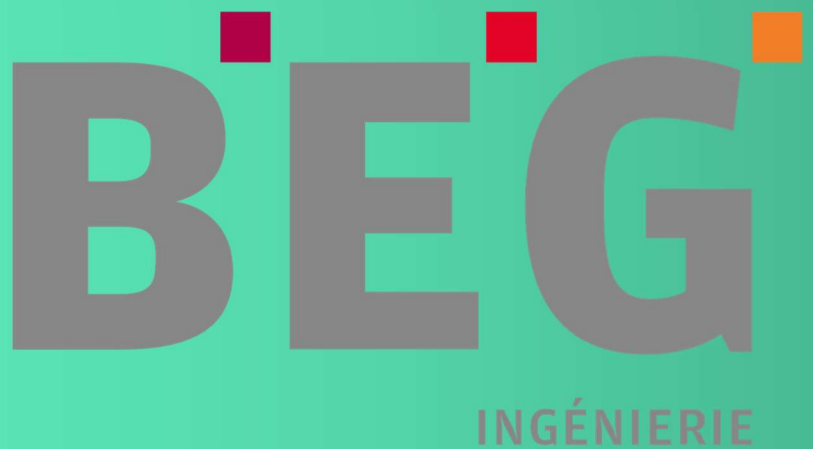


DOCUMENTATION

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	5
CONFIGURATION D'UN ACTIVE DIRECTORY	6
Installation du service :	6
Promouvoir l'AD en tant que contrôleur de domaine :	7
Configuration du contrôleur de domaine :	8
Script :	9
SAUVEGARDE DE L'AD	11
Installation du service :	11
Sauvegarde de l'AD avec Windows Server Backup :	11
RESTAURATION DE L'AD	15
CONFIGURATION D'UN SECOND ACTIVE DIRECTORY	17
Installation du service :	17
MISE EN PLACE D'UN RODC	20
Installation du service :	20
Réplication des mots de passes	25
Retirer le rodc du domaine	28
CHANGER LE SID D'UNE MACHINE	29
CONFIGURATION DU SERVEUR DE FICHIER	30
CRÉATION DES DOSSIERS PRIVATE	32
Partage du dossier :	32
Permissions NTFS :	33
PROFILS ITINÉRANTS	35
Préparer le contrôleur de domaine (AD et GPO) :	35
Création d'une OU pour les GPO :	35
Définir un profil itinérant pour un utilisateur AD :	40
Redirection des dossiers :	41
Le partage et attribution des droits :	42
La GPO de redirection de dossiers :	46
Test de redirection de dossiers :	49
CONFIGURATION DE IPERIUS	50
Créer une sauvegarde :	50

Choisir le dossier de sauvegarde :	52
Planification :	53
Options :	54
CONFIGURATION DU SERVEUR D'IMPRESSION	56
Installation du service :	56
Ajouter un pilote d'impression :	57
Créer un port TCP/IP :	60
Ajouter l'imprimante à partager :	61
Répertorier l'imprimante dans l'annuaire :	62
Création de la GPO :	63
Configuration de l'adresse IP	65
CONFIGURATION DU CŒUR DE RÉSEAU	66
Procédure de réinitialisation :	66
Se connecter au Switch :	66
Configuration de base :	67
Changer le nom :	67
Mise en place de l'adresse IP :	67
Connexion à distance :	67
Mise en place d'un mot de passe pour la connexion (lorsque tu rentres « en ») :	67
Mise en place du chiffrement en MD5 :	67
Mise en place d'une bannière MOTD :	68
Mise en place d'une bannière EXEC :	68
Créer des VLANs :	68
Mettre le mode TRUNK sur les interfaces voulues :	69
CONFIGURATION DU SWITCH	70
Procédure de réinitialisation :	70
Se connecter au Switch :	70
Configuration de base du switch :	71
Configuration des VLANs :	72
Création des VLANs :	72
Ajout des ports dans leur VLAN respectif :	73
Comment se connecter à distance :	73
Sauvegarde TFTP :	74
Restauration d'une sauvegarde :	75
CONFIGURATION DU ROUTEUR.....	76
Procédure de réinitialisation :	76

Configuration de base du routeur :	76
Configuration des VLANS :	77
Configuration du VLAN 10 :	77
Configuration du VLAN 20 :	77
Configuration du VLAN 30 :	78
Test des vlans :	78
Test de requêtes ICMP entre les postes :	78
Avec le routage Inter-VLANS :	78
INSTALLATION D'UNE CLE VENTOY.....	79
CONFIGURATION DU FIREWALL.....	93
Configuration des cartes réseaux :	93
Tests réalisés :	93
Mise en place du routage.....	94
Tests réalisés :	94
Redirection au site web :	95
Tests réalisés :	95
Règles iptables.....	95
Activer le pare-feu :	95
Autoriser toutes les connexions déjà établies :	95
Autoriser le SSH pour seulement l'adresse IP 172.20.34.12 :	95
Autoriser l'accès a la DMZ depuis internet :	96
Comment sauvegarder ses règles iptables :	96
CONFIGURATION D'UN SERVEUR ISS	97
CONFIGURATION D'UN SERVEUR DFS	100
Installation du service :	100
Création d'une racine DFS autonome :	102
INSTALLER LE SERVICE IIS ET ROLE FTP	104
Configurer un site FTP :	106

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.

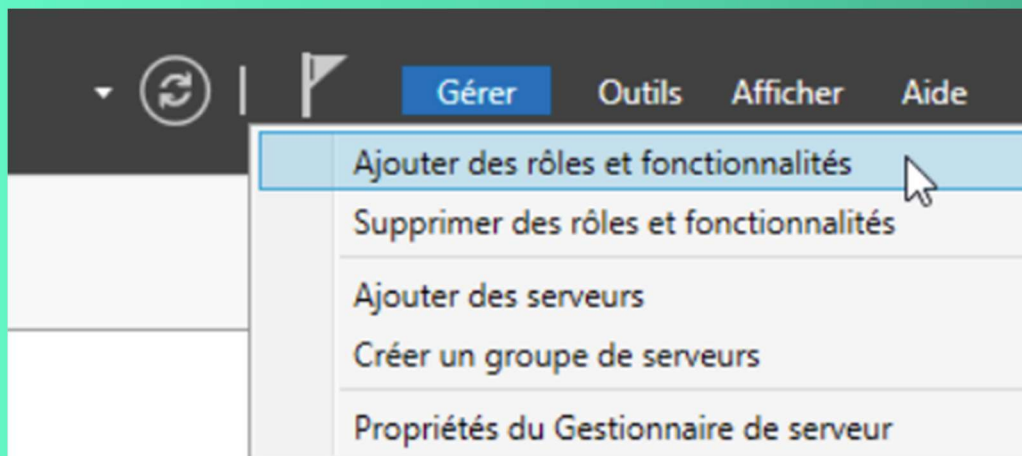
Le projet mené chez BEG couvre plusieurs aspects stratégiques, tels que la configuration d'un Active Directory pour la gestion centralisée des comptes, la mise en place de profils itinérants, la gestion des partages réseau sécurisés, et l'implémentation de services critiques comme les serveurs FTP, pare-feu,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

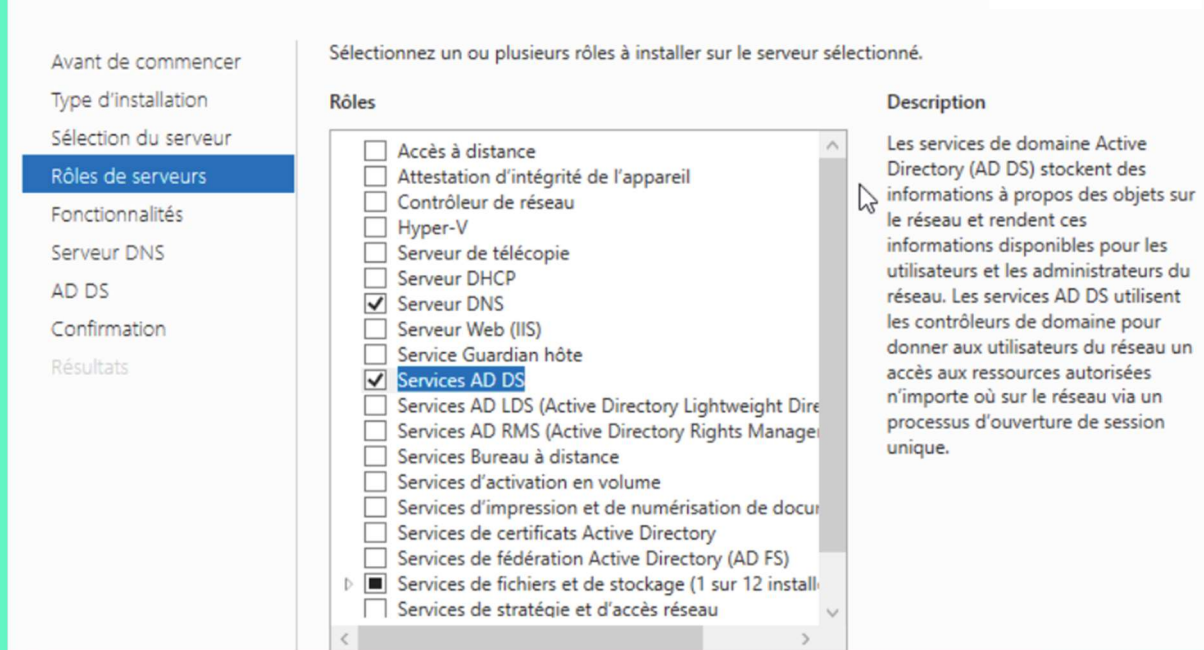
Installation du service :

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'

Sélectionner des rôles de serveurs

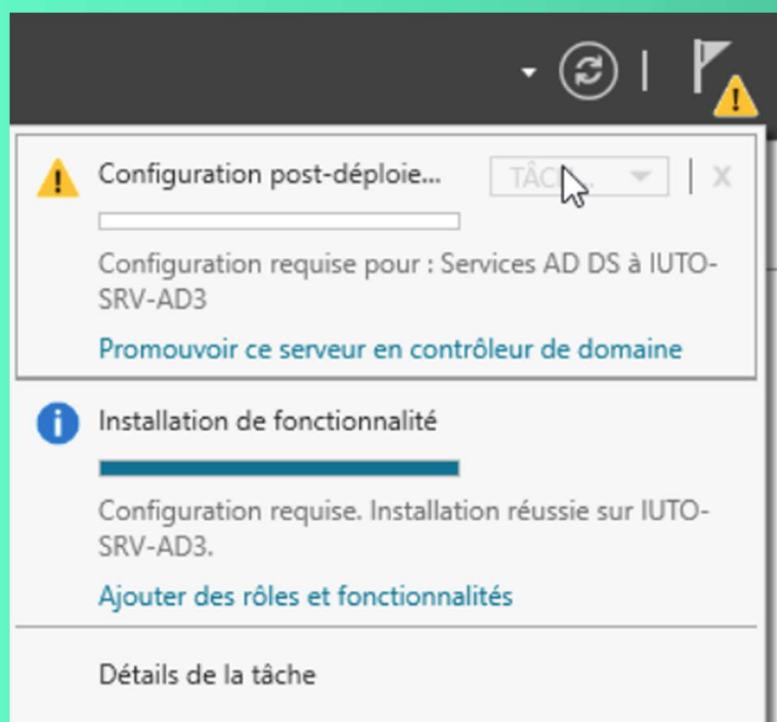


Dans l'onglet 'Confirmation', installer les services

The screenshot shows the 'Confirmer les sélections d'installation' (Confirm installation selections) window. On the left, a navigation pane lists steps: 'Avant de commencer', 'Type d'installation', 'Sélection du serveur', 'Rôles de serveurs', 'Fonctionnalités', 'Serveur DNS', 'AD DS', 'Confirmation' (highlighted), and 'Résultats'. The main area contains instructions: 'Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.' Below this is a checkbox 'Redémarrer automatiquement le serveur de destination, si nécessaire'. A paragraph explains that optional features might be selected automatically and can be deselected by clicking 'Précédent'. A scrollable list shows selected features: 'Outils d'administration de rôles', 'Outils AD DS et AD LDS', 'Module Active Directory pour Windows PowerShell', 'Outils AD DS', 'Centre d'administration Active Directory', 'Composants logiciels enfichables et outils en ligne de commande AD DS', 'Outils du serveur DNS', 'Serveur DNS', and 'Services AD DS'. At the bottom, there are links 'Exporter les paramètres de configuration' and 'Spécifier un autre chemin d'accès source', and navigation buttons: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

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

The screenshot shows the 'Assistant Configuration des services de domaine Active Directory' window. The title bar reads 'Assistant Configuration des services de domaine Active Directory'. The main title is 'Configuration de déploiement'. In the top right corner, it says 'SERVEUR CIBLE BEG-SRV-AD032'. On the left, there is a navigation pane with the following items: 'Configuration de déploiement...' (highlighted), 'Options du contrôleur de...', 'Options DNS', 'Options supplémentaires', 'Chemins d'accès', 'Examiner les options', 'Vérification de la configur...', 'Installation', and 'Résultats'. The main area is titled 'Sélectionner l'opération de déploiement' and contains three radio buttons: 'Ajouter un contrôleur de domaine à un domaine existant', 'Ajouter un nouveau domaine à une forêt existante', and 'Ajouter une nouvelle forêt' (which is selected). Below this, it says 'Spécifiez les informations de domaine pour cette opération'. There is a text box labeled 'Nom de domaine racine :' with the value 'BEG-FR-03-S.PRIV' entered.

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)

The screenshot shows the 'Assistant Configuration des services de domaine Active Directory' window. The title bar reads 'Assistant Configuration des services de domaine Active Directory'. The main title is 'Options du contrôleur de domaine'. In the top right corner, it says 'SERVEUR CIBLE BEG-SRV-AD032'. On the left, there is a navigation pane with the following items: 'Configuration de déploiement...', 'Options du contrôleur de...' (highlighted), 'Options DNS', 'Options supplémentaires', 'Chemins d'accès', 'Examiner les options', 'Vérification de la configur...', 'Installation', and 'Résultats'. The main area is titled 'Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine'. It contains two dropdown menus: 'Niveau fonctionnel de la forêt :' and 'Niveau fonctionnel du domaine :', both set to 'Windows Server 2016'. Below this, it says 'Spécifier les fonctionnalités de contrôleur de domaine'. There are three checkboxes: 'Serveur DNS (Domain Name System)' (checked), 'Catalogue global (GC)' (checked), and 'Contrôleur de domaine en lecture seule (RODC)' (unchecked). Below this, it says 'Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)'. There are two text boxes: 'Mot de passe :' and 'Confirmer le mot de passe :', both containing masked characters. At the bottom, there is a link 'En savoir plus sur les options pour le contrôleur de domaine'. At the very bottom, there are four buttons: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

Ne pas modifier les chemins d'accès

Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL

Dossier de la base de données :	C:\Windows\NTDS	...
Dossier des fichiers journaux :	C:\Windows\NTDS	...
Dossier SYSVOL :	C:\Windows\SYSVOL	...

Installation de la configuration contrôleur de domaine

Vérification de la configuration requise SERVEUR CIBLE
IUTO-SRV-AD3

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour comme... [Afficher plus](#) ✕

- Configuration de déploie...
- Options du contrôleur de...
- Options DNS
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configur...**
- Installation
- Résultats

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

[Réexécuter la vérification de la configuration requise](#)

⬆ Voir les résultats

⚠ Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez

⚠ Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

[En savoir plus sur les conditions préalables](#)

< Précédent Suivant > Installer Annuler

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

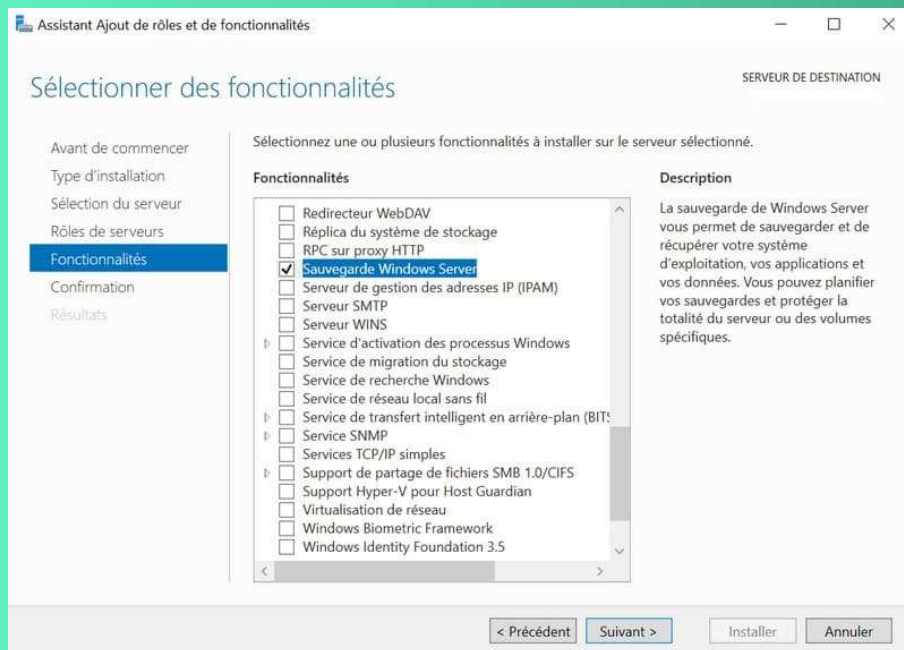
# Vérifier si l'utilisateur existe déjà
if (Get-ADUser -Filter { SamAccountName -eq $UtilisateurLogin }) {
    Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
} else {
    try {
        # Créer un nouvel utilisateur dans Active Directory
        New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
            -DisplayName "$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

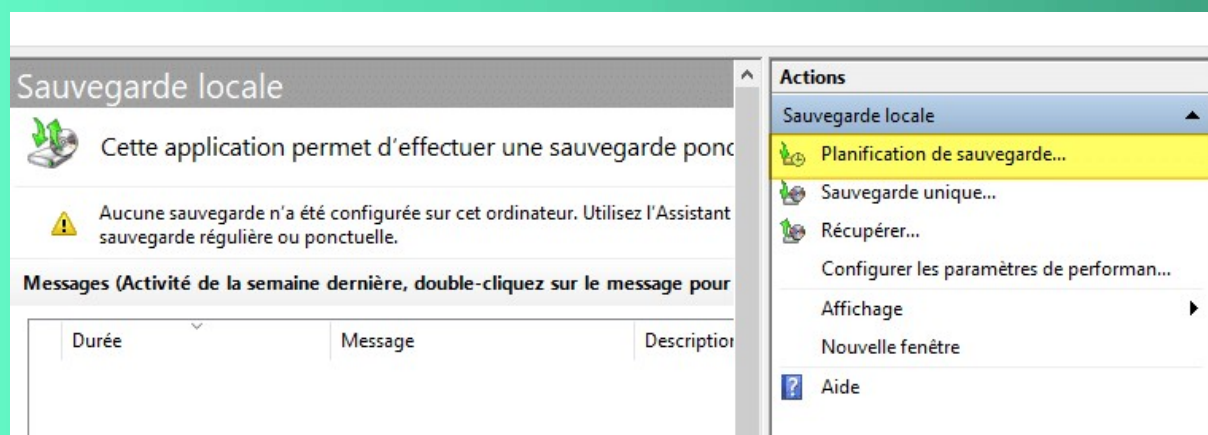
Installation du service :

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)".

Assistant Planification de sauvegarde

Sélectionner la configuration de la sauvegarde

Mise en route

Sélectionner la configurat...

Spécifier l'heure de la sau...

Spécifier le type de destin...

Confirmation

Résumé

Quel type de configuration voulez-vous planifier ?

☒ **Serveur complet (recommandé)**
Je veux sauvegarder toutes les données et les applications présentes sur le serveur, ainsi que l'état du système.
Taille de la sauvegarde : 7,79 Go

☐ **Personnalisé**
Je veux choisir des volumes et des fichiers personnalisés pour la sauvegarde.

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

Assistant Planification de sauvegarde

Spécifier l'heure de la sauvegarde

Mise en route

Sélectionner la configurat...

Spécifier l'heure de la sau...

Spécifier le type de destin...

Confirmation

Résumé

À quelle fréquence et à quel moment voulez-vous exécuter les sauvegardes ?

☒ **Tous les jours**
Sélectionnez une heure : 02:00

☐ **Plusieurs fois par jour**
Cliquez sur une heure disponible, puis sur Ajouter pour l'ajouter à la planification de sauvegarde.

Temps disponible :

00:00
00:30
01:00
01:30
02:00
02:30
03:00
03:30
04:00
04:30

Ajouter >

< Supprimer

Heure planifiée :

21:00

< Précédent

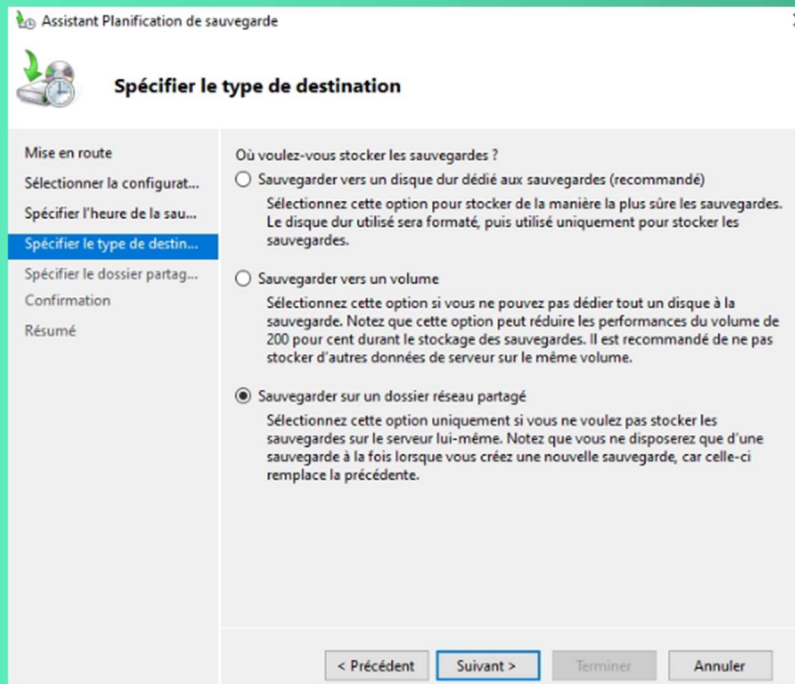
Suivant >

Terminer

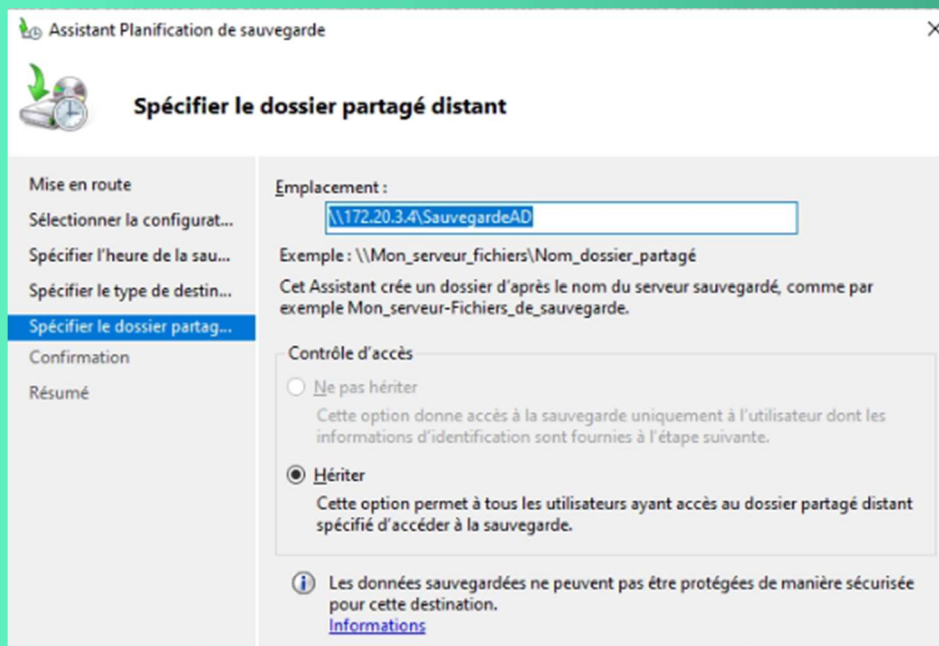
Annuler

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

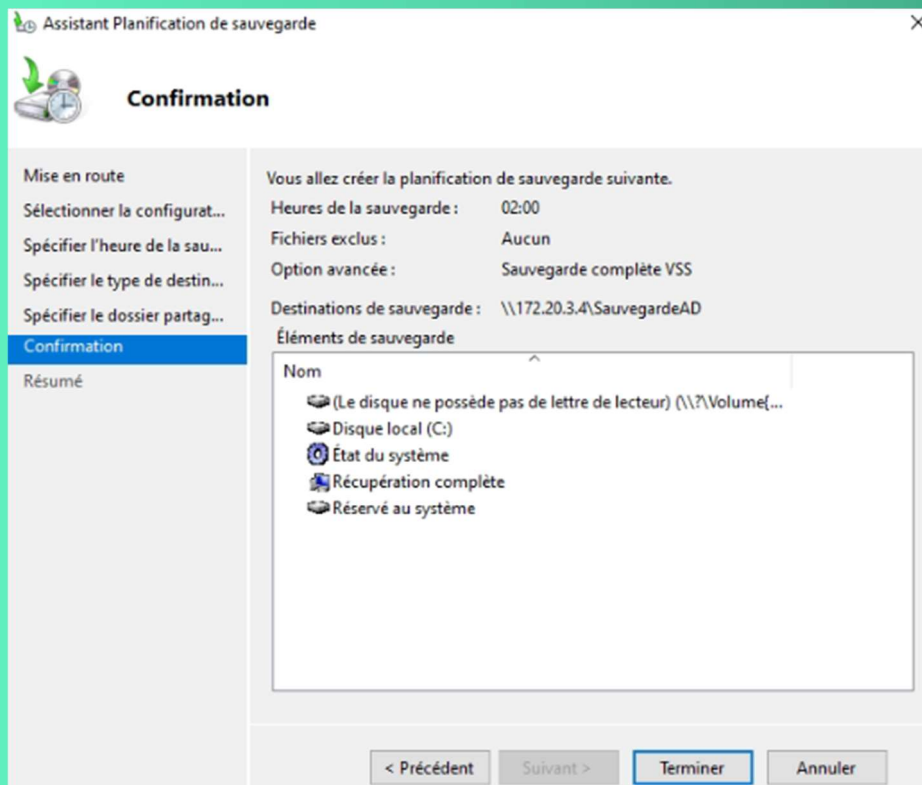
n'est pas recommandé car, avec ce mode, l'outil conserve une seule sauvegarde et il écrase la précédente à chaque fois...!



Ensuite, entrer l'emplacement du fichier partagé



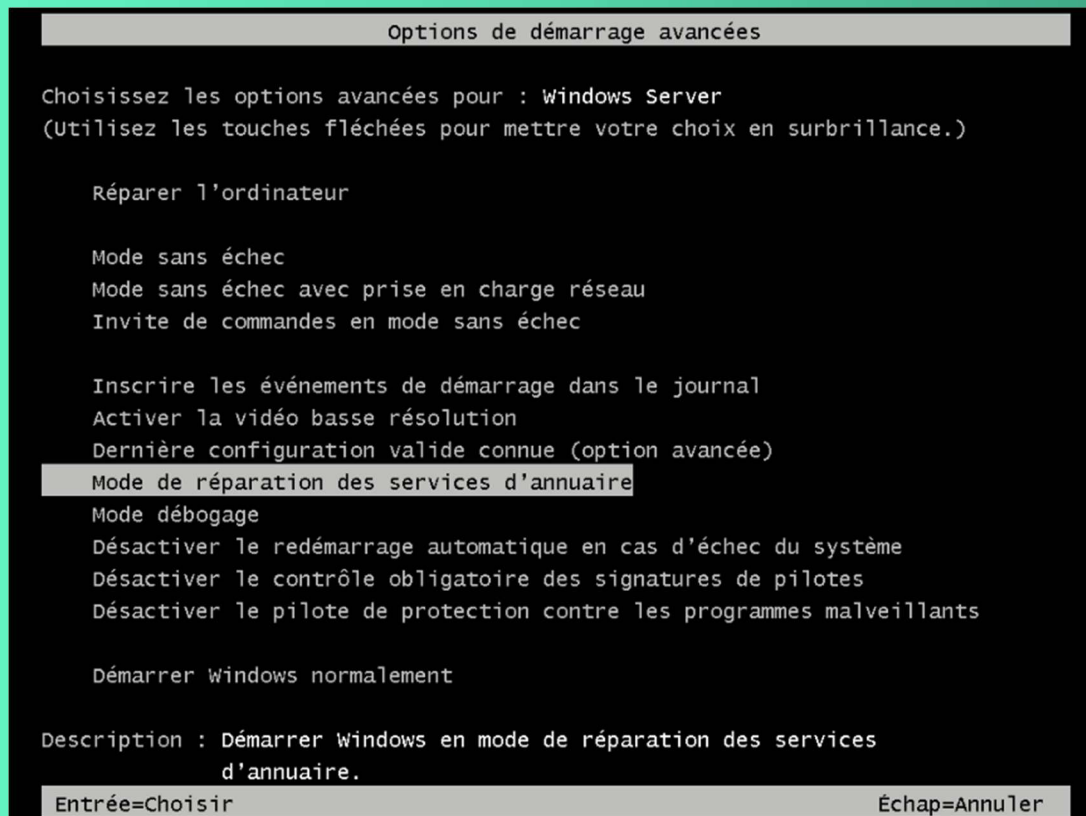
Un résumé s'affiche, cliquons sur "Terminer" pour finaliser la création de la tâche.



RESTAURATION DE L'AD

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

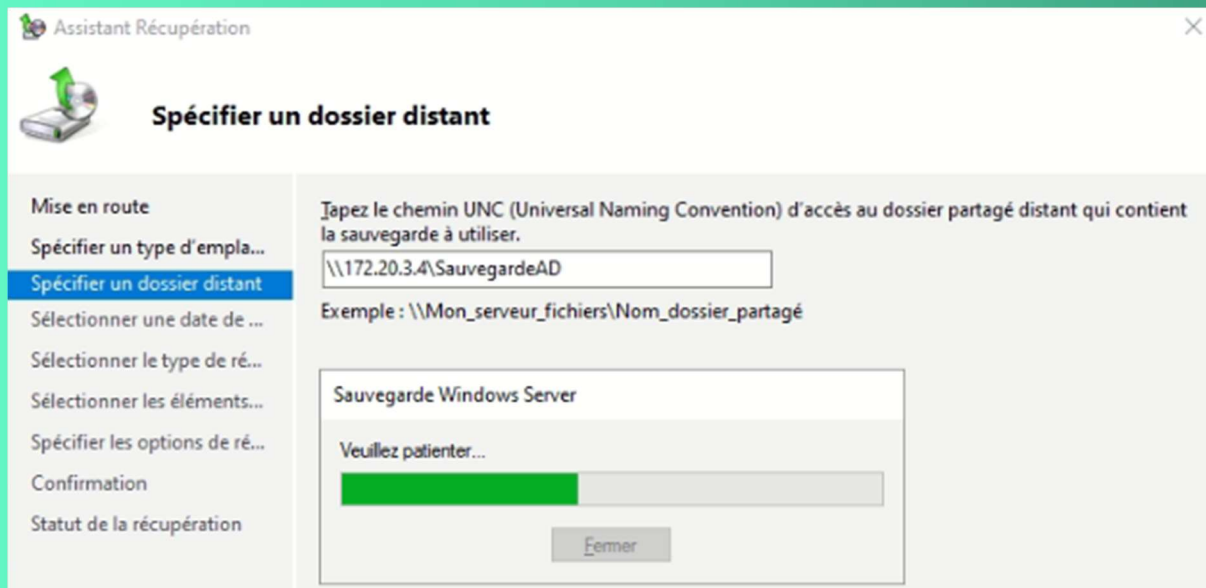
Sélectionner 'mode de réparation des services d'annuaire



Ensuite, choisir autre utilisateur et mettre le compte Administrateur



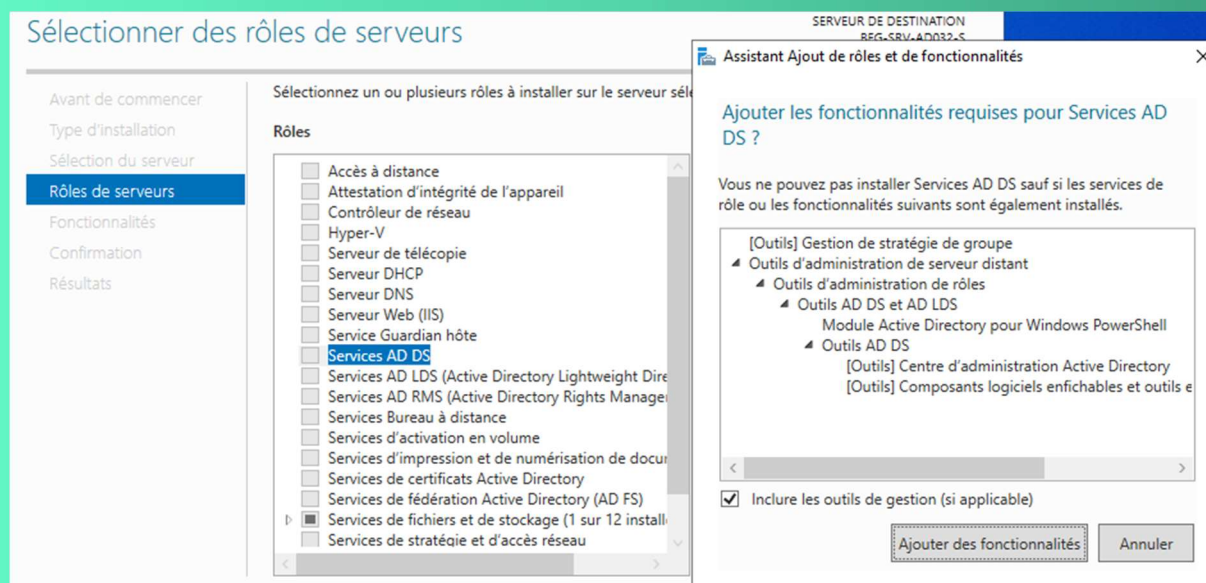
Aller dans l'outil 'Sauvegarde Windows Server'. Cliquez droit sur 'Sauvegarde locale' et sélectionnez 'Récupérer', 'un autre emplacement', 'Dossier Partagé distant' et entrez le chemin de sa sauvegarde (\\172.20.3.4\SauvegardeAD), suivant, 'Etat du système', 'emplacement d'origine' et cochez la case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



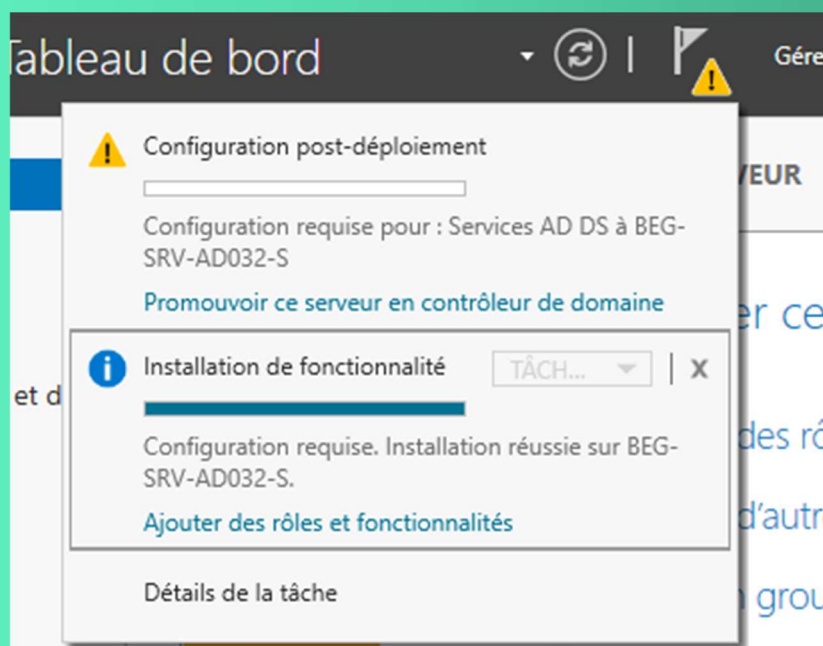
CONFIGURATION D'UN SECOND ACTIVE DIRECTORY

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

The screenshot shows the 'Assistant Configuration des services de domaine Active Directory' window. The title bar reads 'Assistant Configuration des services de domaine Active Directory'. The main heading is 'Configuration de déploiement'. On the right, it says 'SERVEUR CIBLE BEG-SRV-AD032-S'. The left sidebar has a menu with 'Configuration de déploiement...' selected. The main area is titled 'Sélectionner l'opération de déploiement' and contains three radio buttons: 'Ajouter un contrôleur de domaine à un domaine existant' (selected), 'Ajouter un nouveau domaine à une forêt existante', and 'Ajouter une nouvelle forêt'. Below this, it says 'Spécifiez les informations de domaine pour cette opération'. There is a text box for 'Domaine : BEG-FR-03-S.PRIV' and a 'Sélectionner...' button. Further down, it says 'Fournir les informations d'identification pour effectuer cette opération' and shows '<Aucune information d'identification fournie>' with a 'Modifier...' button.

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

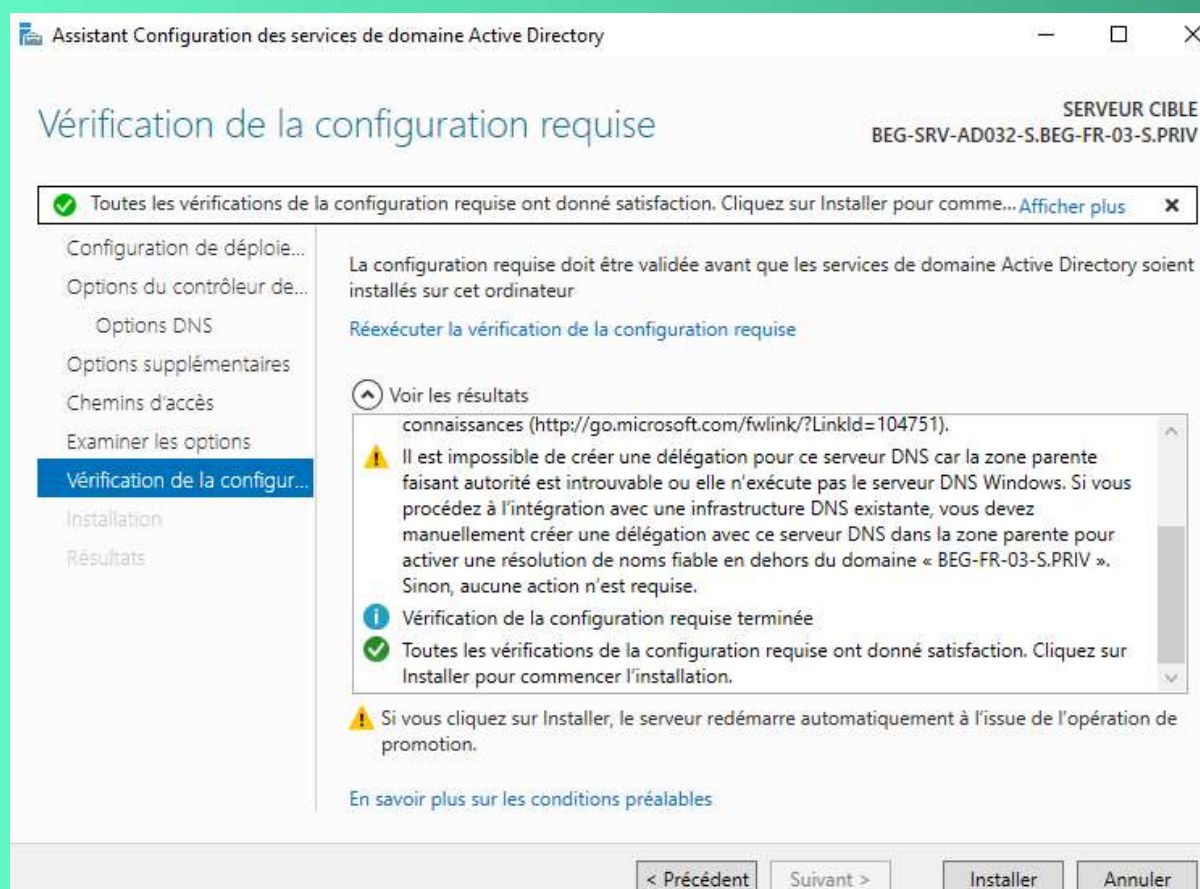
The screenshot shows the 'Assistant Configuration des services de domaine Active Directory' window. The title bar reads 'Assistant Configuration des services de domaine Active Directory'. The main heading is 'Options du contrôleur de domaine'. On the right, it says 'SERVEUR CIBLE BEG-SRV-AD032-S.BEG-FR-03-S.PRIV'. The left sidebar has a menu with 'Options du contrôleur de...' selected. The main area is titled 'Spécifier les capacités du contrôleur de domaine et les informations sur le site'. It contains three checkboxes: 'Serveur DNS (Domain Name System)' (checked), 'Catalogue global (GC)' (checked), and 'Contrôleur de domaine en lecture seule (RODC)' (unchecked). Below these is a dropdown for 'Nom du site : Default-First-Site-Name'. Further down, it says 'Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)'. There are two text boxes for 'Mot de passe :' and 'Confirmer le mot de passe :', both containing masked characters.

Spécifier des options supplémentaires :

Sélectionner 'Tout contrôleur de domaine' dans la case 'Répliquer depuis'

The screenshot shows the 'Assistant Configuration des services de domaine Active Directory' window. The title bar reads 'Assistant Configuration des services de domaine Active Directory'. The main heading is 'Options supplémentaires'. On the right, it says 'SERVEUR CIBLE BEG-SRV-AD032-S.BEG-FR-03-S.PRIV'. The left sidebar has a menu with 'Options supplémentaires' selected. The main area is titled 'Spécifier les options d'installation à partir du support (IFM)'. It contains an unchecked checkbox for 'Installation à partir du support'. Below this, it says 'Spécifier des options de réplication supplémentaires'. There is a dropdown for 'Répliquer depuis : Tout contrôleur de domaine'.

Pour finir, installer le service

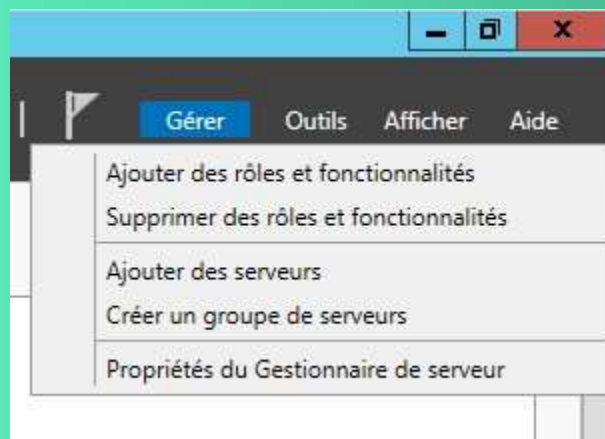


MISE EN PLACE D'UN RODC

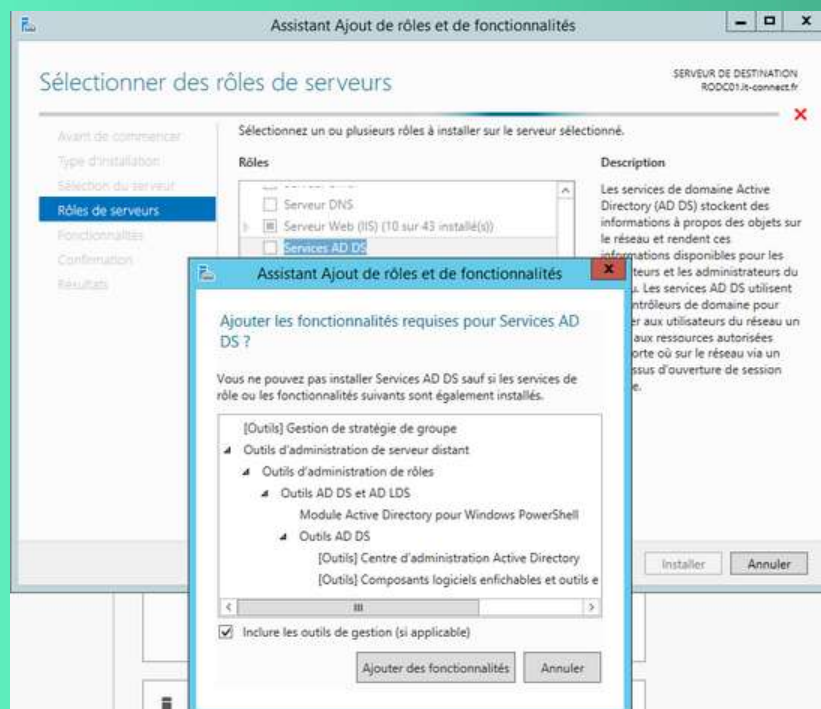
Installation du service :

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.

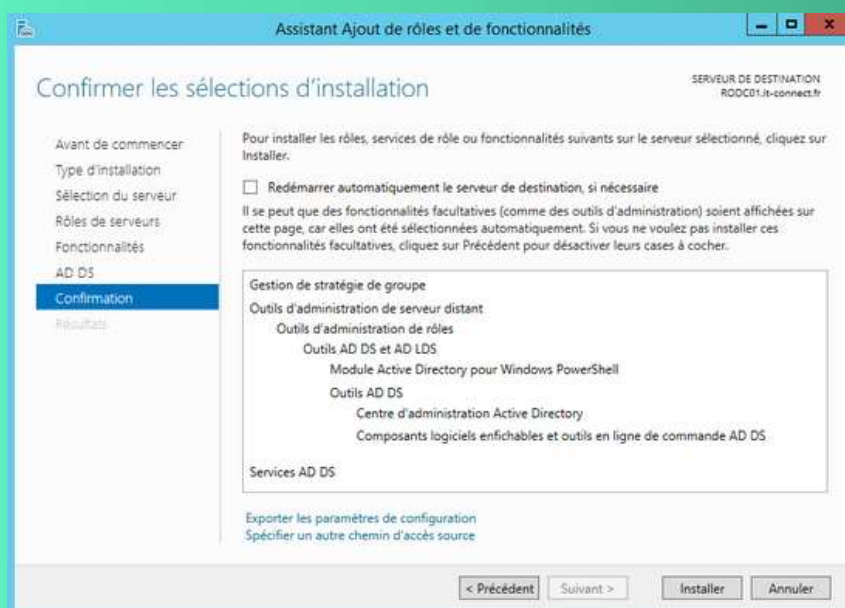
Sur le futur RODC, ouvrez le gestionnaire de serveur puis cliquez sur « Gérer » et « Ajouter des rôles et fonctionnalités ».



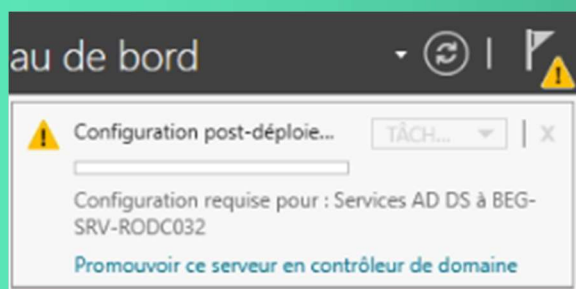
Dans la liste, sélectionnez « Services AD DS », confirmez l'ajout des fonctionnalités requises pour ce rôle et poursuivez.



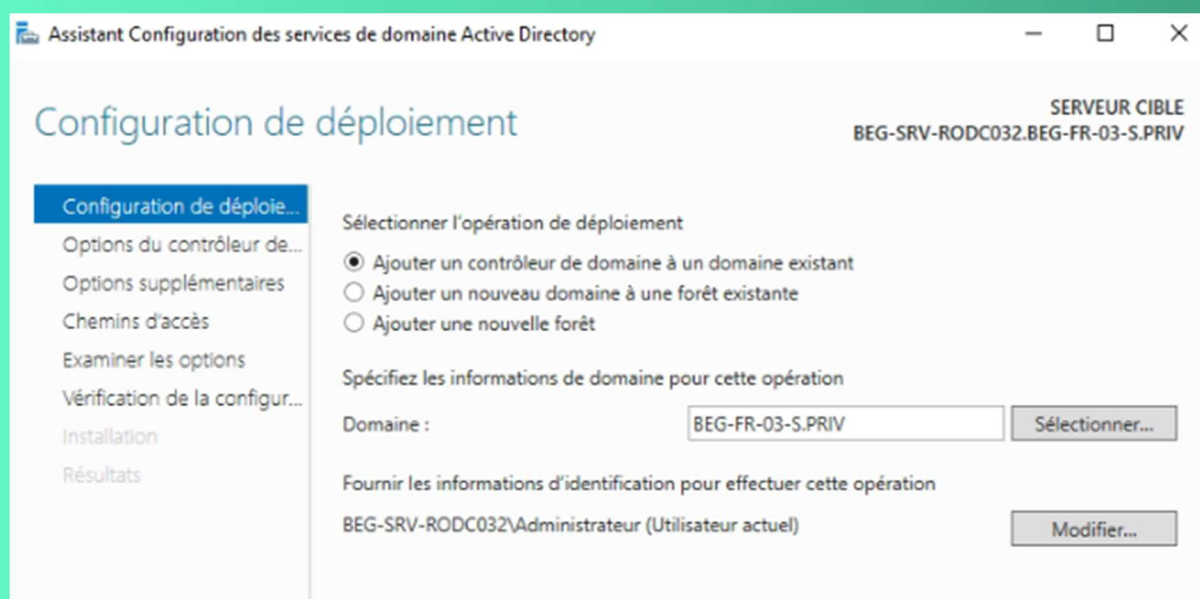
Confirmez que vous souhaitez installer les sélections en cliquant sur « Installer ».



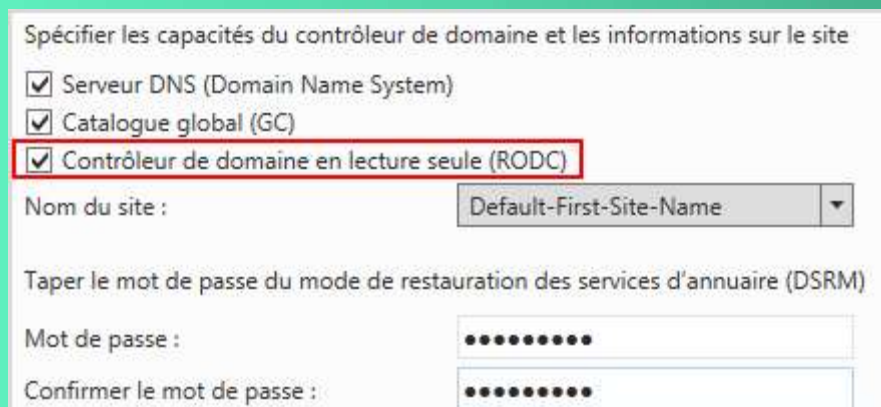
Ensuite, retournez au sein du gestionnaire de serveur, cliquez sur l'icône en « forme de triangle jaune où il y a un point d'exclamation » puis « Promouvoir ce serveur en contrôleur de domaine ».



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, veuillez 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.



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

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

Nom du site : Default-First-Site-Name

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

Mot de passe :

Confirmer le mot de passe :

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 :

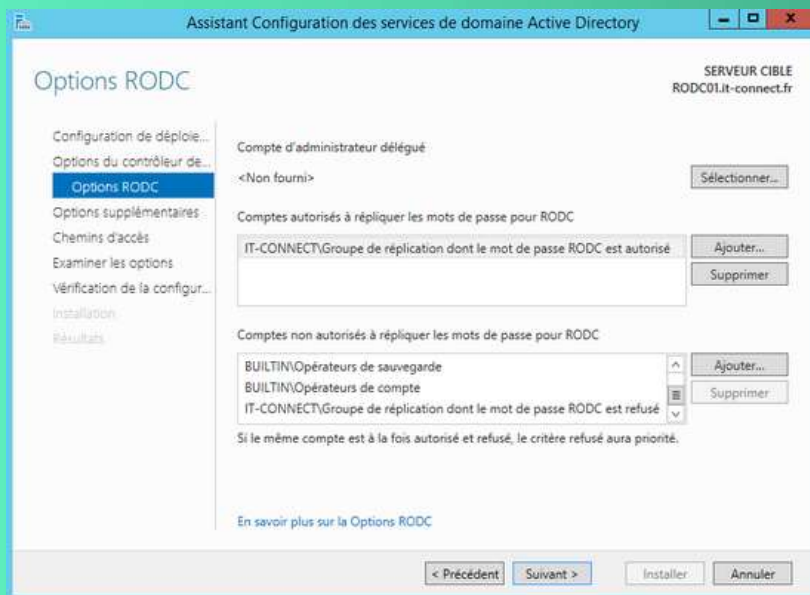
- Groupe de réplication dont le mot de passe RODC est autorisé
- Groupe de réplication dont le mot de passe RODC est refusé

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](#).

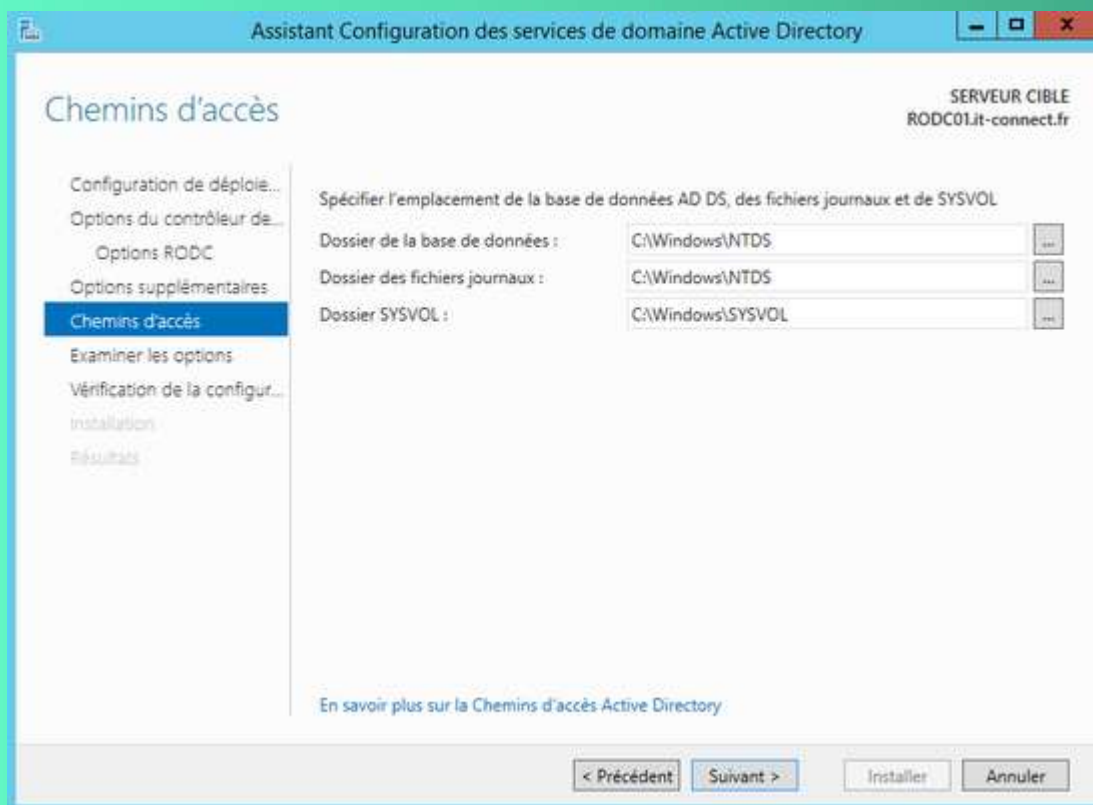
Cliquez sur « Suivant » pour continuer l'installation.



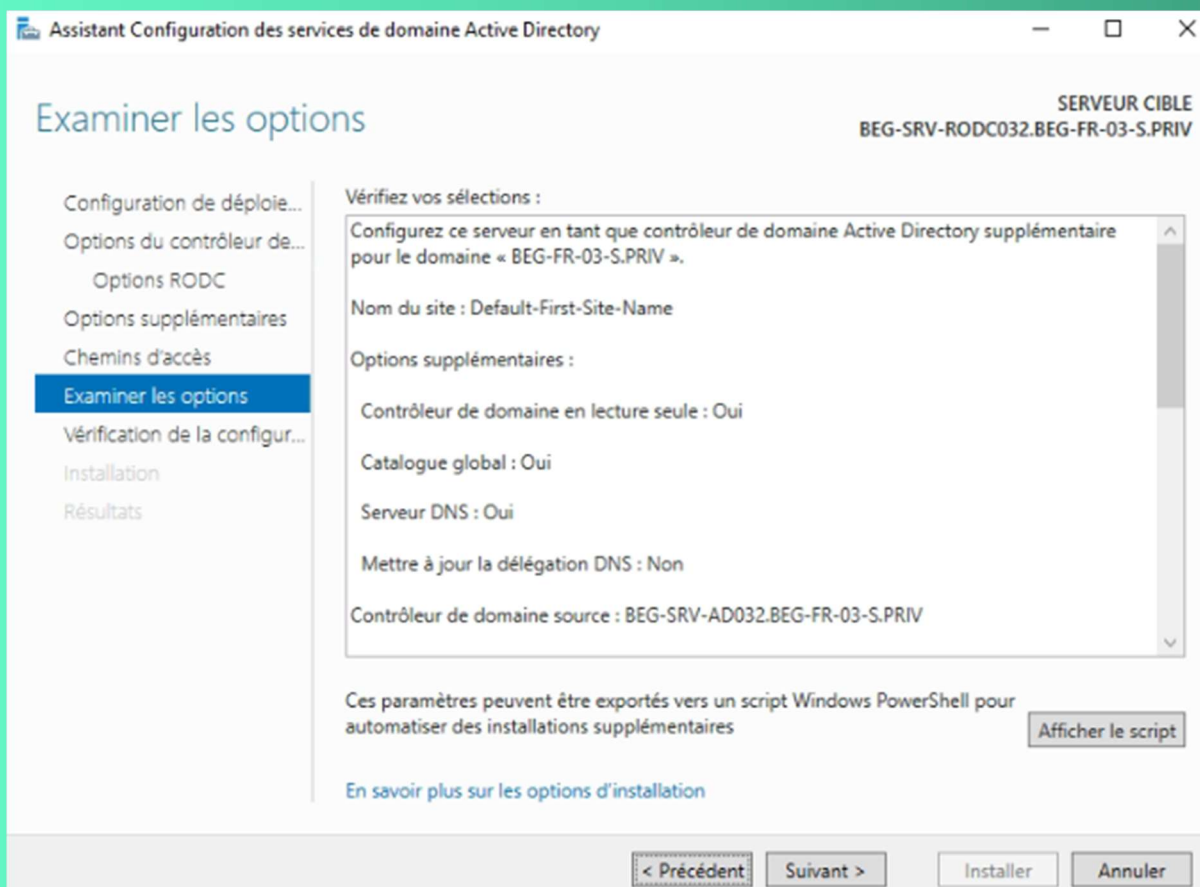
Indiquez un contrôleur de domaine standard depuis lequel répliquer les informations autorisées (ou installer à partir d'un support si vous disposez d'un support prêt – utile pour économiser de la bande passante même lors de la mise en place). Cliquez sur « Suivant ».



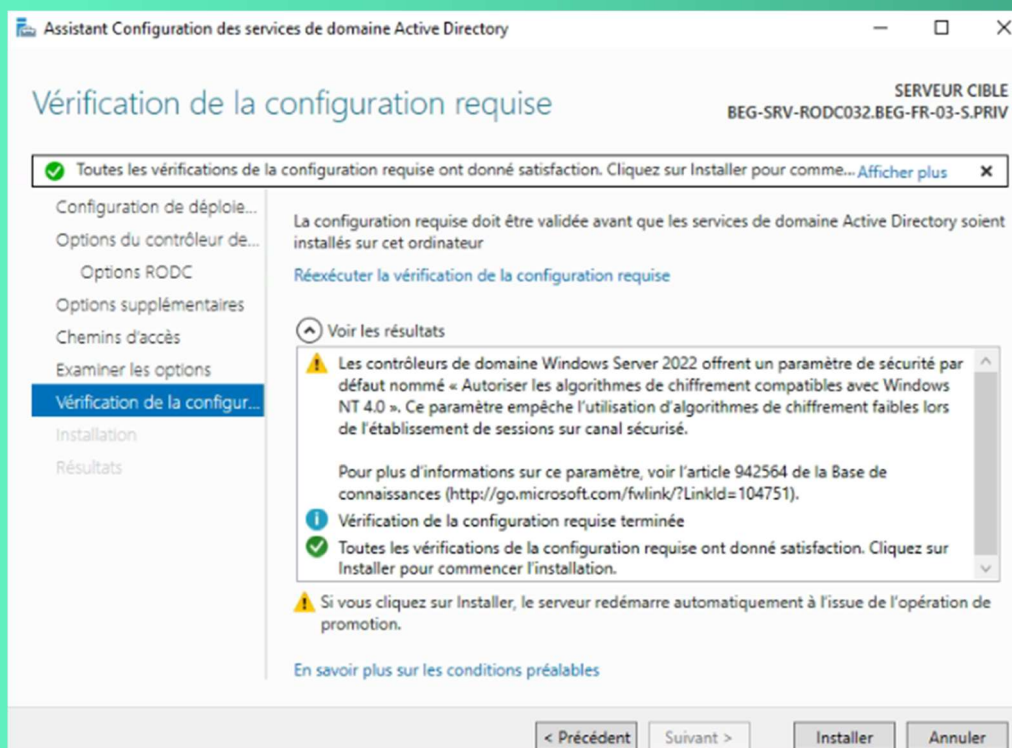
Indiquez l'emplacement de la base de données, des fichiers journaux et de SYSVOL (peuvent être placés sur des disques différents). Cliquez sur « Suivant ».



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



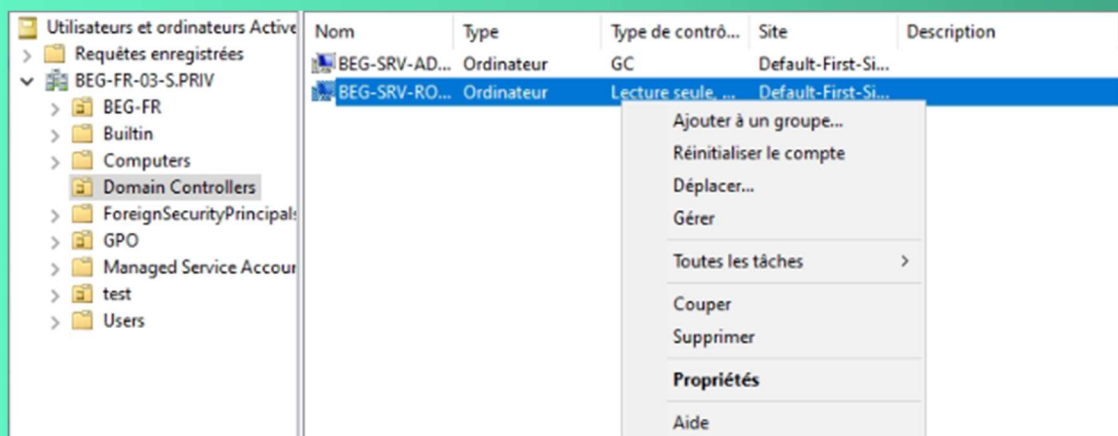
Après que la configuration soit vérifiée, cliquez sur « Installer » et patientez un instant. Le serveur va redémarrer automatiquement à la fin de l'installation.



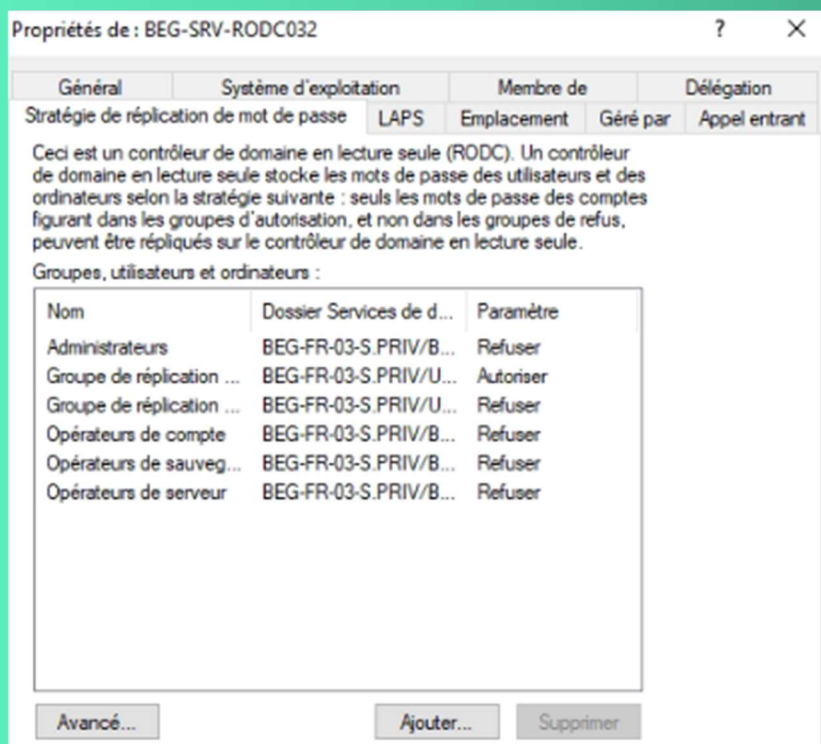
L'installation du RODC est désormais terminée.

Réplication des mots de passes

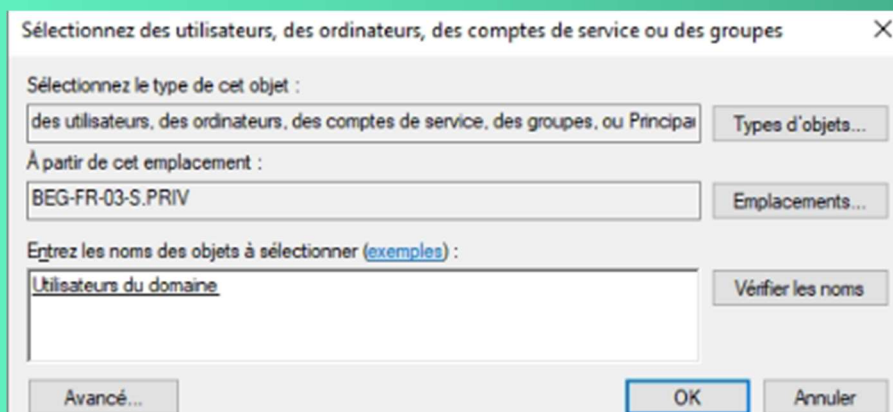
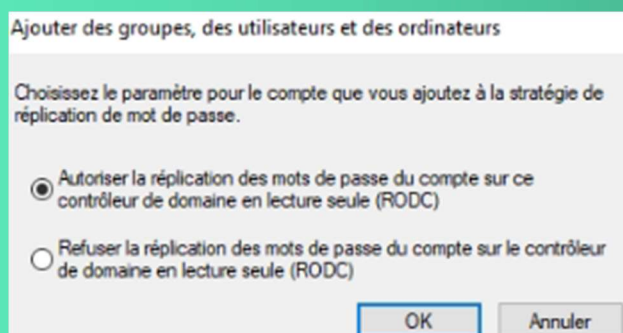
Sur un contrôleur de domaine standard (lecture/écriture), ouvrez la console « Utilisateurs et ordinateurs Active Directory », positionnez-vous sur l'unité d'organisation « Domain Controllers ». Sur la droite, faites clic droit sur l'objet ordinateur correspondant à votre serveur RODC puis « Propriétés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



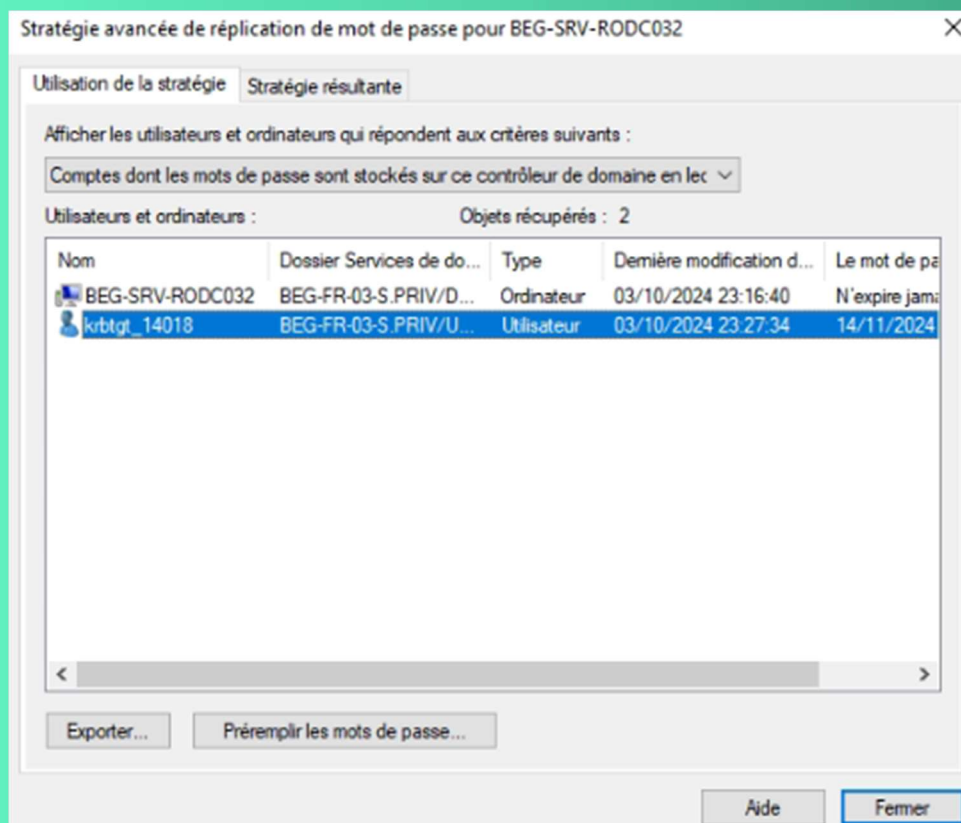
Cliquez ensuite sur l'onglet « Stratégie de réplication de mot de passe » qui concerne donc la stratégie de réplication des mots de passe. La fenêtre affiche les utilisateurs et groupes pour lesquels vous autorisez ou refusez explicitement la réplication des mots de passe.



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.



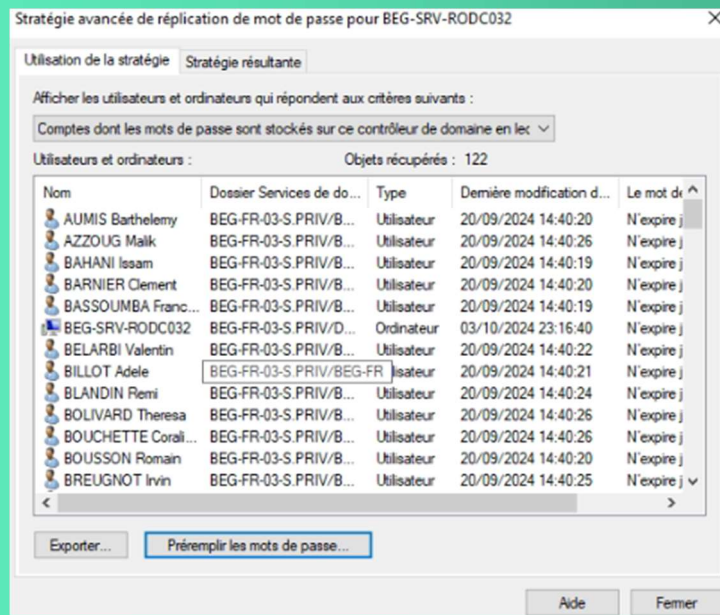
Vous remarquerez la présence d'un utilisateur nommé « krbtgt_14018 » qui est propre à chaque RODC (généré sous la forme krbtgt_XXXX). Il permet de délivrer les tickets Kerberos aux clients.

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 répllication 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

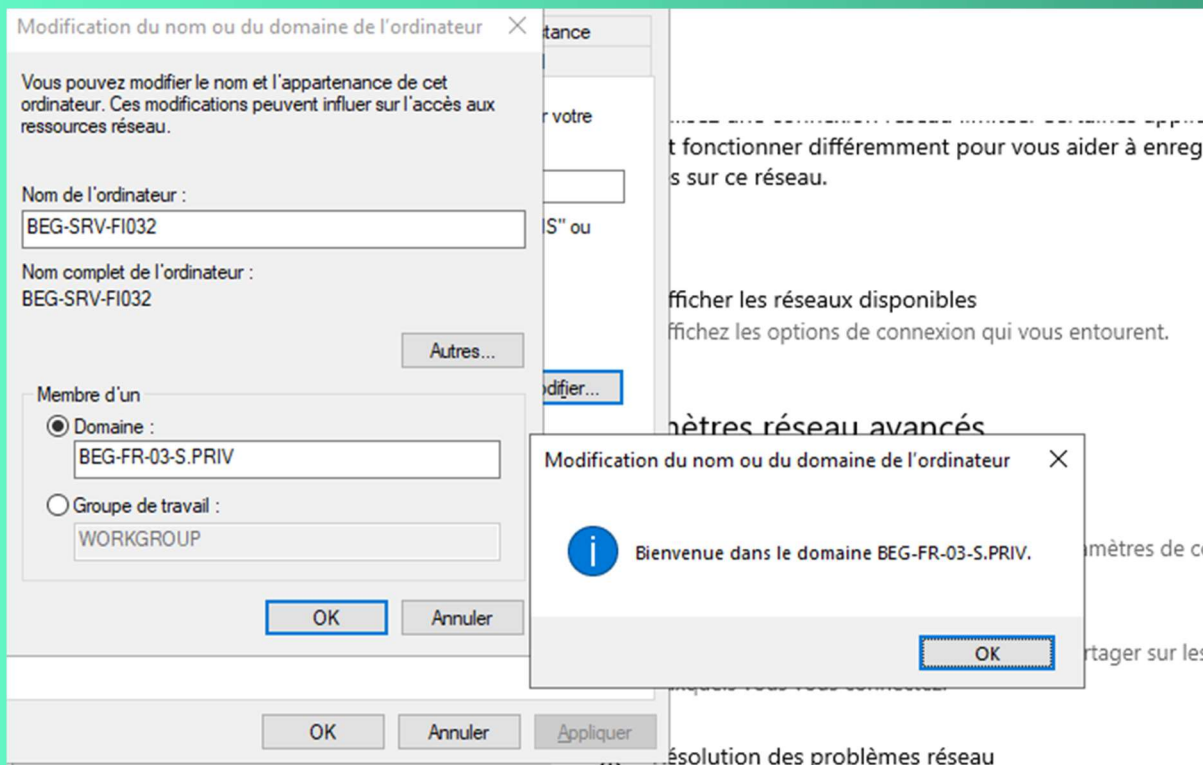
CHANGER LE SID D'UNE MACHINE

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

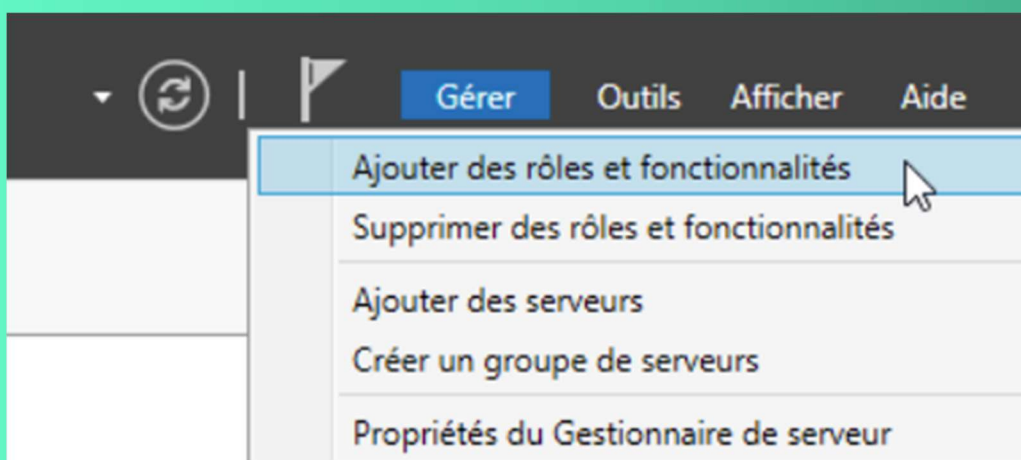
```
C:\Windows\System32\sysprep\sysprep.exe /oobe /generalize /shutdown
```

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'.

Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION
BEG-SRV-FI032

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles	Description
☐ Services de certificats Active Directory	
☐ Services de fédération Active Directory (AD FS)	
☒ Services de fichiers et de stockage (2 sur 12 installé(s))	
☒ Services de fichiers et iSCSI (1 sur 11 installé(s))	
☒ Serveur de fichiers (Installé)	
☐ BranchCache pour fichiers réseau	
☐ Déduplication des données	
☐ Dossiers de travail	
☐ Espaces de noms DFS	
☐ Fournisseur de stockage cible iSCSI (fournisseur de stockage)	
☒ Gestionnaire de ressources du serveur de fichiers	Le Gestionnaire de ressources du serveur de fichiers vous aide à gérer et à comprendre les fichiers et les dossiers sur un serveur de fichiers en planifiant des tâches de gestion de fichiers et des rapports de stockage, en classifiant les fichiers et les dossiers, en configurant des quotas de dossiers et en définissant des stratégies de filtrage de fichiers.
☐ Réplication DFS	
☐ Serveur cible iSCSI	
☐ Serveur pour NFS	
☐ Service Agent VSS du serveur de fichiers	
☒ Services de stockage (Installé)	
☐ Services de stratégie et d'accès réseau	
☐ Services WSUS (Windows Server Update Services)	
☐ Windows Deployment Services	

< Précédent Suivant > Installer Annuler

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

Progression de l'installation

NATION
BEG-SRV-FI032

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Installation réussie sur BEG-SRV-FI032.

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils de services de fichiers

Outils du Gestionnaire de ressources du serveur de fichiers

Services de fichiers et de stockage

Services de fichiers et iSCSI

Gestionnaire de ressources du serveur de fichiers

1 Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

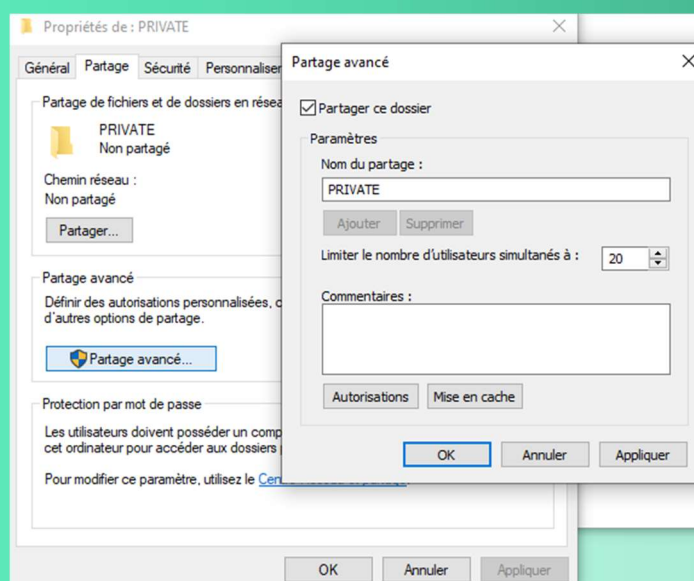
< Précédent Suivant > Fermer Annuler

CRÉATION DES DOSSIERS

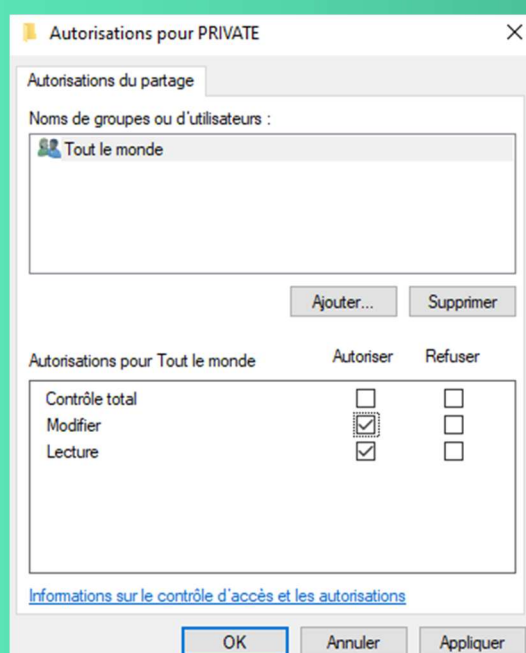
PRIVATE

Partage du dossier :

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

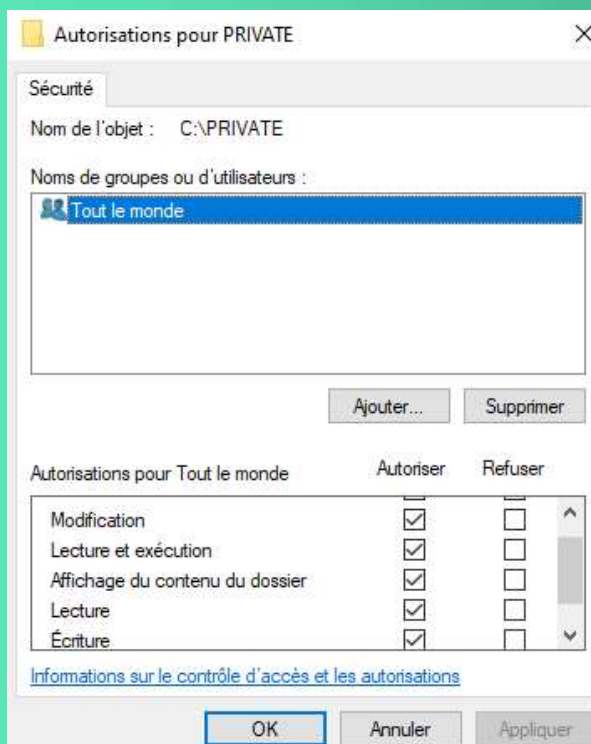


Ensuite, cliquer sur 'Autorisations' et sélectionner tout le monde en lecture et modifier

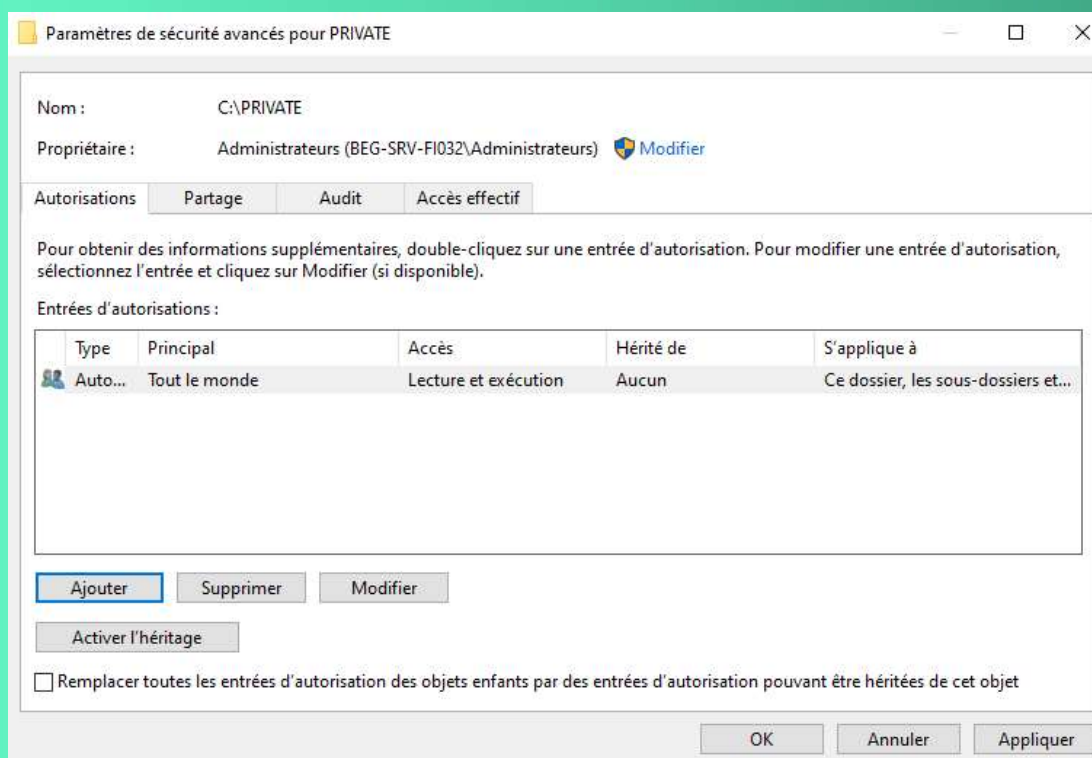


Permissions NTFS :

Pour configurer les 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 sécurité 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

The screenshot shows the 'Propriétés d'éléments multiples' (Multiple Items Properties) dialog box with the 'Profil' (Profile) tab selected. The dialog has five tabs: 'Général', 'Compte', 'Adresse', 'Profil', and 'Organisation'. The 'Profil' tab contains instructions: 'Pour modifier une propriété d'objets multiples, sélectionnez la case à cocher pour activer la modification, puis entrez la modification.' (To modify a property of multiple objects, select the checkbox to activate the modification, then enter the modification.)

Under the 'Profil utilisateur' (User Profile) section, there are three options:

- ☐ Chemin du profil : (empty text box)
- ☐ Script d'ouverture de session : (empty text box)
- ☒ Dossier de base (Basic folder)

Under the 'Dossier de base' section, there are two options:

- ☐ Chemin d'accès local : (empty text box)
- ☒ Connecter : U: [dropdown arrow] à : \\172.20.3.4\private\%username%

At the bottom of the dialog are three buttons: 'OK', 'Annuler', and 'Appliquer' (highlighted with a blue border).

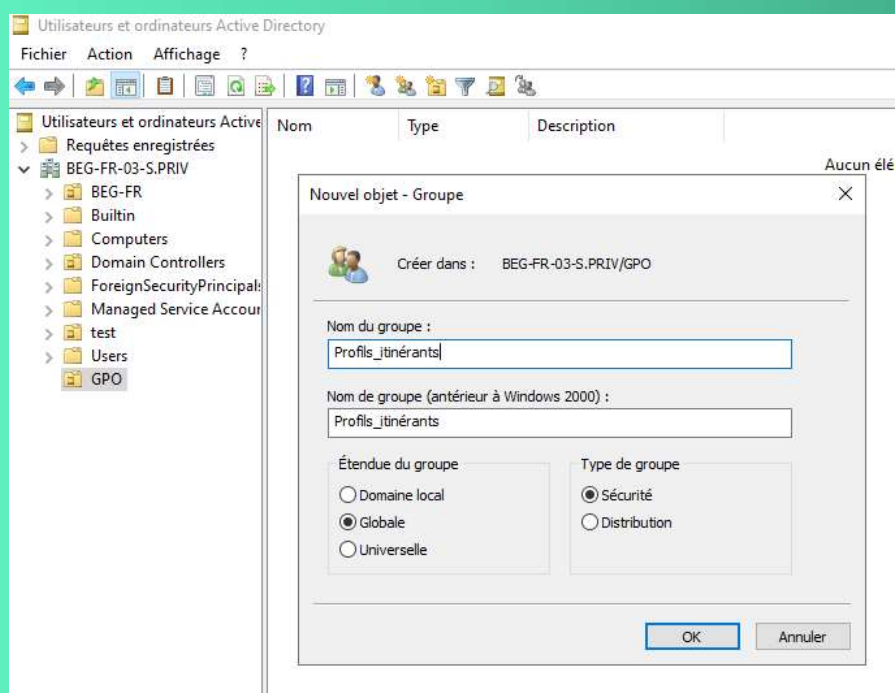
PROFILS ITINÉRANTS

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 :

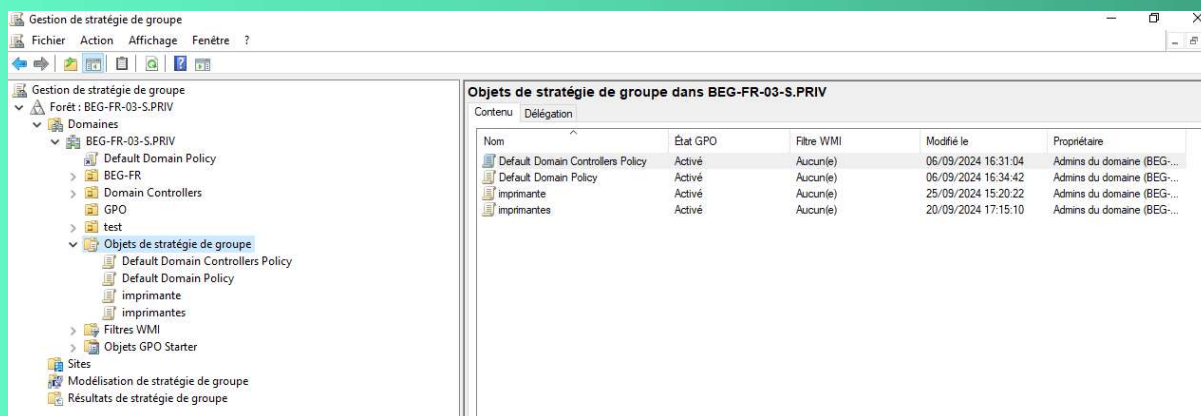
Nous avons créé une Unité d'Organisation nommée GPO puis créer un groupe global nommée 'Profils_itinérants'



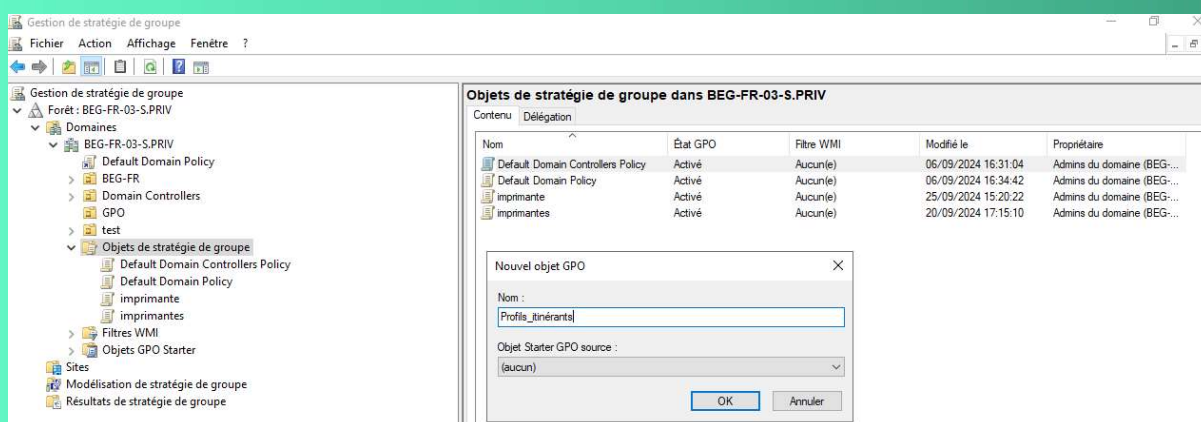
Afin d'éviter des possibles problèmes « un jour » nous allons mettre en place une GPO

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.

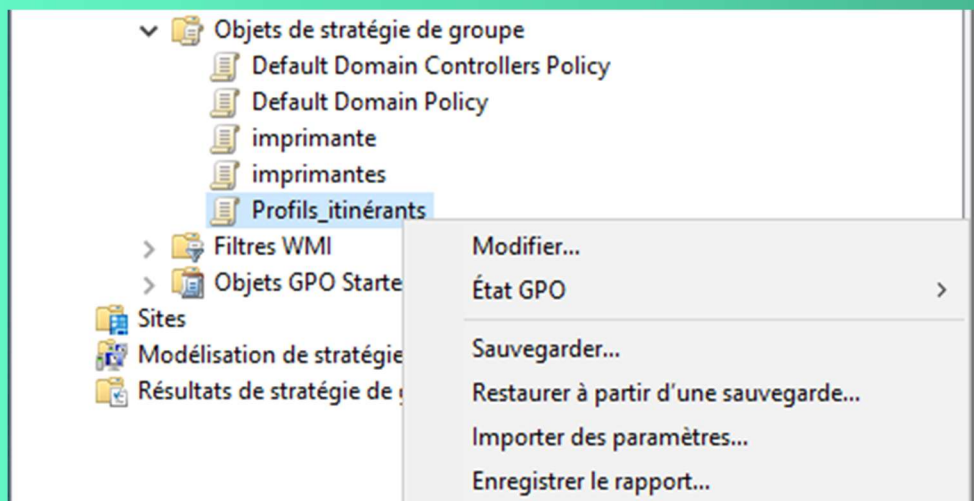
Pour cela, ouvrez votre console de gestion des stratégies de groupe.



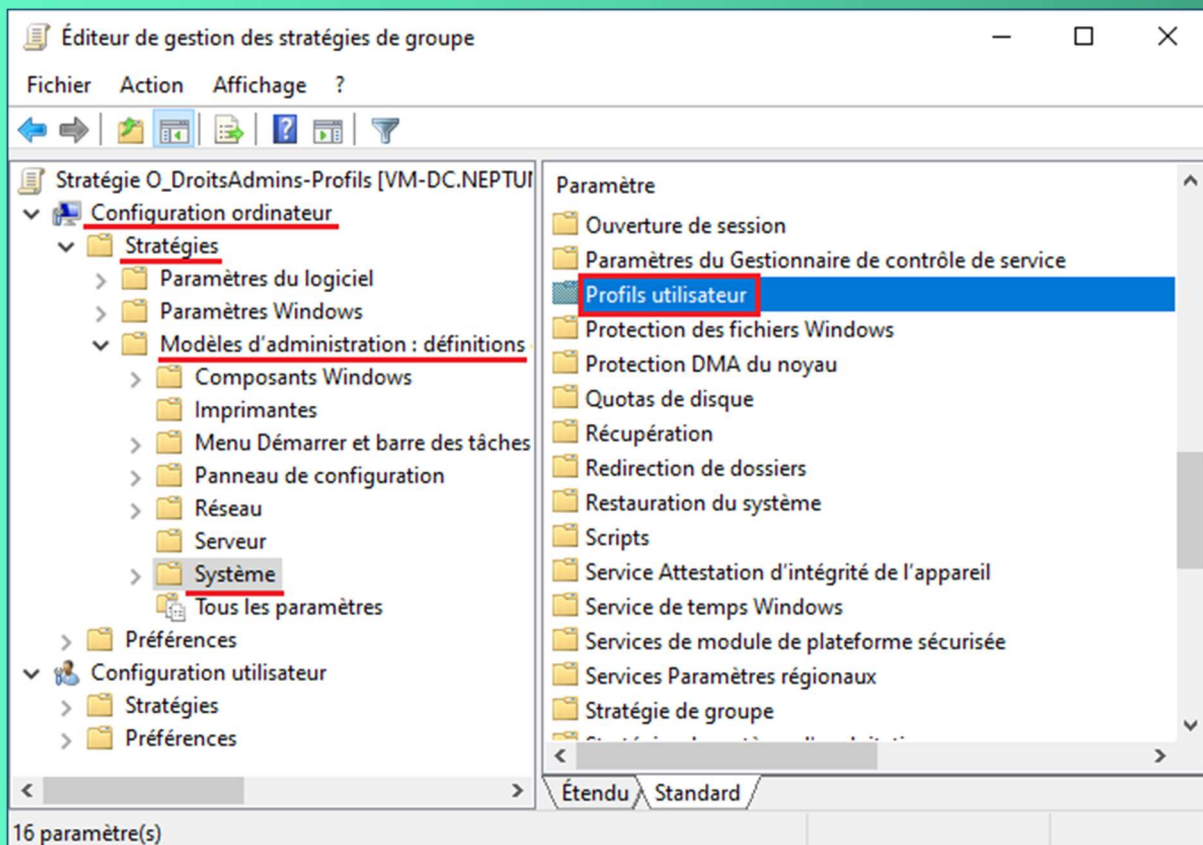
Dans la partie « Objets de stratégie de groupe », faites un clic droit puis « Nouveau ». Ensuite nommer la GPO



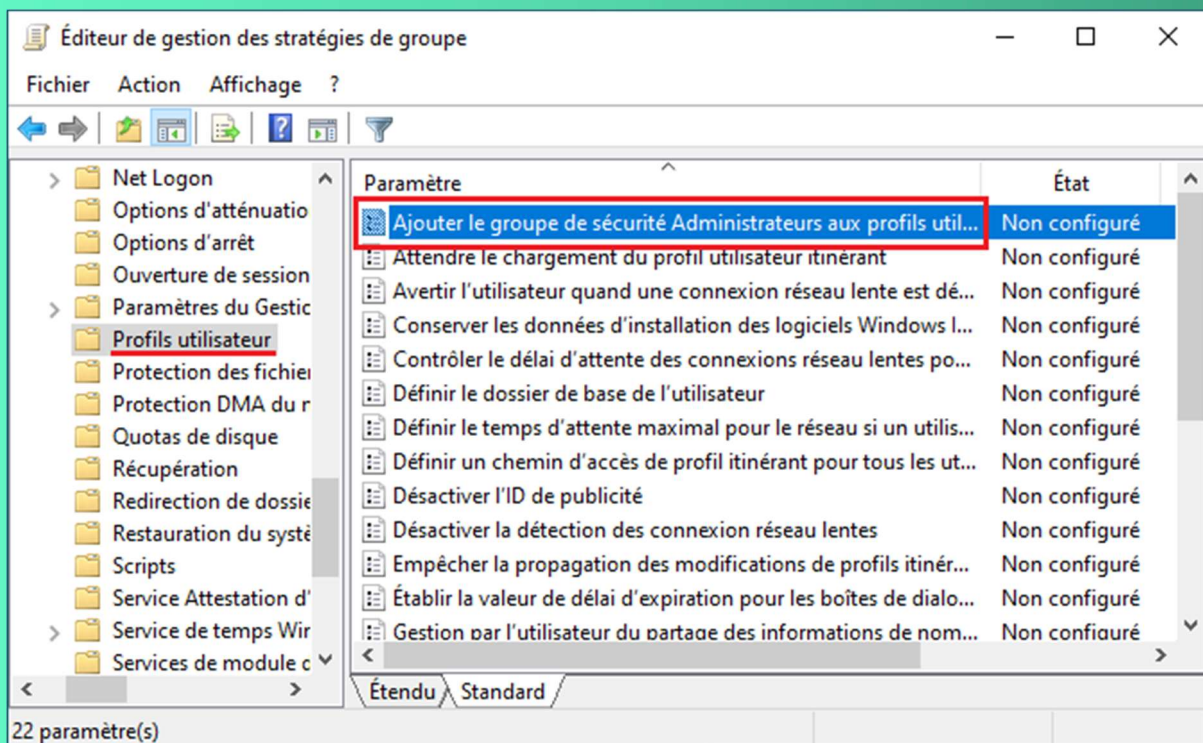
Ensuite faites un clic droit sur son nom puis « Modifier ».



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

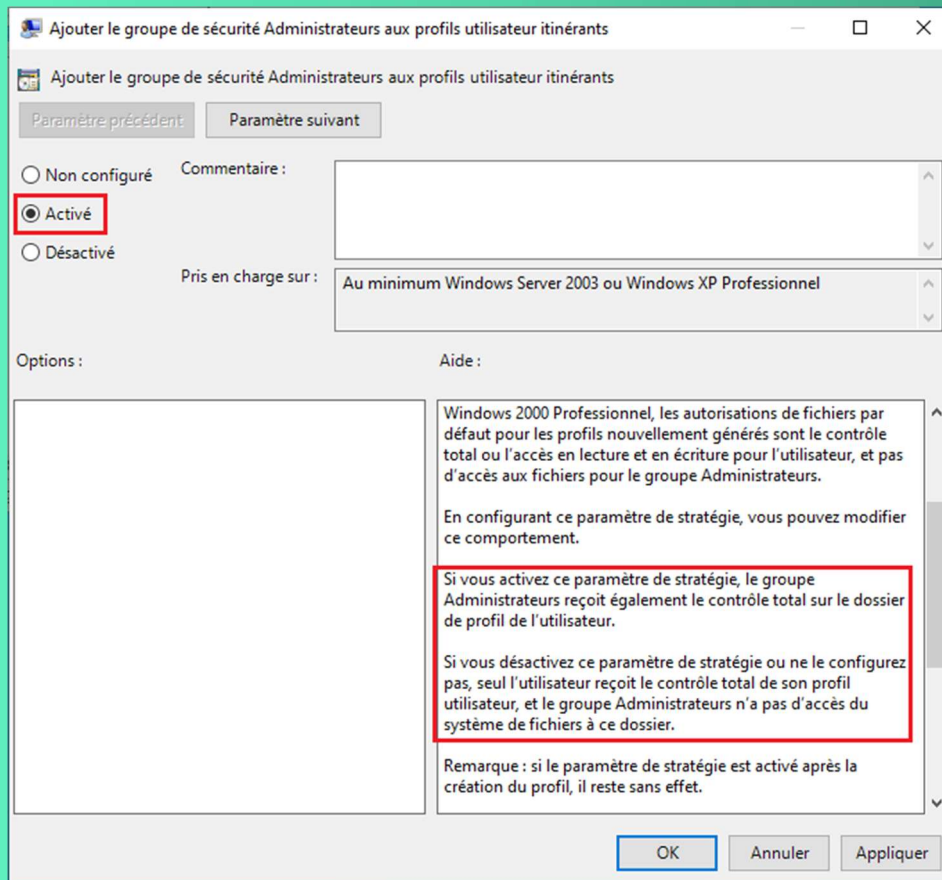


Recherchez sur la droite le paramètre nommé « Ajouter le groupe de sécurité Administrateurs aux profils utilisateur itinérants » et double-cliquez dessus.

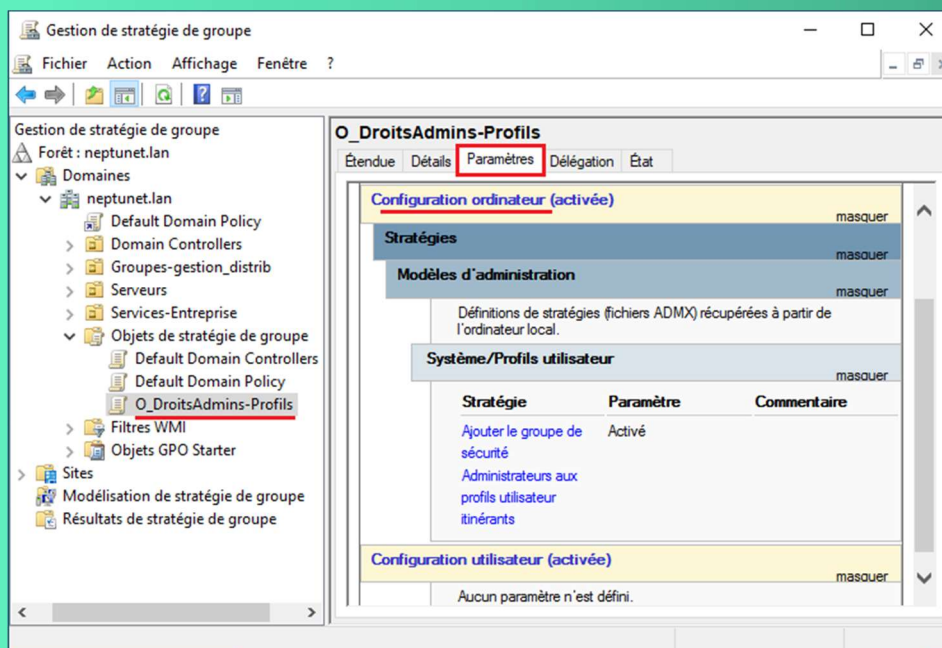


Si on regarde un peu dans la partie « Aide », il y a des infos intéressantes nous précisant ce qu'il se passe si on active ce paramètre, si au contraire on le désactive ou ne le configure pas. Nous voulons

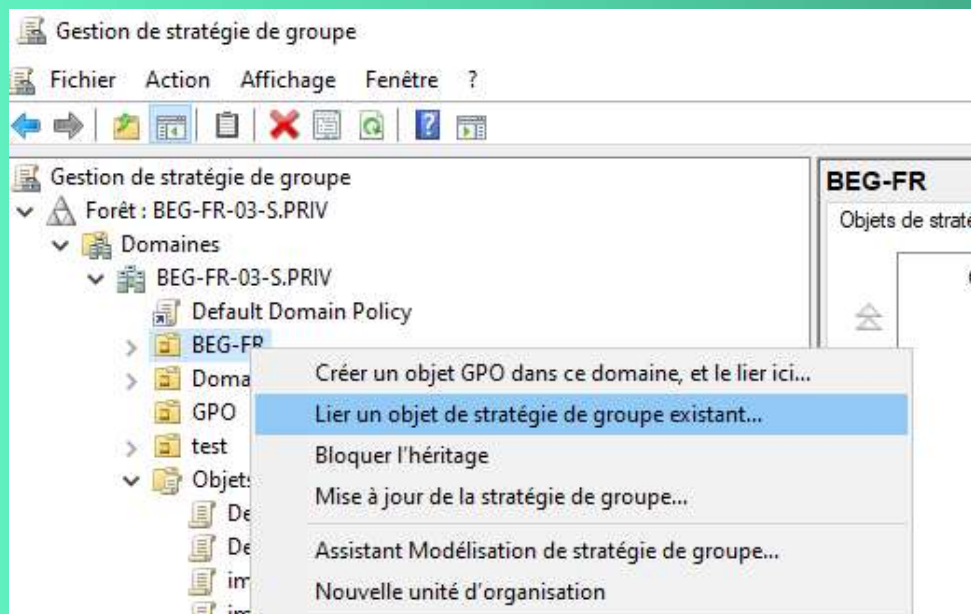
que les admins puissent accéder aux profils dont nous allons l'activer. Cochez la case « Activé » et cliquez sur OK.



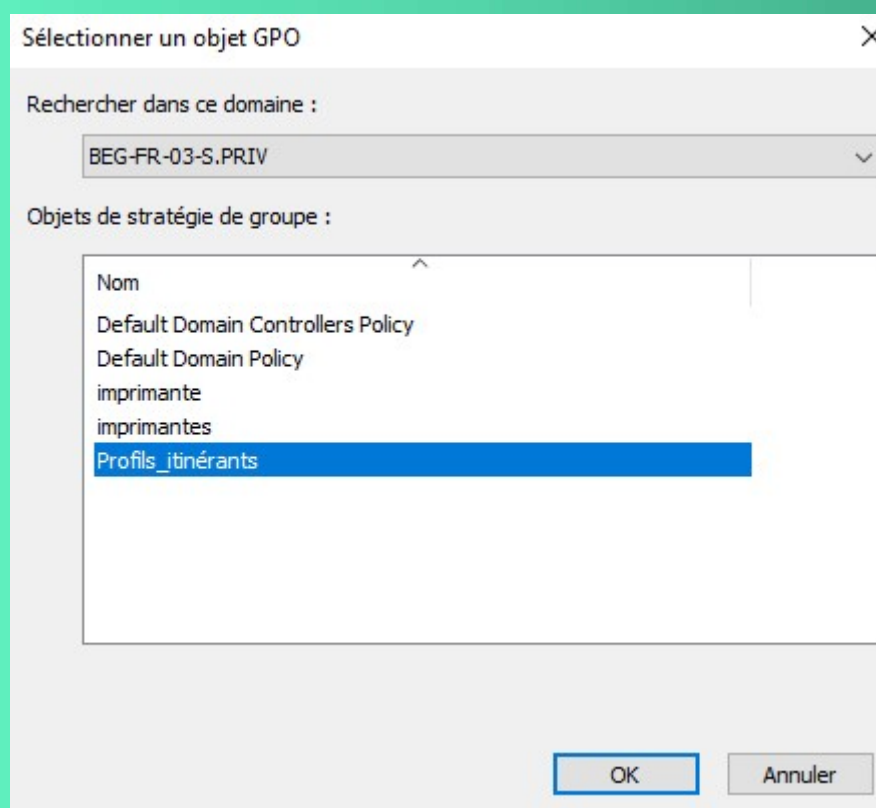
Vous pouvez fermer l'éditeur de stratégies et revenir sur la console de gestion des GPO. Si on jette un coup d'œil dans les paramètres de la GPO que l'on vient de créer, on voit bien ce qu'on a mis en place.



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 ».



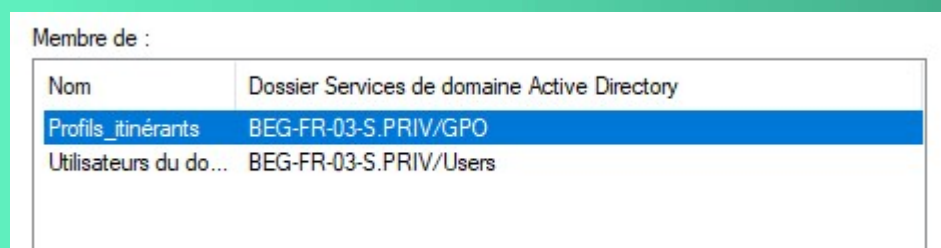
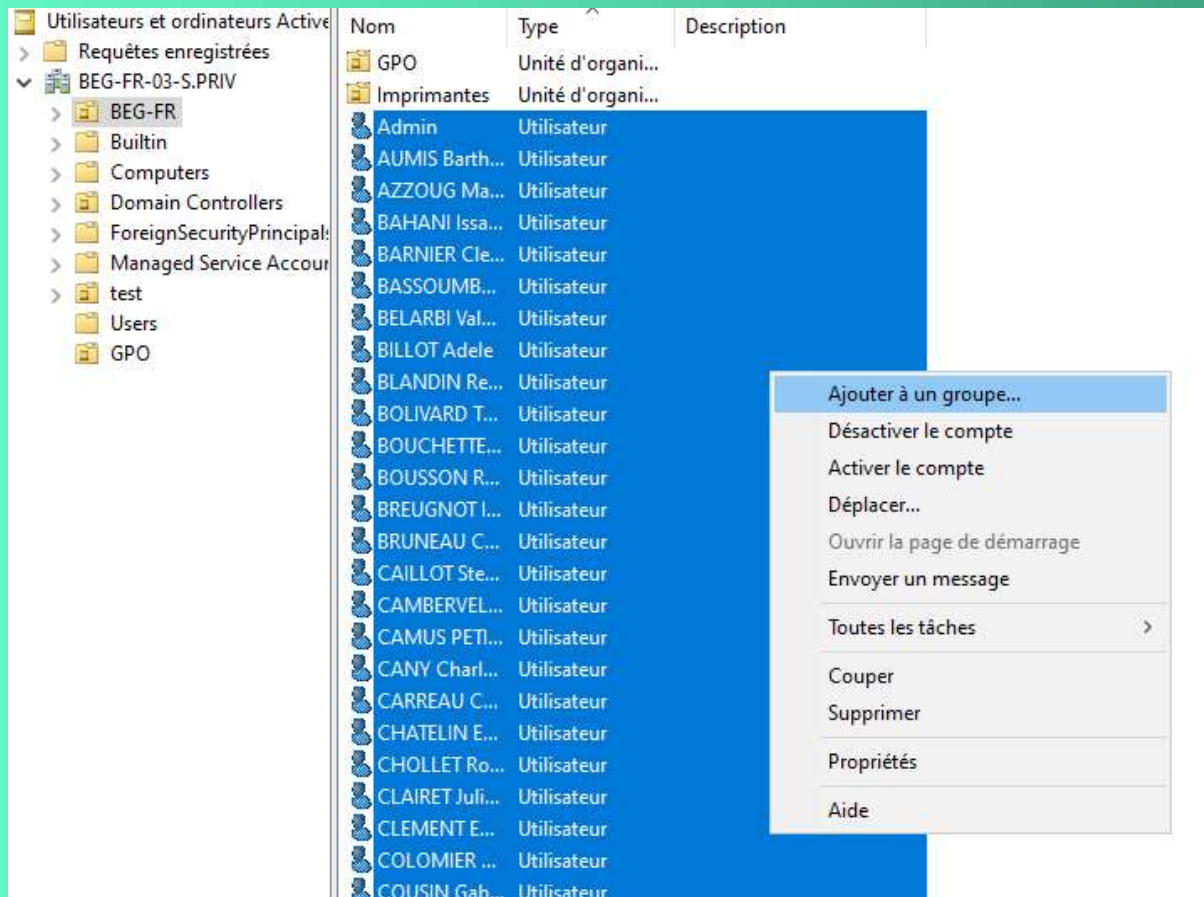
Choisissez dans la liste la GPO que vous venez de créer et cliquez sur OK.



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 ».

Propriétés d'éléments multiples

Général Compte Adresse **Profil** Organisation

Pour modifier une propriété d'objets multiples, sélectionnez la case à cocher pour activer la modification, puis entrez la modification.

Profil utilisateur

☐ Chemin du profil : \\172.20.3.4\Profils_itinerants\$\%u

☐ Script d'ouverture de session :

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 :

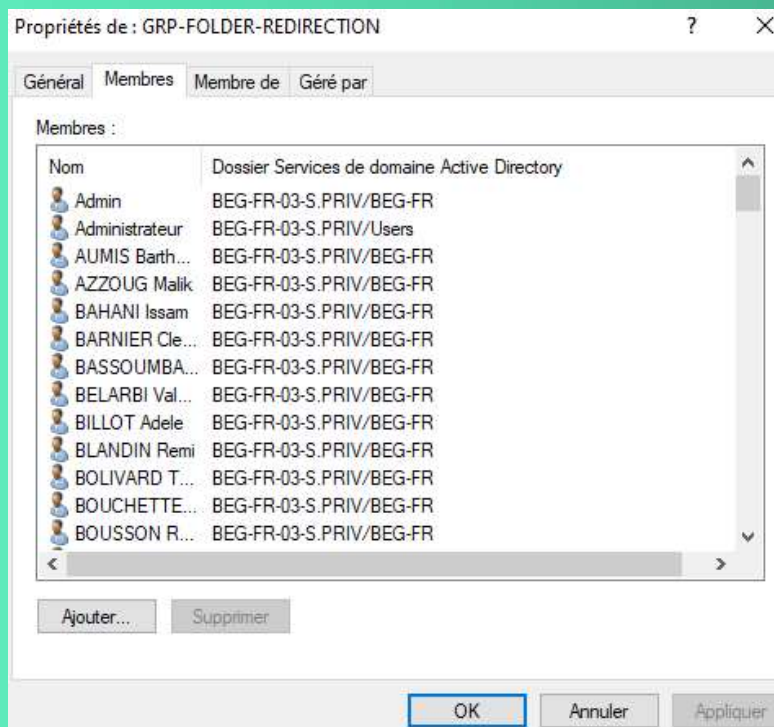
Nous allons créer le groupe de sécurité "GRP-FOLDER-REDIRECTION" avec la commande suivante :
 New-ADGroup -Name "GRP-FOLDER-REDIRECTION" -SamAccountName "GRP-FOLDER-REDIRECTION" -GroupCategory Security -GroupScope DomainLocal -Description "Utilisateurs ayant un profil redirigé"

```
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

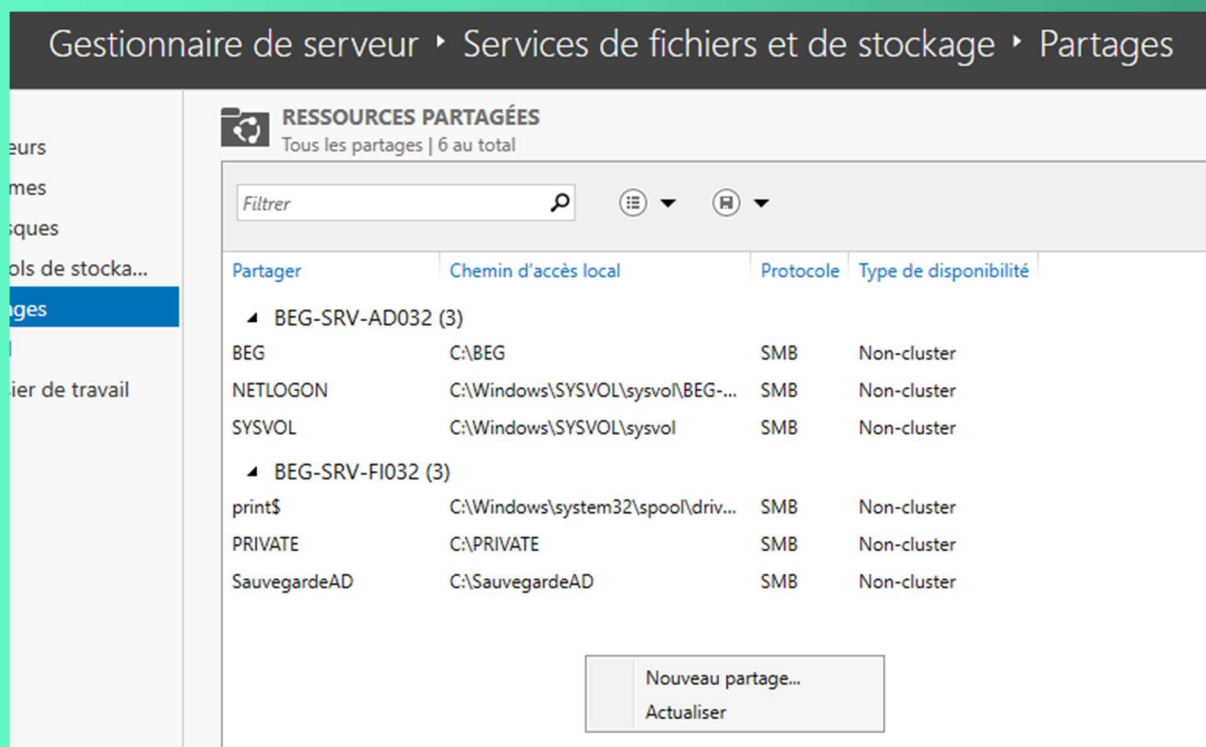
PS C:\Users\Administrateur> New-ADGroup -Name "GRP-FOLDER-REDIRECTION" -SamAccountName "GRP-FOLDER-REDIRECTION" -GroupCategory Security -GroupScope DomainLocal -Description "Utilisateurs ayant un profil redirigé"
```

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

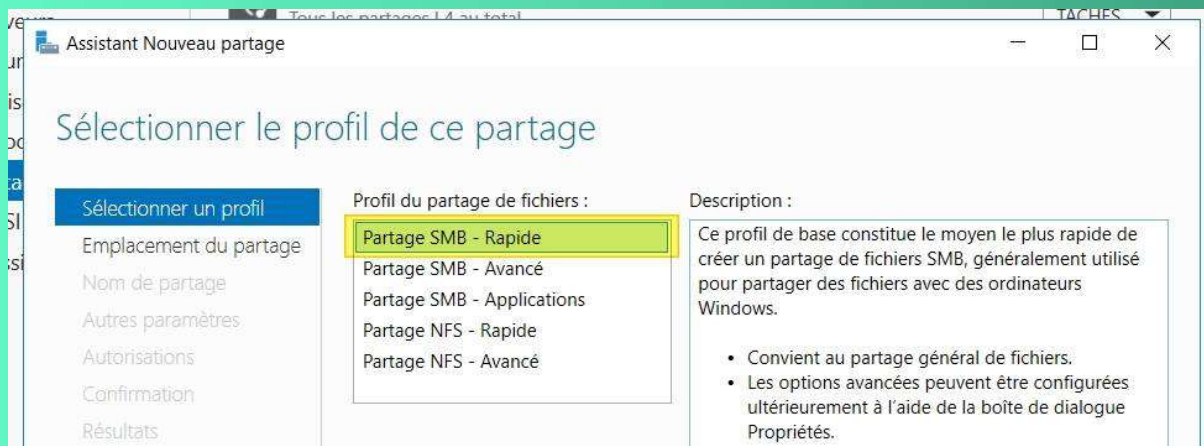


Le partage et attribution des droits :

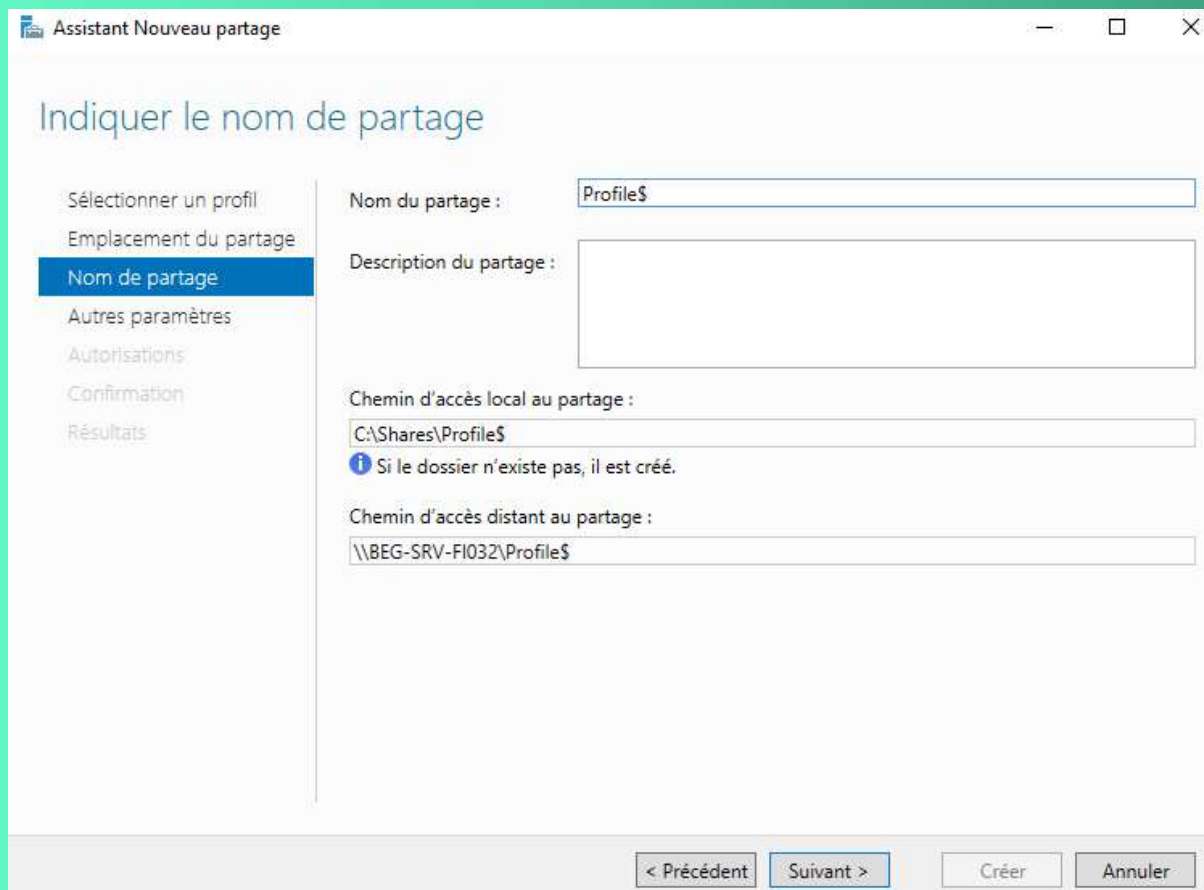
Dans la console "Gestionnaire de serveur", accédez à "Services de fichiers et de stockage" (vous devez installer la fonctionnalité) et ensuite créez un nouveau partage, comme ceci :



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



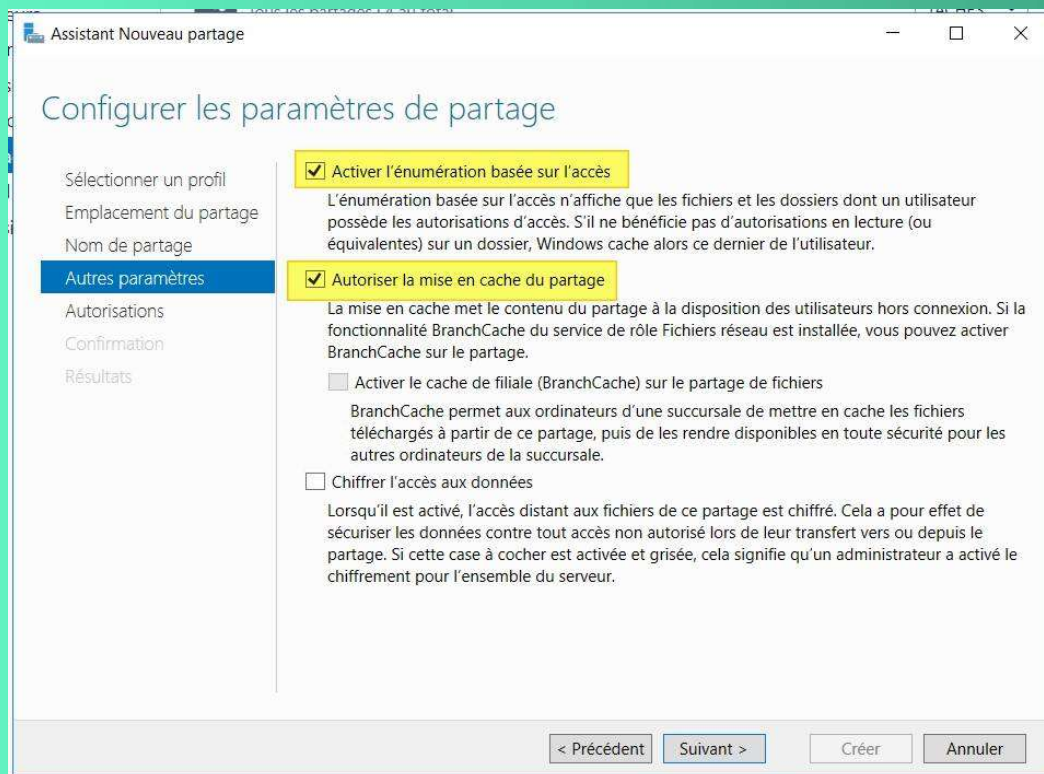
Donnez un nom à votre partage, par exemple : PrProfilsofiles\$. Ce partage étant sensible et qu'il n'y a pas lieu d'y accéder en direct, notamment via la découverte réseau, je vous recommande de mettre un "\$" à la fin du nom pour qu'il soit masqué un minimum.



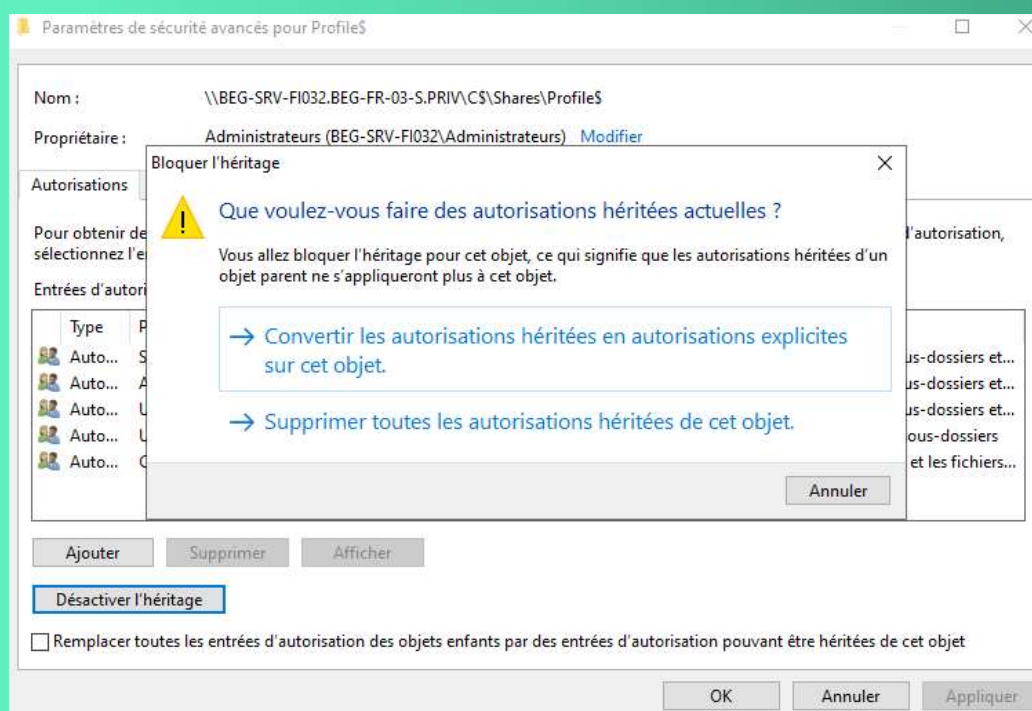
Deux options sont à activer sur cette page :

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 parcourt 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 :

Autorisations pour Profile\$

Principal : GRP-FOLDER-REDIRECTION (IT-CONNECT\GRP-FOLDER-REDIRECTION) [Sélectionnez un principal](#)

Type : Autoriser

S'applique à : Ce dossier seulement

Autorisations avancées :

- ☐ Contrôle total
- ☐ Parcourir le dossier/exécuter le fichier
- ☒ Liste du dossier/lecture de données
- ☒ Attributs de lecture
- ☒ Lecture des attributs étendus
- ☐ Création de fichier/écriture de données
- ☒ Création de dossier/ajout de données
- ☐ Attributs d'écriture
- ☐ Écriture d'attributs étendus
- ☐ Suppression de sous-dossier et fichier
- ☐ Suppression
- ☒ Autorisations de lecture
- ☐ Modifier les autorisations
- ☐ Appropriation

☐ Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

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

Paramètres de sécurité avancés pour Profile\$

Nom : \\BEG-SRV-FI032.BEG-FR-03-S.PRIV\CS\Shares\Profile\$

Propriétaire : Administrateurs (BEG-SRV-FI032\Administrateurs) [Modifier](#)

Autorisations | Partage | Audit | Accès effectif

Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).

Entrées d'autorisations :

Type	Principal	Accès	Hérité de	S'applique à
Auto...	Système	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Auto...	Administrateurs (BEG-SRV-FI0...	Contrôle total	Aucun	Ce dossier, les sous-dossiers et...
Auto...	CREATEUR PROPRIETAIRE	Contrôle total	Aucun	Les sous-dossiers et les fichiers...
Auto...	GRP-FOLDER-REDIRECTION (...)	Spéciale	Aucun	Ce dossier seulement

Ajouter Supprimer Modifier

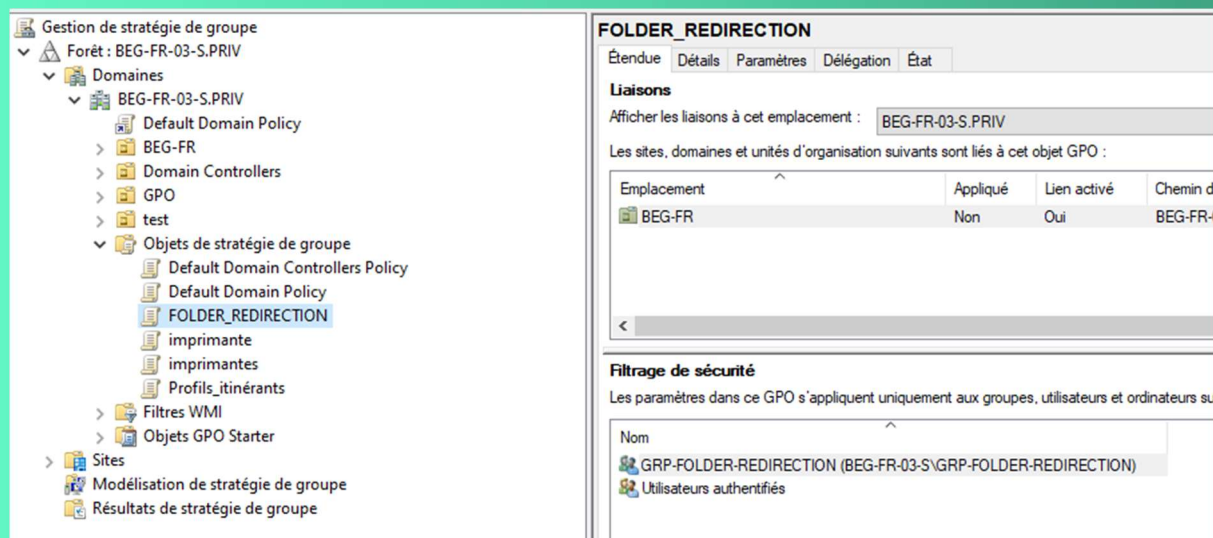
Activer l'héritage

☐ Remplacer toutes les entrées d'autorisation des objets enfants par des entrées d'autorisation pouvant être héritées de cet objet

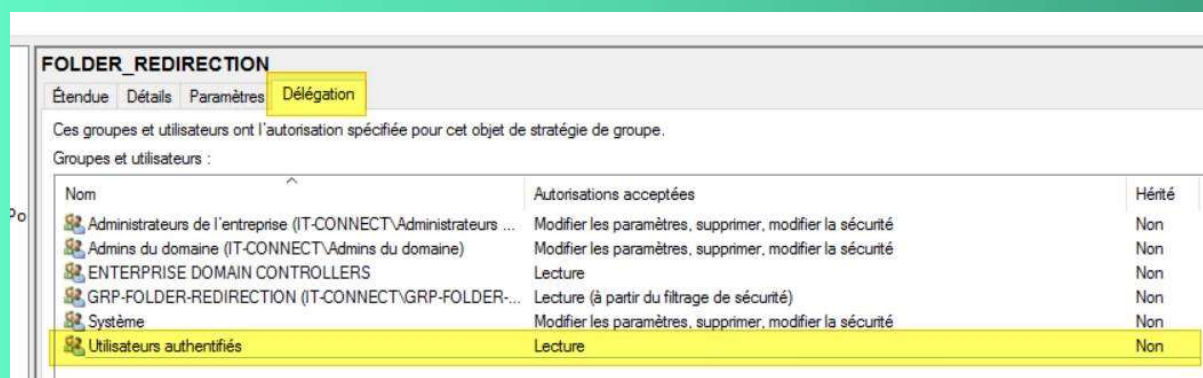
OK Annuler Appliquer

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 :

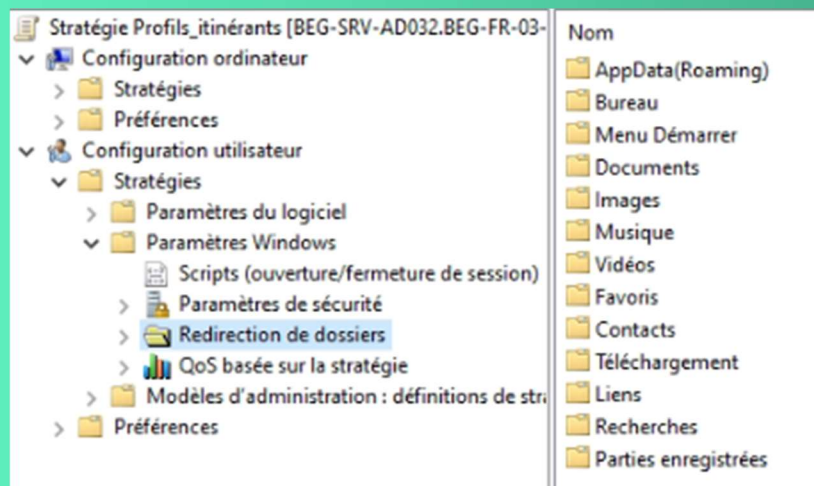


Suite à une mise à jour publiée par Microsoft (MS16-072), il y a eu des changements au niveau de la sécurité et pour que la redirection de profils fonctionne, vous devez ajouter le groupe "Utilisateurs authentifiés" en "Lecture" dans l'onglet "Délégation" :



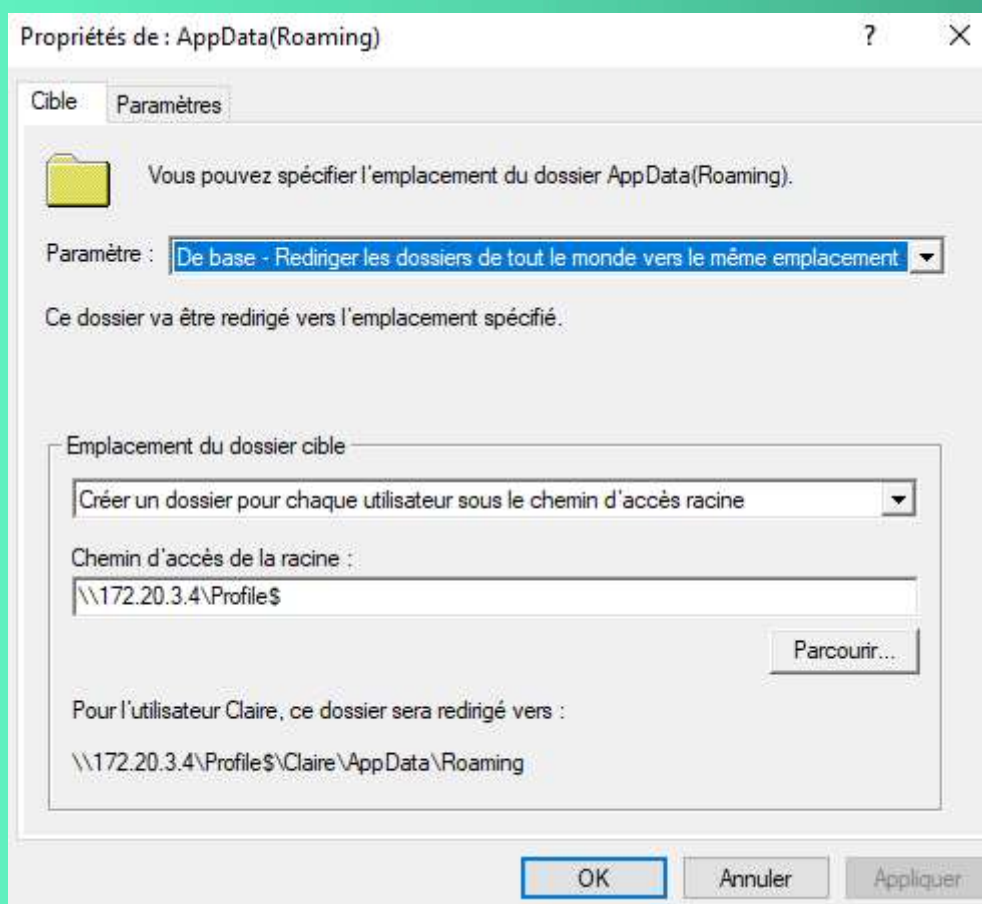
Ensuite, modifiez la GPO pour configurer la redirection de dossiers. Ce paramètre s'applique directement au niveau de l'utilisateur : Configuration utilisateur > Stratégies > Paramètres Windows > Redirection de dossiers

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".



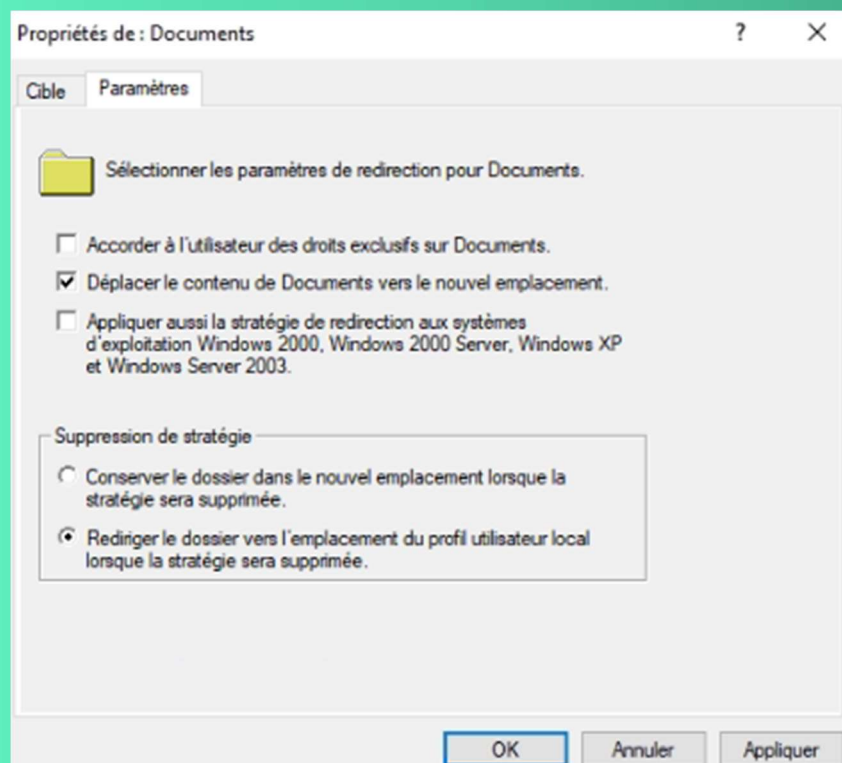
Choisissez l'option "Créer un dossier pour chaque utilisateur le chemin d'accès racine", ce qui rejoint ce que je disais précédemment : à la racine du partage des profils, un dossier va être créé pour l'utilisateur et dans ce dossier, il y aura un dossier "Documents".

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 :

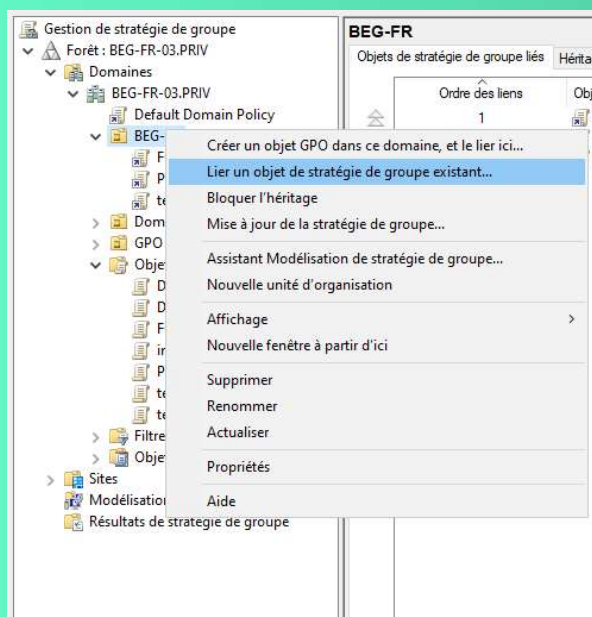
Si vous souhaitez empêcher le compte administrateur d'accéder au dossier et qu'il y ait seulement l'utilisateur qui puisse accéder, alors cochez l'option "Accorder à l'utilisateur des droits exclusifs sur Documents".



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

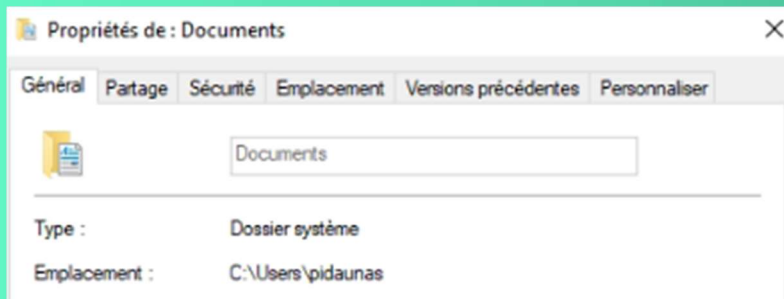
Vous pouvez valider, fermer l'éditeur de GPO et pensez à lier votre GPO sur votre domaine avant de passer à la phase de tests.

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 :

```
J:\>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 touche 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 !

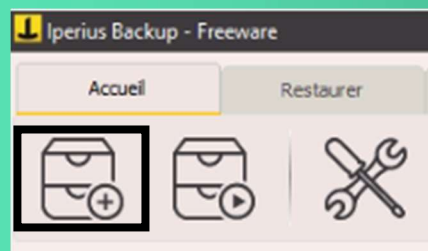
CONFIGURATION DE IPERIUS

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

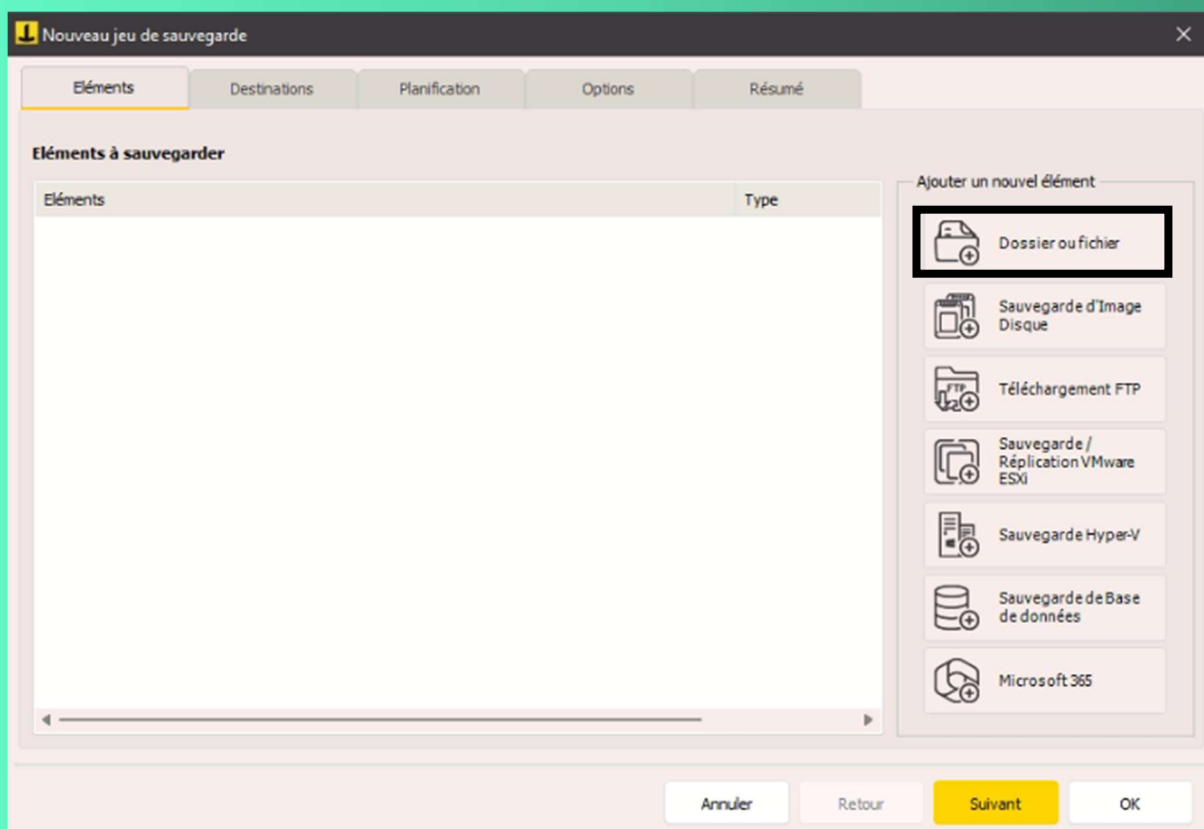
<https://www.iperiusbackup.fr/>

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 :



Après avoir cliquer sur 'Dossier ou fichier', entrer le chemin du dossier que nous souhaitons sauvegarder.

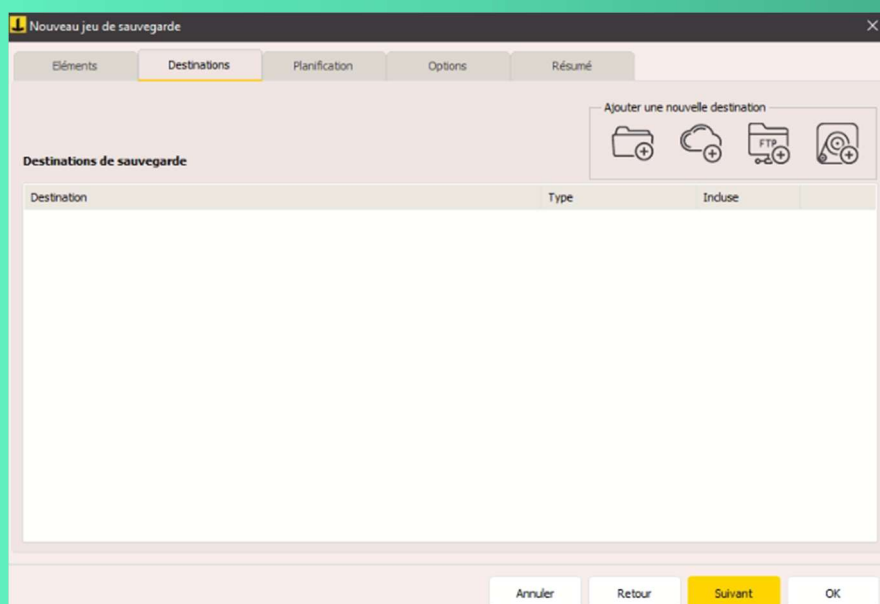
The dialog box 'Ajouter / modifier le dossier' has a title bar with a close button. It contains two radio buttons under 'Type d'élément': 'Dossier' (selected) and 'Fichier'. Below is a 'Chemin' text field with a 'Sélectionner' button and a brace icon. There are three checkboxes: 'Compte utilisateur pour l'accès réseau' (unchecked), 'Copie des autorisations de sécurité' (unchecked, with a note that it's not available in the free version), and 'Recréer le chemin complet de l'élément' (checked, with a note that it's only for local or network peripherals). At the bottom, there are two tabs: 'Filtres' (active) and 'Exclusions'. Under 'Filtres', there is a 'Filtrer par extensions (séparées par ;)' text field, an 'Exclure les extensions spécifiées' dropdown, a 'Filtrer sur la taille' checkbox, and a section 'Exclure les fichiers dont la taille est' with a dropdown, a comparison operator '>', a value '3', and a unit 'Mo'.

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

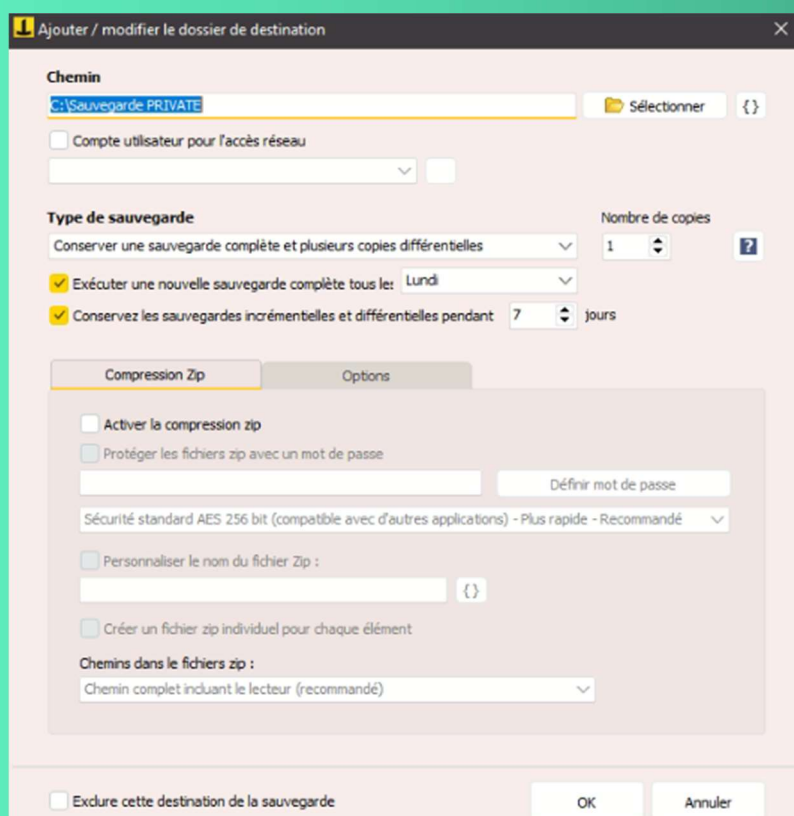
The 'Nouveau jeu de sauvegarde' dialog box has a title bar with a close button and five tabs: 'Éléments' (active), 'Destinations', 'Planification', 'Options', and 'Résumé'. Under 'Éléments à sauvegarder', there is a table with two columns: 'Éléments' and 'Type'. The table contains one row: 'C:\PRIVATE' and 'Dossier'. To the right, there is a section 'Ajouter un nouvel élément' with seven buttons: 'Dossier ou fichier', 'Sauvegarde d'Image Disque', 'Téléchargement FTP', 'Sauvegarde / Réplication VMware ESXi', 'Sauvegarde Hyper-V', 'Sauvegarde de Base de données', and 'Microsoft 365'. At the bottom, there are four buttons: 'Annuler', 'Retour', 'Suivant' (highlighted with a black border), and 'OK'.

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'

The screenshot shows the 'Nouveau jeu de sauvegarde' window with the 'Destinations' tab selected. The window has a title bar with a close button. Below the title bar are five tabs: 'Éléments', 'Destinations' (active), 'Planification', 'Options', and 'Résumé'. In the 'Destinations' tab, there is a section 'Ajouter une nouvelle destination' with four icons: a folder, a cloud, an FTP server, and a hard drive. Below this is a table titled 'Destinations de sauvegarde' with three columns: 'Destination', 'Type', and 'Inclure'. The table contains one entry: 'C:\Sauvegarde PRIVATE' with 'Dossier' as the type and 'Oui' as the inclusion status. At the bottom of the window are four buttons: 'Annuler', 'Retour', 'Suivant' (highlighted with a yellow border), and 'OK'.

Destination	Type	Inclure
C:\Sauvegarde PRIVATE	Dossier	Oui

Planification :

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

The screenshot shows the 'Nouveau jeu de sauvegarde' window with the 'Planification' tab selected. The window has a title bar with a close button. Below the title bar are five tabs: 'Éléments', 'Destinations', 'Planification' (active), 'Options', and 'Résumé'. In the 'Planification' tab, there is a section 'Lancer automatiquement la sauvegarde en utilisant la planification suivante :'. Below this are four radio buttons: 'Hebdomadaire', 'Tous les mois', 'Chaque', and 'Tous les'. The 'Tous les' option is selected. Under 'Tous les', there are three input fields: '1' for 'jours', '0' for 'heures', and '0' for 'minutes'. To the right of these fields is a section 'Liste des planifications :'. Below this section are two buttons: 'Ajouter' and 'Supprimer'. At the bottom of the window are four buttons: 'Annuler', 'Retour', 'Suivant' (highlighted with a yellow border), and 'OK'.

Options :

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

The screenshot shows the 'Options' tab of the 'Nouveau jeu de sauvegarde' window. The 'Notifications' sub-tab is selected. The main option 'Envoyer une notification par e-mail à la fin de la sauvegarde' is unchecked. Below it, the 'Objet' field contains the template '{BACKUP_RESULT} - {JOB_NAME} - Iperius Backup'. There are empty fields for 'Adresses mail des destinataires' and 'Adresses mail des destinataires cachés'. The 'Compte Mail Expéditeur' is set to a dropdown menu with an 'Ajouter / modifier un compte' button. Three checkboxes are present: 'Joindre le fichier de configuration de sauvegarde' (unchecked), 'Fichier journal en pièce jointe (corps du mail si décoché)' (unchecked), and 'Envoyer aux destinataires cachés uniquement si la sauvegarde n'est pas terminée avec succès.' (unchecked). At the bottom, there are radio buttons for 'Toujours envoyer' (selected) and 'Envoyer uniquement dans les cas suivants:'. Navigation buttons 'Annuler', 'Retour', 'Suivant', and 'OK' are at the bottom right.

Résumé :

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

The screenshot shows the 'Résumé' tab of the 'Nouveau jeu de sauvegarde' window. It displays a summary of the configuration: 'Eléments : 1', 'Destinations : 1', 'Planification : Oui', 'Notification par courriel : Non', and 'Autres processus : Non'. On the right, the 'Nom de la sauvegarde' is 'PRIVATE' and the 'Description' field is empty. There is a checked checkbox for 'Connectez et surveillez cette opération de backup avec la console web centralisée (RMM)' with a 'Plus d'informations' link, and an unchecked checkbox for 'Arrêter l'ordinateur à la fin de la sauvegarde'. Navigation buttons 'Annuler', 'Retour', 'Suivant', and 'OK' are at the bottom right.

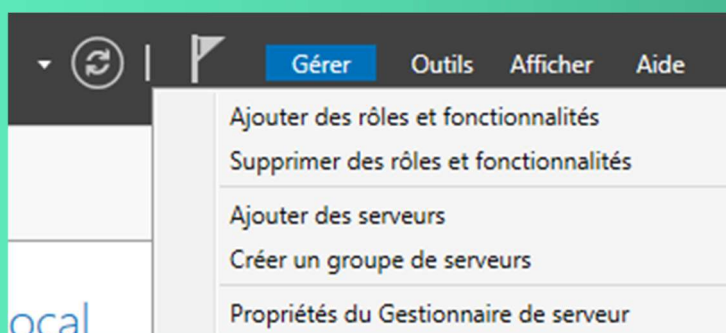
Test de la sauvegarde :

Pour tester la sauvegarde, faire un clic droit et 'lancer la sauvegarde'

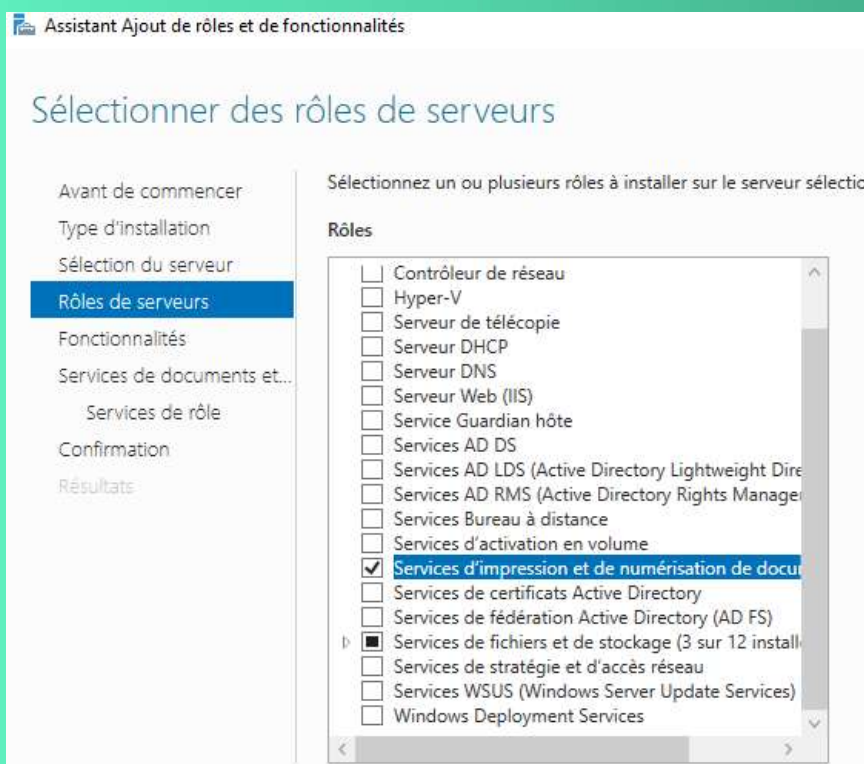
CONFIGURATION DU SERVEUR D'IMPRESSION

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'.

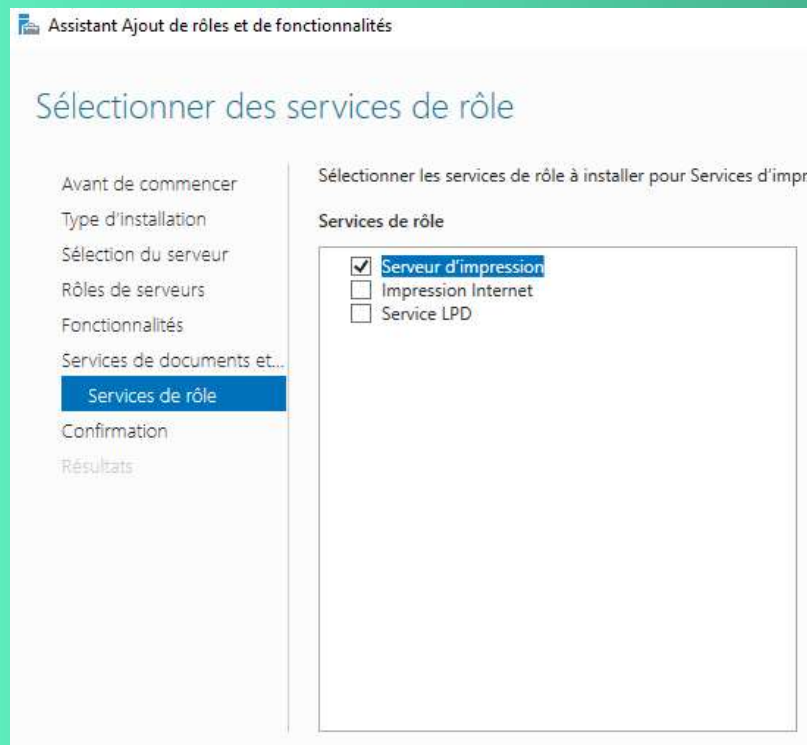


Passez les premières étapes, sélectionnez le rôle 'Services d'impression et de numérisation de documents'



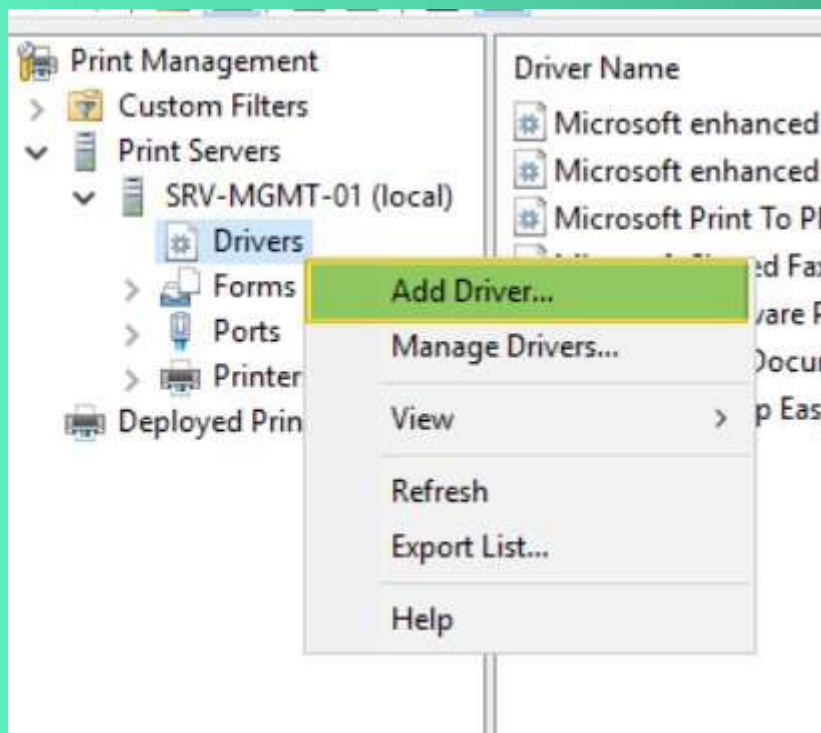
Au niveau des rôles du service d'impression, cochez à minima "Server d'Impression" qui est le serveur d'impression de base. Si vous envisagez de réaliser des impressions depuis des périphériques

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...

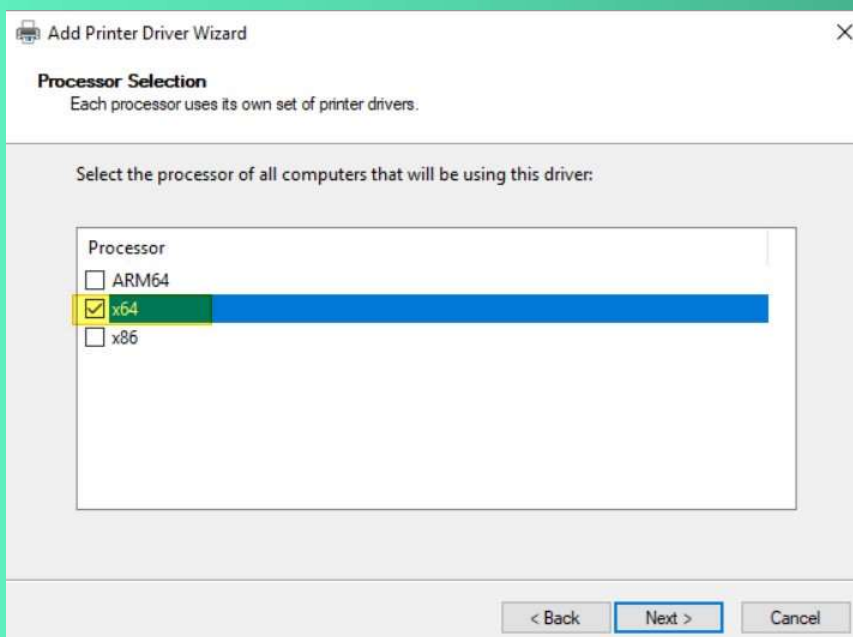


Ajouter un pilote d'impression :

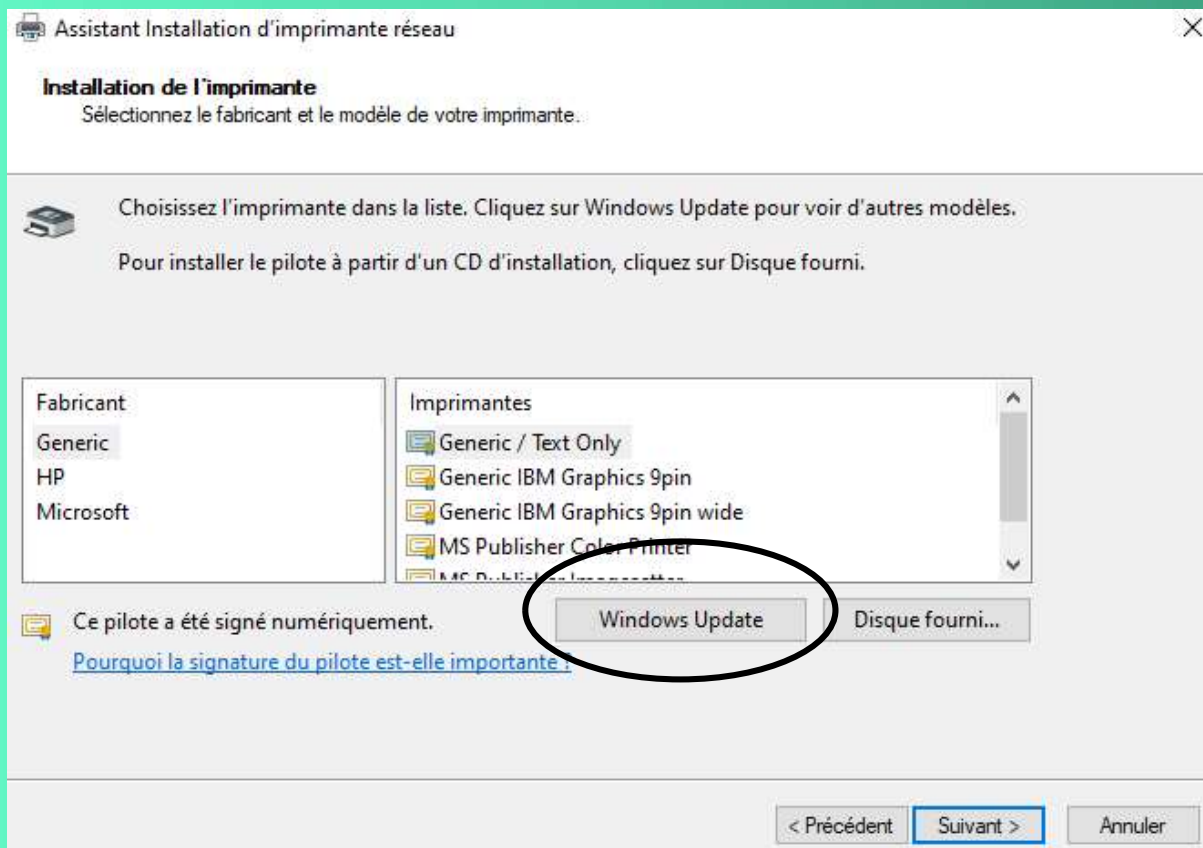
Pour commencer, nous allons donc importer notre pilote sur le serveur d'impression. Ce qui s'effectue de cette manière : Serveurs d'impression > nom de votre serveur > clic droit sur "Pilotes" et "Ajouter un pilote".



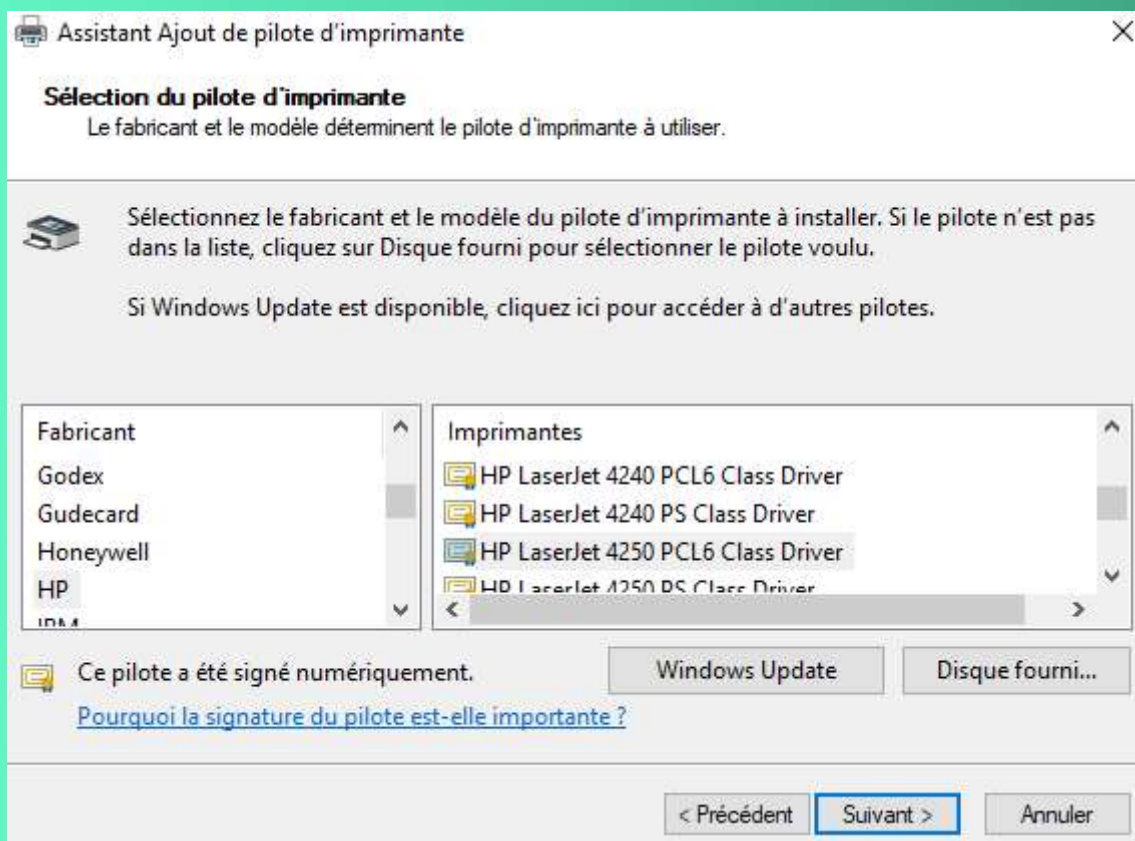
Sélectionnez les architectures processeurs compatibles avec le pilote que vous souhaitez importer.



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.

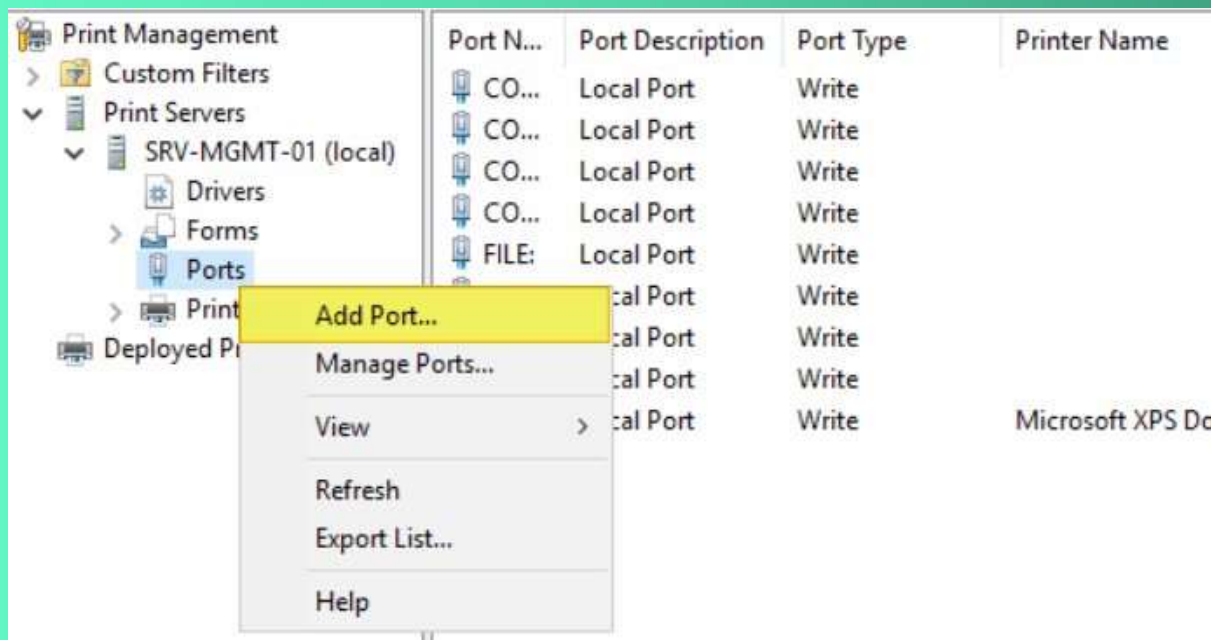


Ensuite, choisir le bon pilote, avec la marque et ensuite le modèle

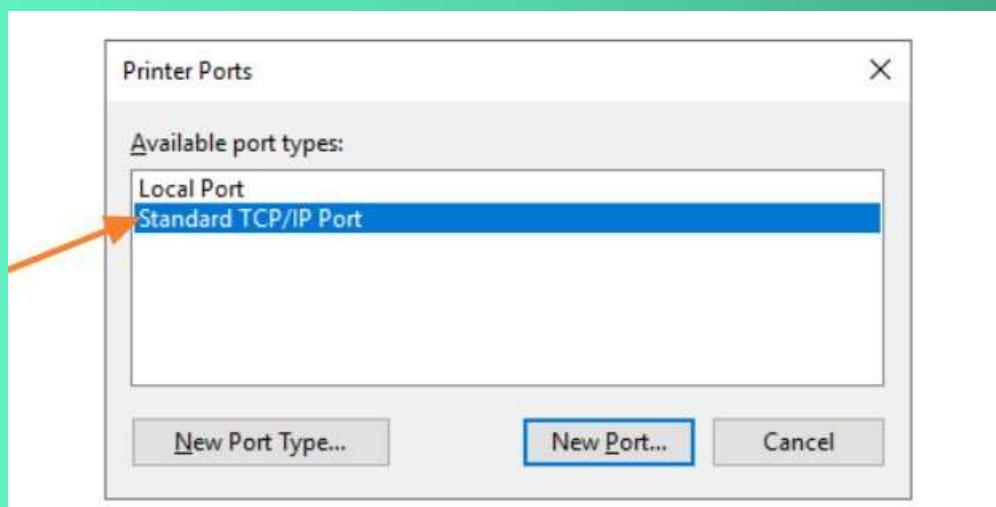


Créer un port TCP/IP :

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.

Assistant Ajout de port imprimante TCP/IP standard

Ajouter un port
Pour quel périphérique voulez-vous ajouter un port ?

Entrez un nom d'imprimante ou une adresse IP, et le nom du port pour le périphérique désiré.

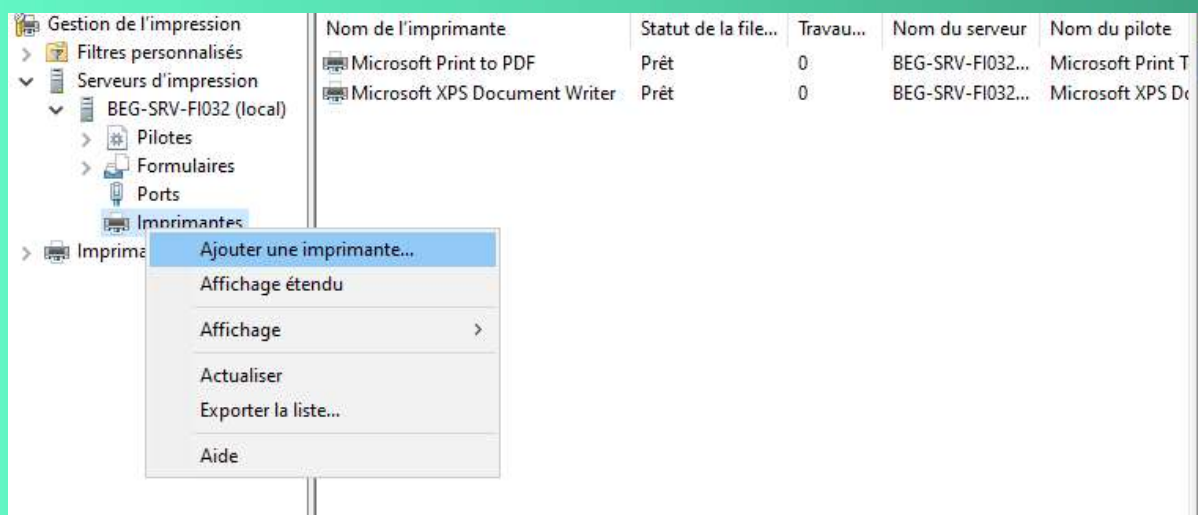
Nom ou adresse IP de l'imprimante :

Nom du port :

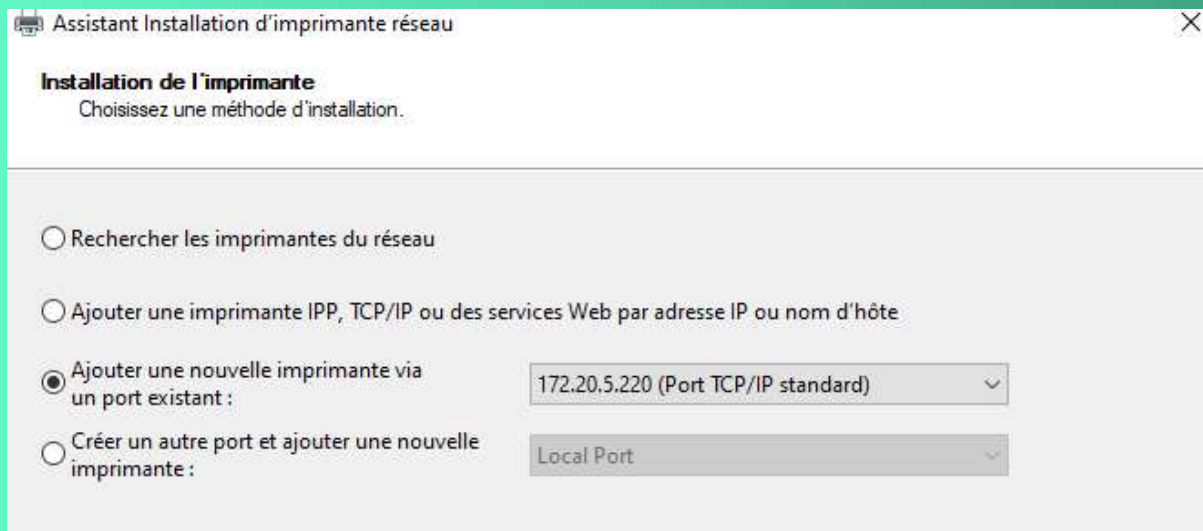
< Précédent Suivant > Annuler

Ajouter l'imprimante à partager :

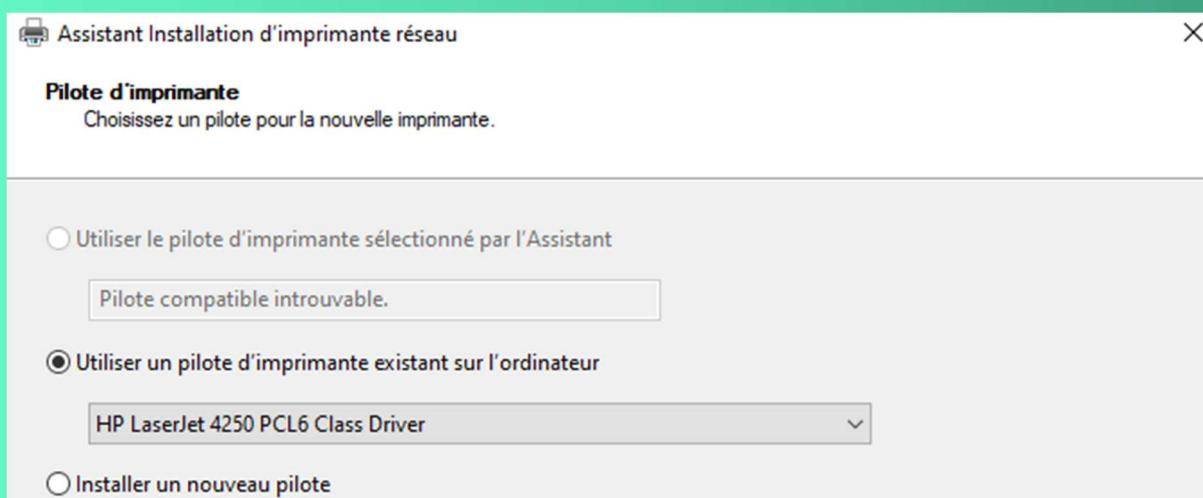
Pour ajouter l'imprimante, effectuez un clic droit sur "Imprimantes" et cliquez sur "Ajouter une imprimante".



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



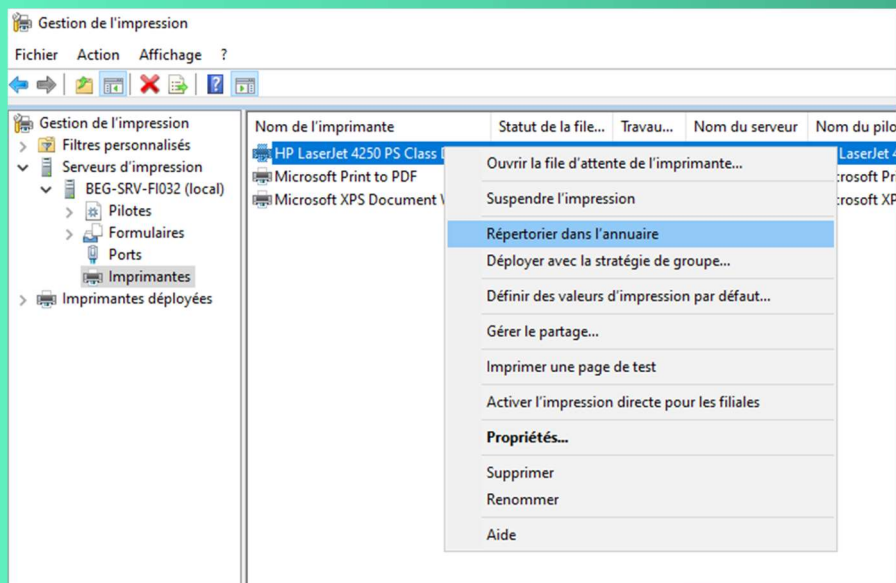
Sélectionner 'utiliser un pilote d'imprimante existant sur l'ordinateur



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 :

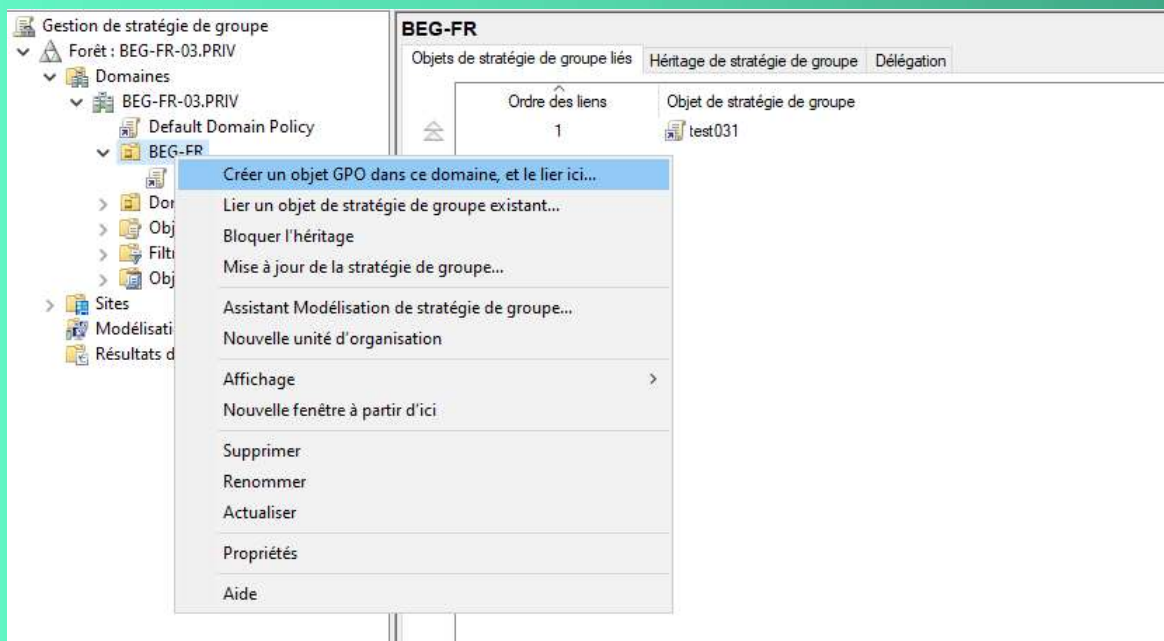
Répertorier l'imprimante dans l'annuaire :

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.

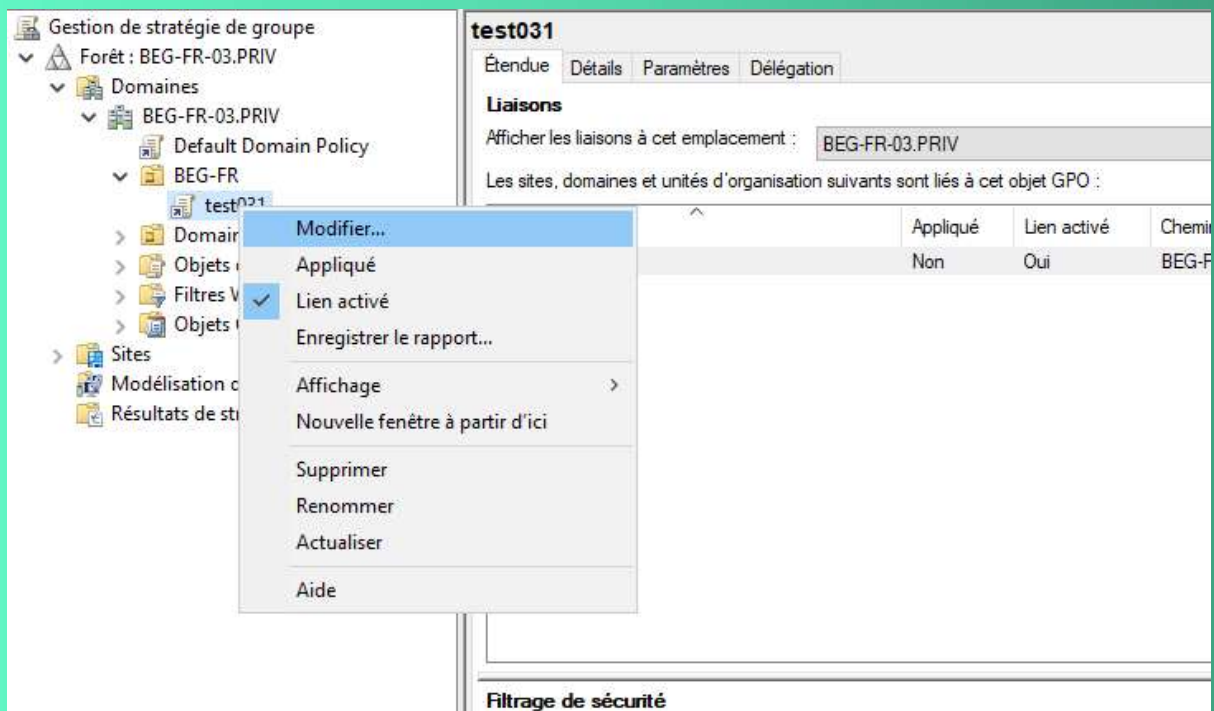


Création de la GPO :

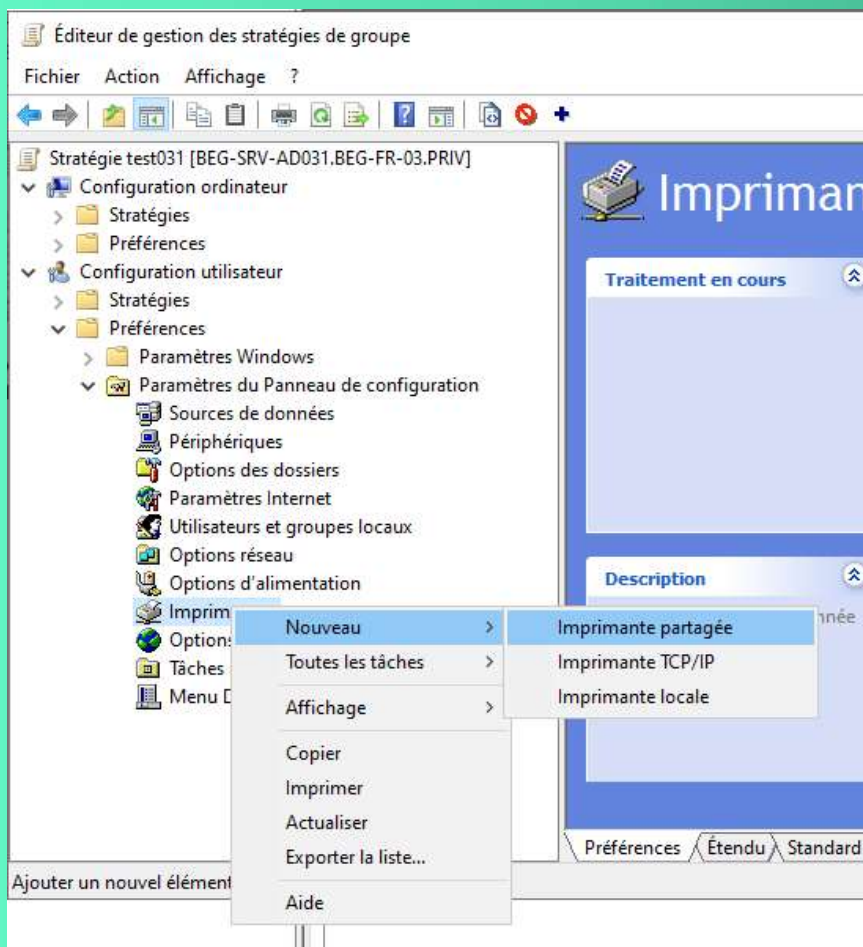
Création d'une GPO nommée 'imprimantes' en faisant clic droit sur une Unité d'Organisation



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

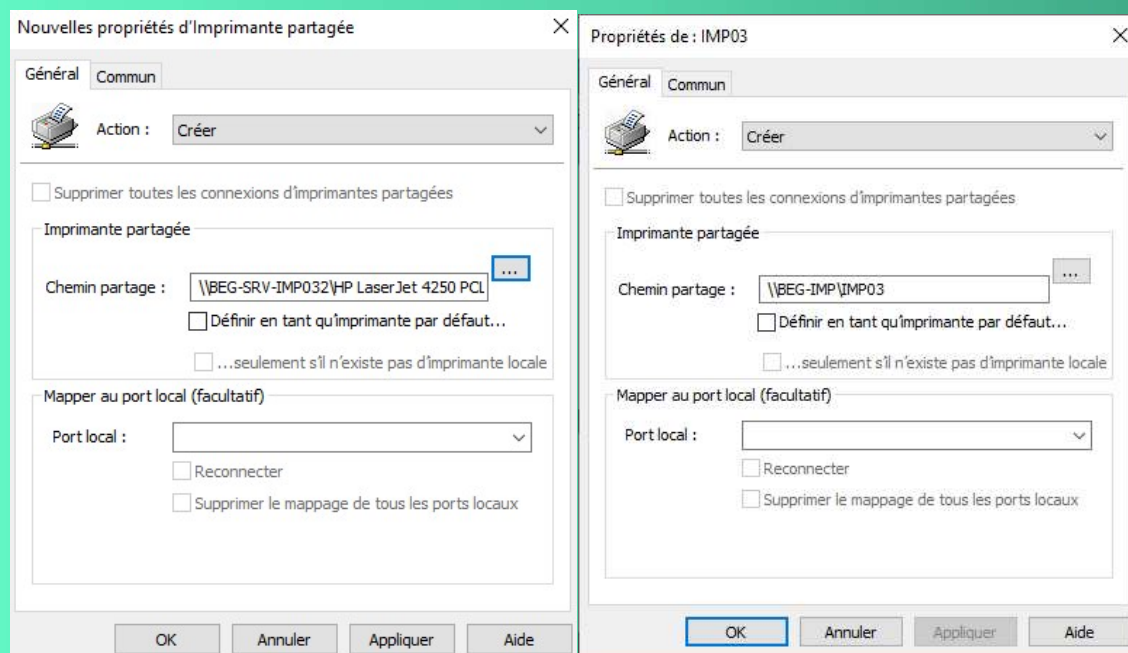


Ensuite, aller dans Configuration utilisateur > Préférences > Paramètres de Panneau de configuration > imprimantes puis faire un clic droit, nouveau et imprimante partagée



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.

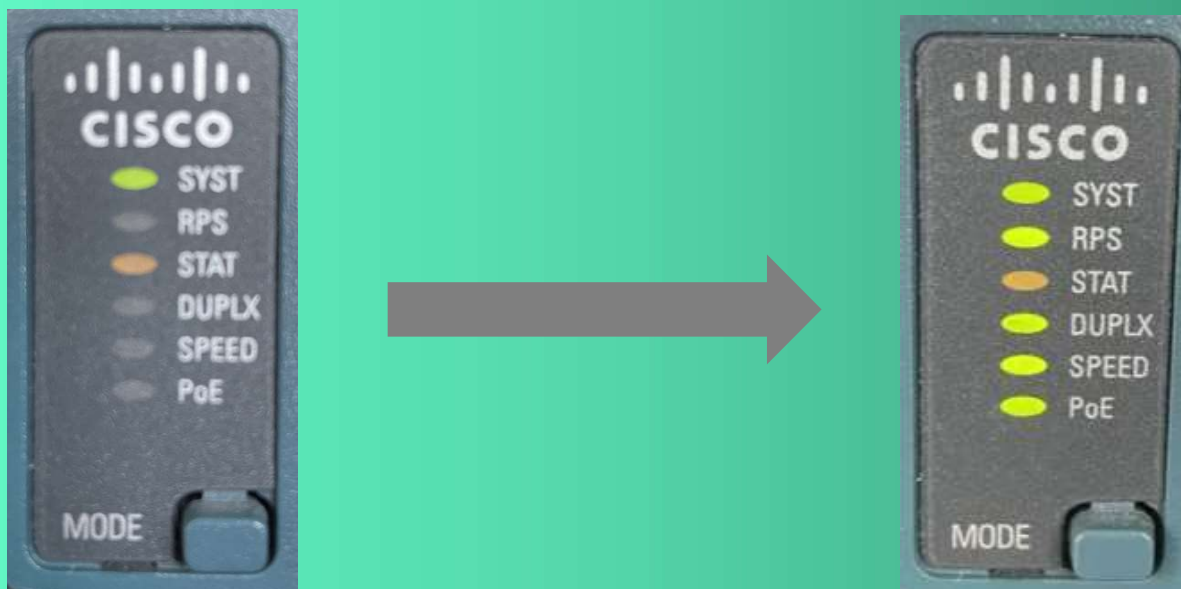
Configuration de l'adresse IP

- ➔ 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 :

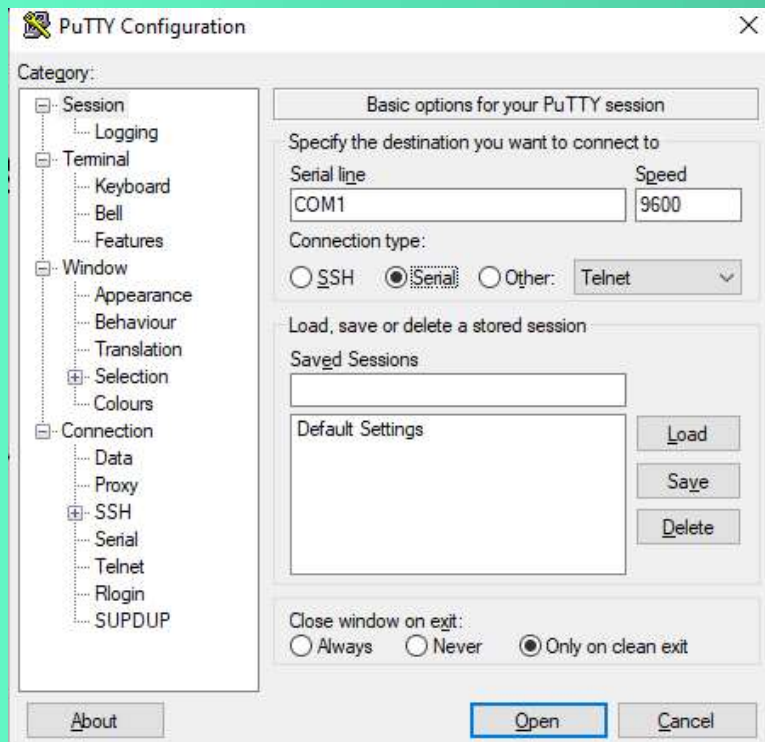
Pour réinitialiser le switch aux paramètres d'usine, il faut appuyer sur le bouton mode et maintenez-le enfoncé, les voyants LED du commutateur commencent à clignoter au bout de 3 secondes. Maintenez toujours le bouton mode enfoncé, les LED cessent de clignoter après 7 secondes supplémentaires puis le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

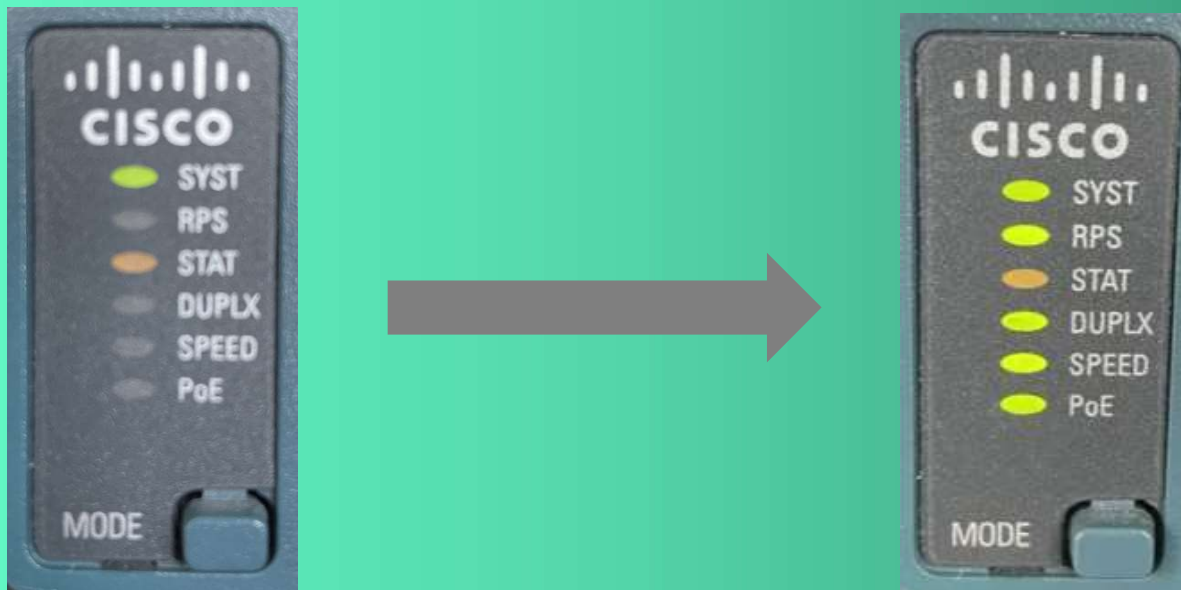
```
!
interface FastEthernet0/1
  switchport mode access
!
interface FastEthernet0/2
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
  switchport nonegotiate
!
interface FastEthernet0/3
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
  switchport nonegotiate
!
interface 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 :

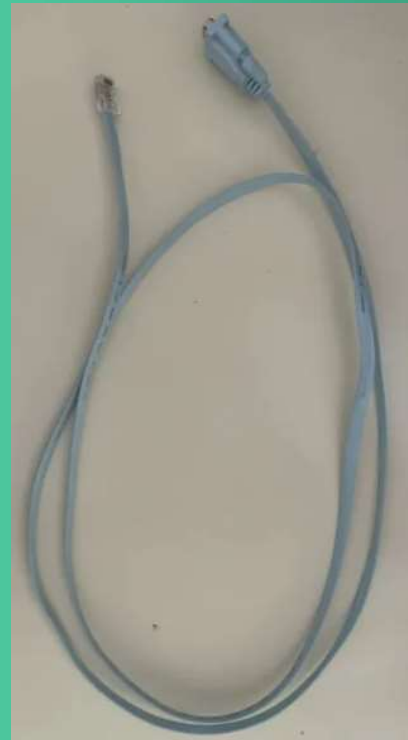
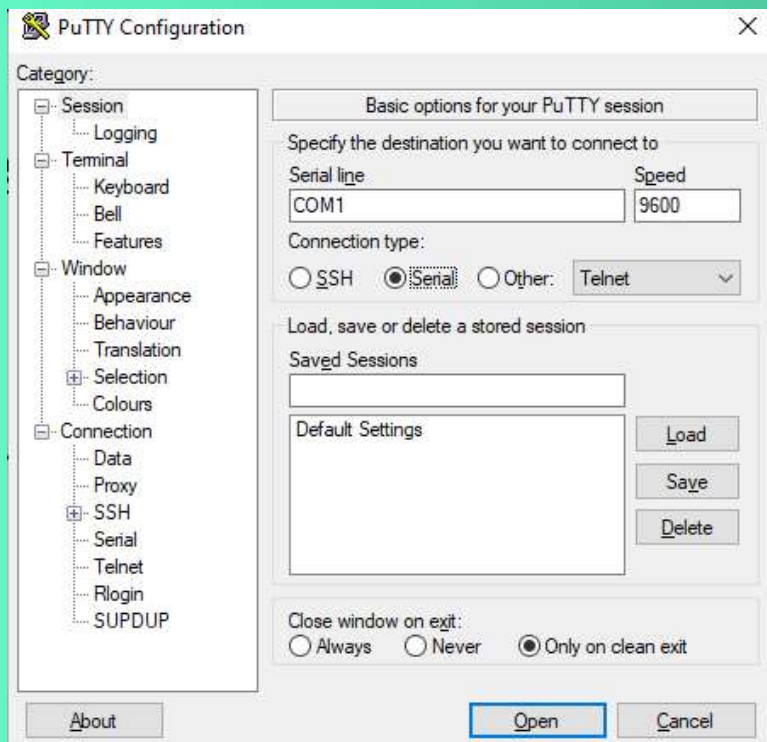
Pour réinitialiser le switch aux paramètres d'usine, il faut appuyer sur le bouton mode et maintenez-le enfoncé, les voyants LED du commutateur commencent à clignoter au bout de 3 secondes. Maintenez toujours le bouton mode enfoncé, les LED cessent de clignoter après 7 secondes supplémentaires puis le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

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 créés, 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
```

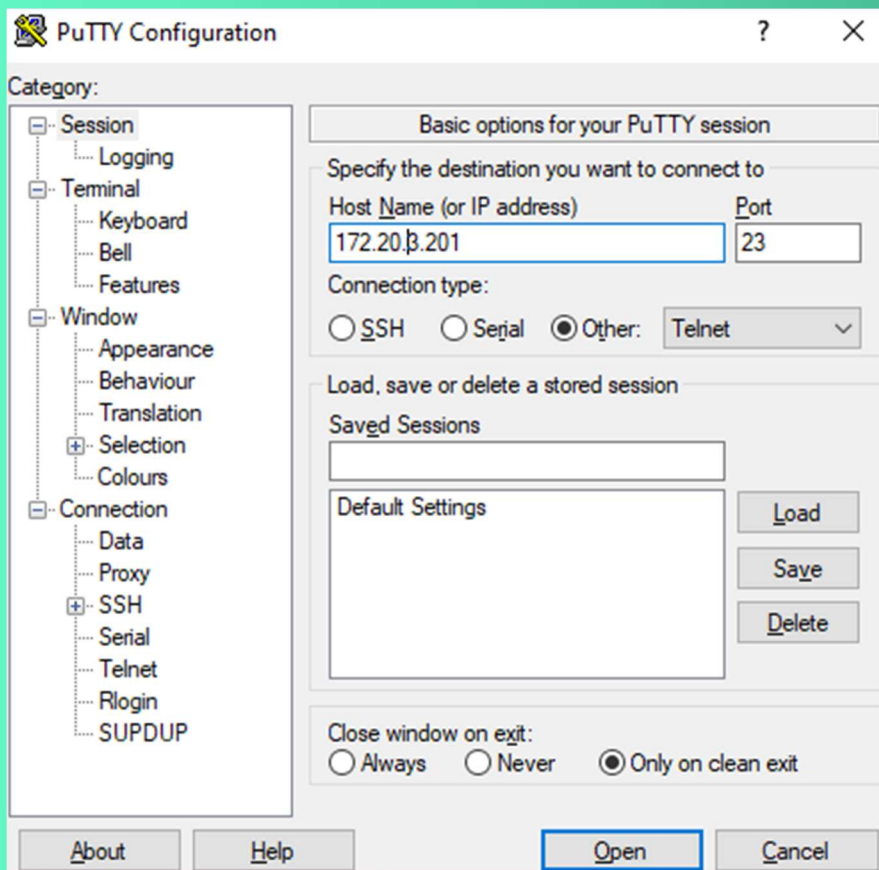
Sur le port 24, nous allons 'taguer le port' en activant le mode trunk et y autoriser le VLAN 10, 20 et 30

```
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.



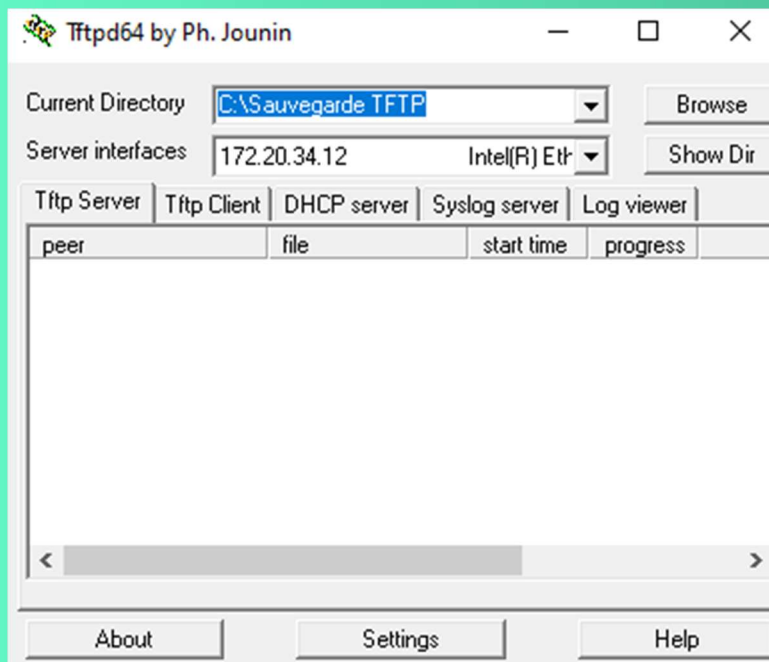


Sauvegarde TFTP :

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 démarrage. 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-config]?
!!
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

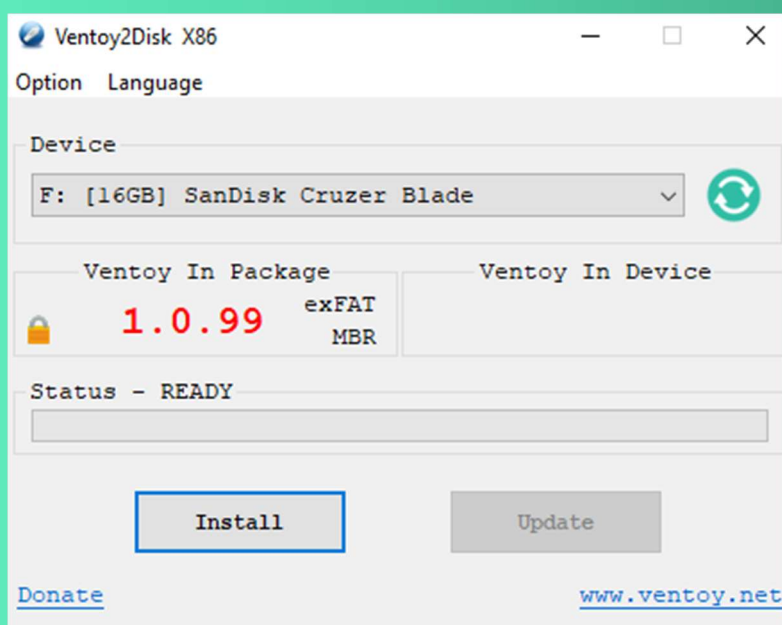
INSTALLATION D'UNE CLE VENTOY

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

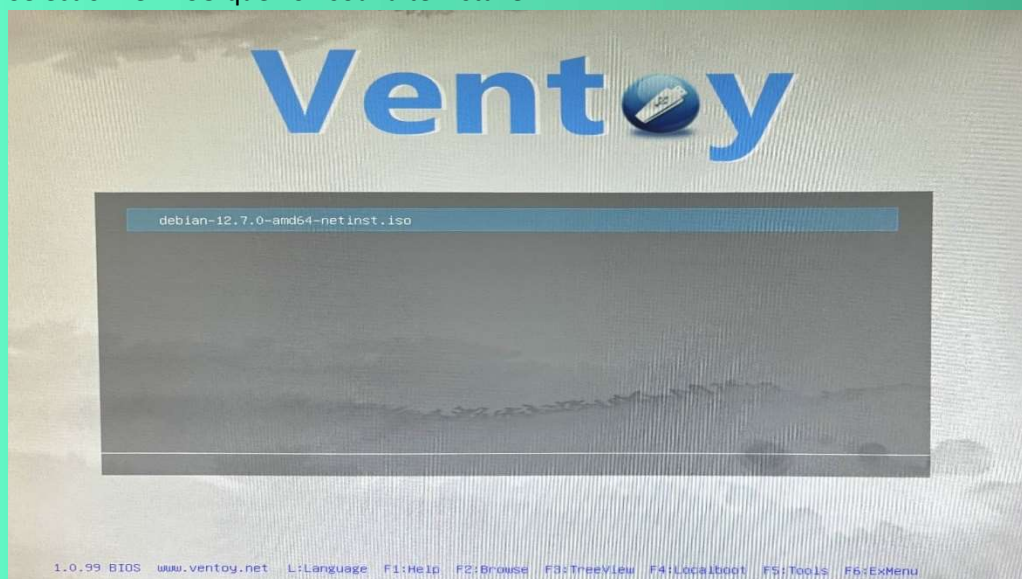
Pour installer ventoy, il faut se rendre sur le site : <https://www.ventoy.net/en/download.html>

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

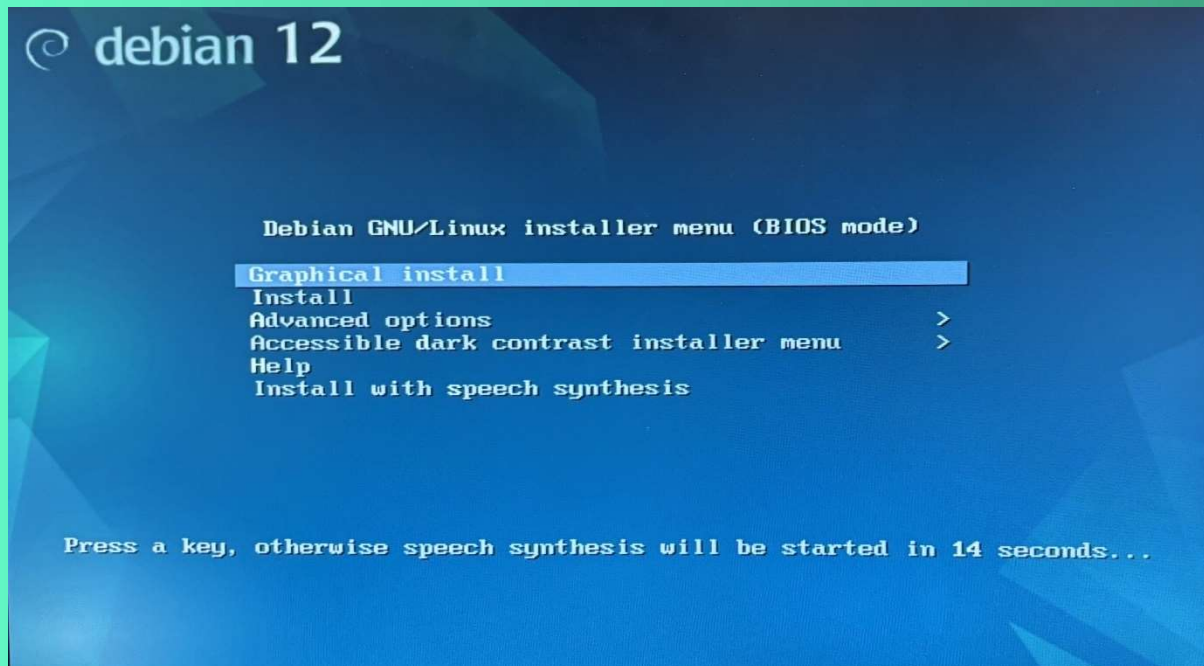
Ensuite, nous avons installé ventoy sur une clé USB en format FAT32



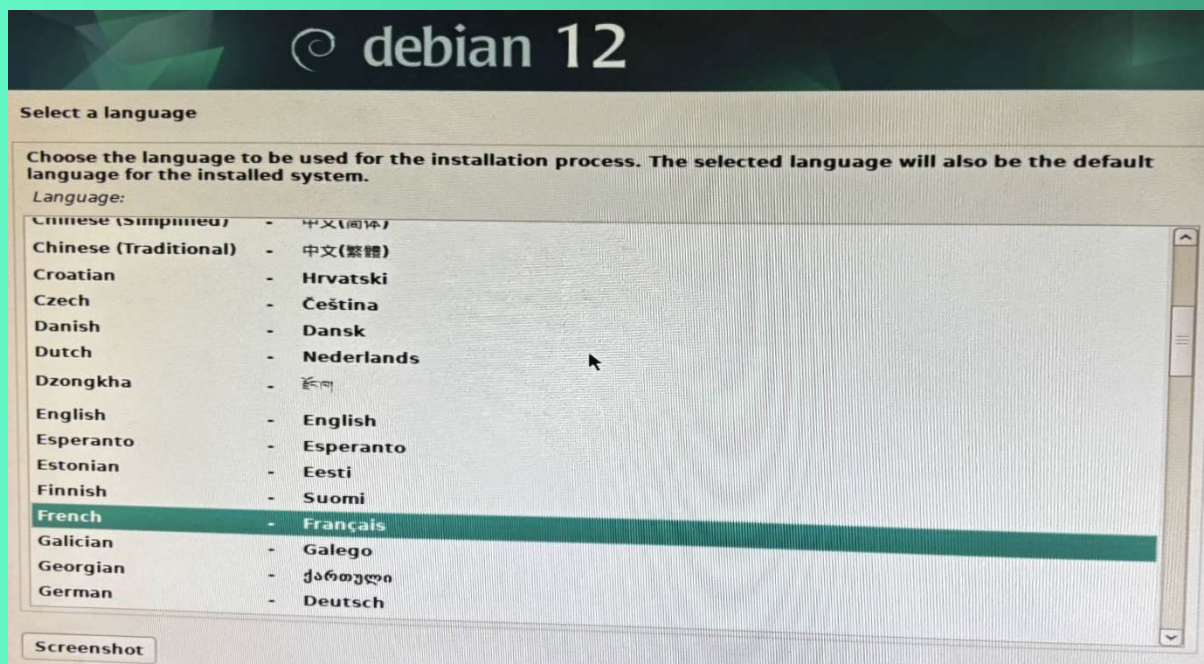
Sélectionner l'ISO que l'on souhaite installer



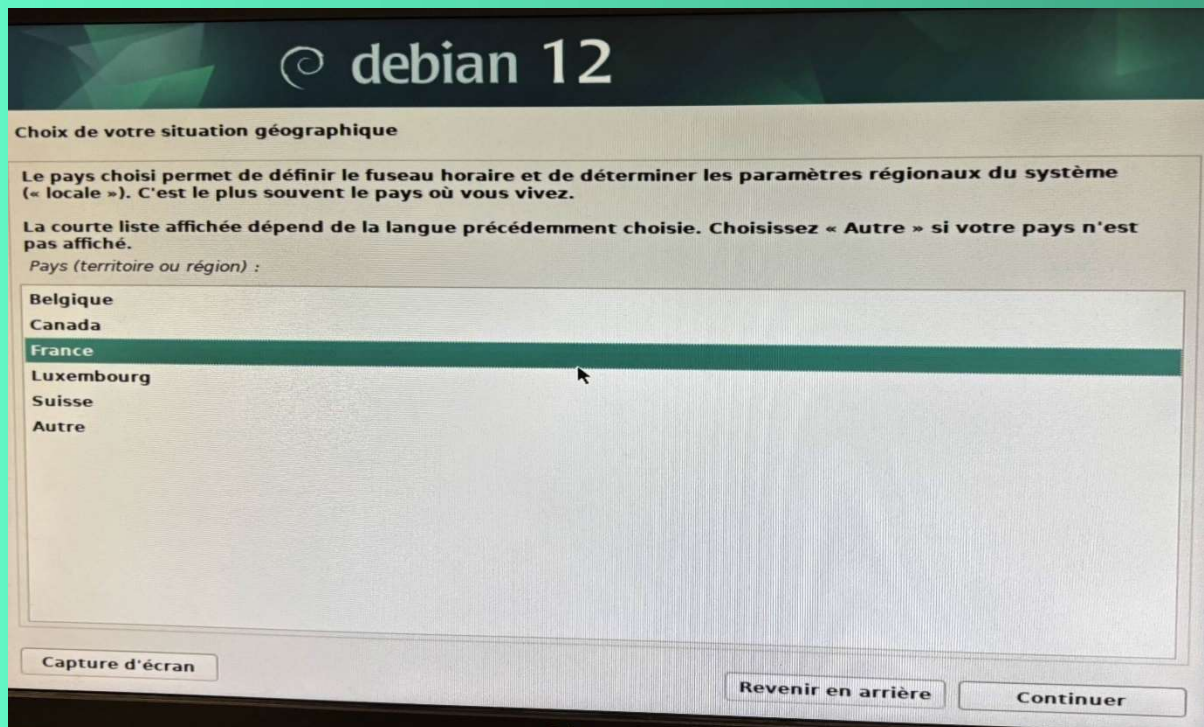
Installation de Debian 12 en version graphique



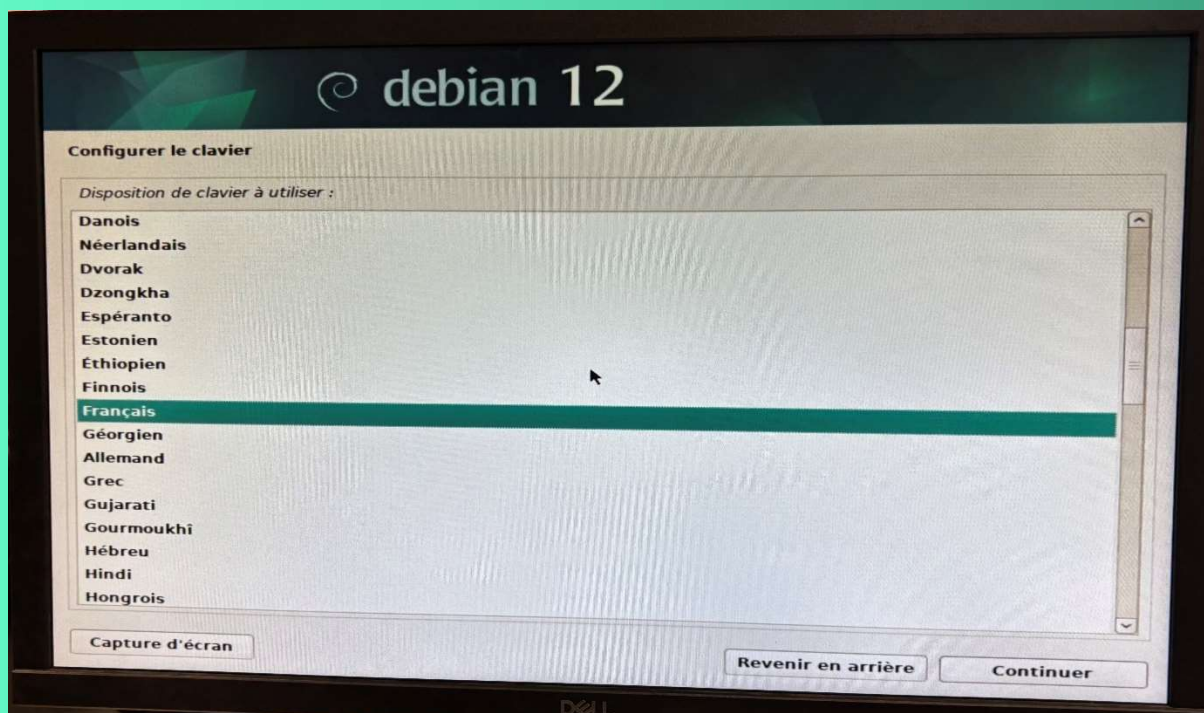
Sélection de la langue qui sera utilisé pour le processus d'installation



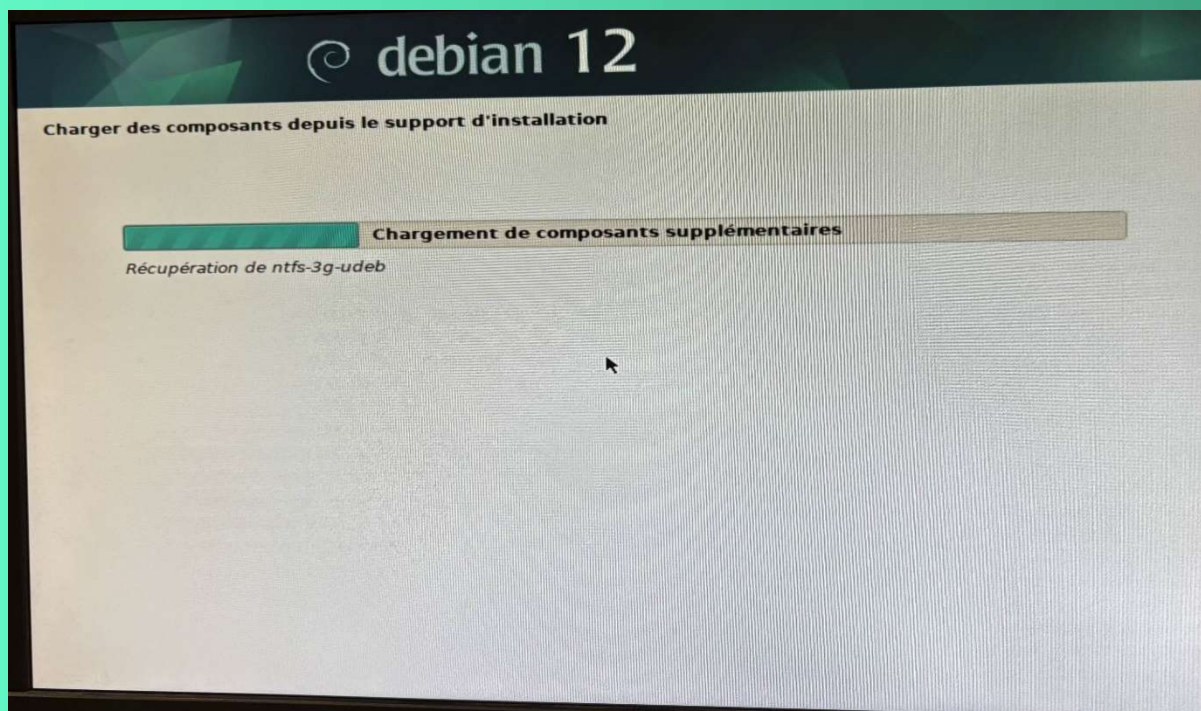
Choisir son pays local permettant de définir le fuseau horaire



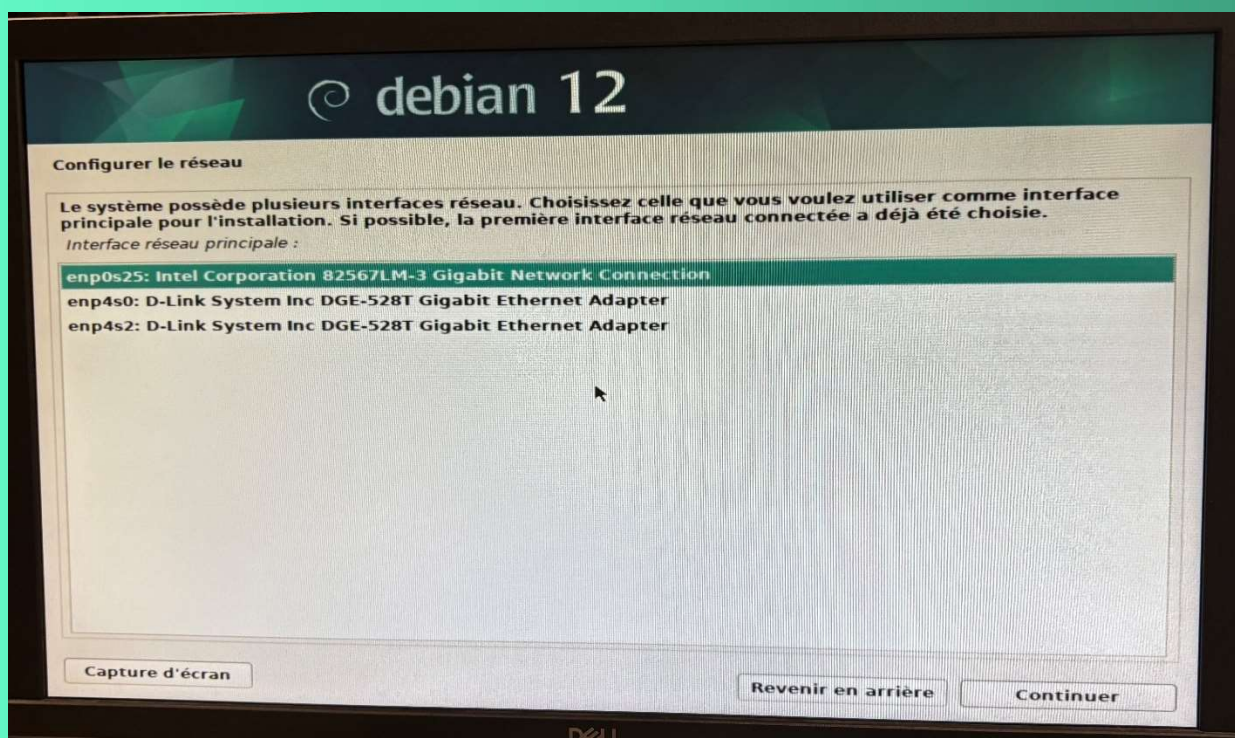
Configurer la langue du clavier



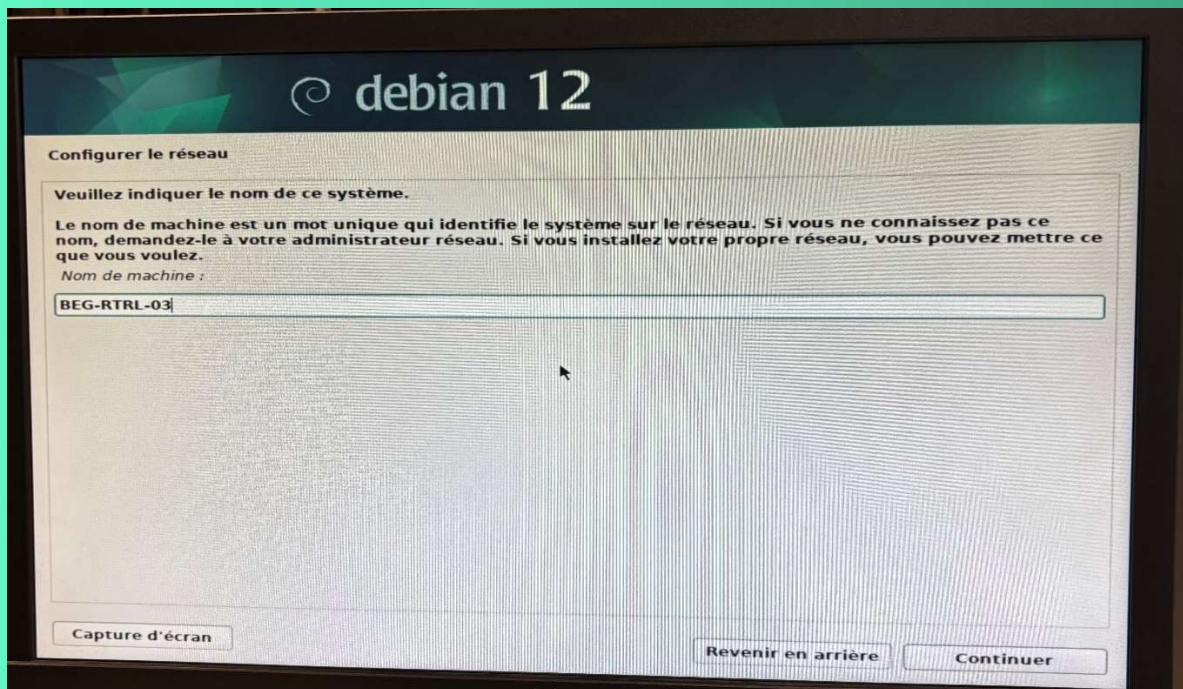
Chargement de composants supplémentaires nécessaires depuis le support d'installation



Sélection de la carte réseau principale



Configuration de nom de la machine



The screenshot shows the 'Configurer le réseau' (Configure network) screen in the Debian 12 installer. The title bar at the top says 'debian 12'. The main heading is 'Configurer le réseau'. Below it, a text box says 'Veuillez indiquer le nom de ce système.' (Please indicate the name of this system). A paragraph explains that the machine name is a unique identifier and provides instructions on where to get it if unknown. A text input field labeled 'Nom de machine :' contains the text 'BEG-RTKL-03'. At the bottom, there are three buttons: 'Capture d'écran' (Screenshot), 'Revenir en arrière' (Go back), and 'Continuer' (Continue).

debian 12

Configurer le réseau

Veuillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

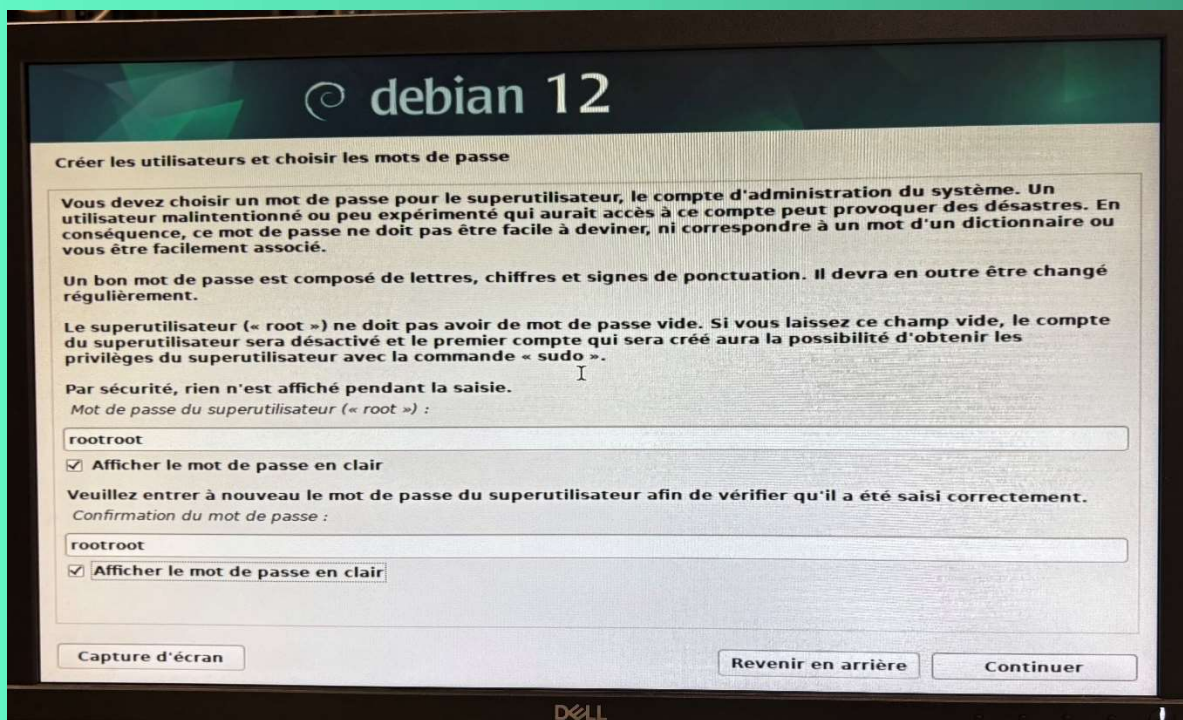
BEG-RTKL-03

Capture d'écran

Revenir en arrière

Continuer

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



The screenshot shows the 'Créer les utilisateurs et choisir les mots de passe' (Create users and choose passwords) screen in the Debian 12 installer. The title bar at the top says 'debian 12'. The main heading is 'Créer les utilisateurs et choisir les mots de passe'. A paragraph explains the importance of choosing a strong password for the superuser. Another paragraph states that a good password is composed of letters, numbers, and punctuation. A third paragraph explains that the superuser ('root') must have a password, and if left empty, it will be disabled. A text input field labeled 'Mot de passe du superutilisateur (« root ») :' contains the text 'rootroot'. Below it, there is a checkbox 'Afficher le mot de passe en clair' (Show password in plain text) which is checked. A paragraph says 'Veuillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.' (Please enter the superuser password again to verify it was entered correctly). Below that, a text input field labeled 'Confirmation du mot de passe :' contains the text 'rootroot'. At the bottom, there are three buttons: 'Capture d'écran' (Screenshot), 'Revenir en arrière' (Go back), and 'Continuer' (Continue).

debian 12

Créer les utilisateurs et choisir les mots de passe

Vous devez choisir un mot de passe pour le superutilisateur, le compte d'administration du système. Un utilisateur malintentionné ou peu expérimenté qui aurait accès à ce compte peut provoquer des désastres. En conséquence, ce mot de passe ne doit pas être facile à deviner, ni correspondre à un mot d'un dictionnaire ou vous être facilement associé.

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Le superutilisateur (« root ») ne doit pas avoir de mot de passe vide. Si vous laissez ce champ vide, le compte du superutilisateur sera désactivé et le premier compte qui sera créé aura la possibilité d'obtenir les privilèges du superutilisateur avec la commande « sudo ».

Par sécurité, rien n'est affiché pendant la saisie.

Mot de passe du superutilisateur (« root ») :

rootroot

☒ Afficher le mot de passe en clair

Veuillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.

Confirmation du mot de passe :

rootroot

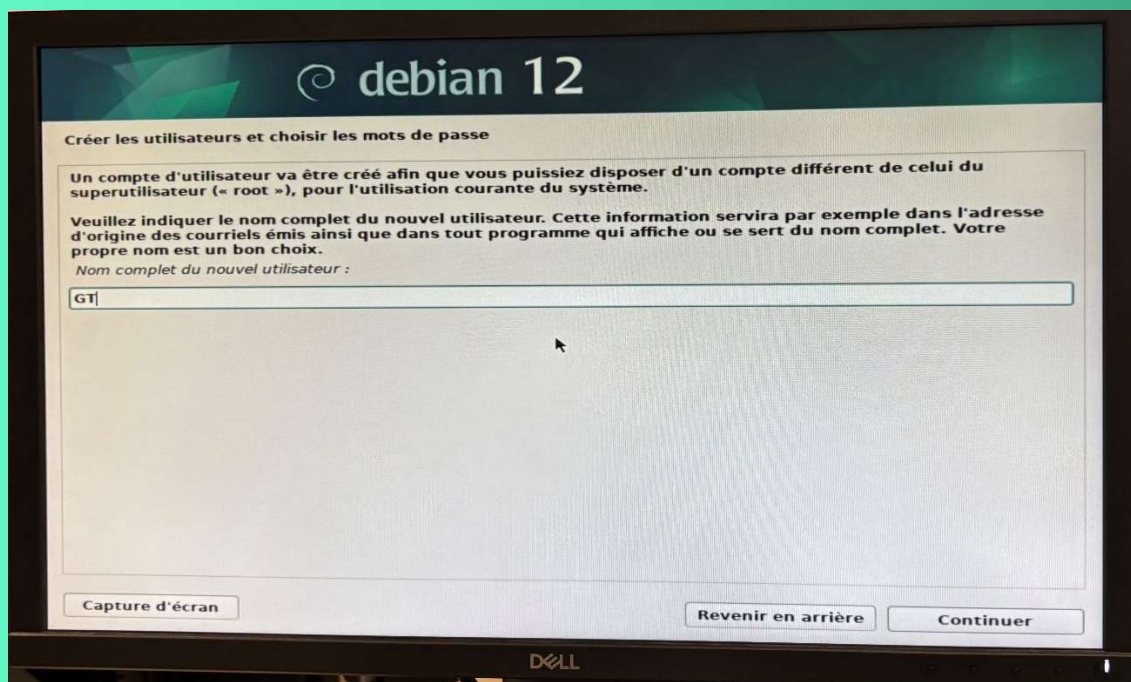
☒ Afficher le mot de passe en clair

Capture d'écran

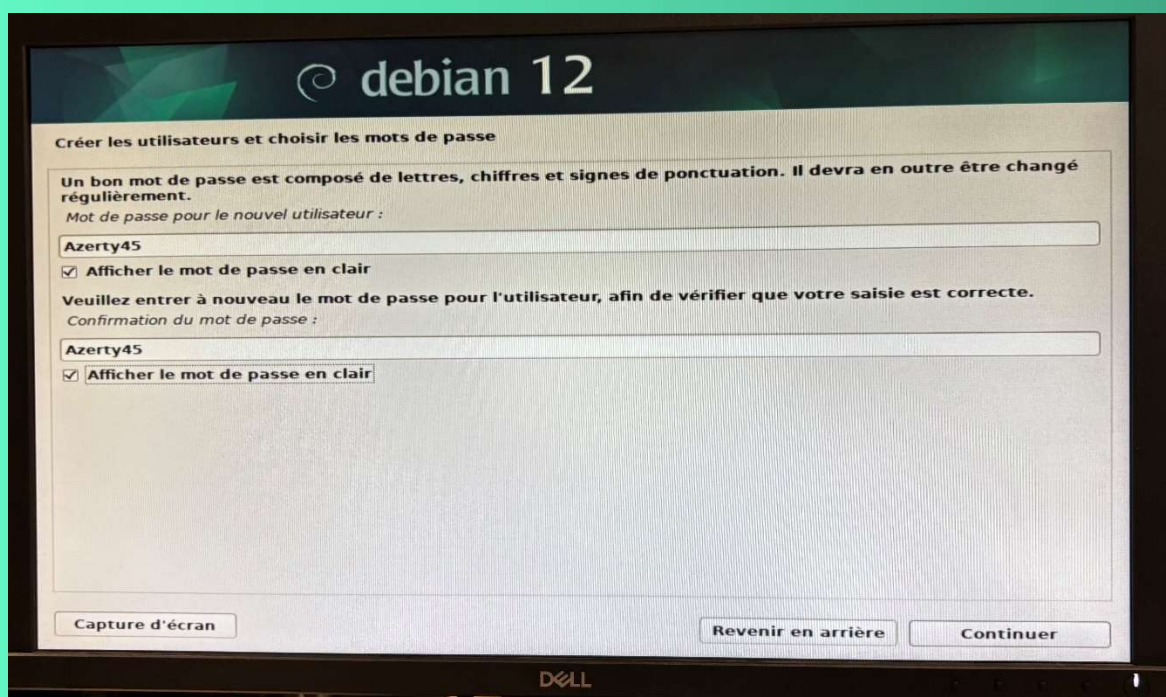
Revenir en arrière

Continuer

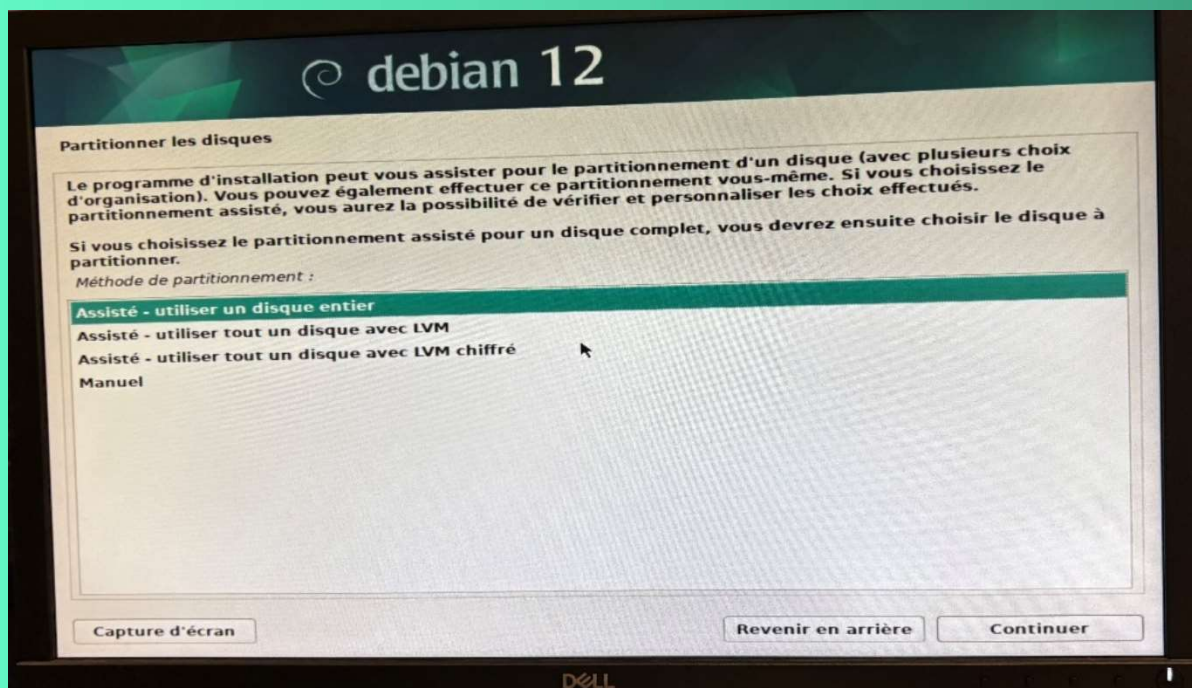
Créer le compte du nouvel utilisateur en choisissant l'identifiant du compte utilisateur



Choisir le mot de passe du compte utilisateur



Méthode de partitionnement



Choisir le disque

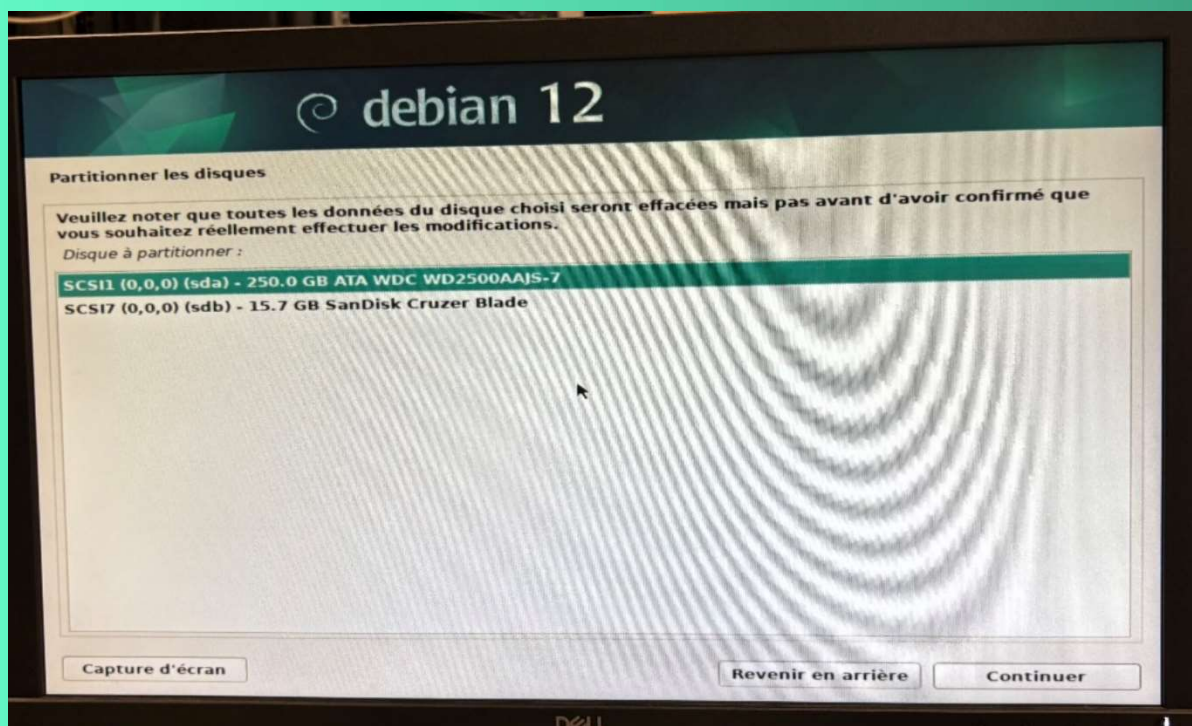
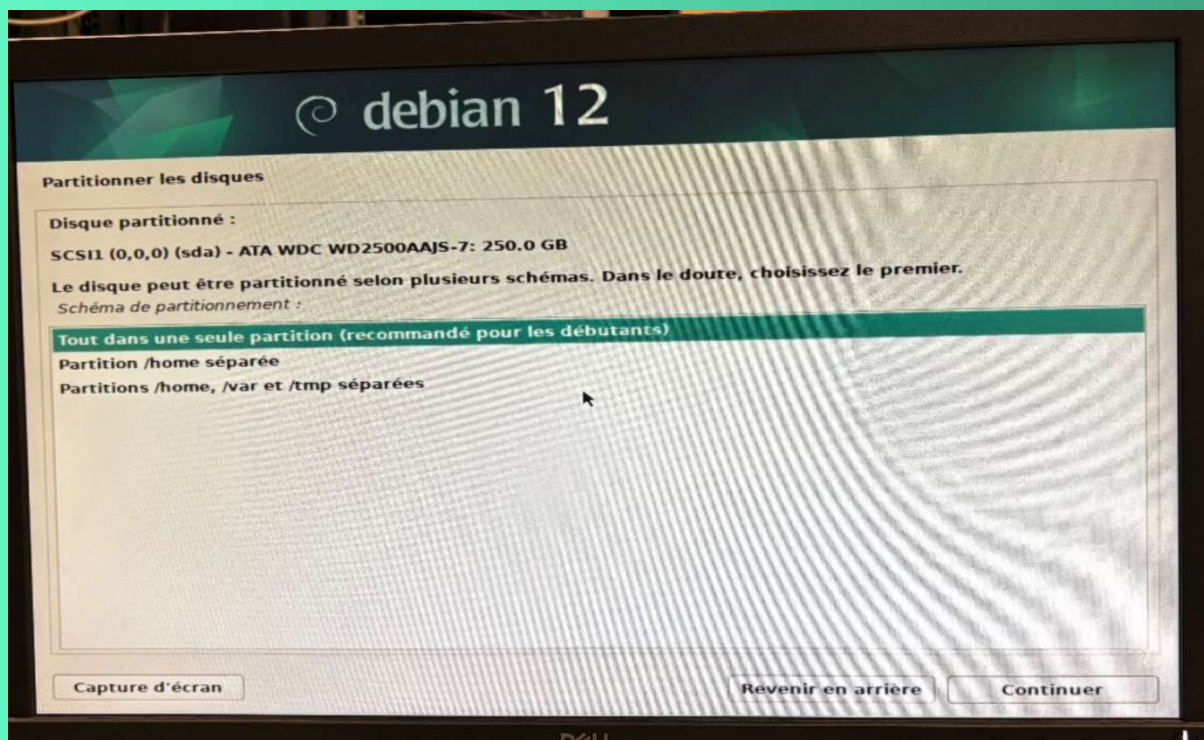
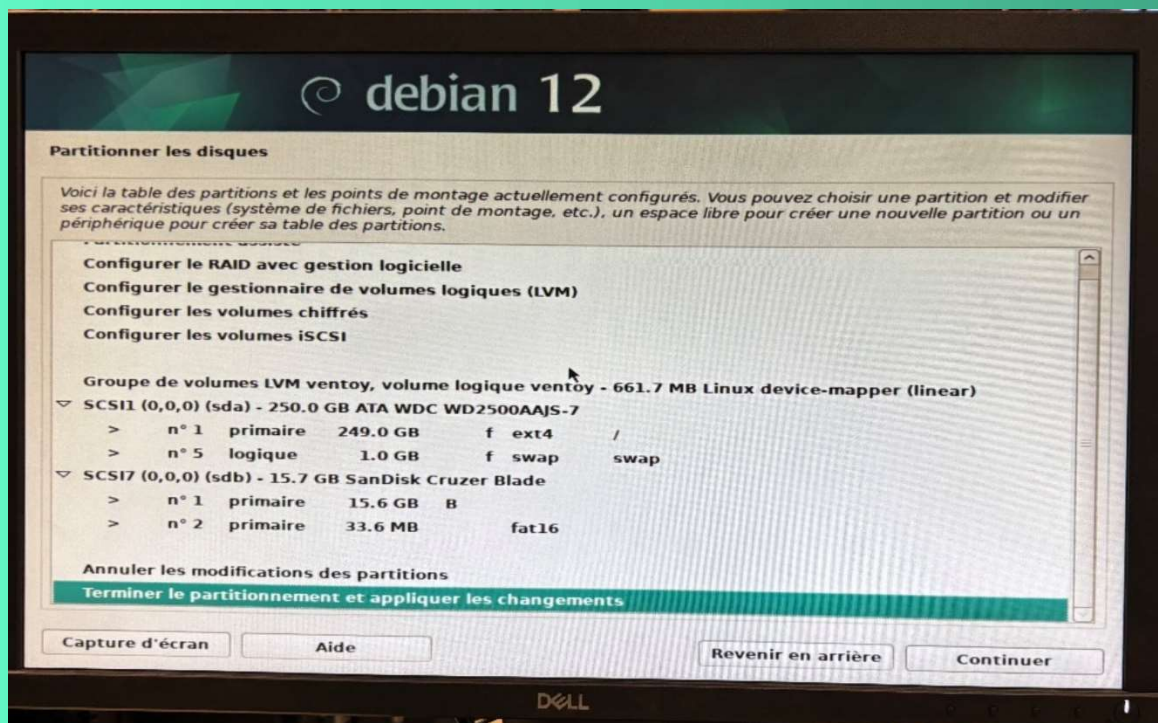


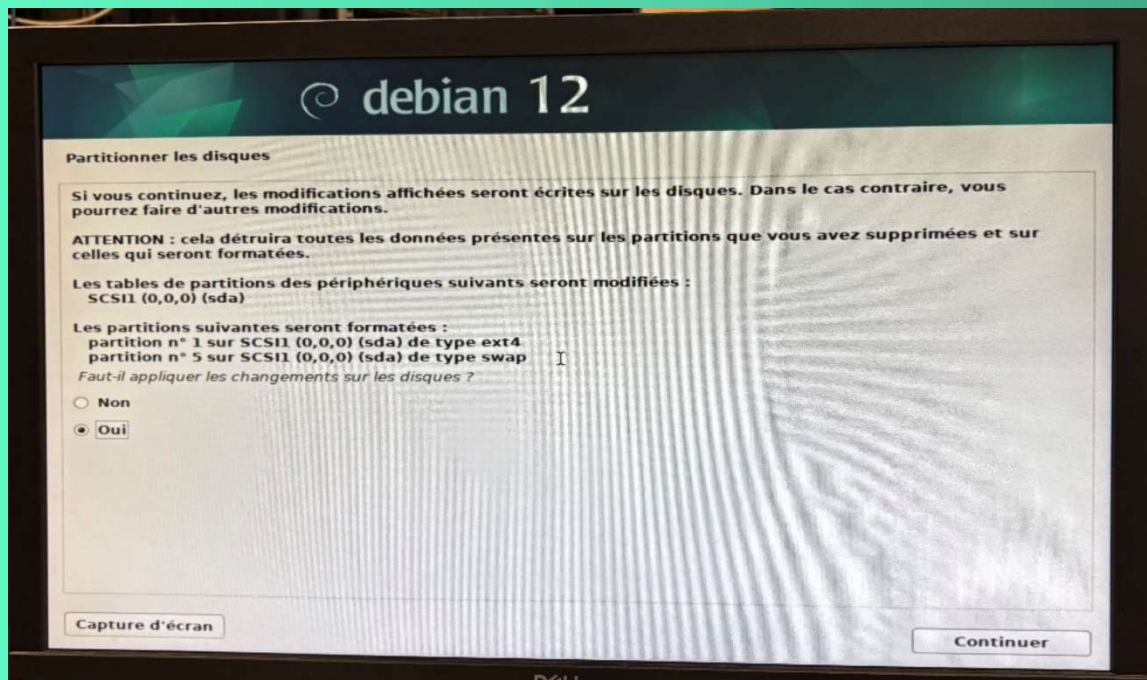
Schéma du partitionnement



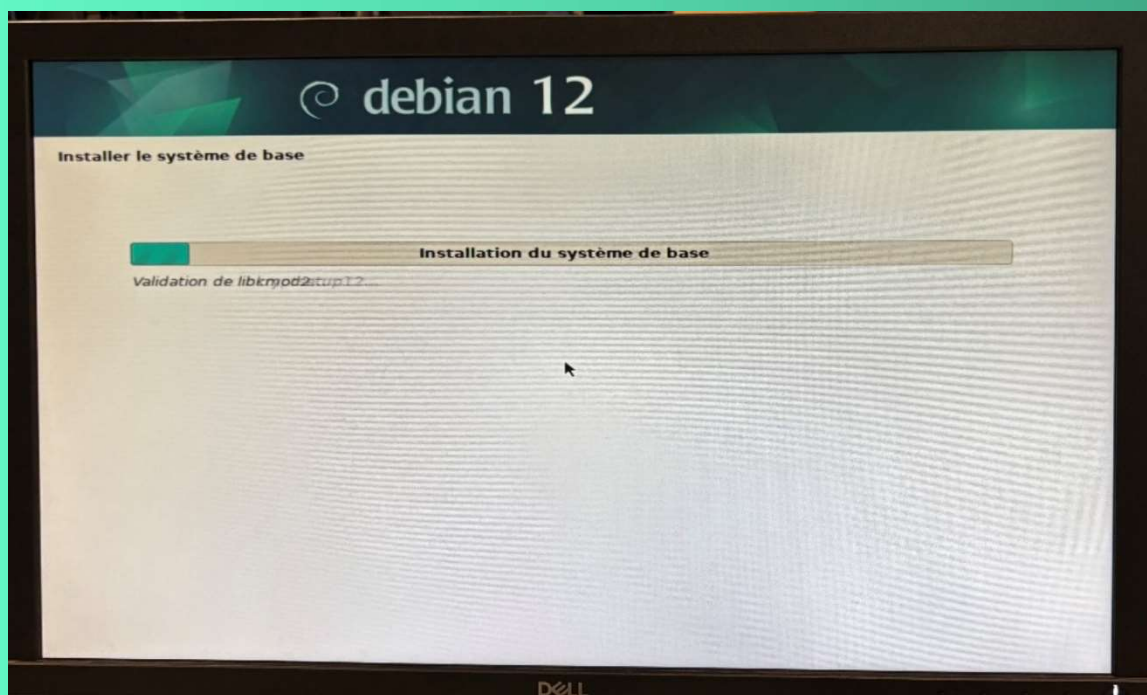
Terminer le partitionnement et appliquer les changements



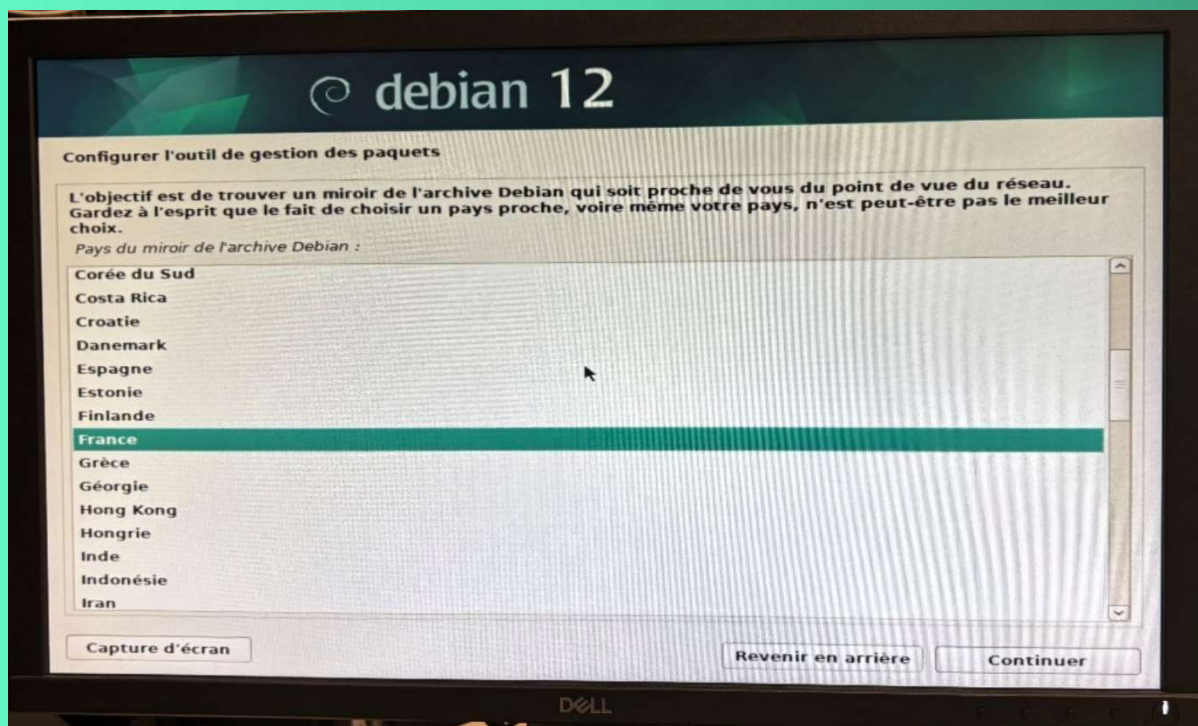
Appliquer les changements sur les disques



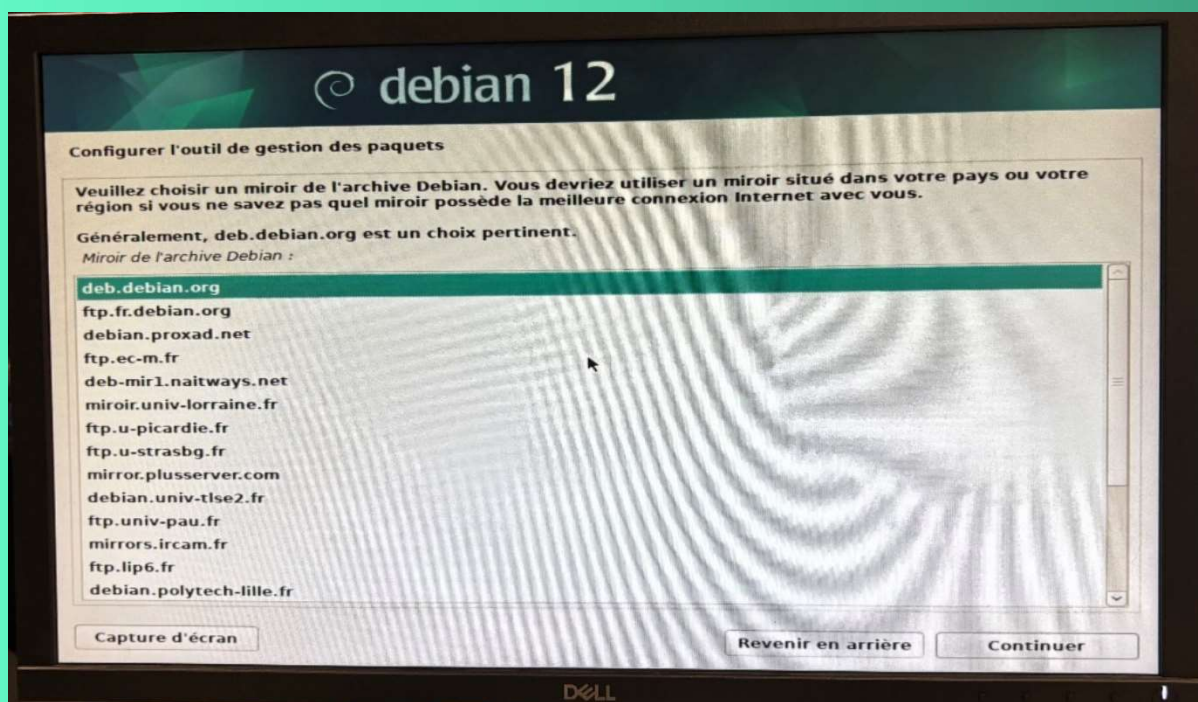
Installation du système de base



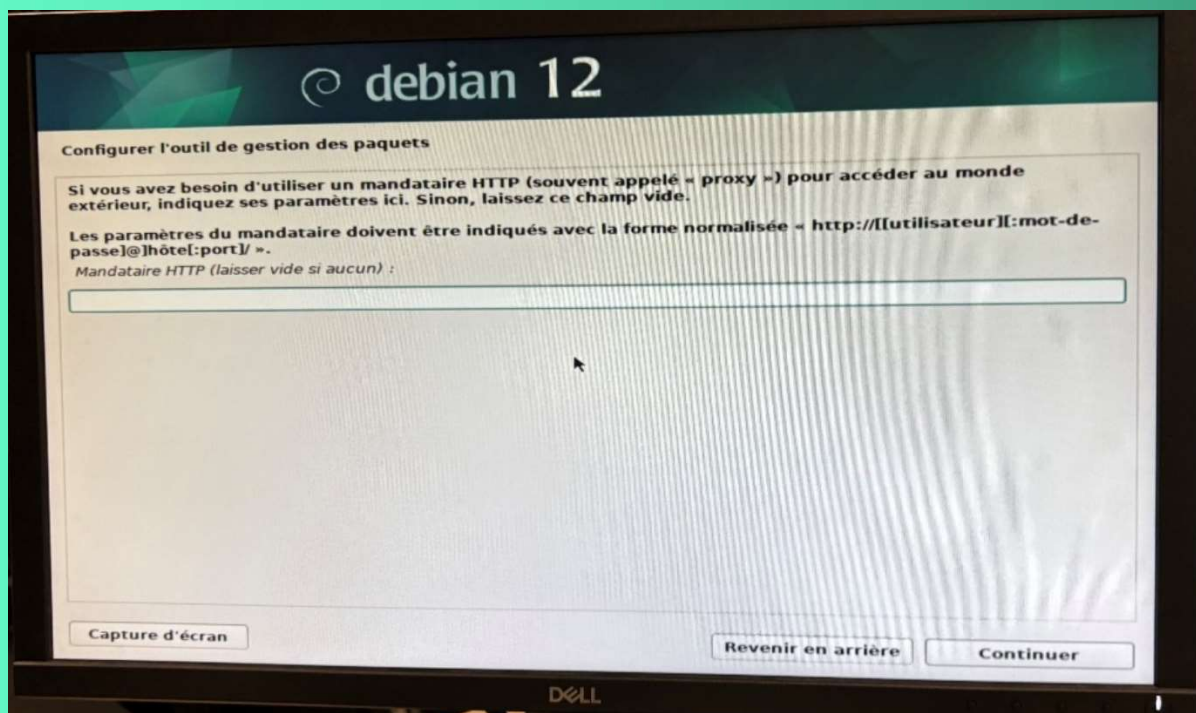
Choisir un miroir de l'archive en prenant le pays le plus proche



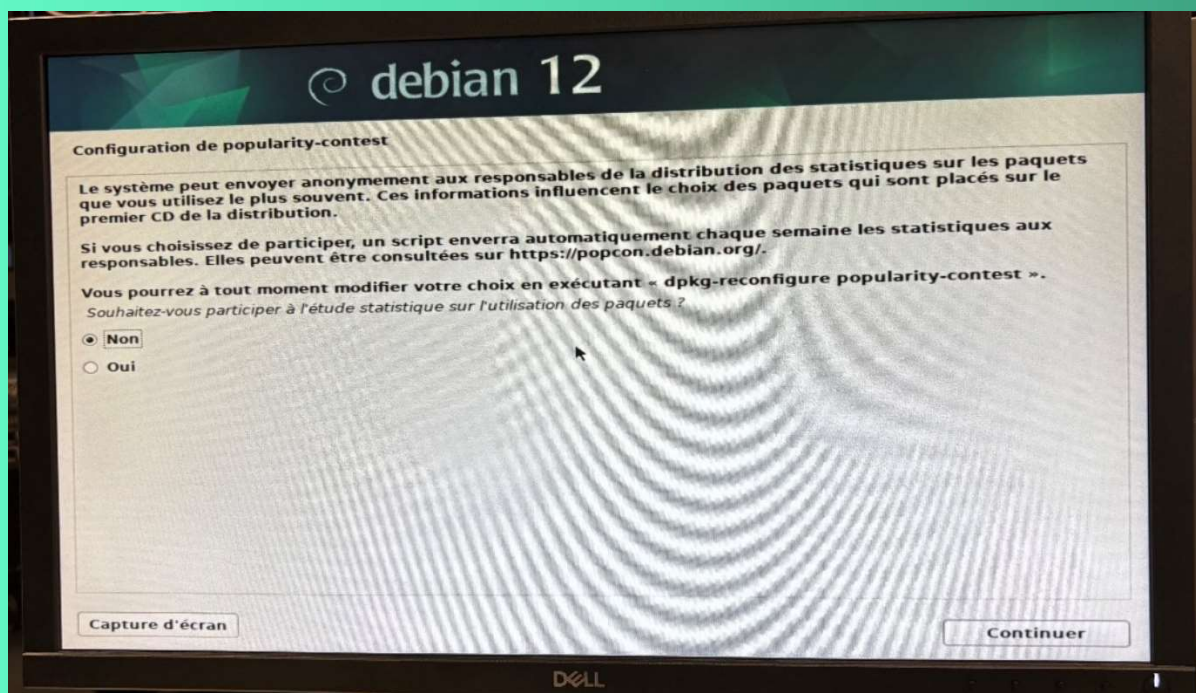
Choisir le miroir de l'archive Debian



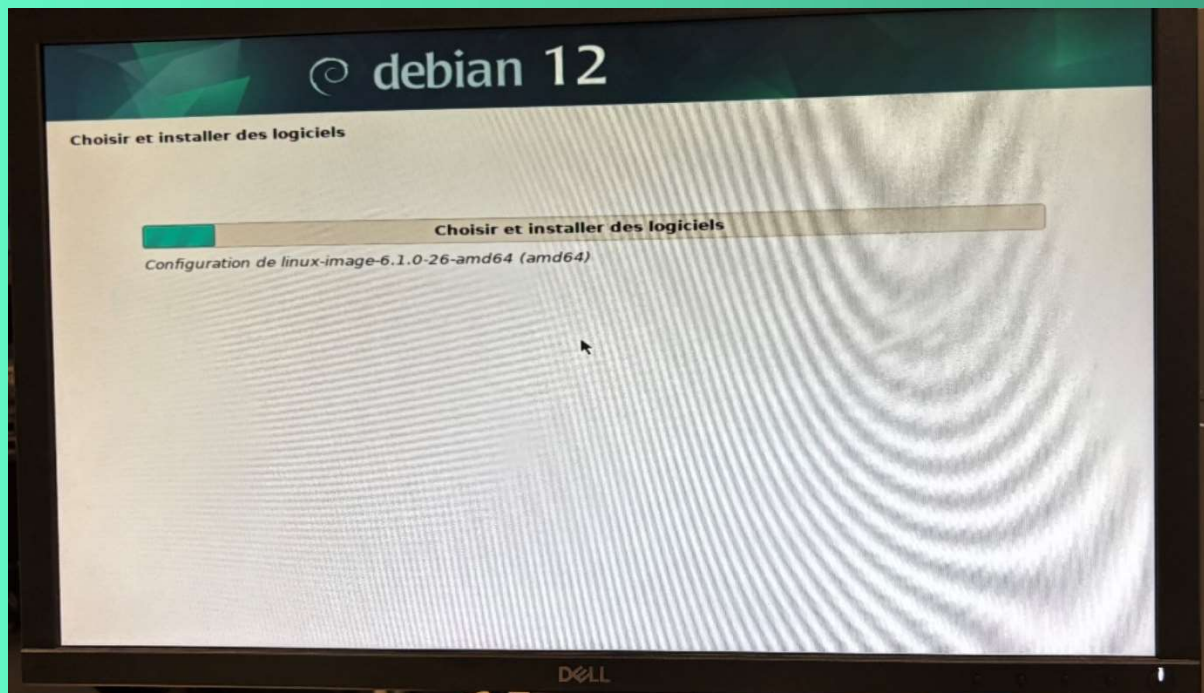
Pas de mandataire http



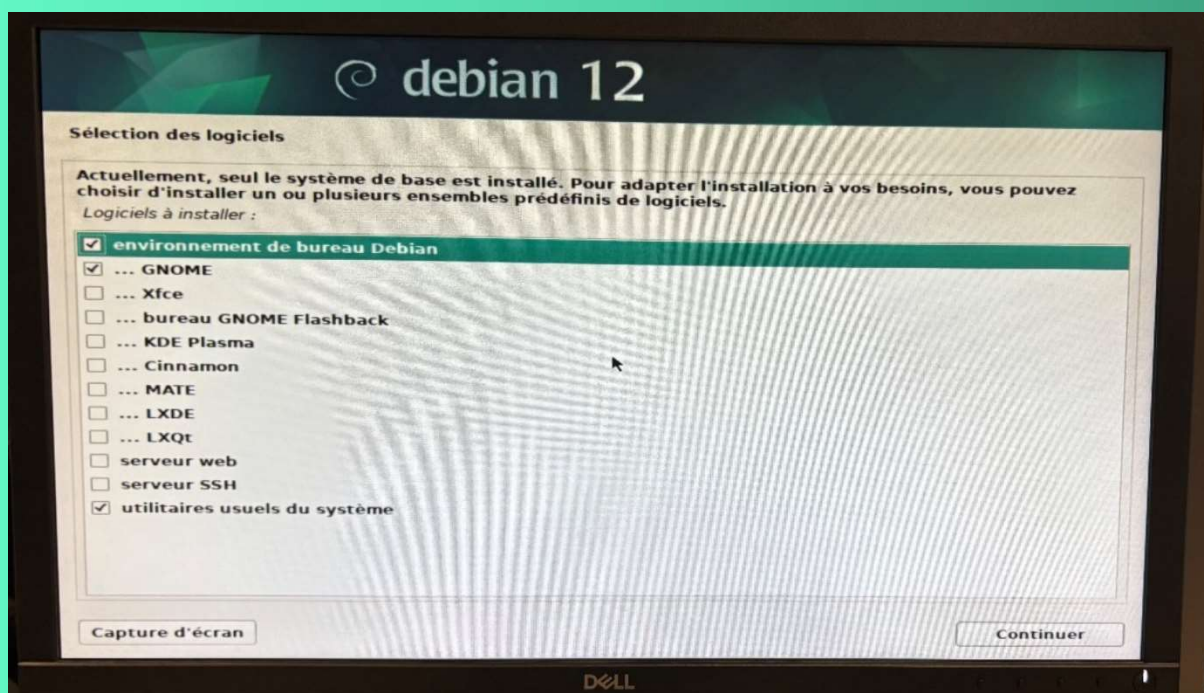
Configurer le popularity-contest



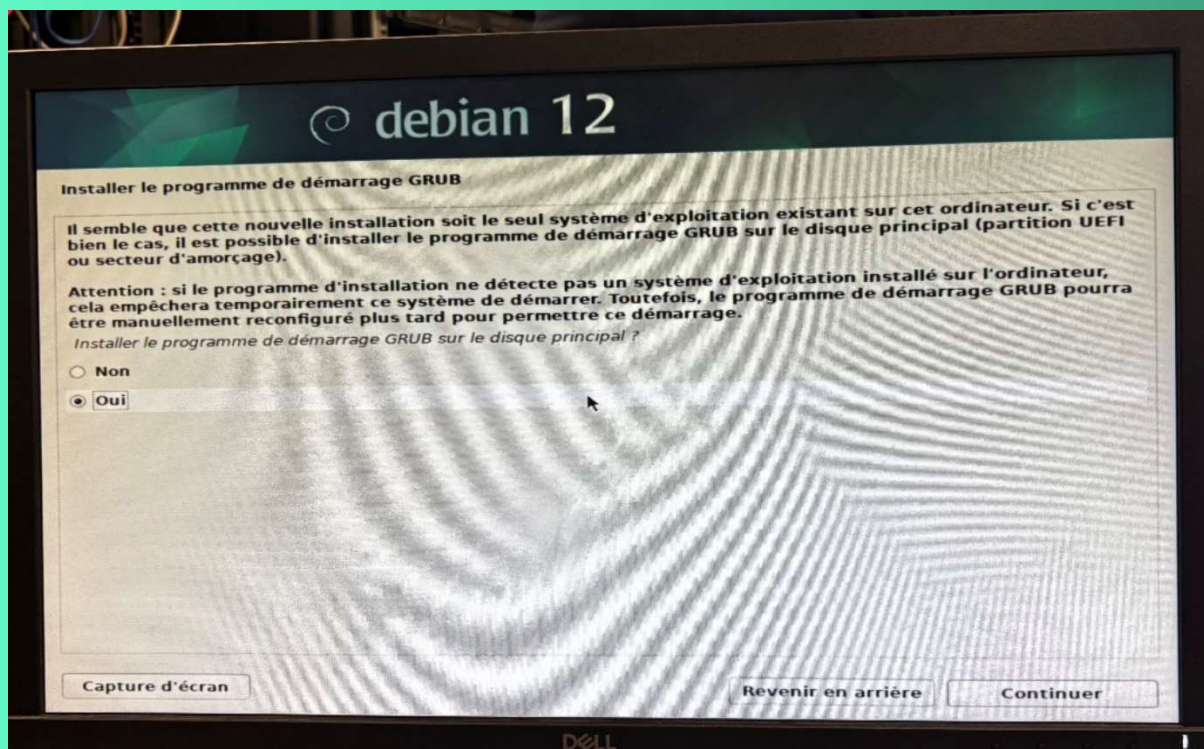
Installation des logiciels



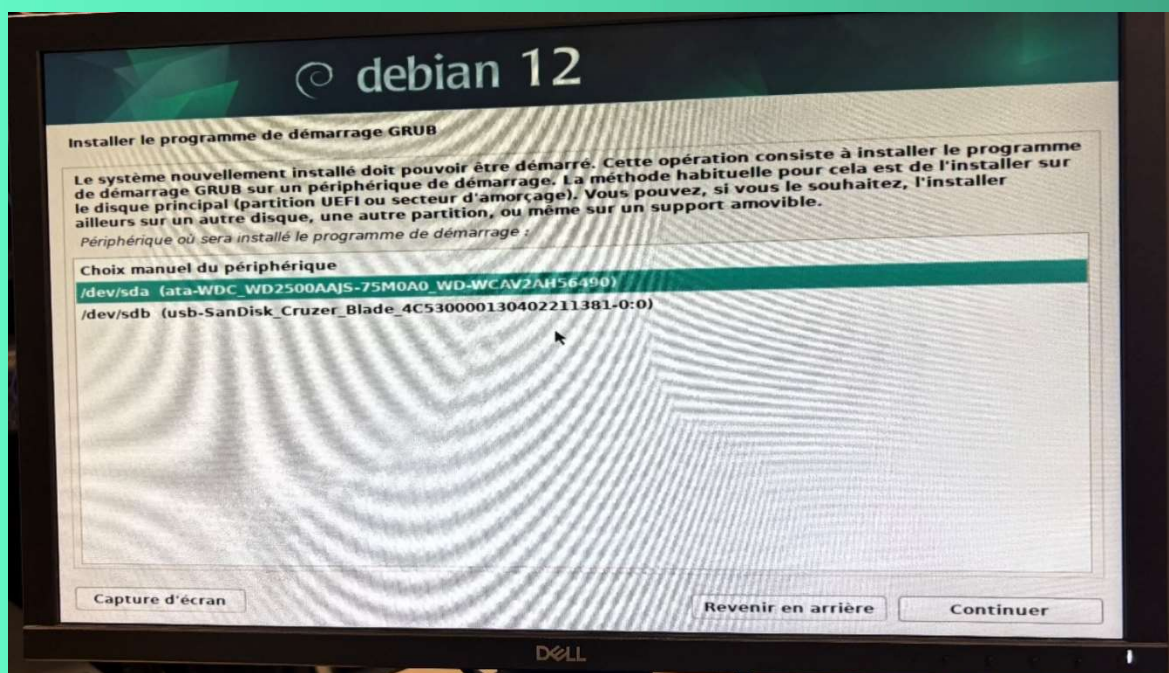
Choix de logiciels prédéfinis



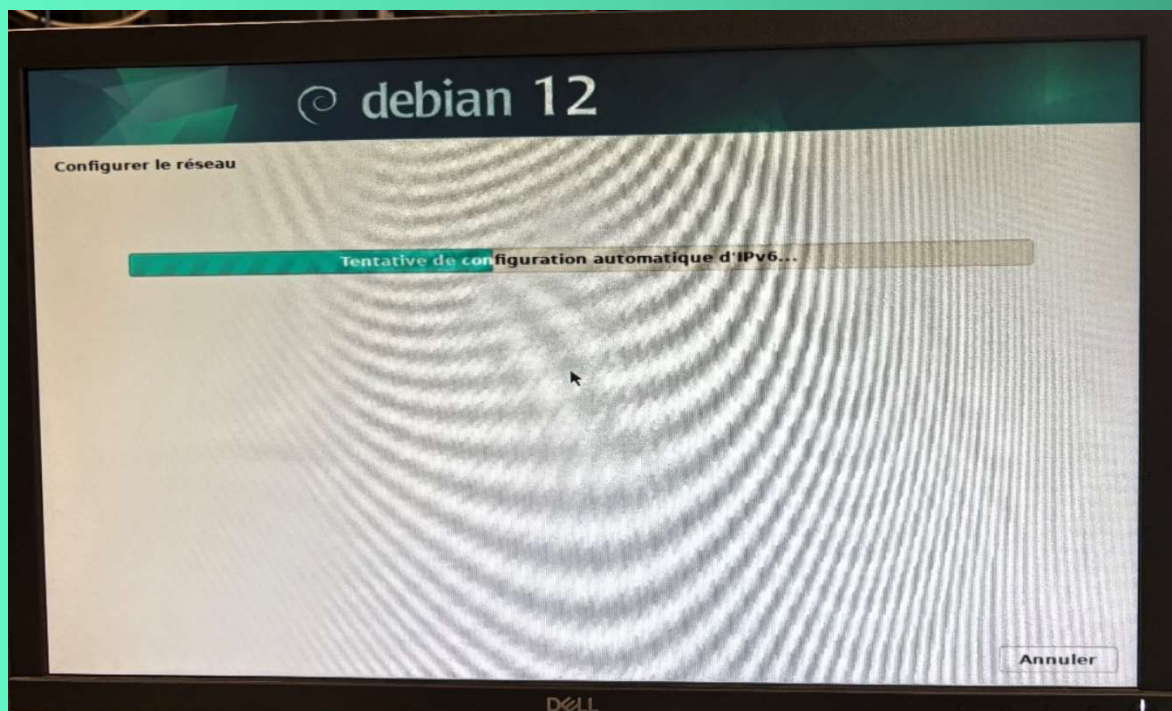
Installer le programme de démarrage GRUB



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 remplacer le 0 par un 1

Tests réalisés :

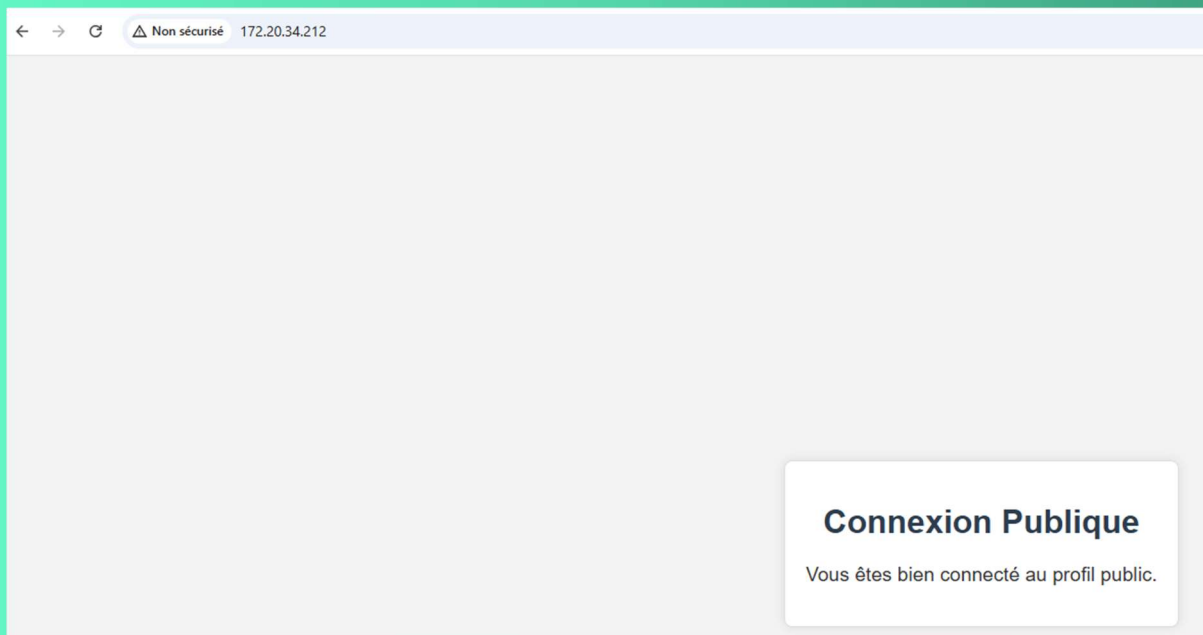
Depuis une machine cliente en 172.20.34.12 à accéder au site internet présent sur le serveur IIS en 192.168.100.10 sur le port 80

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 à 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.

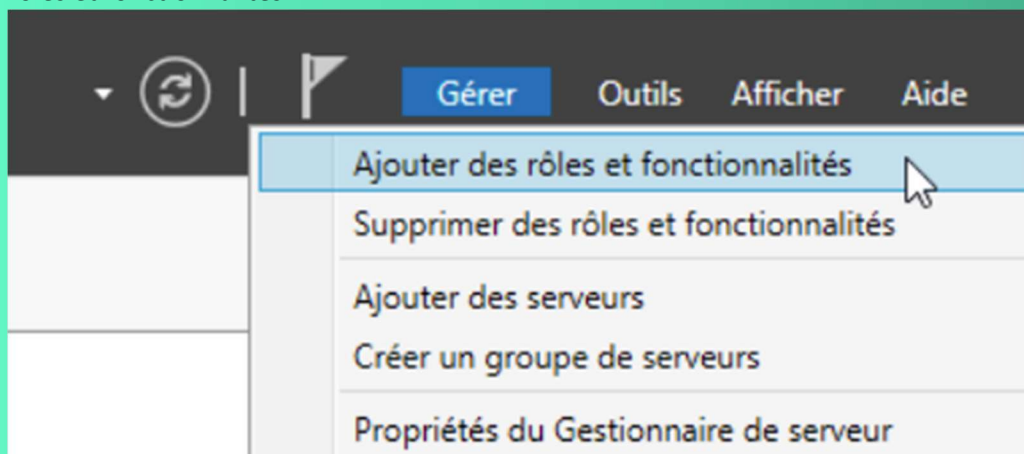
Avec la commande netfilter-persistent save, les règles iptables sont enregistrer dans le fichier :

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

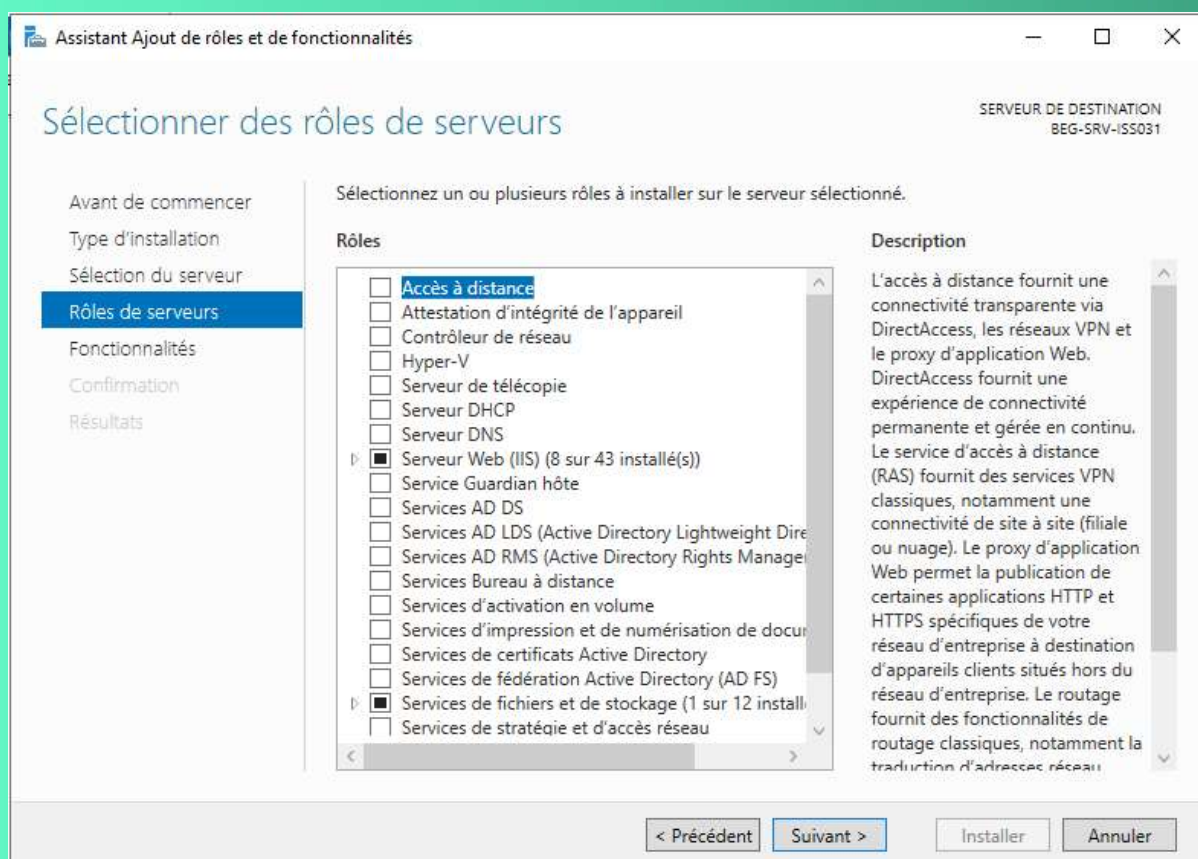
Restart le service avec la commande systemctl restart netfilter-persistent.service

CONFIGURATION D'UN SERVEUR ISS

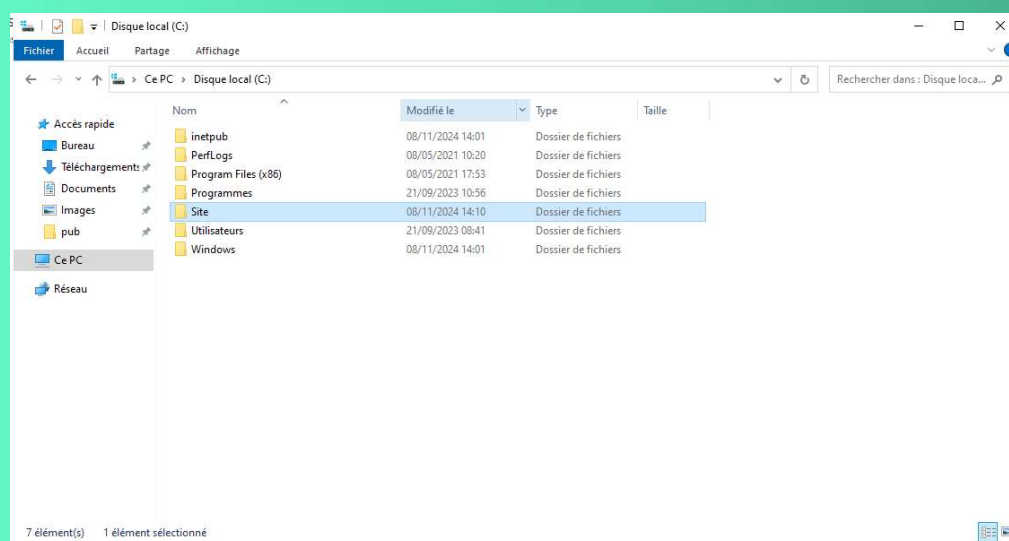
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur 'Gérer' et 'Ajouter des rôles et fonctionnalités'.



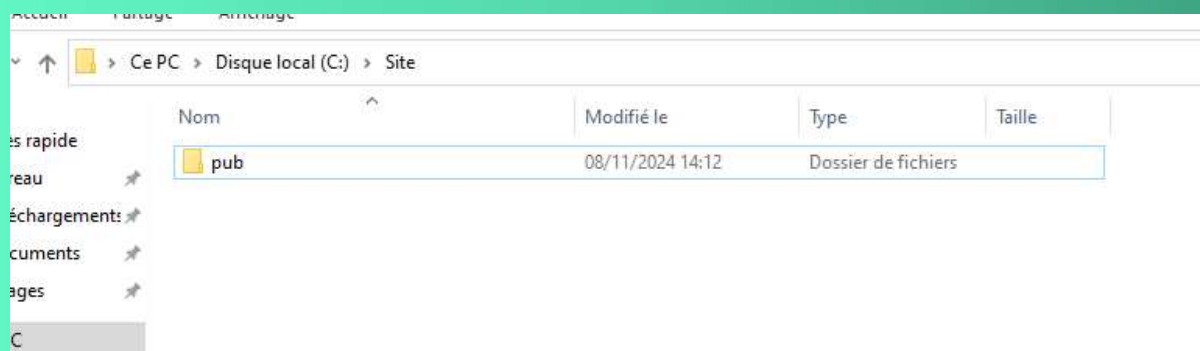
Dans l'onglet 'Rôles de serveurs', cocher 'Serveur Web (IIS)



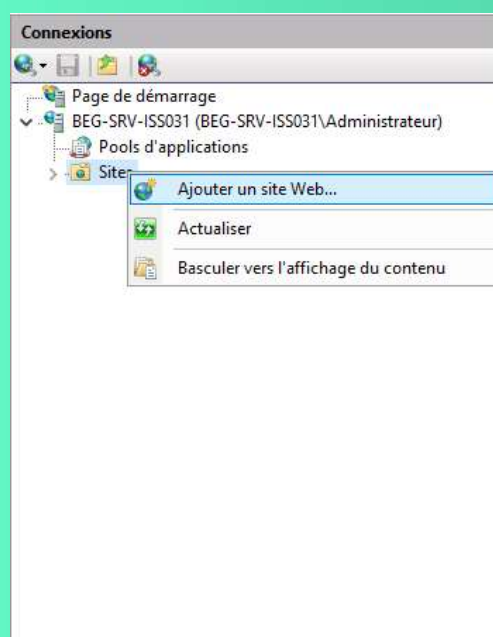
Ensuite, créer un dossier sur notre disque C



Comme sous-dossiers 'pub' signifiant que le site sera public



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



Tester la connexion à son site web

Ajouter un site Web

Nom du site : Pool d'applications :

Répertoire de contenu

Chemin d'accès physique :

Se connecter en tant que 'Administrateur'

Liaison

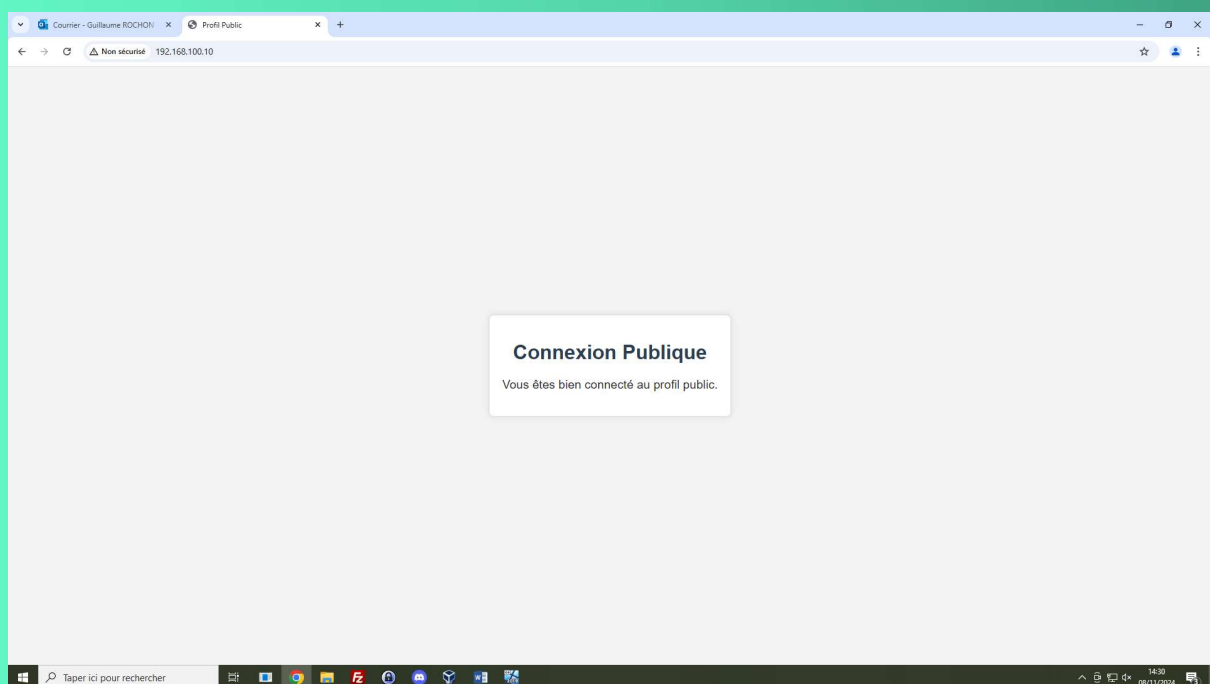
Type : Adresse IP : Port :

Nom de l'hôte :

Exemple : www.contoso.com ou marketing.contoso.com

☒ Démarrez le site Web immédiatement

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 ».

The screenshot shows the 'Assistant Ajout de rôles et de fonctionnalités' window. The title bar reads 'Assistant Ajout de rôles et de fonctionnalités'. The main heading is 'Avant de commencer'. In the top right corner, it says 'SERVEUR DE DESTINATION' and 'BEG-SRV-DFS032.BEG-FR-03.PRIV'. On the left, there is a navigation pane with the following items: 'Avant de commencer' (highlighted), 'Type d'installation', 'Sélection du serveur', 'Rôles de serveurs', 'Fonctionnalités', 'Confirmation', and 'Confirmer les sélections d'installation'. The main content area contains the following text: 'Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.' Below this, it says 'Pour supprimer des rôles, des services de rôle ou des fonctionnalités : Démarrer l'Assistant de Suppression de rôles et de fonctionnalités'. Then, 'Avant de continuer, vérifiez que les travaux suivants ont été effectués :'. A list follows: '• Le compte d'administrateur possède un mot de passe fort', '• Les paramètres réseau, comme les adresses IP statiques, sont configurés', and '• Les dernières mises à jour de sécurité de Windows Update sont installées'. Below the list, it says 'Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.' and 'Cliquez sur Suivant pour continuer.' At the bottom left, there is a checkbox labeled 'Ignorer cette page par défaut'. At the bottom right, there are four buttons: '< Précédent', 'Suivant >' (highlighted), 'Installer', and 'Annuler'.

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

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le type d'installation

SERVEUR DE DESTINATION
BEG-SRV-DFS032.BEG-FR-03.PRIV

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

☒ **Installation basée sur un rôle ou une fonctionnalité**
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

☐ **Installation des services Bureau à distance**
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

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

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
BEG-SRV-DFS032.BEG-FR-03.PRIV

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

☒ Sélectionner un serveur du pool de serveurs
☐ Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

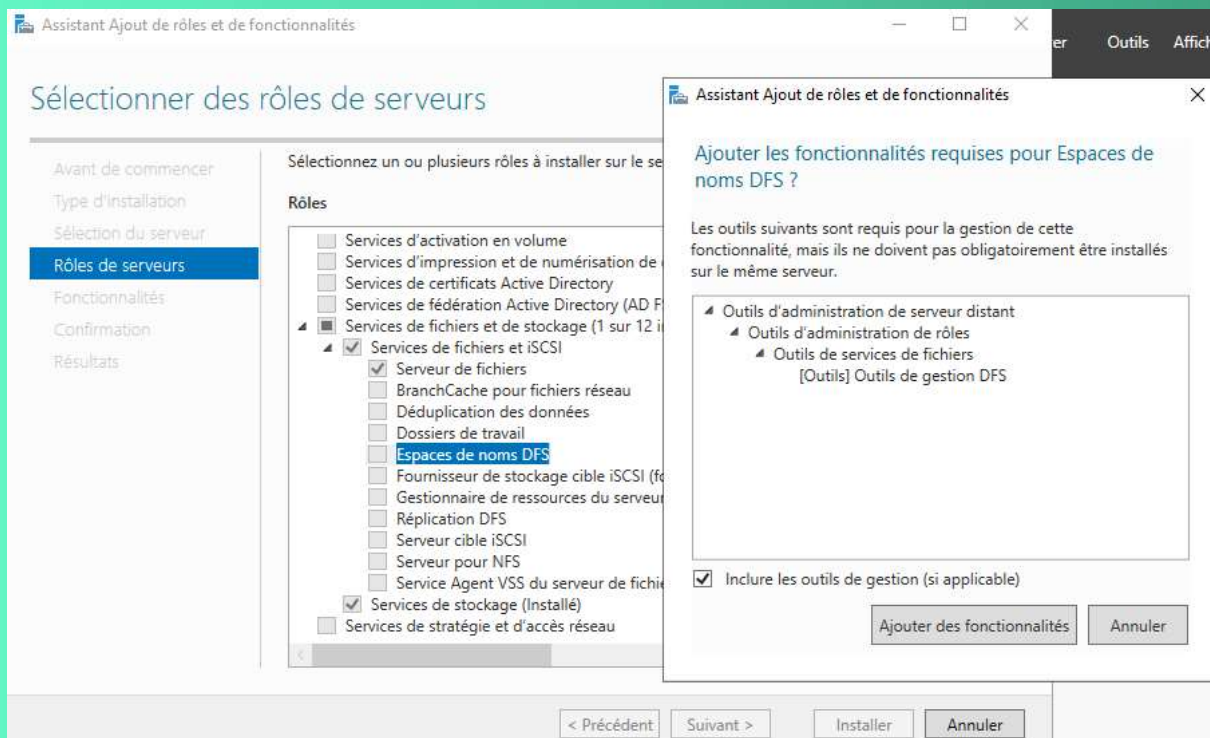
Nom	Adresse IP	Système d'exploitation
BEG-SRV-DFS032.BEG-F...	172.20.3.9	Microsoft Windows Server 2022 Datacenter

1 ordinateur(s) trouvé(s)

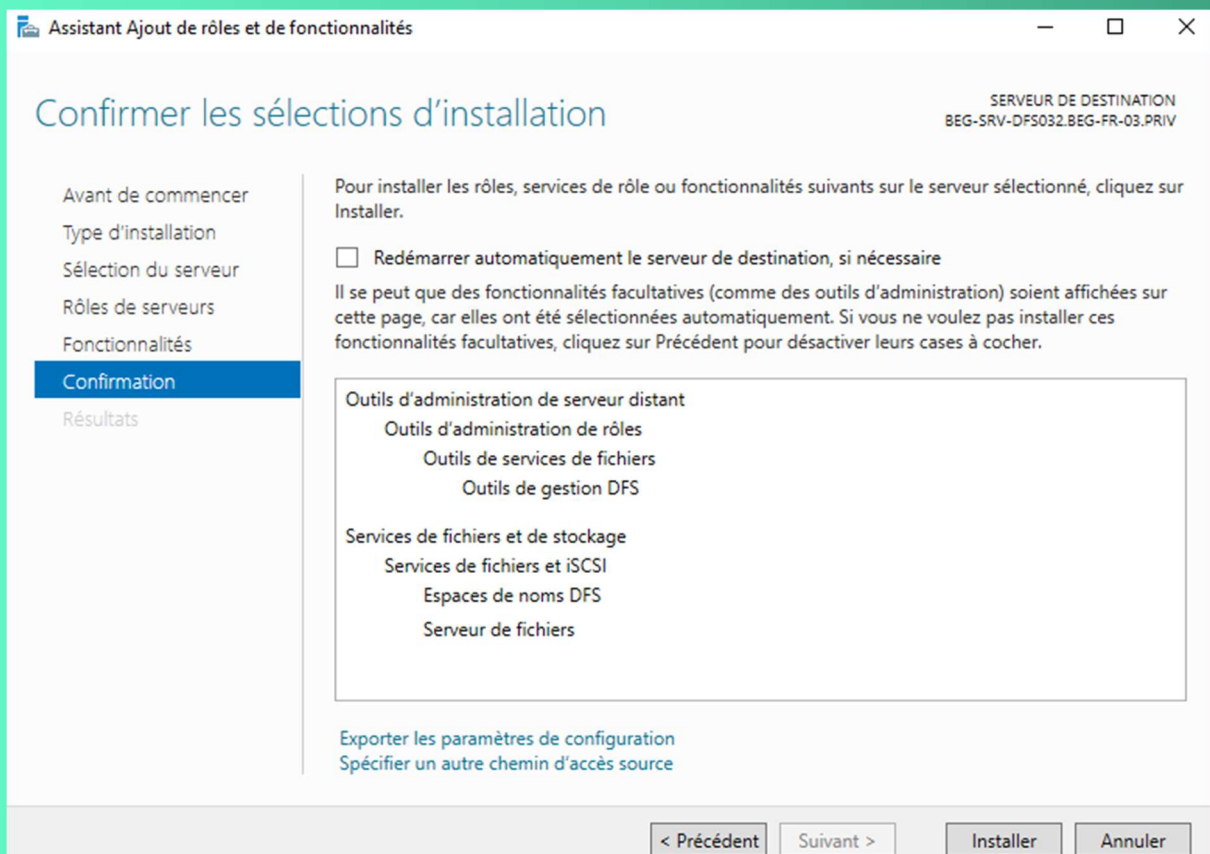
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

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.

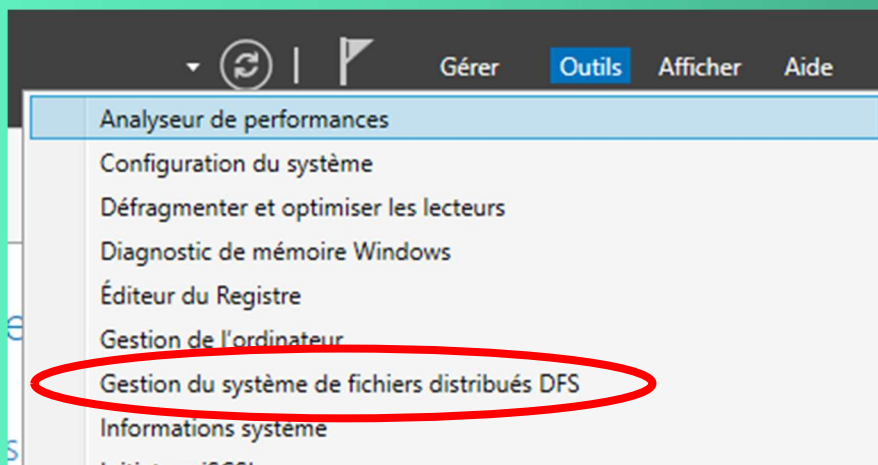


Création d'une racine DFS autonome :

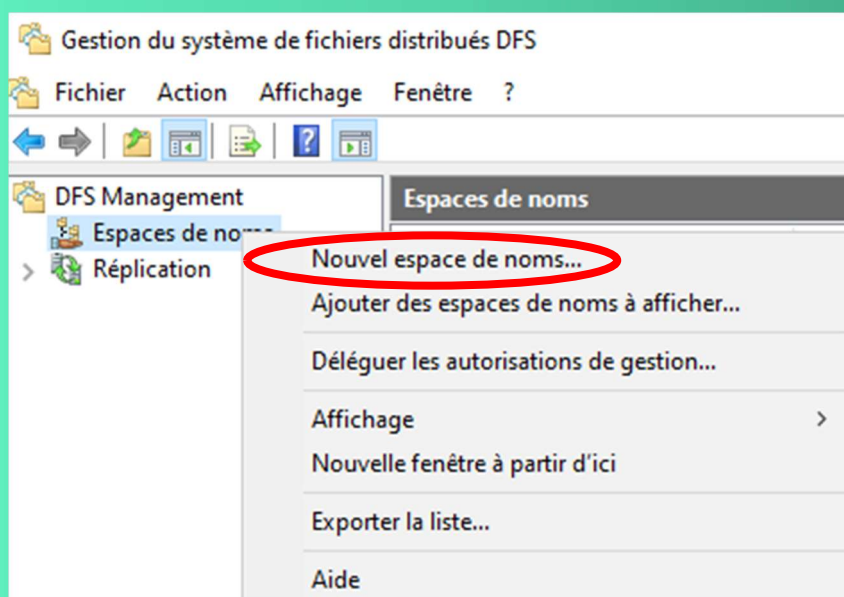
L'infrastructure décrite en début de document nécessite l'utilisation d'une racine de noms de domaine, mais, pour vous montrer la mise en place d'une racine autonome voici la procédure à suivre.

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... ».



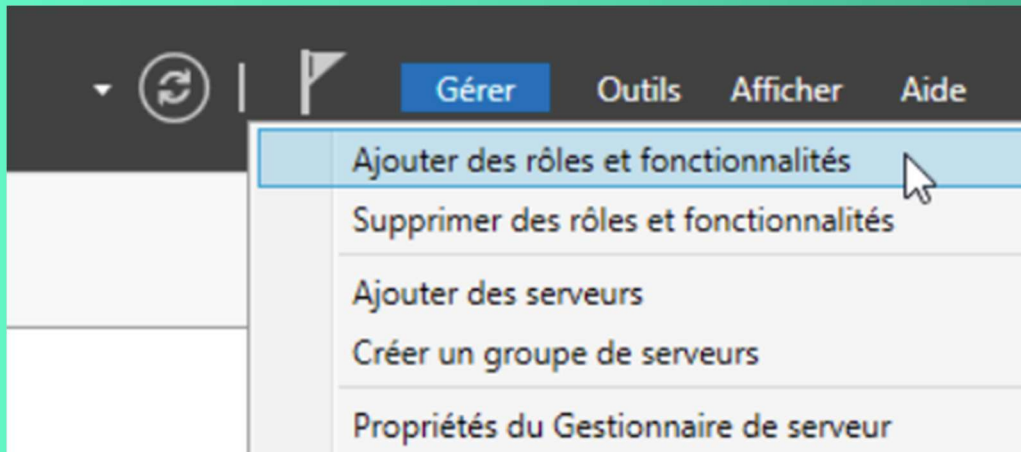
Indiquez le serveur d'espaces de noms qui hébergera donc les espaces de noms, ce serveur n'a pas vocation à héberger lui-même les données. En effet, il sert uniquement de redirecteur entre vos dossiers DFS virtuels et les dossiers partagés physiques qui contiennent les données, des données qui sont stockées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

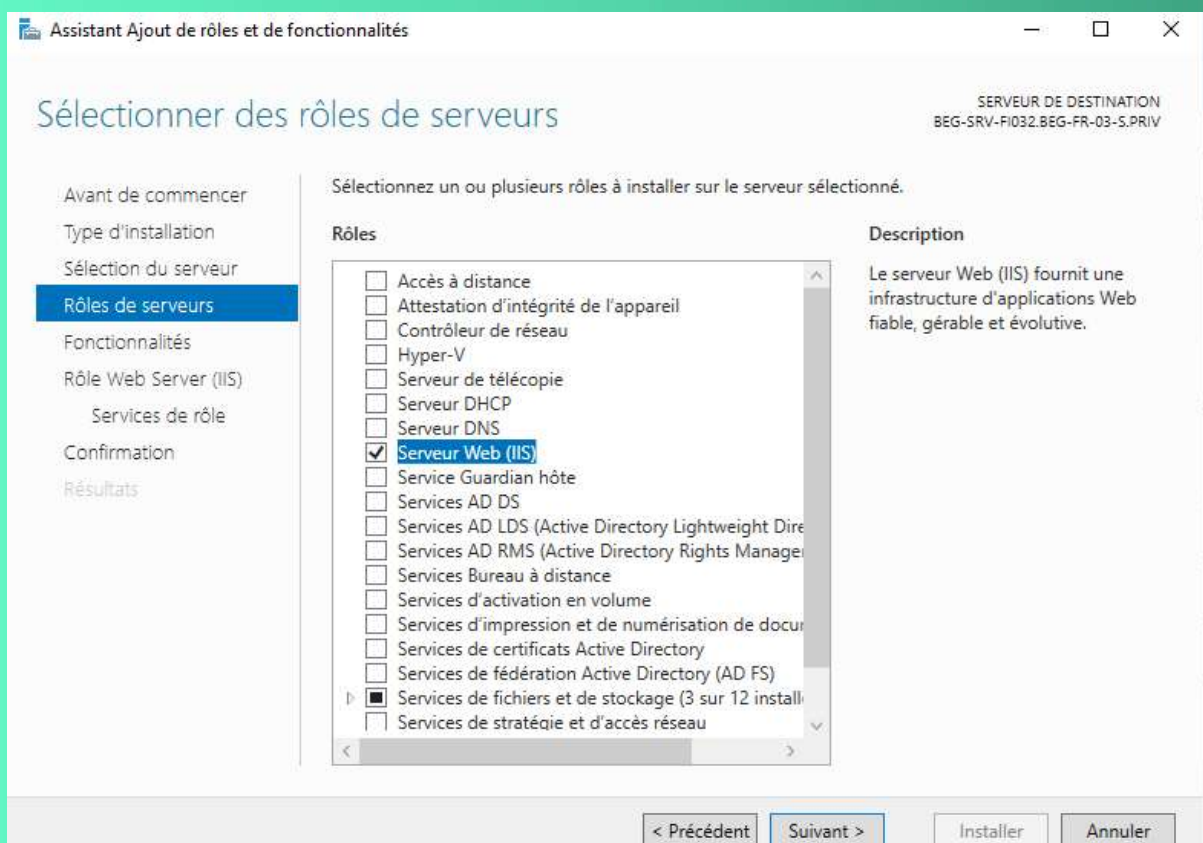
Cliquez sur « Parcourir... » pour rechercher le serveur qui hébergera l'espace de noms en cours de création. Cliquez sur « Suivant » une fois la sélection effectuée.

INSTALLER LE SERVICE IIS ET ROLE FTP

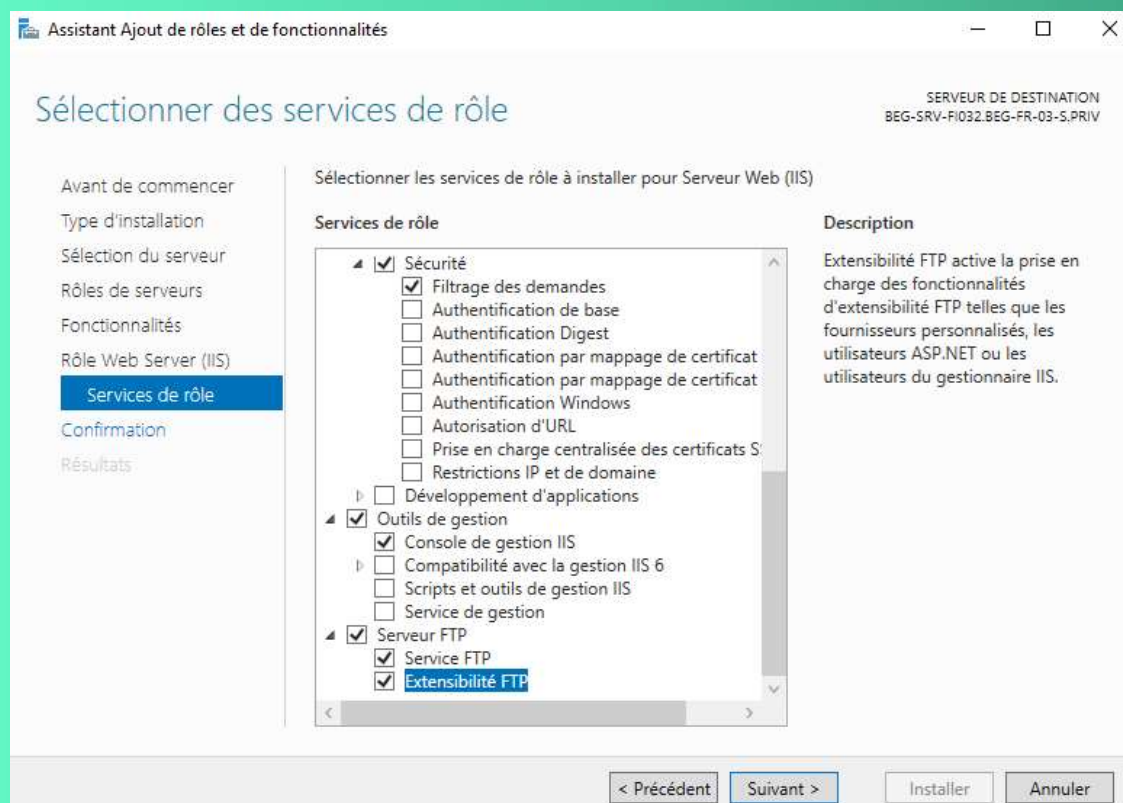
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur 'Gérer' et 'Ajouter des rôles et fonctionnalités'.



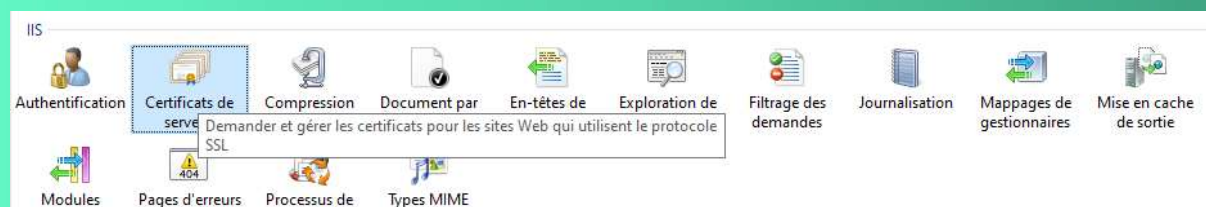
Dans l'onglet 'Rôles de serveurs', cocher 'Serveur Web (IIS)



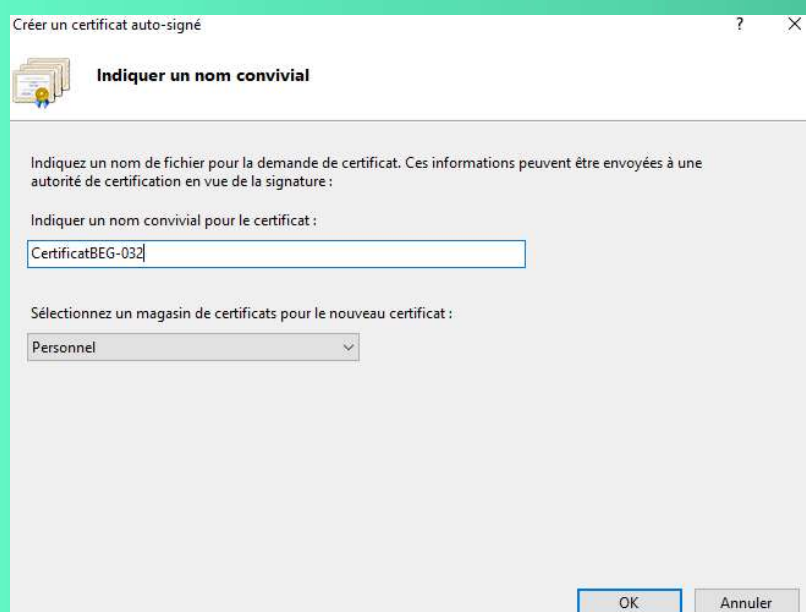
Dans l'onglet 'Services de rôle', cocher 'Service FTP' et 'Extensibilité FTP'



Créer le certificat



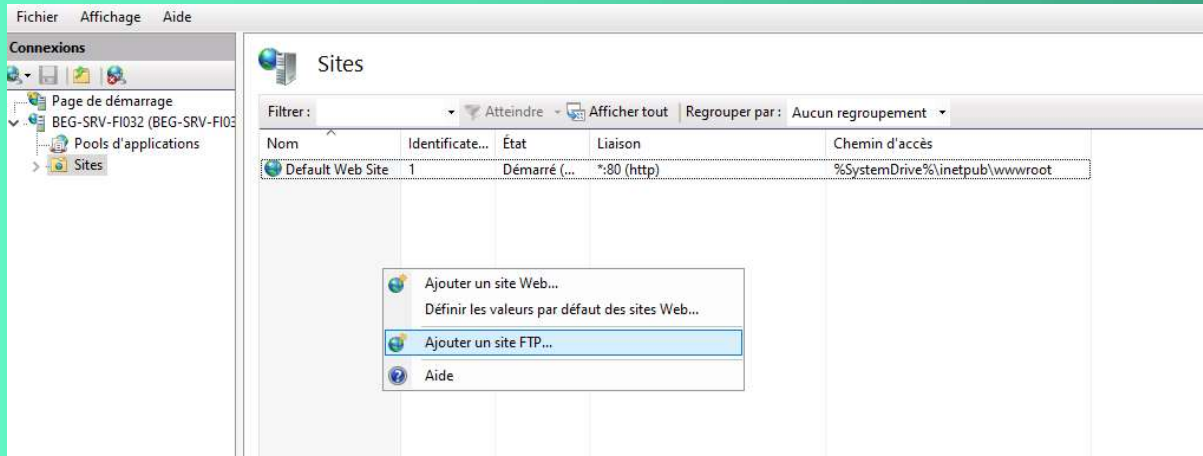
Créer un certificat autosigné



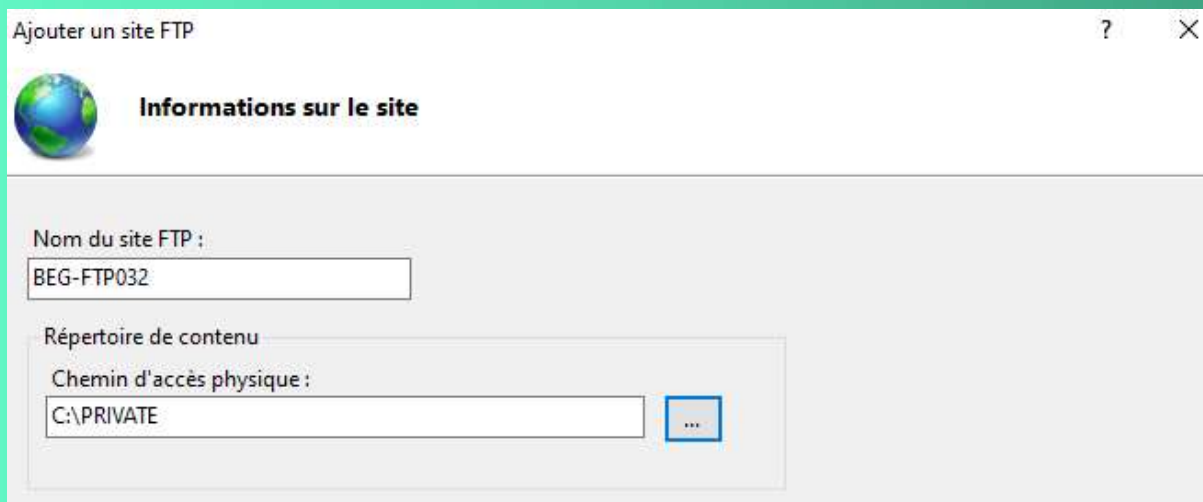
Configurer un site FTP :

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

Ajouter un site FTP ? X

 **Liaison et paramètres SSL**

Liaison

Adresse IP : 172.20.3.4 Port : 21

☐ Activer les noms des hôtes virtuels :
Hôte virtuel (exemple : ftp.contoso.com) :

☒ Démarrer automatiquement le site FTP

SSL

☐ Pas de SSL
☐ Autoriser SSL
☒ Exiger SSL

Certificat SSL : CertificatBEG-032 Sélectionner... Afficher...

Précédent Suivant Terminer Annuler

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

Ajouter un site FTP ? X

 **Informations sur les autorisations et l'authentification**

Authentification

☐ Anonyme
☒ De base

Autorisation

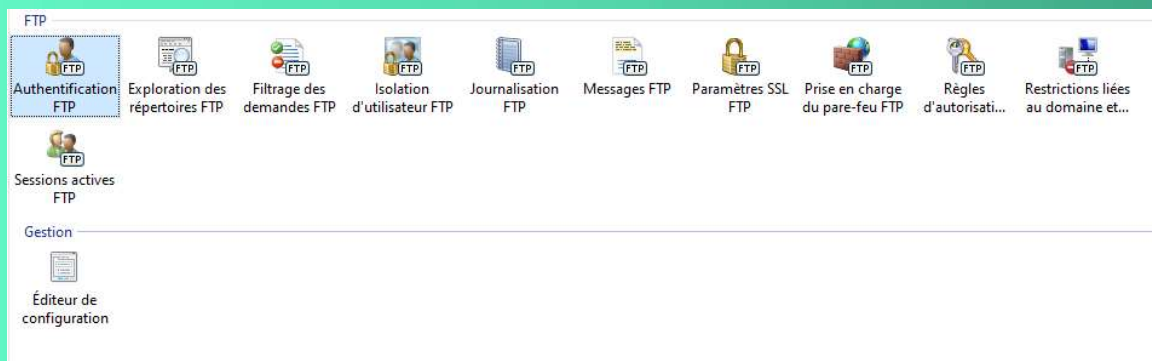
Autoriser l'accès à :
Rôles ou groupes d'utilisateurs définis
BEG-FR

Autorisations

☒ Lecture
☒ Écriture

Précédent Suivant Terminer Annuler

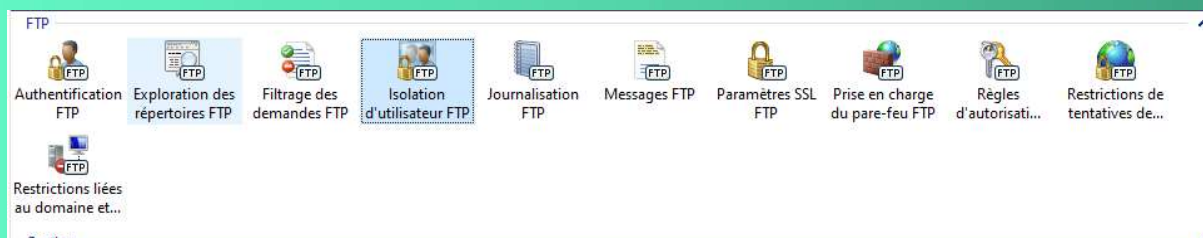
Configurer l'isolation des utilisateurs :



Activé l'authentification de base

Regrouper par : Aucun regroupement ▾		
Mode	État	Type
Authentification anonyme	Désactivé	Intégré
Authentification de base	Activé	Intégré

Sélectionner Isolation d'utilisateur FTP



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

Isolation d'utilisateur FTP

L'isolation d'utilisateur FTP empêche les utilisateurs d'accéder au répertoire FTP de base d'un autre utilisateur sur ce site FTP.

Ne pas isoler les utilisateurs. Les utilisateurs démarrent dans :

- ☐ Répertoire racine FTP
- ☐ Répertoire des noms d'utilisateurs

Isoler les utilisateurs. Limiter les utilisateurs au répertoire suivant :

- ☐ Répertoire des noms d'utilisateurs (désactiver les répertoires)
- ☐ Répertoire physique des noms d'utilisateurs (activer les répertoires)
- ☒ Répertoire de base FTP configuré dans Active Directory
-
- ☐ Personnalisé

Définir les informations d'identification

Nom d'utilisateur :

Administrateur

Mot de passe :

.....

Confirmer le mot de passe :

.....