4 MB.
- Squid Memory Cache Settings:** Memory Cache Size is 64 MB, and Maximum Object Size in RAM is 256 KB. Memory Replacement Policy is set to "Heap GDSF".
- Dynamic and Update Content:** Cache Dynamic Content is enabled. Custom refresh_patterns are defined in a text area.

A blue "Save" button is located at the bottom right of the configuration area.

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

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 3128
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.
Important: Transparent proxy mode works without any additional configuration being necessary on clients.

Transparent Proxy Interface(s) WAN
LAN
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 192.168.2.10;192.168.2.55;10-2004.MON-ORDINATEUR
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 192.168.2.10
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 Enable SSL filtering.

SSL/MITM Mode Splice All
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. i

SSL Intercept Interface(s) 10.10.10.1 (pfB DNSBL - DO NOT EDIT)
WAN
LAN

The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port 3129
This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

SSL Proxy Compatibility Mode Modern
The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details. i

DHParams Key Size 2048 (default)
DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA DemoCA
Select Certificate Authority to use when SSL interception is enabled. i

SSL Certificate Daemon Children 5
This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

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

Logging Settings

Enable Access Logging This will enable the access log.
Warning: Do NOT enable if available disk space is low.

Log Store Directory /var/squid/logs
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.

Rotate Logs 365
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Log Pages Denied by SquidGuard Makes it possible for SquidGuard denied log to be included on Squid logs.
Click Info for detailed instructions. i

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' configuration page. It includes fields for 'Visible Hostname' (localhost), 'Administrator's Email' (admin@localhost), 'Error Language' (fr), 'X-Forwarded Header Mode' (on), 'Disable VIA Header' (unchecked), 'URI Whitespace Characters Handling' (strip), and 'Suppress Squid Version' (checked). At the bottom are 'Save' and 'Show Advanced Options' buttons.

Figure 65 : PFSense Filtrage /Configuration de Squid

Configuration de SquidGuard

Sélectionner « Services » et « SquidGuard Proxy Filter »

The screenshot shows the pfSense Status / Dashboard. The Services menu is open, listing various services: 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, and SquidGuard Proxy Filter. The SquidGuard Proxy Filter option is highlighted with a yellow background.

Activer SquidGuard « Enable »

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

- Header:** pfSense COMMUNITY EDITION, System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.
- Breadcrumbs:** Package / Proxy filter SquidGuard: General settings / General settings
- Toolbar:** CO, E, I, L, ?, Refresh
- Navigation:** General settings, Common ACL, Groups ACL, Target categories, Times, Rewrites, Blacklist, Log, XMLRPC Sync.
- Section:** 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.**
- Buttons:** Apply
- Status:** SquidGuard service state: STOPPED

Activer « Enable Log » et « Enable log rotation »

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

- Section:** 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 insérer dans **Blacklist URL** : http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Puis cliquez sur « **Save** »

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

- Section:** 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:** http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.
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).
- Buttons:** Save

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

The screenshot shows the pfSense web interface under the SquidGuard package. The 'Blacklist' tab is selected. A progress bar indicates a 'Blacklist DB rebuild progress' at 1%. Below it, a text input field contains the URL 'http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz'. There are three buttons: 'Download' (green), 'Cancel' (orange), and 'Restore Default' (blue). A note below says 'Enter FTP or HTTP path to the blacklist archive here.' Below this is a 'Blacklist update Log' section 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 under the Proxy filter SquidGuard: Common Access Control List (ACL) package. The 'Common ACL' tab is selected. In the 'General Options' section, there is a 'Target Rules' input field. Below it is a 'Target Rules List' section with a '+ -' button. The 'Target Rules List' section is currently empty.

Sélectionner les catégories à bloquer (ou à 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_agressif]	access deny ▾
[blk_blacklists_arjal]	access — ▾
[blk_blacklists_associations_religieuses]	access — ▾
[blk_blacklists_astrology]	access — ▾
[blk_blacklists_audio_video]	access — ▾
[blk_blacklists_bank]	access — ▾
[blk_blacklists_bitcoin]	access — ▾
[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_droge]	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 \$g[product_name] proxy"	
Redirect mode	<input type="text" value="int error page (enter error message)"/> <input type="button" value="▼"/>
Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not 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)"/> <input type="button" value="▼"/>
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

10 PRTG :



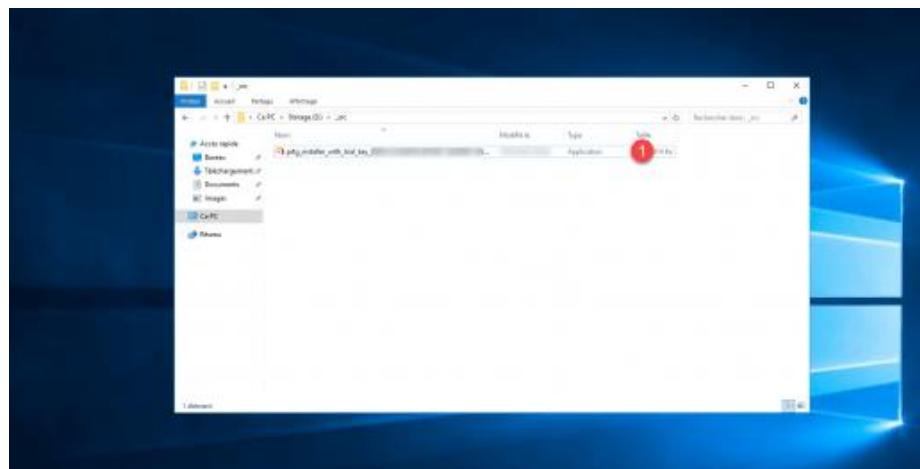
La page d'accueil peut avoir changée depuis la rédaction de ce tutoriel.

La première étape va être de télécharger PRTG sur le site officiel.

1. Aller sur le site de l'éditeur : [Paessler – The Monitoring Experts.](https://www.paessler.com/fr)
2. Depuis la page d'accueil cliquer sur le bouton TÉLÉCHARGER GRATUIT



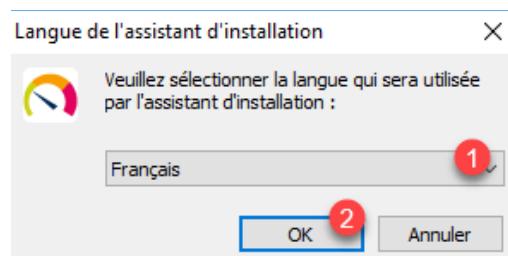
3. Le téléchargement devrait démarrer automatique. Copier dans un fichier texte la clé de licence **1** qui s'affiche.



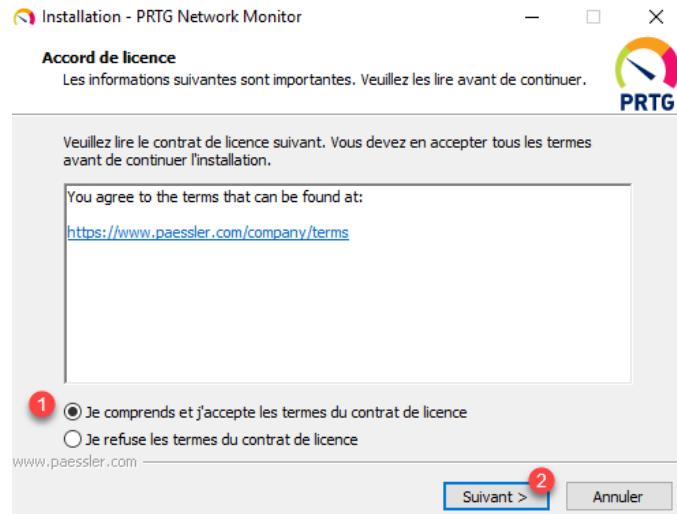
Installation de PRTG

Maintenant que nous avons la clé de licence et le fichier, nous allons passer à son installation.

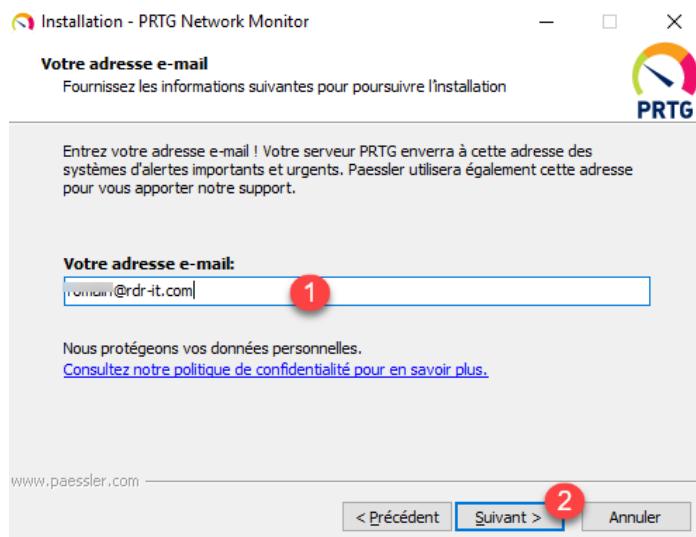
1. Exécuter le fichier téléchargé **1**.



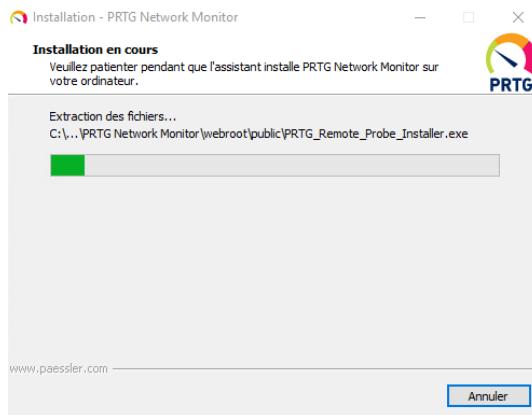
2. Choisir la langue **1** de l'assistant d'installation et cliquer sur le bouton OK **2**.



3. Accepter le contrat de licence **1** et cliquer sur Suivant **2**.



4. Entrer une adresse e-mail **1** et cliquer sur le bouton Suivant **2**.



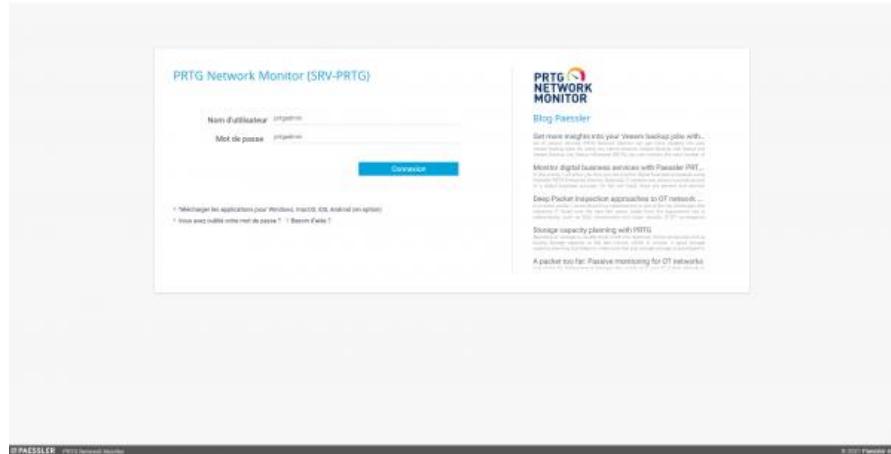
5. Patienter pendant l'installation de PRTG ...

Figure 67 : PRTG / Téléchargement et Installation



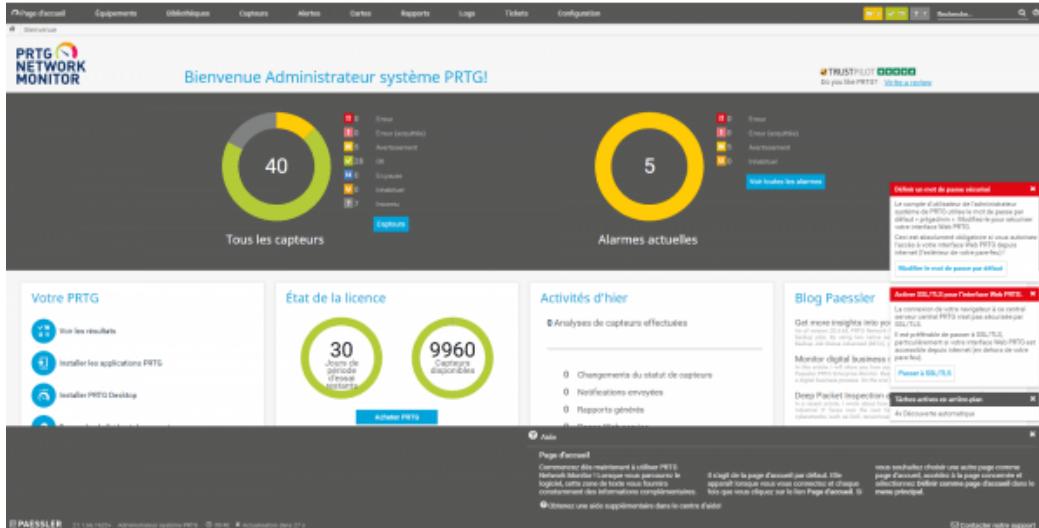
6. Normalement le navigateur s'ouvre directement sur PRTG ... patienter pendant l'initialisation de celui-ci.

Figure 62 : PRTG /

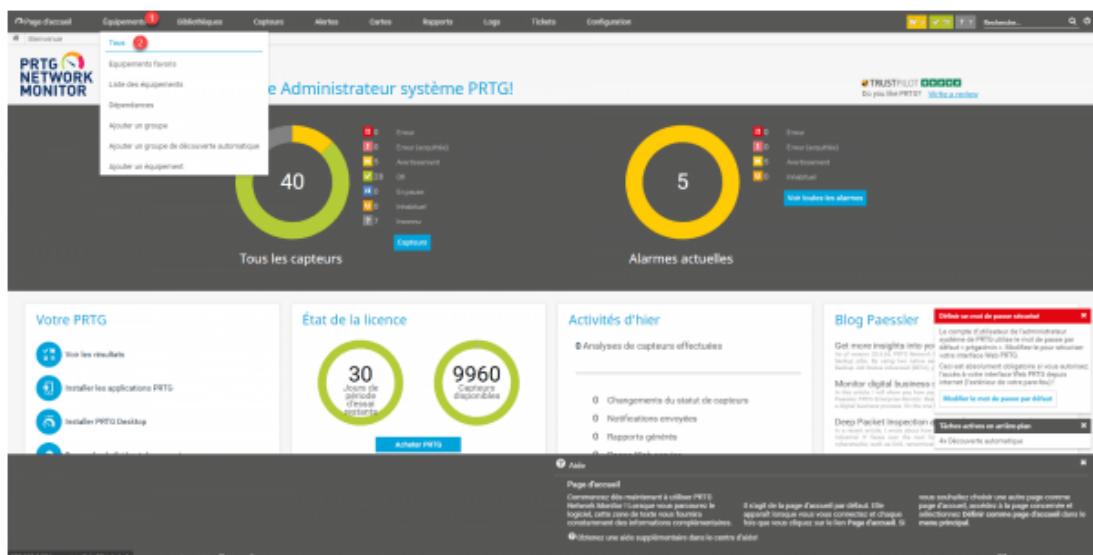


Une fois PRTG entièrement démarré, se connecter à l'aide de l'identifiant prtgadmin et du mot de passe prtgadmin.

Figure 62 : PRTG /



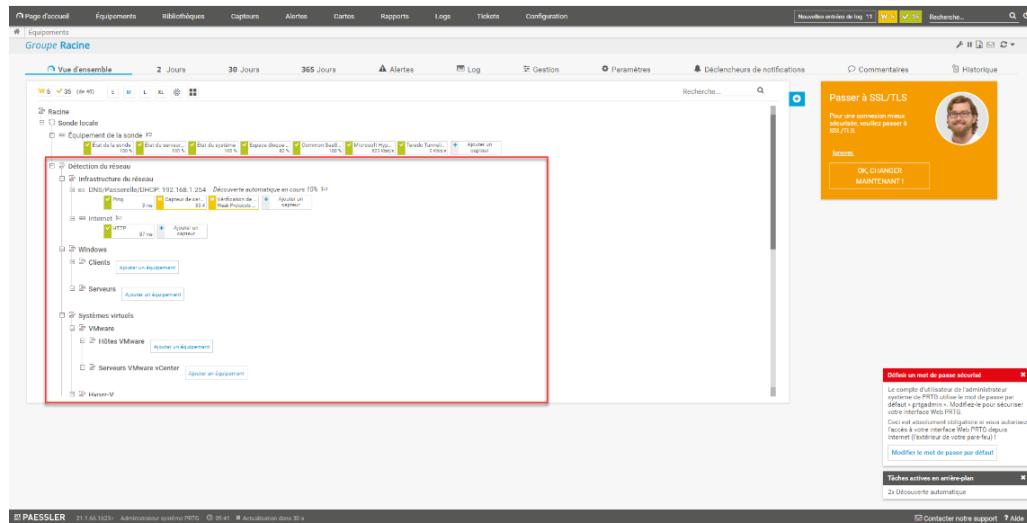
Le tableau de bord se charge.



Prise en main de PRTG

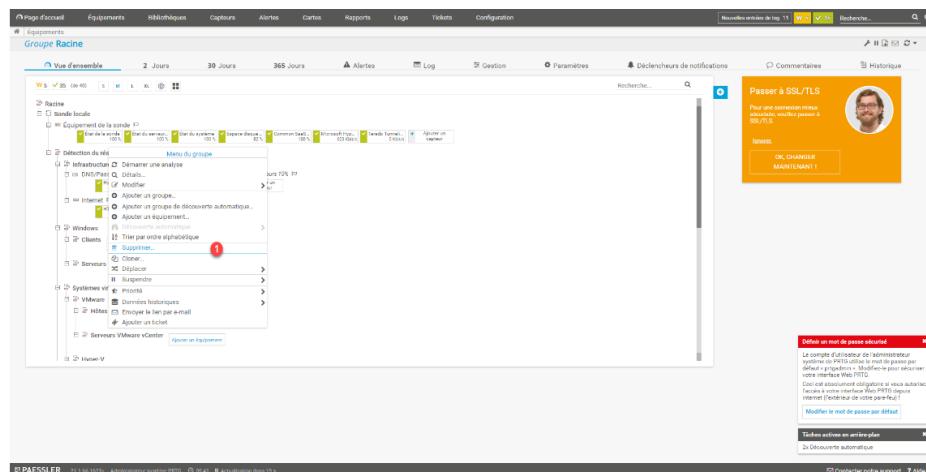
Lors de son installation et de son premier démarrage, PRTG va lancer un scan automatique du réseau pour essayer d'ajouter les équipements automatiques.

Passer le curseur de souris sur Équipements **1** puis cliquer sur Tous **2**.

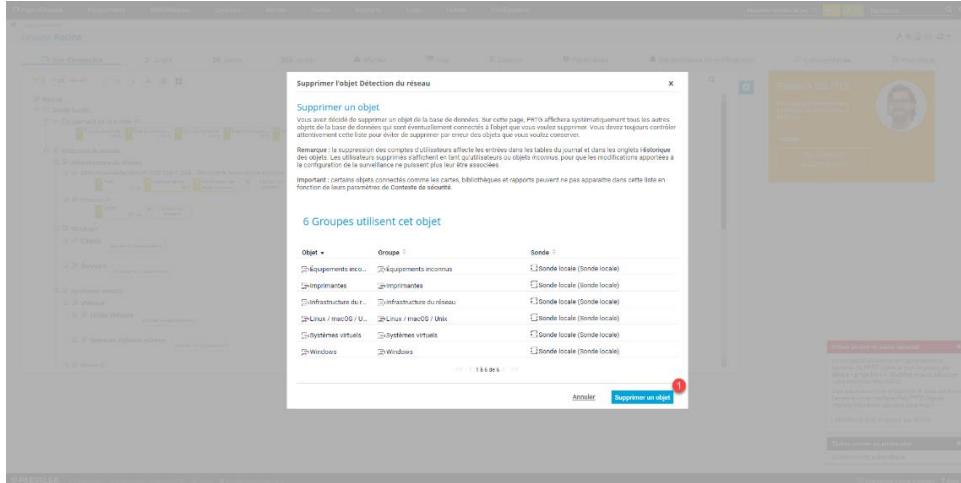


Cette première vue affiche, l'ensemble des équipements disponible dans PRTG.

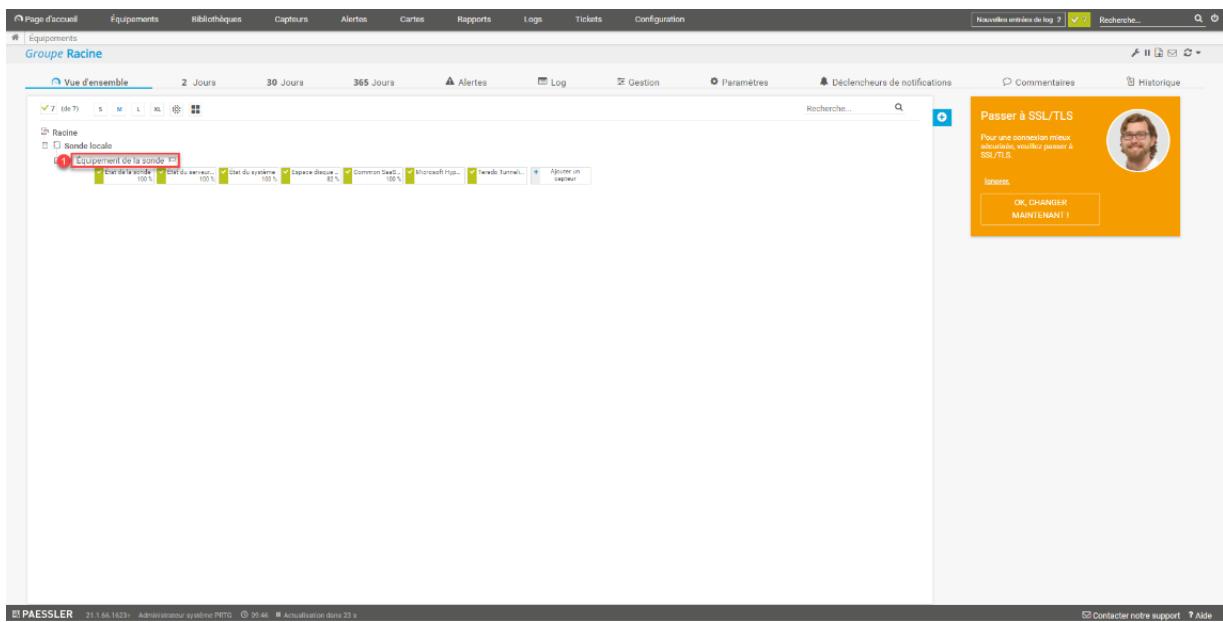
Par défaut, on peut voir que PRTG à créer un groupe Détection automatique **1** dans lequel il a rangé les équipements qu'il a découverts.



Personnellement, je n'utilise jamais la découverte automatique d'équipement de PRTG, pour supprimer le groupe, faire un clic droit dessus et cliquer sur Supprimer **1**.



Confirmer la suppression de groupe et des objets en cliquant sur le bouton Supprimer un objet **1**.



Maintenant ce que vous pouvez également faire (pour ma part, je procède ainsi), c'est de supprimer les capteurs « inutile » sur Équipement de la sonde. Par défaut plusieurs capteurs sont créé.

Pour aller sur la vue détaillée de l'équipement, cliquer sur son nom **1**.

Selectionner tous les capteurs **1** sauf les 3 premiers, qui ne peuvent être supprimés et cliquer sur l'icône de suppression **2**.

Confirmer la suppression des capteurs sélectionnés en cliquant sur le bouton Supprimer les objets **1**.

Figure 67 : PRTG / Prise en main de PRTG

Utiliser PRTG

Maintenant que l'on est familiarisé avec PRTG, je vais vous expliquer comment mettre en supervision des équipements, pour ce tutoriel, je vais utiliser deux serveurs Web Linux et je vais utiliser le 1er serveur comme modèle.

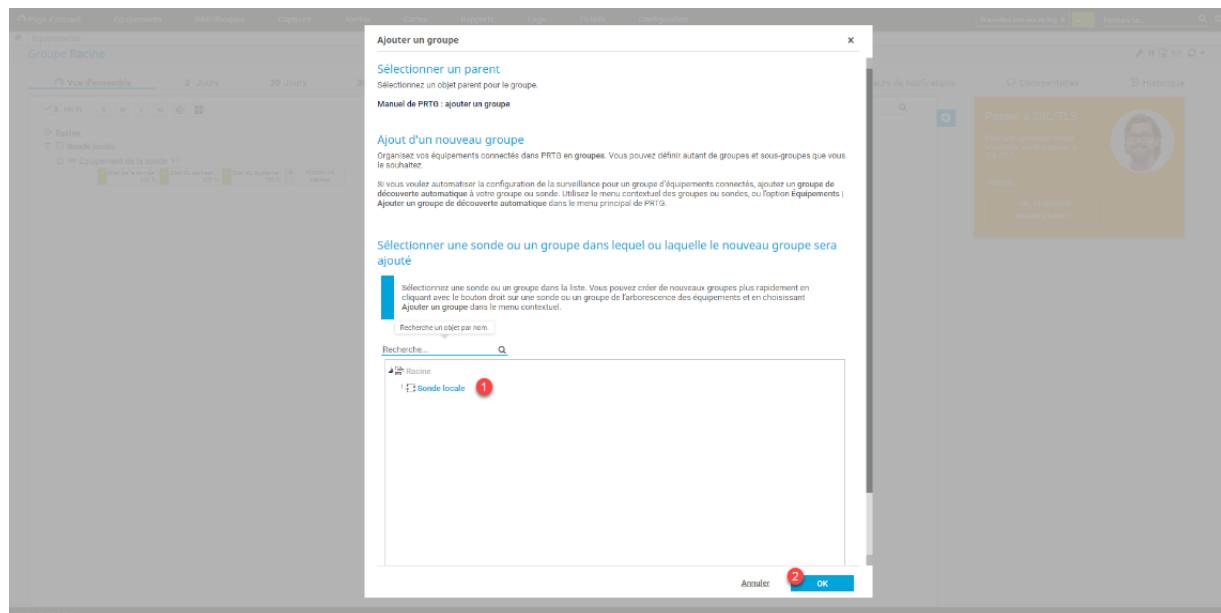
Sur les serveurs, le service SNMP est déjà installé et configuré.

Créer un groupe d'équipement

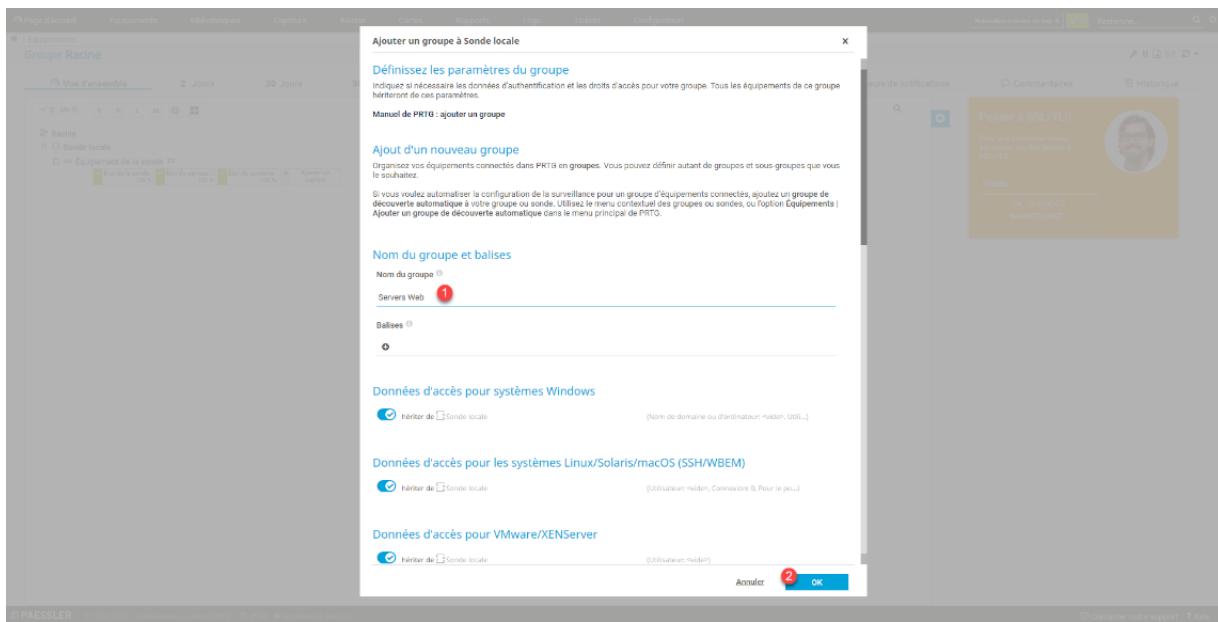
Avant de créer les équipements, je vais créer un groupe, un groupe à plusieurs utilités :

- Organiser les équipements
- Configurer des paramètres qui peuvent être hérités

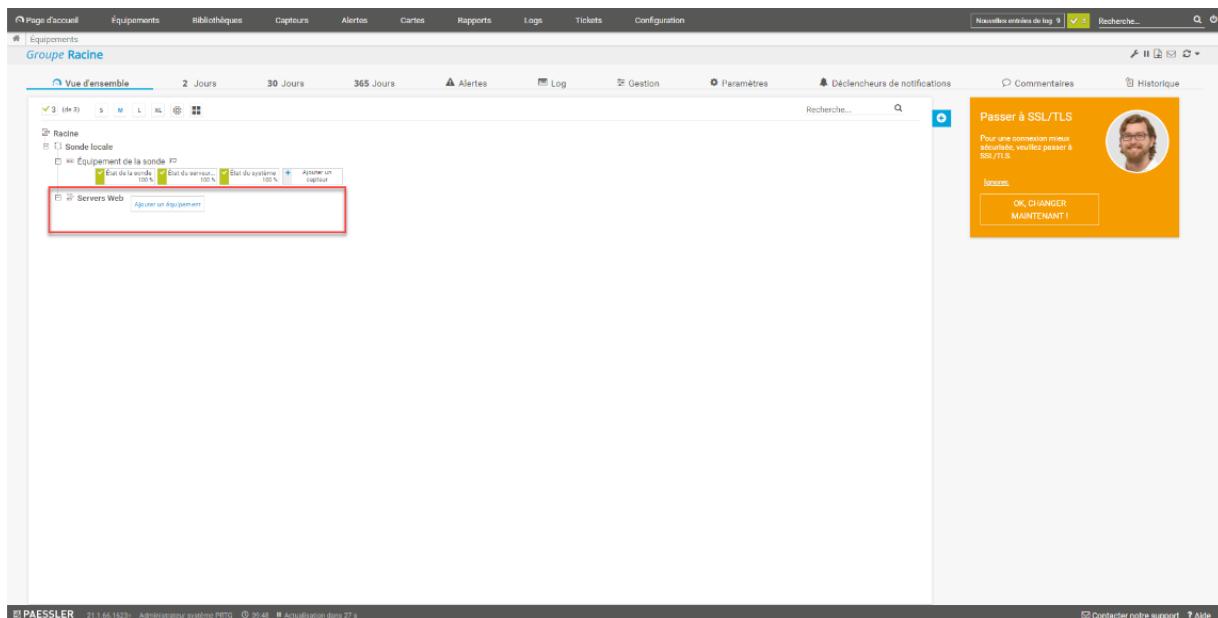
Depuis la vue d'ensemble, cliquer sur le bouton + 1 qui se trouve sur la droite de l'encart centrale puis cliquer sur Ajouter un groupe 2.



Sélectionner son emplacement 1 et cliquer sur OK 2.



Nommer le groupe **1** et cliquer sur OK **2**.

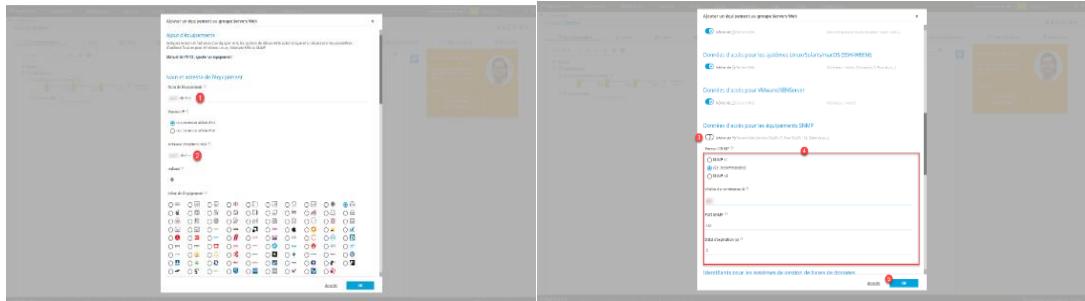


Le groupe est créé et visible depuis la vue d'ensemble.

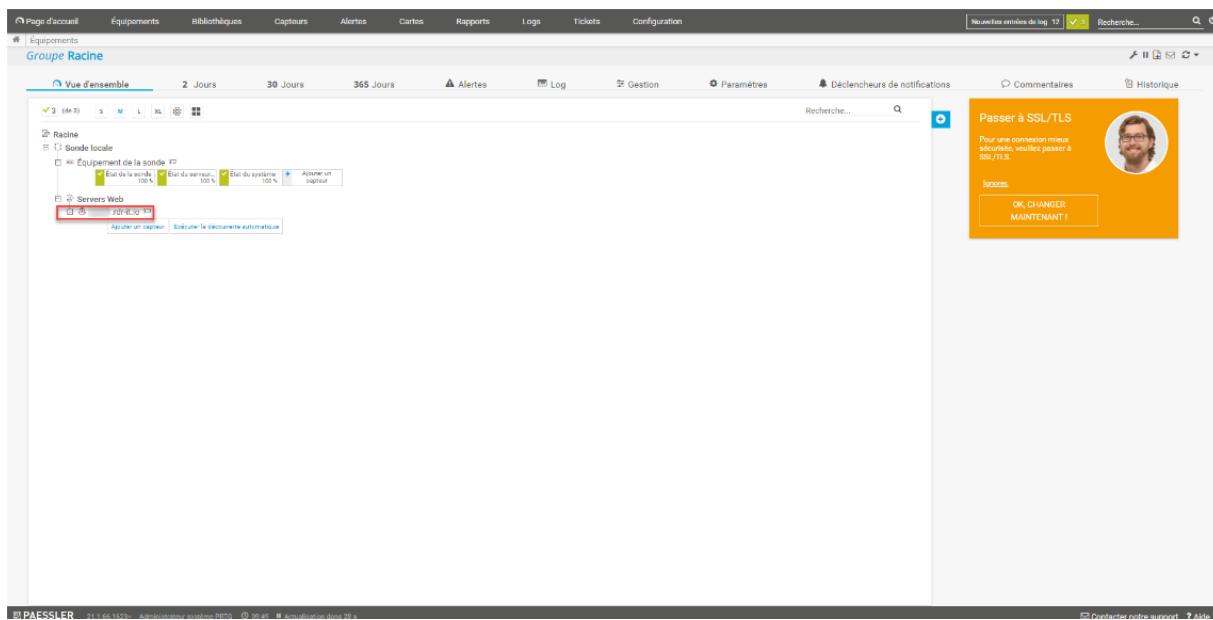
Ajouter un équipement

Je vais maintenant vous montrer comment ajouter un équipement, pour rappel dans le tutoriel je vais configurer un serveur linux qui est sous Ubuntu avec le service SNMP.

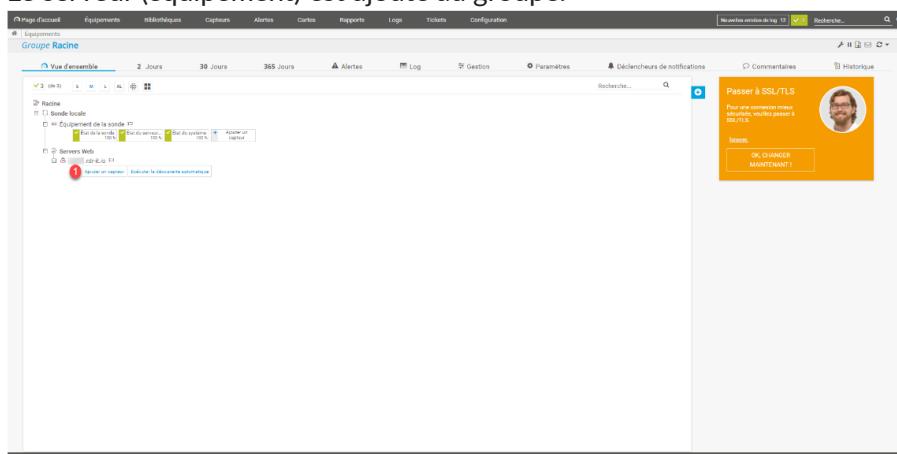
Depuis la vue d'ensemble, cliquer sur Ajouter un équipement **1**.



Commencer par nommer l'équipement **1**, ensuite ajouter son nom DNS ou son adresse **2**. Plus bas dans la configuration, décocher hériter de **3**, configurer la communauté SNMP **4** et cliquer sur OK **5** pour créer l'équipement.



Le serveur (équipement) est ajouté au groupe.



Ajouter des capteurs à un équipement

Maintenant que l'équipement est ajouté, nous allons voir comment ajouter des capteurs à celui-ci. Dans ce tutoriel, je vais vous montrer les capteurs standard que l'on peut configurer sur un serveur (Ping, CPU, RAM ...).

Figure 68 : PRTG / Utiliser PRTG

Capteur ping

Ce capteur envoie un ou plusieurs pings afin de savoir si l'équipement est en ligne.

Depuis la vue d'ensemble, cliquer sur le bouton Ajouter un capteur disponible **1** disponible au niveau de l'équipement.

The screenshot shows the 'Ajouter un capteur à l'équipement' (Add sensor to device) configuration page. In the search bar, the word 'ping' is typed, highlighted by a red circle labeled '1'. Below the search bar, a list of available sensors is shown, with the 'Ping' sensor highlighted by a red circle labeled '2'. The 'Ping' sensor card provides a brief description: 'Surveille la connectivité en utilisant PING'. The page also includes sections for monitoring types, target system types, and technologies used.

Dans la zone de recherche, entrer ping **1** puis cliquer sur le capteur ping **2**.

The screenshot shows the 'Paramètres de base du capteur' (Sensor base settings) configuration page. The 'Nom du capteur' (Sensor name) field is set to 'Ping', highlighted by a red box and a red arrow pointing to a red circle labeled '1'. At the bottom right of the page, there is a 'Créer' (Create) button, which is also highlighted by a red box and a red arrow pointing to a red circle labeled '2'.

Configurer le capteur en fonction de vos besoins **1** et cliquer sur le bouton Créer **2**.

Le capteur est ajouté, celui est pour le moment en « inconnu » car aucun ping a été effectué.

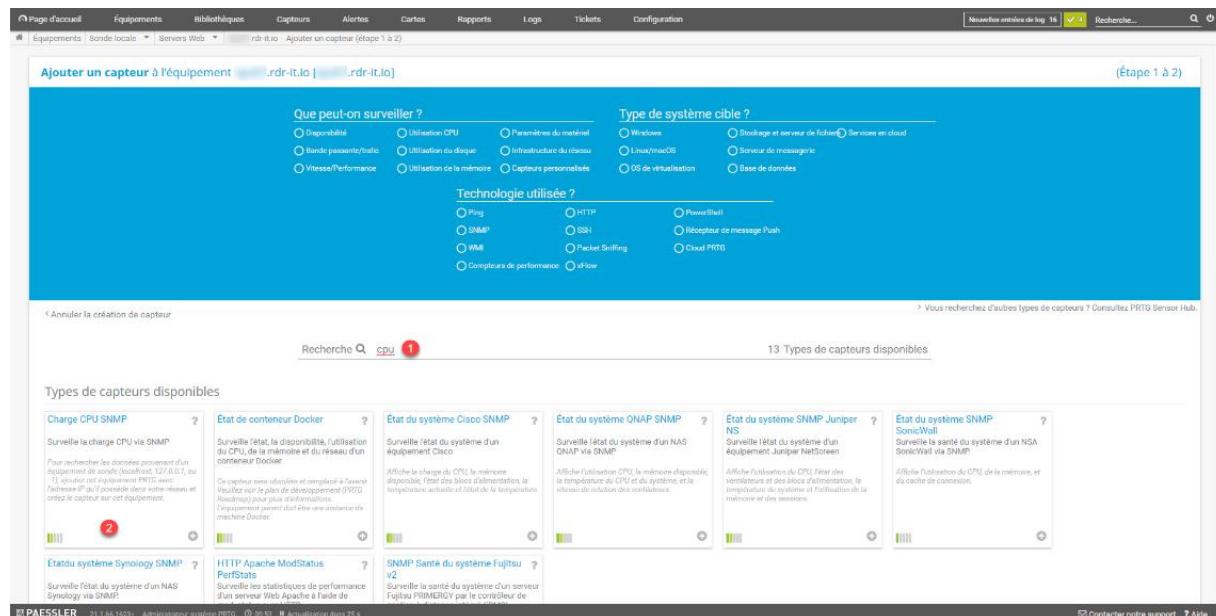
Au bout de quelques minutes (2/3), le capteur doit passer au vert, s'il arrive à effectuer un ping sur l'équipement.

Figure 69 : PRTG / Capteur Ping

Capteur : CPU SNMP

Ce capteur va permettre de connaitre la charge CPU de l'équipement.

Depuis la vue d'ensemble de l'équipement, cliquer le bouton + 1 puis sur Ajouter un capteur 2.

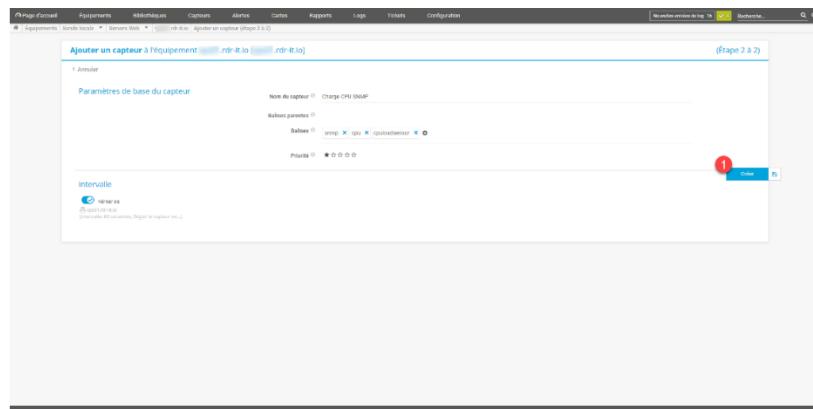


The screenshot shows the 'Ajouter un capteur à l'équipement' (Add Sensor to Device) dialog in PRTG. It's divided into four main sections:

- Que peut-on surveiller ?**: Options include Disponibilité, Bande passante/traffic, Vitesse/Performance, Utilisation CPU, Utilisation du disque, Utilisation de la mémoire, Paramètres du matériel, Infrastructure du réseau, Captures personnalisées.
- Type de système cible ?**: Options include Windows, Linux/macOS, OS de virtualisation, Stockage et serveur de fichiers, Serveur en cloud, Serveur de messagerie, Base de données.
- Technologie utilisée ?**: Options include Ping, SNMP, WMI, Générateurs de performance, HTTP, SSH, Packet Sniffing, vFlow, PowerShell, Récepteur de message Push, Cloud PRTG.
- Types de capteurs disponibles**: A list of available sensors, with 'Charge CPU SNMP' highlighted with a red circle.

A search bar at the top right contains the text 'cpu' with a red circle around it. The bottom of the dialog shows a note: 'Vous recherchez d'autres types de capteurs ? Consultez PRTG Sensor Hub.'

Dans la zone de recherche de capteur, saisir cpu 1 et sélectionner le capteur Charge CPU SNMP 2.



The screenshot shows the 'Ajouter un capteur à l'équipement' dialog with the following details:

- Paramètres de base du capteur**:
 - Nom du capteur: Charge CPU SNMP
 - Sous-système: snmp x cpu x personnalisé x
 - Période: 10s
- Intervalle**:
 - interval
 - Pour une collecte toutes les 10 secondes, cliquer le bouton "Créer".

A red circle is around the 'Créer' button in the interval section.

Le capteur Charge CPU SNMP n'a pas de paramètre de personnalisation, on peut seulement agir sur l'intervalle, cliquer sur le bouton Créer 1.

Maintenant le capteur est ajouté, patienter le temps que le serveur PRTG effectue la requête SNMP

Au bout de quelques minutes, si la communauté SNMP est correctement configurée, le capteur passe au vert.

En cliquant sur le nom du capteur, une vue détaillé de celui-ci s'affiche.

Dans le détail, on peut voir que chaque processeur est remonté et qu'un canal somme est disponible, attention : le nom est trompeur, il affiche la moyenne des processeurs et non le cumul des processeurs individuels.

The screenshot shows the PRTG Network Monitor interface with the following details:

- Page d'accueil**: The main dashboard view.
- Équipements**: Equipment management section.
- Bibliothèques**: Library section.
- Capteurs**: Sensors section.
- Alertes**: Alerts section.
- Cards**: Cards section.
- Rapports**: Reports section.
- Logs**: Logs section.
- Tickets**: Tickets section.
- Configuration**: Configuration section.
- Technologie utilisée ?**: Technology used dropdown menu.
- Recherche**: Search bar with the query "mémoire".
- 16 Types de capteurs disponibles**: 16 types of sensors available.
- Types de capteurs disponibles**: List of sensor types:
 - Contrôleur de mémoire HPE**: Monitors memory controller in an HPE server.
 - Etat de conteneur Docker**: Monitors Docker container status.
 - Etat du système Cisco SNMP**: Monitors Cisco system via SNMP.
 - Etat du système QNAP SNMP**: Monitors QNAP NAS system via SNMP.
 - Etat du système Juniper NS**: Monitors Juniper NS system health.
 - Etat du système Juniper Juniper**: Monitors Juniper Juniper system health.
 - Etat du système SNMP v2**: Monitors system via SNMP v2.
 - Étatu système Synology SNMP**: Monitors Synology system via SNMP.
 - Info sur la mémoire SNMP Linux**: Monitors memory usage in a Linux system via SNMP.
 - Mémoire physique IBM System X**: Monitors physical memory in an IBM System X server.
 - Mémoire SNMP**: Monitors memory usage via SNMP.
 - SNMP Santé du système Fujitsu v2**: Monitors Fujitsu PRIMERGY system health via SNMP v2.
- PAESSLER**: Company logo.
- 21.1.66.162**: IP address.
- Administrateur système PRTG**: User name.
- 96/85**: Alert level.
- Actualisation tous 15 s**: Refresh rate.
- Contacter notre support**: Contact support link.

Figure 70 : PRTG / Capteur CPU

Capteur mémoire

Le capteur mémoire permet d'avoir un retour sur le mémoire disponible, certaine application comme des serveurs de bases de données vont utiliser toute la mémoire disponible.

Dans la zone de recherche d'ajout d'un nouveau capteur, entrer mémoire **1** et choisir Mémoire SNMP **2**.

The screenshot shows the configuration of a new sensor for memory usage:

- Ajouter un capteur à l'équipement**: Add a sensor to the equipment.
- Étape 2 à 2**: Step 2 of 2.
- Paramètres de base du capteur**: Basic sensor settings.
- Balises**: Tags: `inopérant`, `memory`, `mémoire`, `empty`.
- paramétrage**: Configuration:
 - Type de mémoire**: Physical Memory, Virtual Memory, Swap Space.
 - intervalle**: Interval: 15 minutes.
 - 30 une réponse du capteur déclenche**: 30 responses trigger an alert.
- Créer**: Create button.

En fonction de ce que l'on souhaite sélectionner la types de mémoire **1** (généralement mémoire Physique même pour une vm), configurer l'intervalle **2** (toutes les 60 sec n'a pas d'intérêt) et cliquer sur le bouton Créer **3**.

Le capteur est ajouté, patienter pendant sa première interrogation ...

Une fois le capteur fonctionnel, voici le type d'information qu'il retourne :

Figure 71 : PRTG / Capteur mémoire

Espace disque

Rechercher disque **1** et choisir le capteur Espace disque disponible SNMP **2**.

Selectionner le ou les disques à superviser **1**, configurer l'intervalle **2** et cliquer sur OK **3**.

Le capteur est ajouté.

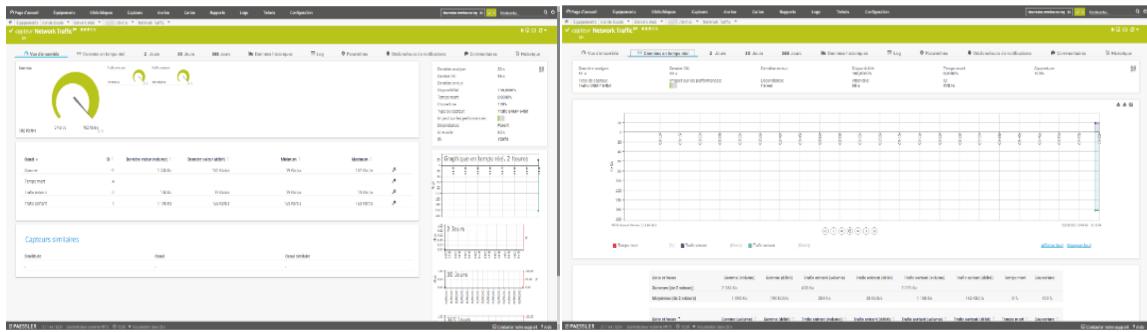
Figure 72 : PRTG / Capteur Espace disque

Traffic réseau / carte réseau

Ce capteur permet d'avoir supervision du trafic réseau sur une carte.

Dans le champ recherche, entrer **trafic** 1 et cliquer sur le capteur **Traffic SNMP** 2.

Selectionner la ou les cartes réseaux à superviser 1, dans la partie affichage du capteur, sélectionner l'option Afficher le trafic entrant et sortant sous la forme d'une graphique en aires positifs et négatifs 2 puis cliquer sur le bouton Créer 3.



Voici un aperçu du capteur :

The configuration section of the PRTG configuration page for a NIC is highlighted with a red box. It includes the following settings:

- Types d'unités du canal**: Type de canal: Mo, Unité: Mbit / secon..
- Unités de données**: Octets (bande passante)

Dans les paramètres du capteur, il est possible de modifier les unités de Ko en Mo pour avoir quelque chose de plus parlant.

Figure 73 : PRTG / Capteur carte réseau