DOCUMENTATION

Documentation projet BEG

Réalisé le 05 novembre 2024

Rédigé par : MICHEL Thibaud & ROCHON Guillaume

Révisé par : MICHEL Thibaud & ROCHON Guillaume

Validé par : MICHEL Thibaud & ROCHON Guillaume

Table des matières

INTRODUCTION

Pôle SISL, spécialisé dans la gestion et l'intégration de systèmes d'information, intervient auprès de l'entreprise BEG pour renforcer et moderniser son infrastructure informatique. Notre mission consiste à déployer des services essentiels afin d'optimiser la gestion des utilisateurs, la sécurité des données, et la performance des réseaux.

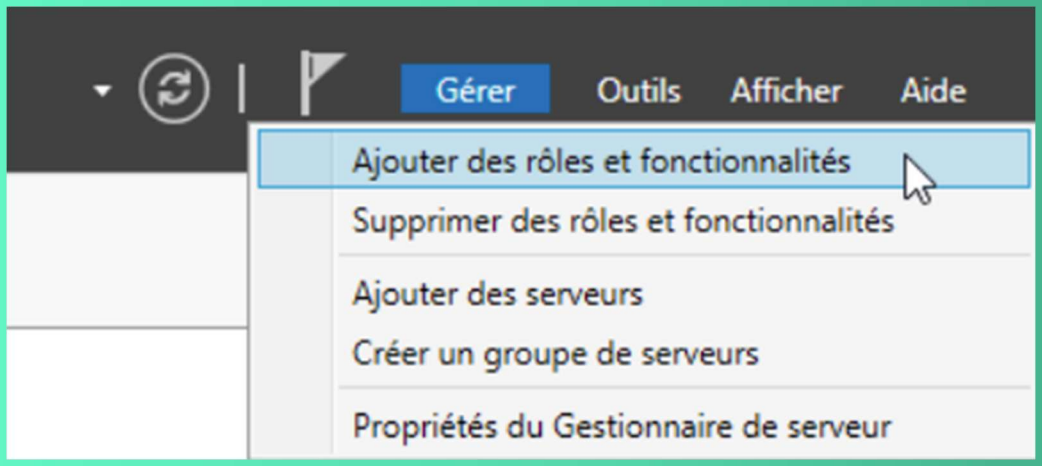
Le projet mené chez BEG couvre plusieurs aspects stratégiques, tels que la configuration d'un Active Directory pour la gestion centralisée des comptes, la mise en place de profils itinérants, la gestion des partages réseau sécurisés, et l'implémentation de services critiques comme les serveurs FTP, pare-feu, et serveurs d'impression.

Cette documentation détaille chaque étape des configurations réalisées, tout en mettant en avant les procédures de sauvegarde et de restauration pour assurer une continuité de service optimale.

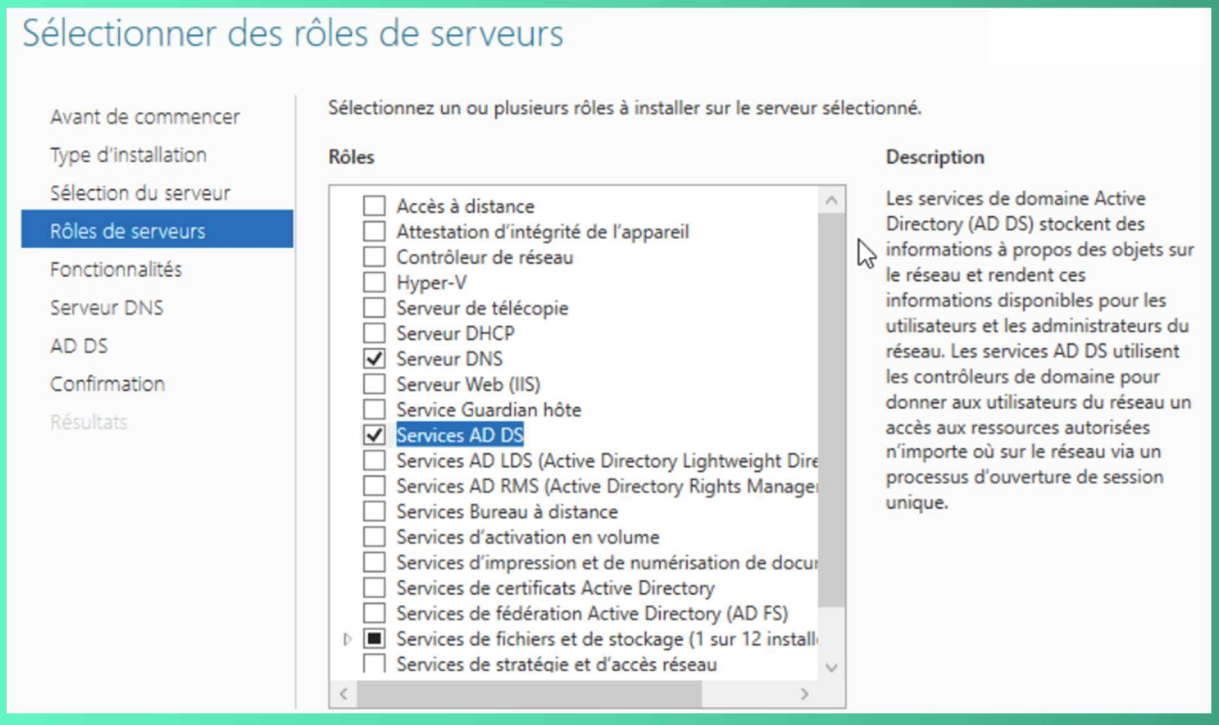
CONFIGURATION D'UN ACTIVE DIRECTORY

Installation du service :

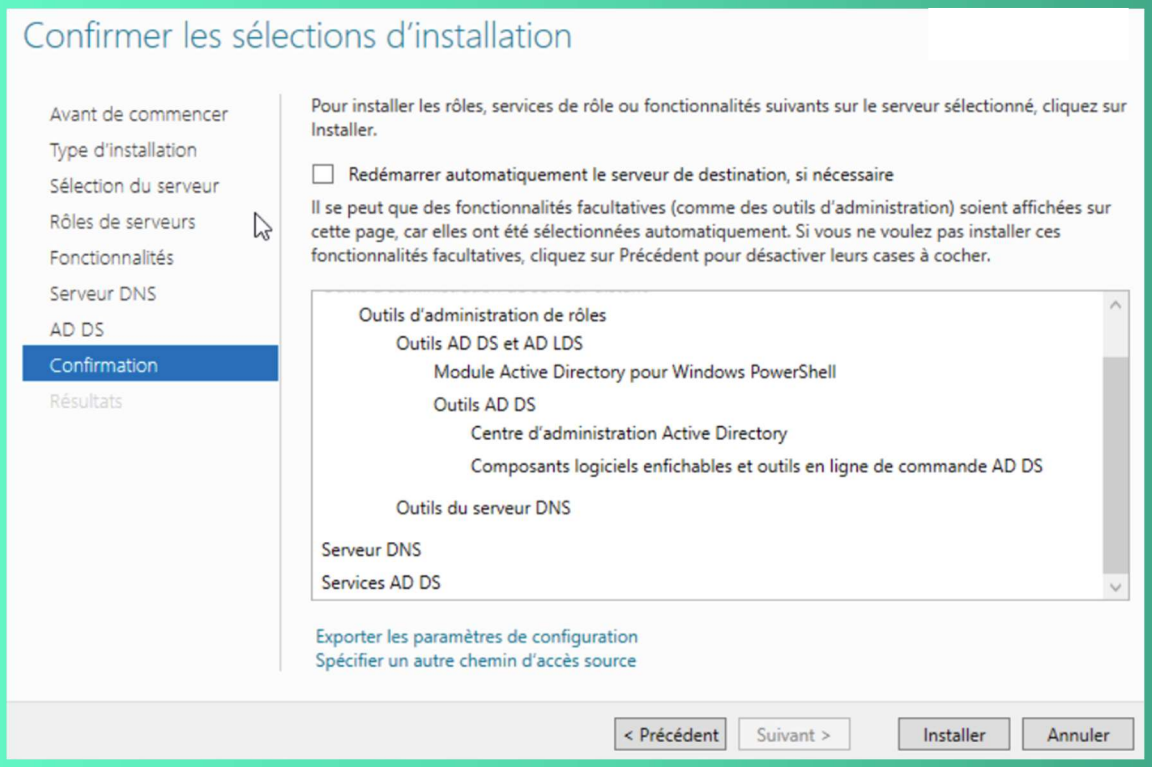
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur 'Gérer' et 'Ajouter des rôles et fonctionnalités'.



Dans l'onglet 'Rôles de serveurs', cocher 'Serveur DNS' et 'Services AD DS'

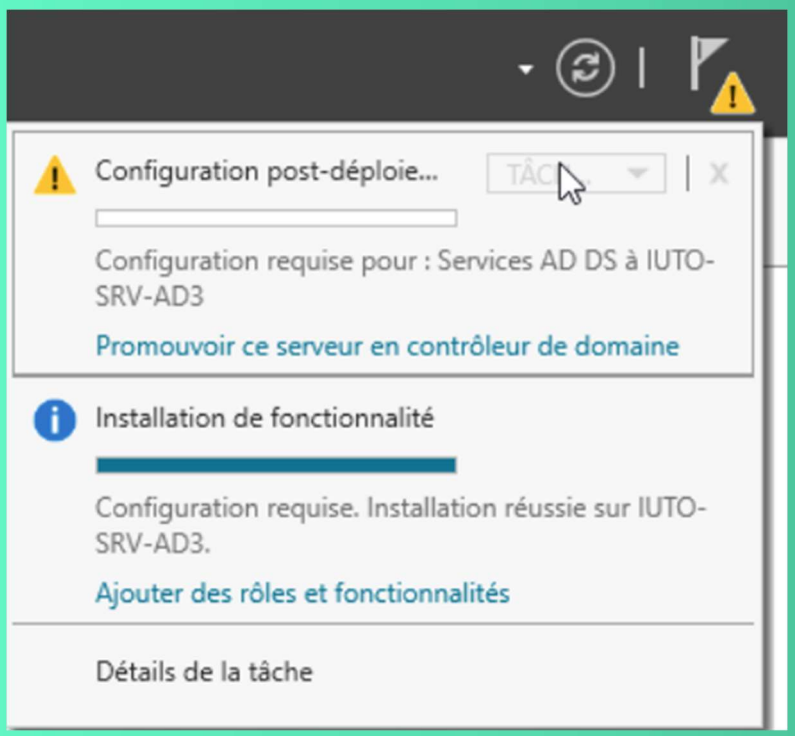


Dans l'onglet 'Confirmation', installer les services



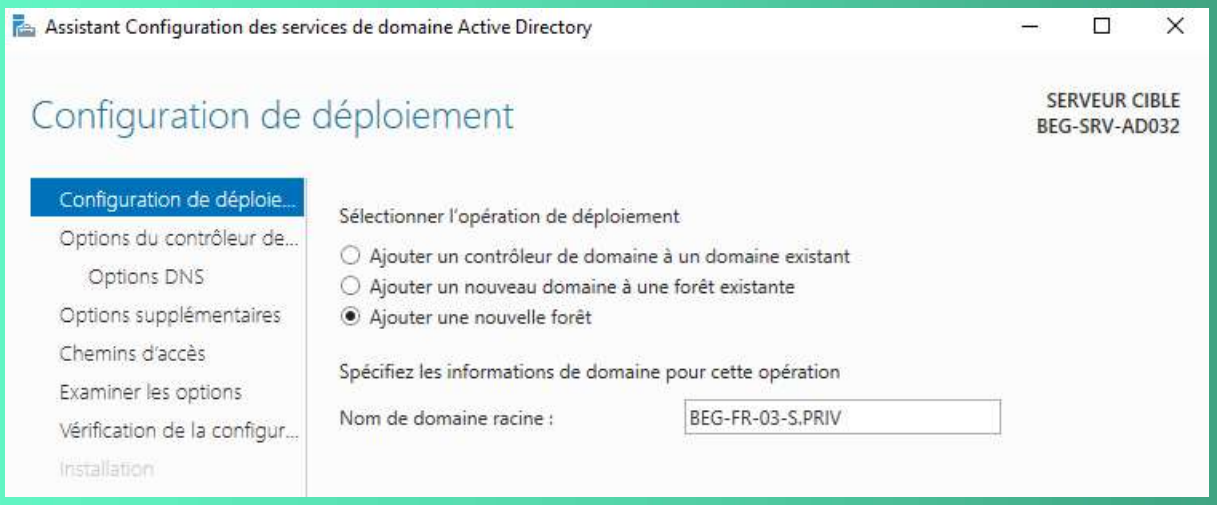
Promouvoir l'AD en tant que contrôleur de domaine :

Pour promouvoir l'AD en tant que contrôleur de domaine, il faut cliquer sur le drapeau en haut et cliquer sur 'Promouvoir ce serveur en contrôleur de domaine'.

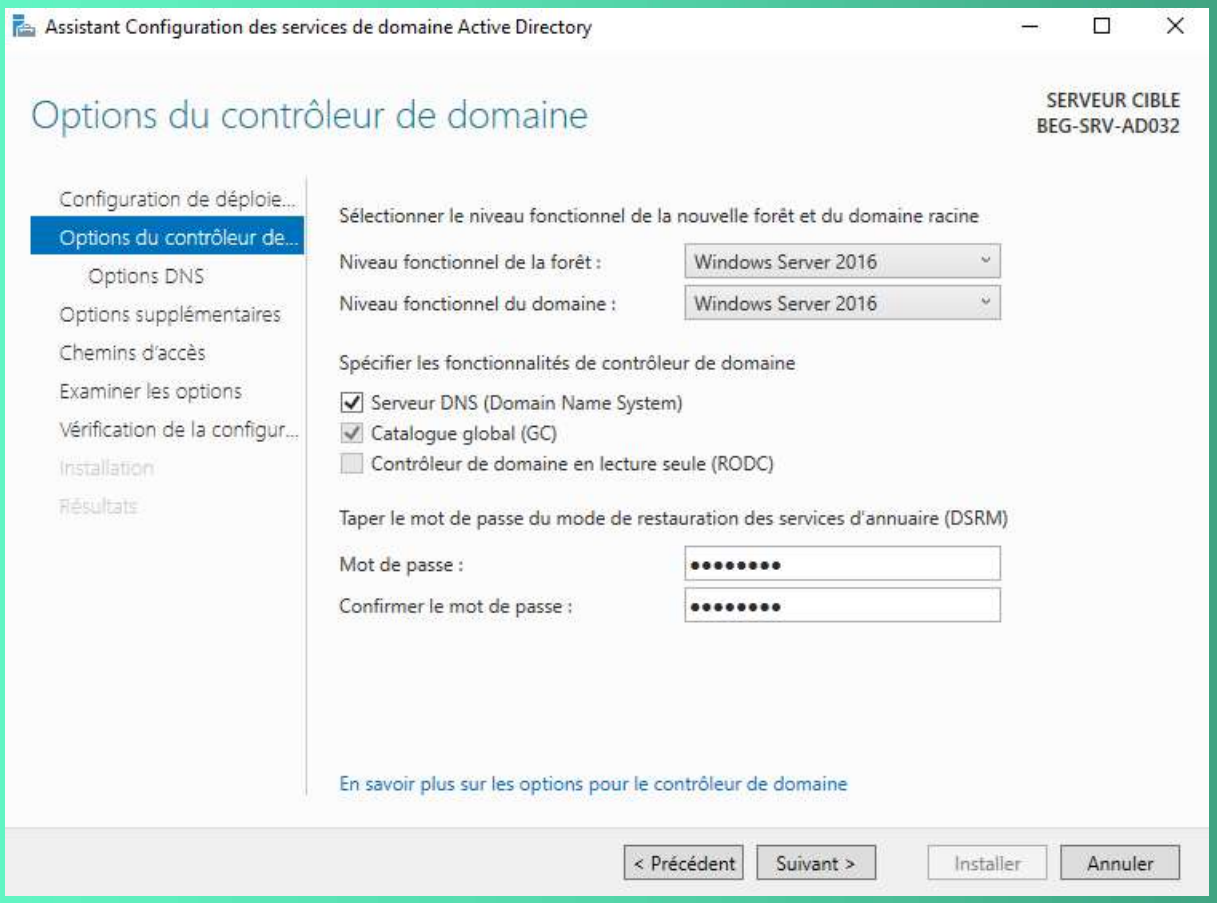


Configuration du contrôleur de domaine :

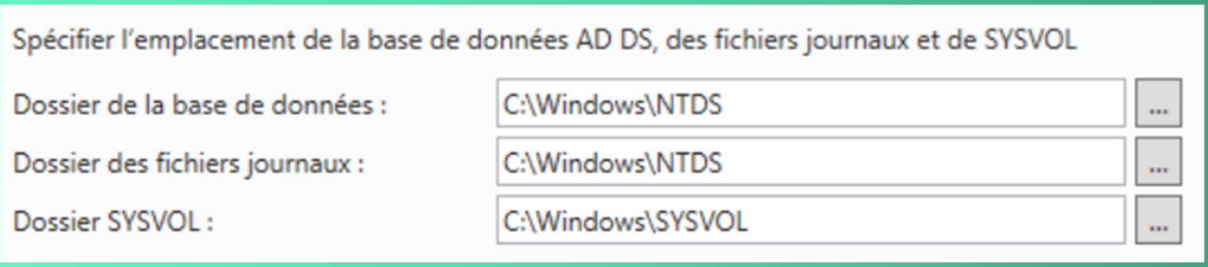
Il faut commencer par créer une nouvelle forêt et lui donner un nom qui sera le nom de domaines



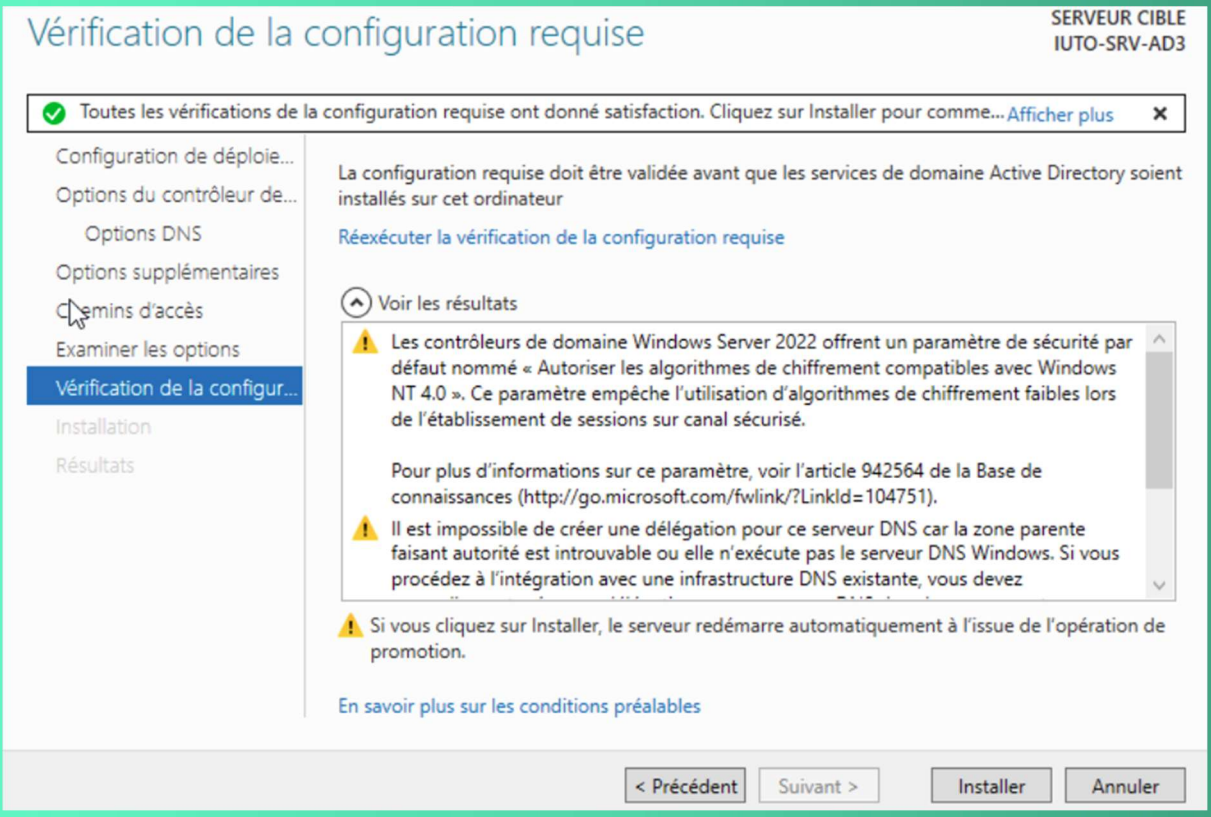
Ne pas modifier le niveau fonctionnel de la forêt et du domaine puis taper le mot de passe du mode de restauration des services d'annuaire (DSRM)



Ne pas modifier les chemins d'accès



Installation de la configuration contrôleur de domaine



Script :

Script réalisé pour ajouter tous les étudiants dans l'AD

```
$CSVFile = "C:\Users\Administrateur\Desktop\Resultats.csv"

# Importer les données du fichier CSV
$CSVData = Import-Csv -Path $CSVFile -Delimiter ";" -Encoding UTF8

# Boucle à travers chaque utilisateur dans les données CSV
foreach ($Utilisateur in $CSVData) {
   # Récupérer les informations de l'utilisateur
   $UtilisateurPrenom = $Utilisateur.FirstName
   $UtilisateurNom = $Utilisateur.LastName
   $UtilisateurLogin = ($UtilisateurPrenom.Substring(0, 2) + $UtilisateurNom).ToLower()
   $UtilisateurEmail = "$UtilisateurLogin@BEG.fr"
   $UtilisateurMotDePasse = $Utilisateur.Password
   $UtilisateurFonction = $Utilisateur.Fonction  # Pas de colonne Fonction dans le CSV
```

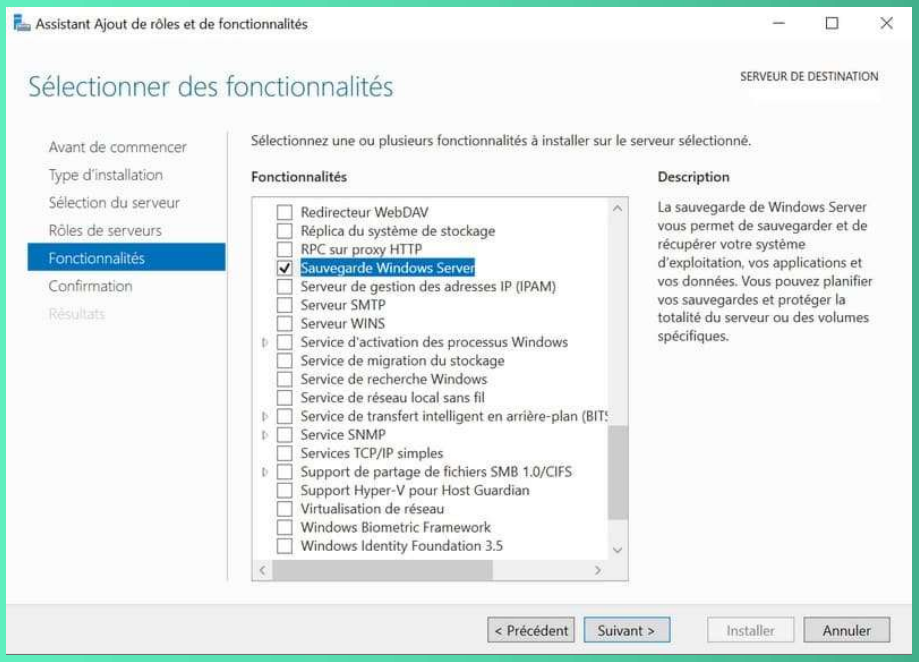
```
    # Validation des valeurs
    if ([string]::IsNullOrWhiteSpace($UtilisateurPrenom) -or
        [string]::IsNullOrWhiteSpace($UtilisateurNom) -or
        [string]::IsNullOrWhiteSpace($UtilisateurLogin) -or
        [string]::IsNullOrWhiteSpace($UtilisateurMotDePasse)) {
        Write-Warning "Les données sont manquantes pour l'utilisateur $UtilisateurLogin. L'utilisateur ne sera pas créé."
        continue
    }

    # Vérifier si l'utilisateur existe déjà
    if (Get-ADUser -Filter { SamAccountName -eq $UtilisateurLogin }) {
        Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
    } else {
        try {
            # Créer un nouvel utilisateur dans Active Directory
            New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
                       -DisplayName "$UtilisateurNom $UtilisateurPrenom" `
                       -GivenName $UtilisateurPrenom `
                       -Surname $UtilisateurNom `
                       -SamAccountName $UtilisateurLogin `
                       -UserPrincipalName "$UtilisateurLogin@BEG-FR-03-S.PRIV" `
                       -EmailAddress $UtilisateurEmail `
                       -Title $UtilisateurFonction `
                       -Path "OU=BEG-FR,DC=BEG-FR-03-S,DC=PRIV" `
                       -AccountPassword (ConvertTo-SecureString -AsPlainText -Force $UtilisateurMotDePasse) `
                                        -Enabled $true `
                                        -PasswordNeverExpires $true `
                       -CannotChangePassword $true
            Write-Output "Création de l'utilisateur : $UtilisateurLogin ($UtilisateurNom $UtilisateurPrenom)"
        } catch {
            Write-Error "Erreur lors de la création de l'utilisateur $UtilisateurLogin : $_"
        }
    }
}
```

SAUVEGARDE DE L'AD

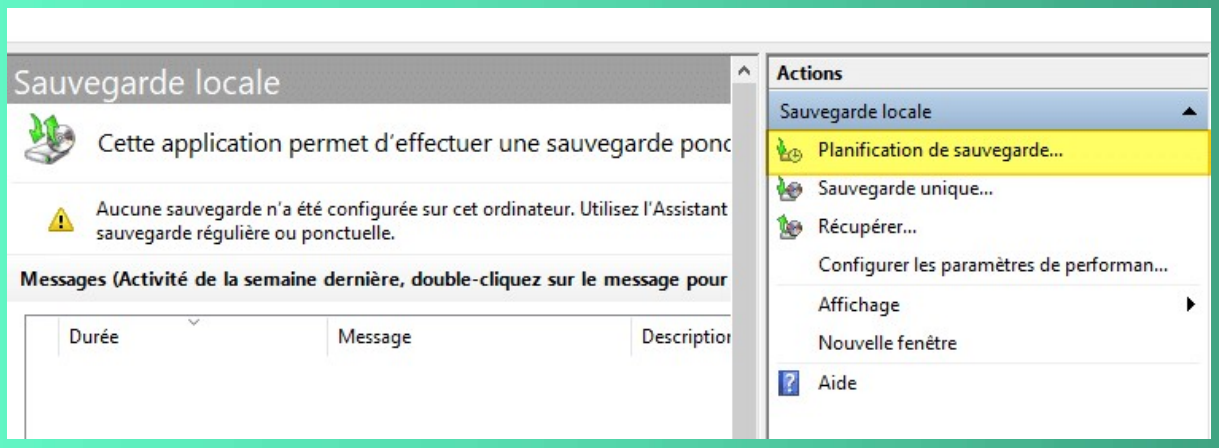
Installation du service :

Pour installer Windows Server Backup, nous avons l'embarras du choix comme bien souvent... En mode graphique, voici ce qu'il faut choisir :



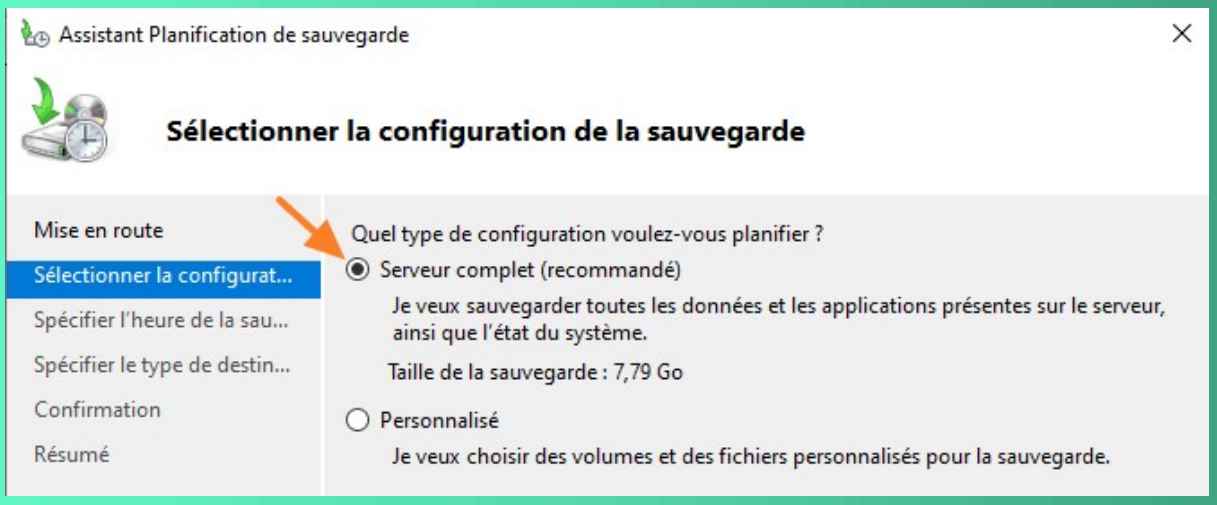
Sauvegarde de l'AD avec Windows Server Backup :

Commençons par cliquer sur "Planification de sauvegarde" en haut à droite.

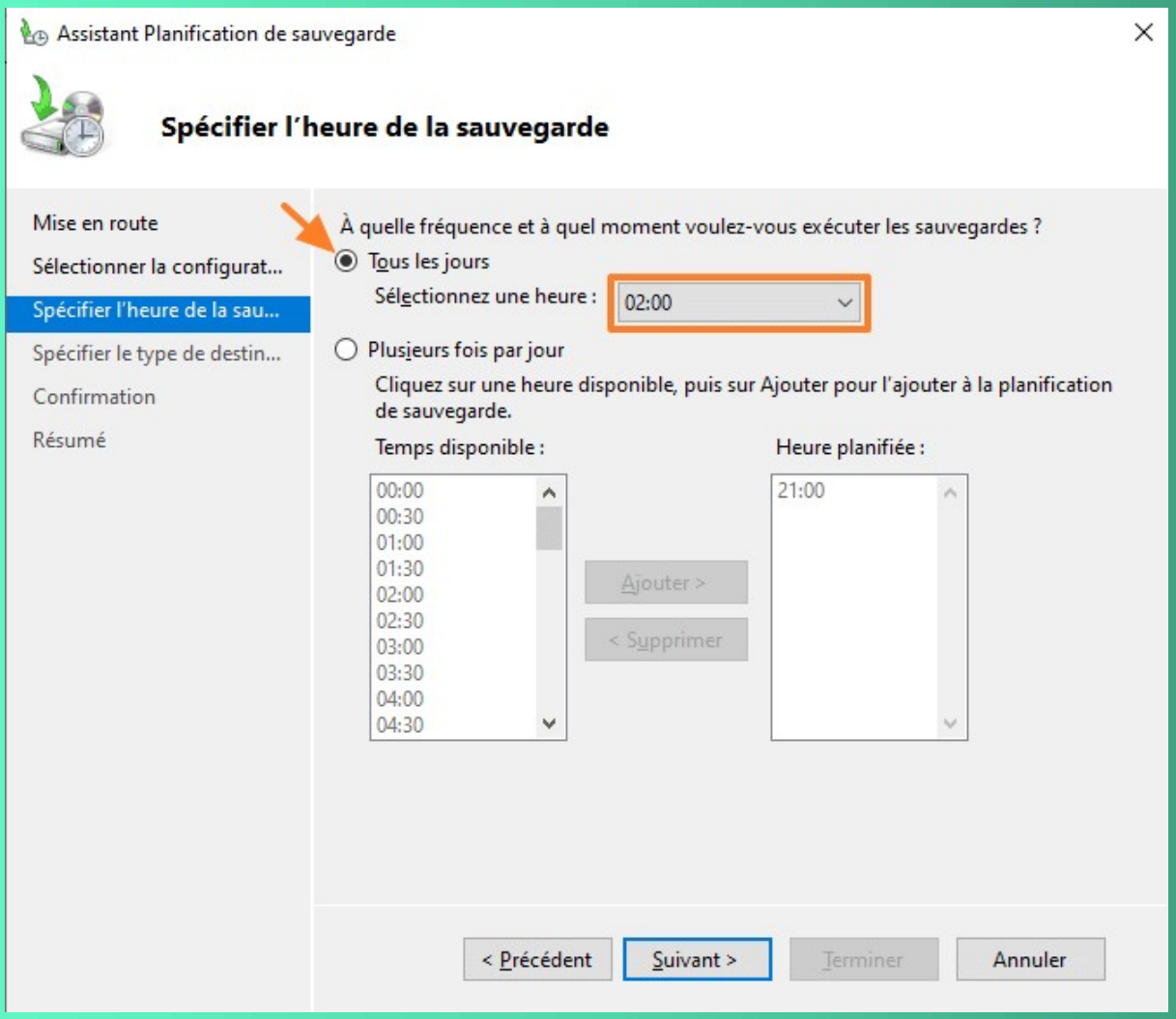


Poursuivons en cliquant sur "Suivant".

L'étape "Sélectionner la configuration de la sauvegarde" apparaît. On sélectionne "Serveur complet (recommandé)".

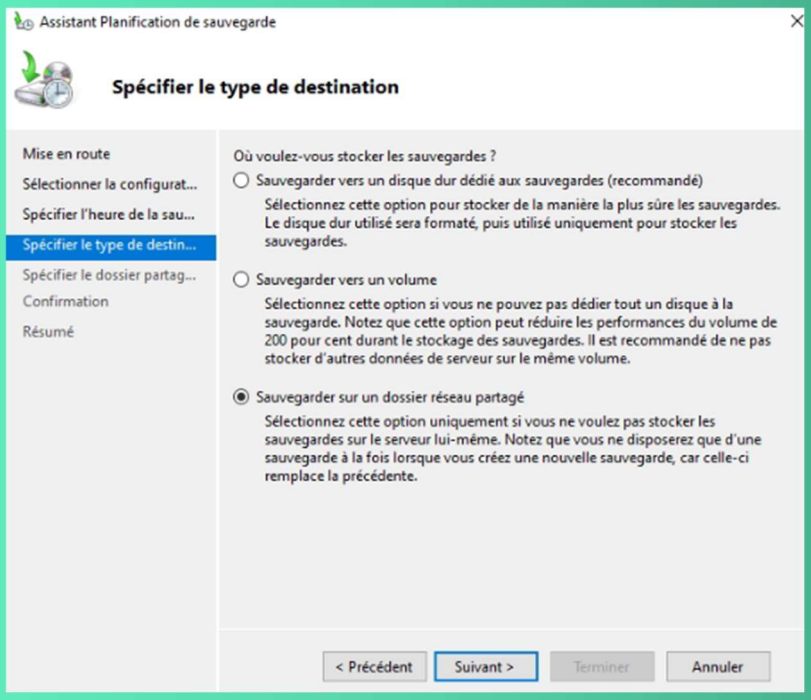


Ensuite, l'heure et la fréquence de la sauvegarde doivent être définit. Dans cet exemple, on sélectionne "Tous les jours" à 02:00.

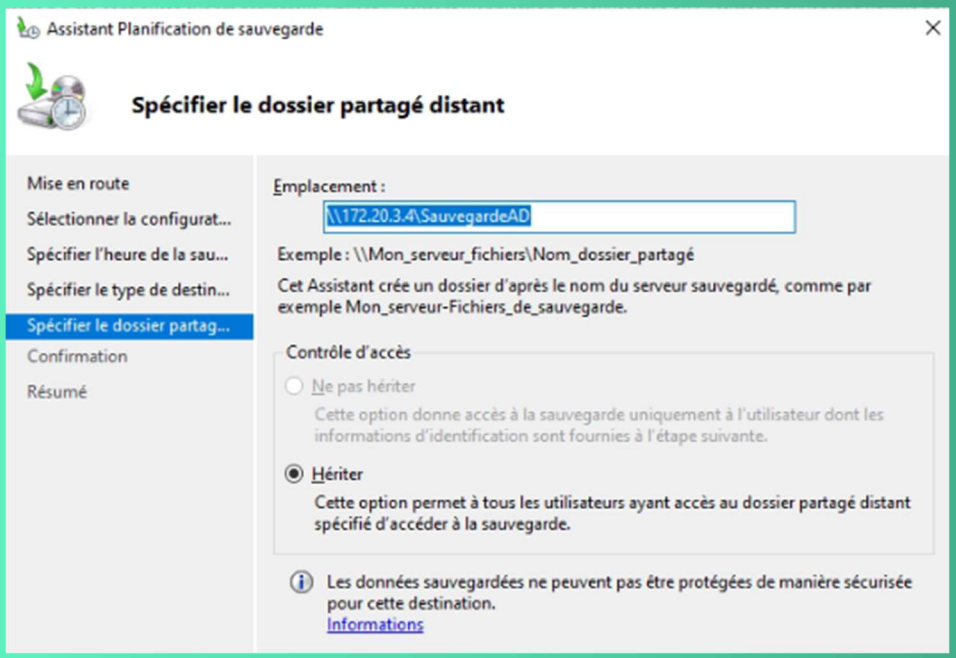


Puis, nous devons choisir la destination de la sauvegarde. Il est recommandé d'utiliser l'option "Sauvegarder vers un disque dur dédié aux sauvegardes". Bien que ça peut être tentant de choisir la dernière option pour stocker la sauvegarde sur un espace partagé (sur un NAS, par exemple), ce

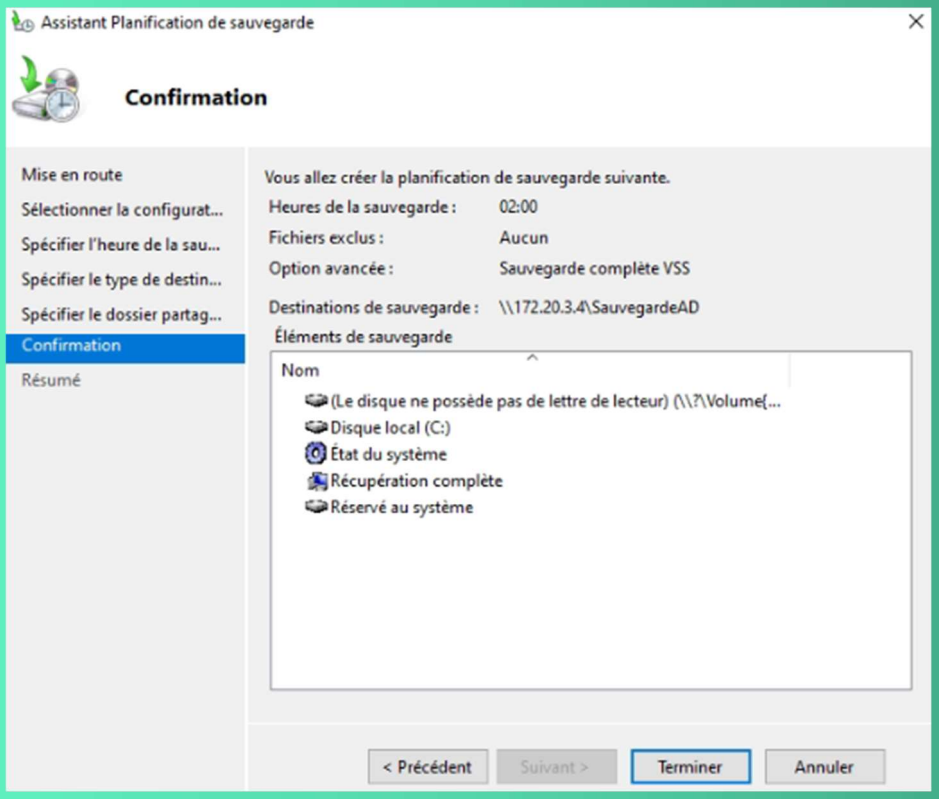
n'est pas recommandé car, avec ce mode, l'outil conserve une seule sauvegarde et il écrase la précédente à chaque fois...!



Ensuite, entrer l'emplacement du fichier partagé



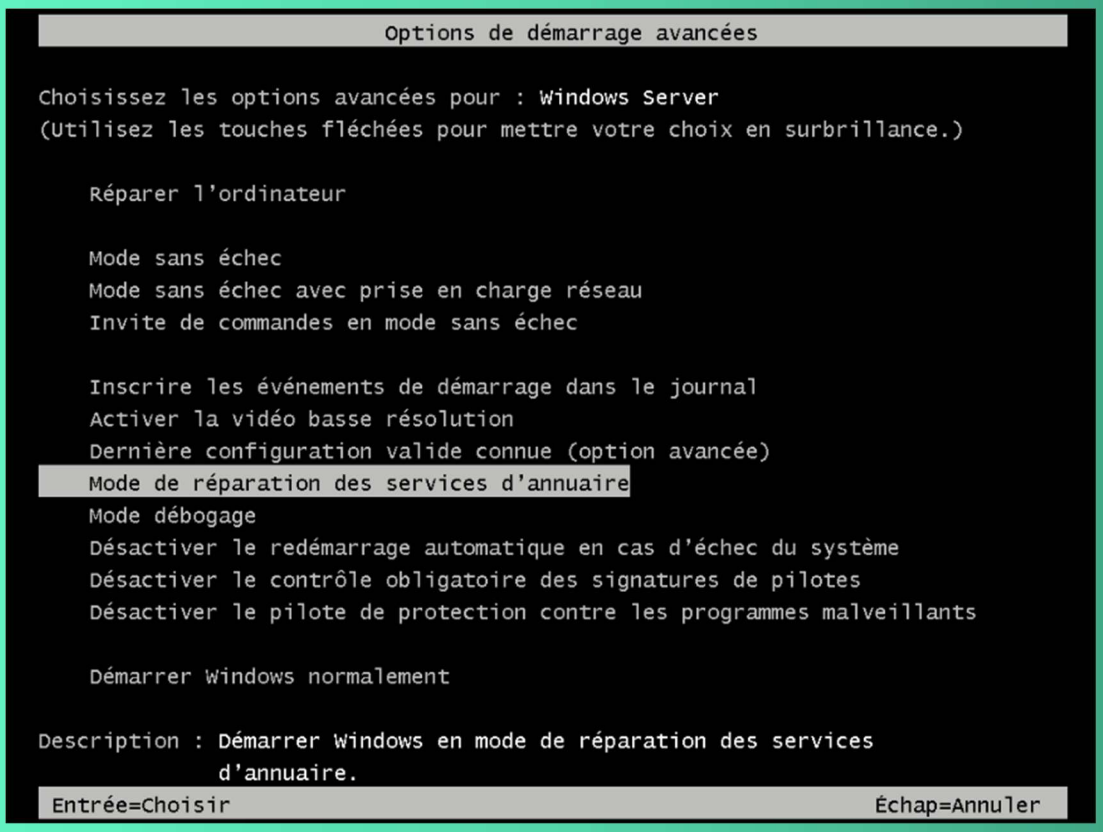
Un résumé s'affiche, cliquons sur "Terminer" pour finaliser la création de la tâche.


Assistant Planification de sauvegarde
Confirmation
Mise en route
Sélectionner la configurat...
Spécifier l'heure de la sau...
Spécifier le type de destin...
Spécifier le dossier partag...
Confirmation
Résumé
Vous allez créer la planification de sauvegarde suivante.
Heures de la sauvegarde : 02:00
Fichiers exclus : Aucun
Option avancée : Sauvegarde complète VSS
Destinations de sauvegarde : \\172.20.3.4\SauvegardeAD
Éléments de sauvegarde
Nom
(Le disque ne possède pas de lettre de lecteur) (\\?\Volume{...
Disque local (C:)
État du système
Récupération complète
Réservé au système
< Précédent
Suivant >
Terminer
Annuler

RESTAURATION DE L'AD

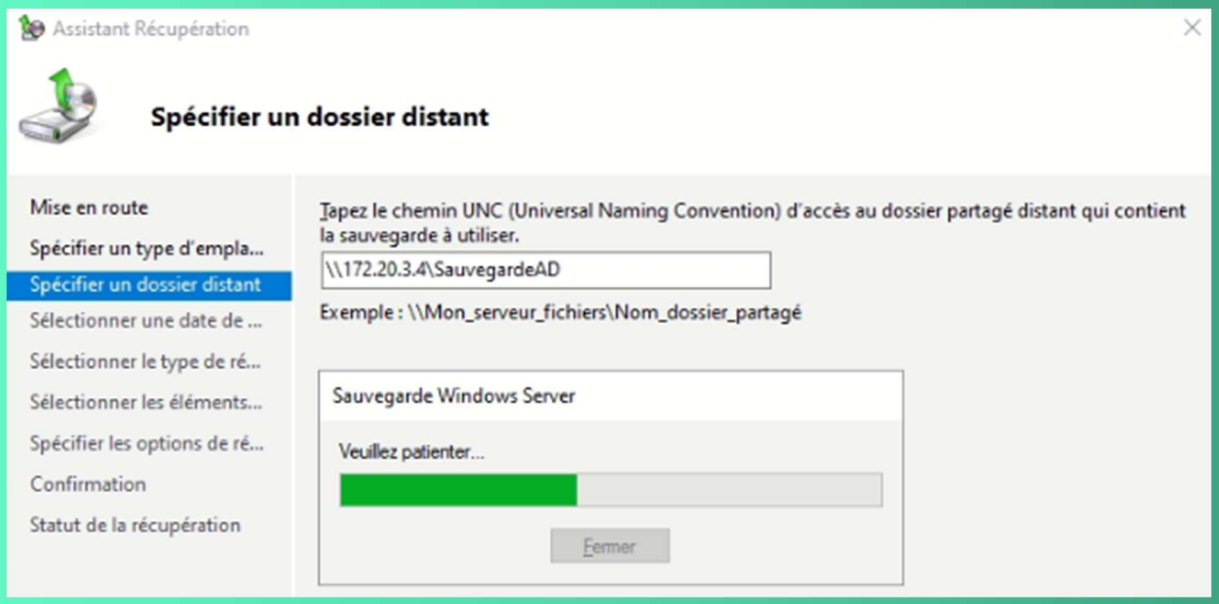
Pour commencer la restauration, démarrer la machine et appuyer sur F8.

Sélectionner 'mode de réparation des services d'annuaire



Ensuite, choisir autre utilisateur et mettre le compte Administrateur

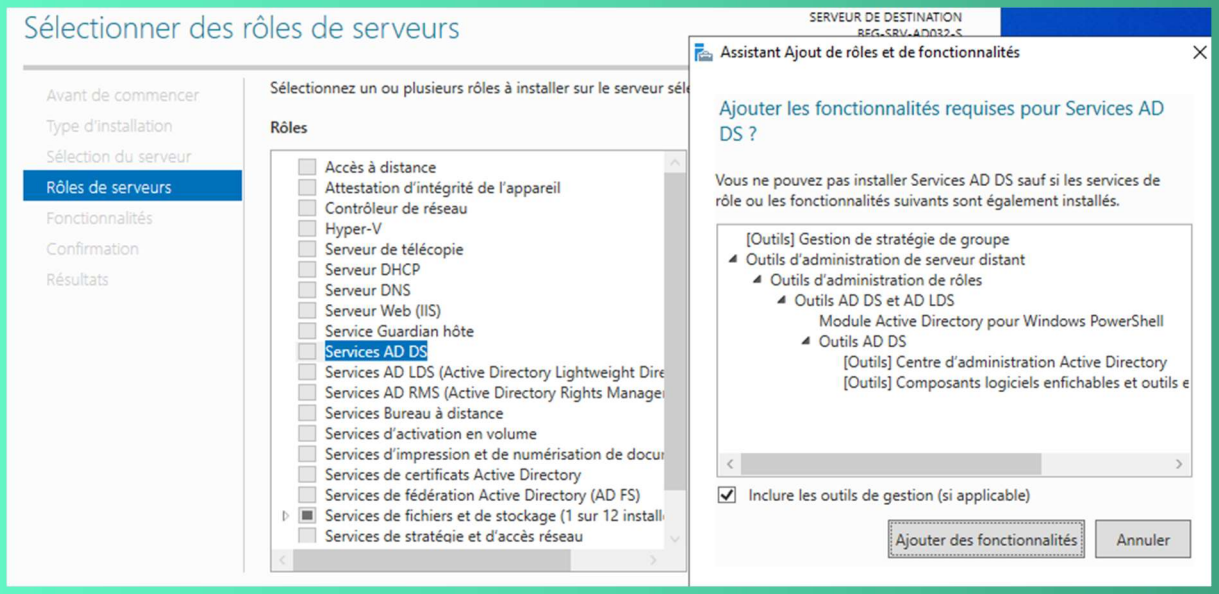
Aller dans l'outil 'Sauvegarde Windows Server'. Clique droit sur 'Sauvegarde locale' et sélectionner 'Récupérer, 'un autre emplacement', 'Dossier Partagé distant' et entrer le chemin de sa sauvegarde (\\172.20.3.4\SauvegardeAD), suivant, 'Etat du système', 'emplacement d'origine' et cocher la case pour l'autorité



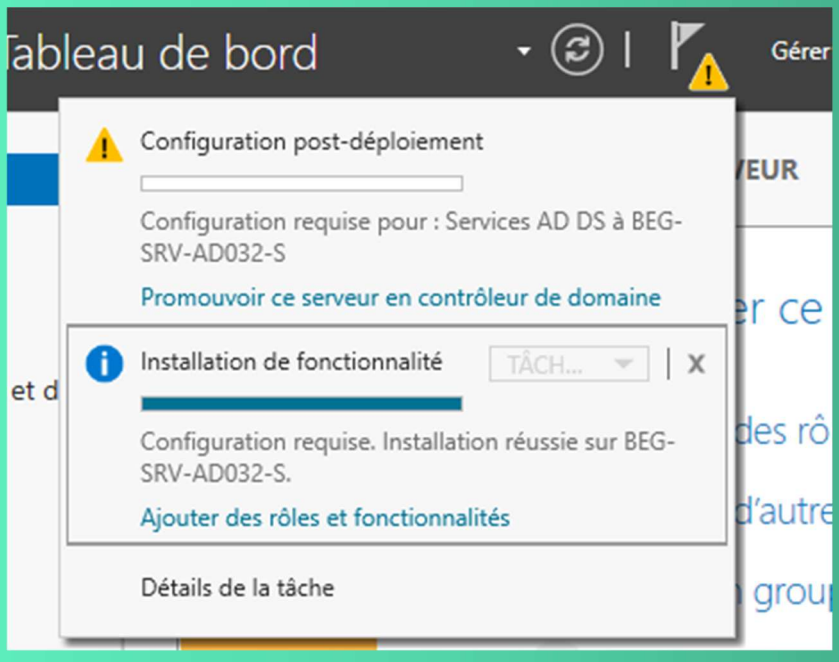
CONFIGURATION D'UN SECOND ACTIVE DIRECTORY

Installation du service :

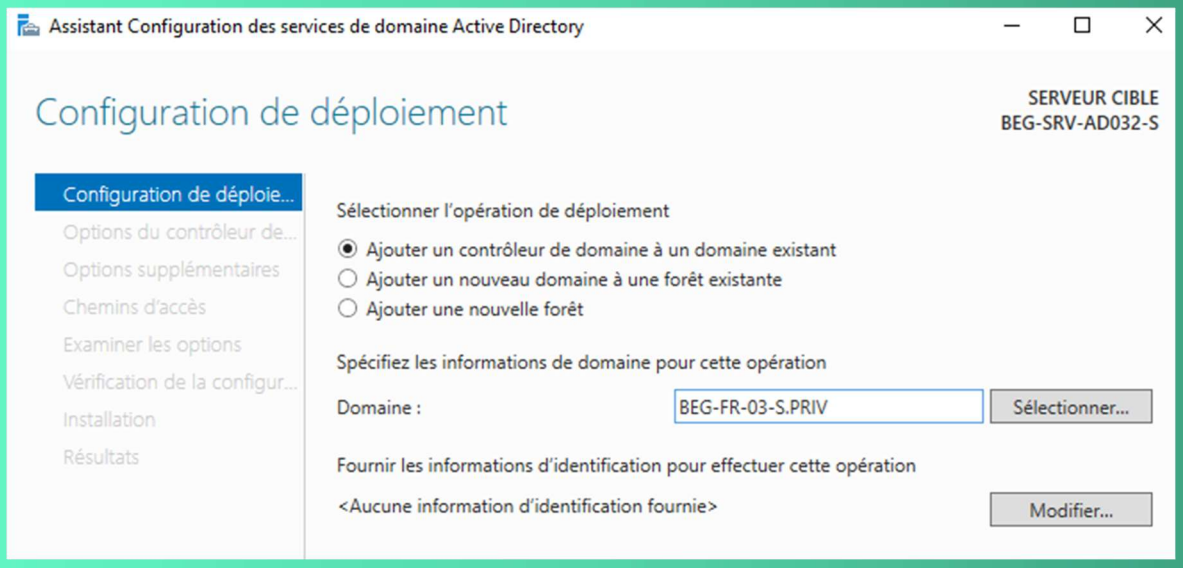
Pour installer le service active directory, il faut installer le service AD DS



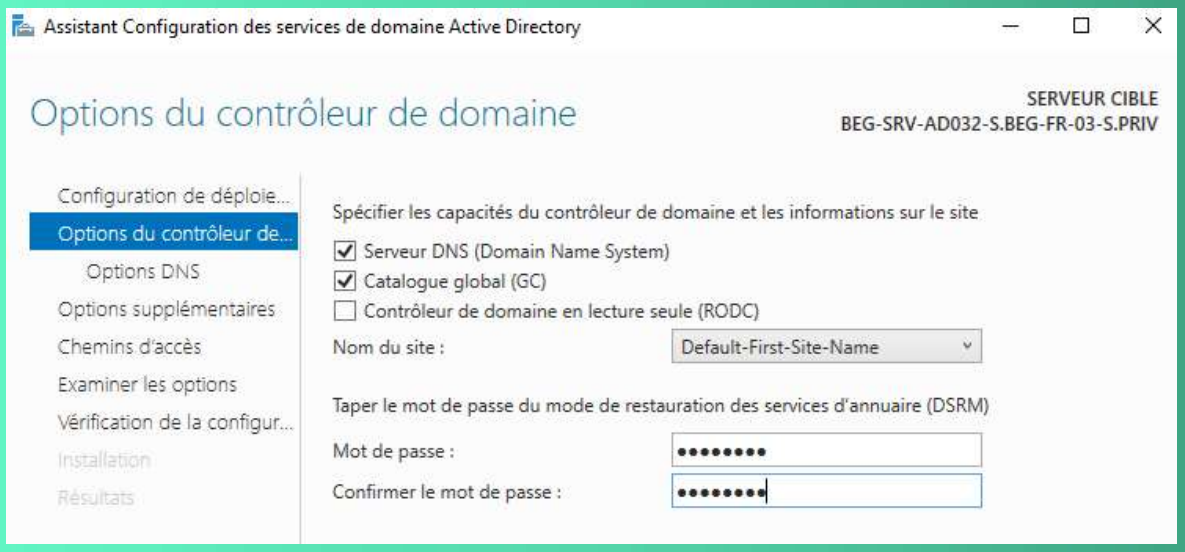
Ensuite, promouvoir ce serveur en contrôleur de domaine



Sélectionner ‘Ajouter un contrôleur de domaine à un domaine existant’ et entrer notre nom de domaine



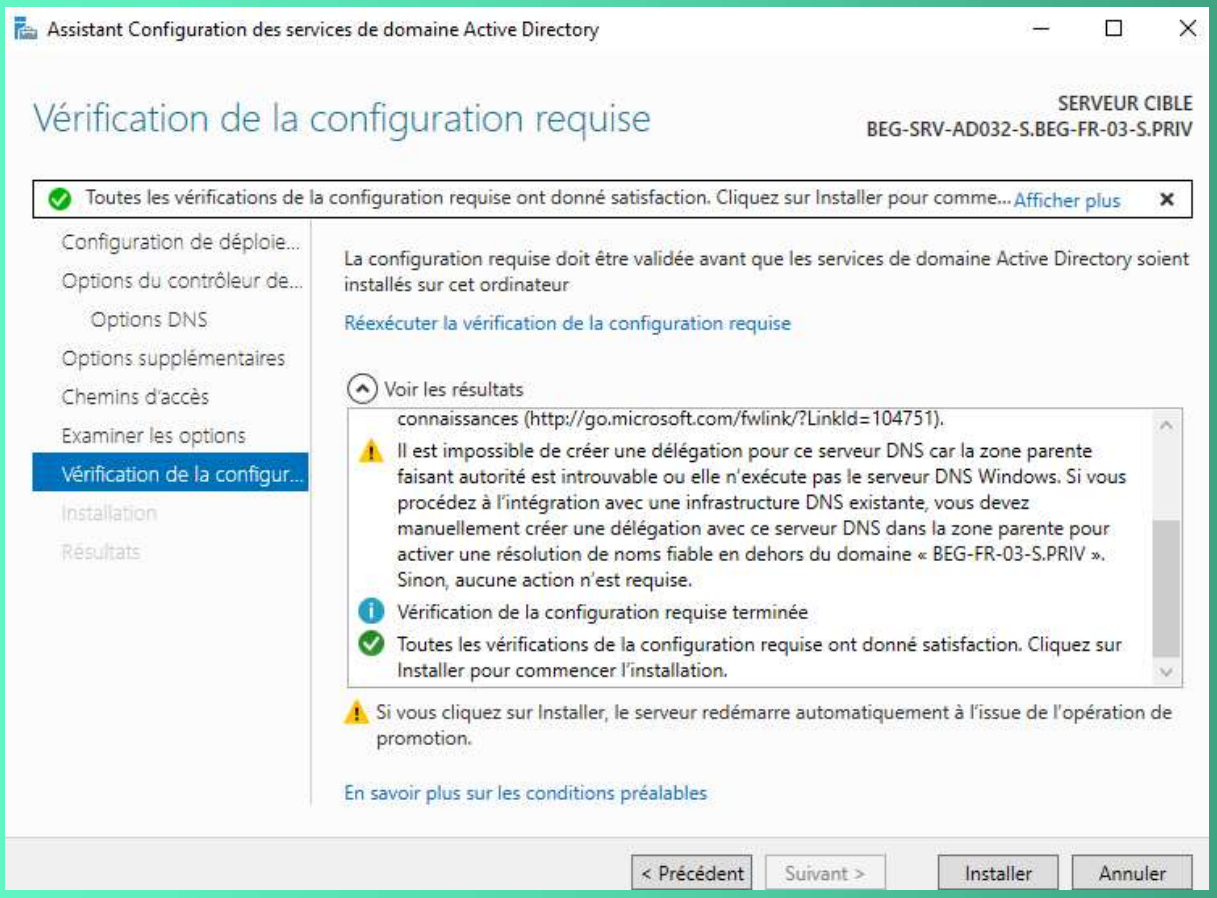
Spécifier les capacités du contrôleur de domaine et les informations sur le site



Spécifier des options supplémentaires :

Sélectionner ‘Tout contrôleur de domaine’ dans la case ‘Répliquer depuis

Pour finir, installer le service

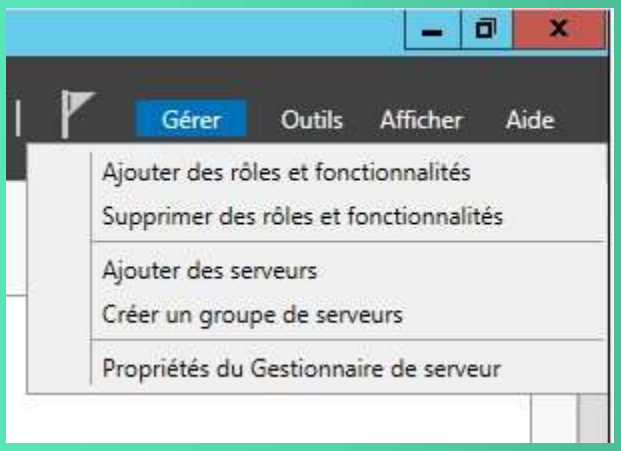


MISE EN PLACE D'UN RODC

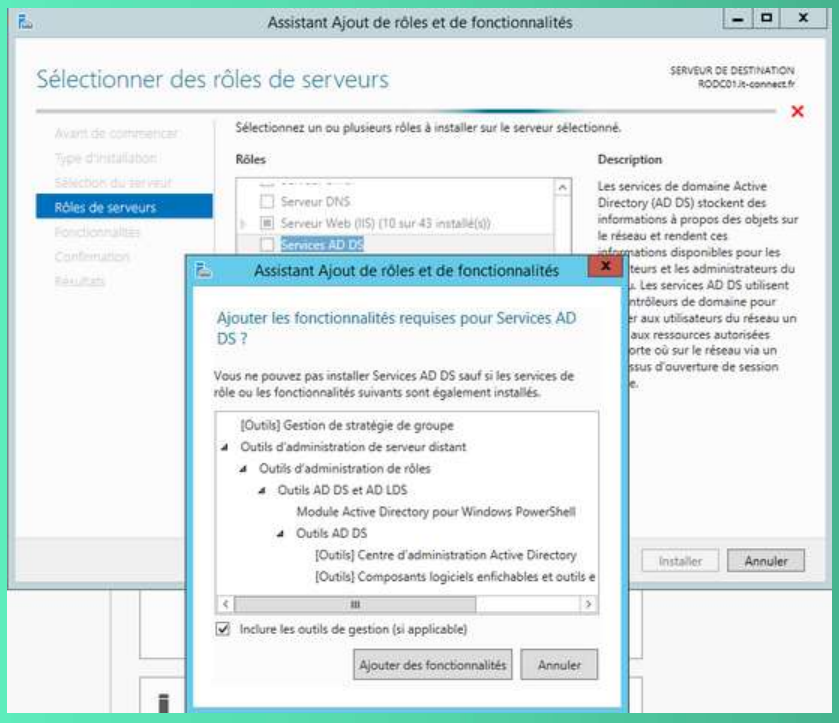
Installation du service :

Nous allons pouvoir passer à la mise en place d'un RODC, pour ma part le serveur qui doit devenir RODC est sous Windows Server 2022, dans le domaine BEG-FR-03-S.PRIV en niveau fonctionnel Windows Server 2022.

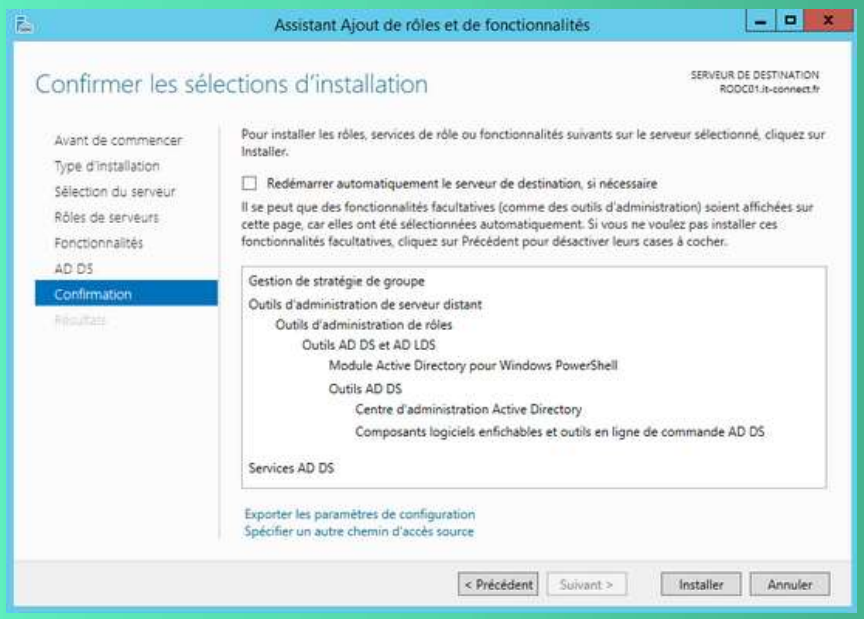
Sur le futur RODC, ouvrez le gestionnaire de serveur puis cliquez sur « Gérer » et « Ajouter des rôles et fonctionnalités ».



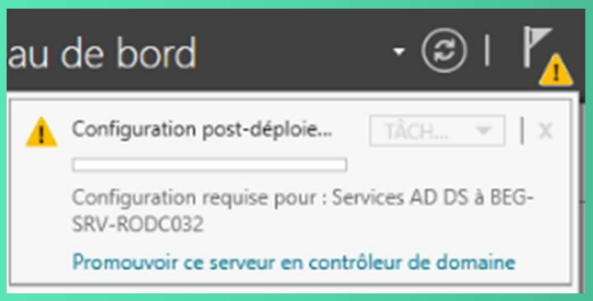
Dans la liste, sélectionnez « Services AD DS », confirmez l'ajout des fonctionnalités requises pour ce rôle et poursuivez.



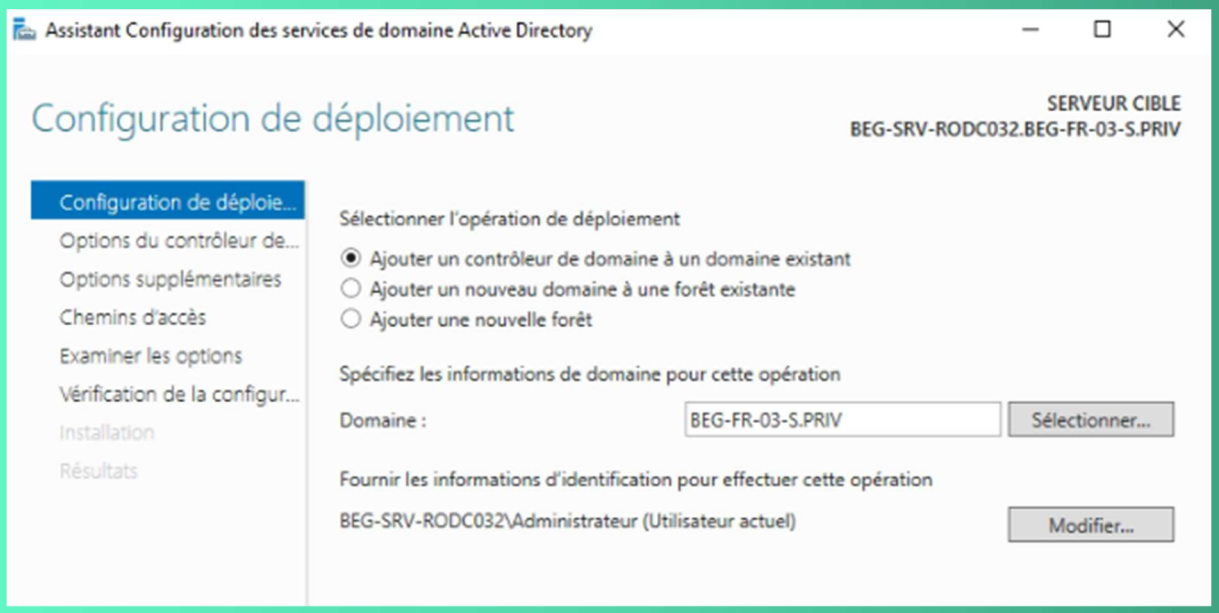
Confirmez que vous souhaitez installer les sélections en cliquant sur « Installer ».



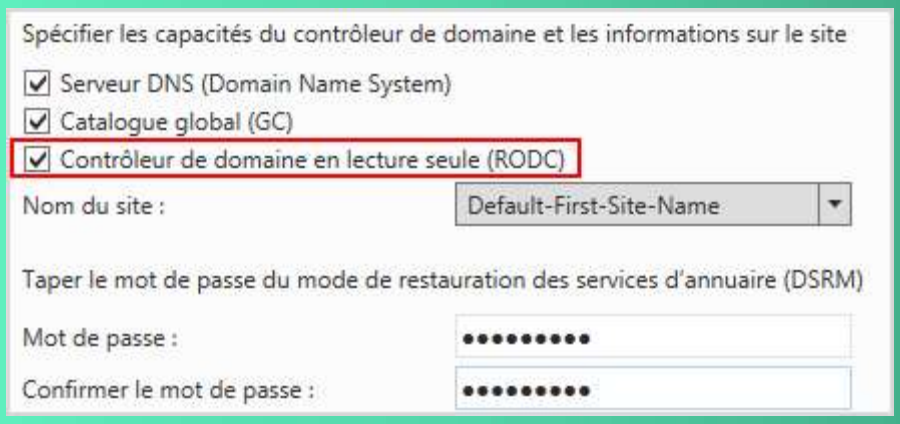
Ensuite, retournez au sein du gestionnaire de serveur, cliquez sur l'icône en « forme de triangle jaune où il y a un point d'exclamation » puis « Promouvoir ce serveur en contrôleur de domaine ».



Concernant la configuration de déploiement, sélectionnez « Ajouter un contrôleur de domaine à un domaine existant » (seul choix possible dans le cas de la mise en place d'un RODC). Cliquez sur « Suivant ».



Maintenant, veillez à cocher l'option « Contrôleur de domaine en lecture seule (RODC) » et éventuellement le DNS et le GC si vous souhaitez bénéficier des avantages du RODC pour ces rôles également.



Les options RODC doivent être définies :

- Compte d'administrateur délégué : Il a un rôle d'administrateur local du serveur et peut de ce fait installer des pilotes, gérer les services ou encore redémarrer le serveur. Toutefois, il n'a aucun privilège sur un autre contrôleur de domaine ou un autre RODC. Son champ d'action est uniquement local pour des raisons de sécurité.

Les utilisateurs pour lesquels le mot de passe est répliqué ou non sur le contrôleur de domaine en lecture seule se gère via l'appartenance à deux groupes :

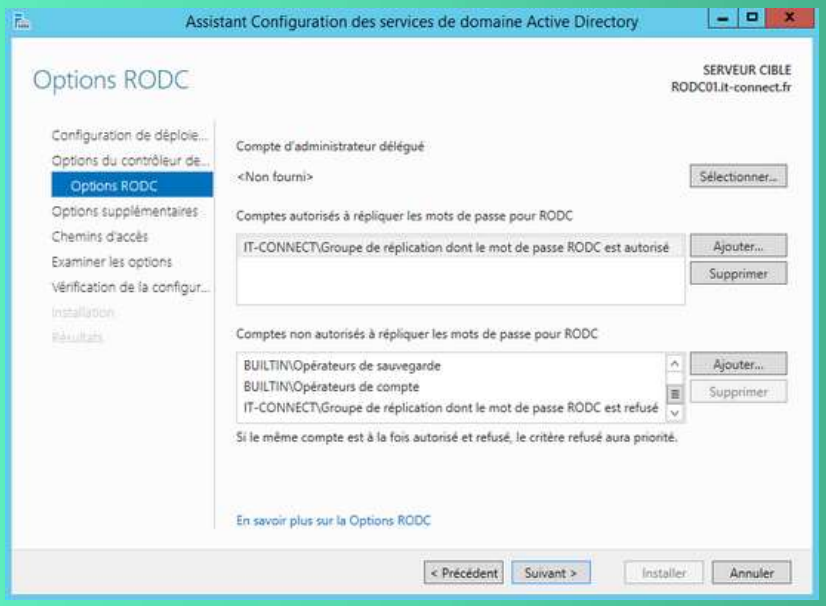
- Groupe de réplication dont le mot de passe RODC est autorisé
- Groupe de réplication dont le mot de passe RODC est refusé

Si par erreur, vous ajoutez un utilisateur dans les deux groupes, sachez que le droit « refusé » sera prioritaire donc le mot de passe de cet utilisateur ne sera pas répliqué.

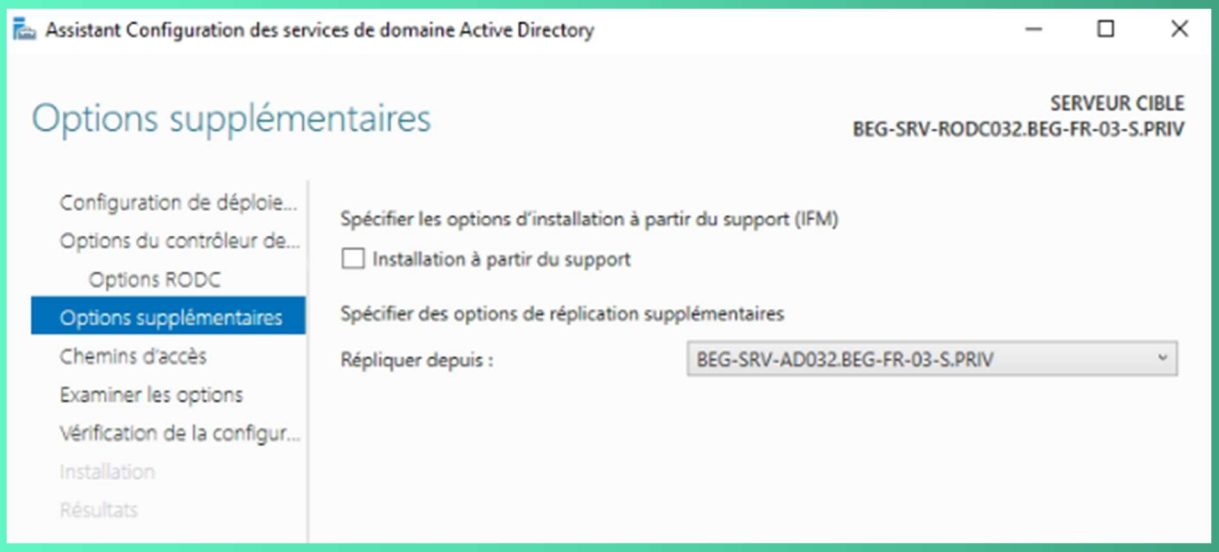
- Comptes autorisés à répliquer les mots de passe pour RODC : Ajouter des utilisateurs ou groupes pour lesquels vous souhaitez autoriser la réplication. Le mieux, c'est de laisser uniquement le groupe « Groupe de réplication dont le mot de passe RODC est autorisé » et dans l'Active Directory d'ajouter à ce groupe les objets (utilisateurs/groupes) pour lesquels vous souhaitez autoriser la réplication.

- Comptes non autorisés à répliquer les mots de passe pour RODC : Ajouter des utilisateurs ou groupes pour lesquels vous ne souhaitez pas autoriser la réplication. Par défaut, tous les comptes et groupes sensibles (comme Administrateur, admins du domaine, etc…) sont ajoutés, il est fortement déconseillé en termes de sécurité d'autoriser la réplication pour les objets sensibles. Comme pour le cas précédent, le mieux c'est d'ajouter les utilisateurs et les groupes non autorisés au groupe « Groupe de réplication dont le mot de passe RODC est refusé » directement dans l'annuaire Active Directory.

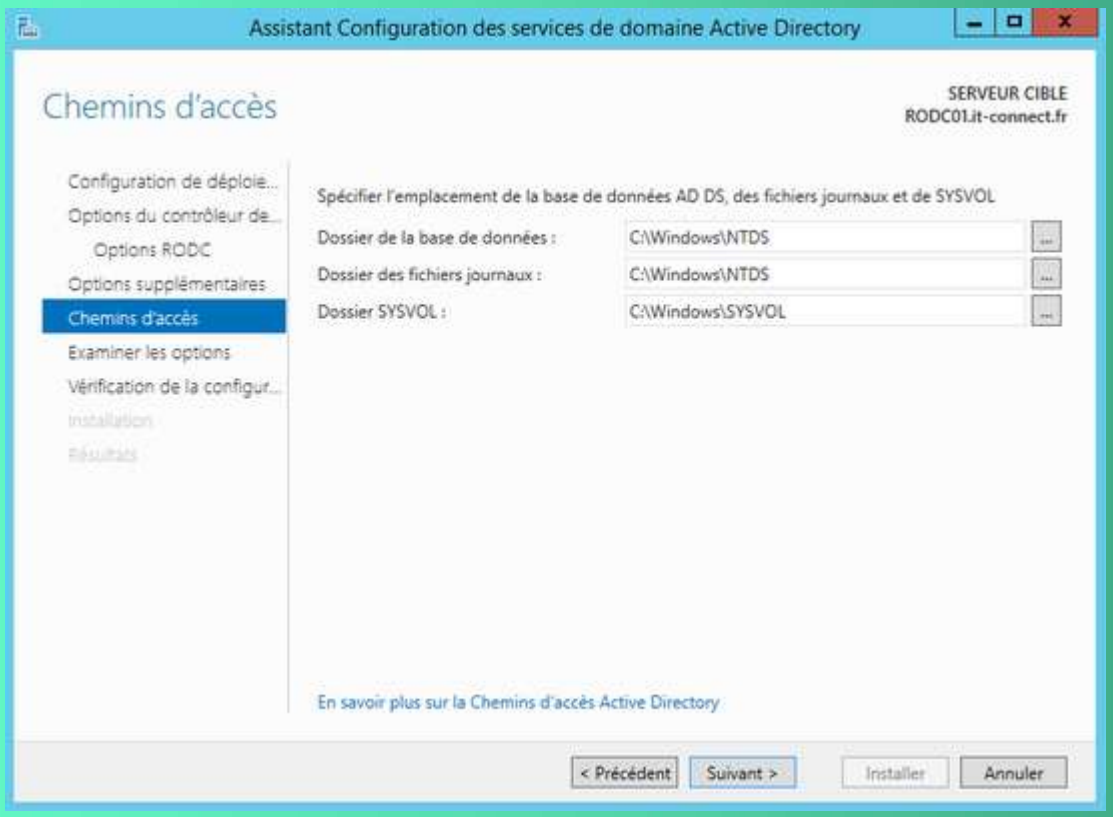
Cliquez sur « Suivant » pour continuer l'installation.



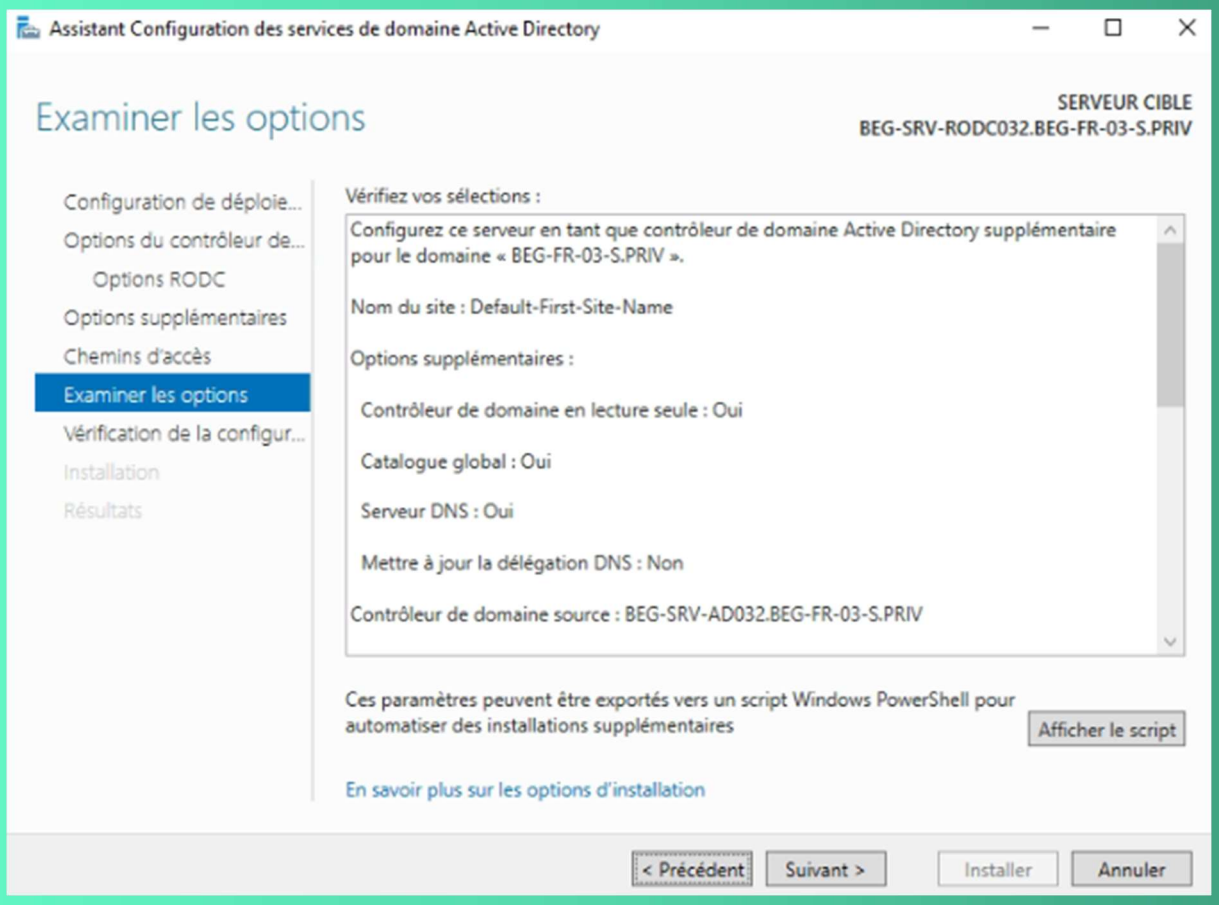
Indiquez un contrôleur de domaine standard depuis lequel répliquer les informations autorisées (ou installer à partir d'un support si vous disposez d'un support prêt – utile pour économiser de la bande passante même lors de la mise en place). Cliquez sur « Suivant ».



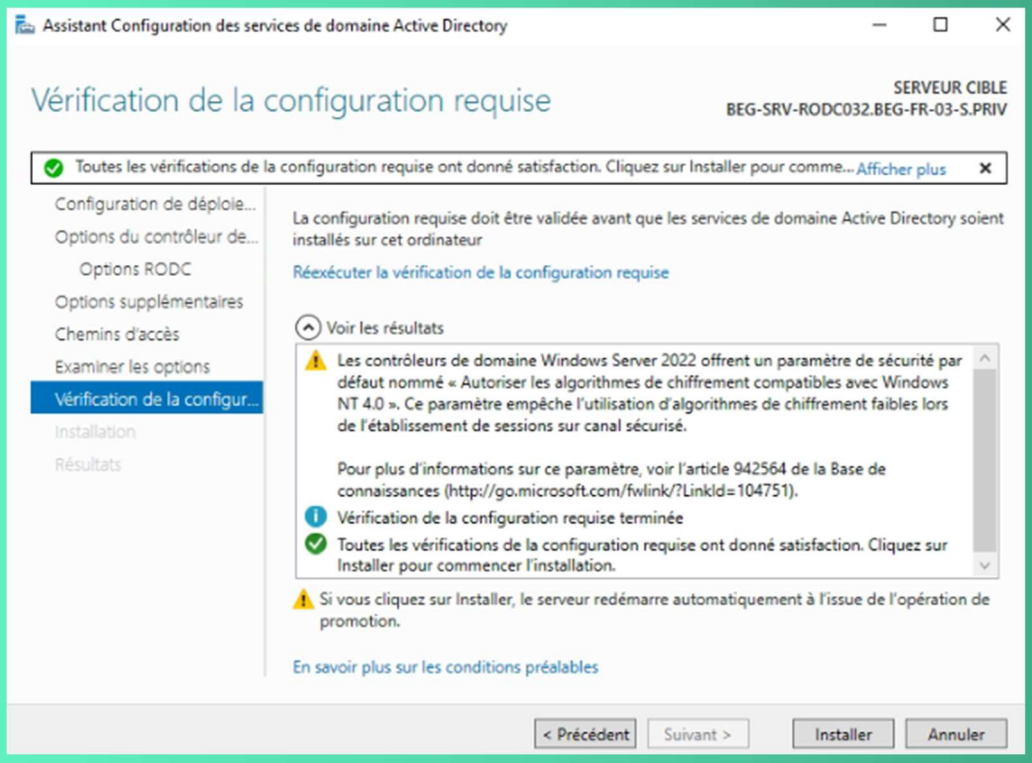
Indiquez l'emplacement de la base de données, des fichiers journaux et de SYSVOL (peuvent être placés sur des disques différents). Cliquez sur « Suivant ».



Examiner une dernière fois les options avant de cliquer sur « Suivant » et d'exécuter l'installation.



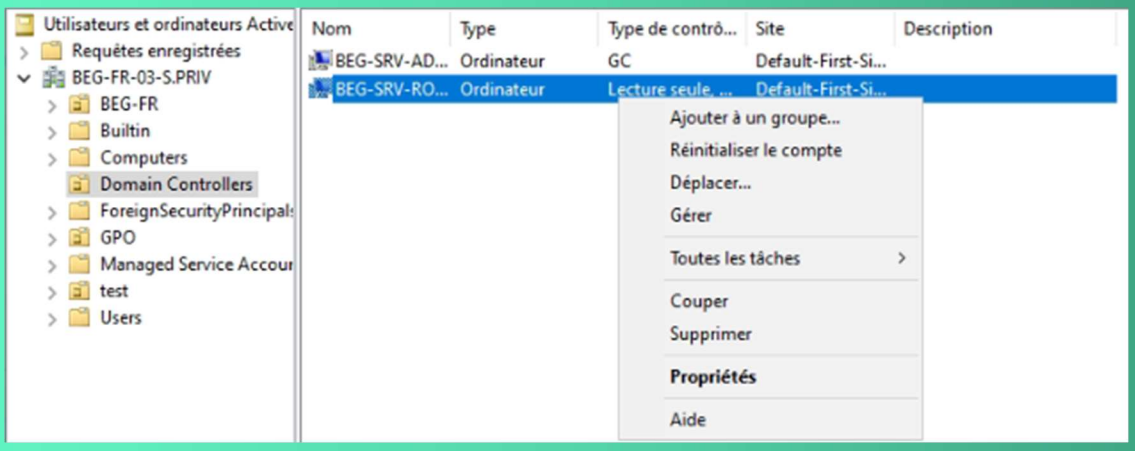
Après que la configuration soit vérifiée, cliquez sur « Installer » et patientez un instant. Le serveur va redémarrer automatiquement à la fin de l'installation.



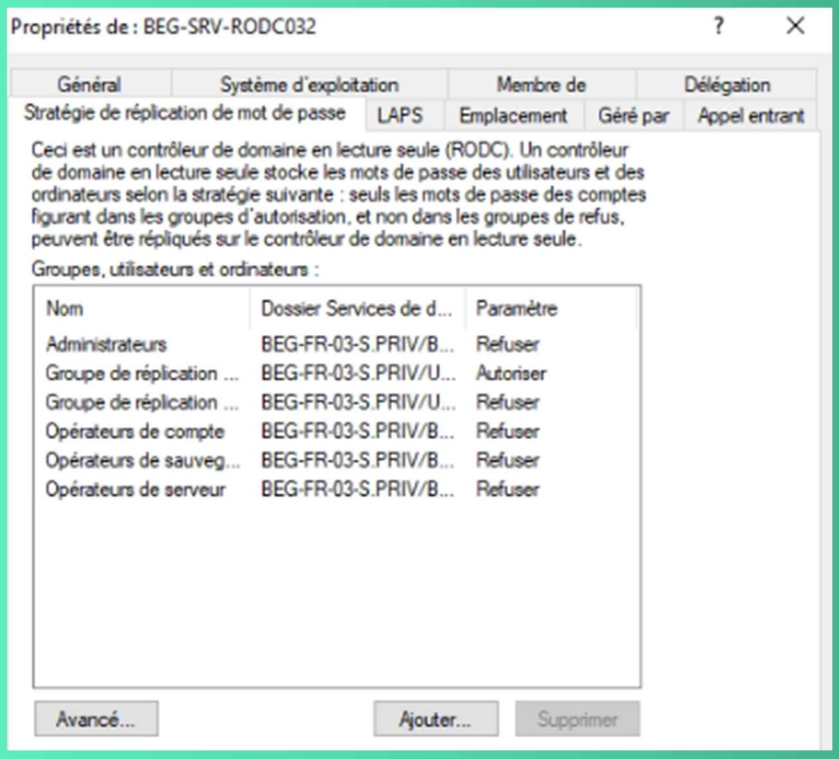
L'installation du RODC est désormais terminée.

Réplication des mots de passes

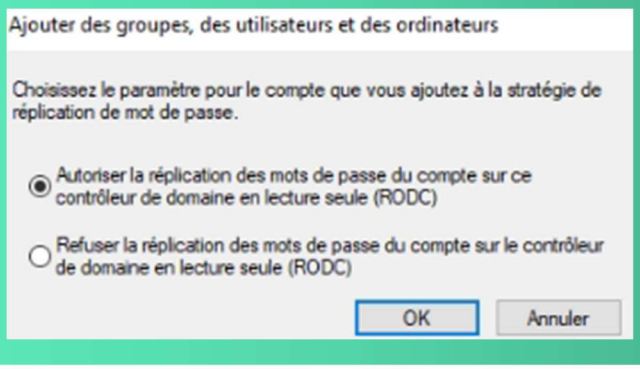
Sur un contrôleur de domaine standard (lecture/écriture), ouvrez la console « Utilisateurs et ordinateurs Active Directory », positionnez-vous sur l'unité d'organisation « Domain Controllers ». Sur la droite, faites clic droit sur l'objet ordinateur correspondant à votre serveur RODC puis « Propriétés ».

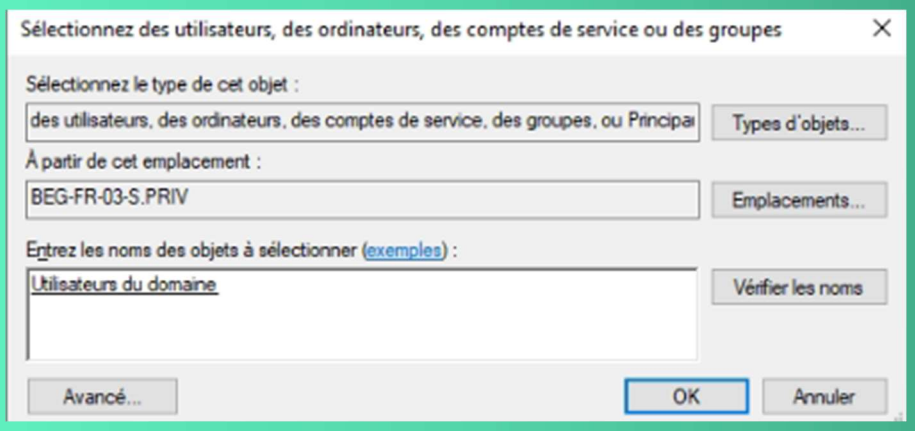


Cliquez ensuite sur l'onglet « Stratégie de réplication de mot de passe » qui concerne donc la stratégie de réplication des mots de passe. La fenêtre affiche les utilisateurs et groupes pour lesquels vous autorisez ou refusez explicitement la réplication des mots de passe.

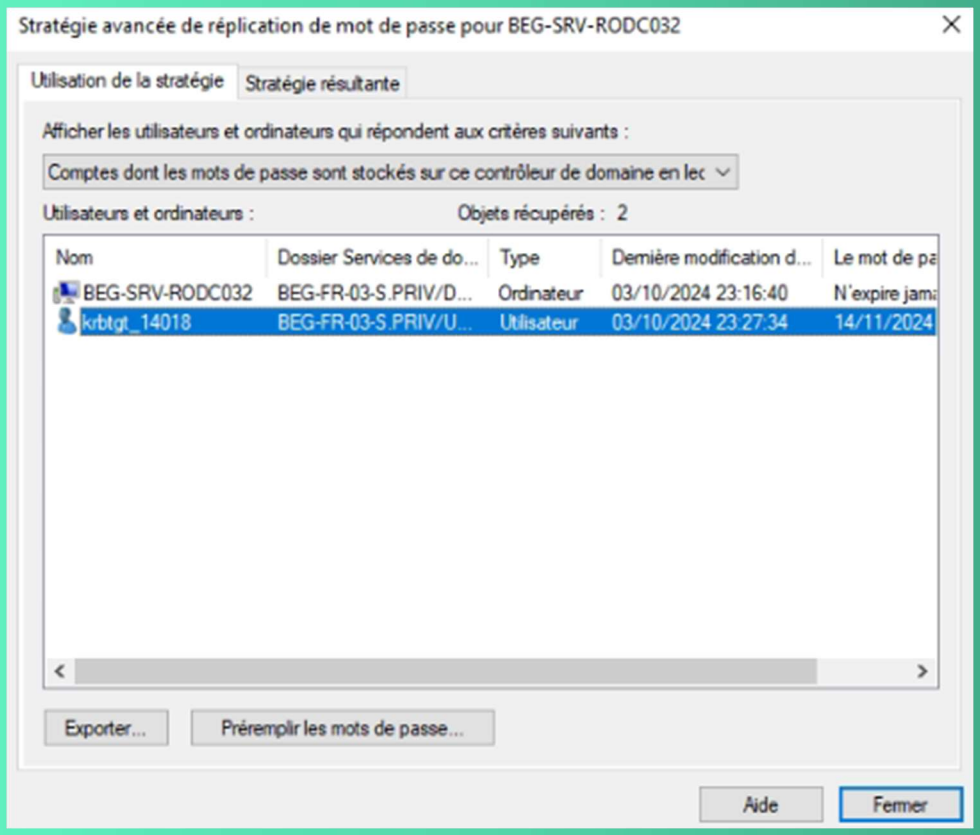


Pour ajouter un nouvel objet, cliquez sur « Ajouter… » et ensuite indiquez si c'est un ajout pour une autorisation ou un refus (voir ci-dessous). Cliquez sur « OK ». Une nouvelle fenêtre apparaît, recherchez dans l'annuaire le groupe ou utilisateur concerné pour l'ajouter.





Par ailleurs, si vous cliquez sur le bouton « Avancé » de l'onglet « Stratégie de réplication de mot de passe », vous pouvez voir quels utilisateurs ont leur mot de passe stocké sur le RODC sélectionné.



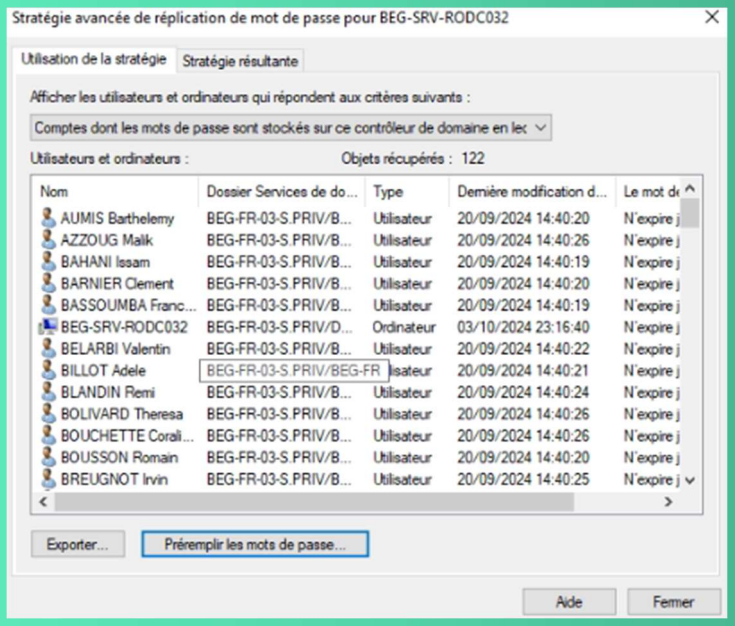
Vous remarquerez la présence d'un utilisateur nommé « krbtgt_14018 » qui est propre à chaque RODC (généré sous la forme krbtgt_xxxxx). Il permet de délivrer les tickets Kerberos aux clients.

Si vous changez dans la liste déroulante et que vous choisissez « Comptes authentifiés sur ce contrôleur de domaine en lecture seule », ainsi, vous pourrez voir les comptes utilisateurs qui se sont déjà authentifiés en passant par ce RODC. Cela vous permet de savoir éventuellement qui se connecte depuis ce site distant et ensuite de gérer la stratégie selon les besoins.

Il est également possible de « Préremplir les mots de passe », ce qui est intéressant si vous préparez le serveur RODC sur le site principal avant de le mettre en production sur le site distant. En fait, les mots de passe seront mis en cache maintenant afin d'éviter de charger la liaison WAN lors de la mise en production et de la première demande d'authentification de l'utilisateur.

Pour ajouter un mot de passe au cache, cliquez sur le bouton « Préremplir les mots de passe », recherchez votre utilisateur dans l'annuaire et validez. Ensuite, cliquez sur « Oui » pour confirmer la mise en cache.

Il est à noter que vous devez autoriser la réplication du mot de passe de cet utilisateur pour pouvoir le mettre en cache, ce qui est logique.



Vous êtes désormais en mesure de comprendre l'intérêt d'un RODC et d'en mettre un en place au sein de votre infrastructure.

Retirer le rodc du domaine

Pour retirer le RODC, il faut suivre plusieurs étapes :

Rétrograder l’AD

Désinstaller la fonctionnalité AD DS ainsi que le DNS

Retirer le RODC du domaine

Retirer le RODC sur l’AD

Retirer le RODC du DNS

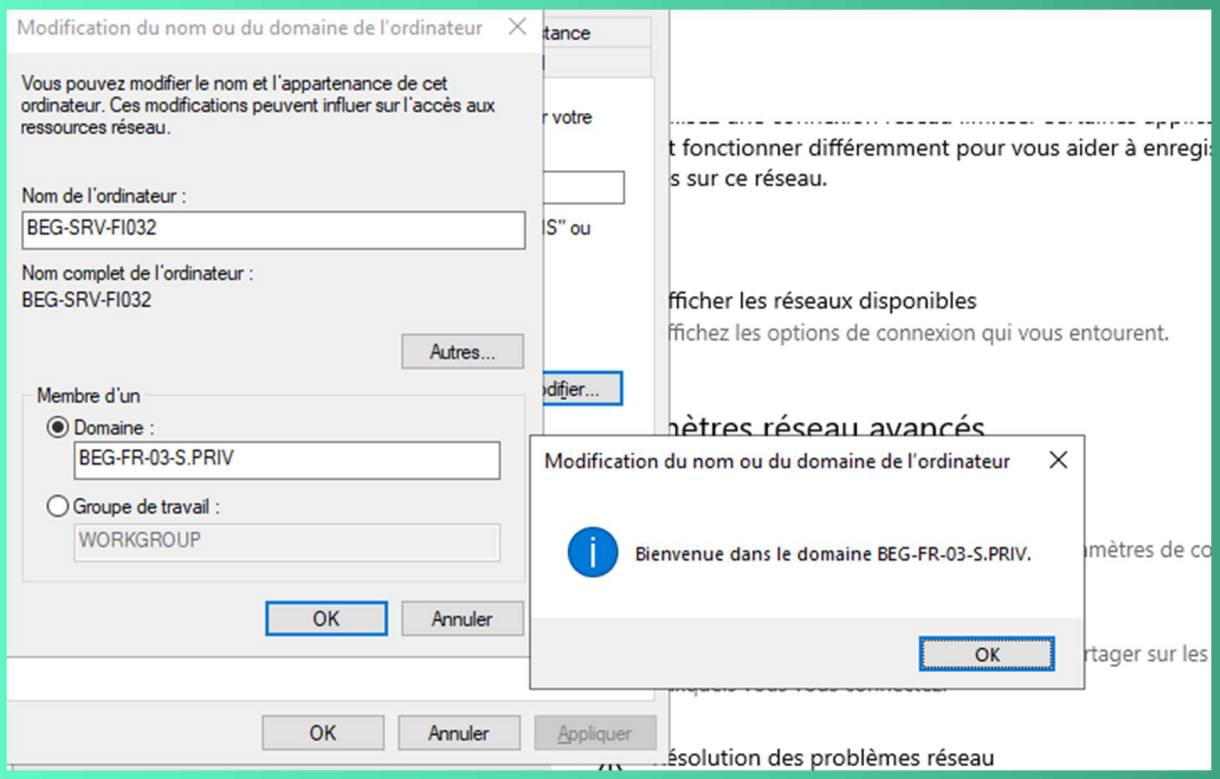
CHANGER LE SID D'UNE MACHINE

Pour changer le SID d'une machine, entrer cette commande :

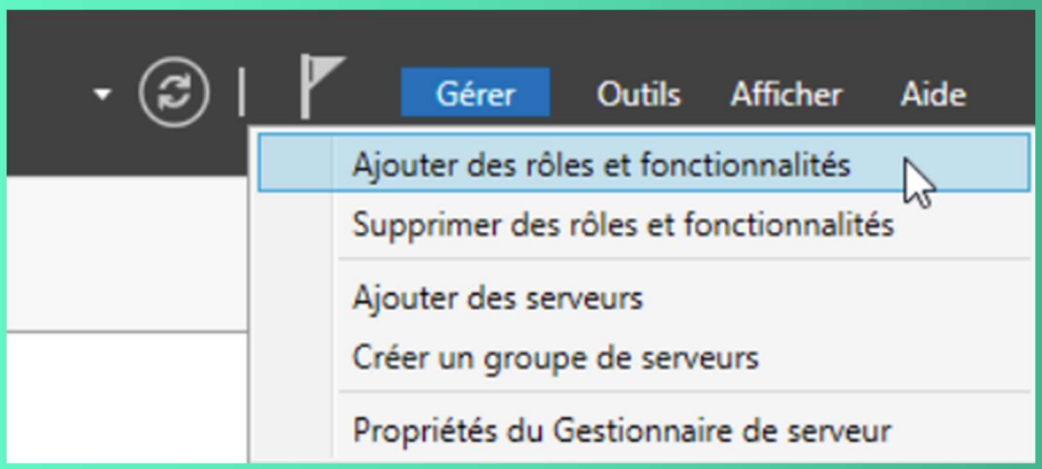
```
C:\Windows\System32\sysprep\sysprep.exe /oobe /generalize /shutdown
```

CONFIGURATION DU SERVEUR DE FICHIER

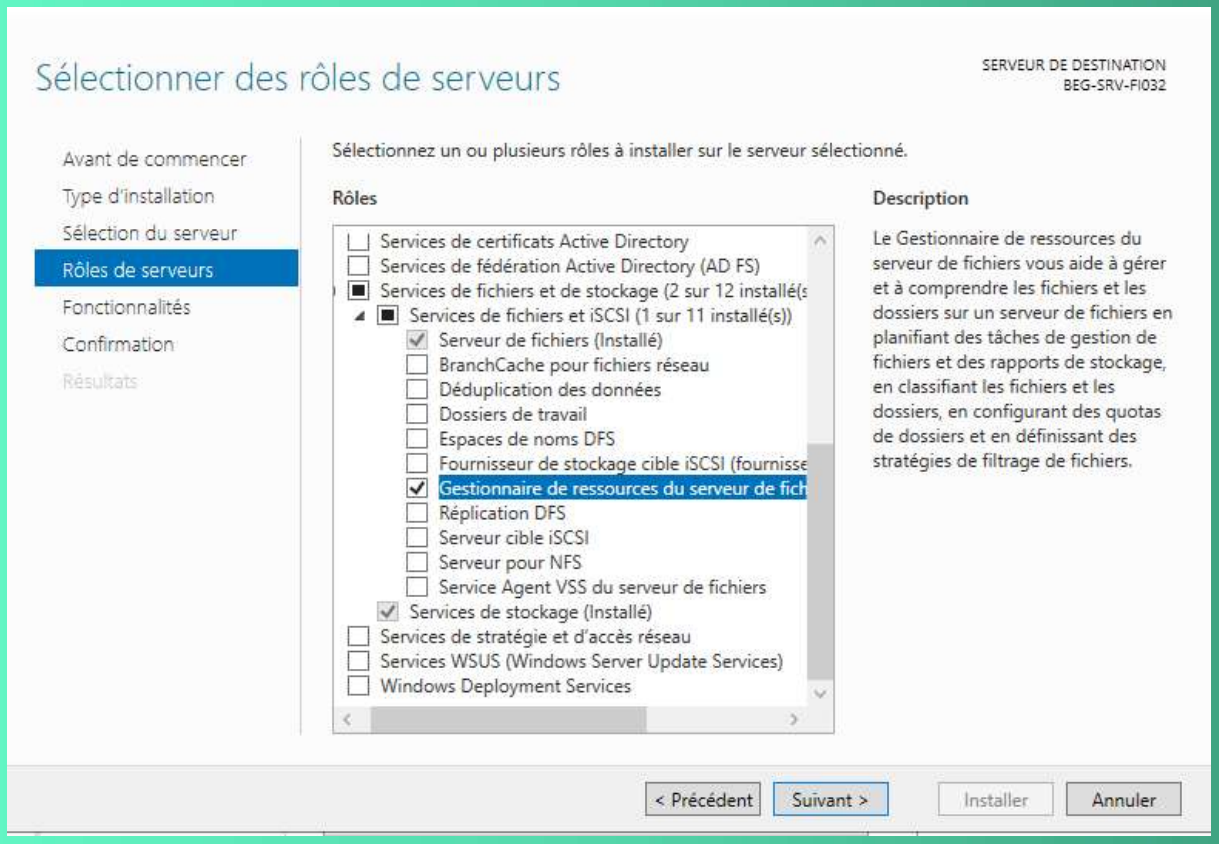
Nous avons ajouté le serveur de fichier sur notre AD ainsi que dans le domaine



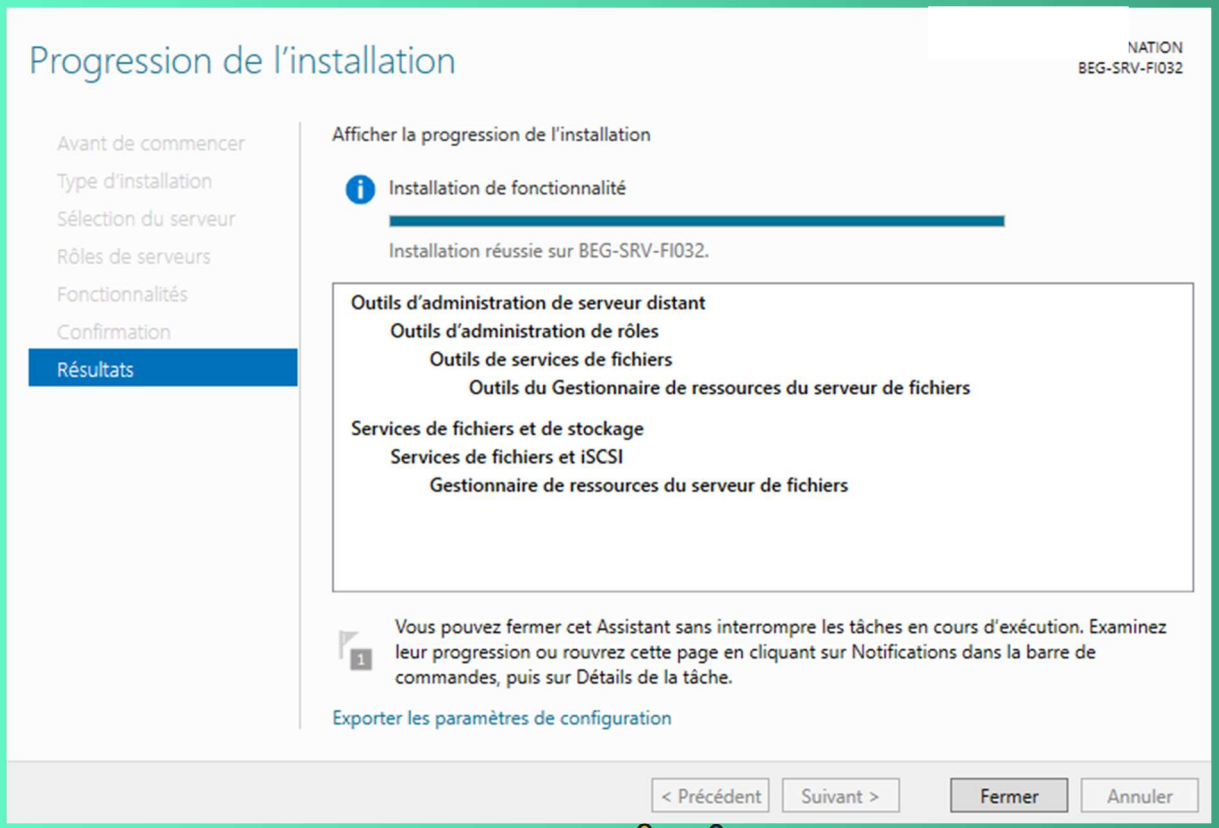
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur 'Gérer' et 'Ajouter des rôles et fonctionnalités'.



Dans l'onglet 'Rôles de serveurs', cocher 'Services de fichiers et iSCSi' puis 'gestionnaire de ressources du serveur de fichier'.



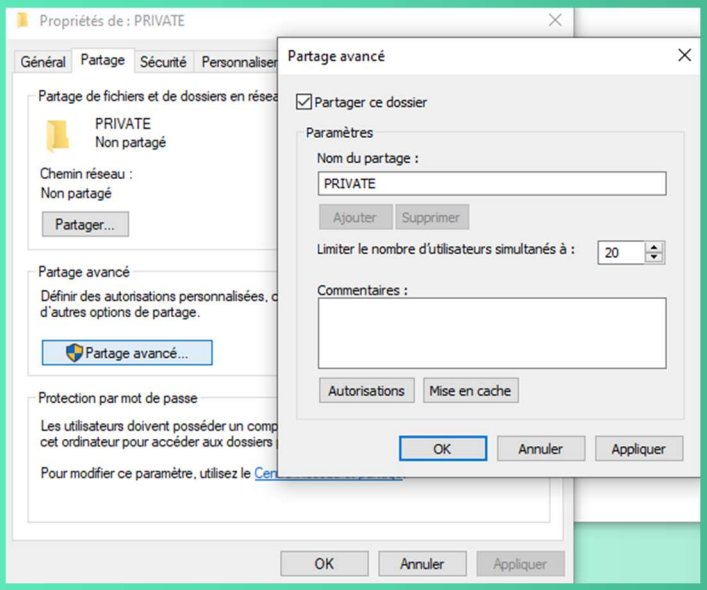
Dans l'onglet 'Confirmation', installer les services.



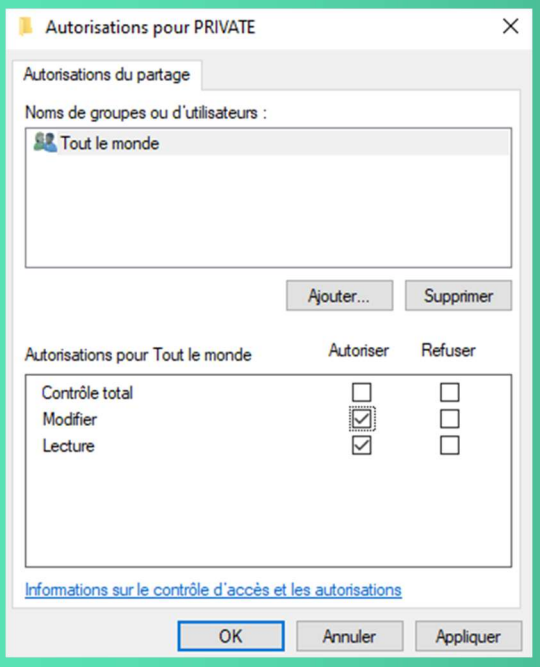
CRÉATION DES DOSSIERS PRIVATE

Partage du dossier :

Aller dans les propriétés du dossier que l'on souhaite partager, puis partage avancer et donner un nom au partage.

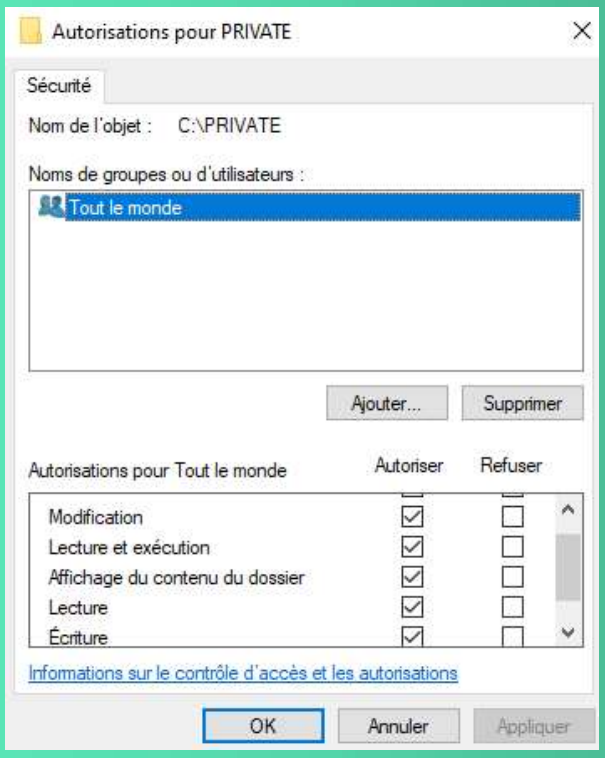


Ensuite, cliquer sur 'Autorisations' et sélectionner tout le monde en lecture et modifier

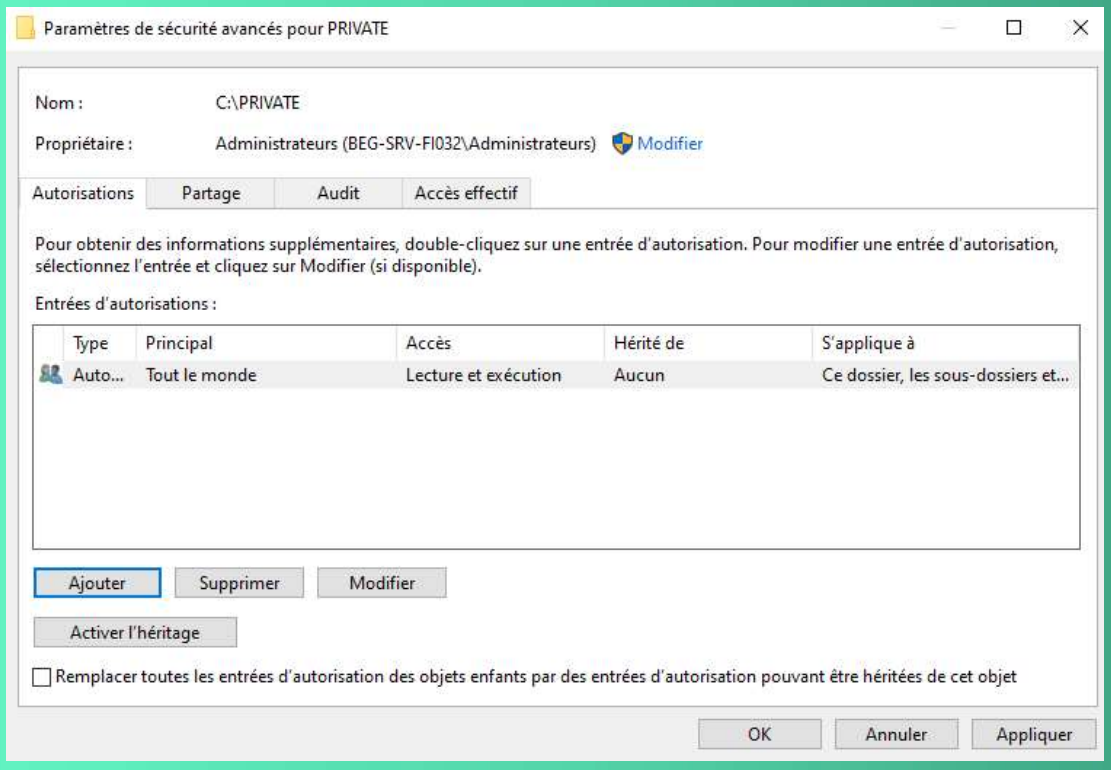


Permissions NTFS :

Pour configurer le permissions NTFS, il faut aller dans l'onglet sécurité puis sur modifier et ajouter le groupe « tout le monde » avec lecture et exécution uniquement



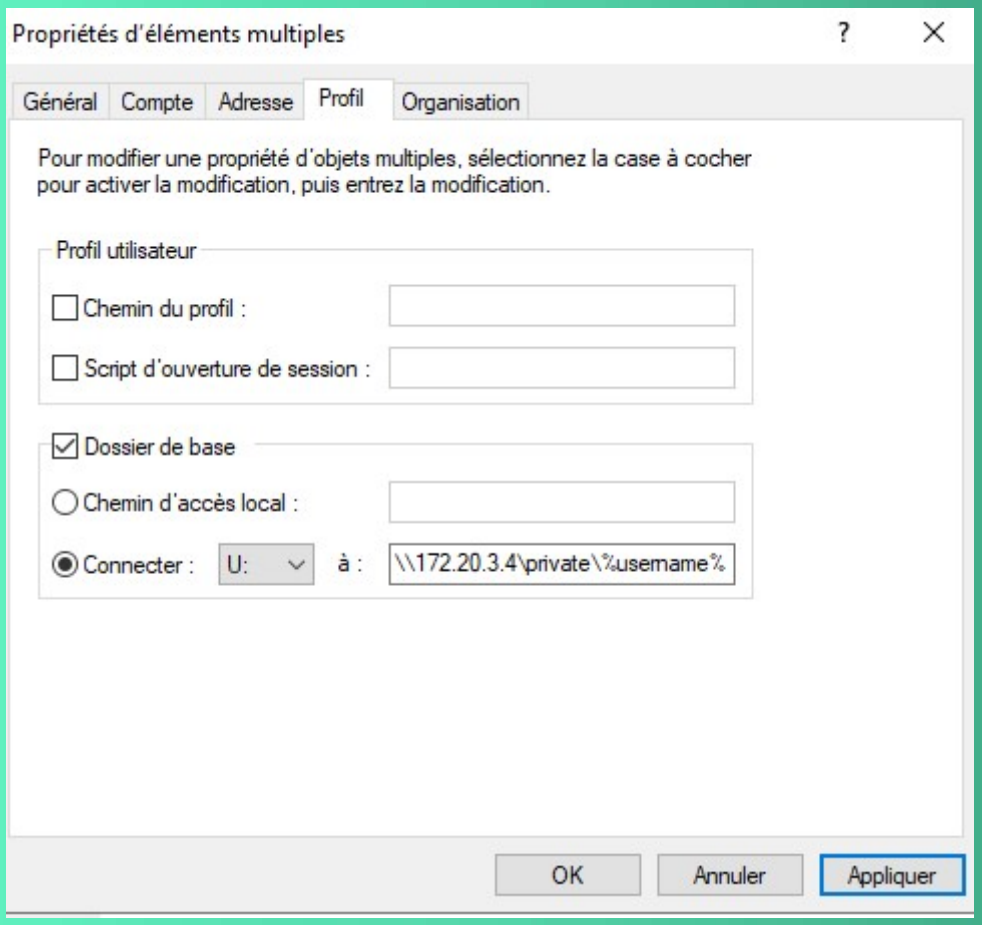
Ensuite il faut désactiver l'héritage dans les paramètres de sécurités avancés du dossier PRIVATE



Création des fichiers pour chaque utilisateur :

Sélectionner tous les utilisateurs présents dans l'AD, clic droit puis propriétés.

Ensuite dans l'onglet 'profil', cocher le chemin du profil et entrer l'endroit où le dossier utilisateur PRIVATE se situe



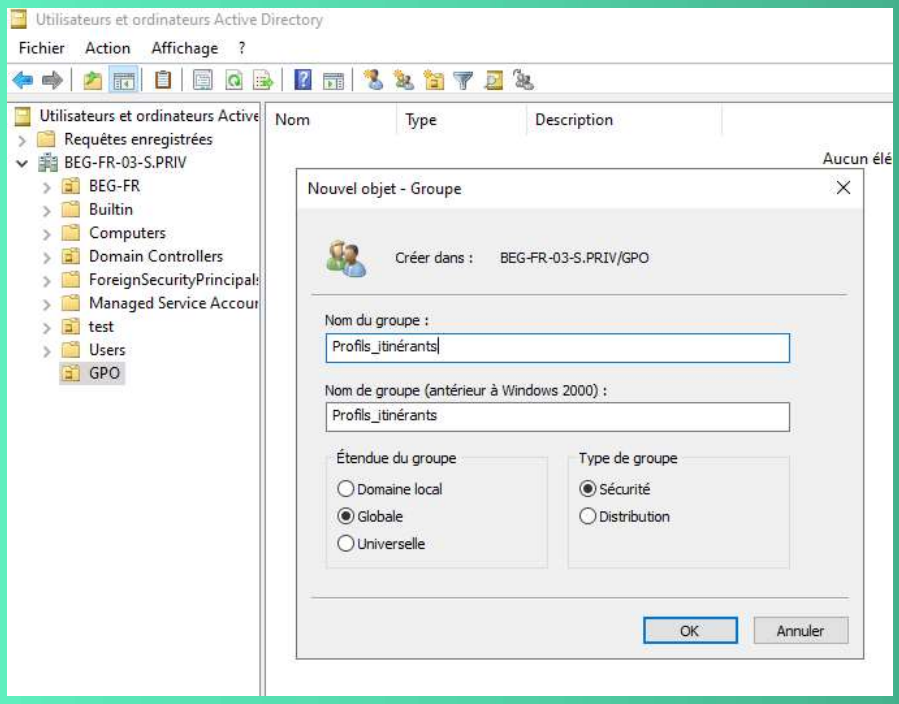
PROFILS ITINÉRANTS

Préparer le contrôleur de domaine (AD et GPO) :

La première chose à faire est de préparer son AD correctement.

Création d'une OU pour les GPO :

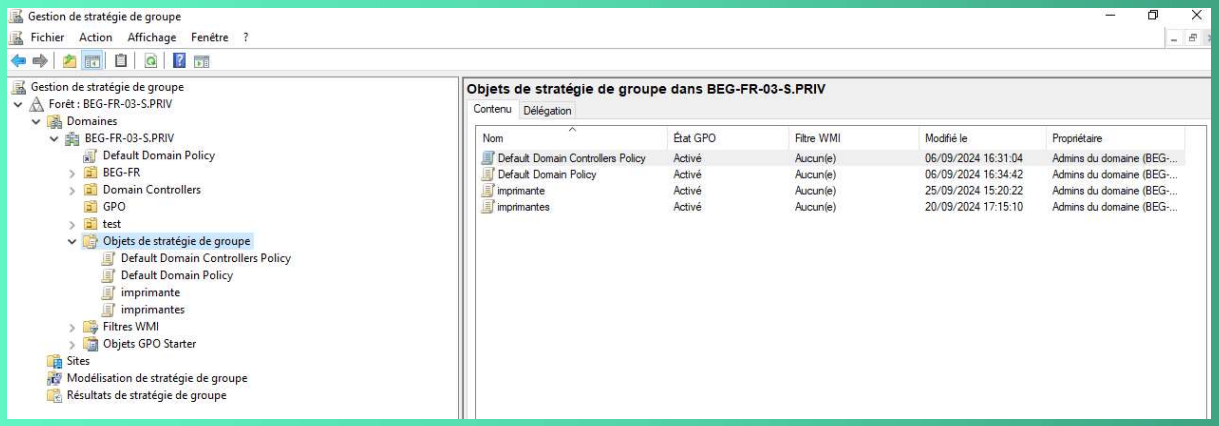
Nous avons créé une Unité d'Organisation nommée GPO puis créer un groupe global nommée 'Profils_itinérants'



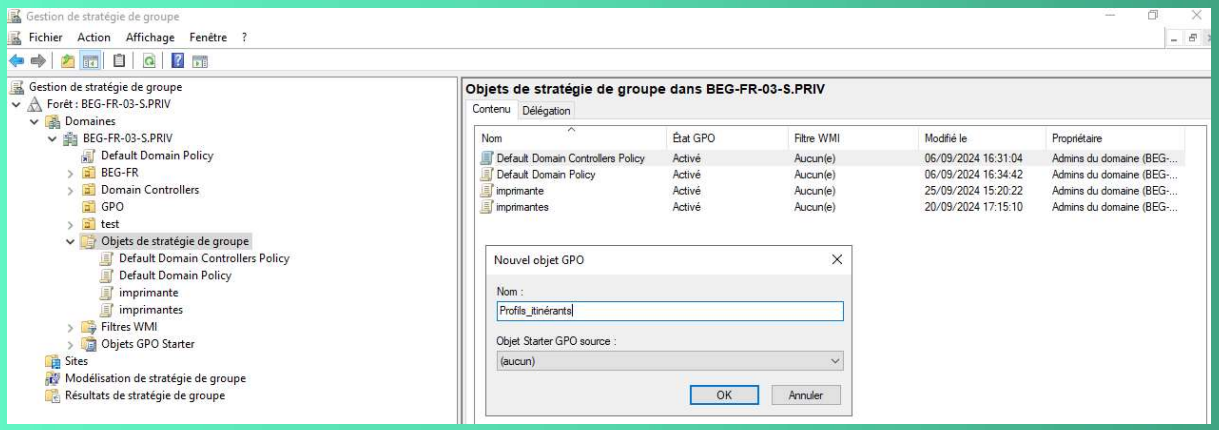
Afin d'éviter des possibles problèmes « un jour » nous allons mettre en place une GPO

Par défaut, lorsque le dossier de profil d'un utilisateur sera créé sur le serveur de fichiers, seul l'utilisateur lui-même sera habilité à y accéder. Ce n'est pas bien grave mais si nous avons besoin d'y accéder en tant qu'administrateur, ne serait-ce que pour dépanner ou restaurer quelque chose, on va se retrouver bloquer et il n'est pas du tout recommandé de changer les autorisations sur un dossier de profil existant au risque de tout faire péter et que l'utilisateur se retrouve sur son PC avec un profil « temporaire ». Le but de la GPO que nous allons créer maintenant est justement d'ajouter automatiquement des droits sur les dossiers des profils aux admins.

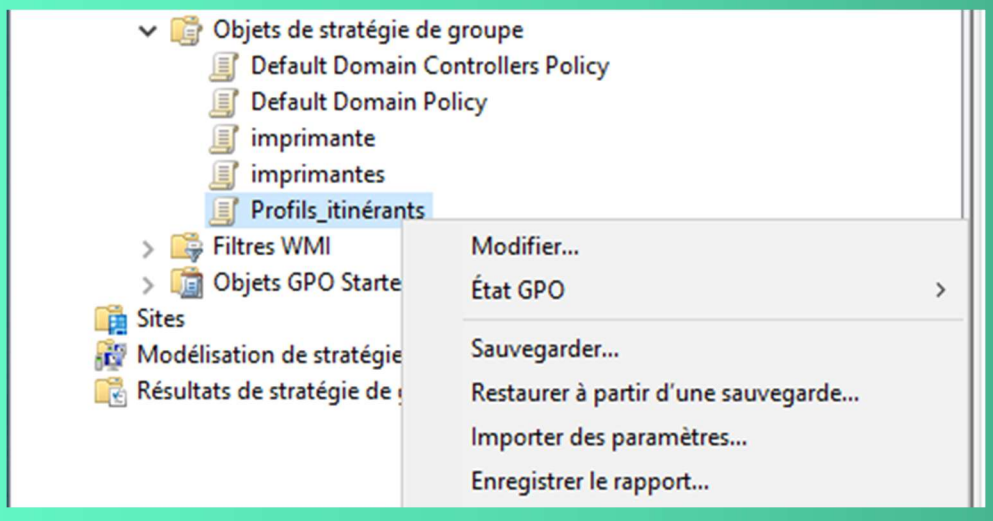
Pour cela, ouvrez votre console de gestion des stratégies de groupe.



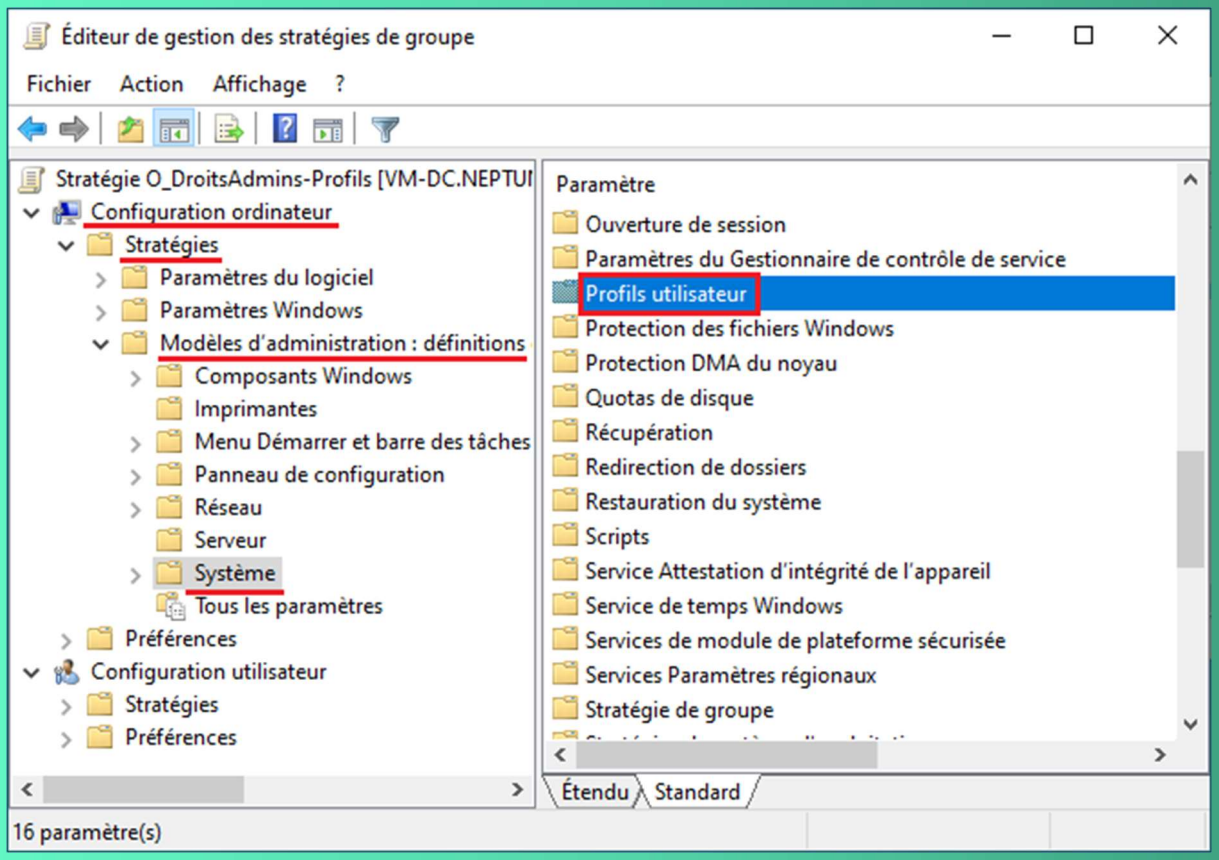
Dans la partie « Objets de stratégie de groupe », faites un clic droit puis « Nouveau ». Ensuite nommer la GPO



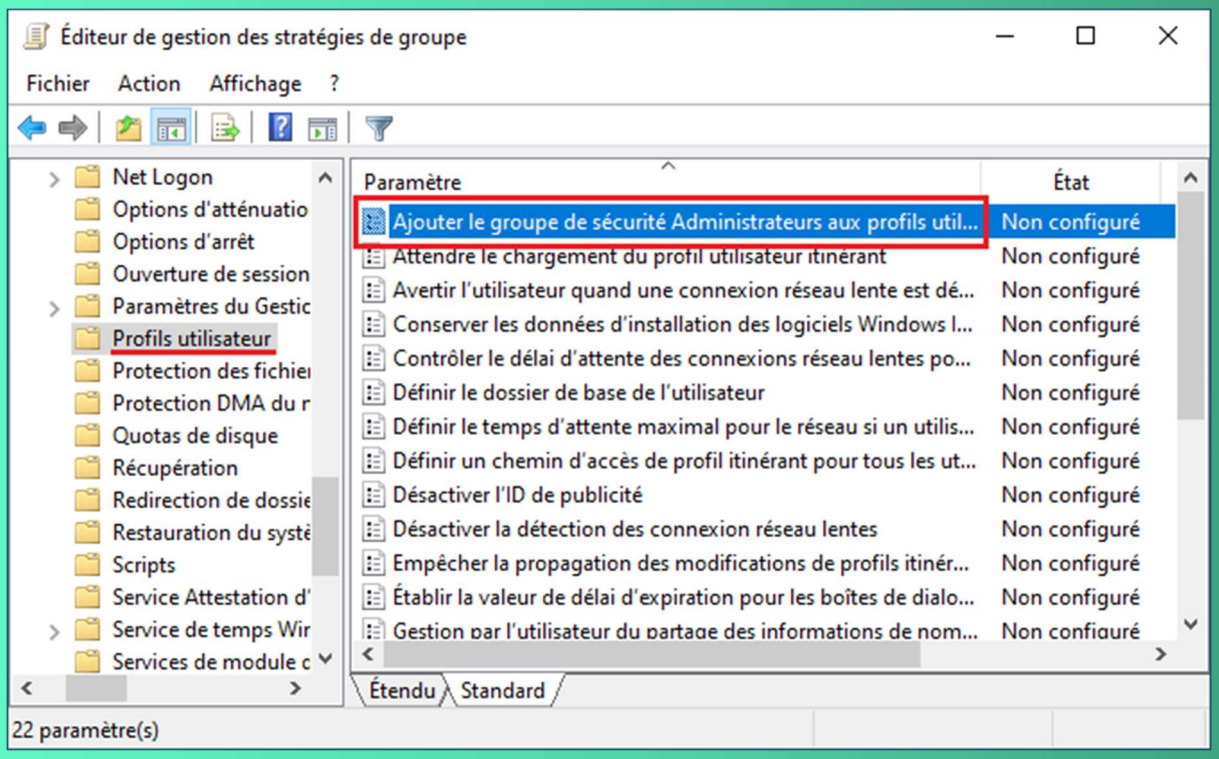
Ensuite faites un clic droit sur son nom puis « Modifier ».



Dans l'éditeur de GPO, allez dans Configuration ordinateur > Stratégies > Modèles d'administration > Système > Profils utilisateur.

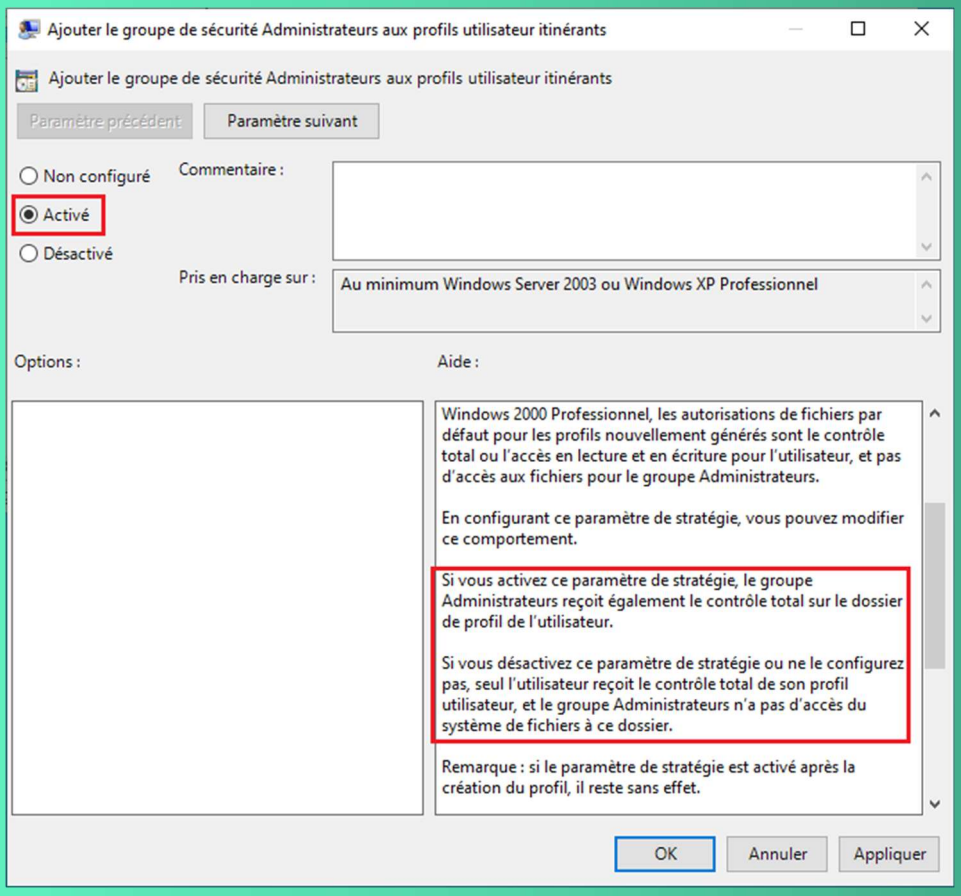


Recherchez sur la droite le paramètre nommé « Ajouter le groupe de sécurité Administrateurs aux profils utilisateur itinérants » et double-cliquez dessus.

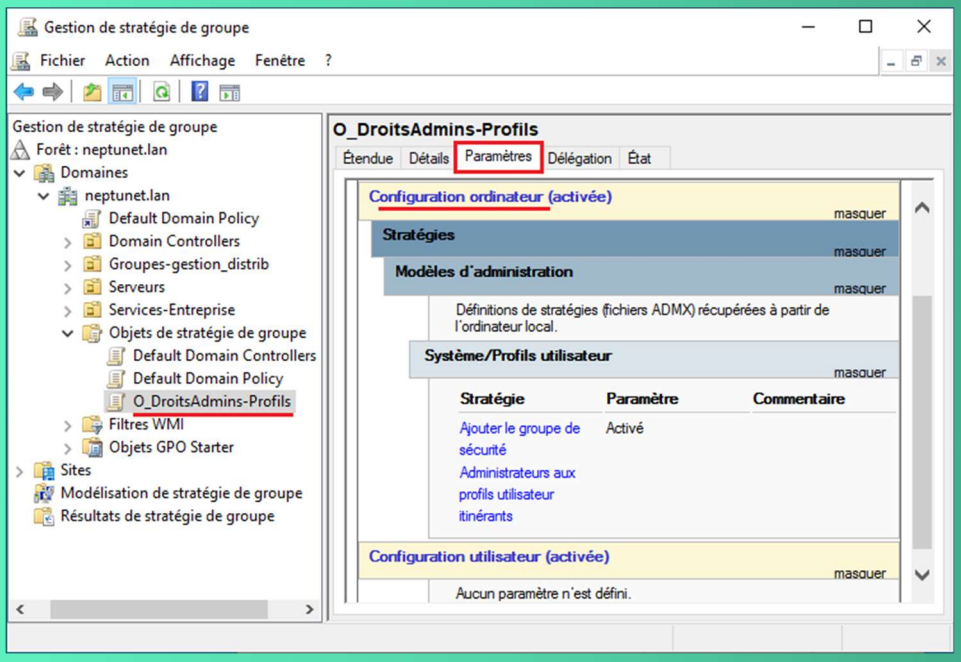


Si on regarde un peu dans la partie « Aide », il y a des infos intéressantes nous précisant ce qu'il se passe si on active ce paramètre, si au contraire on le désactive ou ne le configure pas. Nous voulons

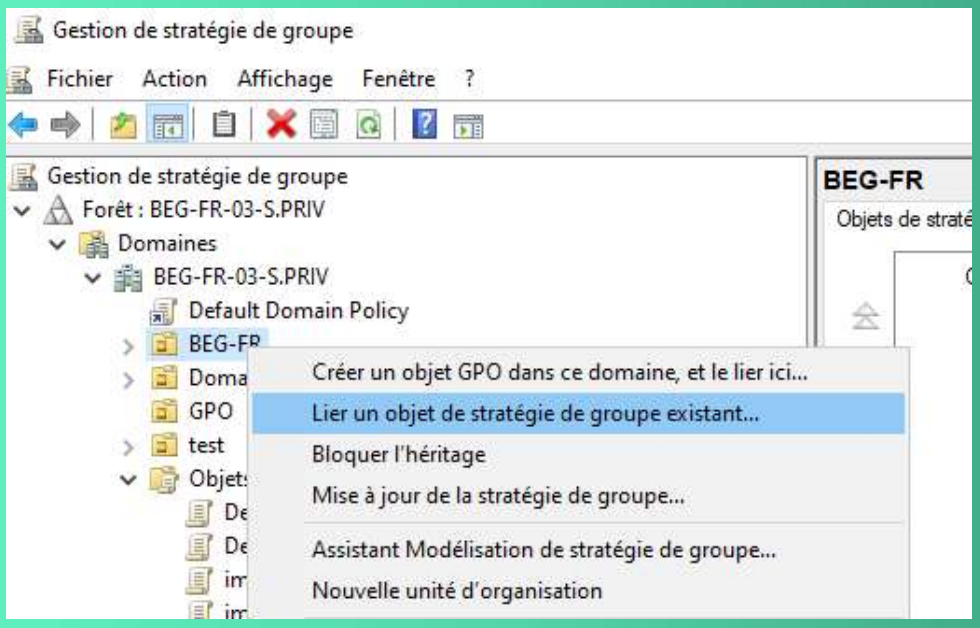
que les admins puissent accéder aux profils dont nous allons l'activer. Cochez la case « Activé » et cliquez sur OK.



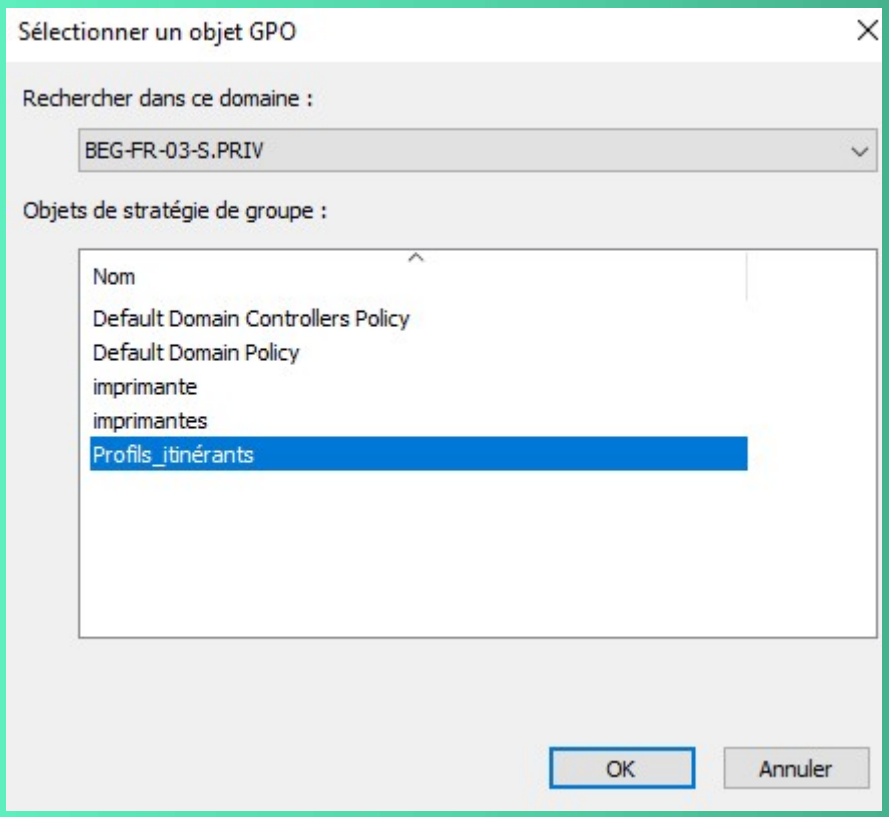
Vous pouvez fermer l'éditeur de stratégies et revenir sur la console de gestion des GPO. Si on jette un coup d'œil dans les paramètres de la GPO que l'on vient de créer, on voit bien ce qu'on a mis en place.



Il faut maintenant placer la GPO au bon endroit pour qu'elle fonctionne. Il faut que cette GPO s'applique sur tous les postes sur lesquels mes utilisateurs auront besoin de leur profil itinérant. Pour moi c'est simple, j'ai une OU qui regroupe mes utilisateurs et mes ordinateurs des différents services et qui s'appelle « BEG-FR ». C'est donc précisément ici que je vais la placer. Faites un clic droit sur votre OU puis « Lier un objet de stratégie de groupe existant ».



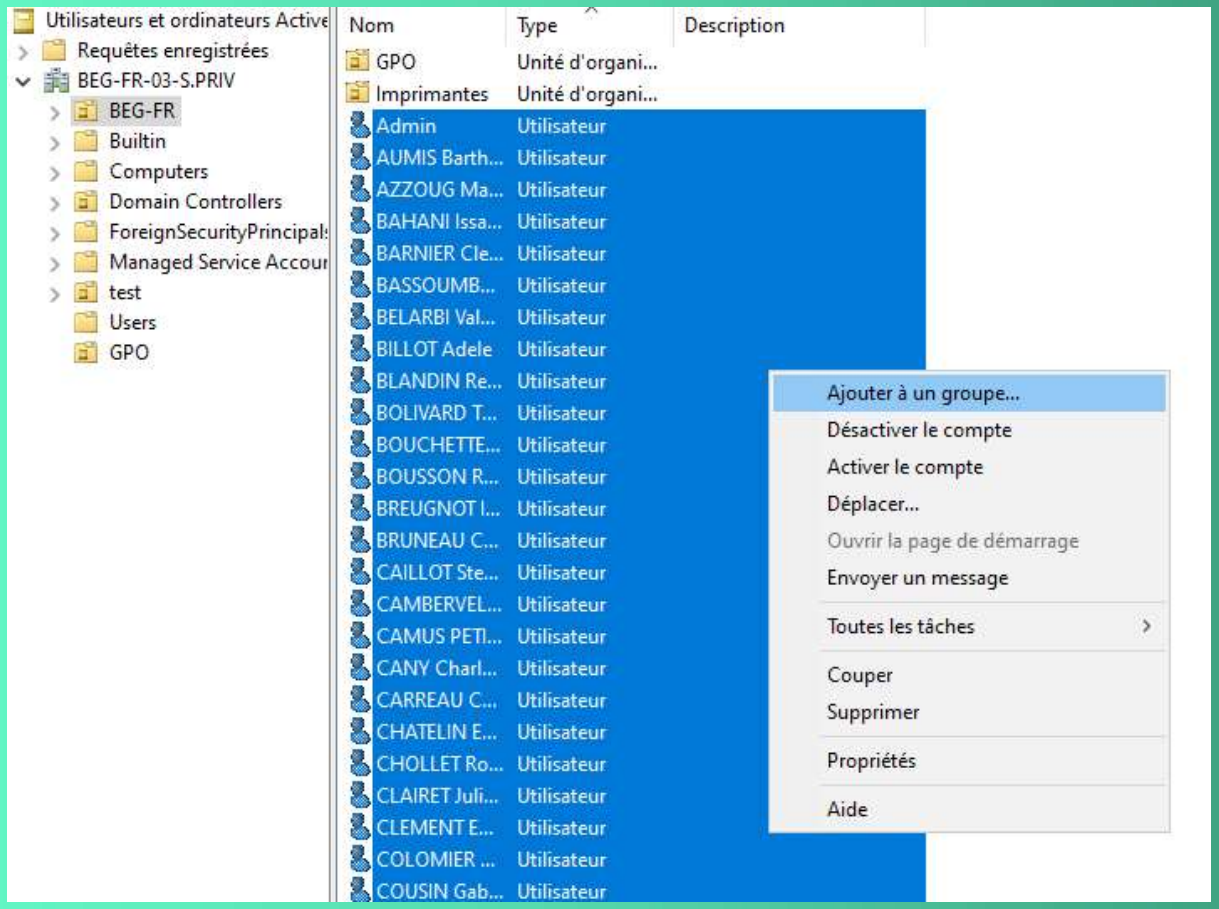
Choisissez dans la liste la GPO que vous venez de créer et cliquez sur OK.

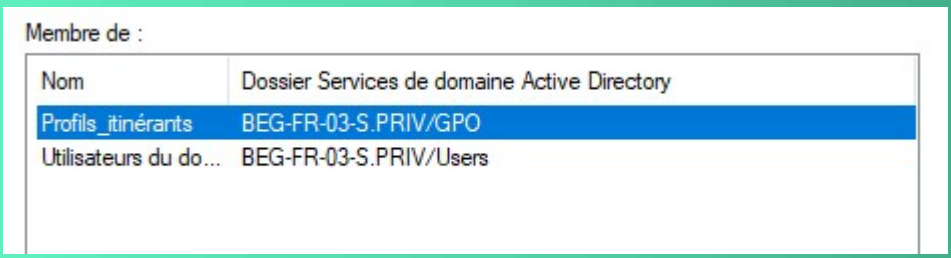


C'est tout ce qu'il y a à faire côté serveur AD pour le moment, passons à l'étape suivante.

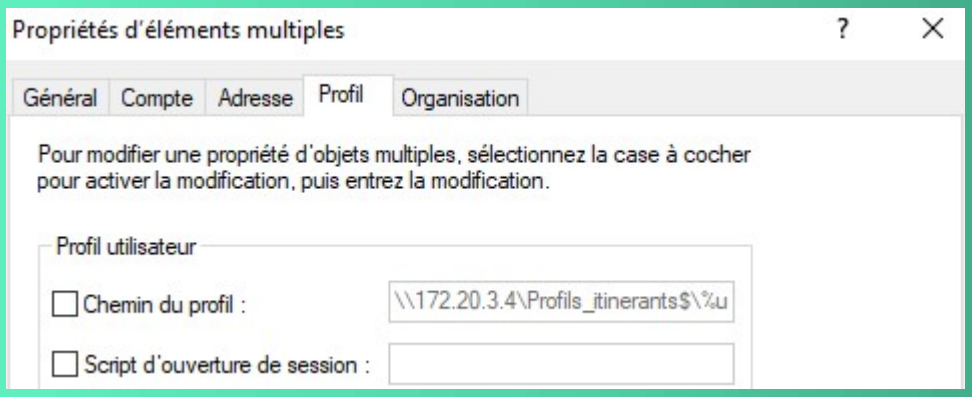
Définir un profil itinérant pour un utilisateur AD :

Retournons dans notre AD, faire un clic droit sur les utilisateurs que l'ont souhaite ajouté dans notre groupe puis faire un clic droit et 'ajouter à un groupe'





Rendez-vous ensuite dans l'onglet « Profil ». La partie qui nous intéresse ici dans le champ « Chemin du profil ».



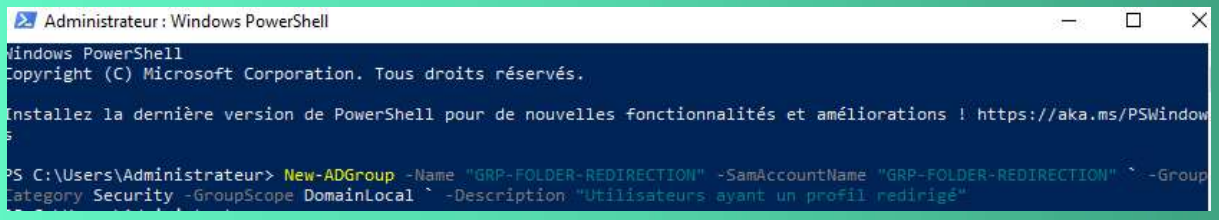
Il faut renseigner ici le chemin réseau du partage contenant les profils, suivi du nom du dossier de profil qui sera créé pour l'utilisateur lui-même et qui devra donc être unique. Pour éviter les problèmes, je vous conseille de nommer le dossier de profil comme le login de l'utilisateur (un login dans un domaine étant unique, cela limite le champ des erreurs). Vous pouvez utiliser la variable « %USERNAME% » pour récupérer directement le login de l'utilisateur. Dans mon cas, le chemin de profil que je vais saisir sera donc le suivant :

\\172.20.3.4\Profils_itinerants$\%username%

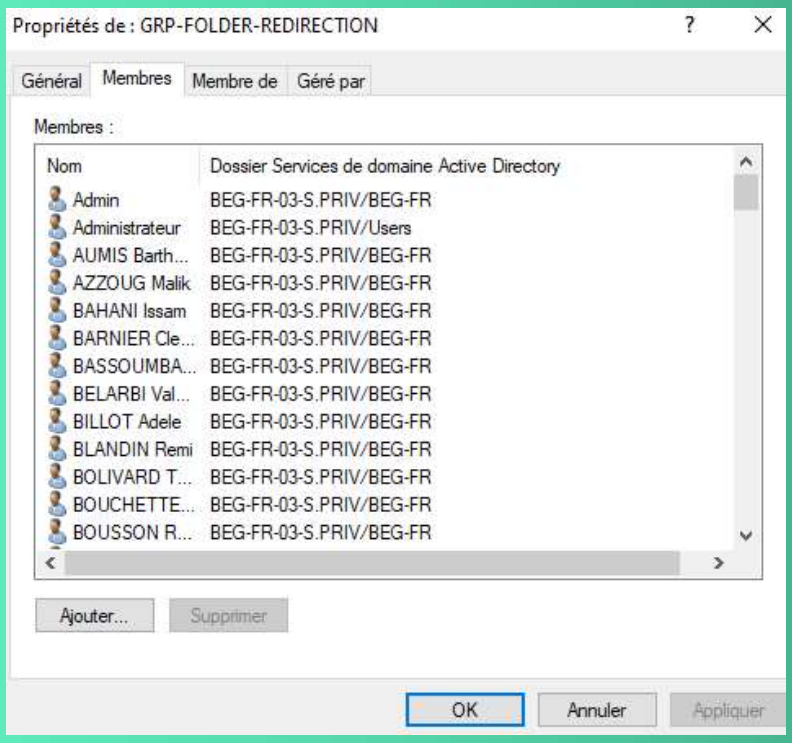
Cliquez sur Appliquer pour valider l'attribution d'un chemin de profil. La variable prendra automatiquement le login de l'utilisateur en cours de modification. Cliquez sur OK quand vous avez terminé. Il ne nous reste plus qu'à connecter l'utilisateur sur son PC pour voir ce que ça donne.

Redirection des dossiers :

Nous allons créer le groupe de sécurité "GRP-FOLDER-REDIRECTION" avec la commande suivante :
New-ADGroup -Name "GRP-FOLDER-REDIRECTION" -SamAccountName "GRP-FOLDER-REDIRECTION" ` -GroupCategory Security -GroupScope DomainLocal ` -Description "Utilisateurs ayant un profil redirigé"

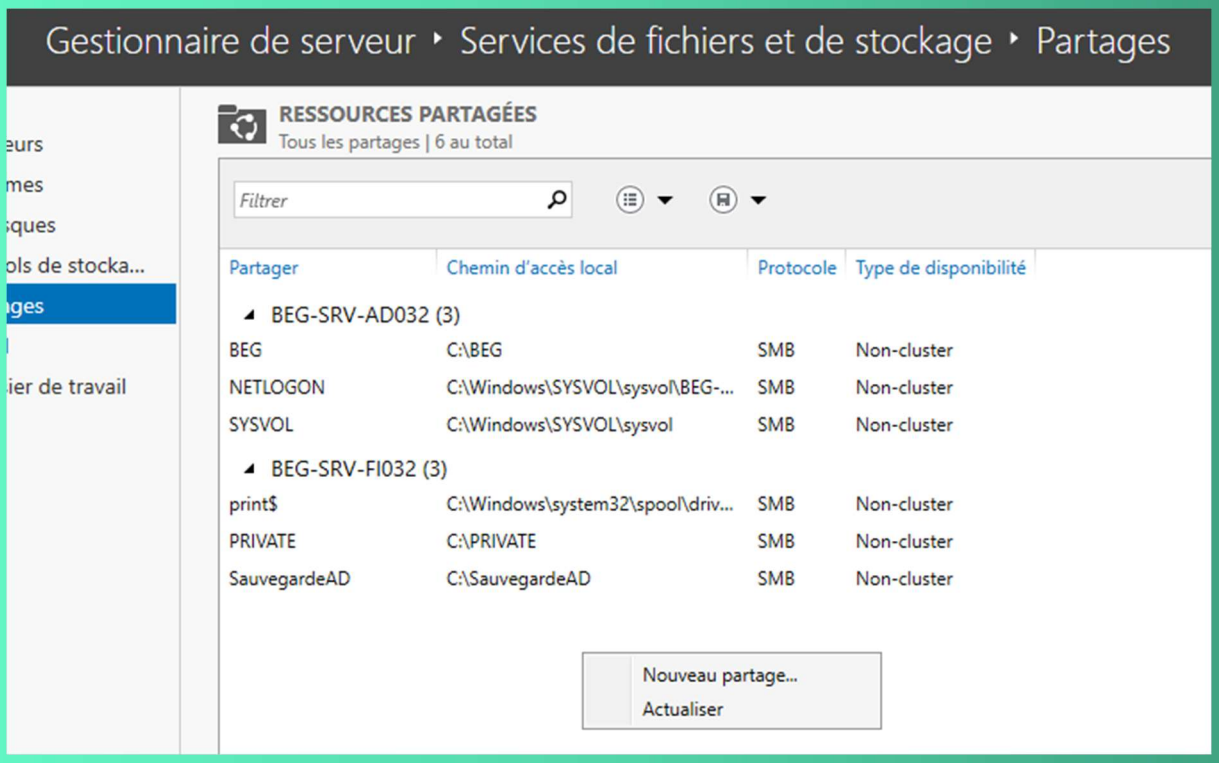


Pour l'ajout des utilisateurs au groupe, soit vous passez par la console AD, soit vous pouvez réaliser l'opération en PowerShell toujours :

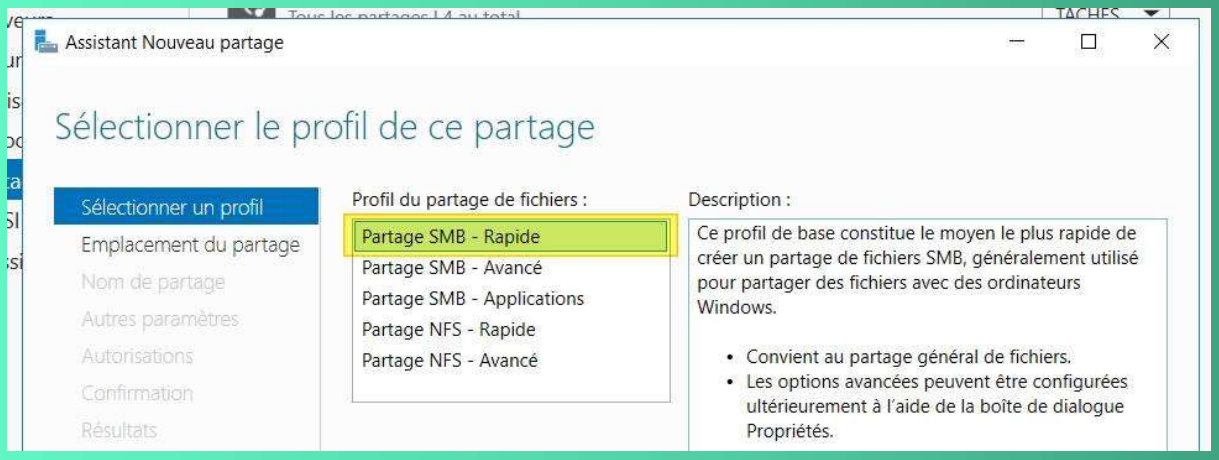


<u>Le partage et attribution des droits :</u>

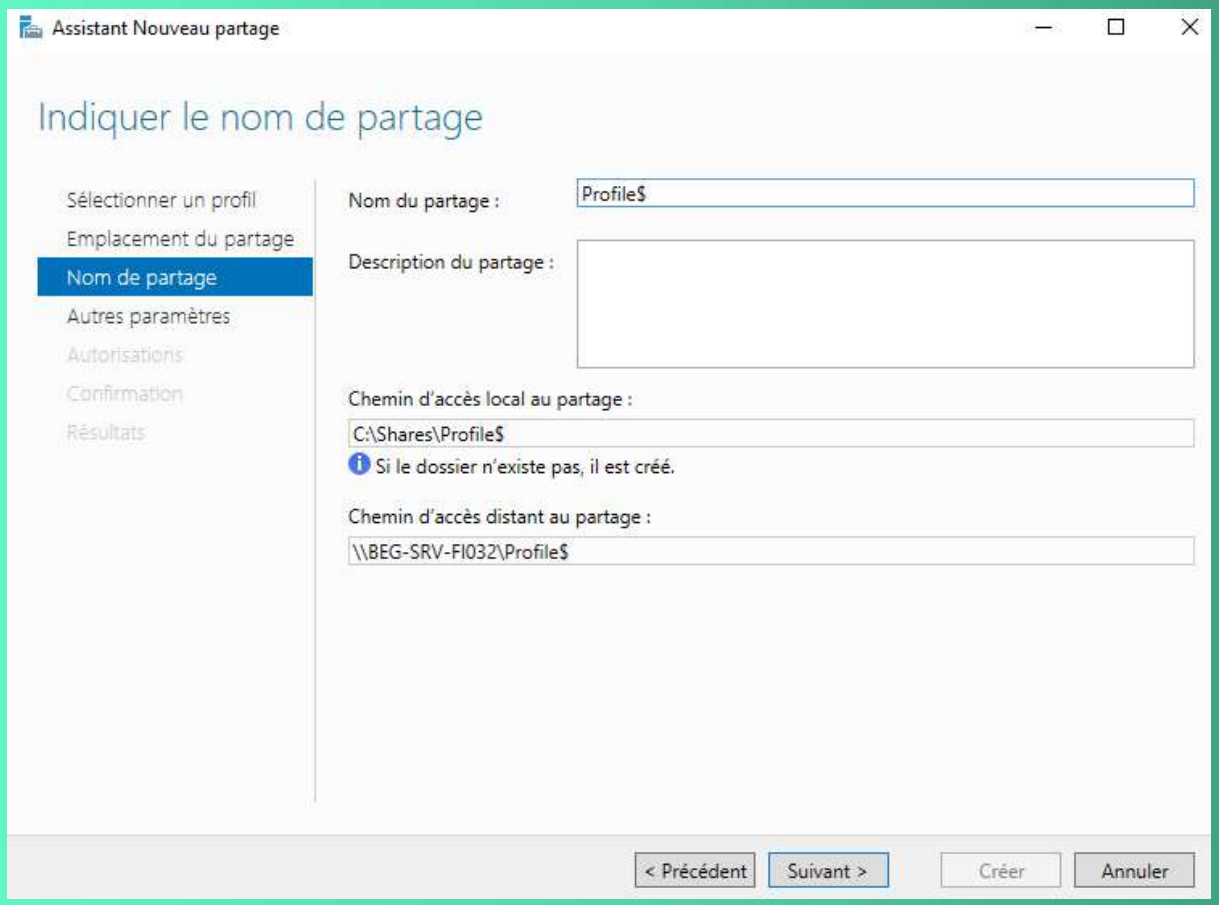
Dans la console "Gestionnaire de serveur", accédez à "Services de fichiers et de stockage" (vous devez installer la fonctionnalité) et ensuite créez un nouveau partage, comme ceci :



Pour faire de l'hébergement de fichiers comme nous le souhaitons, sélectionnez "Partage SMB - Rapide".



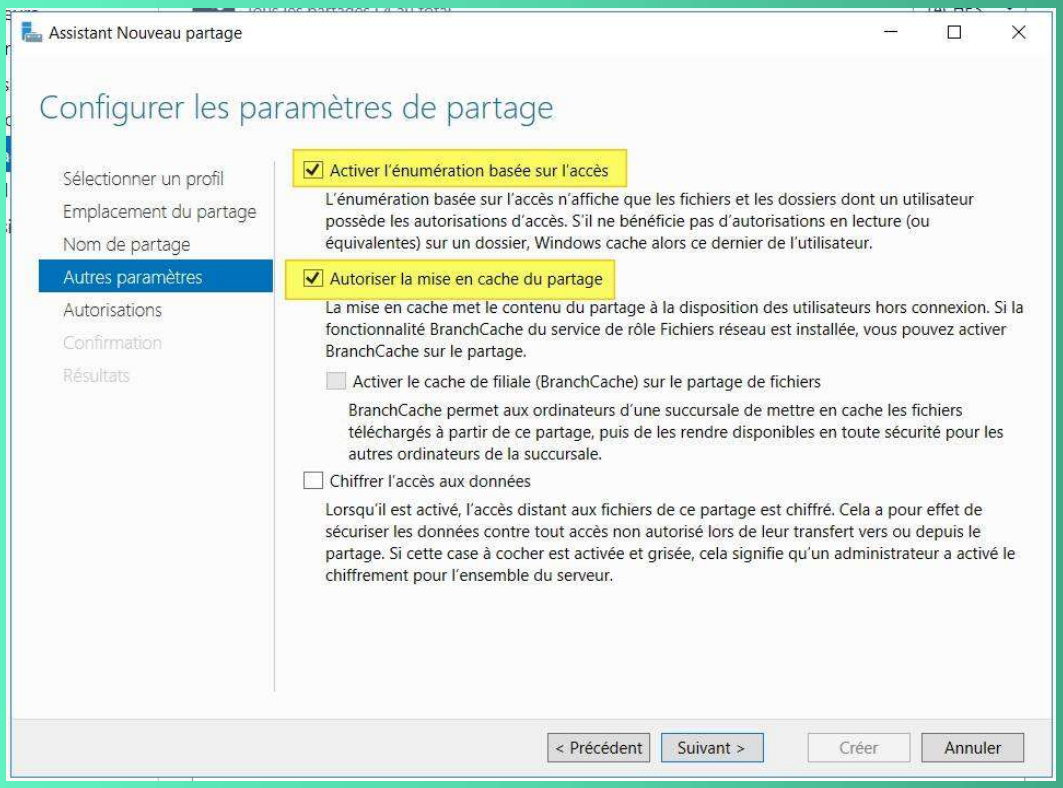
Donnez un nom à votre partage, par exemple : PrProfilsofiles$. Ce partage étant sensible et qu'il n'y a pas lieu d'y accéder en direct, notamment via la découverte réseau, je vous recommande de mettre un "$" à la fin du nom pour qu'il soit masqué un minimum.



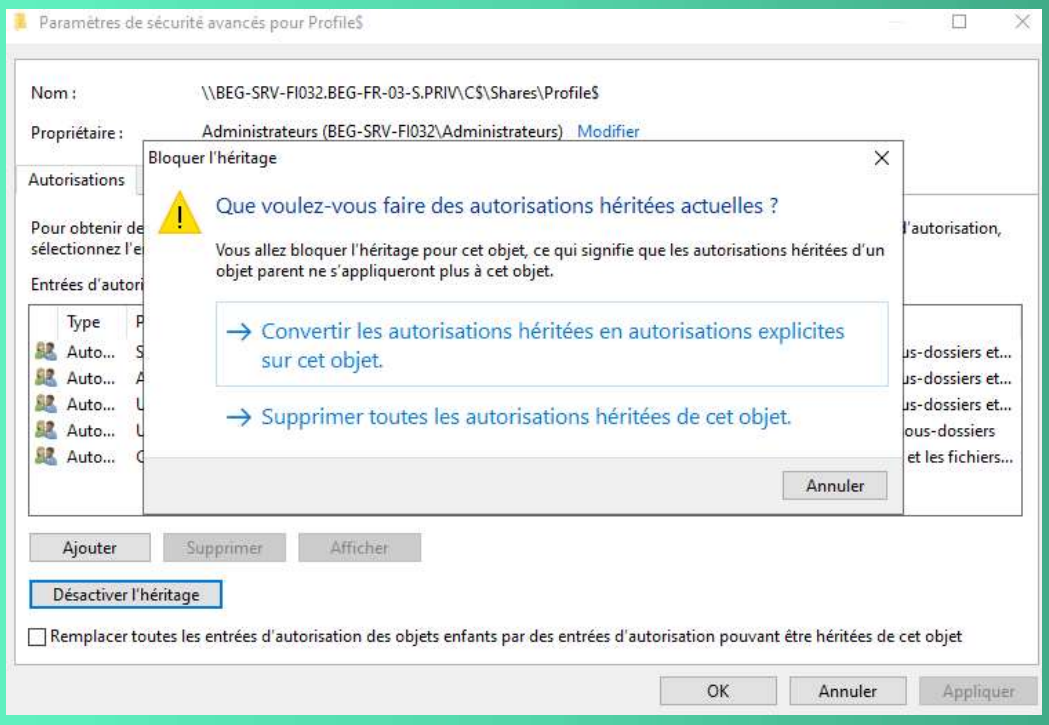
Deux options sont à activer sur cette page :

Activer l'énumération basée sur l'accès : l'utilisateur ayant les droits que sur son dossier "perso" alors il verra uniquement son dossier s'il parcoure le partage - l'affichage dans l'explorateur se base sur les droits de l'utilisateur.

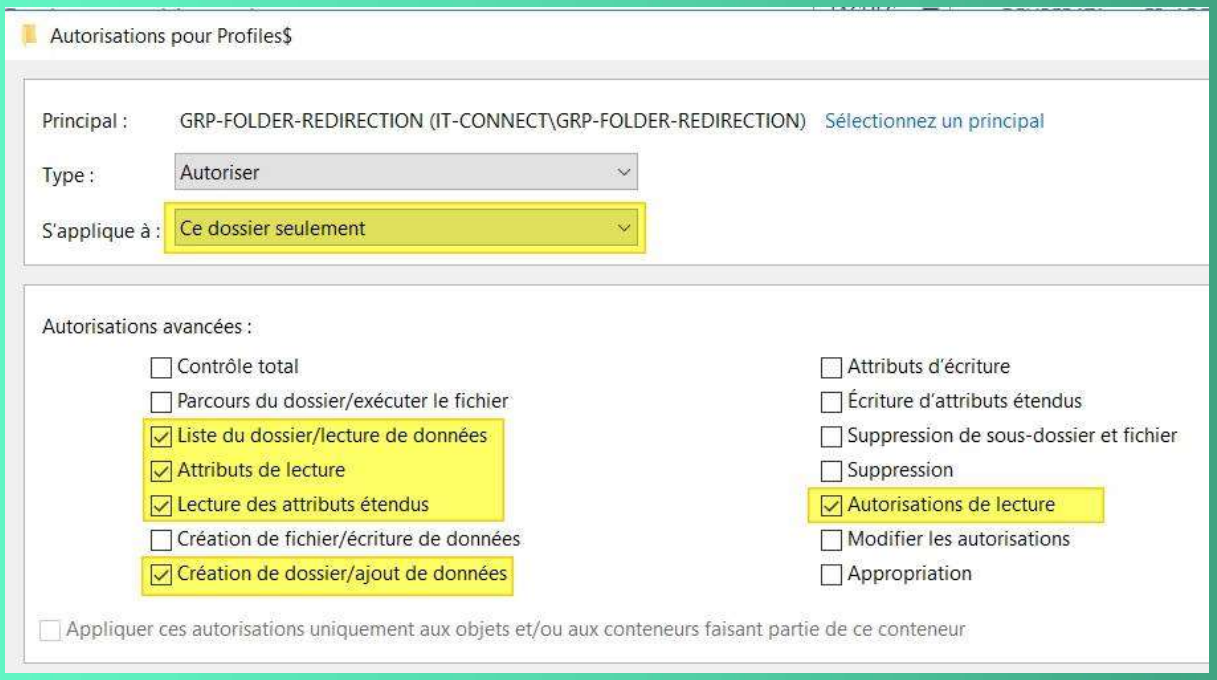
Autoriser la mise en cache du partage : cette option permettra à l'utilisateur d'utiliser la synchronisation des fichiers hors connexion sur ce partage pour que ses données soient synchronisées sur son poste. Sans cela, ce sera refusé par le serveur.



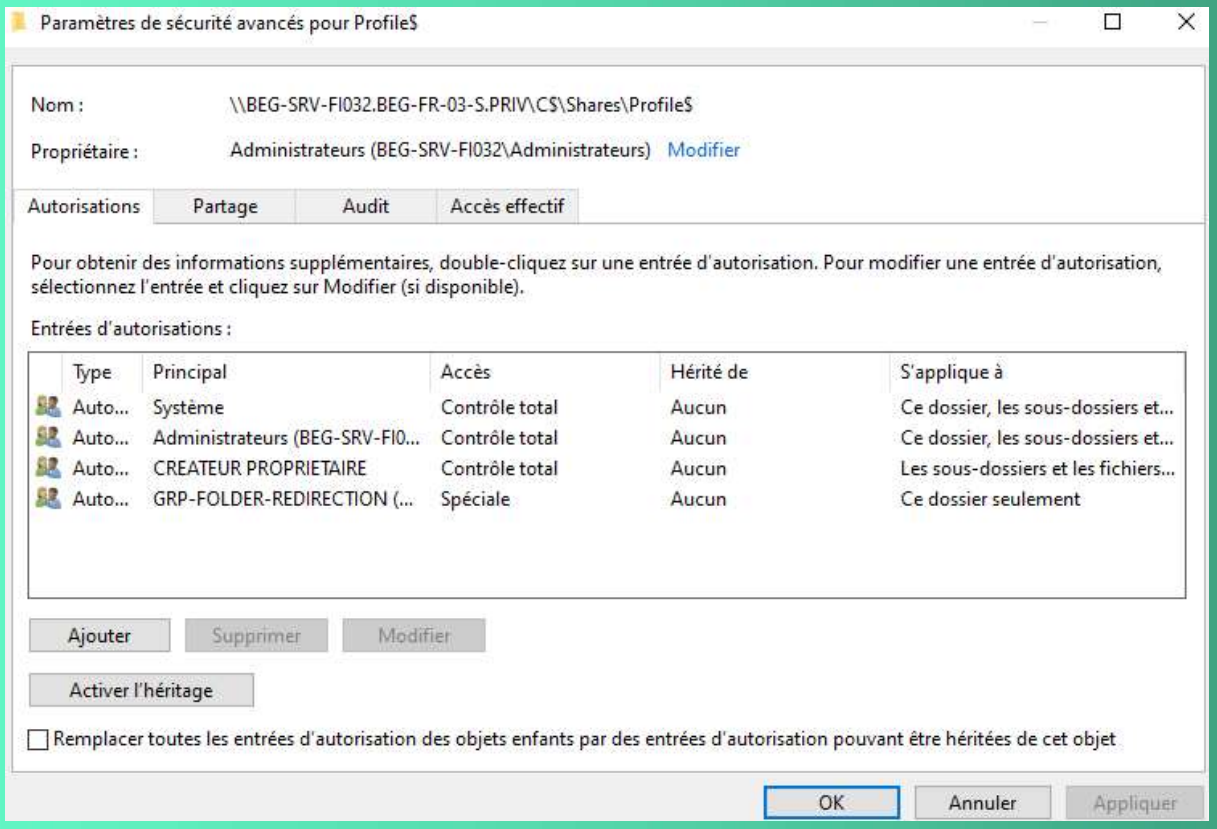
Il faut maintenant passer à l'étape la plus délicate : les autorisations NTFS. Nous allons donner les bons droits sur le partage afin que, lorsqu'un utilisateur se connecte, un dossier de profil puisse être généré (le nom sera son identifiant AD) et qu'il puisse écrire dans ce dossier. Il aura les droits exclusifs sur le dossier de son profil (+ l'administrateur) et ne pourra pas accéder aux autres dossiers de profils. Commencez par cliquer sur "Désactiver l'héritage" et cliquez sur "Convertir les autorisations héritées en autorisations explicites sur cet objet" pour récupérer les droits actuels. Nous allons les faire évoluer.



Maintenant, ajoutez des autorisations pour le groupe "GRP-FOLDER-REDIRECTION" et configurez comme ceci :

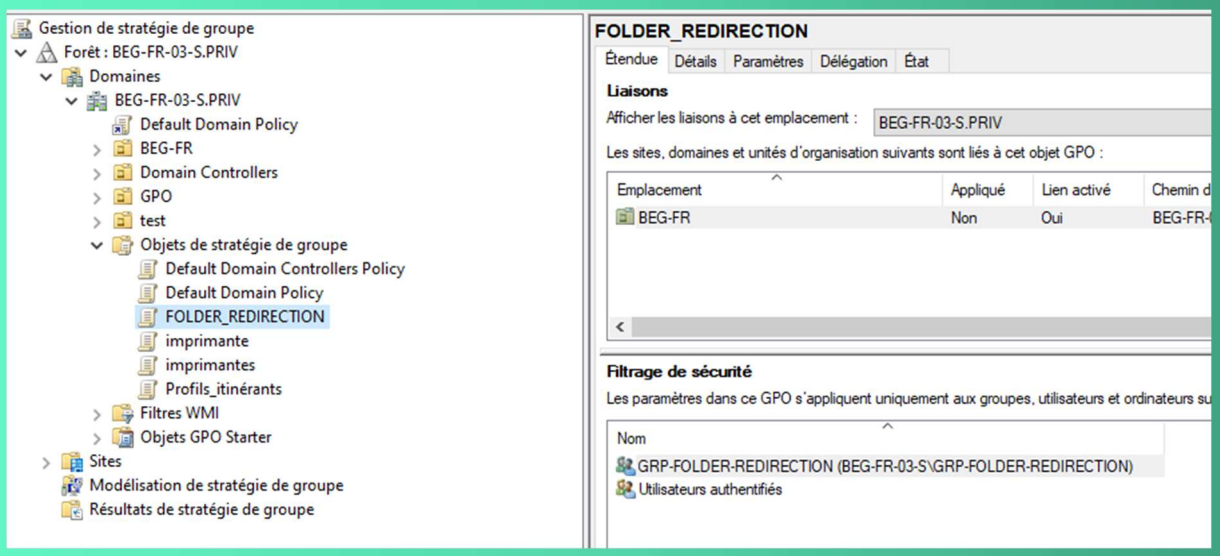


Au final, vous devez avoir les droits identiques à ceux ci-dessous (attention au champ "S'applique à") :

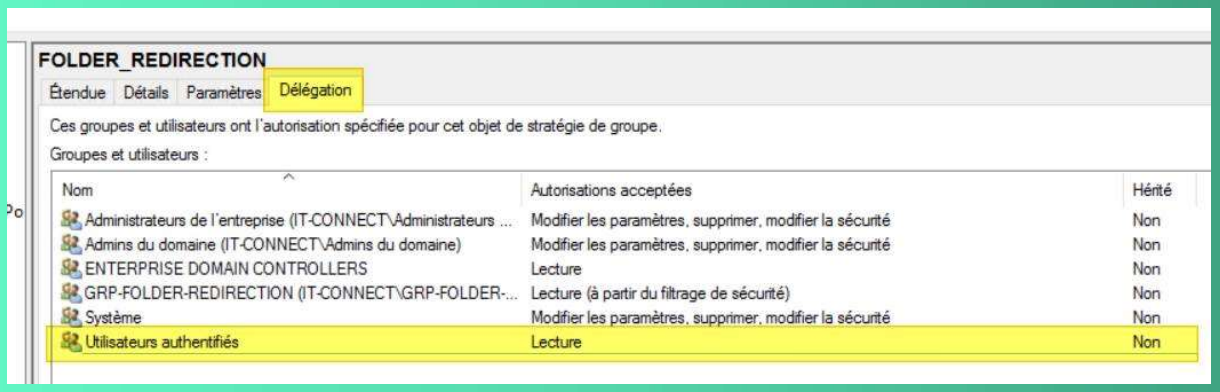


La GPO de redirection de dossiers :

Avant de procéder aux tests, nous devons créer la GPO et la configurer. Via la console "Gestion de stratégie de groupe", créez une nouvelle GPO nommée "FOLDER_REDIRECTION" (par exemple) et modifiez le filtrage de sécurité pour qu'il y ait le groupe "GRP-FOLDER-REDIRECTION" seulement, comme ceci :

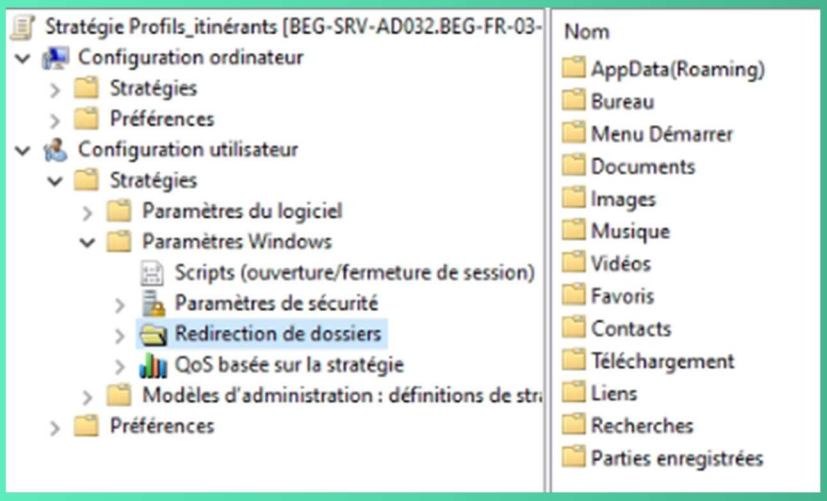


Suite à une mise à jour publiée par Microsoft (MS16-072), il y a eu des changements au niveau de la sécurité et pour que la redirection de profils fonctionne, vous devez ajouter le groupe "Utilisateurs authentifiés" en "Lecture" dans l'onglet "Délégation" :



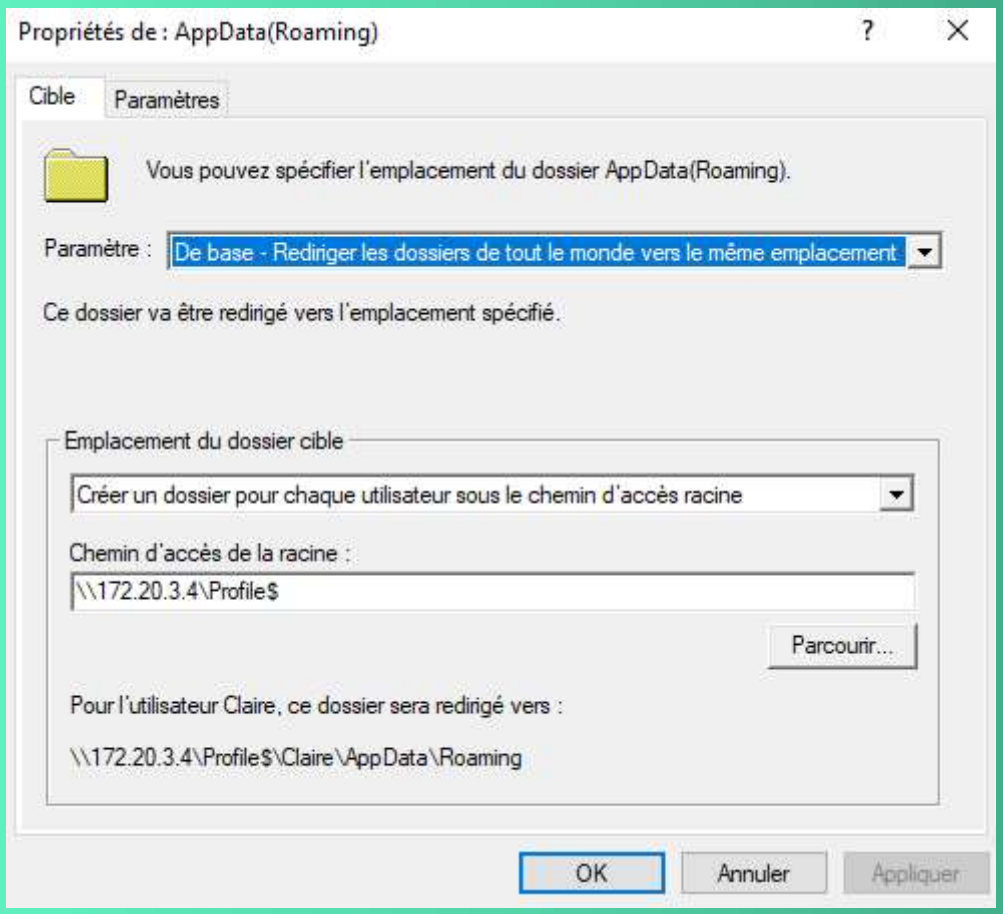
Ensuite, modifiez la GPO pour configurer la redirection de dossiers. Ce paramètre s'applique directement au niveau de l'utilisateur : Configuration utilisateur > Stratégies > Paramètres Windows > Redirection de dossiers

Pour l'exemple, je vais seulement le faire pour les documents mais la procédure est identique à chaque fois. Cliquez droit sur "Documents" et "Propriétés".



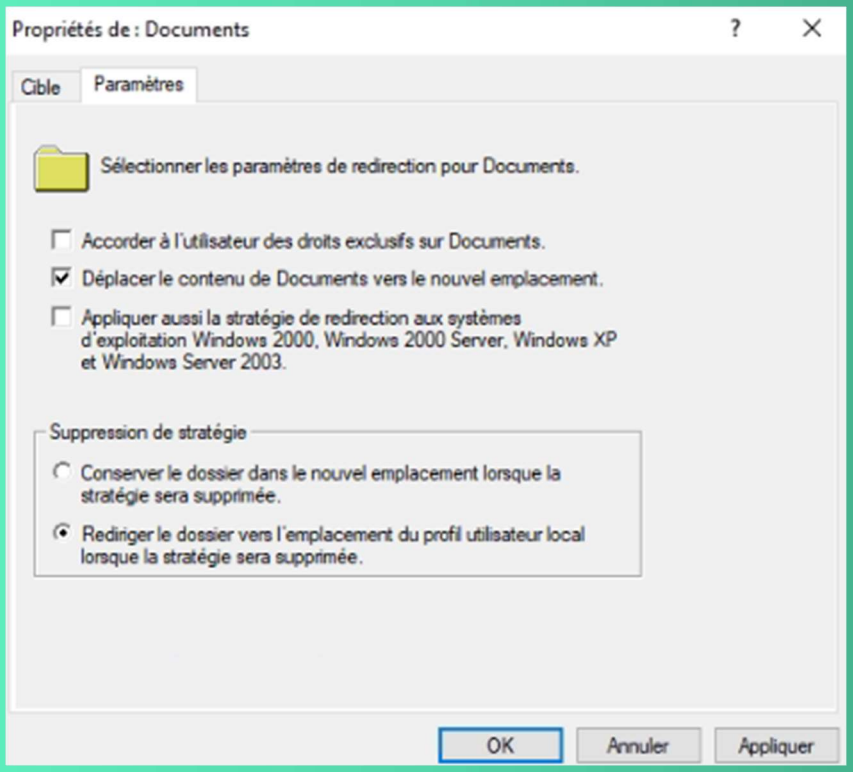
Choisissez l'option "Créer un dossier pour chaque utilisateur le chemin d'accès racine", ce qui rejoins ce que je disais précédemment : à la racine du partage des profils, un dossier va être créé pour l'utilisateur et dans ce dossier, il y aura un dossier "Documents".

Indiquez le chemin complet vers le partage dans le champ "Chemin d'accès à la racine".



Avant de valider, jetez un œil à l'onglet "Paramètres" pour le configurer comme ceci :

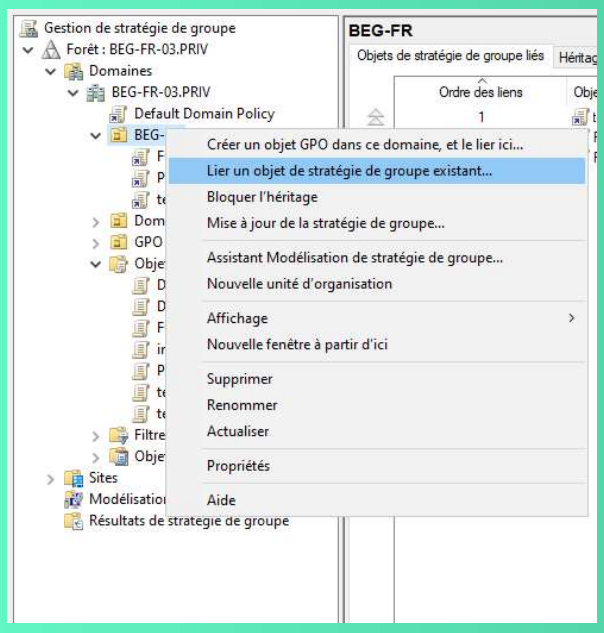
Si vous souhaitez empêcher le compte administrateur d'accéder au dossier et qu'il y ait seulement l'utilisateur qui puisse accéder, alors cochez l'option "Accorder à l'utilisateur des droits exclusifs sur Documents".



Je le fais pour tous les dossiers sauf Vidéos, je ne souhaite pas que les vidéos soient conservées sur le serveur de fichier.

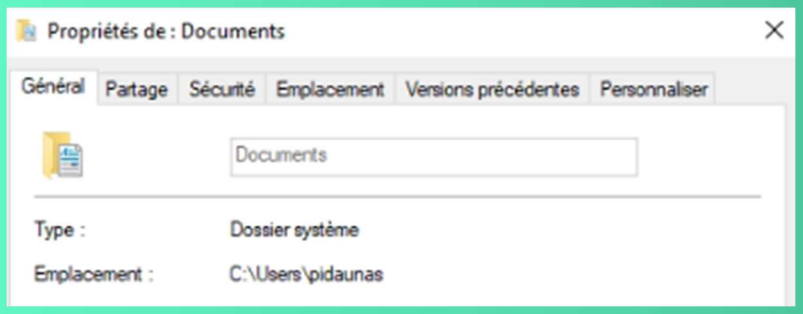
Vous pouvez valider, fermer l'éditeur de GPO et pensez à lier votre GPO sur votre domaine avant de passer à la phase de tests.

Mettre dans ‘‘Gestion de stratégie de groupe’’ la GPO ‘’FOLDER_REDIRECTION’’



Test de redirection de dossiers :

Pour ma part, je passe donc sur un poste client Windows 10 pour tester la redirection de dossiers. Actuellement, on peut voir quand lorsque je regarde les propriétés d'un fichier dans "Documents", il est stocké en local comme le confirme l'emplacement.



Maintenant, vous allez ouvrir une invite de commandes en tant qu'administrateur sur le poste (ou PowerShell) et actualiser les GPO :

```
U:\>gpupdate /force
```

Logiquement, la commande va vous avertir qu'il y a une redirection de dossiers configurée et que pour l'appliquer il faut fermer la session, vous pourrez valider avec "O" puis la touchée Entrée.

Reconnectez-vous avec le même utilisateur. On peut voir que dans "Documents" les fichiers sont toujours là sauf qu'ils sont maintenant stockés sur le serveur directement !

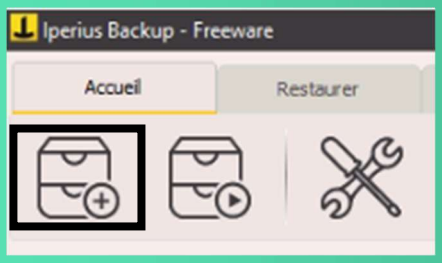
CONFIGURATION DE IPERIUS

Pour installer Iperius, il faut aller sur le site officiel et télécharger l'éxécutable :

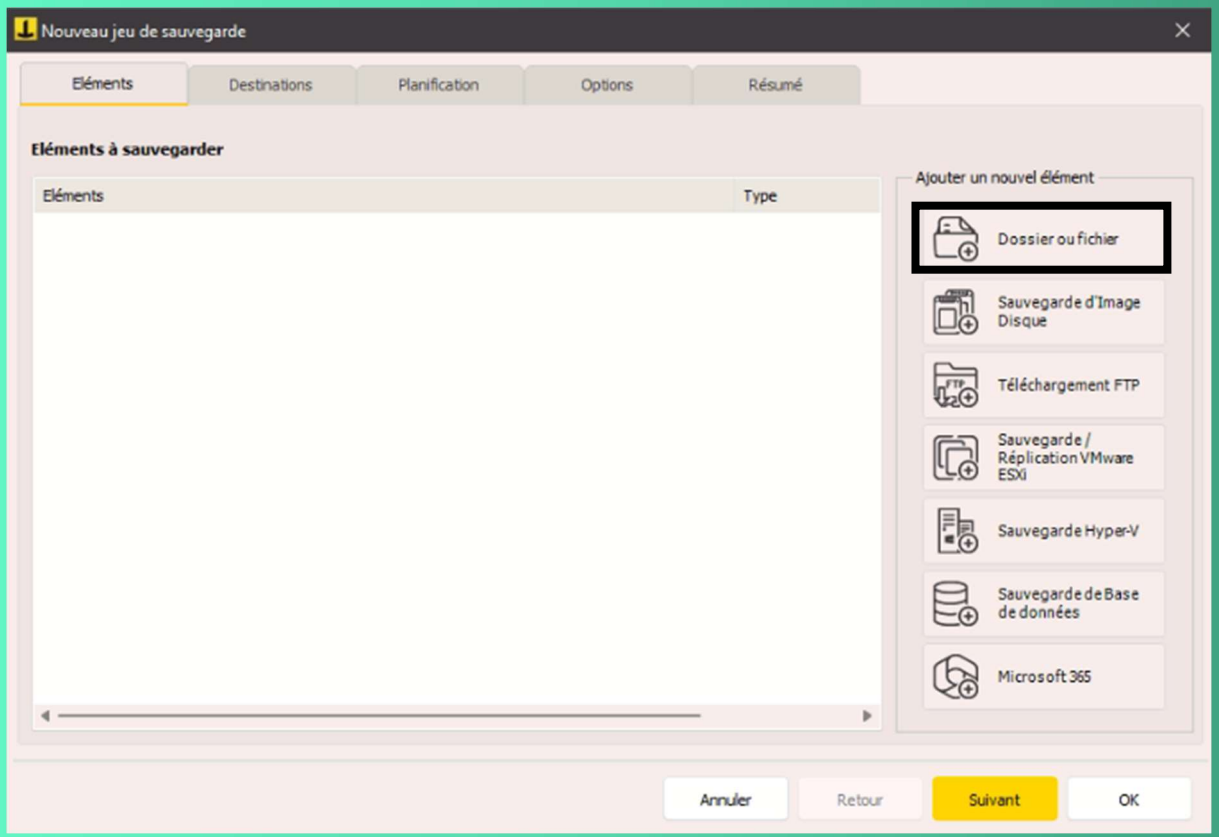
https://www.iperiusbackup.fr/

Créer une sauvegarde :

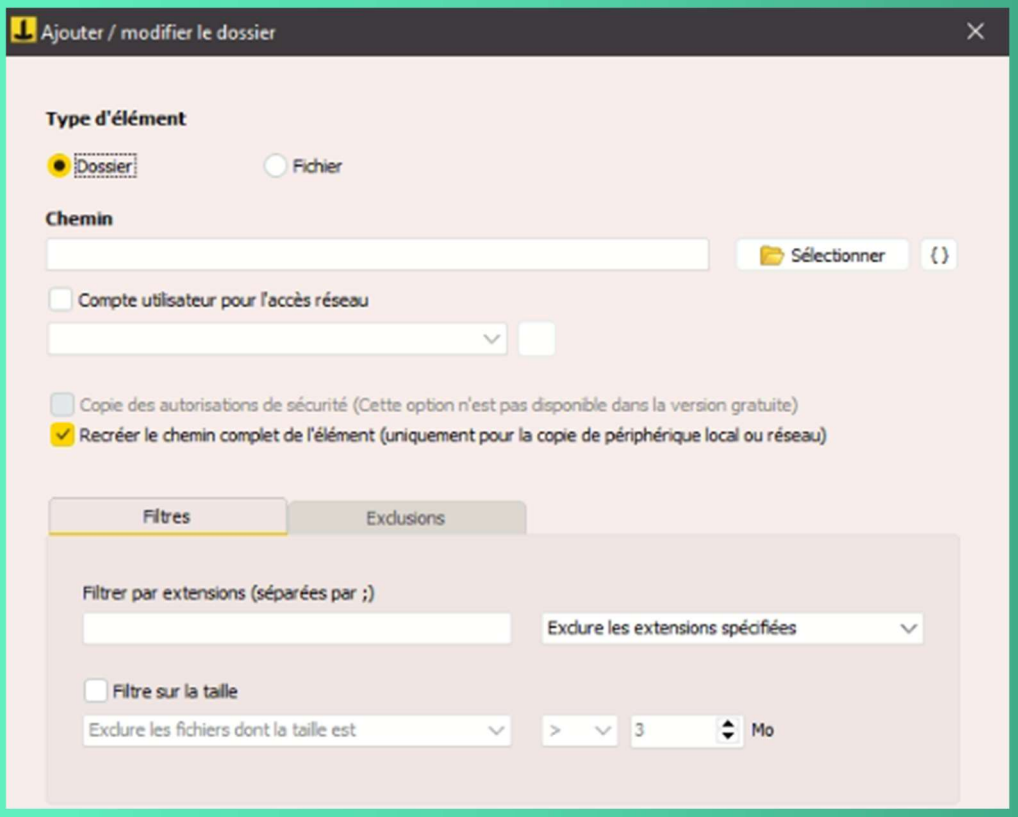
Pour créer une sauvegarde sur Iperius, il faut cliquer sur 'créer un nouveau jeu de sauvegarde'



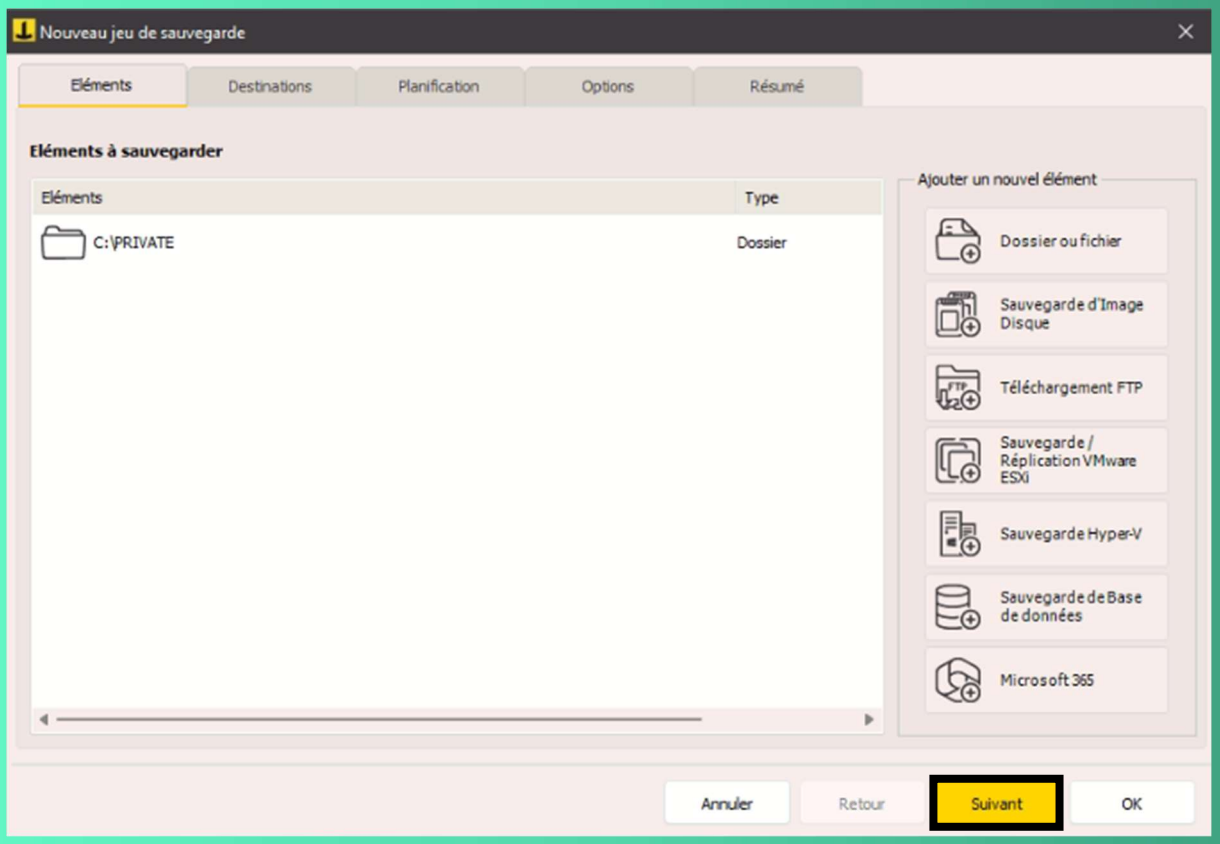
Ensuite, sélectionner le nouvel élément de sauvegarde en fonction de ce que nous voulons sauvegarder. Dans notre cas, nous avons sauvegardé un dossier :



Apres avoir cliquer sur ‘Dossier ou fichier’, entrer le chemin du dossier que nous souhaitons sauvegarder.

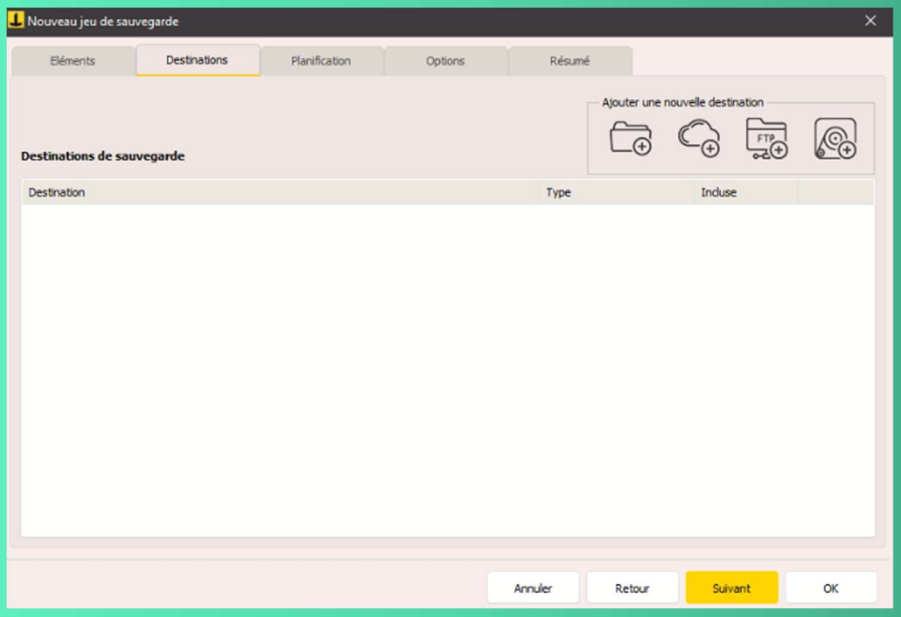


Maintenant que le chemin de notre dossier private à sauvegarder est créé, cliquer sur ‘suivant’

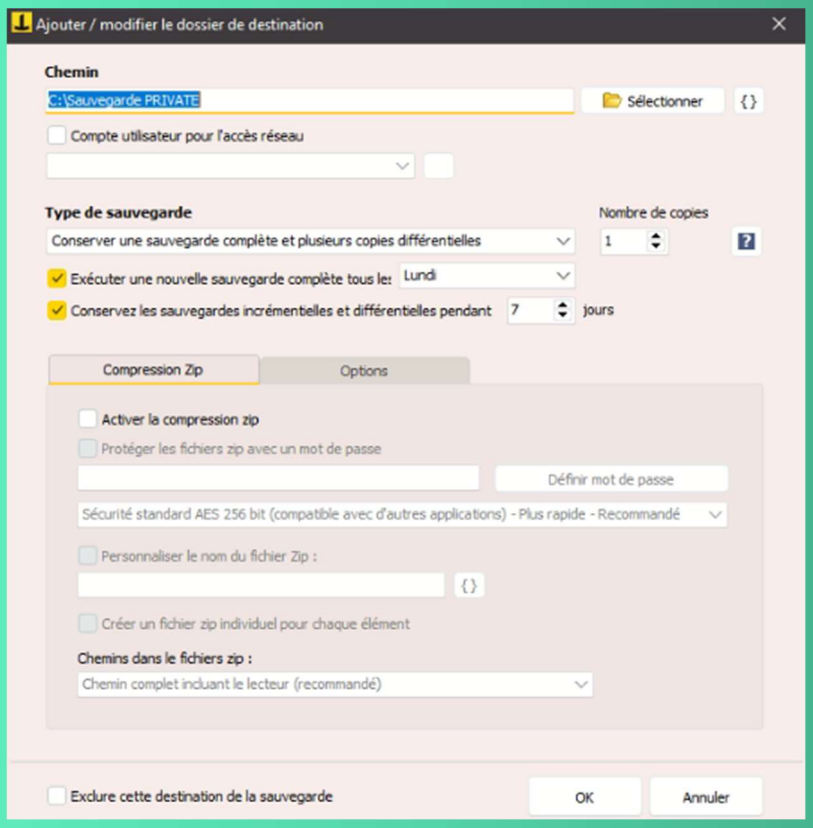


Choisir le dossier de sauvegarde :

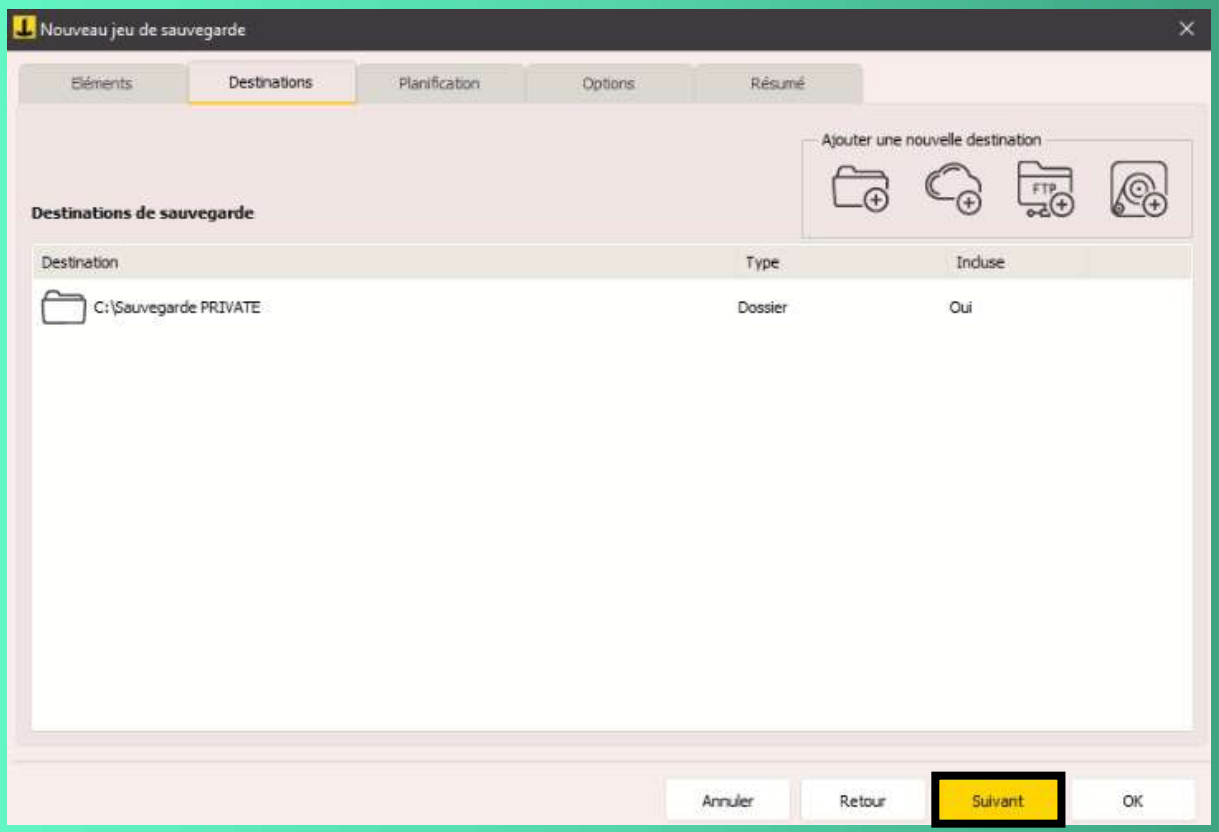
Pour choisir un dossier ou la sauvegarde sera enregistrer, cliquer sur ‘Ajouter un dossier de destination’, il est aussi possible de faire une sauvegarde sur le cloud, sur un serveur FTP ou alors une bande



Ensuite, sélectionner le chemin de sauvegarde, ainsi que le type de sauvegarde que vous souhaitez. Nous avons choisi de conserver une sauvegarde complète tous les lundis et de conserver plusieurs copies différentielles durant 7 jours

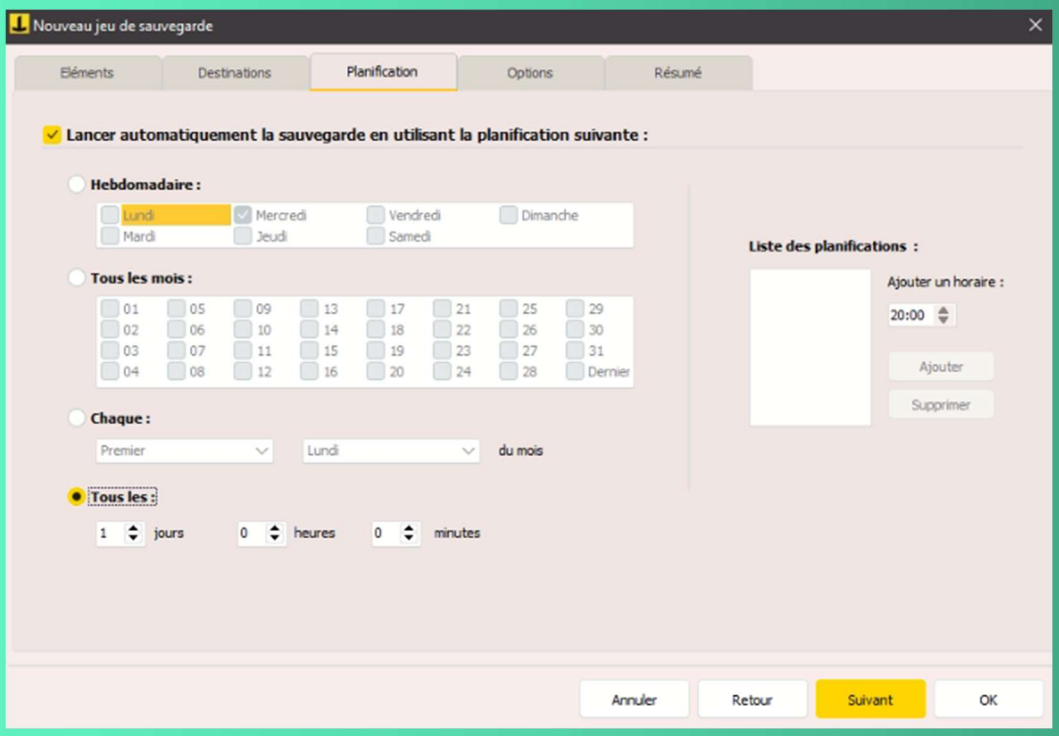


Maintenant que le chemin du dossier de sauvegarde est créé, cliquer sur ‘suivant’



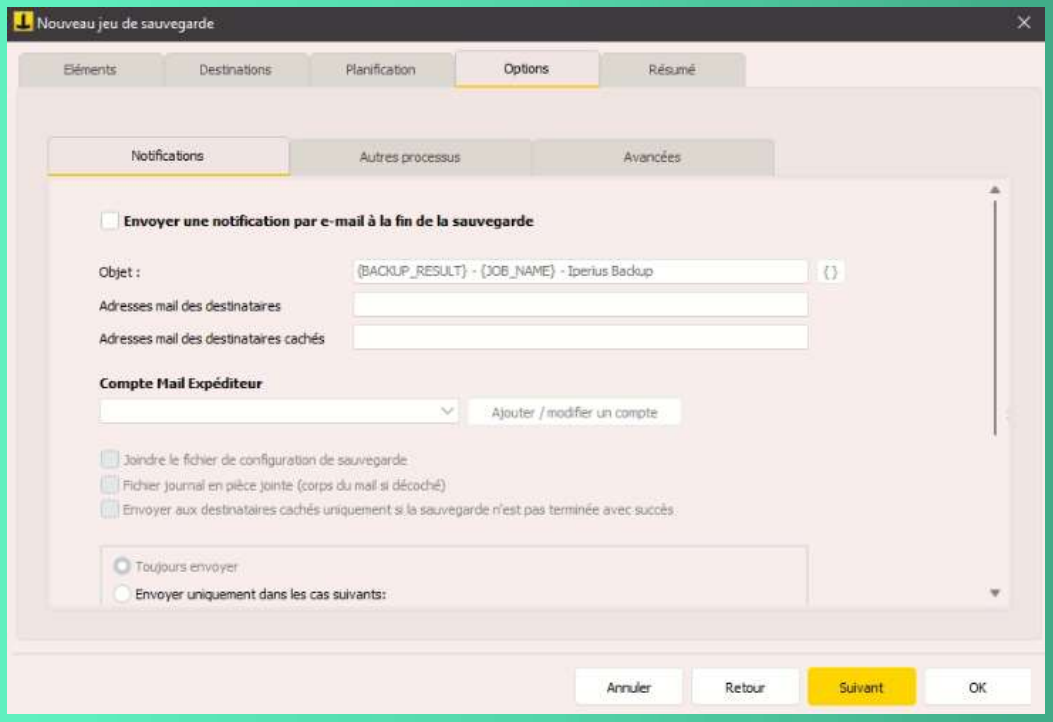
Planification :

Planifier le lancement automatique de la sauvegarde en fonction de vos choix :



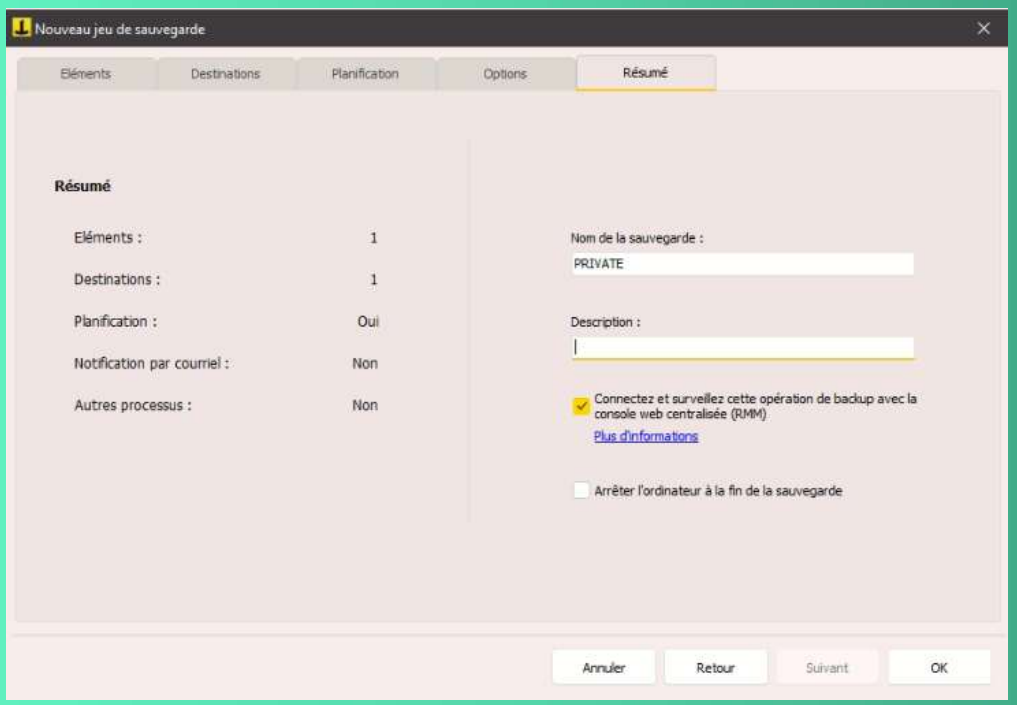
Options :

Sélectionner les options comme l'envoi d'un mail à la fin d'une sauvevarde, ou alors l'éxécution d'un script avant ou après la sauvegarde.



Résume :

Vérifiez le nom de la sauvegarde ect puis cliquer sur 'ok' pour valider la sauvegarde



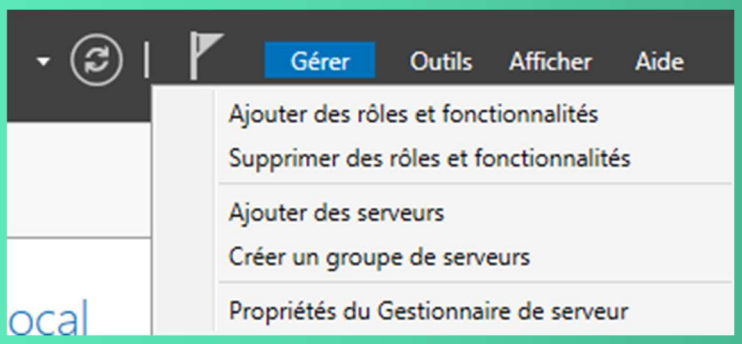
Test de la sauvegarde :

Pour tester la sauvegarde, faire un clic droit et ‘lancer la sauvegarde’

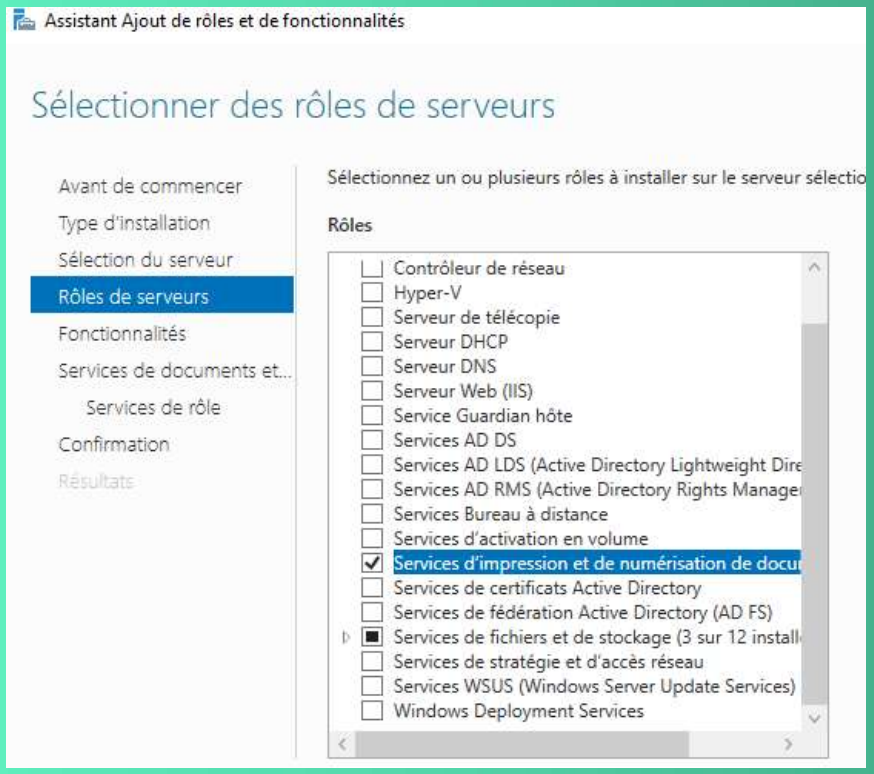
CONFIGURATION DU SERVEUR D'IMPRESSION

Installation du service :

Les ressources de votre serveur d'impression seront à définir en fonction du nombre d'utilisateurs et du nombre d'imprimantes à gérer. Pour commencer l'installation, connectez-vous à votre serveur Accédez au gestionnaire de serveur, cliquez sur 'Gérer' puis sur 'Ajouter des rôles et fonctionnalités'.

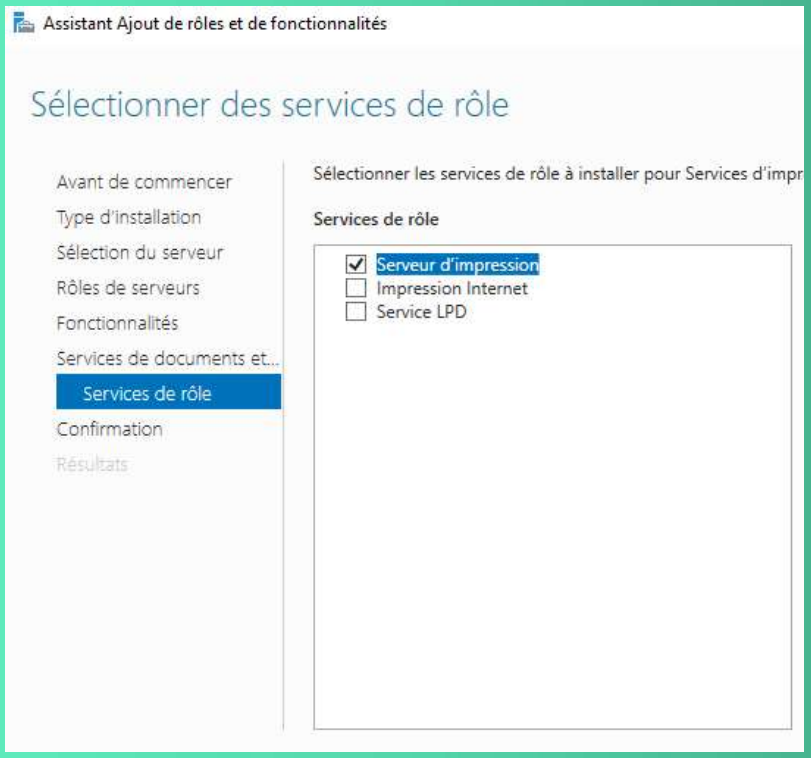


Passez les premières étapes, sélectionnez le rôle 'Services d'impression et de numérisation de documents'



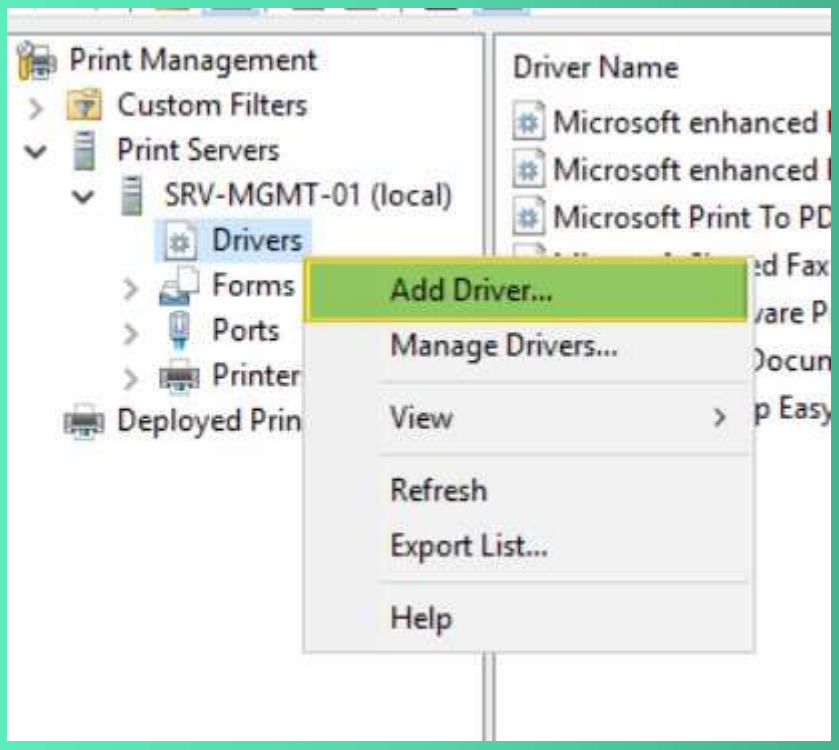
Au niveau des rôles du service d'impression, cochez à minima "Server d'Impression" qui est le serveur d'impression de base. Si vous envisagez de réaliser des impressions depuis des périphériques

Unix ou Android, cochez également "LPD Service" afin d'installer ce service complémentaire qui sera utile dans ce cas. Poursuivez jusqu'au lancement de l'installation...

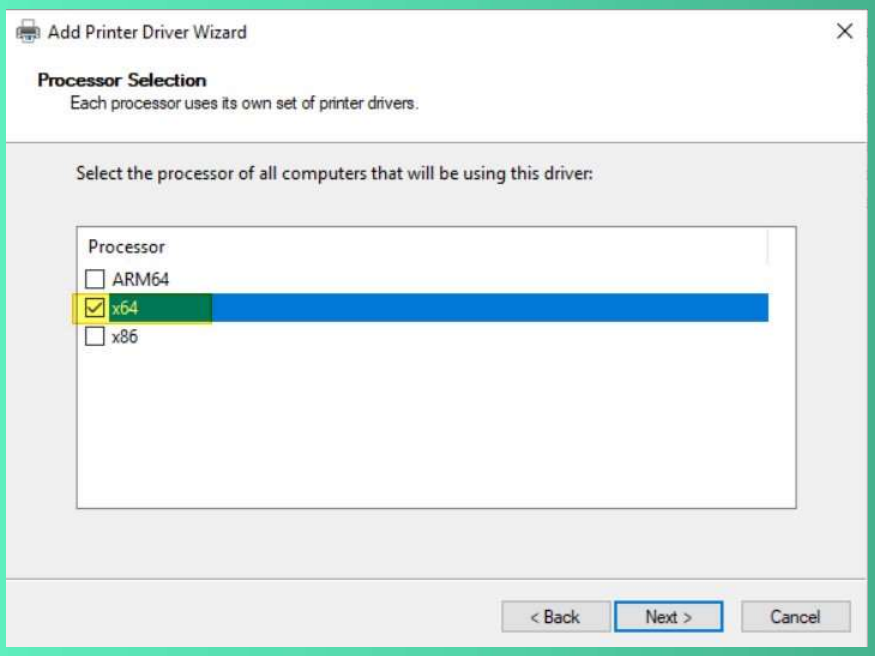


Ajouter un pilote d'impression :

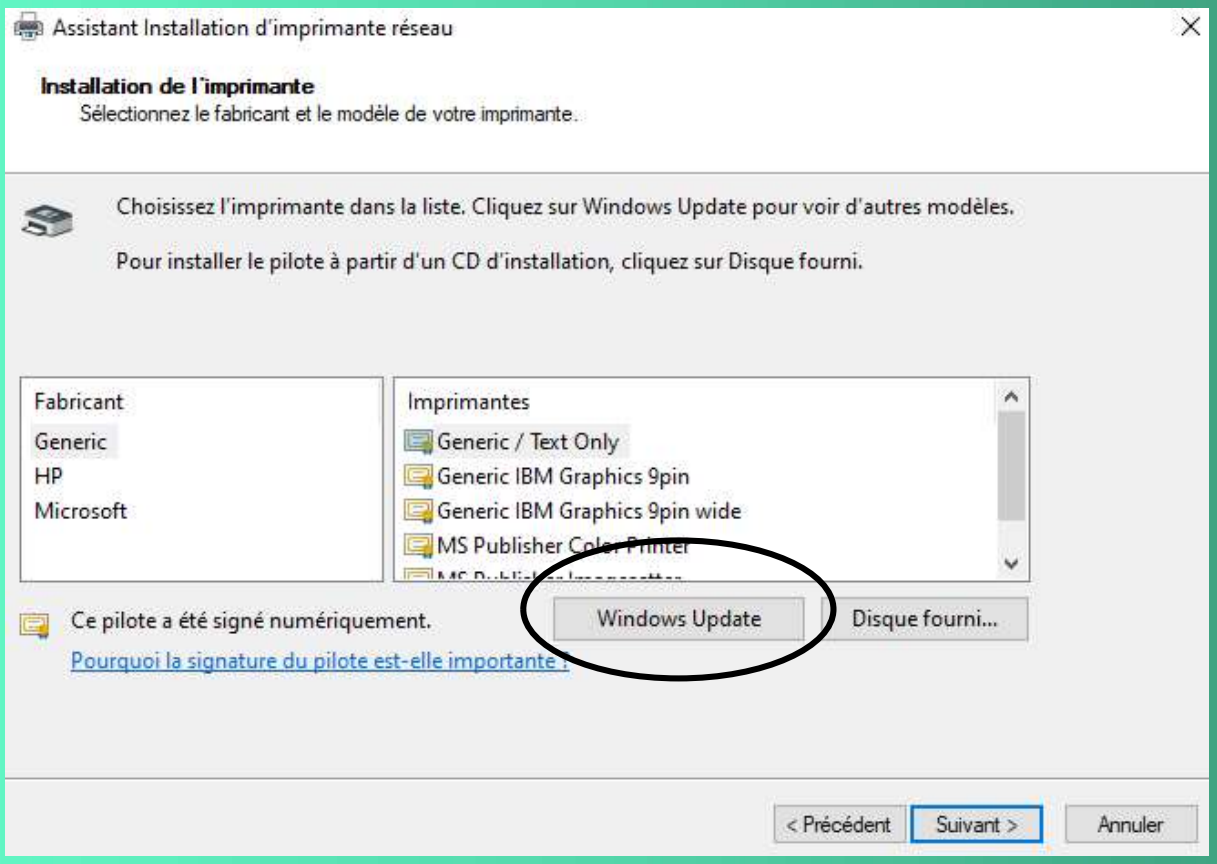
Pour commencer, nous allons donc importer notre pilote sur le serveur d'impression. Ce qui s'effectue de cette manière : Serveurs d'impression > nom de votre serveur > clic droit sur "Pilotes" et "Ajouter un pilote".



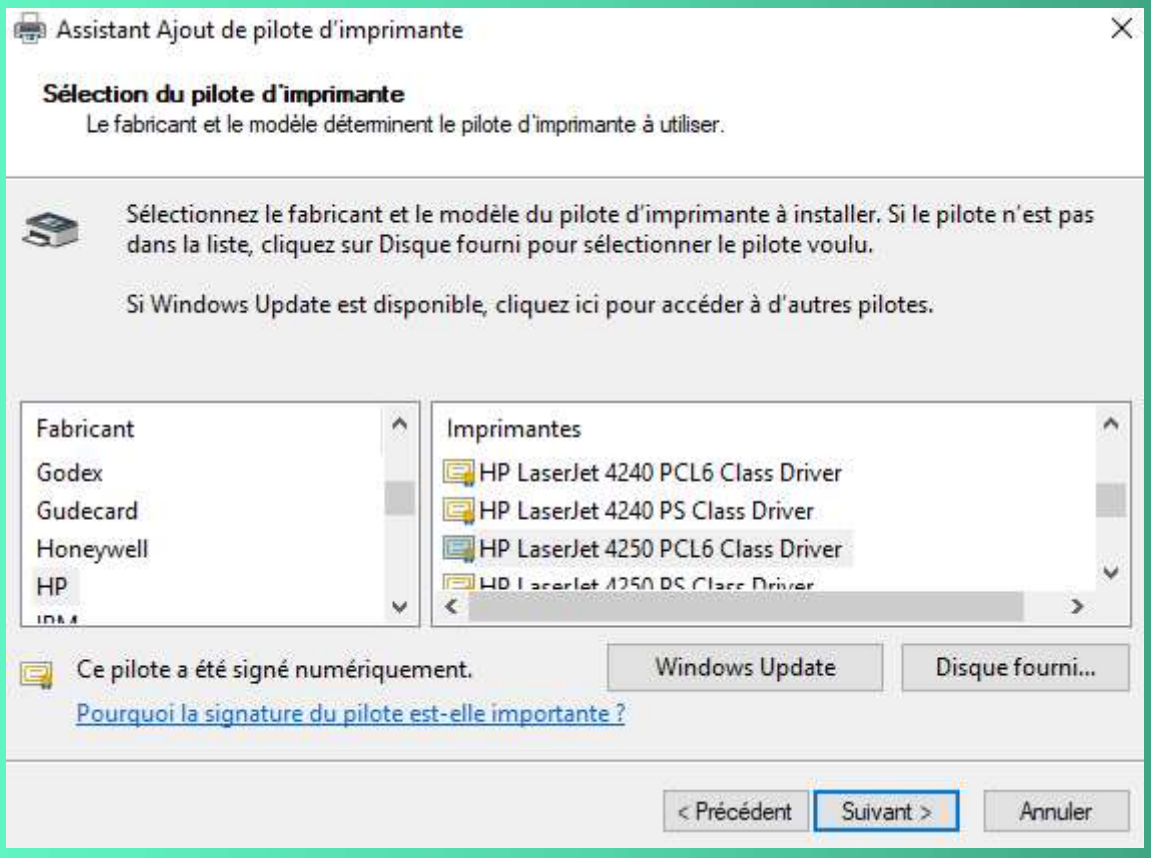
Sélectionnez les architectures processeurs compatibles avec le pilote que vous souhaitez importer.



Maintenant, cliquez sur "Windows update" pour indiquer le chemin vers votre fichier, puis dans la liste sélectionnez votre modèle d'imprimante avant de poursuivre jusqu'à la fin de l'assistant pour importer le pilote.

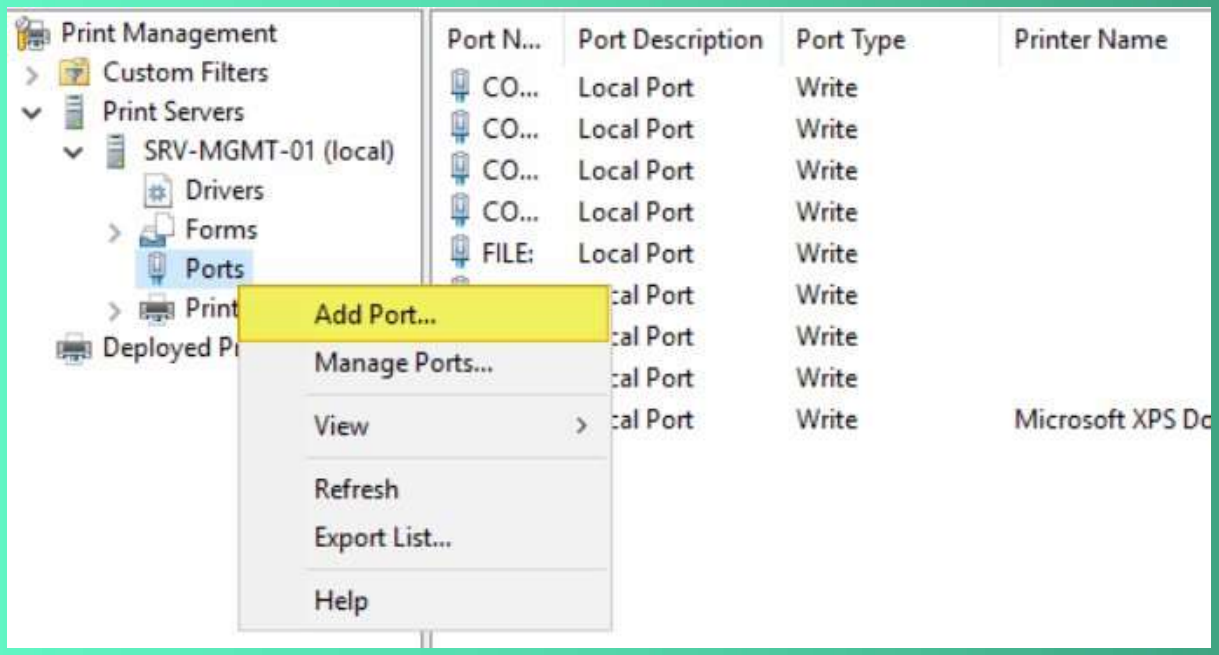


Ensuite, choisir le bon pilote, avec la marque et ensuite le modèle

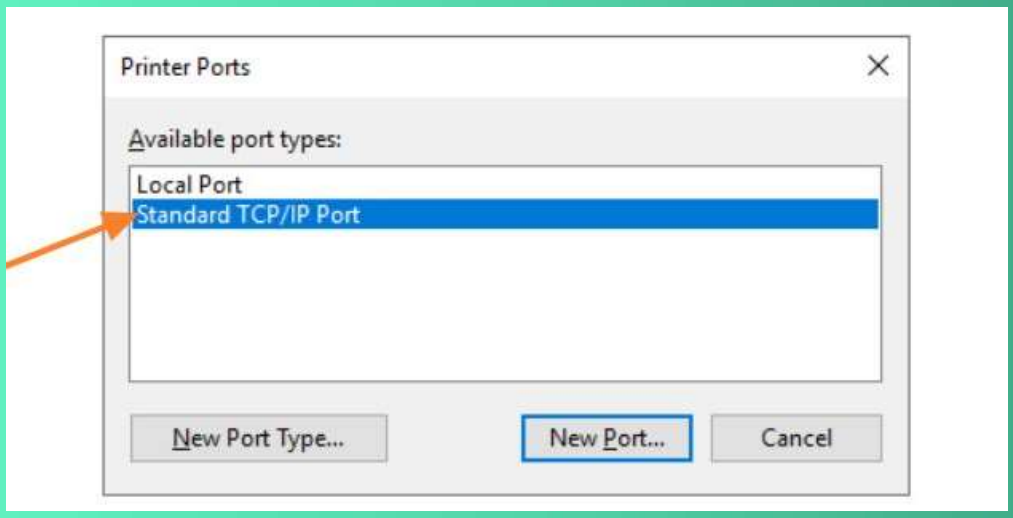


Créer un port TCP/IP :

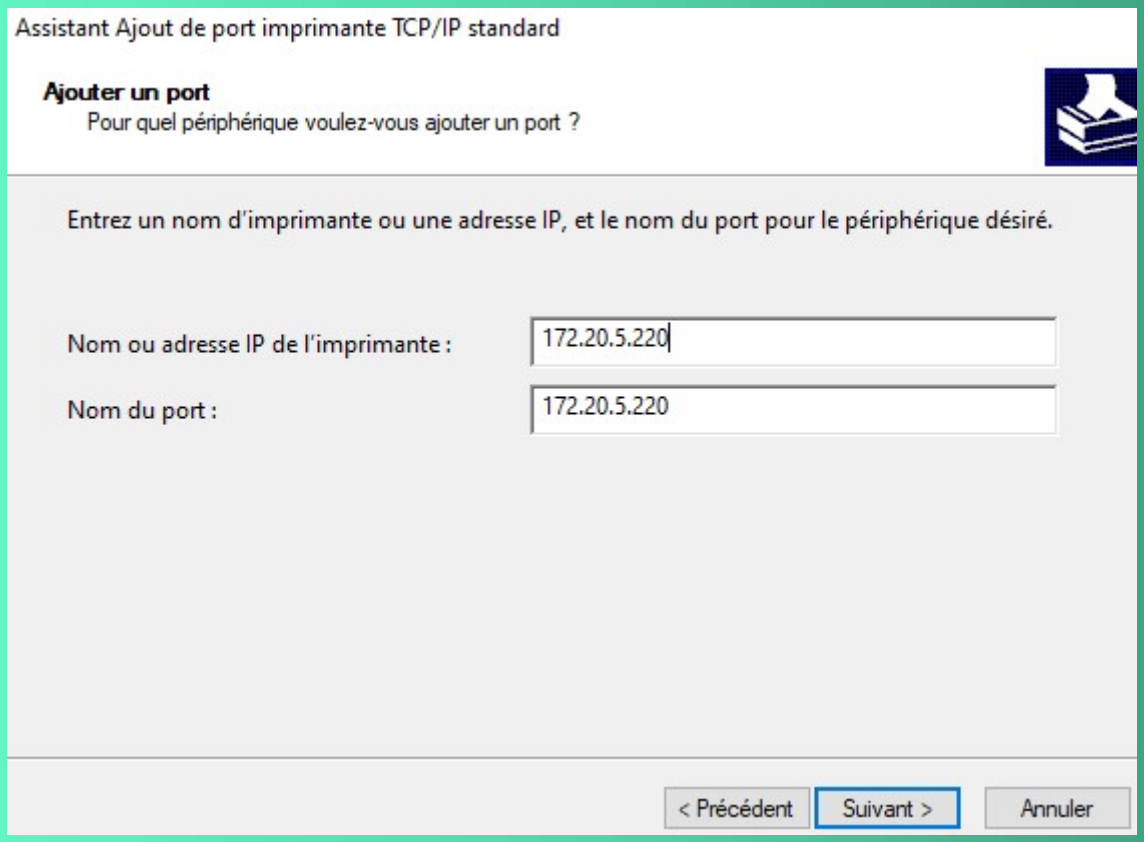
Sur le même principe que pour ajouter un pilote, la création d'un port s'effectue via un clic droit sur "Ports" puis "Ajouter un Port".



Sélectionnez "Standard TCP/IP Port" et cliquez sur "Ajouter Port".

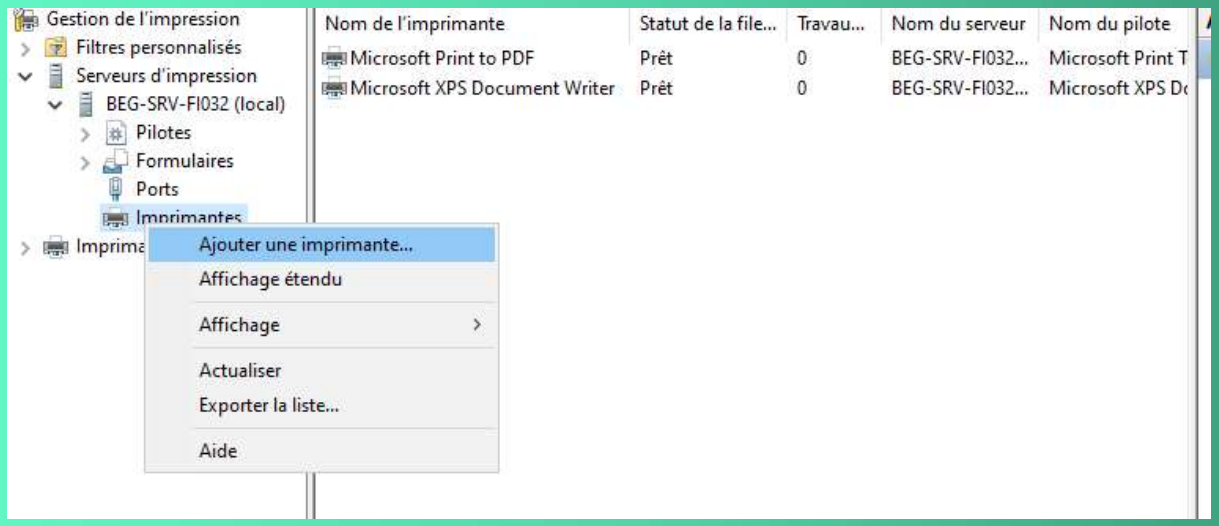


Remplissez le premier champ, nommé "Nom ou adresse IP de l'imprimante" en indiquant l'adresse IP de votre imprimante. Ensuite, donnez un nom à ce port en remplissant le champ "Nom du port", par exemple indiquez le nom de l'imprimante suivi de l'adresse IP, ce qui sera pratique visuellement dans la console.

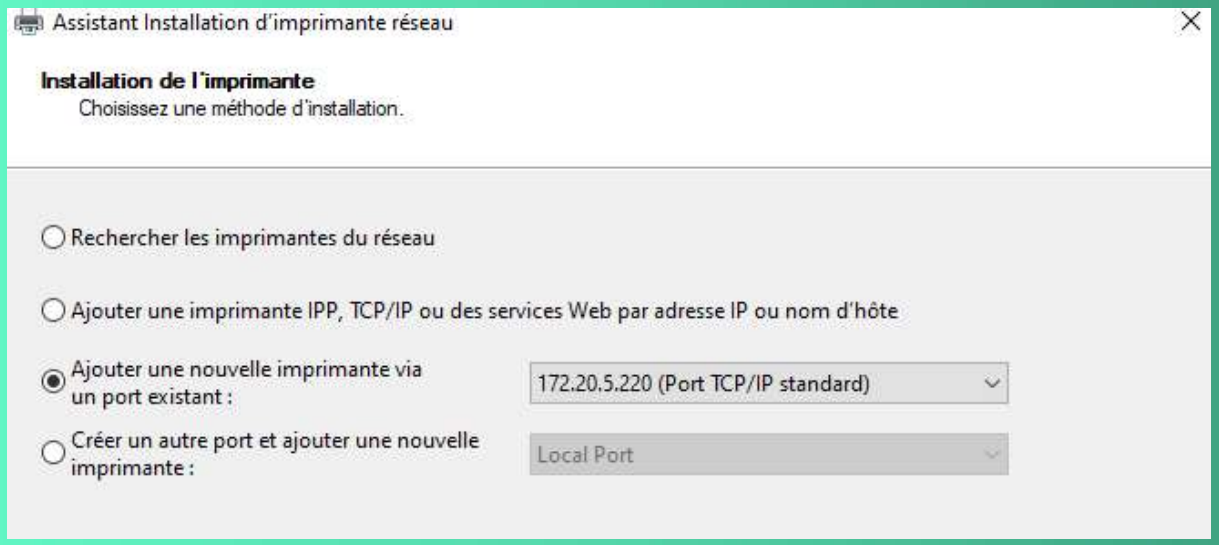


Ajouter l'imprimante à partager :

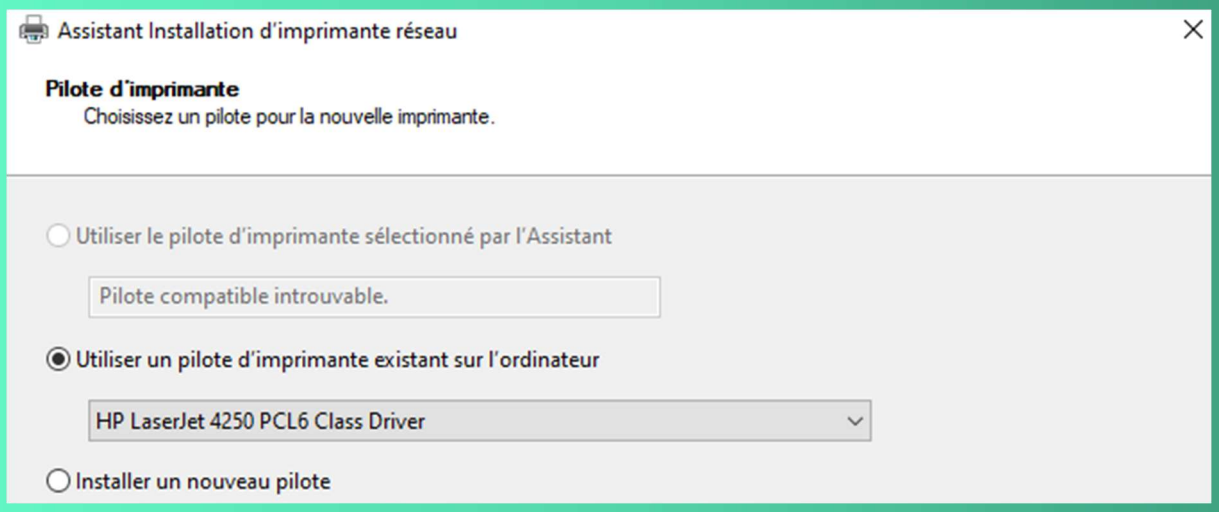
Pour ajouter l'imprimante, effectuez un clic droit sur "Imprimantes" et cliquez sur "Ajouter une imprimante".



Sélectionnez "Ajouter une nouvelle imprimante via un port existant" pour utiliser un port existant et sélectionnez le port que l'on a créé précédemment.



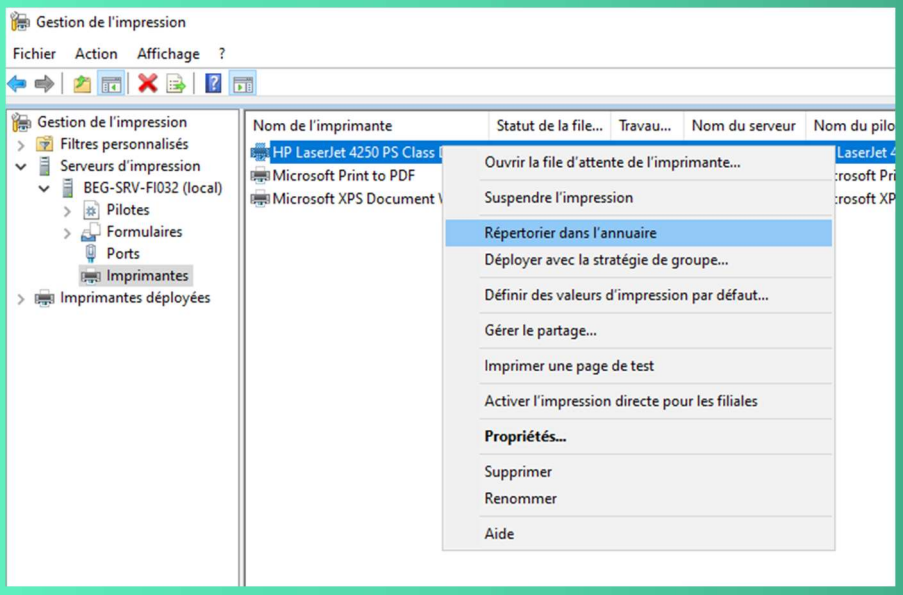
Sélectionner ‘utiliser un pilote d’imprimante existant sur l’ordinateur



Maintenant, nous allons devoir nommer l'imprimante : c'est le nom qu'elle aura sur le serveur d'impression. Il est également indispensable de la partager pour l'utiliser ensuite sur vos postes clients, cocher l'option "Partager cette imprimante". Indiquez :

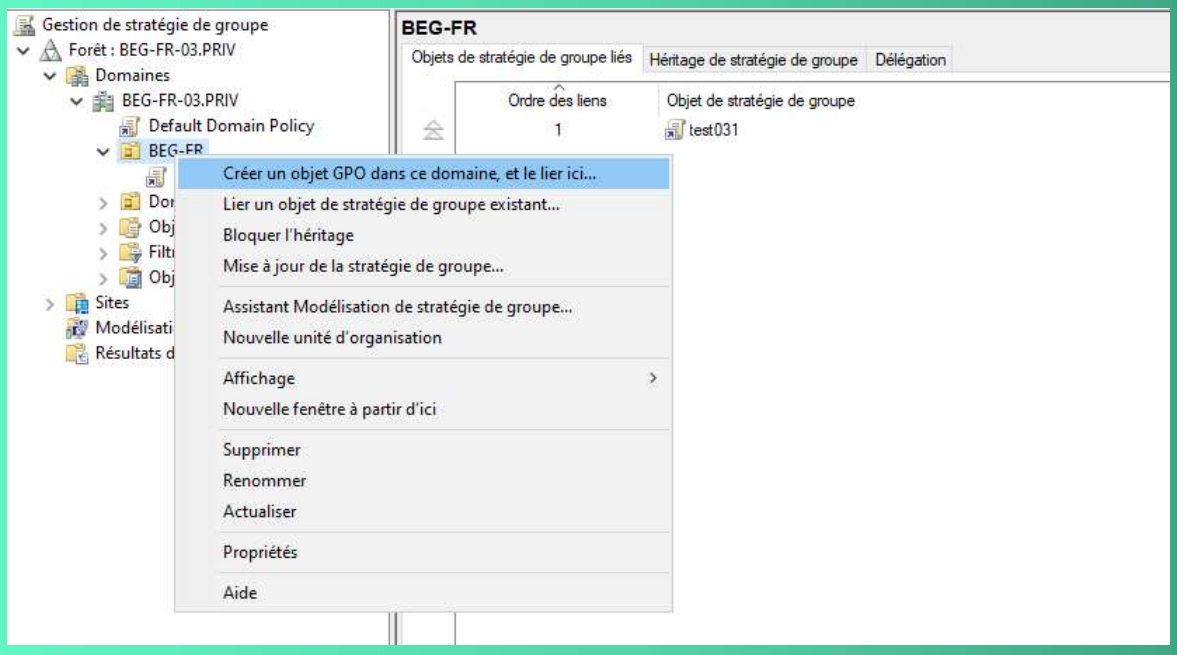
Répertorier l’imprimante dans l’annuaire :

Dans la liste des imprimantes du serveur, elle doit s'afficher. Maintenant, nous allons répertorier l'imprimante dans l'annuaire Active Directory pour faciliter l'accès depuis les postes clients. Effectuez un clic droit sur l'imprimante puis cliquez sur "Répertorier dans l’annuaire" (Lister dans l'annuaire). Un clic suffit, il n'y a pas de message de confirmation.

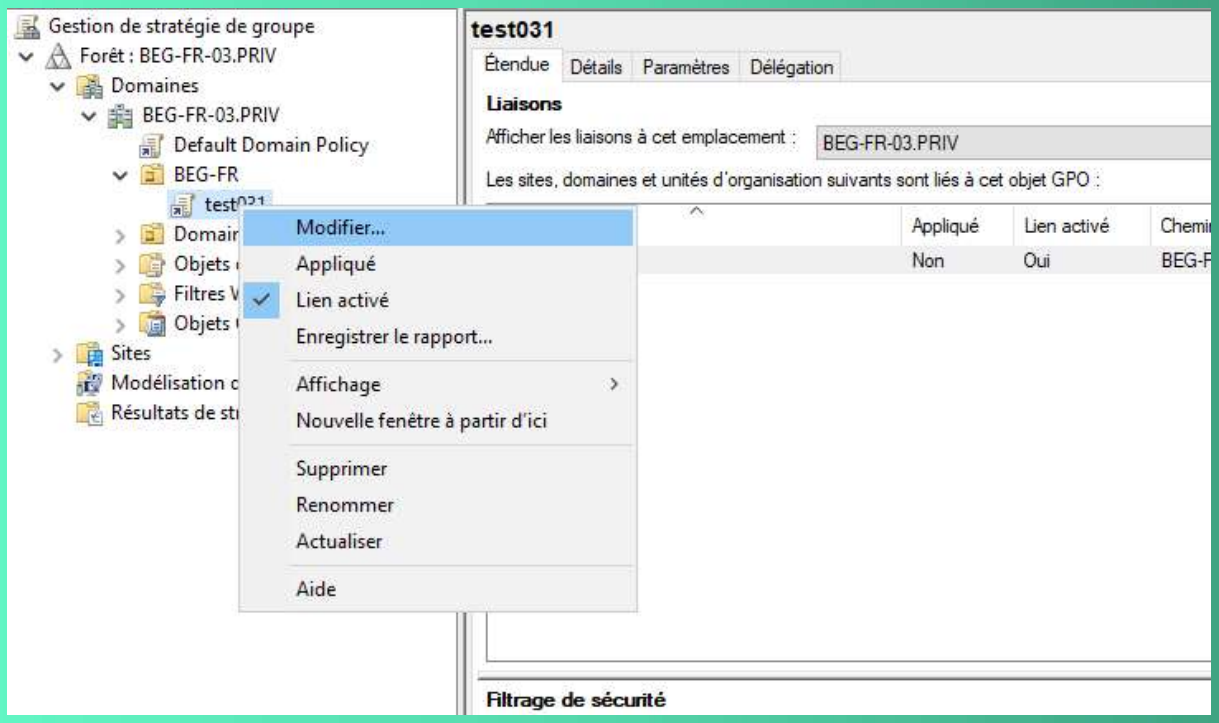


Création de la GPO :

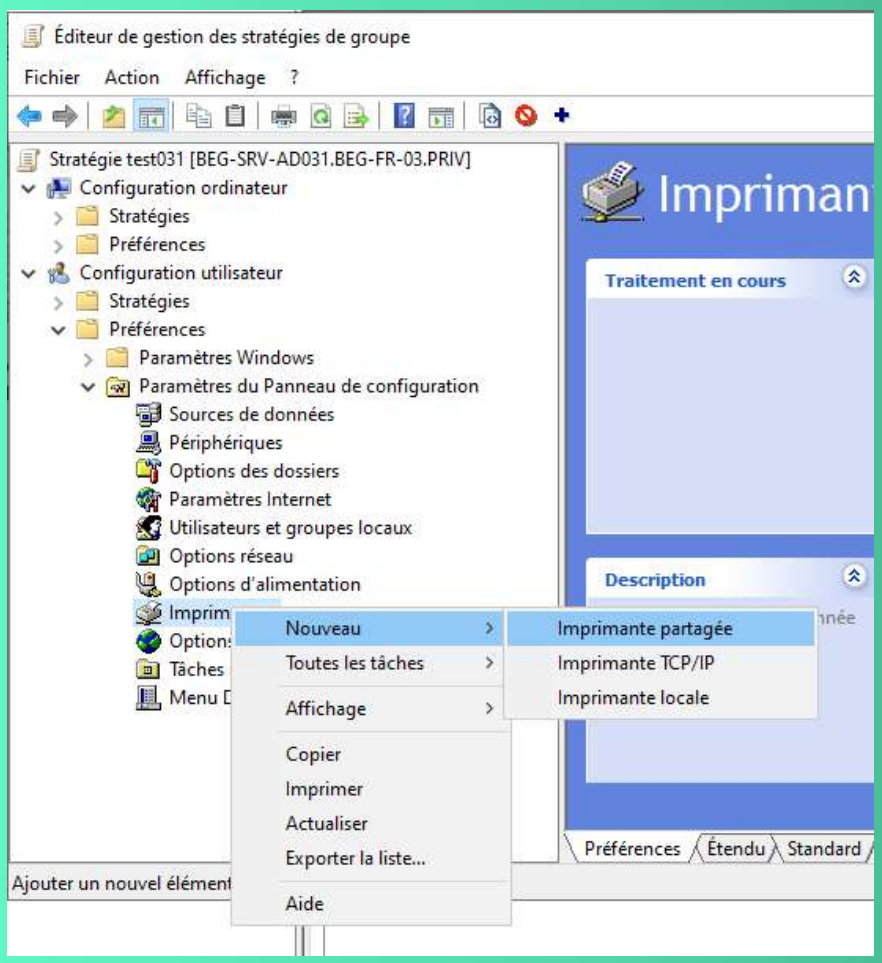
Création d'une GPO nommée 'imprimantes' en faisant clic droit sur une Unité d'Organisation



Ensuite, faire un clic droit sur la GPO que l'on vient de créer et cliquer sur 'modifier'

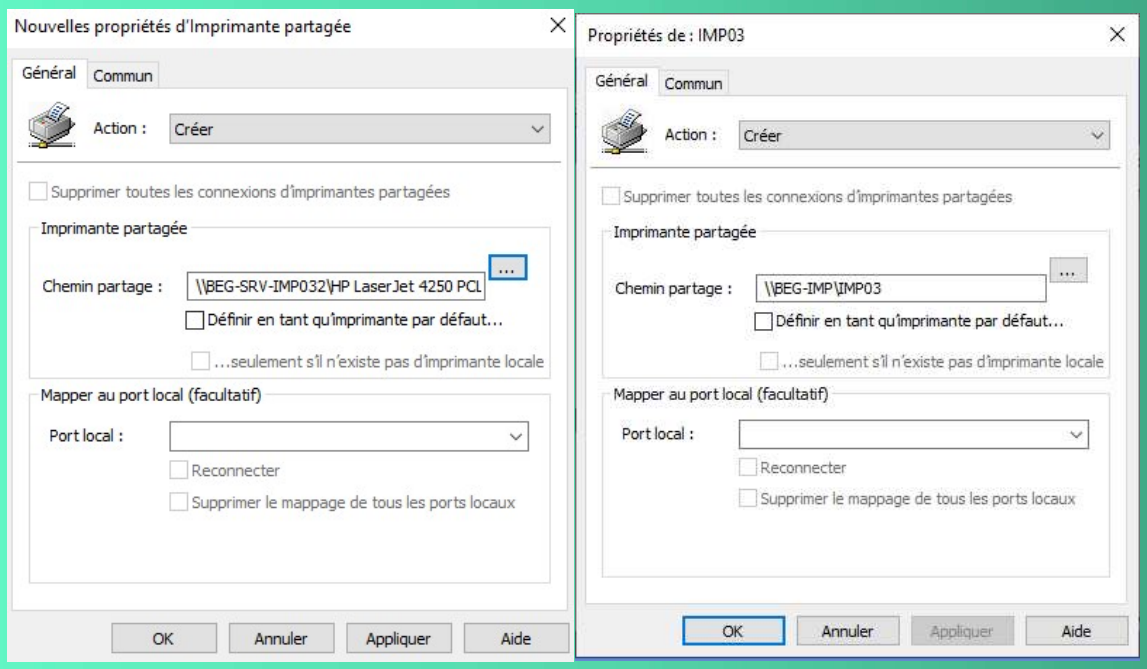


Ensuite, aller dans Configuration utilisateur > Préférences > Paramètres de Panneau de configuration > imprimantes puis faire un clic droit, nouveau et imprimante partagée



Modifier action : Créer

Choisir le Chemin de partage en direction de notre serveur d'impression



Pour finir, faire un gpupdate /force sur un cmd en mode admin pour recharger les GPO.

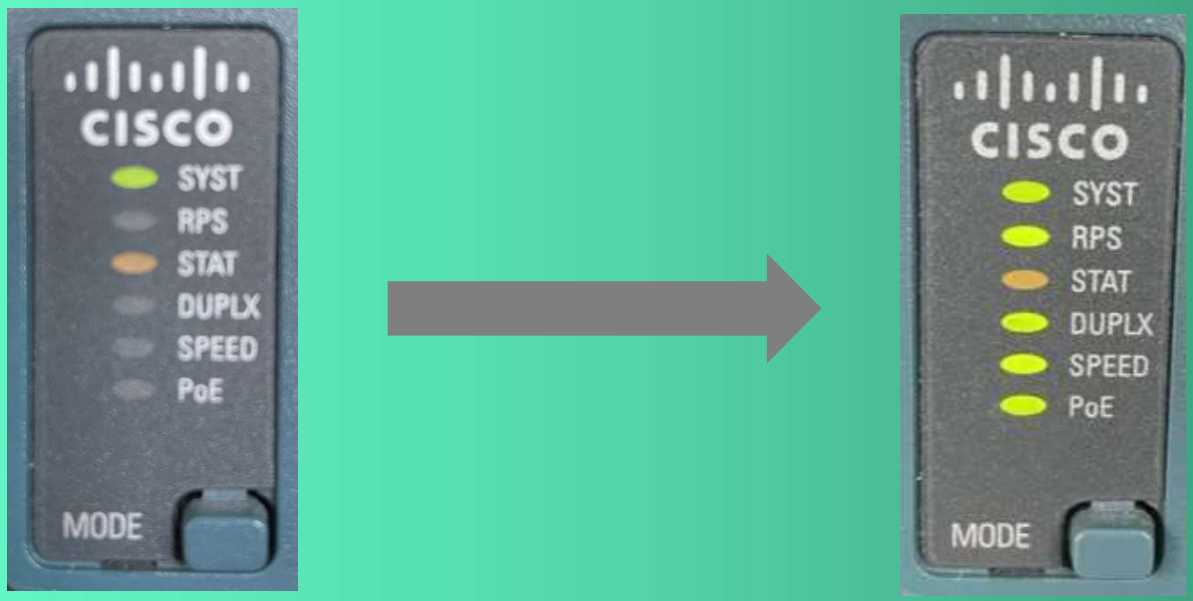
Configuration de l'adresse IP

- ➔ Bouton MENU
- ➔ Configuration Périphérique
- ➔ E/S
- ➔ MENU JETDIRECT INTEGRE
- ➔ TCP/IP
- ➔ Paramètres Manuels
- ➔ Adresse IP
- ➔ Masque de sous-réseau
- ➔ Passerelle par défaut

CONFIGURATION DU CŒUR DE RÉSEAU

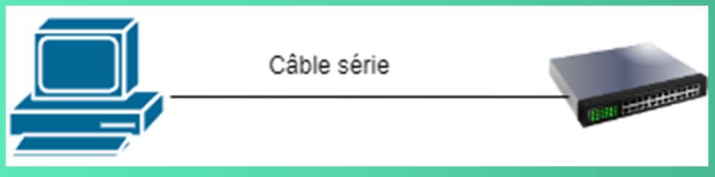
Procédure de réinitialisation :

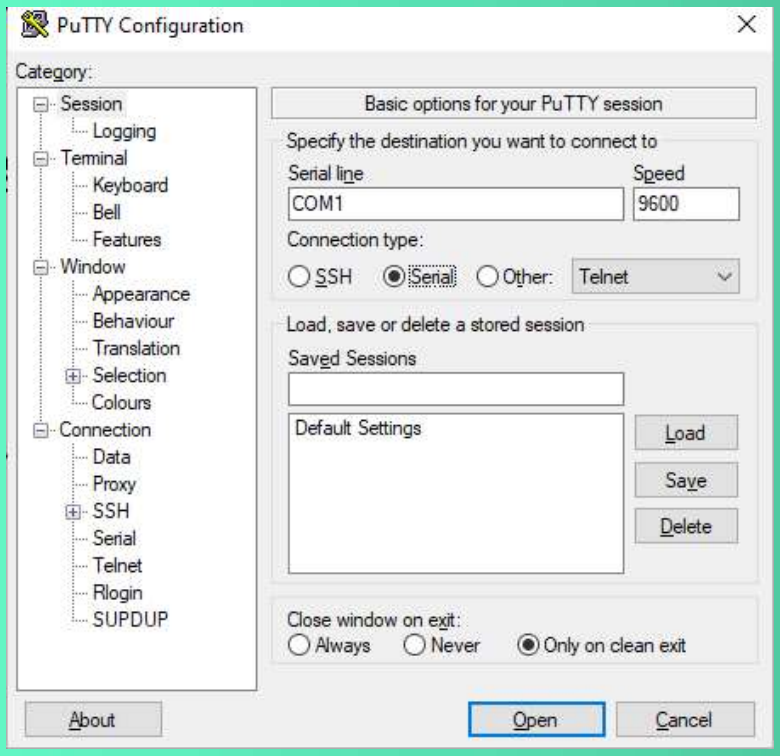
Pour réinitialiser le switch aux paramètres d'usine, il faut appuyer sur le bouton mode et maintenez-le enfoncé, les voyants LED du commutateur commencent à clignoter au bout de 3 secondes. Maintenez toujours le bouton mode enfoncé, les LED cessent de clignoter après 7 secondes supplémentaires puis le commutateur redémarre quand la LED SYST clignote.



Se connecter au Switch :

Pour se connecter au switch la première fois, il faut un câble série brancher à l'arrière du PC et au port console situé à l'arrière du switch. Pour se connecter au switch avec un câble série nous avons utilisé le logiciel PuTTY





Configuration de base :

Changer le nom :

```
Switch(config)#hostname BEG-CR-031
BEG-CR-031(config)#
```

Mise en place de l'adresse IP :

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 172.20.3.200 255.255.0.0
```

```
Switch(config-if)#no shutdown
```

Connexion à distance :

```
Switch(config-line)#line vty 0
Switch(config-line)#password Azerty45
```

Mise en place d'un mot de passe pour la connexion (lorsque tu rentres « en ») :

```
BEG-CR-031(config)#enable password Azerty45
```

Mise en place du chiffrement en MD5 :

```
BEG-CR-031(config)#service password-encryption
BEG-CR-031(config)#
```

Mise en place d'une bannière MOTD :

```
BEG-CR-031(config)#banner motd
BEG-CR-031(config)#$ '######################################################
Enter TEXT message.  End with the character '''.
#                                                 #
#   ##############################################  #
#   #                                            #  #
#   #                                            #  #
#   #          Authorized access only            #  #
#   #          Disconnect IMMEDIATELY            #  #
#   #     if you are not an authorized user !    #  #
#   #                                            #  #
#   #                                            #  #
#   ##############################################  #
#                                                 #


'
BEG-CR-031(config)#
```

Mise en place d'une bannière EXEC :

```
BEG-CR-031(config)#banner exec '                    .           .
Enter TEXT message.  End with the character '''.
                  |           |
                 |||         |||
               .|| ||.     .|| ||.
             .:||| | |||:..:||| | |||:.
              C i s c o  S y s t e m s


######################################################


              Session activated.
          Enter commands at the prompt.
   You have entered $(hostname) on line VTY $(line).


######################################################'
BEG-CR-031(config)#
```

Créer des VLANs :

```
BEG-CR-031(config)#vlan 10
BEG-CR-031(config-vlan)#name DATA
BEG-CR-031(config-vlan)#exit
BEG-CR-031(config)#vlan 20
BEG-CR-031(config-vlan)#name TELIP
BEG-CR-031(config-vlan)#exit
BEG-CR-031(config)#vlan 30
BEG-CR-031(config-vlan)#name VISIO
BEG-CR-031(config-vlan)#exit
```

Mettre le mode TRUNK sur les interfaces voulues :

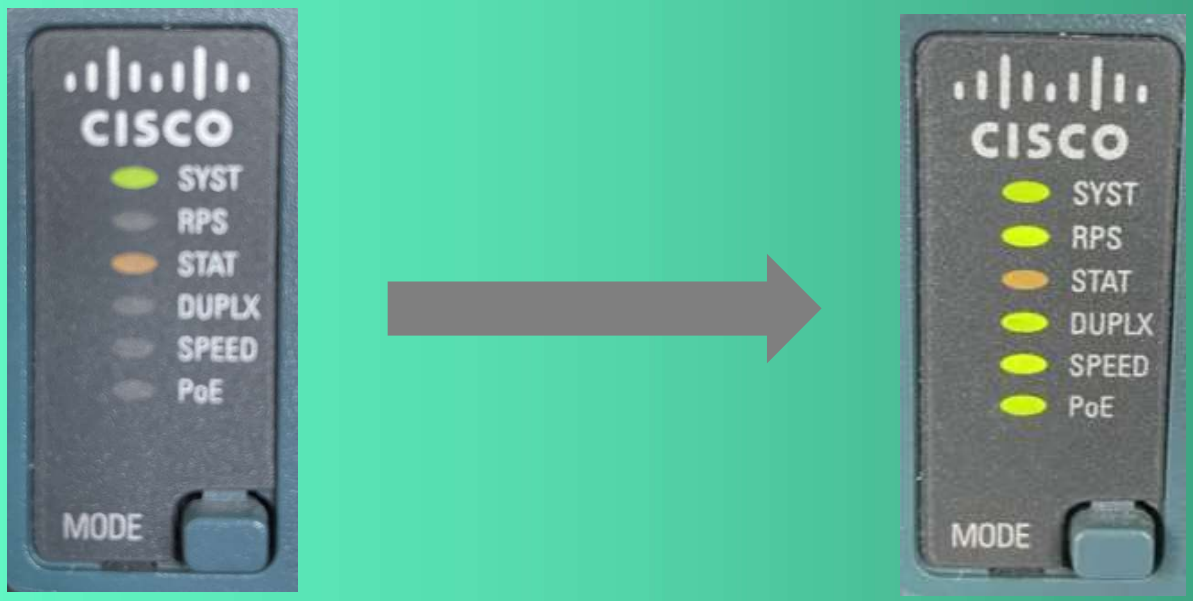
```
interface FastEthernet0/1
 switchport mode access
!
interface FastEthernet0/2
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/4
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/5
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/6
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/7
 switchport trunk allowed vlan 10,20,30
```

```
interface FastEthernet0/24
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 switchport nonegotiate
```

CONFIGURATION DU SWITCH

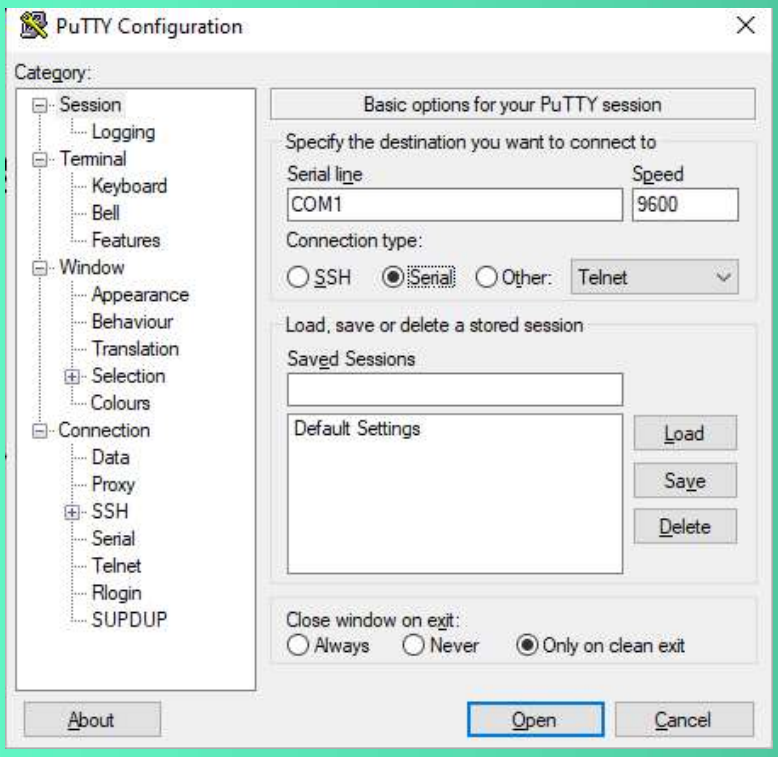
Procédure de réinitialisation :

Pour réinitialiser le switch aux paramètres d'usine, il faut appuyer sur le bouton mode et maintenez-le enfoncé, les voyants LED du commutateur commencent à clignoter au bout de 3 secondes. Maintenez toujours le bouton mode enfoncé, les LED cessent de clignoter après 7 secondes supplémentaires puis le commutateur redémarre quand la LED SYST clignote.



Se connecter au Switch :

Pour se connecter au switch la première fois, il faut un câble série brancher à l'arrière du PC et au port console situé à l'arrière du switch. Pour se connecter au switch avec un câble série nous avons utilisé le logiciel PuTTY



Configuration de base du switch :

Sur le switch, nous avons modifier le nom en BEG-SW-031

```
Switch(config)#hostname BEG-SW-031
```

Nous avons ajouté comme mot de passe 'Azerty45'

```
BEG-SW-031(config)#enable password Azerty45
BEG-SW-031(config)#service password-encryption
```

Nous avons aussi ajouté un mot de passe telnet pour la connexion à distance

```
BEG-SW-031(config-line)#line vty 0
BEG-SW-031(config-line)#password Azerty45
```

Et ajouter une adresse IP

```
BEG-SW-031(config-if)#interface vlan 1
BEG-SW-031(config-if)#ip address 172.20.3.201 255.255.0.0
```

Pour enregistrer la configuration, il faut entrer cette commande :

```
BEG-SW-031#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuration des VLANS :

Des contraintes sont à respectées :

- Le port 1 du switch de BEG est dédié à la gestion du commutateur et utilisé occasionnellement
- Les ports 2 à 10 seront réservés à la téléphonie
- Les ports 11 à 21 seront réservés aux PC et aux copieurs
- Les ports 22 et 23 sont réservés à la visio-conférence et désactivés
- Le port 24 est réservé pour le lien avec le cœur de réseau

Création des VLANS :

Les VLANS servent à segmenter les réseaux ainsi que les domaines de diffusion.

Nous devons créer 3 VLAN différents, le VLAN 10 nommée DATA, le VLAN 20 nommée TELIP ainsi que le VLAN 30 nommée VISIO

```
BEG-SW-031(config)#vlan 10
BEG-SW-031(config-vlan)#name DATA
BEG-SW-031(config-vlan)#exit
BEG-SW-031(config)#vlan 20
BEG-SW-031(config-vlan)#name TELIP
BEG-SW-031(config-vlan)#exit
BEG-SW-031(config)#vlan 30
BEG-SW-031(config-vlan)#name VISIO
```

Pour vérifier que les VLAN sont crées, entre la commande ‘show vlan’

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Fa0/25, Fa0/26, Fa0/27, Fa0/28
                                                 Fa0/29, Fa0/30, Fa0/31, Fa0/32
                                                 Fa0/33, Fa0/34, Fa0/35, Fa0/36
                                                 Fa0/37, Fa0/38, Fa0/39, Fa0/40
                                                 Fa0/41, Fa0/42, Fa0/43, Fa0/44
                                                 Fa0/45, Fa0/46, Fa0/47, Fa0/48
                                                 Gi0/1, Gi0/2, Gi0/3, Gi0/4
10   DATA                              active
20   TELIP                             active
30   VISIO                             active
```

Ajout des ports dans leur VLAN respectif :

Ajouter le port 2 à 10 dans le VLAN 20 en mode access réservés à la téléphonie IP :

```
BEG-SW-031(config)#interface range fastEthernet 0/2-10
BEG-SW-031(config-if-range)#switchport mode access
BEG-SW-031(config-if-range)#switchport access vlan 20
```

Ajouter le port 11 à 21 dans le VLAN 10 en mode access réservés à la DATA :

```
BEG-SW-031(config)#interface range fastEthernet 0/11-21
BEG-SW-031(config-if-range)#switchport mode access
BEG-SW-031(config-if-range)#switchport access vlan 10
```

Ajouter le port 22 et 23 dans le VLAN 30 en mode access réservés à la VISIO et désactivés :

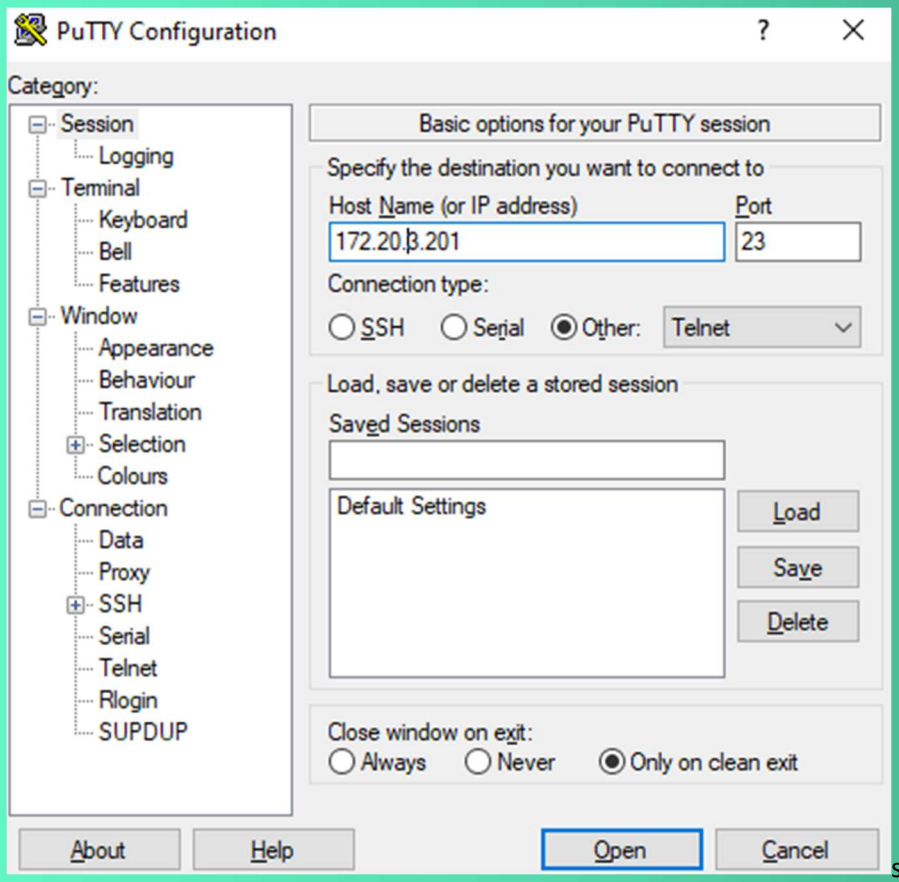
```
BEG-SW-031(config)#interface range fastEthernet 0/22-23
BEG-SW-031(config-if-range)#switchport mode access
BEG-SW-031(config-if-range)#switchport access vlan 30
BEG-SW-031(config-if-range)#shutdown
```

Sur le port 24, nous allons 'taguer le port' en activant le mode trunk et y autoriser le VLAN 10, 20 et 30

```
BEG-SW-031(config)#interface fastEthernet 0/24
BEG-SW-031(config-if)#switchport mode trunk
BEG-SW-031(config-if)#switchport trunk allowed vlan 10,20,30
```

Comment se connecter à distance :

Pour se connecter à distance, il faut connecter le PC au switch avec un câble RJ 45 et ensuite en utilisant le logiciel PuTTY en utilisant son adresse IP.

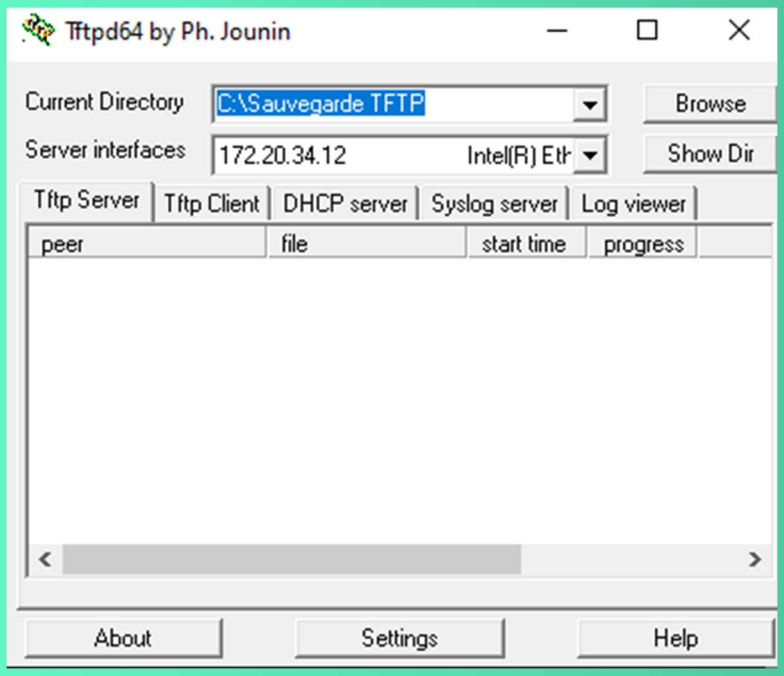


s

Sauvegarde TFTP :

Pour réaliser une sauvegarde TFTP, il faut installer logiciel 'Tftpd64' sur un poste. Si le logiciel refuse de s'ouvrir, dans le gestionnaire de tâches vous trouverez un serveur de démarrer. Il suffit de le fermer.

Une fois le logiciel ouvert, cette page s'ouvre. Sur cette page vous pourrez modifier le répertoire ou sera enregistrer le fichier ainsi que l'interface réseau.



Pour effectuer une sauvegarde sur un serveur TFTP, il faut entrer la commande ‘copy startup-config tftp’ puis entrer l’adresse IP du serveur TFTP

```
BEG-SW-031#copy startup-config tftp
Address or name of remote host []? 172.20.34.12
Destination filename [beg-sw-031-confg]?
!!
2200 bytes copied in 0.051 secs (43137 bytes/sec)
```

Restauration d’une sauvegarde :

Pour restaurer une sauvegarde, il faut entrer sur le switch la commande ‘copy tftp running-config’

CONFIGURATION DU ROUTEUR

Procédure de réinitialisation :

Pour réinitialiser le routeur, il faut entrer plusieurs commandes :

```
Router(config)#config-register 0x2142
Router(config)#exit
Router#
*Jan  1 02:18:51.135: %SYS-5-CONFIG_I: Configured from console by console
Router#reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

Configuration de base du routeur :

Sur le routeur, nous avons modifier le nom en BEG-RTR-031

```
Router(config)#hostname BEG-RTR-031
```

Nous avons ajouté comme mot de passe 'Azerty45'

```
BEG-RTR-031(config)#enable password Azerty45
BEG-RTR-031(config)#service password-encryption
```

Mise en place de la bannière MOTD

```
BEG-RTR-031(config)#banner motd '
Enter TEXT message.  End with the character '''.
##########################################################
#                                                        #
#   ###################################################  #
#   #                                                 #  #
#   #                                                 #  #
#   #          Authorized access only                 #  #
#   #          Disconnect IMMEDIATELY                 #  #
#   #     if you are not an authorized user !         #  #
#   #                                                 #  #
#   #                                                 #  #
#   ###################################################  #'
BEG-RTR-031(config)#
```

Mise en place de la bannière EXEC

```
BEG-RTR-031(config)#banner exec '
Enter TEXT message.  End with the character '''.
                    .            .
                    |            |
                   |||          |||
                 .|| ||.      .|| ||.
               .:||| | |||:..:||| | |||:.
                C i s c o  S y s t e m s


############################################################


                Session activated.
            Enter commands at the prompt.
   You have entered $(hostname) on line VTY $(line).


############################################################'
BEG-RTR-031(config)#
```

Et ajouter une adresse IP sur l'interface FastEthernet0/0

```
BEG-RTR-031(config)#interface fa0/0
BEG-RTR-031(config-if)#ip address 172.20.3.210 255.255.0.0
```

Configuration des VLANS :

Le VLAN 10 nommée DATA aura comme réseau 172.21.3.0/16

Le VLAN 20 nommée TELIP aura comme réseau 172.22.3.0/16

Le VLAN 30 nommée VISIO aura comme réseau 172.23.3.0/16

Configuration du VLAN 10 :

```
BEG-RTR-031(config)#interface fa0/0.10
BEG-RTR-031(config-subif)#encapsulation dot1Q 10
BEG-RTR-031(config-subif)#ip address 172.21.3.254 255.255.0.0
BEG-RTR-031(config-subif)#no shutdown
```

Configuration du VLAN 20 :

```
BEG-RTR-031(config)#interface fa0/0.20
BEG-RTR-031(config-subif)#encapsulation dot1Q 20
BEG-RTR-031(config-subif)#ip address 172.22.3.254 255.255.0.0
BEG-RTR-031(config-subif)#no shutdown
```

Configuration du VLAN 30 :

```
BEG-RTR-031(config)#interface fa0/0.30
BEG-RTR-031(config-subif)#encapsulation dot1Q 30
BEG-RTR-031(config-subif)#ip address 172.23.3.254 255.255.0.0
BEG-RTR-031(config-subif)#no shutdown
```

Test des vlans :

Test de requêtes ICMP entre les postes :

PC 1 VLAN 10 -> PC 2 VLAN 10 = FONCTIONNEL

PC 1 VLAN 10 -> PC 2 VLAN 20 = NON FONCTIONNEL

PC 1 VLAN 20 -> PC 2 VLAN 20 = FONCTIONNEL

PC 1 VLAN 20 -> PC 2 VLAN 30 = NON FONCTIONNEL

PC 1 VLAN 30 -> PC 2 VLAN 30 = FONCTIONNEL

PC 1 port shutdown -> PC 2 VLAN 10,20,30 = NON FONCTIONNEL

PC 1 port 1 -> PC 2 VLAN 10,20,30 = NON FONCTIONNEL

PC 1 port 24 -> PC 2 VLAN 10,20,30 = NON FONCTIONNEL

Avec le routage Inter-VLANS :

PC 1 dans le VLAN 10 -> PC 2 VLAN 20 = FONCTINNEL

PC 1 dans le VLAN 20 -> PC 2 dans le VLAN 30 = FONC

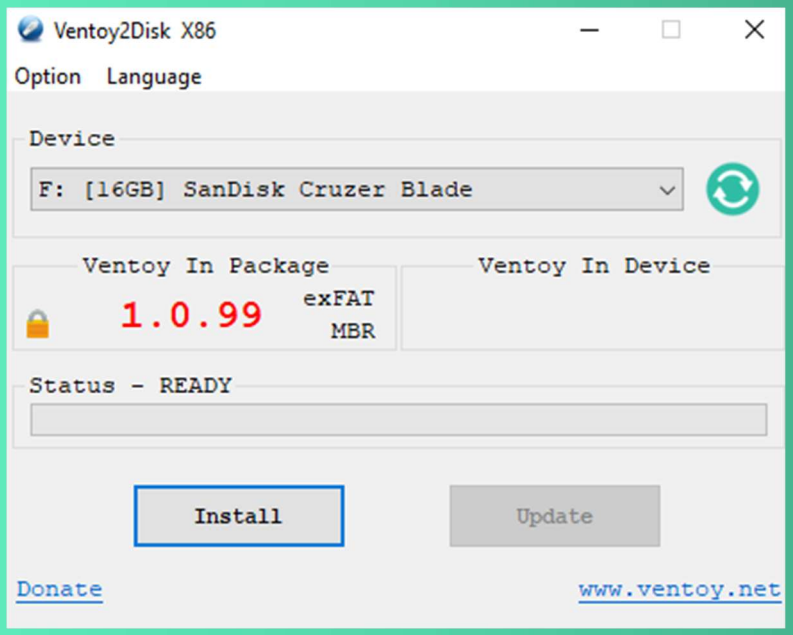
INSTALLATION D'UNE CLE VENTOY

Pour installer le routeur, nous avons utilisé une clé ventoy pour installer Debian12 sur une machine

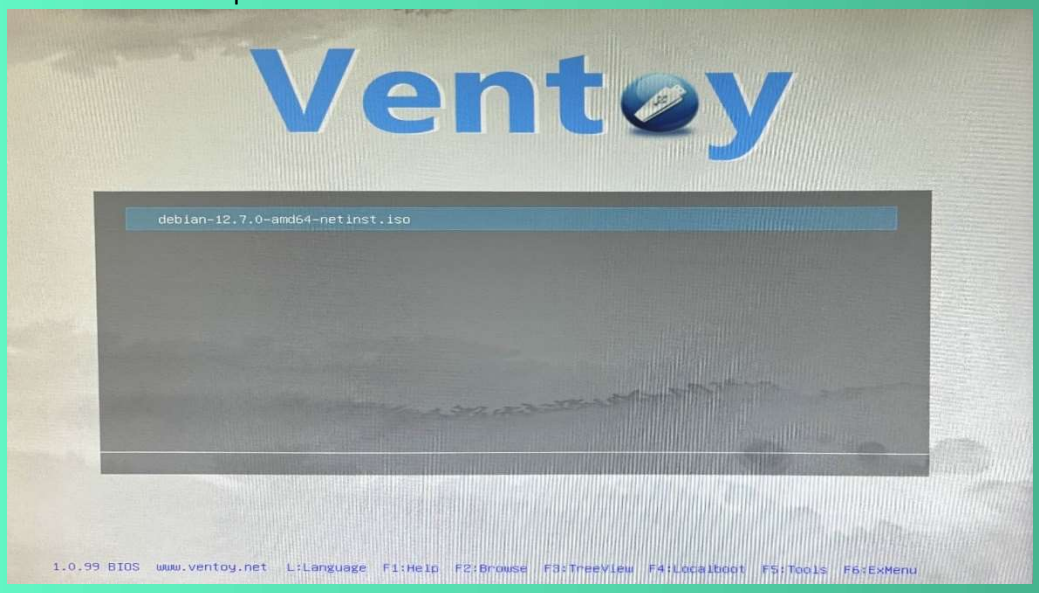
Pour installer ventoy, il faut se rendre sur le site : https://www.ventoy.net/en/download.html

Pour télécharger Debian12 en mode netinstall : https://www.debian.org/download

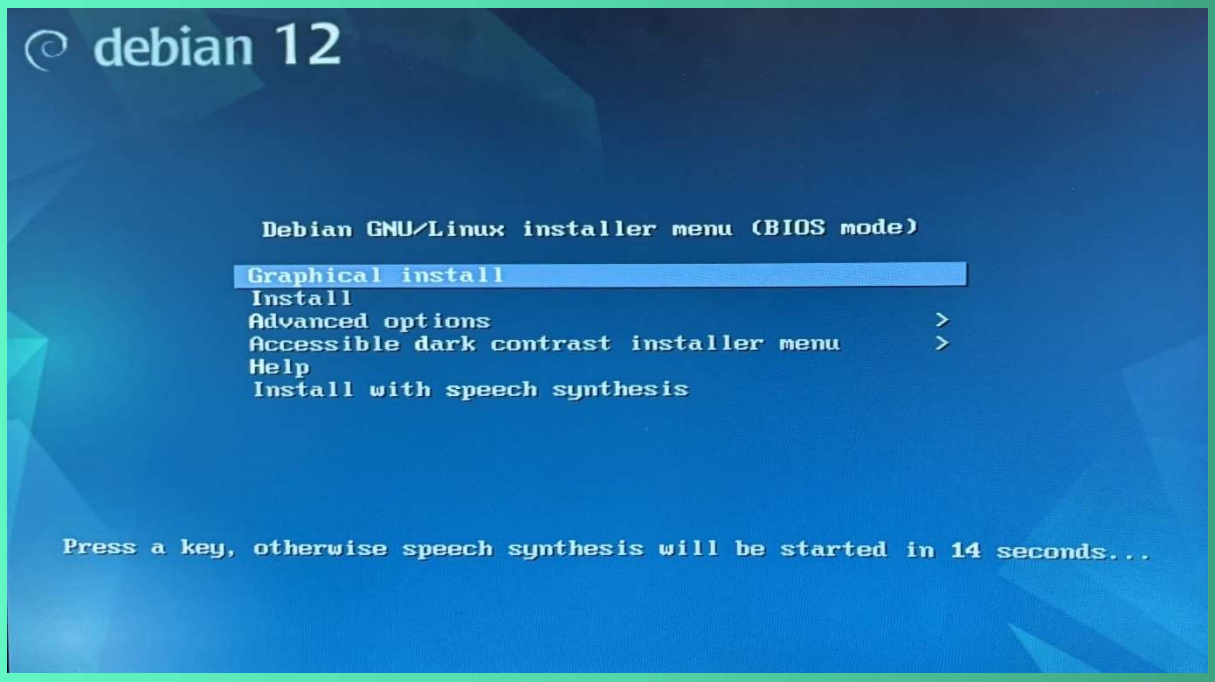
Ensuite, nous avons installé ventoy sur une clé USB en format FAT32



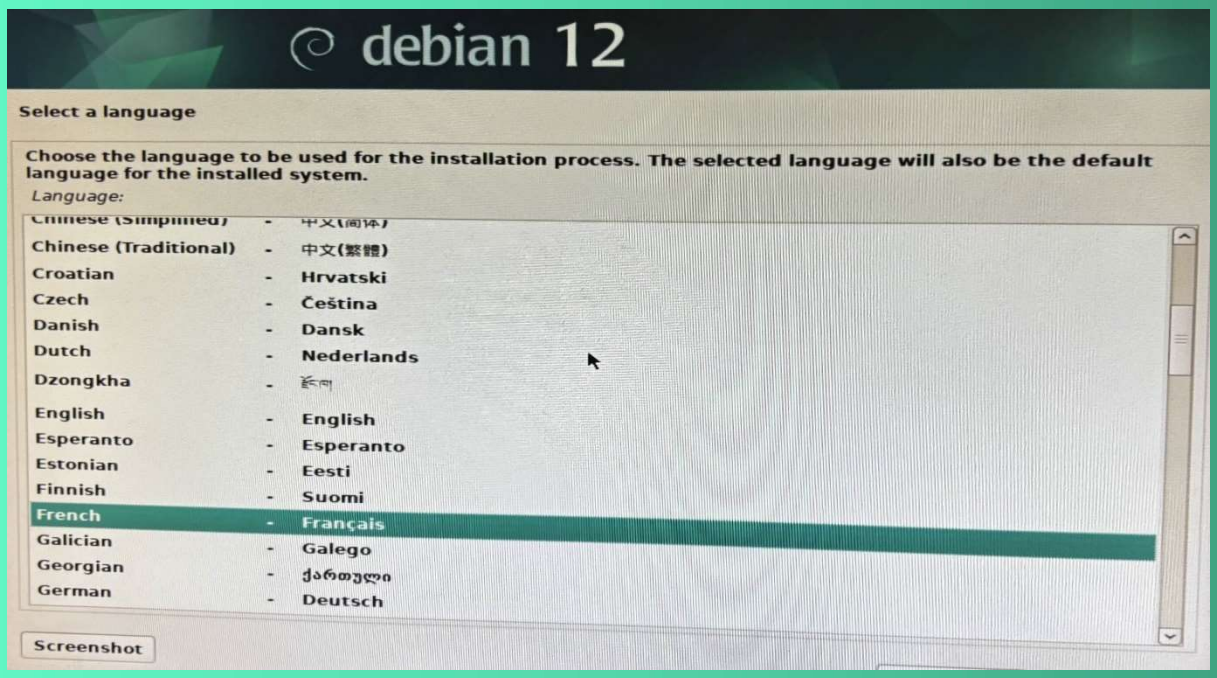
Sélectionner l'ISO que l'on souhaite installer



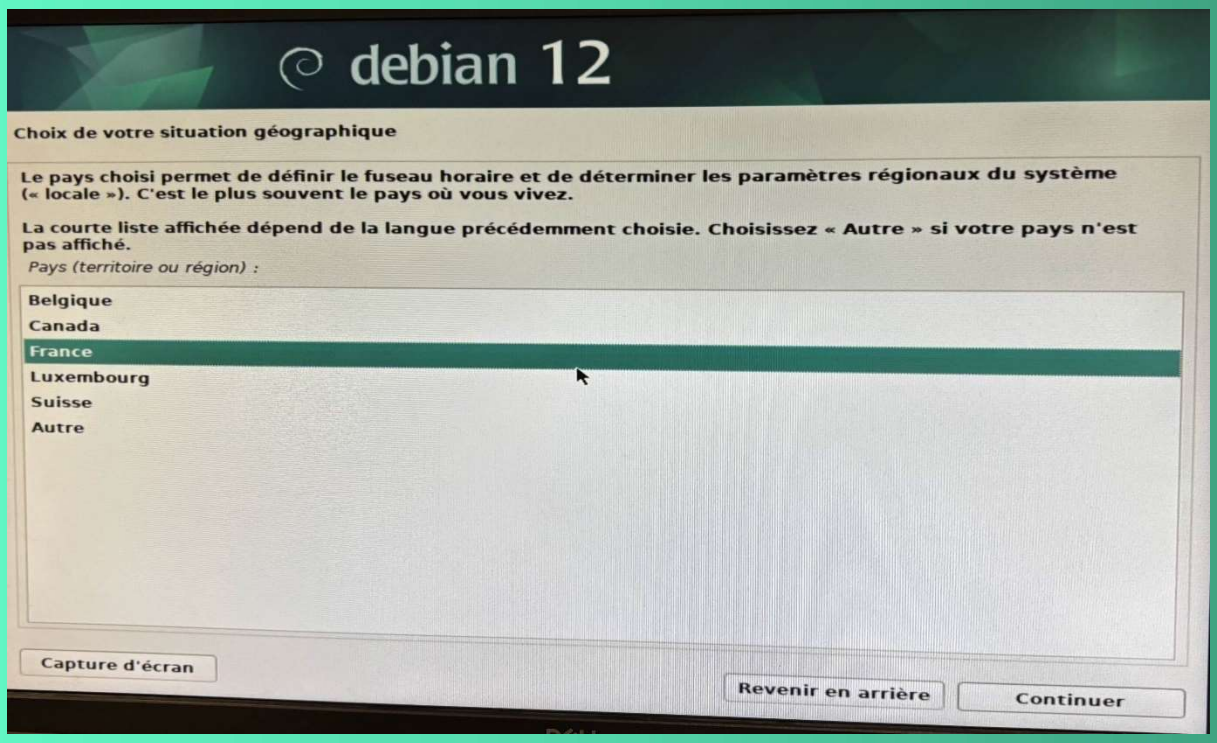
Installation de Debian 12 en version graphique



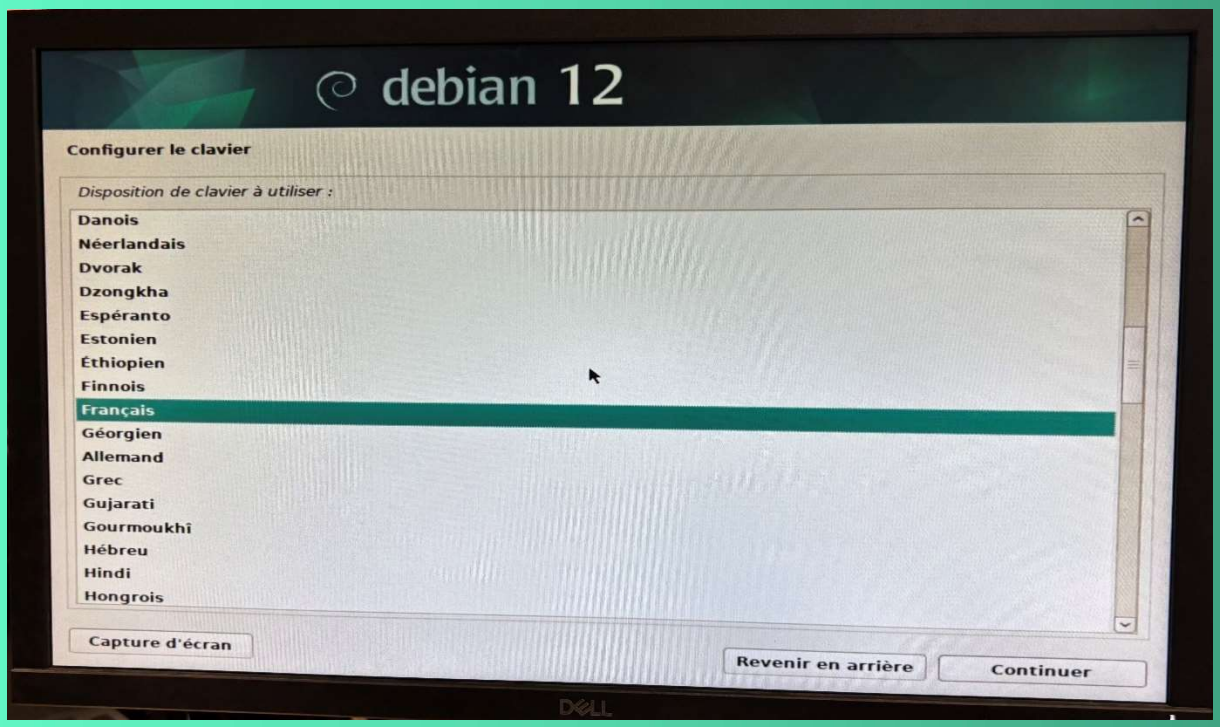
Sélection de la langue qui sera utilisé pour le processus d'installation



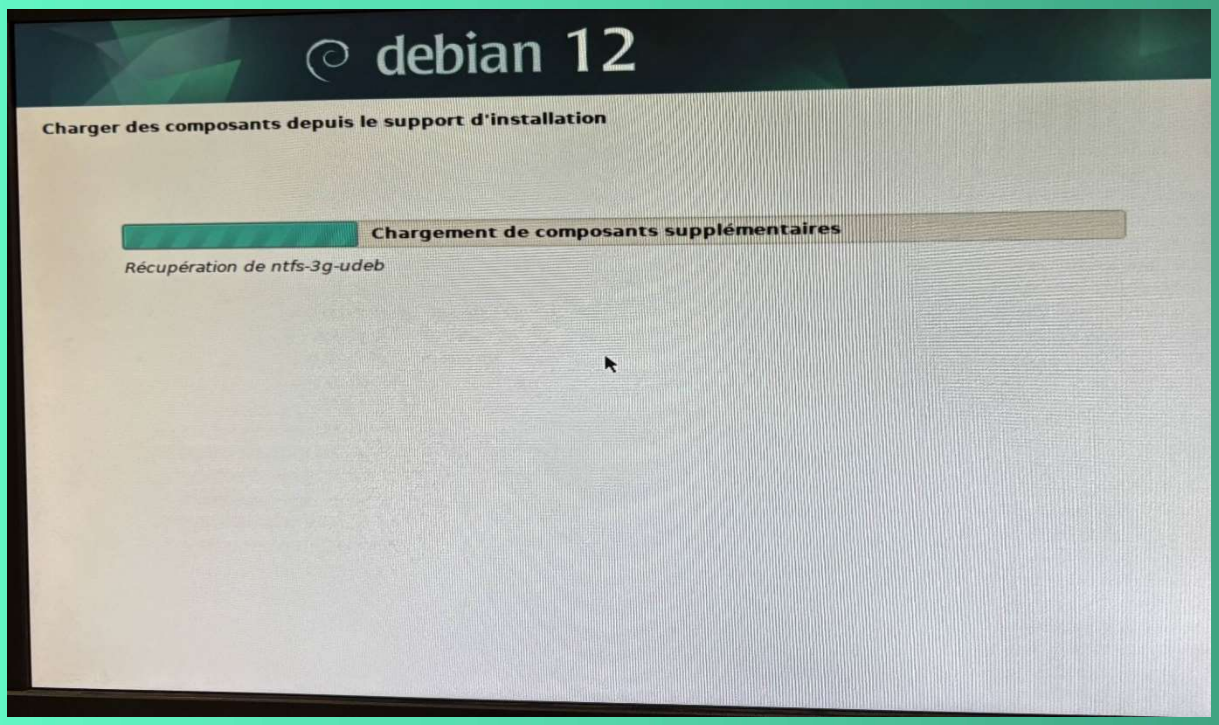
Choisir son pays local permettant de définir le fuseau horaire



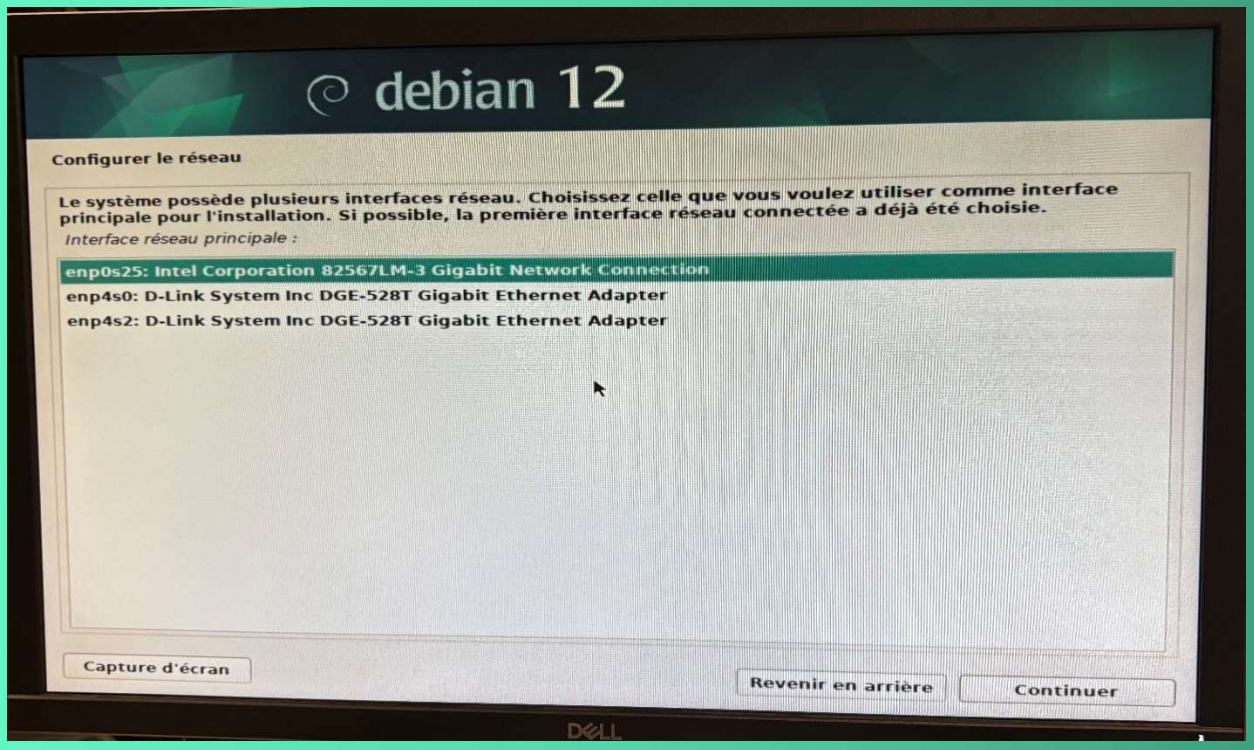
Configurer la langue du clavier



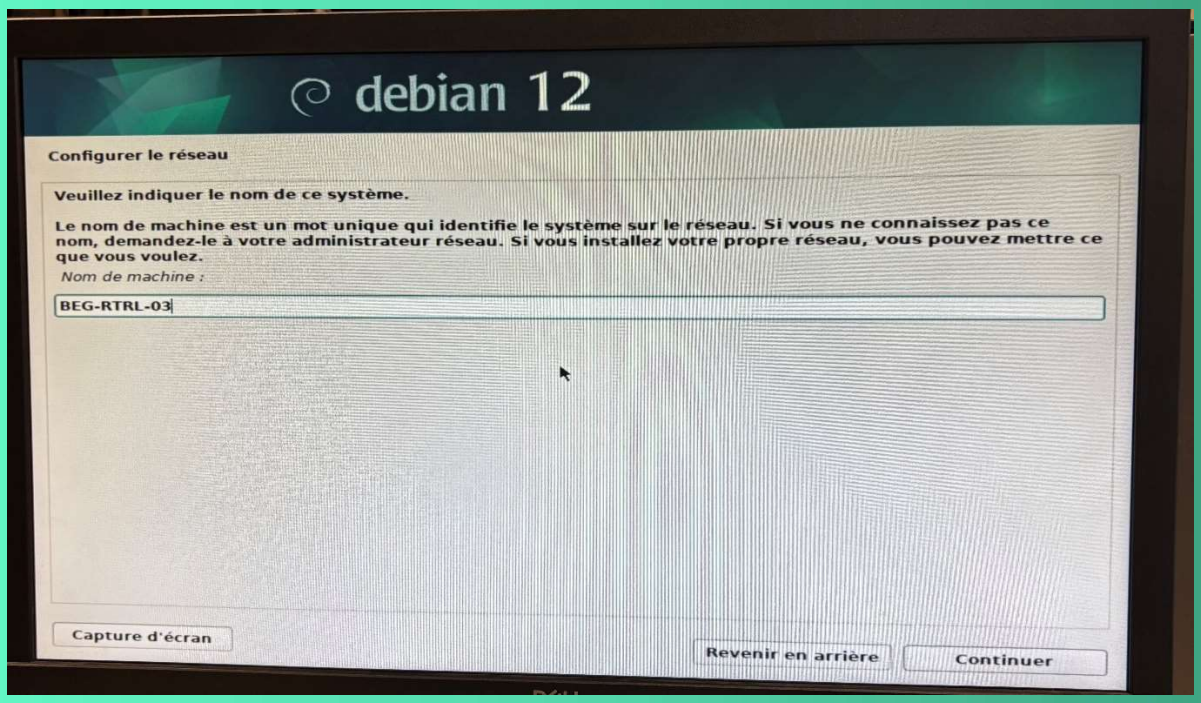
Chargement de composants supplémentaires nécessaires depuis le support d'installation



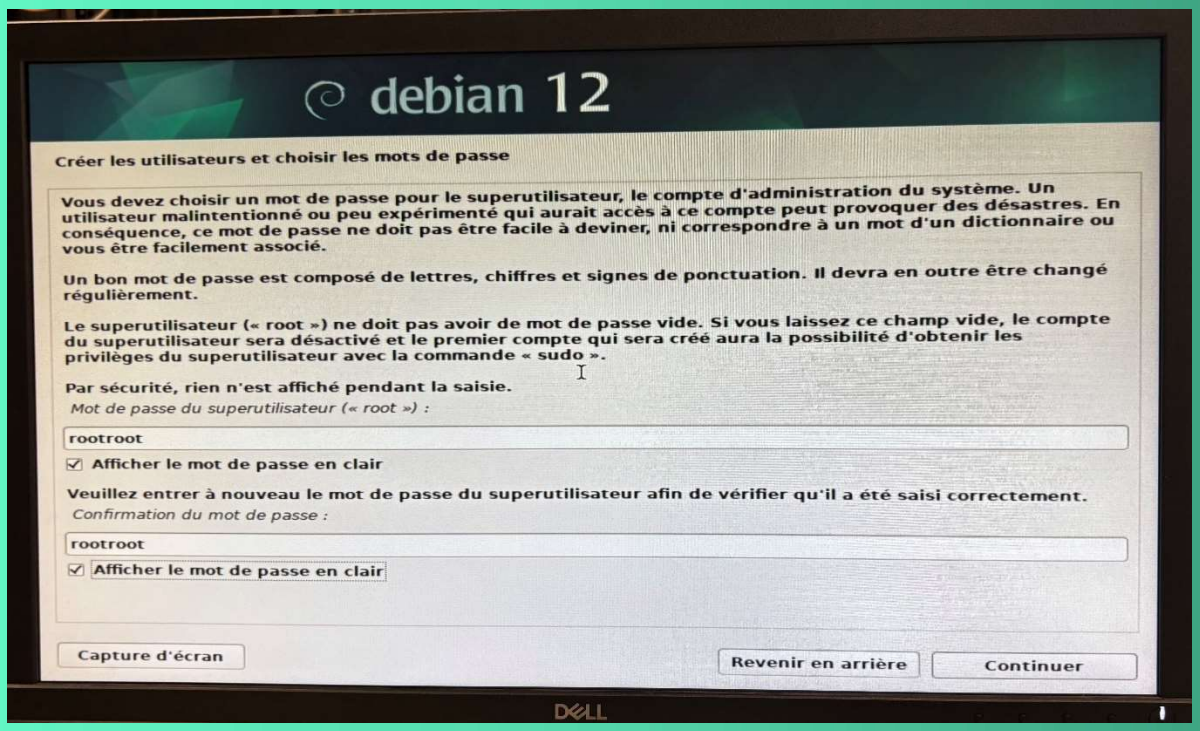
Sélection de la carte réseau principale



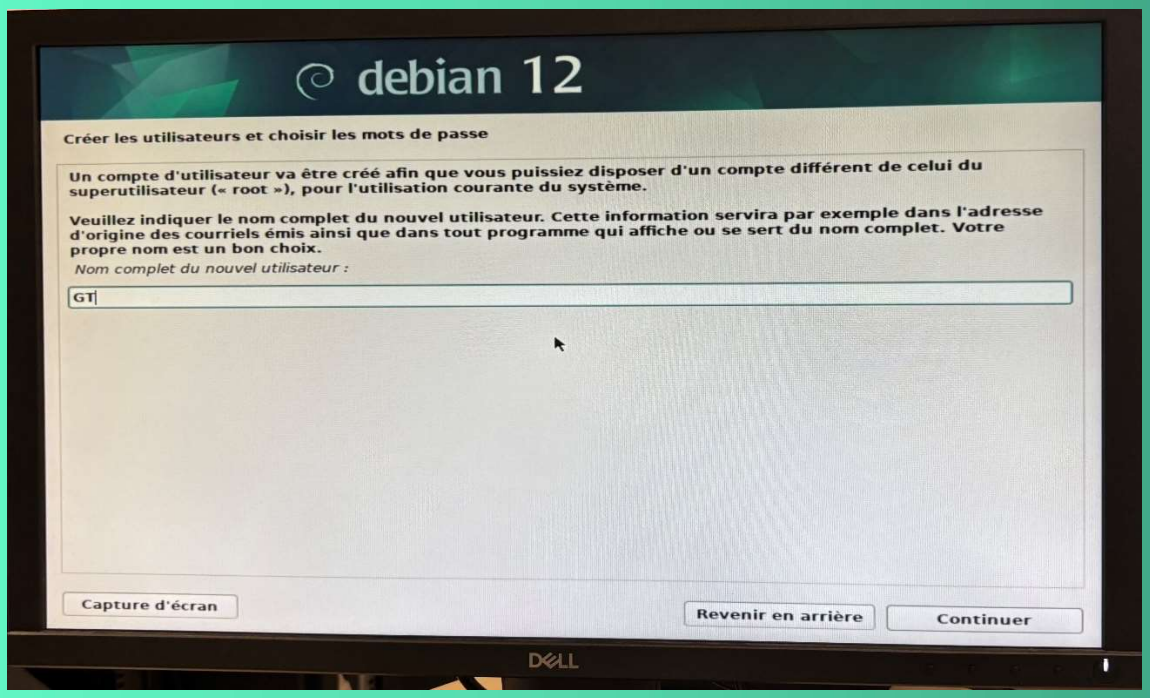
Configuration de nom de la machine



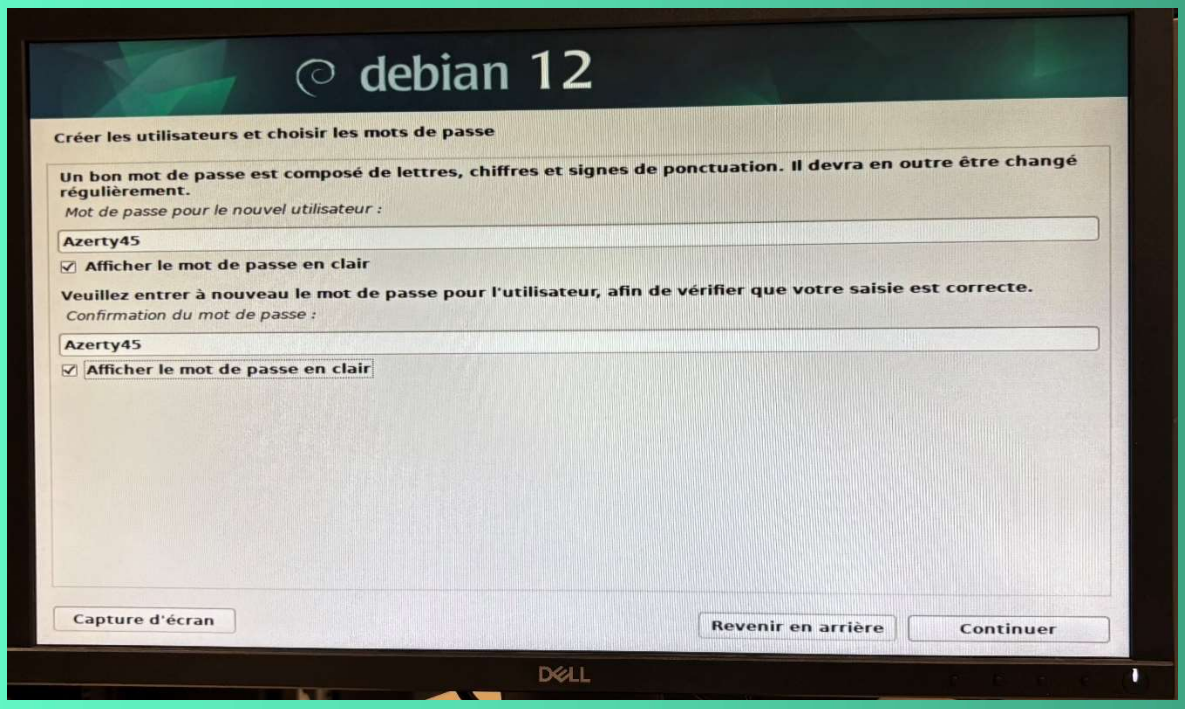
Création du mot de passe pour le compte superutilisateur / d'administration du système



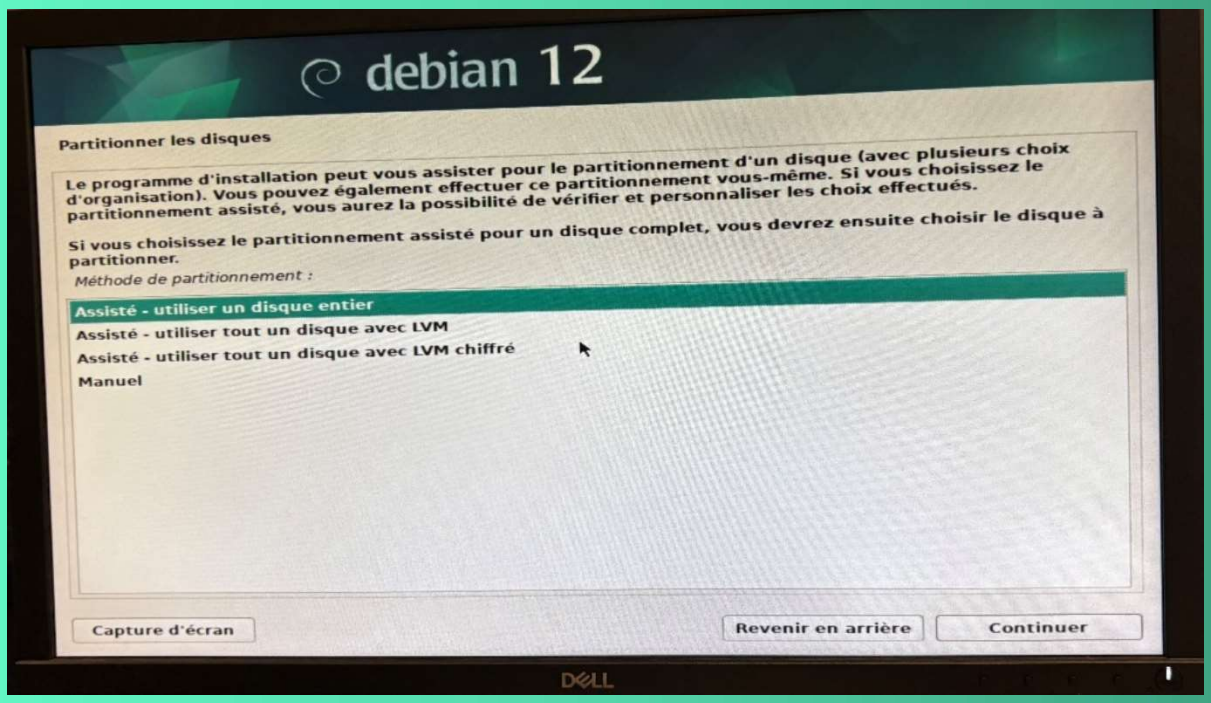
Créer le compte du nouvel utilisateur en choisissant l'identifiant du compte utilisateur



Choisir le mot de passe du compte utilisateur



Méthode de partitionnement



Choisir le disque

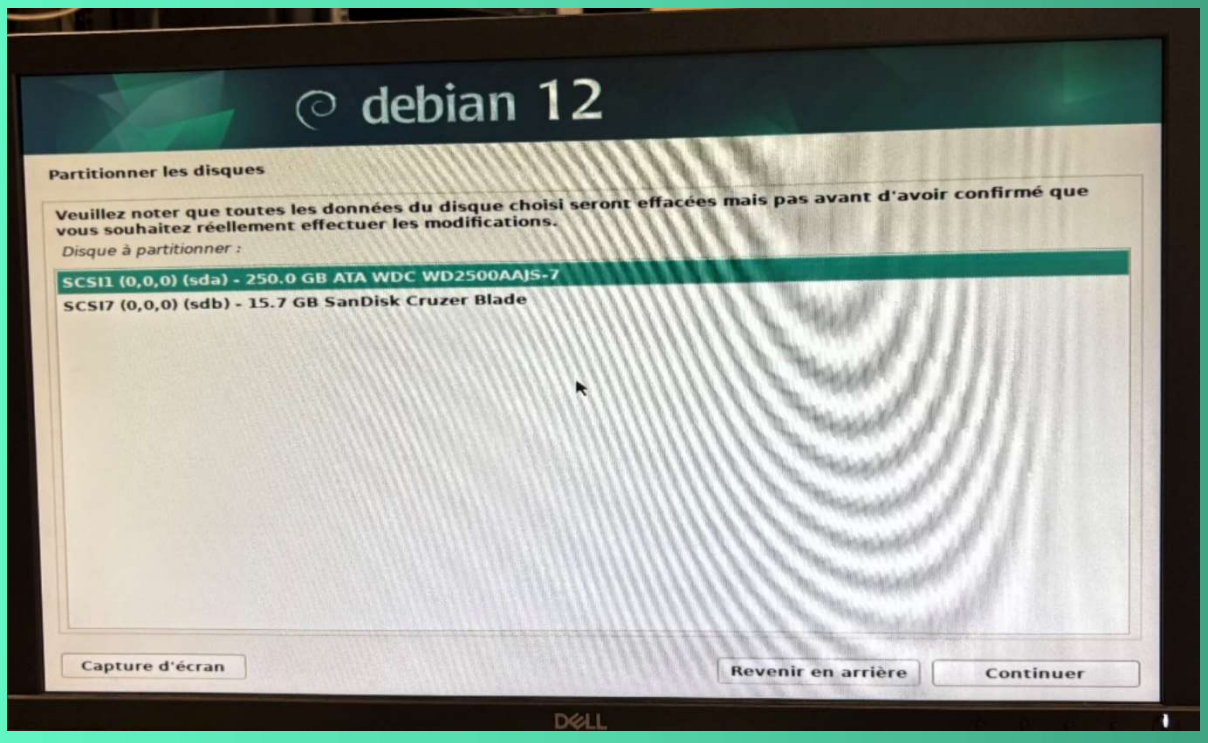
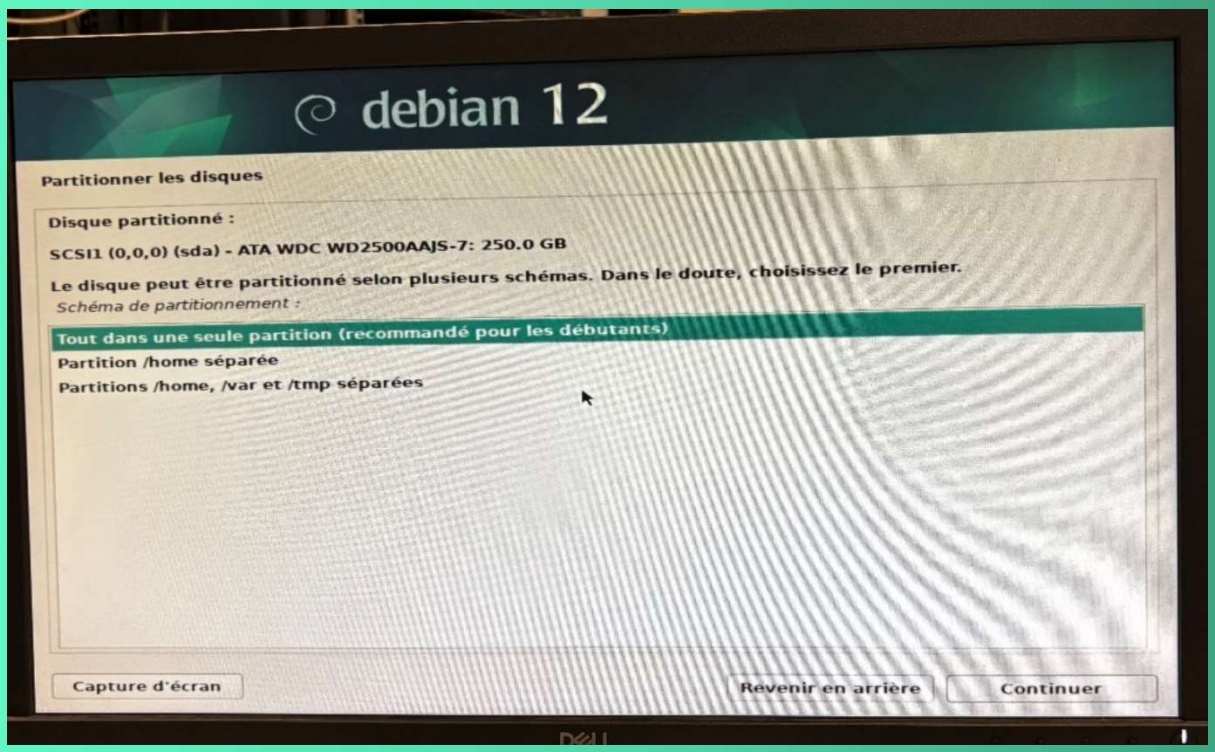
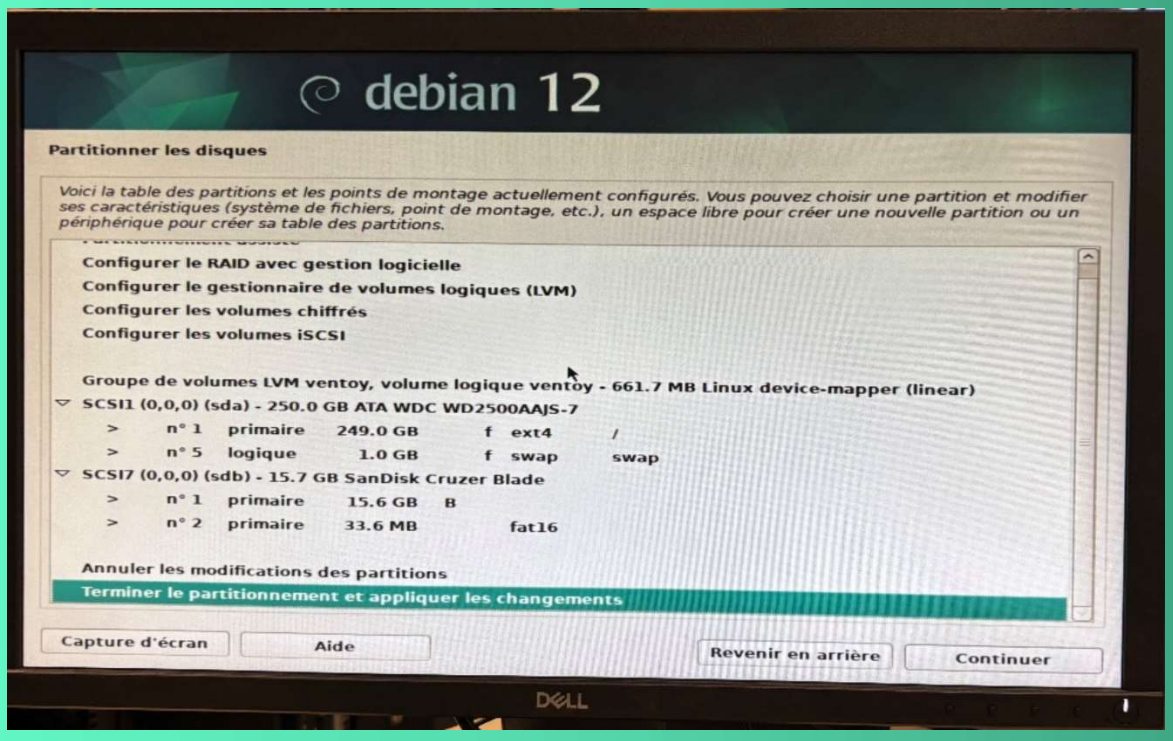


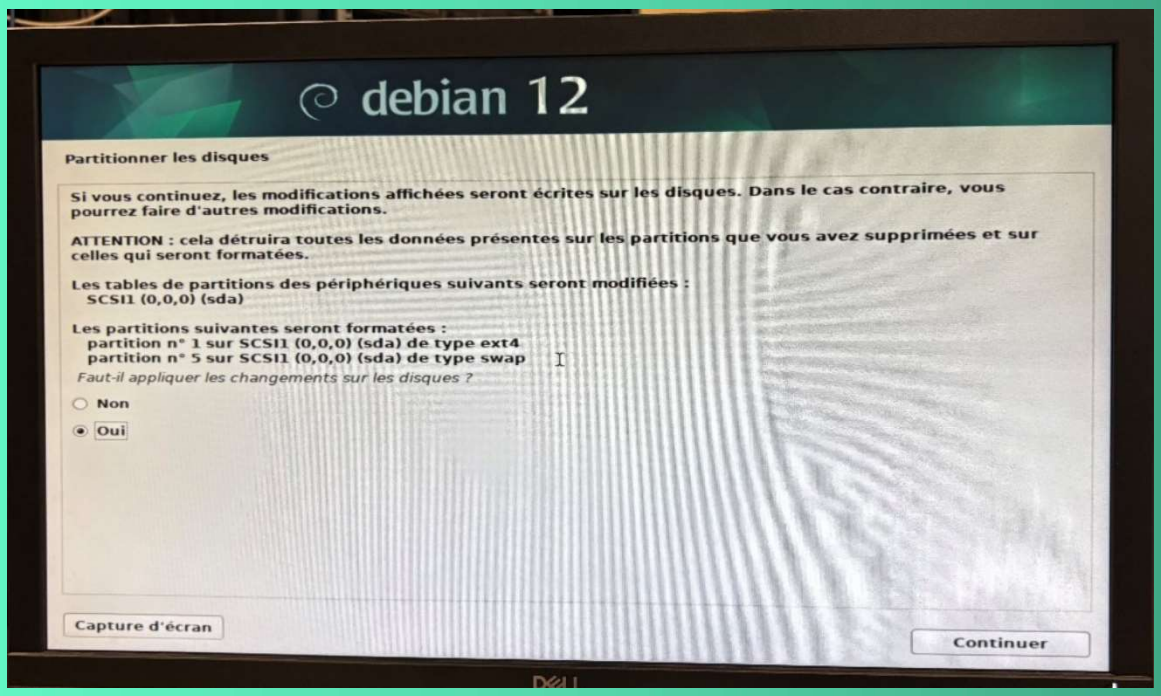
Schéma du partitionnement



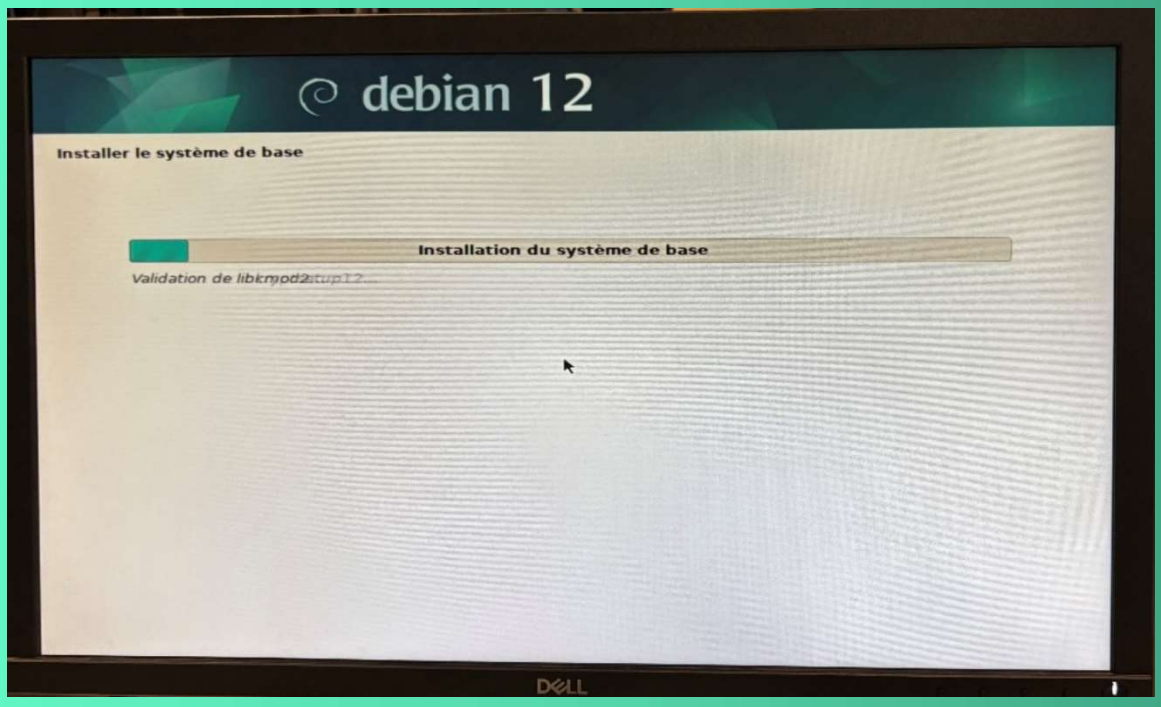
Terminer le partitionnement et appliquer les changements



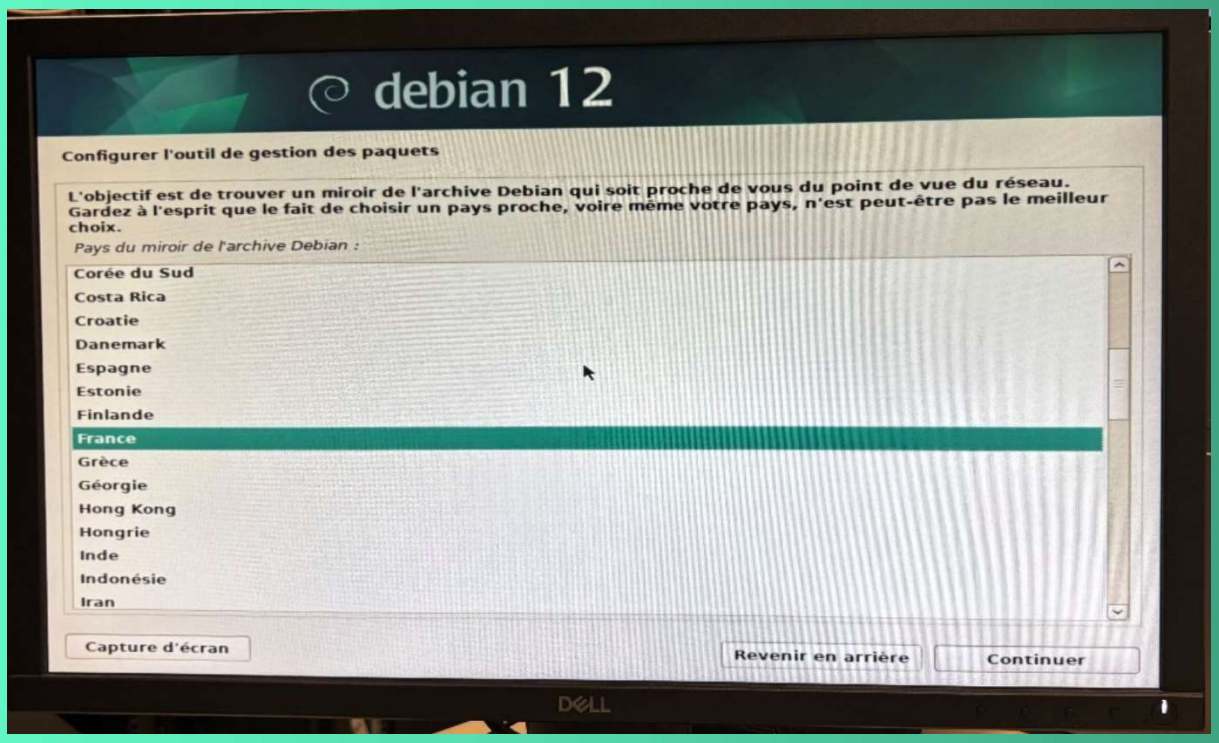
Appliquer les changements sur les disques



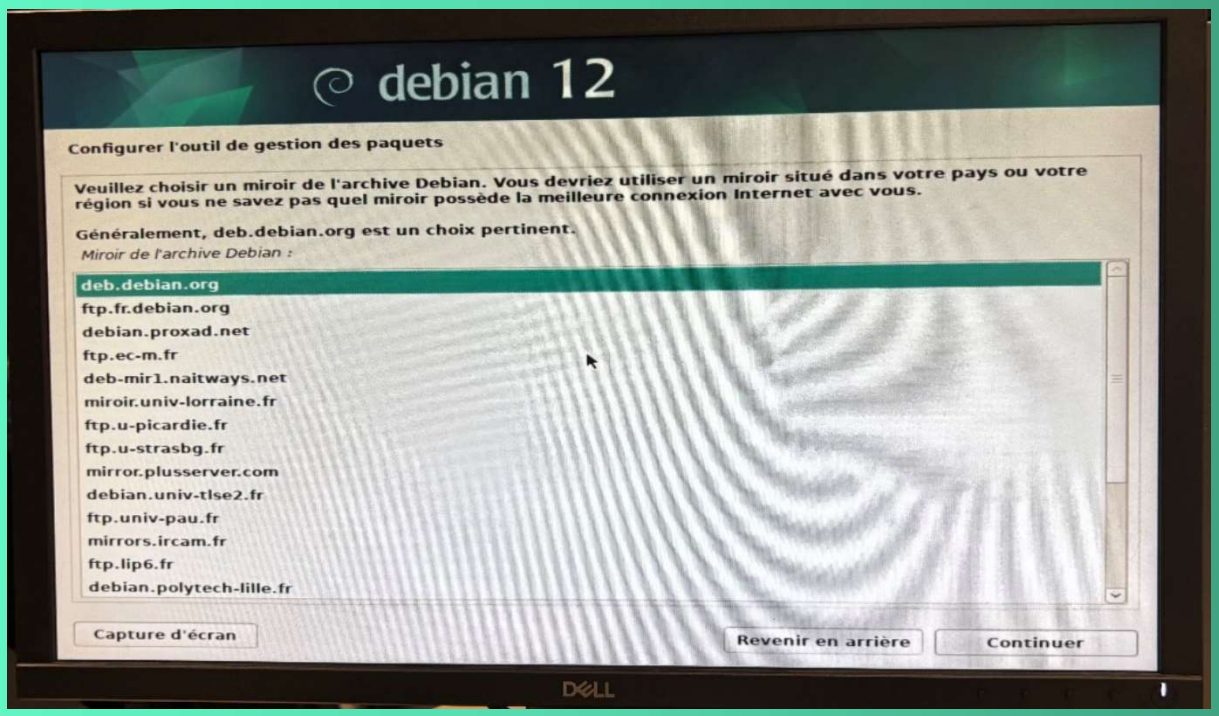
Installation du système de base



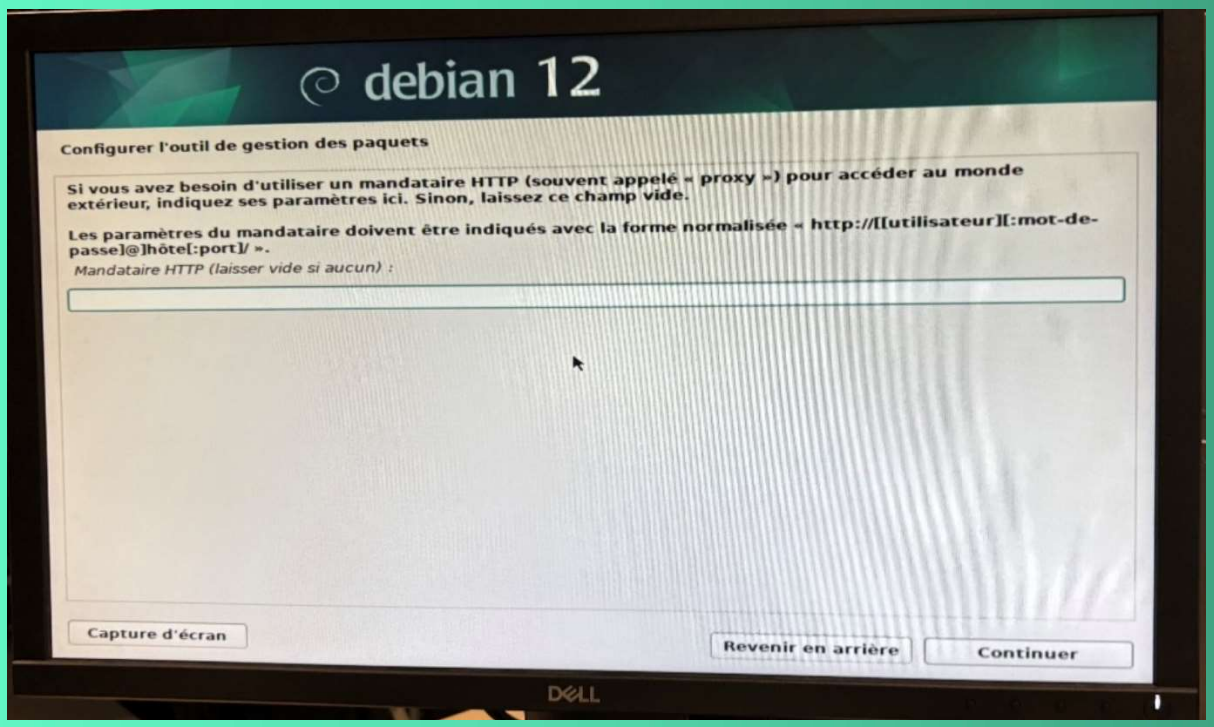
Choisir un miroir de l’archive en prenant le pays le plus proche



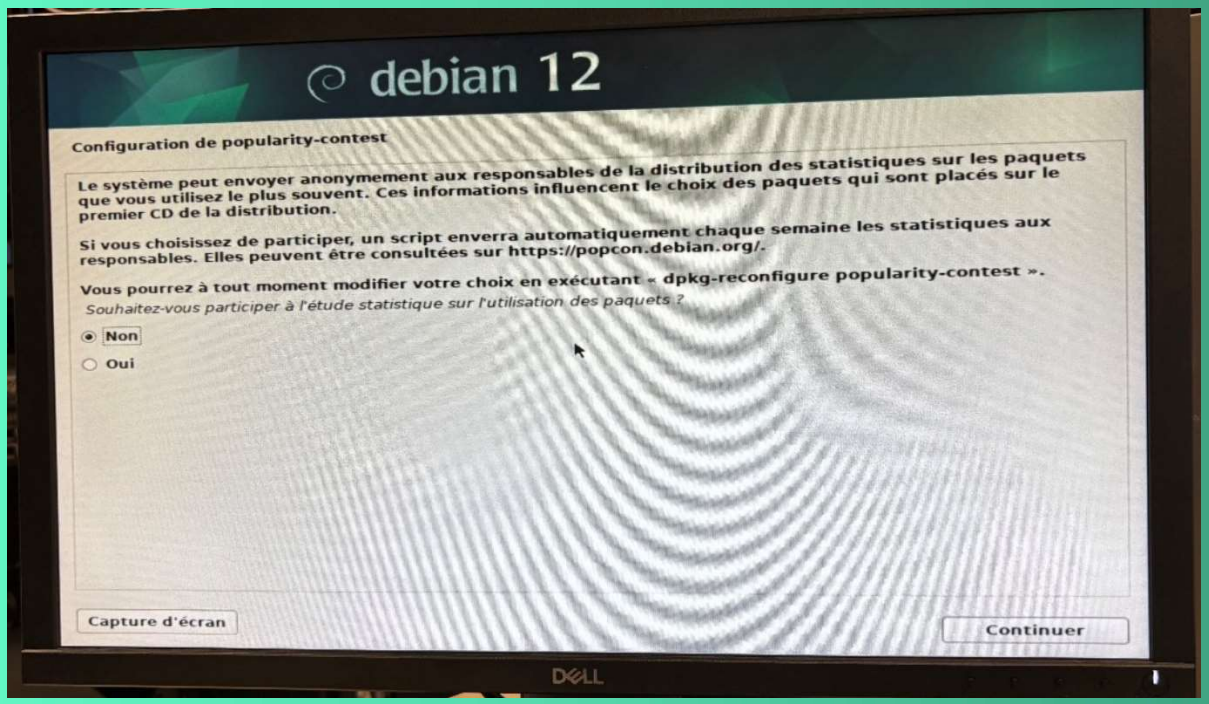
Choisir le miroir de l’archive Debian



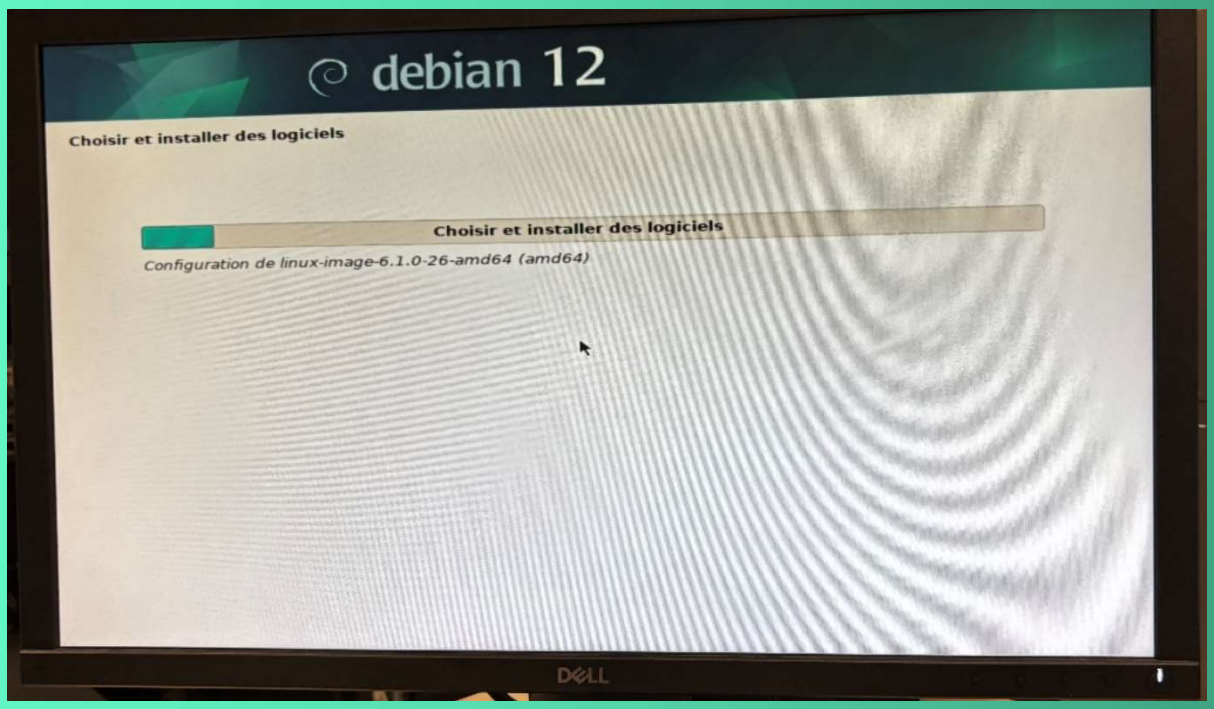
Pas de mandataire http



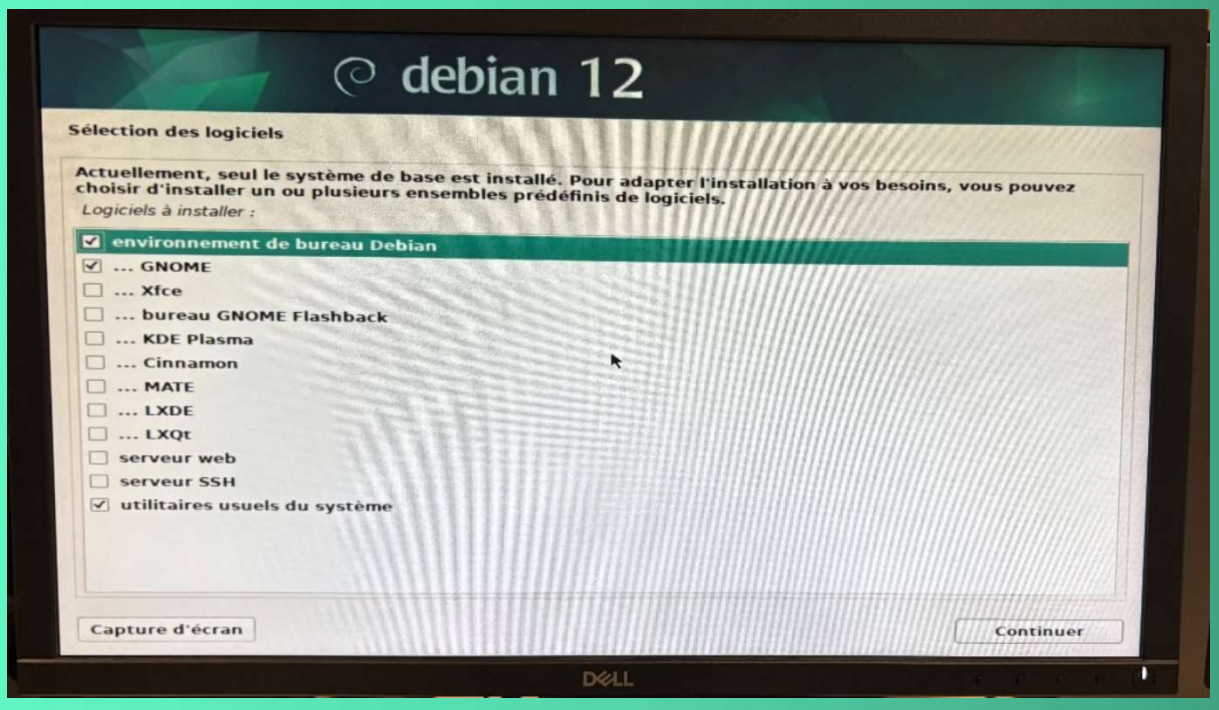
Configurer le popularity-contest



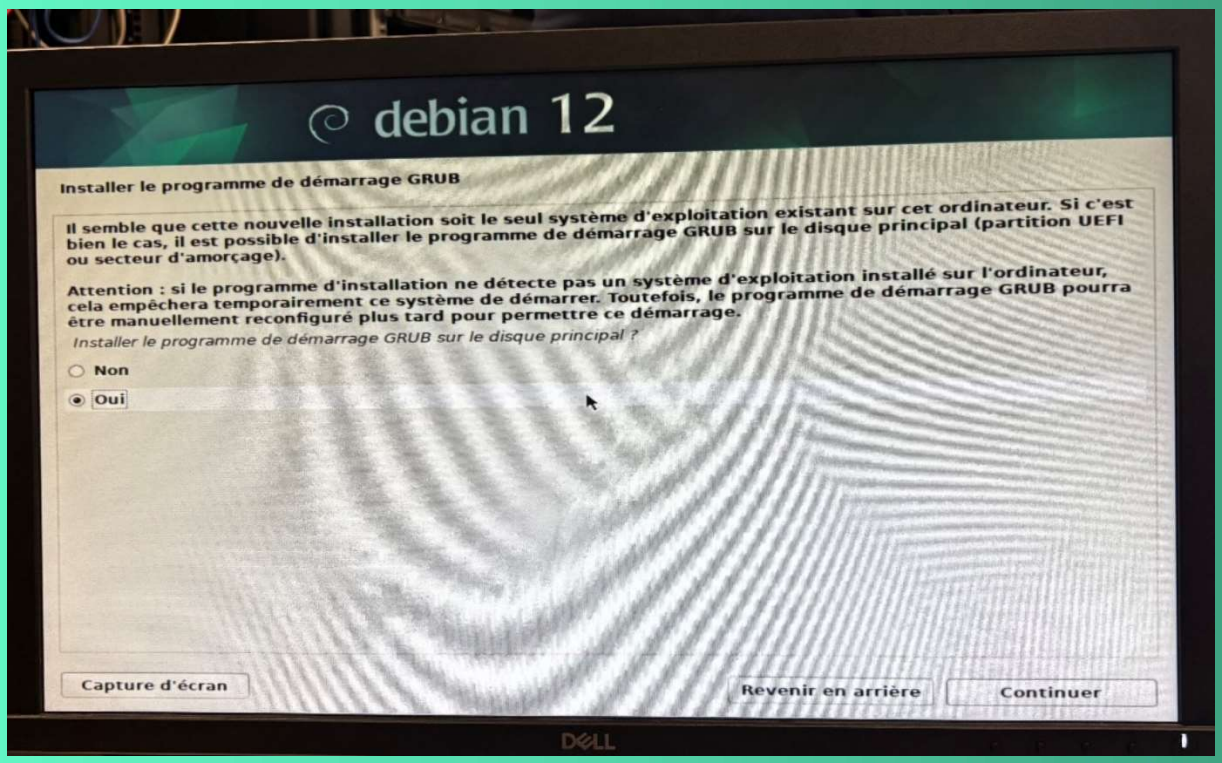
Installation des logiciels



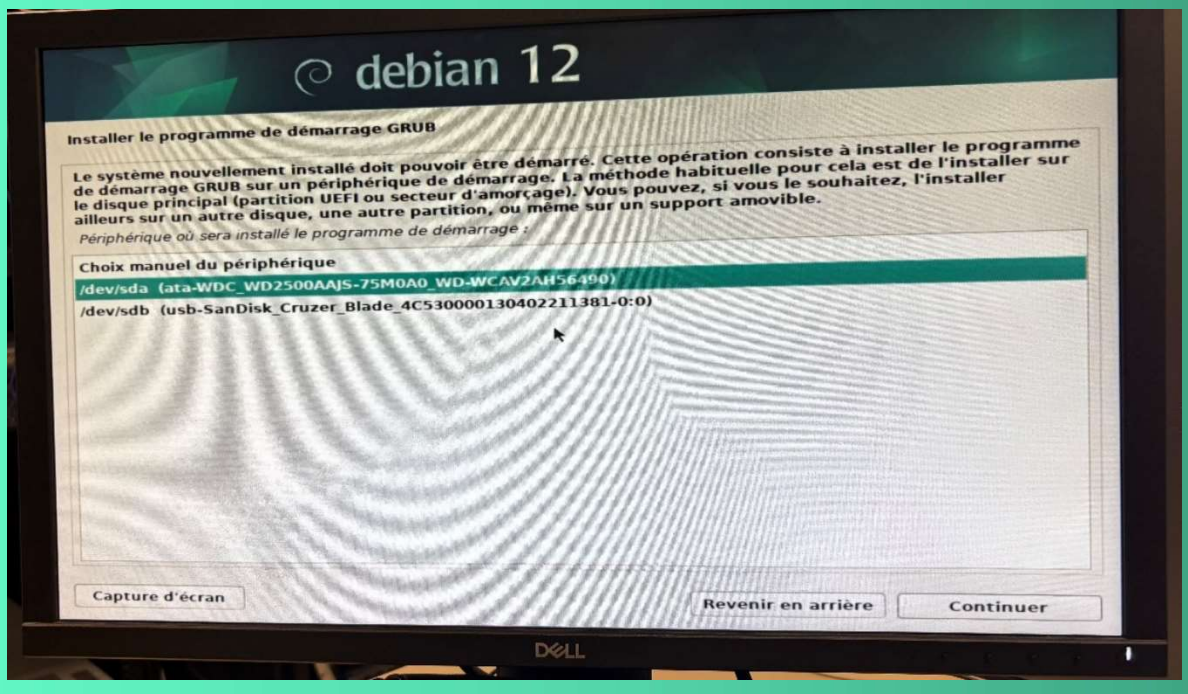
Choix de logiciels prédéfinis



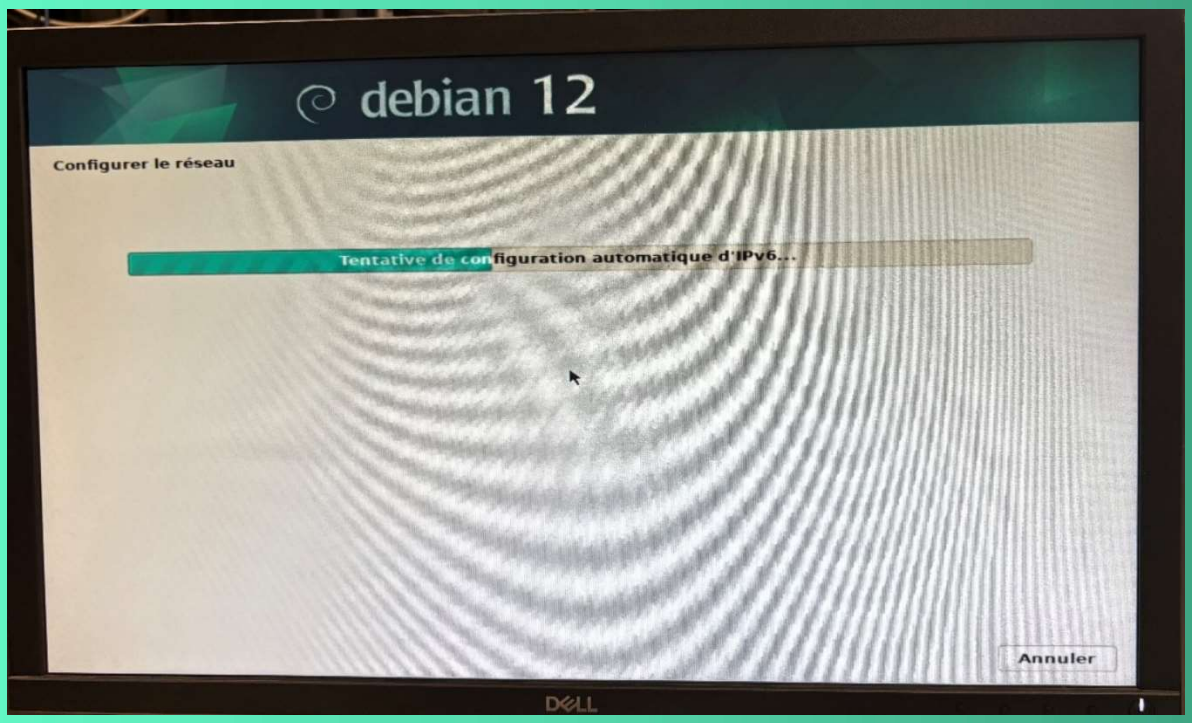
Installer le programme de démarrage GRUB



Installer le périphérique de démarrage



Fin de l’installation



CONFIGURATION DU FIREWALL

Avant de mettre en place le routage, il faut tout d'abord configurer la machine.

Configuration des cartes réseaux :

Enp0s25 (lien LAN)

Auto enp0s25

Iface enp0s25 inet static

Adress 172.21.3.254/16

Enp4s0 (lien DMZ)

Auto enp4s0

Iface enp4s0 inet static

Adress 192.168.100.254/24

Enp4s2 (lien INTERNET)

Auto enp4s2

Iface enp4s2 inet static

Adress 172.20.34.212/16

Gateway 172.20.2.254

Tests réalisés :

Nous avons envoyé une requête ICMP sur l'adresse 172.20.3.250 depuis un ordinateur en 172.20.34.11

```
C:\Users\gurochon>ping 172.20.3.254

Envoi d'une requête 'Ping'  172.20.3.254 avec 32 octets de données :
Réponse de 172.20.3.254 : octets=32 temps<1ms TTL=64
Réponse de 172.20.3.254 : octets=32 temps<1ms TTL=64
Réponse de 172.20.3.254 : octets=32 temps<1ms TTL=64
Réponse de 172.20.3.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 172.20.3.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Modifier dans le fichier etc/resolv.conf

Nameserver 8.8.8.8

Nameserver 1.1.1.1

Mise en place du routage

Pour mettre en place le routage le routage, il faut se rendre dans le fichier

Etc/sysctl.conf puis décommenter la ligne net.ipv4.ip_forward=1

Ensuite, dans le fichier proc/sys/net/ipv4/ip_forward puis remplacé le 0 par un 1

Tests réalisés :

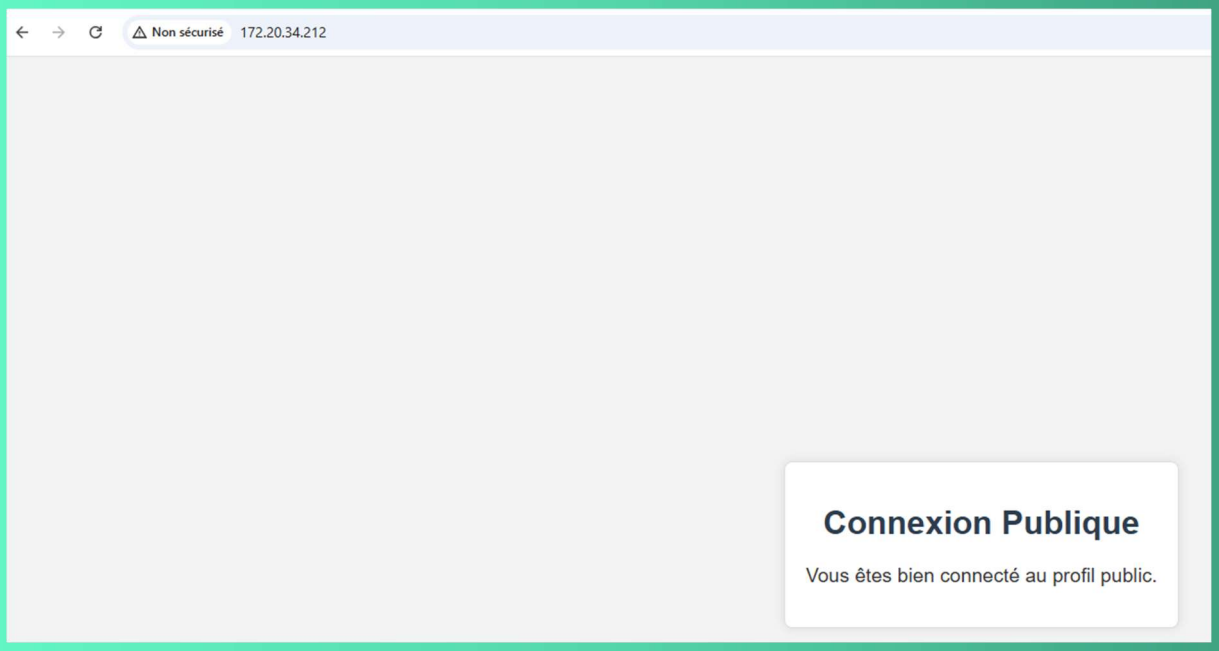
Depuis une machine cliente en 172.20.34.12 à accéder au site internet présent sur le serveur IIS en 192.168.100.10 sur le port 80

Redirection au site web :

Iptables -t nat -A PREROUTING -p tcp –dport 8012 -i enp4s2 -j DNAT –to-destination 192.168.100.10 :80

Iptables -t nat -A POSTROUTING -o enp4s2 -j MASQUERADE

Tests réalisés :



Sur les VM, activer le mode promiscuité allow all en cas d'erreur

Règles iptables

Activer le pare-feu :

Iptables -P INPUT DROP

Iptables -P OUTPUT DROP

Iptables -P FORWARD DROP

Autoriser toutes les connexions déjà établies :

Iptables -A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT

Autoriser le SSH pour seulement l'adresse IP 172.20.34.12 :

Iptables -A INPUT -p tcp –dport 22 -s 172.20.34.12 -j ACCEPT

Iptables -A OUTPUT -p tcp –sport 22 -d 172.20.34.12 -j ACCEPT

test en ssh depuis le pc en 172.20.34.12 sur l'interface du routeur 172.20.34.212

```
C:\Users\thmichel>ssh gt@172.20.34.212
gt@172.20.34.212's password:
Linux BEG-RTRL-03 6.1.0-27-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-11-01) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 20 15:47:45 2024 from 172.20.34.12
gt@BEG-RTRL-03:~$
```

Test en ssh depuis le pc en 192.168.100.1233 sur l'interface du routeur 192.168.100.254

```
C:\Users\gurochon>ssh gt@192.168.100.254
ssh: connect to host 192.168.100.254 port 22: Connection timed out
```

Autoriser l'accès a la DMZ depuis internet :

Iptables -A FORWARD -p tcp --dport 80 -d 192.168.100.10 -j ACCEPT

Comment sauvegarder ses règles iptables :

Pour sauvegarder iptables, il faut installer iptables-persistent

Apt install iptables-persistent

Les règles sont enregistrées dans le fichier de configuration /etc/iptables/rules.v4. Ces règles seront chargées au prochain redémarrage de la machine.

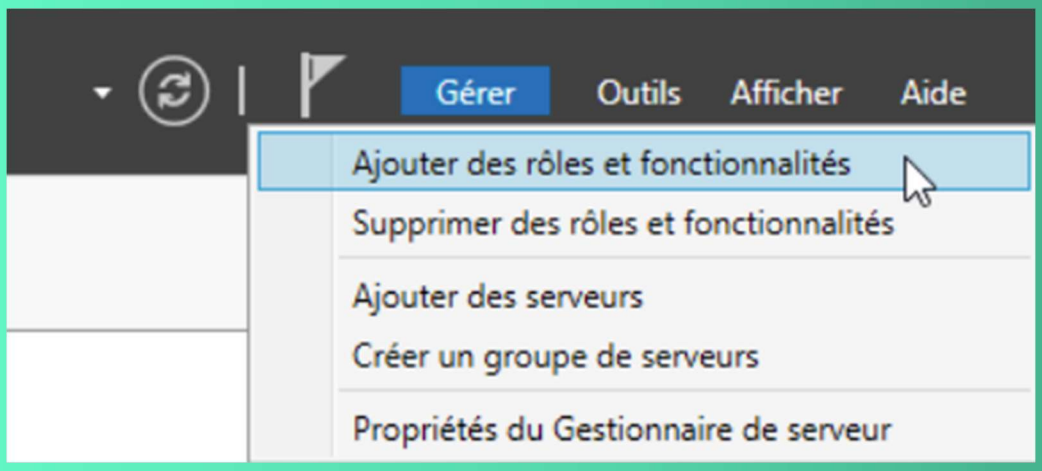
Avec la commande netfilter-persistent save, les règles iptables sont enregistrer dans le fichier :

/usr/share/netfilter-persistent/plugins.d/15-ip4tables save

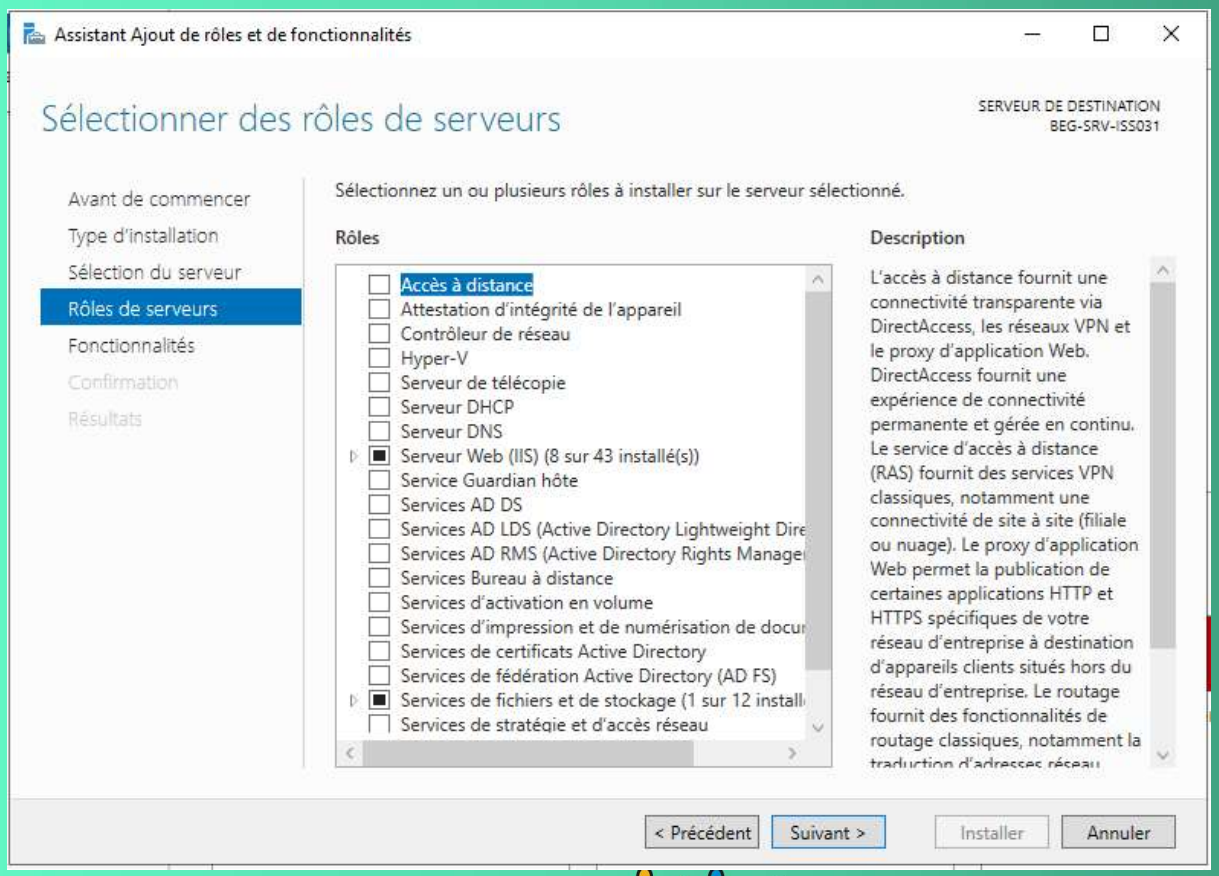
Restart le service avec la commande systemctl restart netfilter-persistent.service

CONFIGURATION D'UN SERVEUR ISS

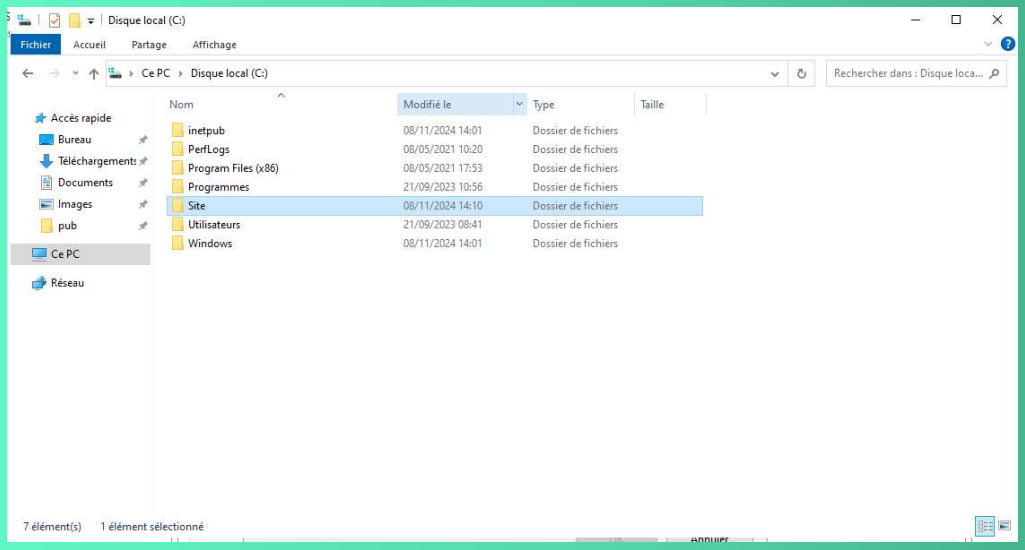
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur 'Gérer' et 'Ajouter des rôles et fonctionnalités'.



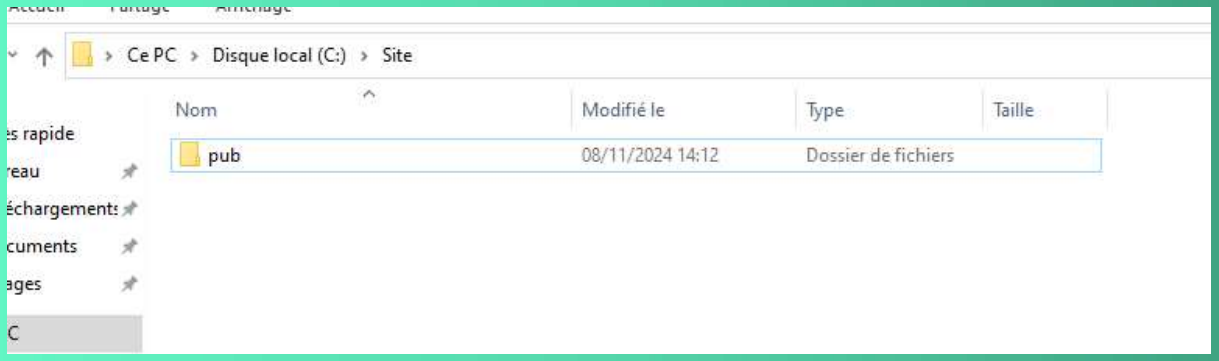
Dans l'onglet 'Rôles de serveurs', cocher 'Serveur Web (IIS)



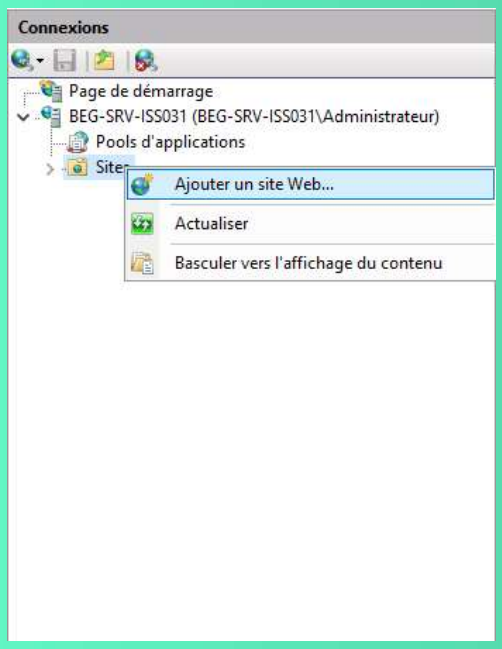
Ensuite, créer un dossier sur notre disque C



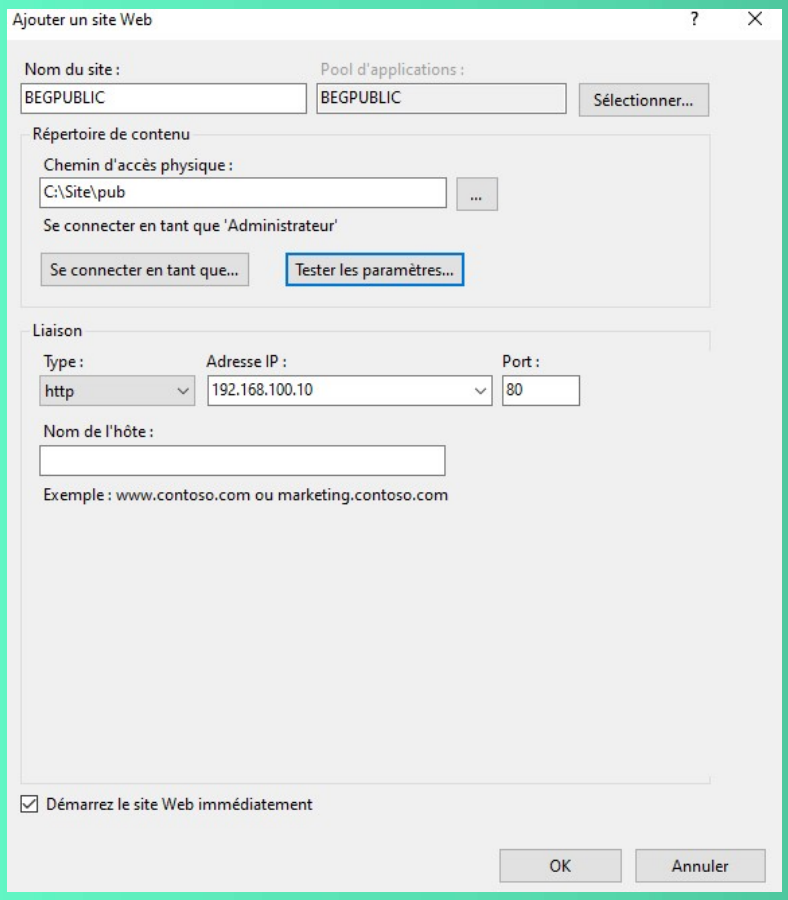
Comme sous-dossiers ‘pub’ signifiant que le site sera public



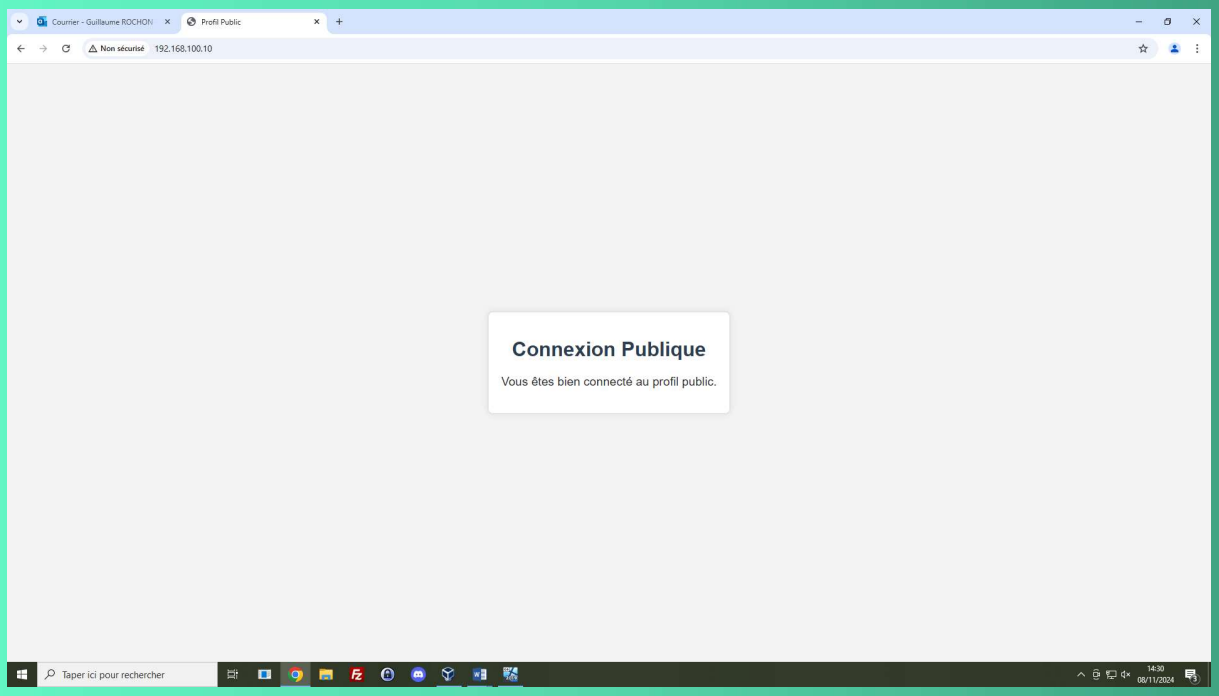
Pour le site « pub » crée un ficher html avec une indication pour vérifier que c’est bon



Tester la connexion à son site web



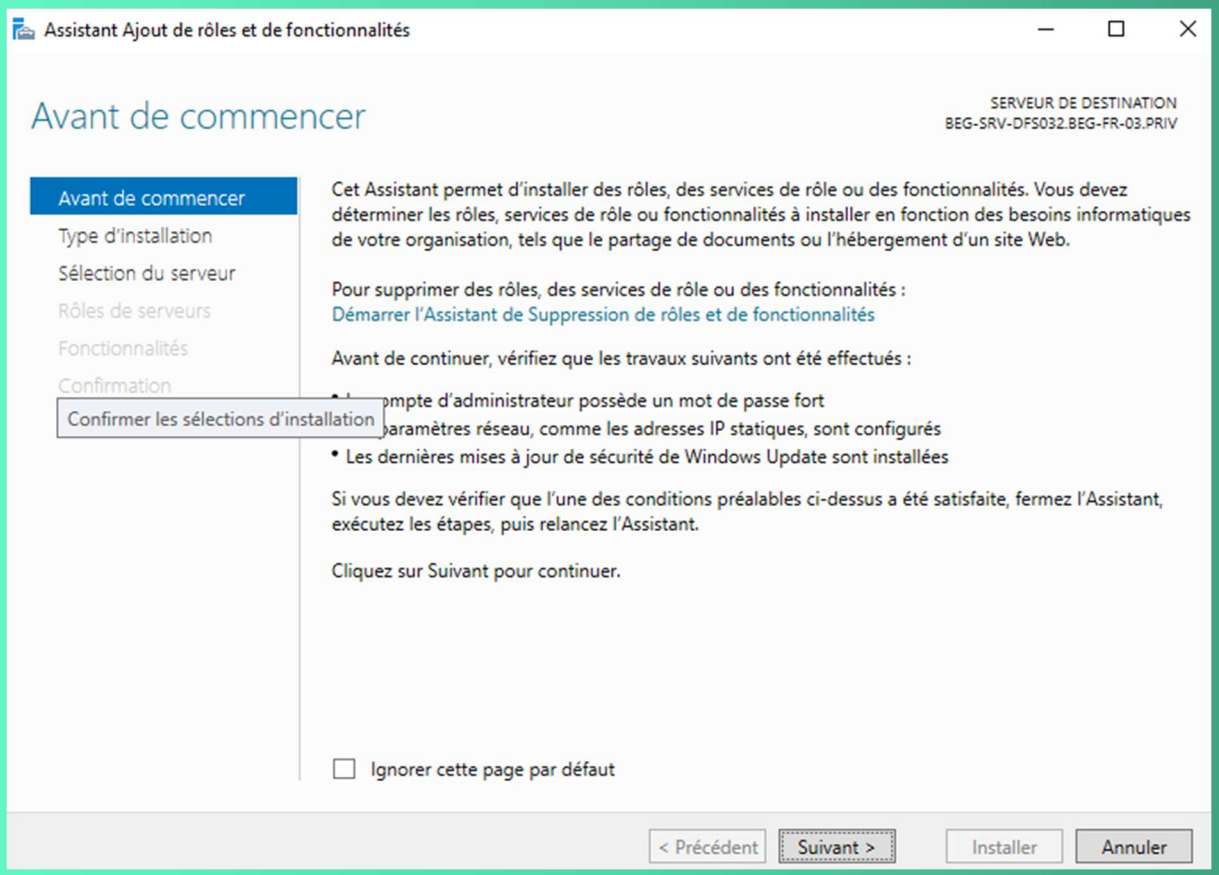
Résultat :



CONFIGURATION D'UN SERVEUR DFS

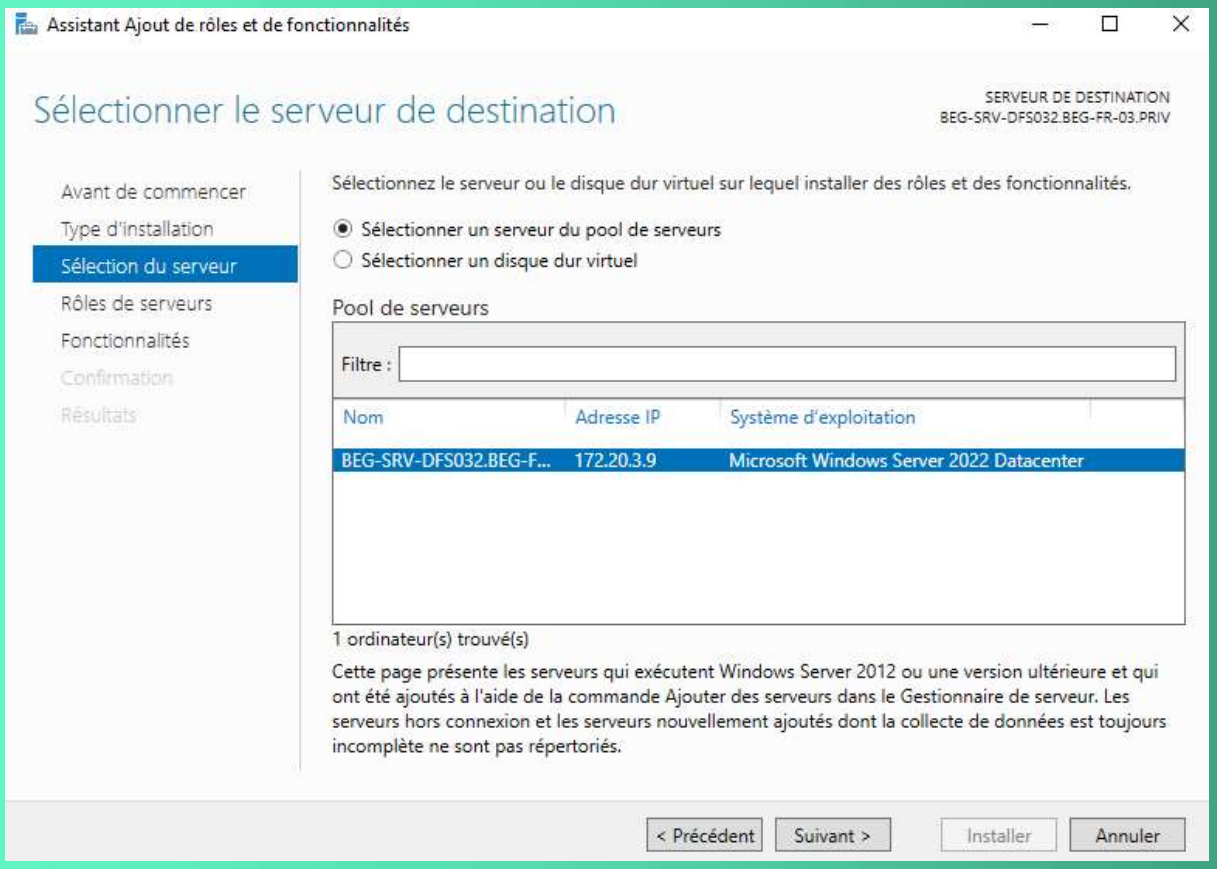
Installation du service :

Commencez par ouvrir le « Gestionnaire de serveur », cliquez sur « Gérer » puis « Ajouter des rôles et fonctionnalités » dans le menu. Cliquez sur « Suivant » afin de passer l'étape « Avant de commencer ».

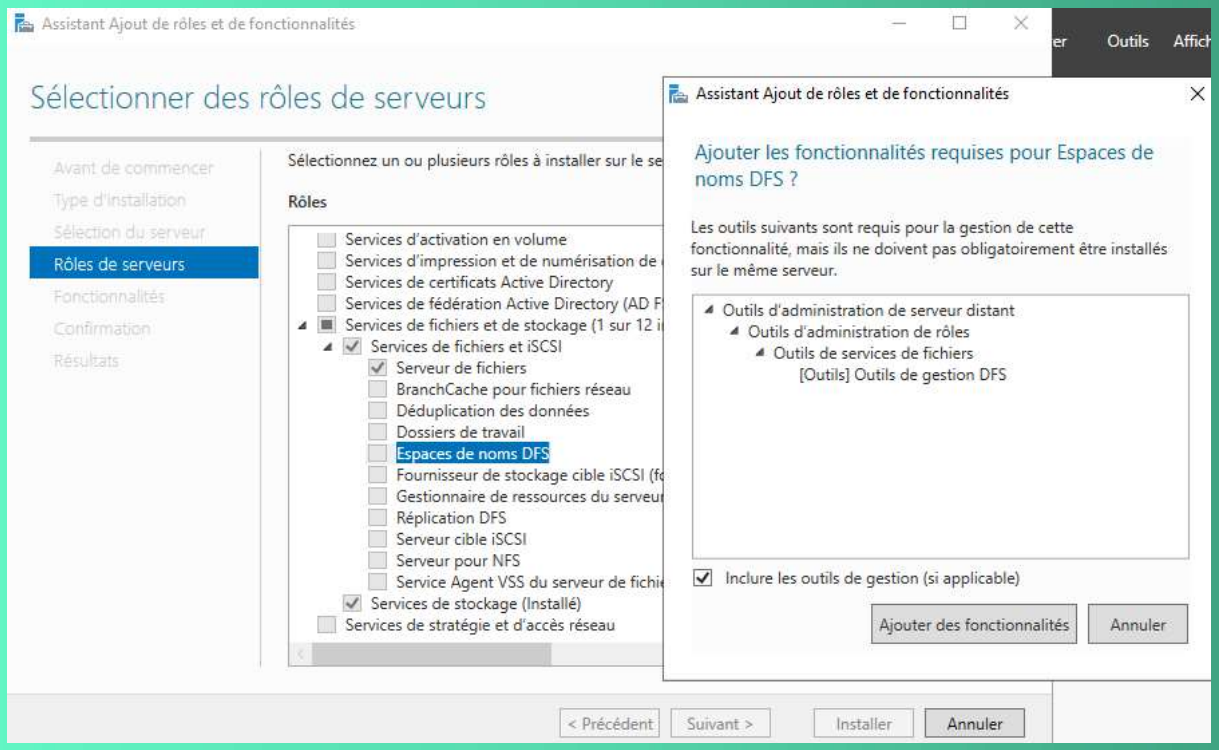


Concernant le « Type d'installation », laissez le choix par défaut et cliquez sur « Suivant ».

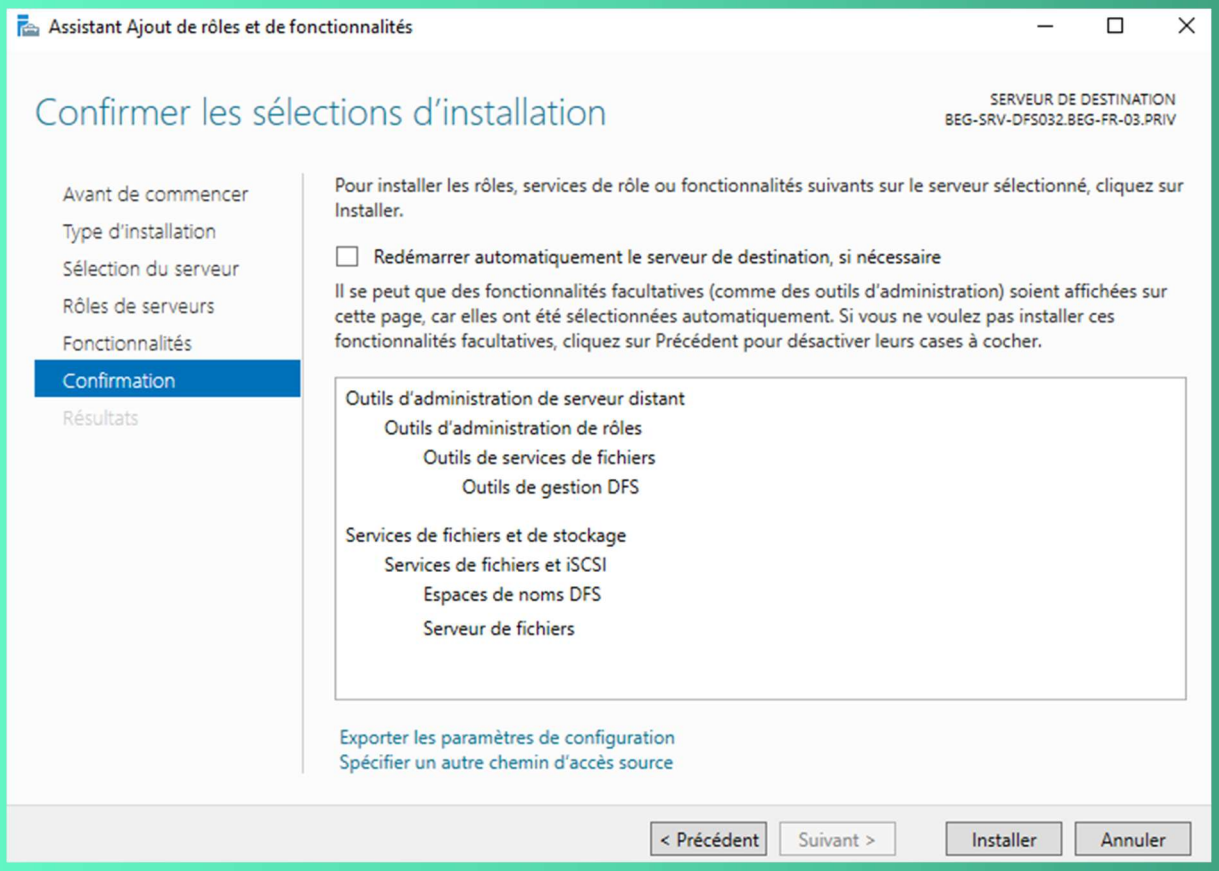
Sélectionnez le serveur sur lequel vous souhaitez installer le serveur DFS, puis, cliquez sur « Suivant » une nouvelle fois.



Cliquez sur « Service de fichiers et de stockage » puis sous « Services de fichiers et iSCSI » cochez « Espaces de nom DFS ». Une fenêtre apparaît, cliquez sur « Ajouter des fonctionnalités » pour installer les fonctionnalités nécessaires au bon fonctionnement du rôle. Cliquez sur « Suivant » deux fois.



Cliquez sur « Installer » et patientez un instant pendant l'installation des éléments.

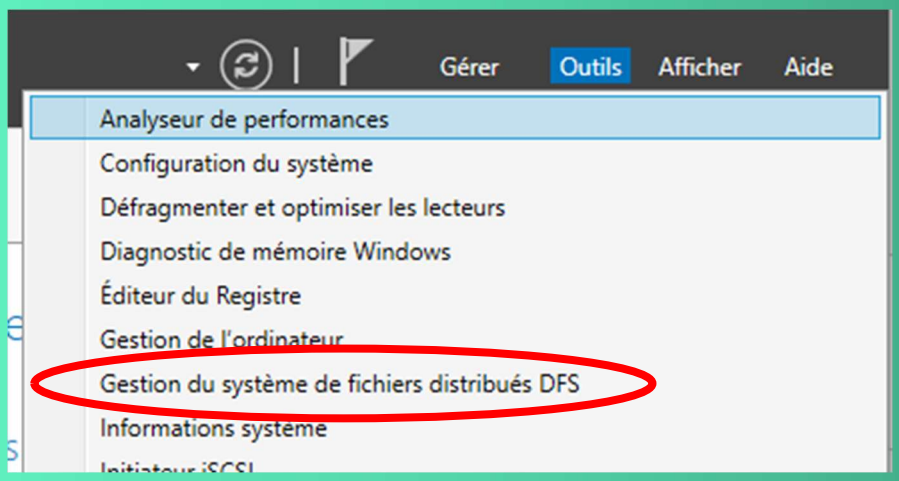


Création d'une racine DFS autonome :

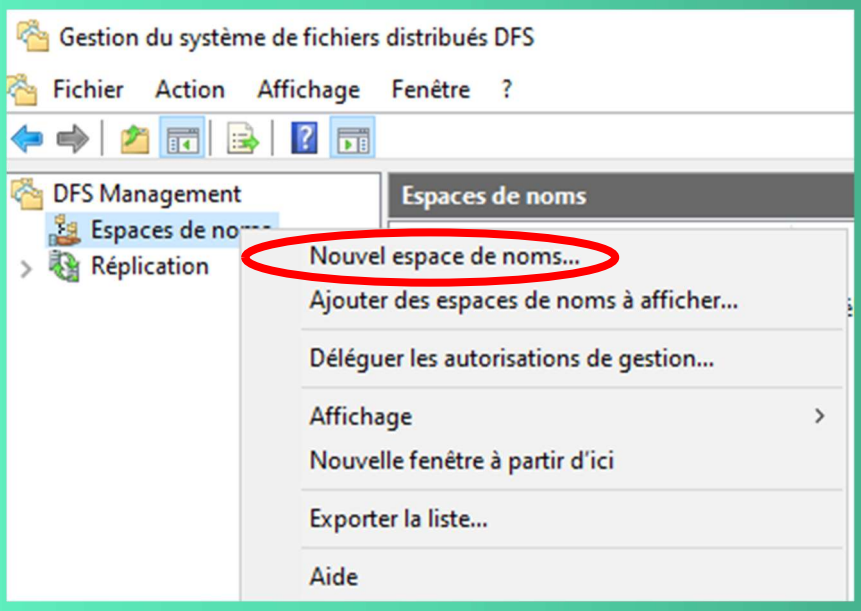
L'infrastructure décrite en début de document nécessite l'utilisation d'une racine de noms de domaine, mais, pour vous montrer la mise en place d'une racine autonome voici la procédure à suivre.

Dans ce cas, je vais créer une racine autonome nommée « BEG-AUTONOME ».

Ouvrez le gestionnaire de serveur, cliquez sur « Outils » puis ouvrez la console « Gestion du système de fichiers distribués DFS ».



Effectuez un clic droit sur « Espaces de noms » et « Nouvel espace de noms… ».



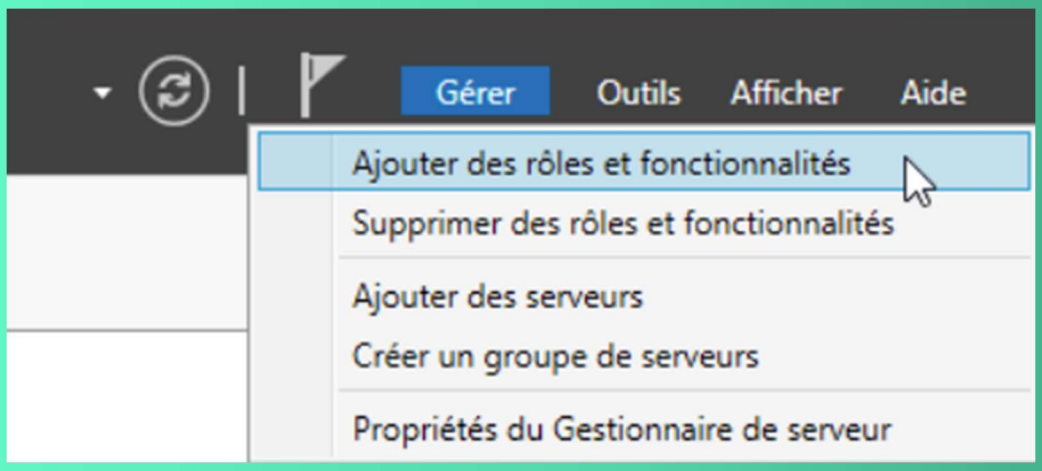
Indiquez le serveur d'espaces de noms qui hébergera donc les espaces de noms, ce serveur n'a pas vocation à héberger lui-même les données. En effet, il sert uniquement de redirecteur entre vos dossiers DFS virtuels et les dossiers partagés physiques qui contiennent les données, des données qui sont stockées sur un ou plusieurs autres serveurs.

Il est recommandé d'utiliser un serveur pour l'espace de noms, et, plusieurs autres serveurs pour l'hébergement des données.

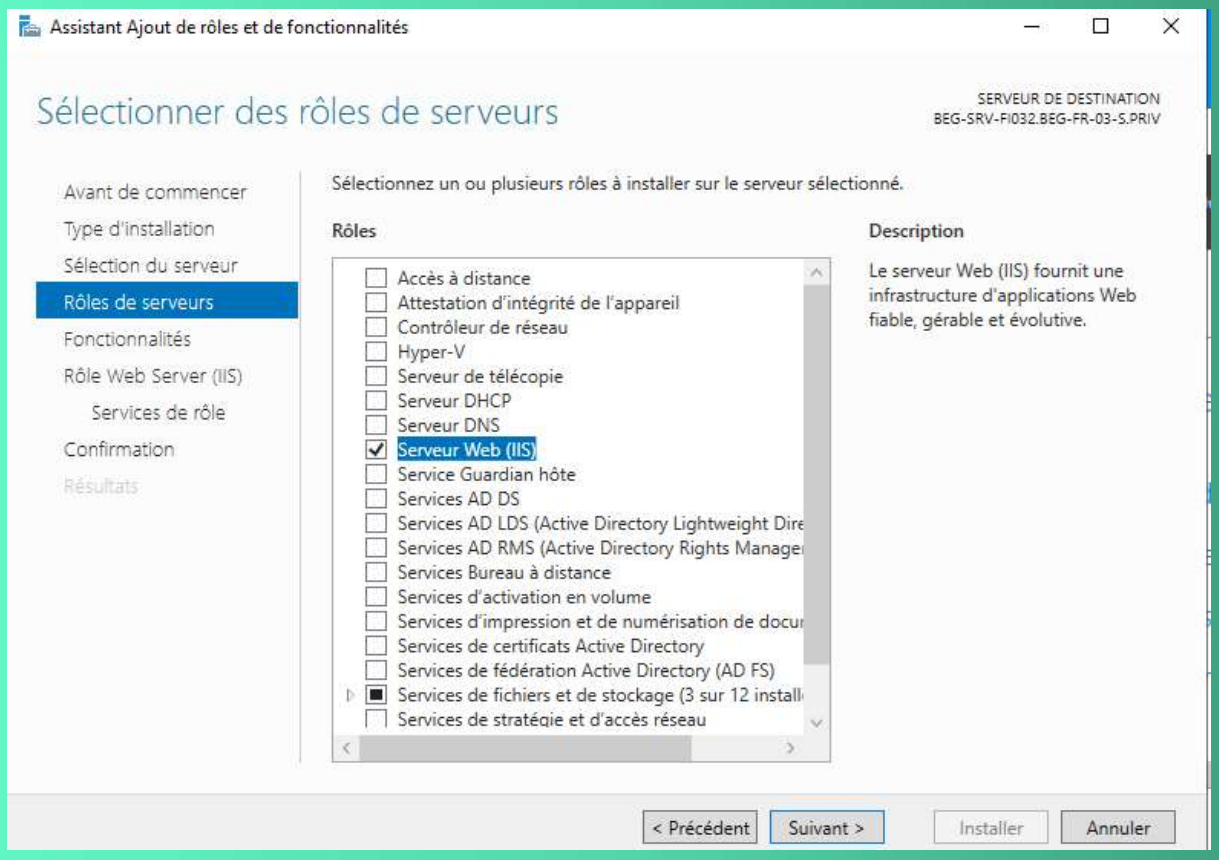
Cliquez sur « Parcourir… » pour rechercher le serveur qui hébergera l'espace de noms en cours de création. Cliquez sur « Suivant » une fois la sélection effectuée.

INSTALLER LE SERVICE IIS ET ROLE FTP

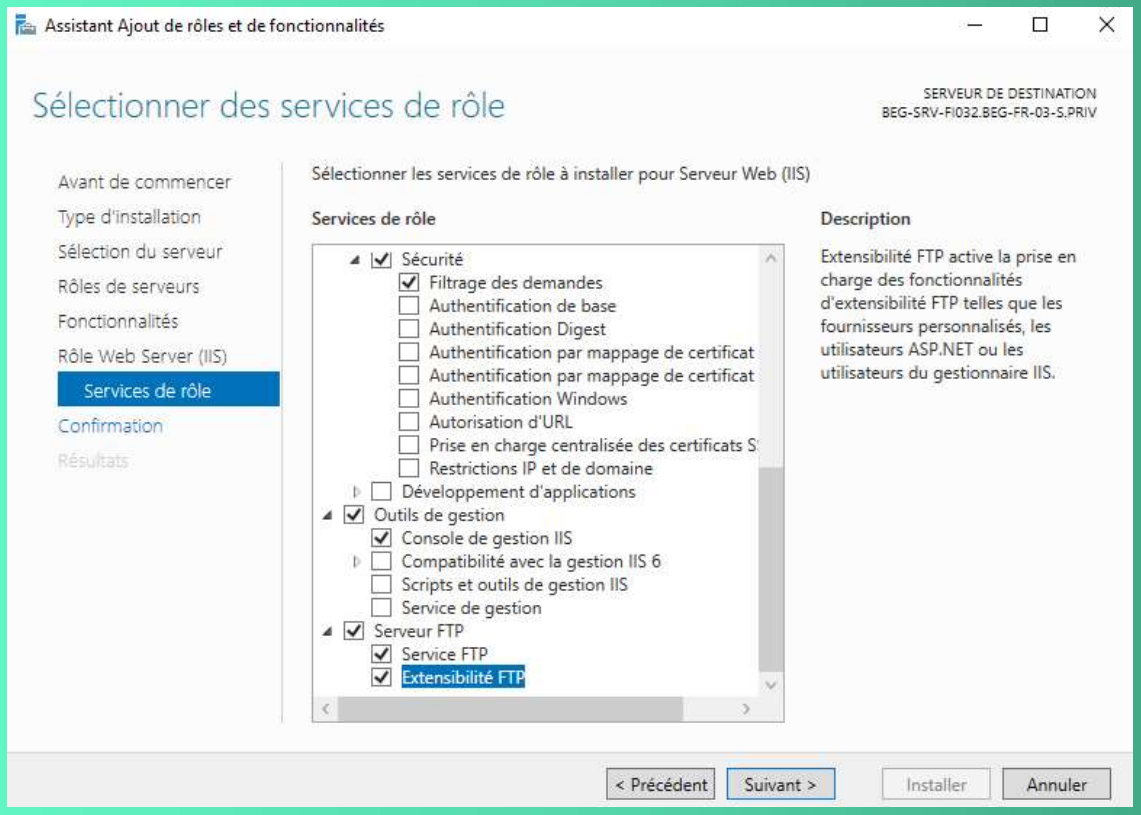
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur ‘Gérer’ et ‘Ajouter des rôles et fonctionnalités’.



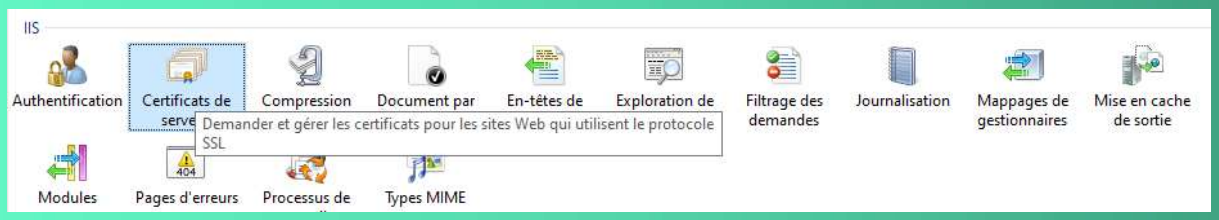
Dans l’onglet ‘Rôles de serveurs’, cocher ‘Serveur Web (IIS)



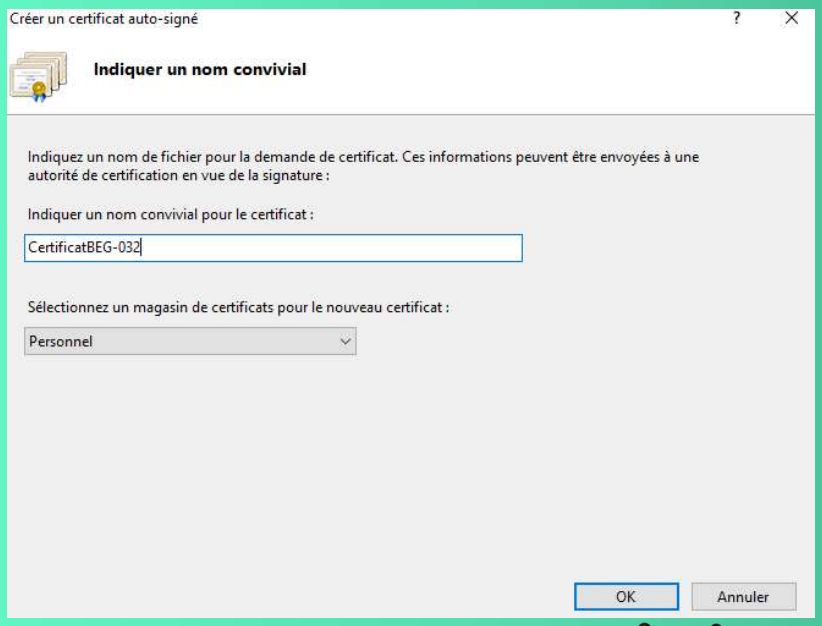
Dans l'onglet 'Services de rôle', cocher 'Service FTP' et 'Extensibilité FTP'



Créer le certificat



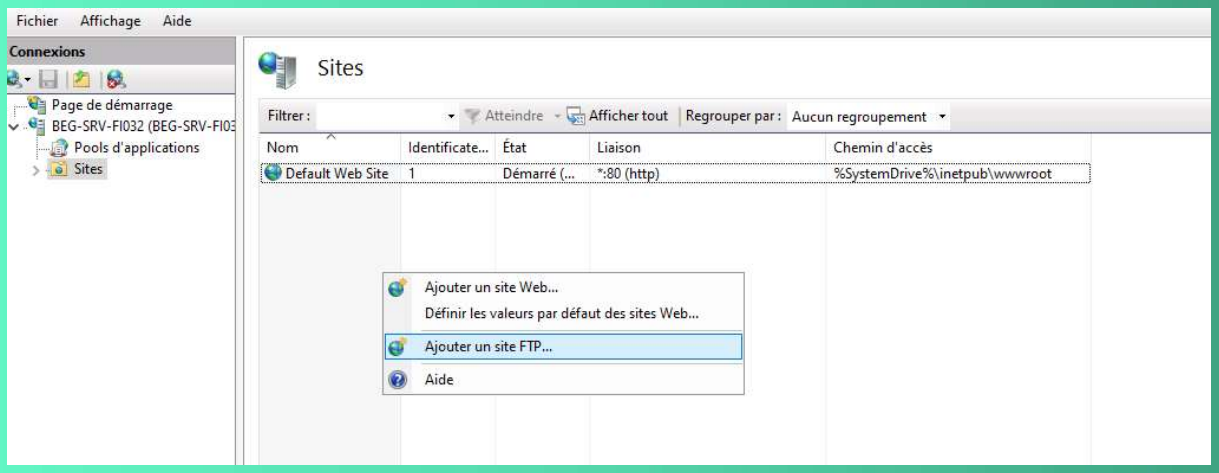
Créer un certificat autosigné



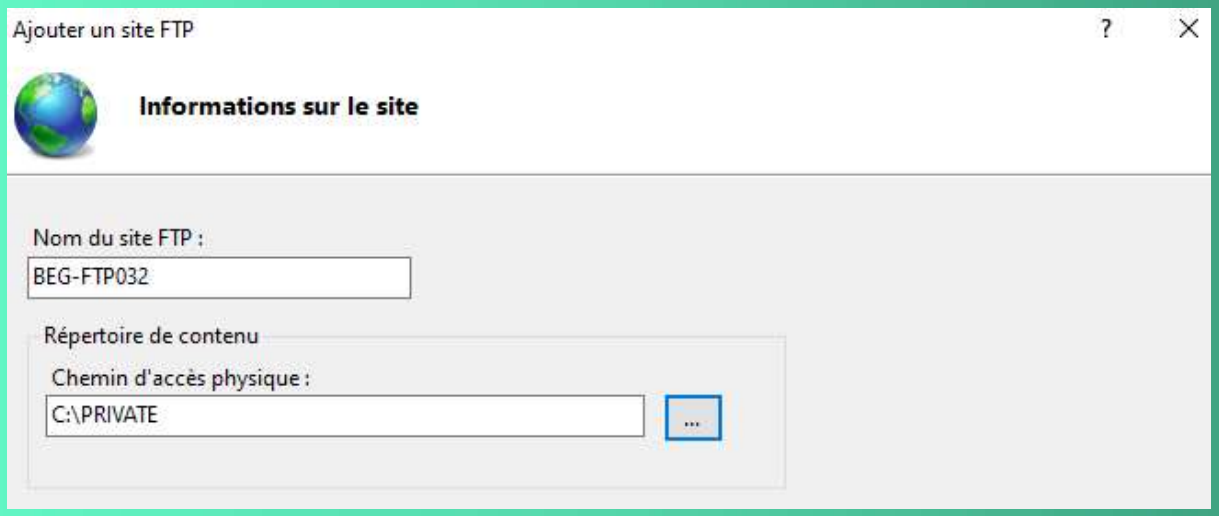
Configurer un site FTP :

Lancez le gestionnaire IIS

Faites un clic droit sur ‘Sites’ et ‘Ajouter un site FTP’

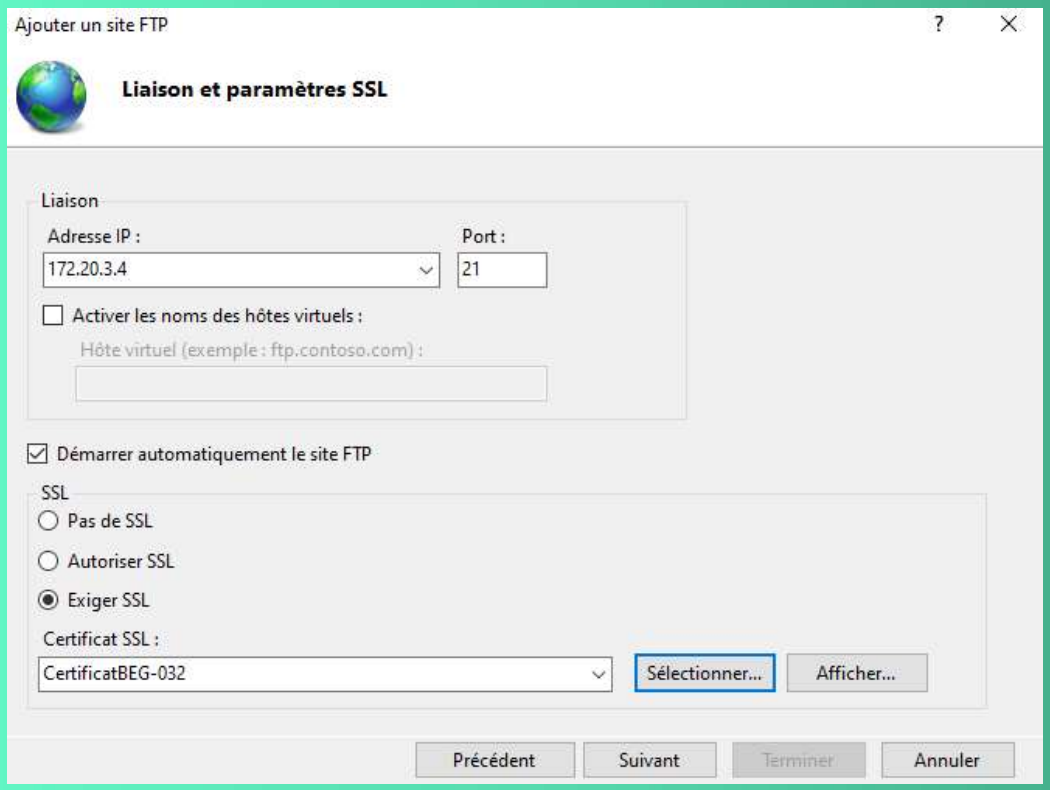


Configurer le nom du site et le chemin physique du répertoire de base

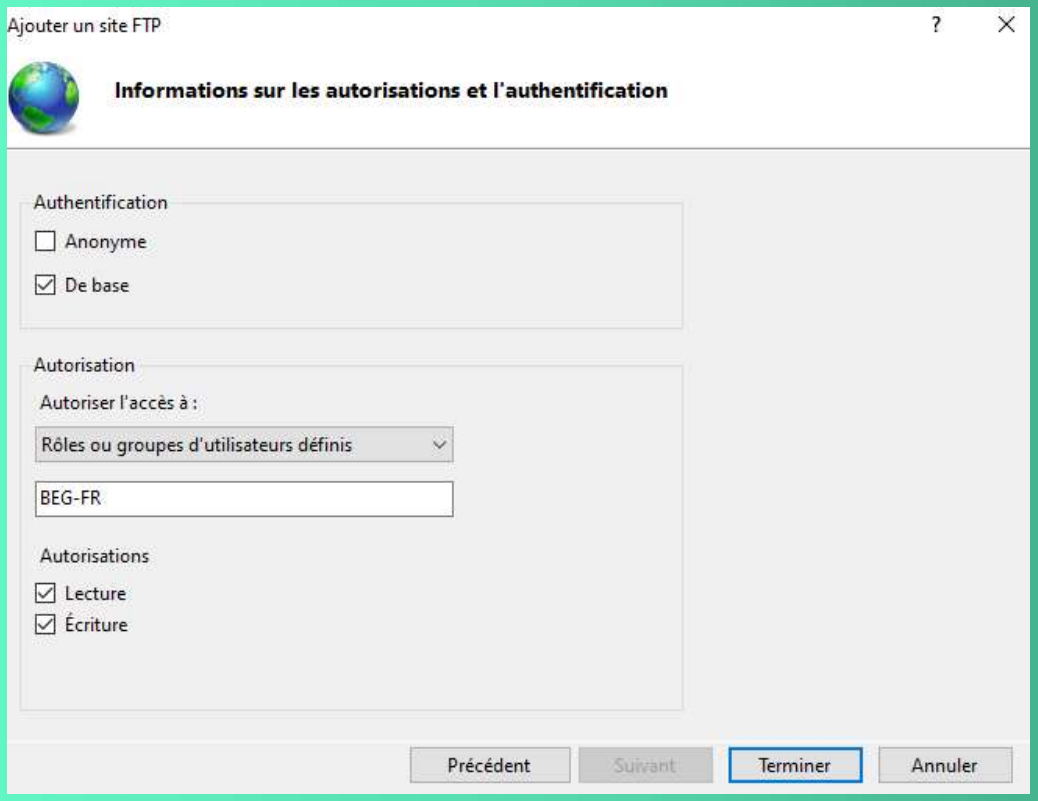


Entrer l’adresse IP et le port choisi

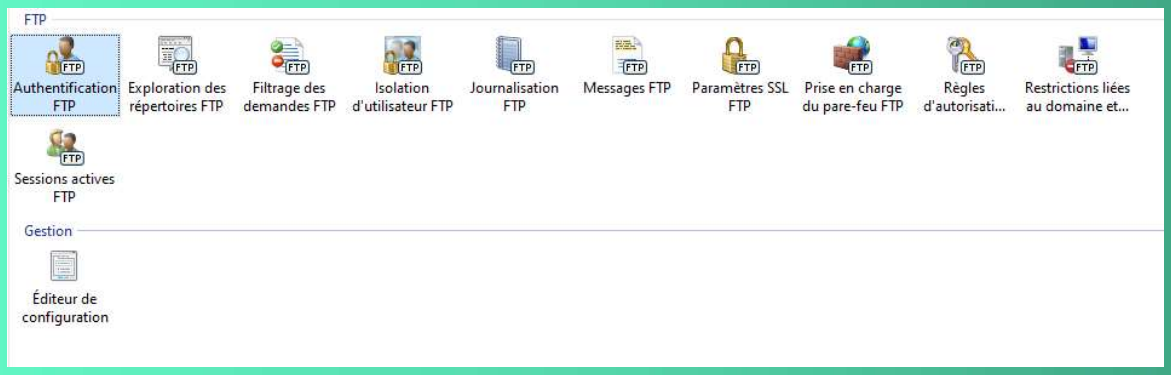
Exiger un SSL et rajouter le certificat



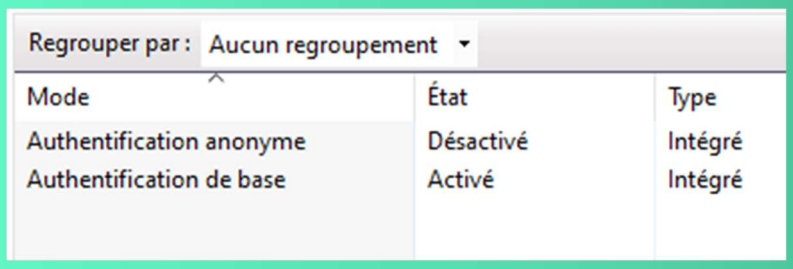
Autoriser l'accès seulement aux utilisateurs du groupe BEG-FR



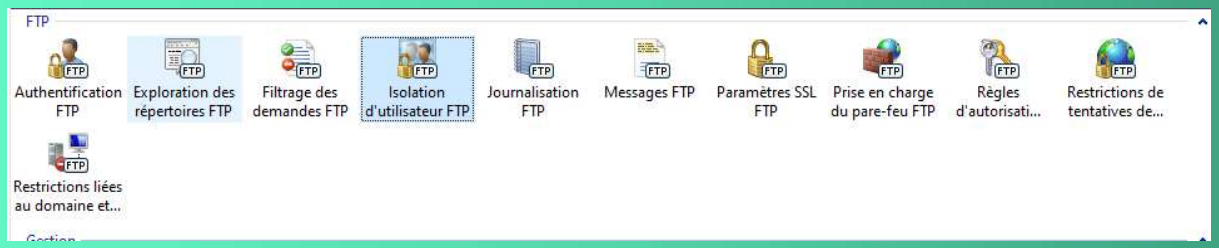
Configurer l'isolation des utilisateurs :



Activé l'authentification de base



Sélectionner Isolation d'utilisateur FTP



Sélectionner 'Répertoire de base FTP configuré dans Active Directory' et entrer un utilisateur ayant accès à l'Active Directory