

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.

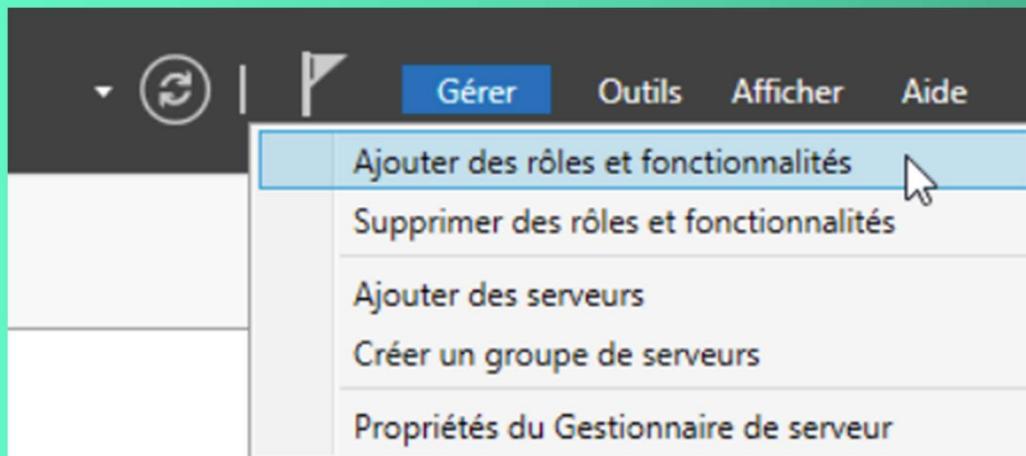
Le projet mené chez BEG couvre plusieurs aspects stratégiques, tels que la configuration d'un Active Directory pour la gestion centralisée des comptes, la mise en place de profils itinérants, la gestion des partages réseau sécurisés, et l'implémentation de services critiques comme les serveurs FTP, pare-feu,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

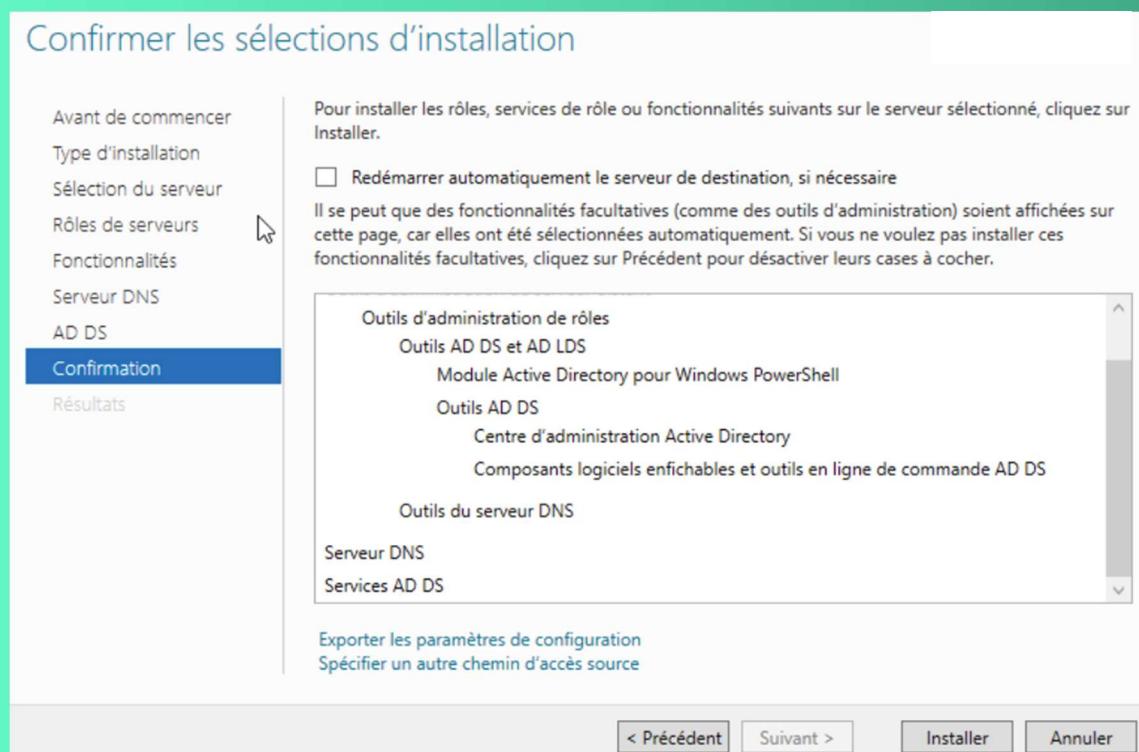
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur ‘Gérer’ et ‘Ajouter des rôles et fonctionnalités’.



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

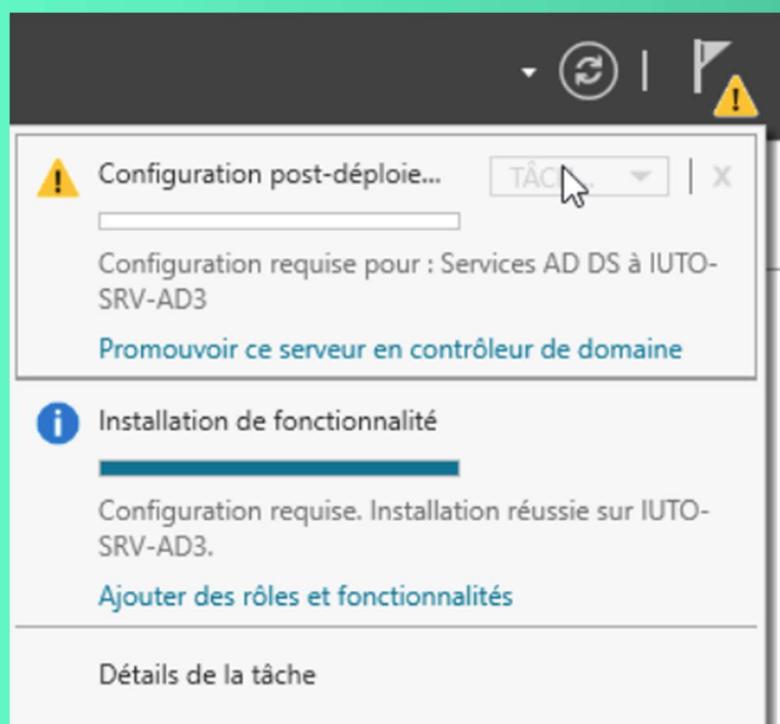
The screenshot shows the 'Selectionner des rôles de serveurs' (Select Server Roles) wizard. On the left, a navigation pane lists steps: 'Avant de commencer', 'Type d'installation', 'Sélection du serveur', 'Rôles de serveurs' (which is selected and highlighted in blue), 'Fonctionnalités', 'Serveur DNS', 'AD DS', 'Confirmation', and 'Résultats'. The main pane is titled 'Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.' It contains two columns: 'Rôles' and 'Description'. The 'Rôles' column lists several checkboxes, some of which are checked: 'Accès à distance', 'Attestation d'intégrité de l'appareil', 'Contrôleur de réseau', 'Hyper-V', 'Serveur de télécopie', 'Serveur DHCP', 'Serveur DNS' (checked), 'Serveur Web (IIS)', 'Service Guardian hôte', 'Services AD DS' (checked), 'Services AD LDS (Active Directory Lightweight Directories)', 'Services AD RMS (Active Directory Rights Management)', 'Services Bureau à distance', 'Services d'activation en volume', 'Services d'impression et de numérisation de documents', 'Services de certificats Active Directory', 'Services de fédération Active Directory (AD FS)', 'Services de fichiers et de stockage (1 sur 12 installés)', and 'Services de stratégie et d'accès réseau'. The 'Description' column provides a detailed explanation for the 'Services AD DS' role, stating that it stores information about objects on the network and provides access to authorized resources via a unique session opening.

Dans l'onglet 'Confirmation', installer les services



Promouvoir l'AD en tant que contrôleur de domaine :

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

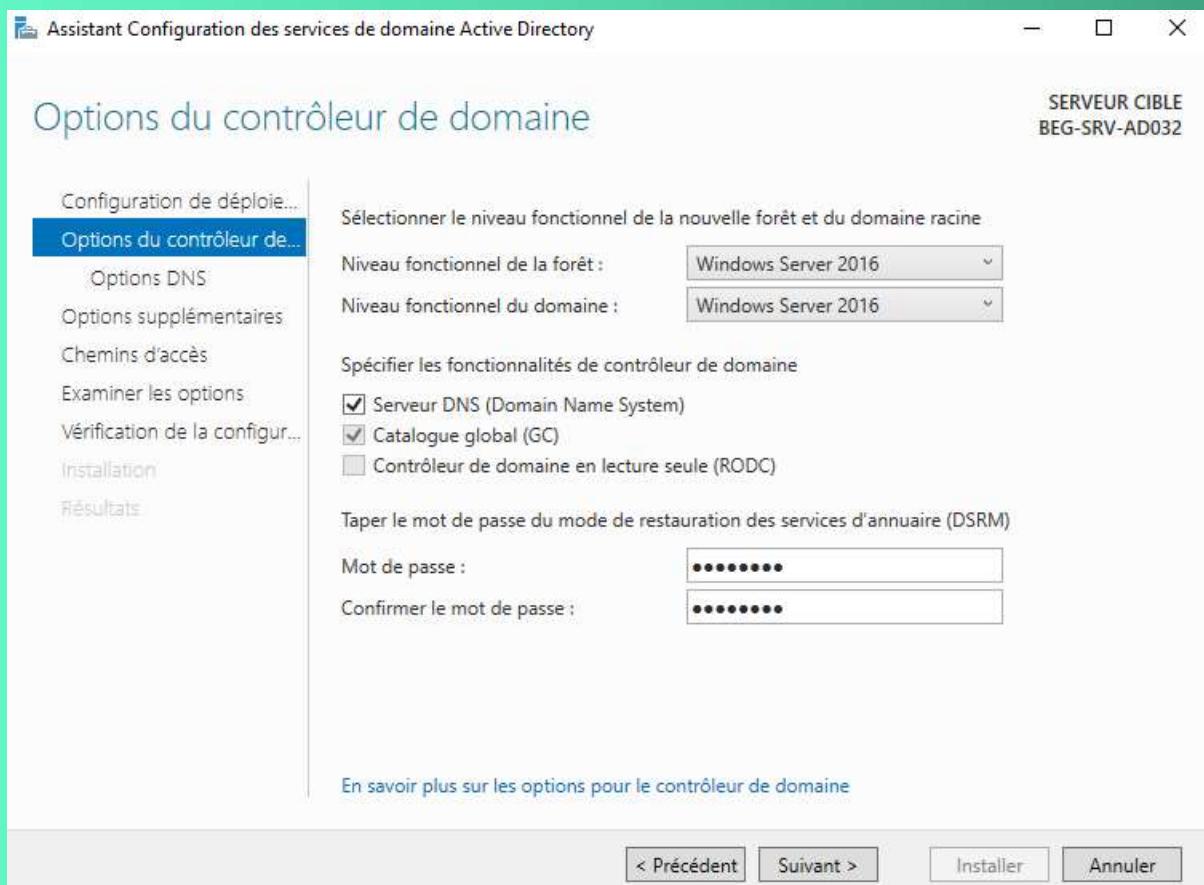


Configuration du contrôleur de domaine :

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



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



Ne pas modifier les chemins d'accès

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 commencer... [Afficher plus](#) [x](#)

Configuration de déploiement	La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur
Options du contrôleur de domaine	Réexécuter la vérification de la configuration requise
Options DNS	
Options supplémentaires	
Chemins d'accès	
Examiner les options	
Vérification de la configuration	<p>⚠ 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.</p> <p>Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com/fwlink/?LinkId=104751).</p> <p>⚠ 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</p> <p>⚠ Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.</p>
Installation	
Résultats	

[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

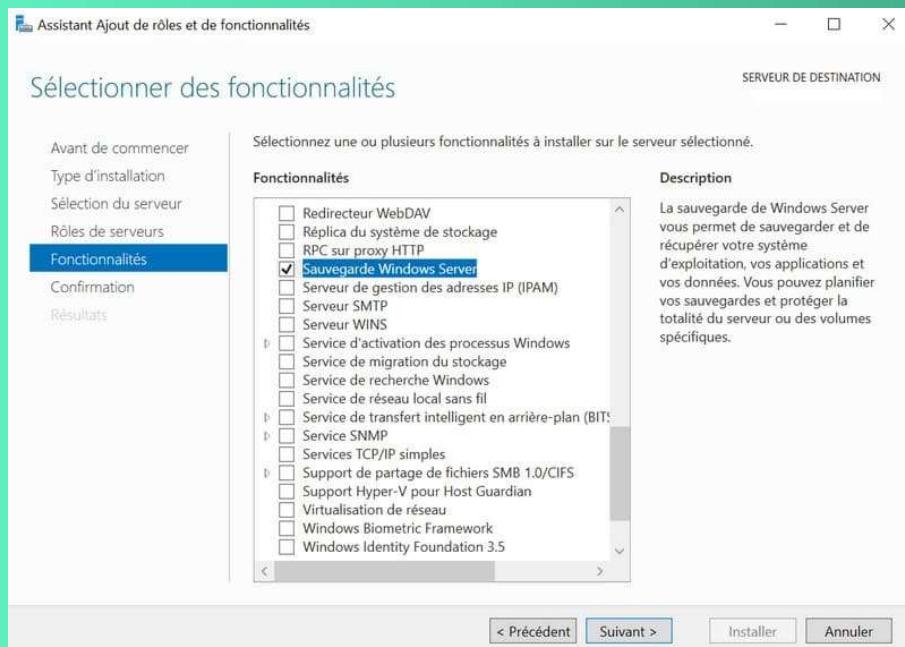
        Write-Output "Création de l'utilisateur : $UtilisateurLogin ($UtilisateurNom $UtilisateurPrenom)"
    } catch {
        Write-Error "Erreur lors de la création de l'utilisateur $UtilisateurLogin : $_"
    }
}
}

```

SAUVEGARDE DE L'AD

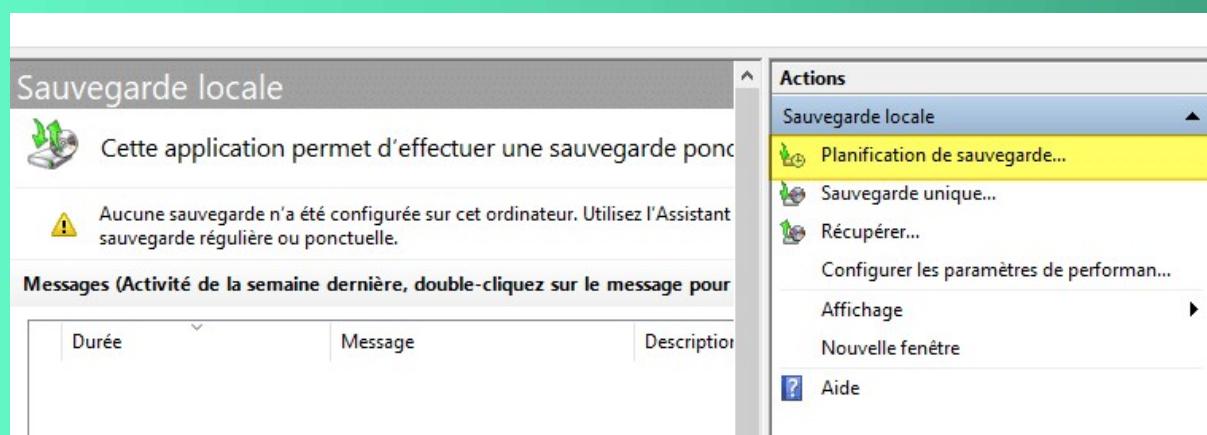
Installation du service :

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



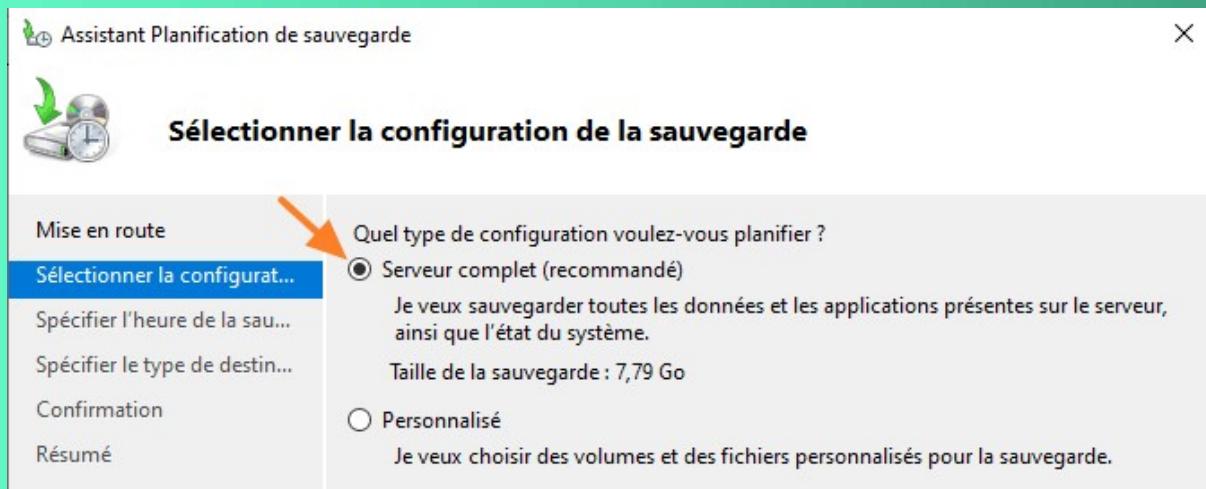
Sauvegarde de l'AD avec Windows Server Backup :

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

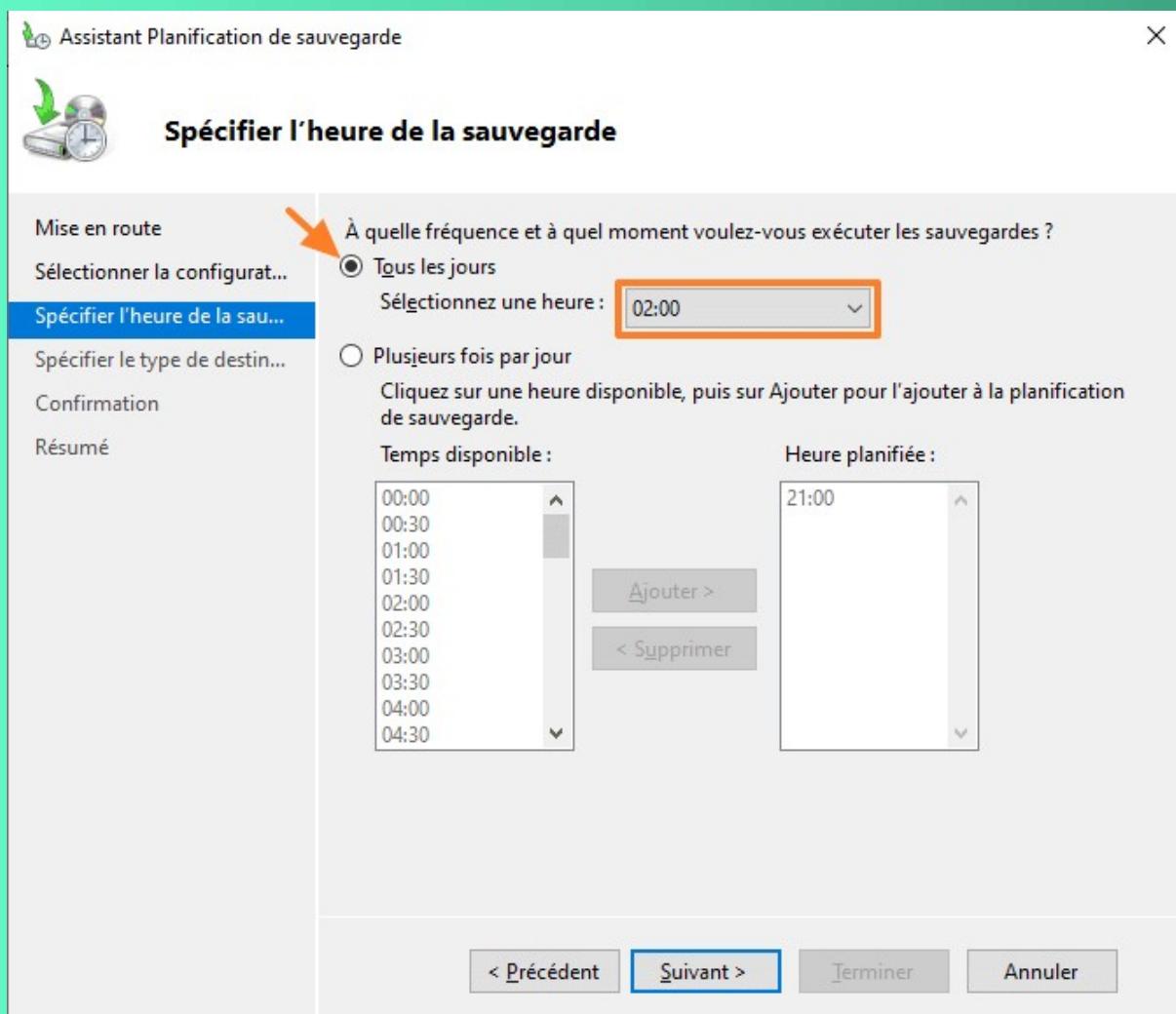


Poursuivons en cliquant sur "Suivant".

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

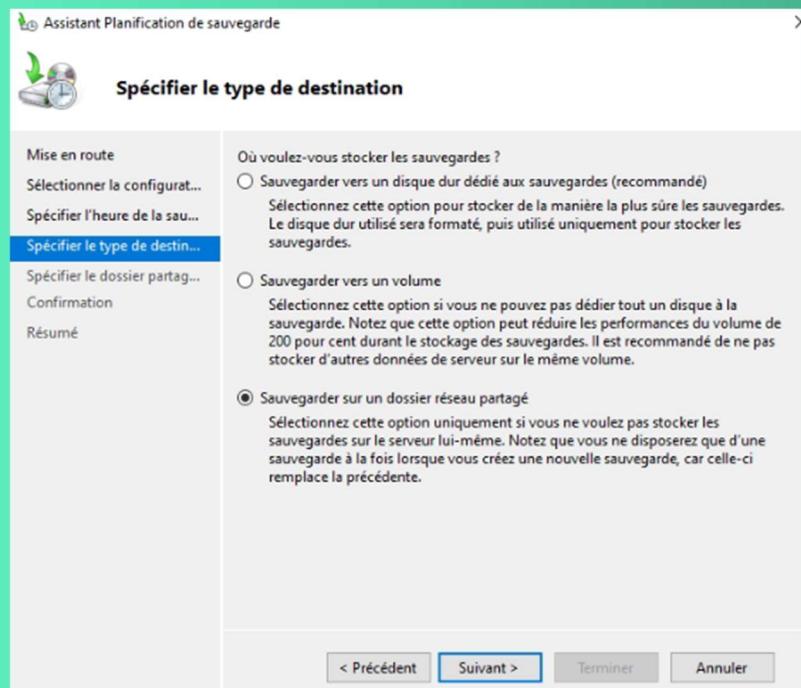


Ensuite, l'heure et la fréquence de la sauvegarde doivent être définies. Dans cet exemple, on sélectionne "Tous les jours" à 02:00.

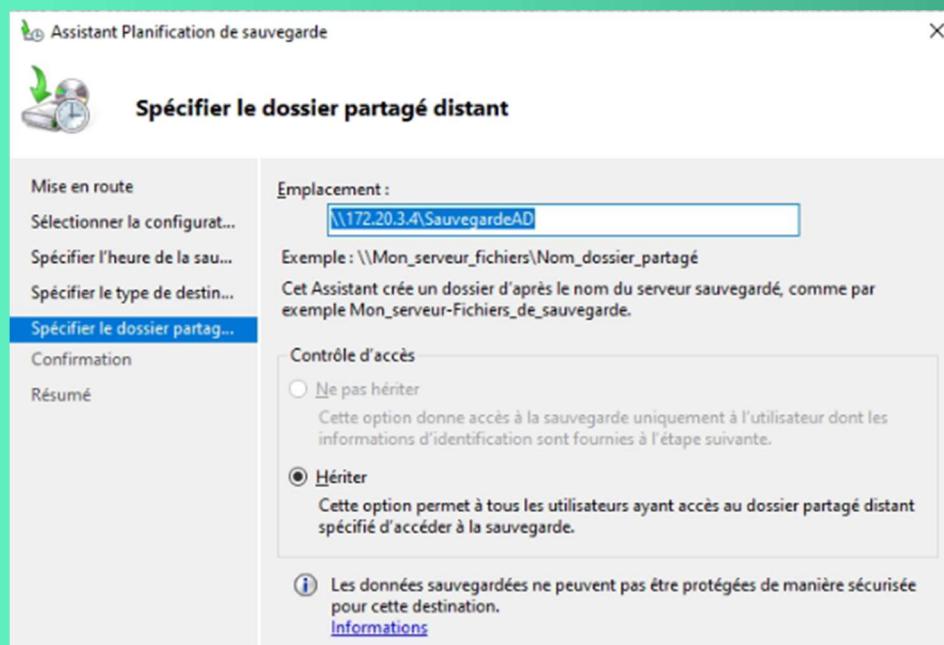


Puis, nous devons choisir la destination de la sauvegarde. Il est recommandé d'utiliser l'option "Sauvegarder vers un disque dur dédié aux sauvegardes". Bien que ça peut être tentant de choisir la dernière option pour stocker la sauvegarde sur un espace partagé (sur un NAS, par exemple), ce

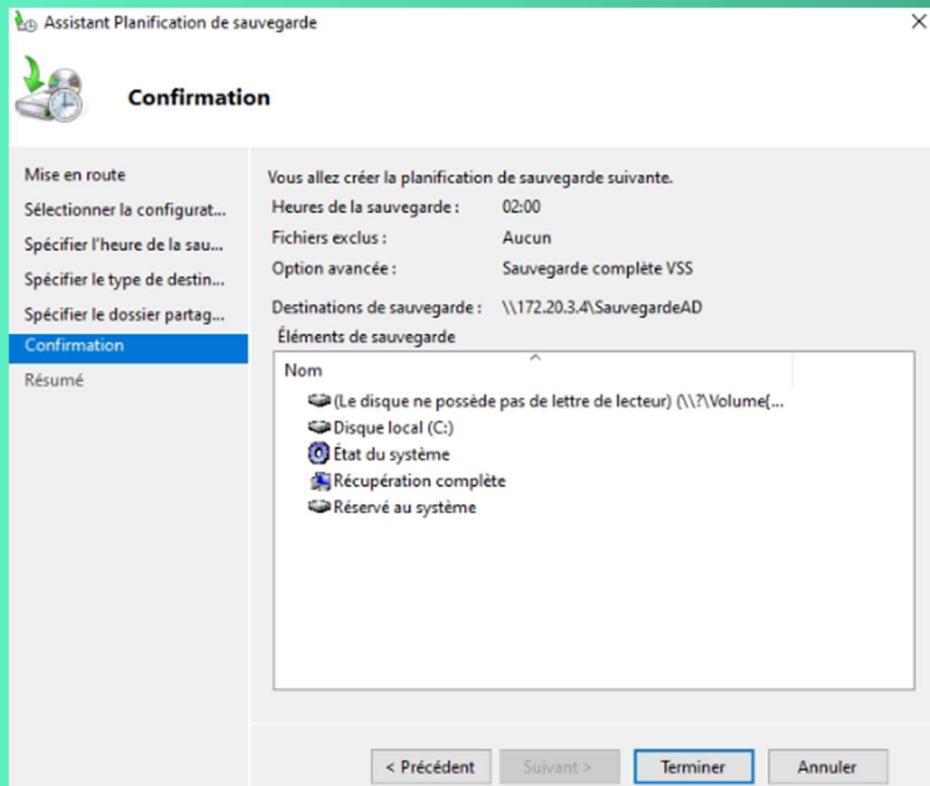
n'est pas recommandé car, avec ce mode, l'outil conserve une seule sauvegarde et il écrase la précédente à chaque fois...!



Ensute, entrer l'emplacement du fichier partagé



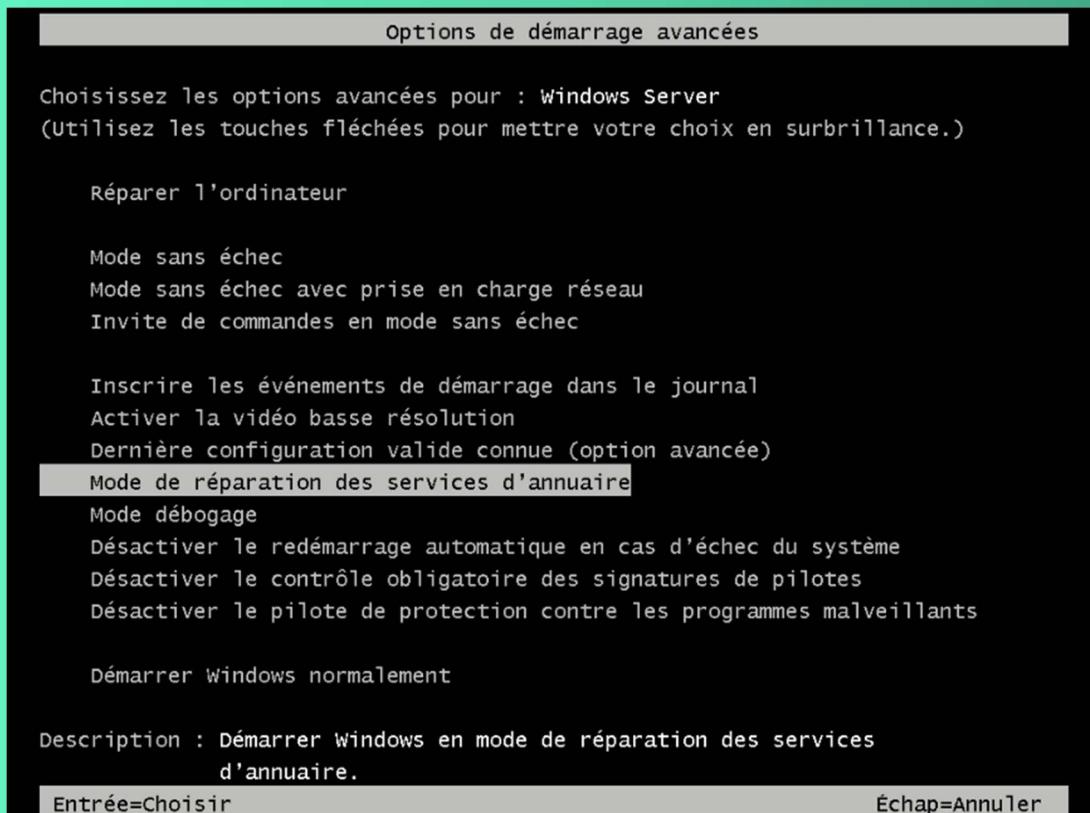
Un résumé s'affiche, cliquons sur "Terminer" pour finaliser la création de la tâche.



RESTAURATION DE L'AD

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

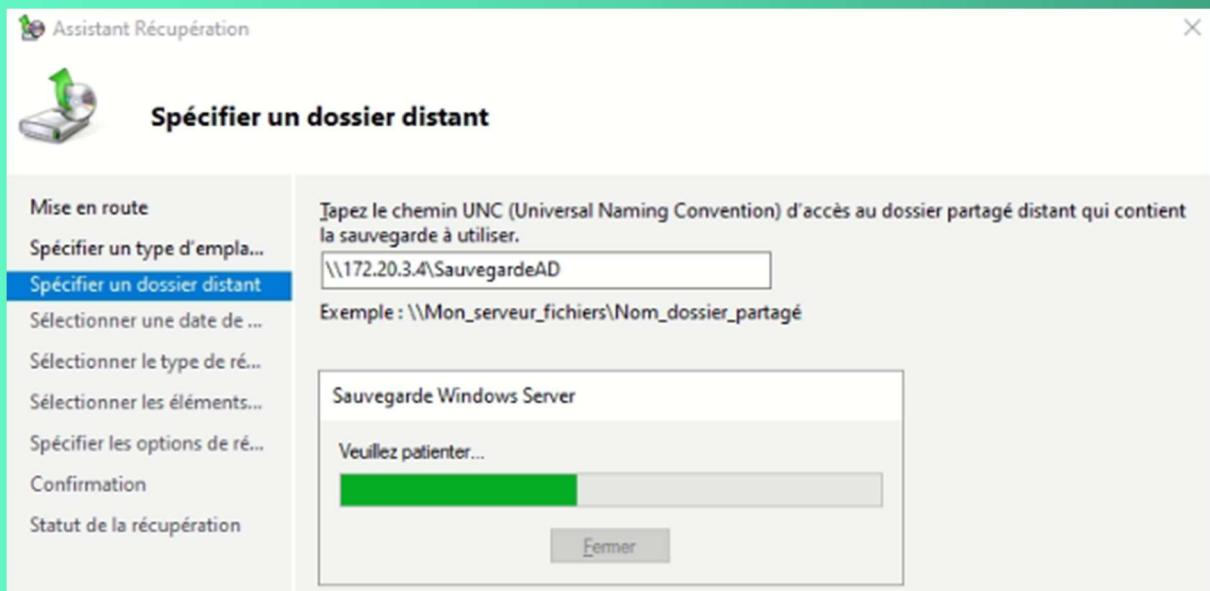
Sélectionner ‘mode de réparation des services d’annuaire



Ensuite, choisir autre utilisateur et mettre le compte Administrateur



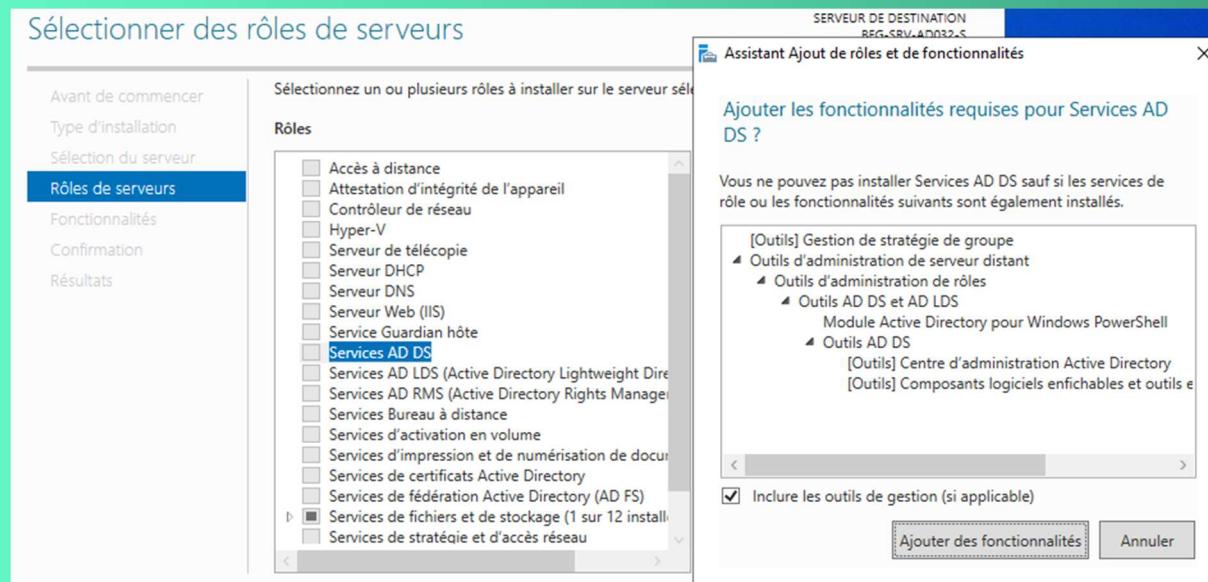
Aller dans l'outil 'Sauvegarde Windows Server'. Clique droit sur 'Sauvegarde locale' et sélectionner 'Récupérer', 'un autre emplacement', 'Dossier Partagé distant' et entrer le chemin de sa sauvegarde (\\\172.20.3.4\SauvegardeAD), suivant, 'Etat du système', 'emplacement d'origine' et cocher la case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



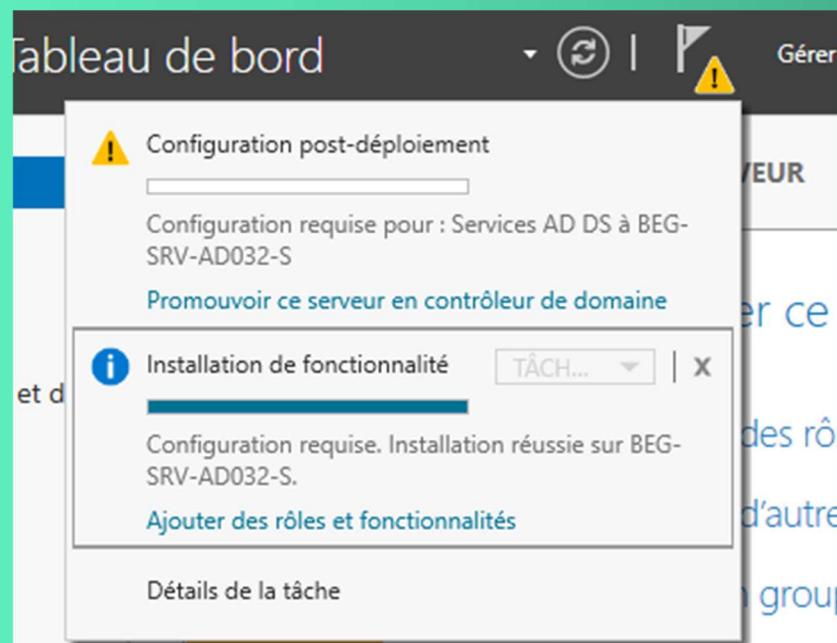
CONFIGURATION D'UN SECOND ACTIVE DIRECTORY

Installation du service :

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



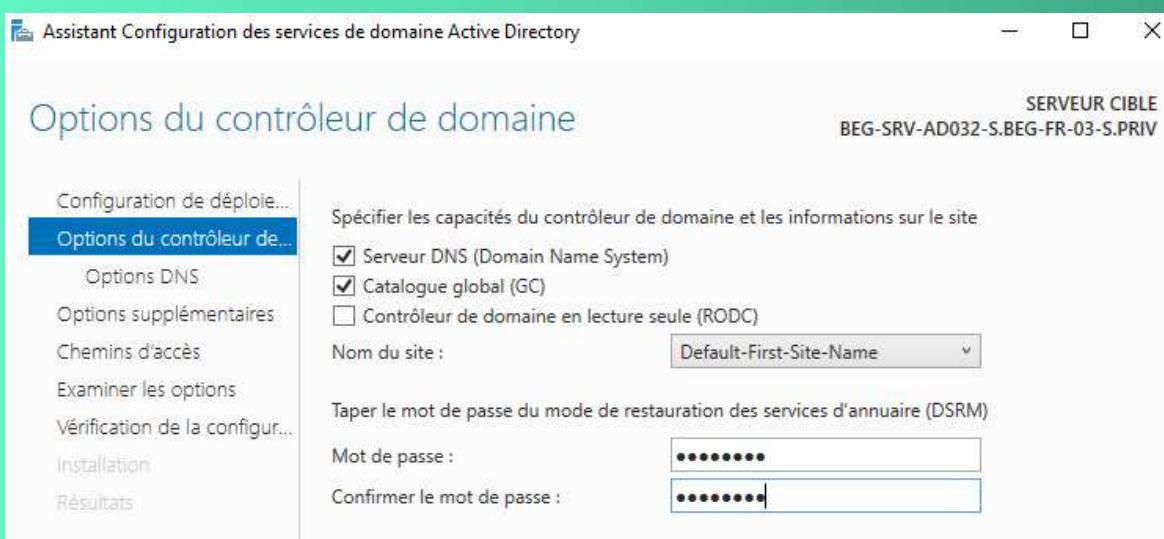
Ensuite, promouvoir ce serveur en contrôleur de domaine



Selectionner 'Ajouter un contrôleur de domaine à un domaine existant' et entrer notre nom de domaine



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



Spécifier des options supplémentaires :

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



Pour finir, installer le service

Assistant Configuration des services de domaine Active Directory

Vérification de la configuration requise

SERVEUR CIBLE
BEG-SRV-AD032-S.BEG-FR-03-S.PRIV

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation... [Afficher plus](#) ×

Configuration de déploiement
Options du contrôleur de domaine
Options DNS
Options supplémentaires
Chemins d'accès
Examiner les options
Vérification de la configuration requise

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
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 manuellement créer une délégation avec ce serveur DNS dans la zone parente pour activer une résolution de noms fiable en dehors du domaine « BEG-FR-03-S.PRIV ». Sinon, aucune action n'est requise.

(+) Vérification de la configuration requise terminée
✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation.

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

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

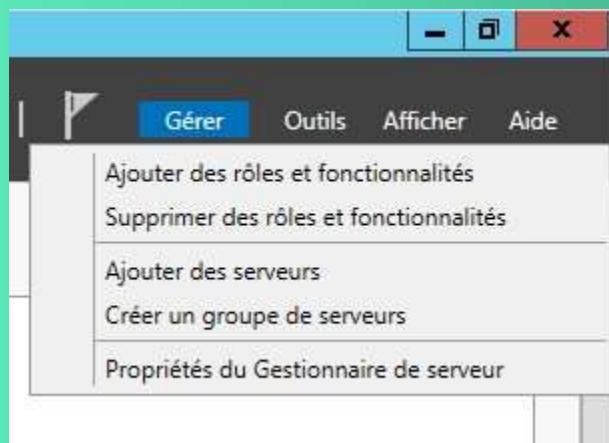
[< Précédent](#) [Suivant >](#) Installer Annuler

MISE EN PLACE D'UN RODC

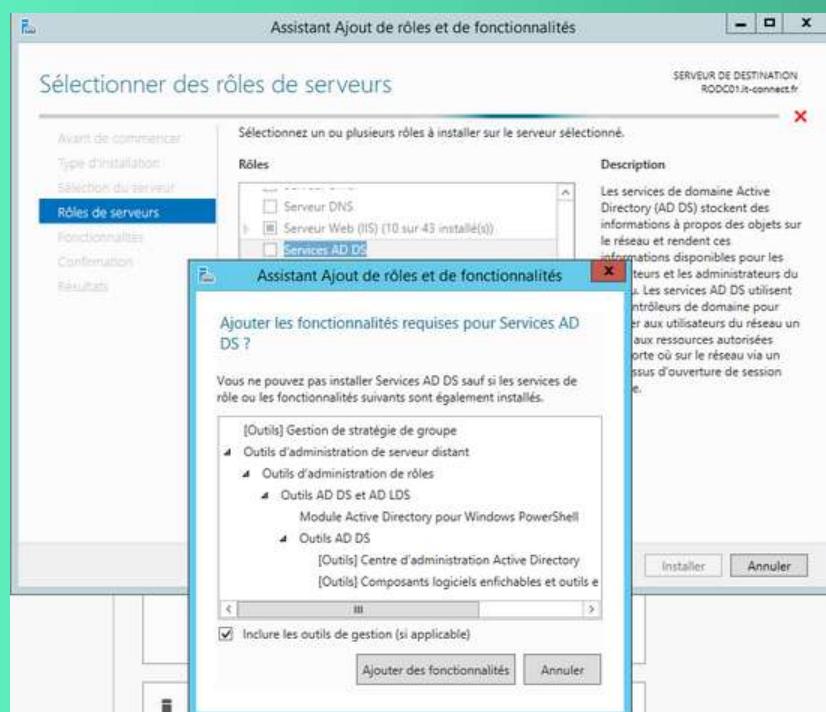
Installation du service :

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

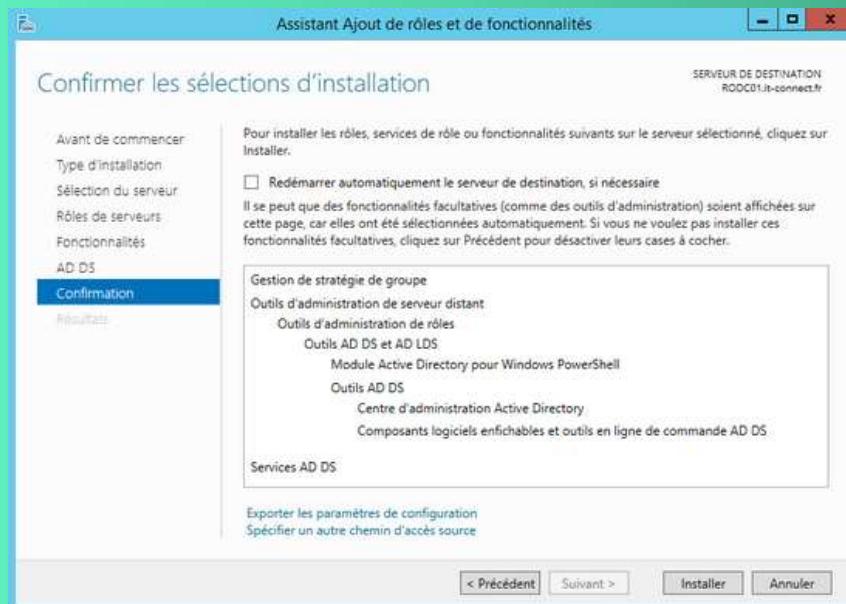
Sur le futur RODC, ouvrez le gestionnaire de serveur puis cliquez sur « Gérer » et « Ajouter des rôles et fonctionnalités ».



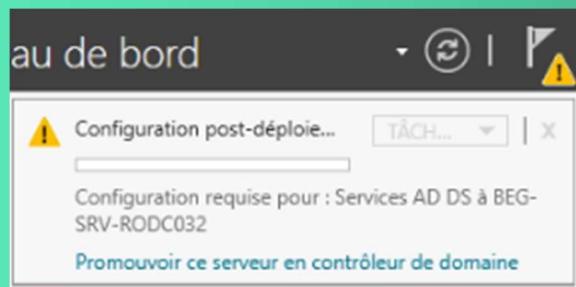
Dans la liste, sélectionnez « Services AD DS », confirmez l'ajout des fonctionnalités requises pour ce rôle et poursuivez.



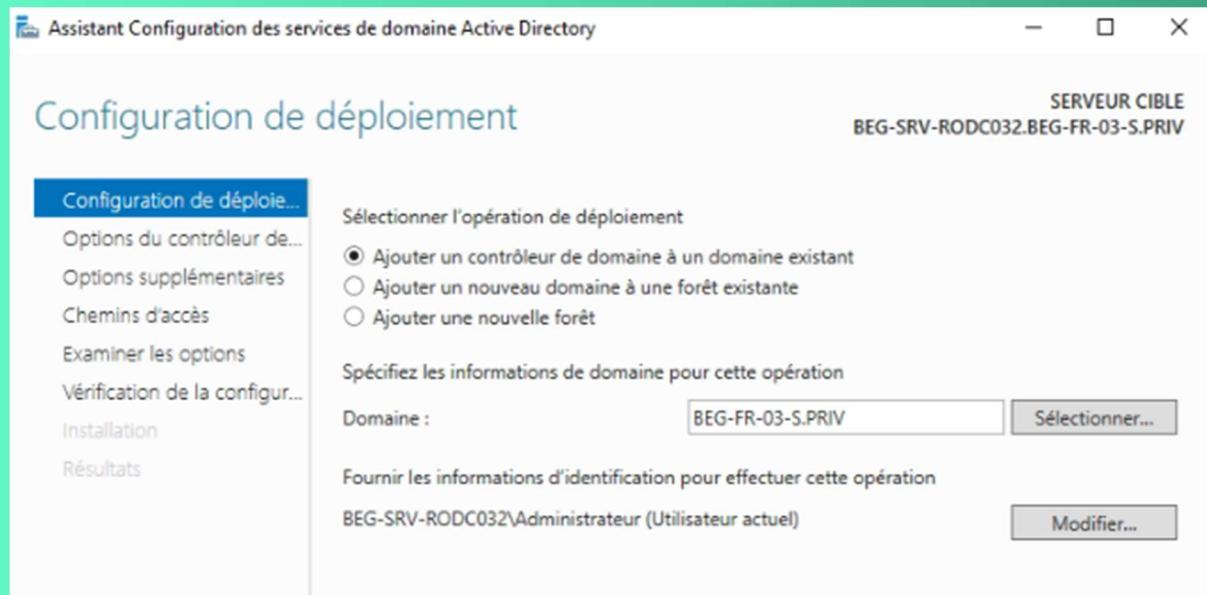
Confirmez que vous souhaitez installer les sélections en cliquant sur « Installer ».



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



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



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

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 : 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 :

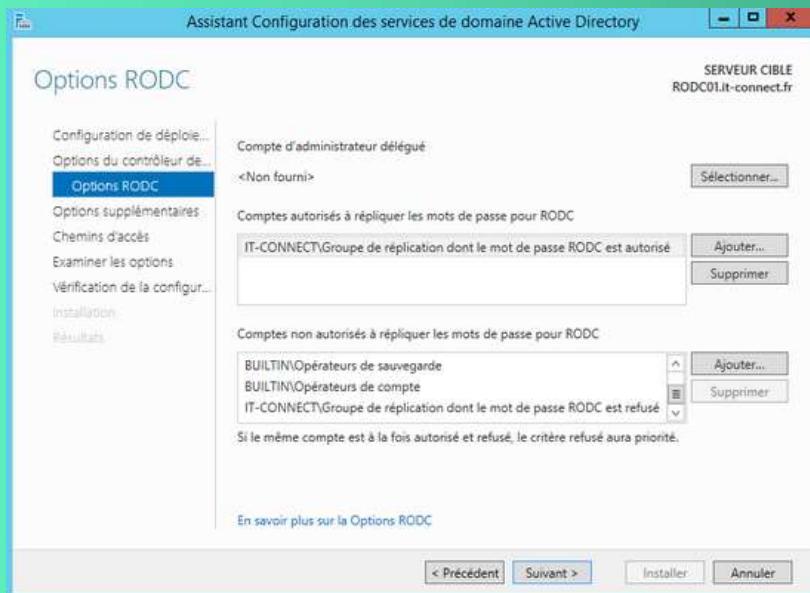
- Groupe de réPLICATION dont le mot de passe RODC est autorisé
- Groupe de réPLICATION dont le mot de passe RODC est refusé

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.

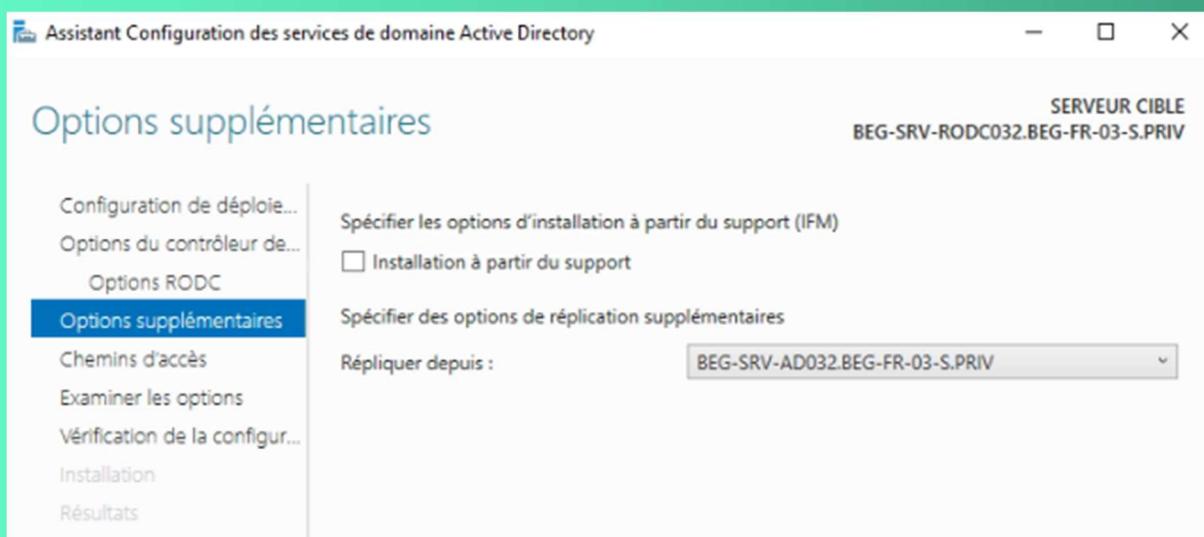
- Comptes autorisés à répliquer les mots de passe pour RODC : Ajouter des utilisateurs ou groupes pour lesquels vous souhaitez autoriser la réPLICATION. Le mieux, c'est de laisser uniquement le groupe « Groupe de réPLICATION dont le mot de passe RODC est autorisé » et dans l'Active Directory d'ajouter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

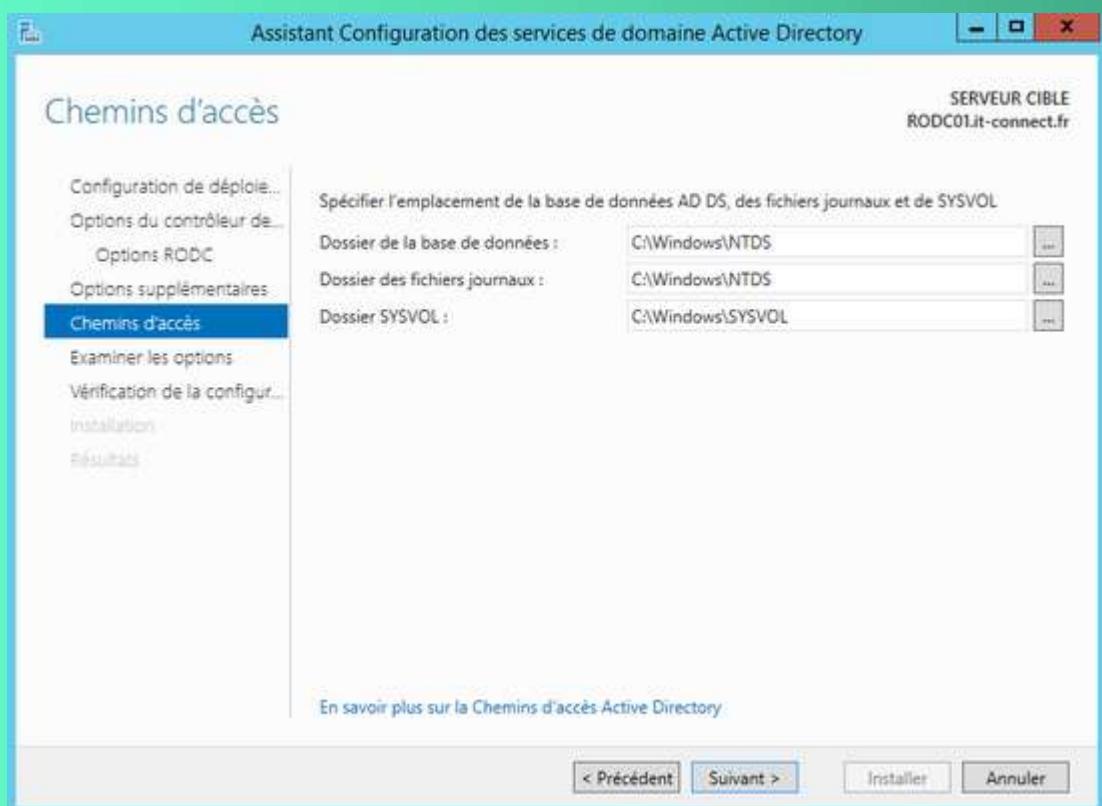
Cliquez sur « Suivant » pour continuer l'installation.



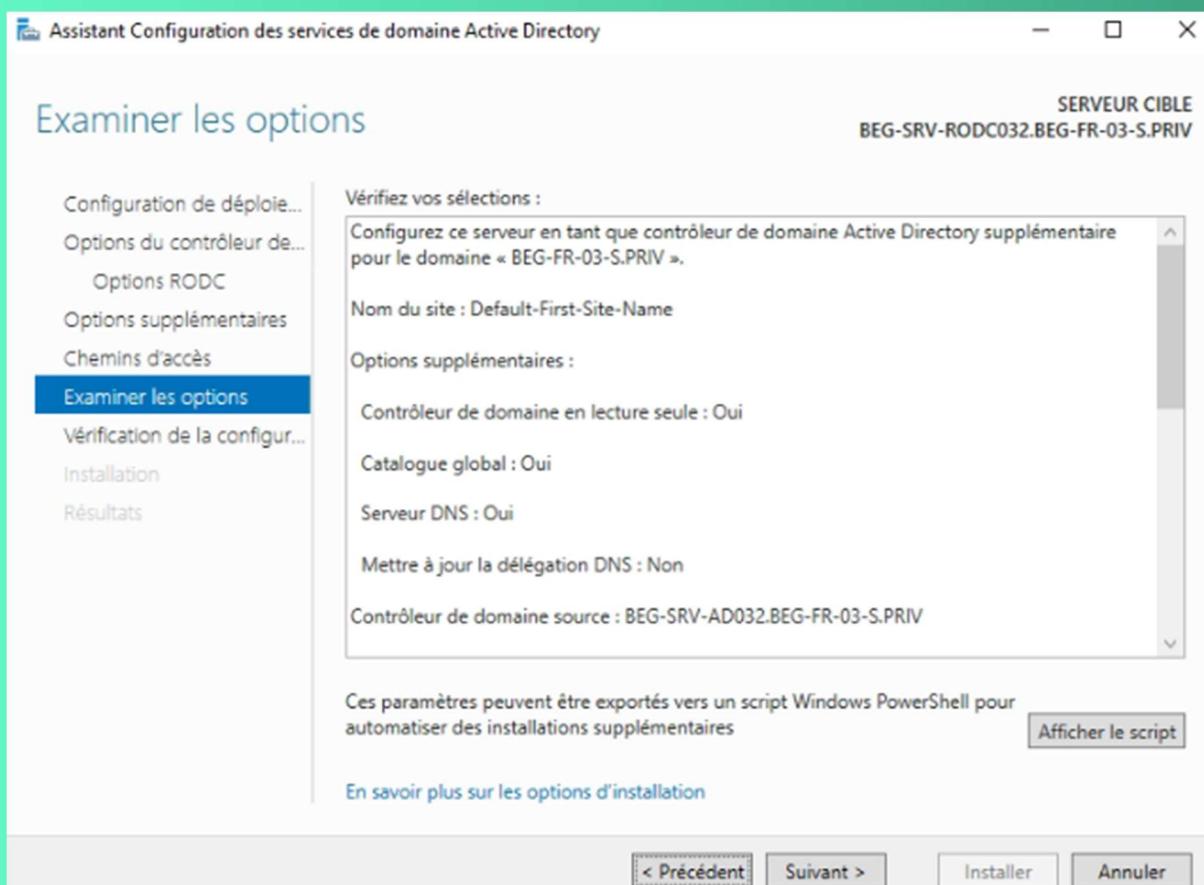
Indiquez un contrôleur de domaine standard depuis lequel répliquer les informations autorisées (ou installer à partir d'un support si vous disposez d'un support prêt – utile pour économiser de la bande passante même lors de la mise en place). Cliquez sur « Suivant ».



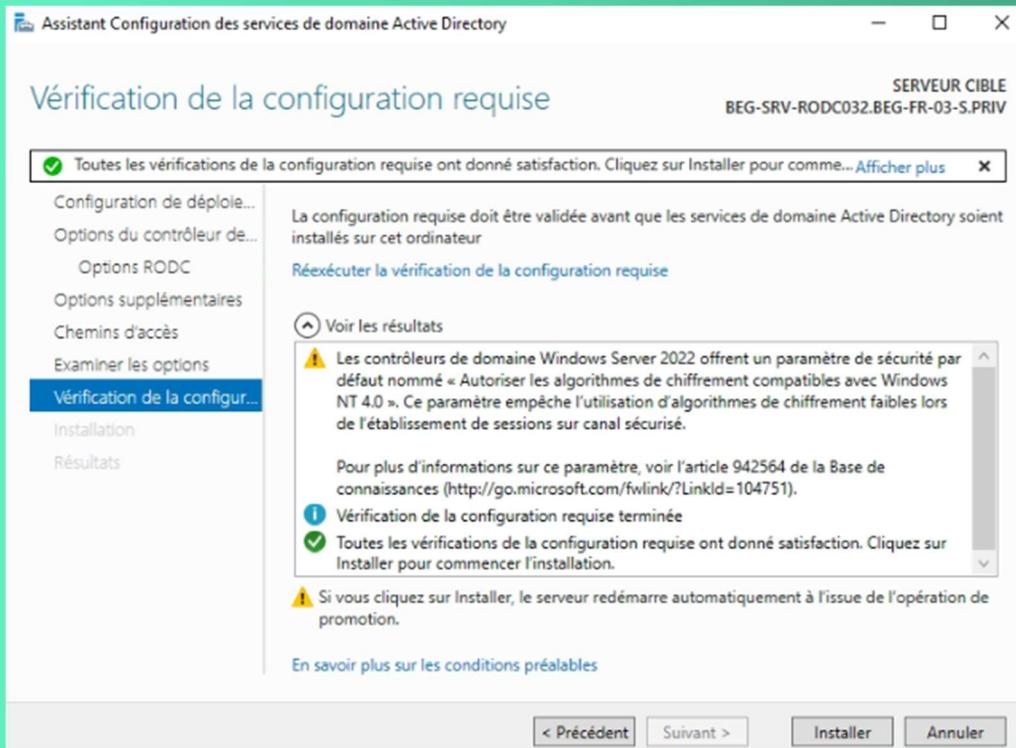
Indiquez l'emplacement de la base de données, des fichiers journaux et de SYSVOL (peuvent être placés sur des disques différents). Cliquez sur « Suivant ».



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



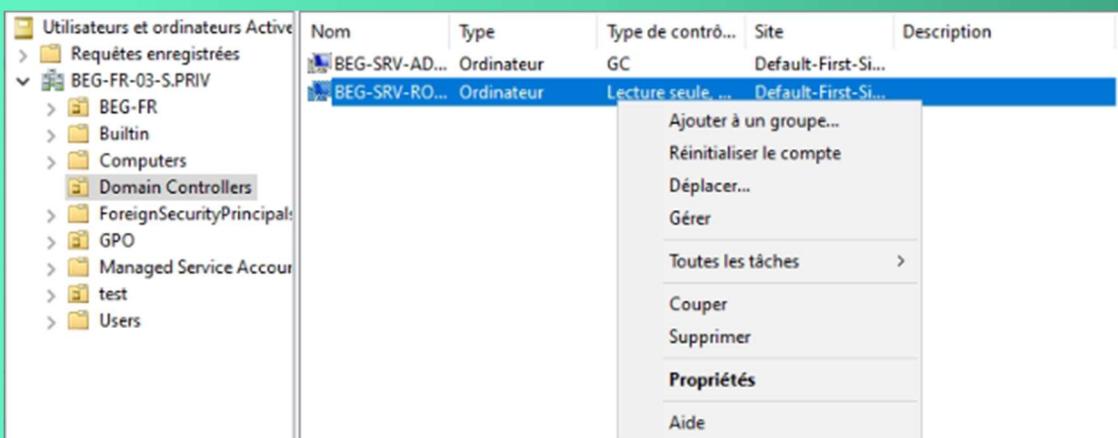
Après que la configuration soit vérifiée, cliquez sur « Installer » et patientez un instant. Le serveur va redémarrer automatiquement à la fin de l'installation.



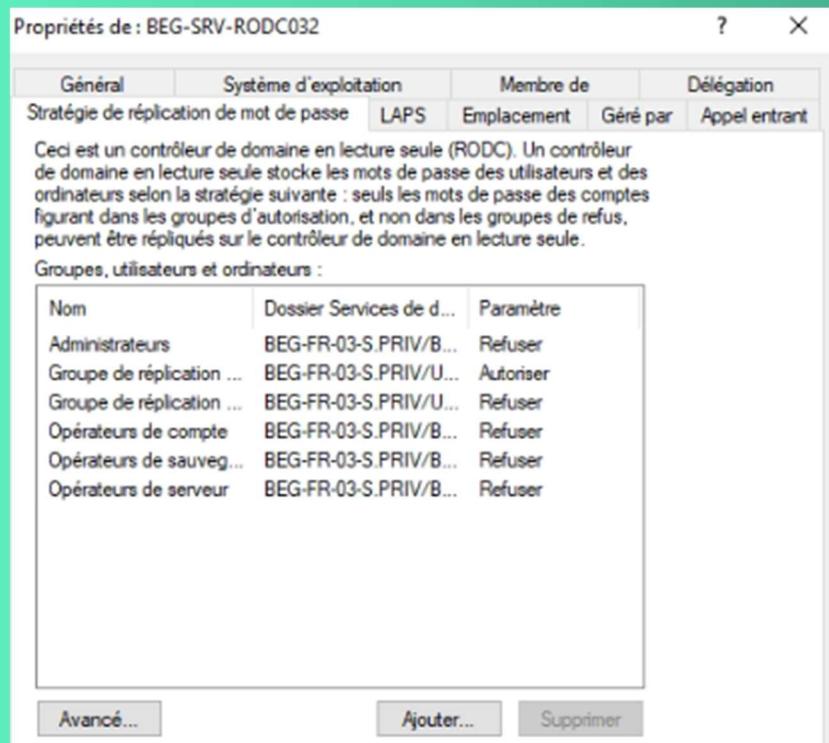
L'installation du RODC est désormais terminée.

RéPLICATION DES MOTS DE PASSES

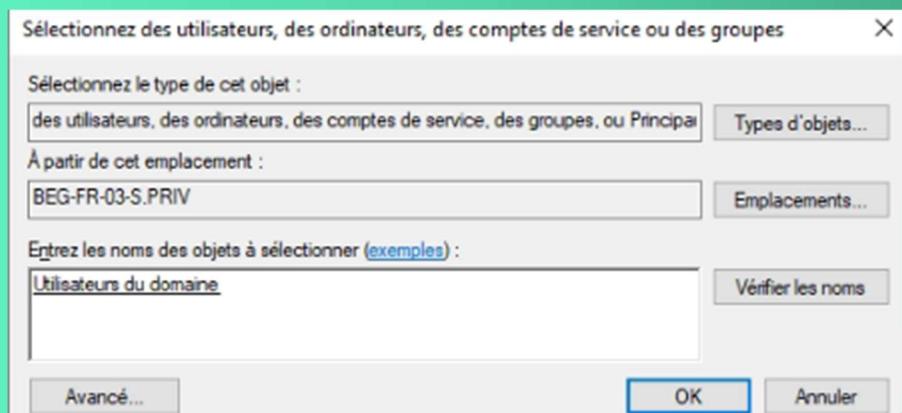
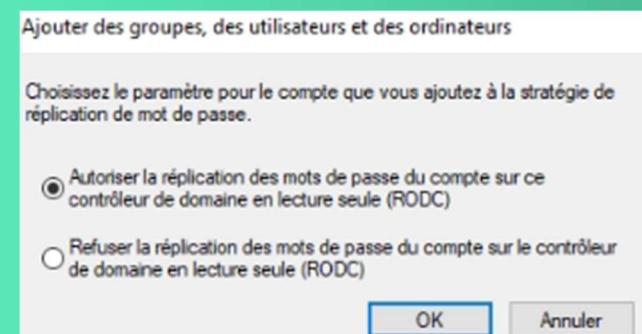
Sur un contrôleur de domaine standard (lecture/écriture), ouvrez la console « Utilisateurs et ordinateurs Active Directory », positionnez-vous sur l'unité d'organisation « Domain Controllers ». Sur la droite, faites clic droit sur l'objet ordinateur correspondant à votre serveur RODC puis « Propriétés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



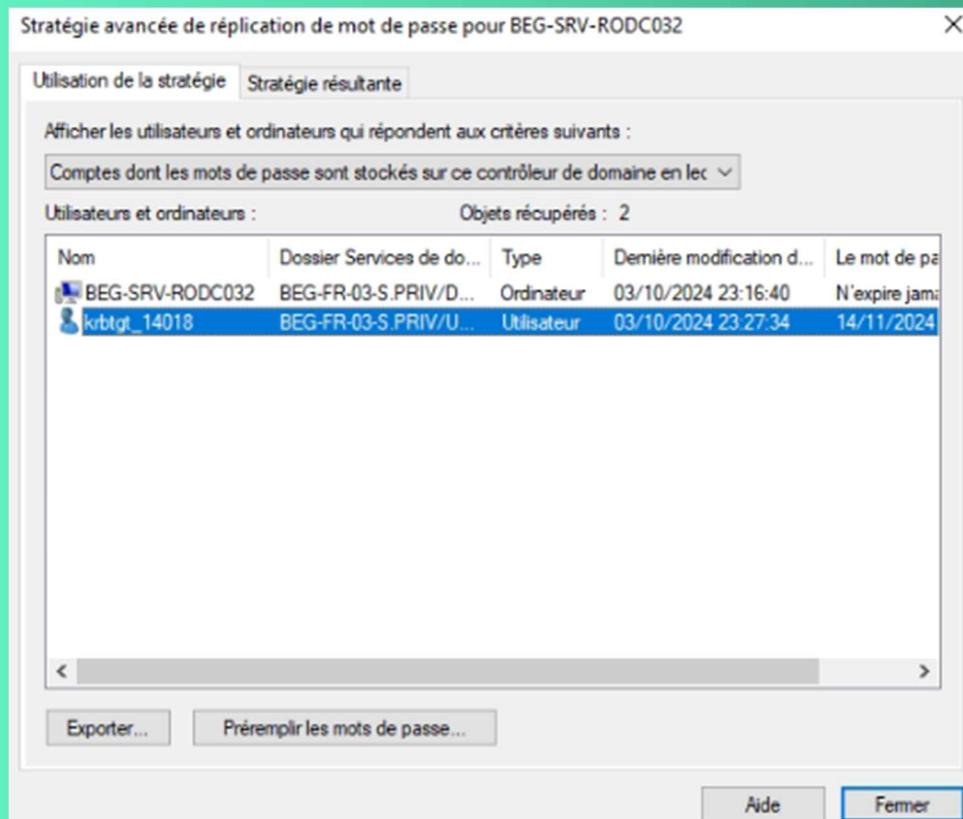
Cliquez ensuite sur l'onglet « Stratégie de réPLICATION de mot de passe » qui concerne donc la stratégie de réPLICATION des mots de passe. La fenêtre affiche les utilisateurs et groupes pour lesquels vous autorisez ou refusez explicitement la réPLICATION des mots de passe.



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_xxxxx). Il permet de délivrer les tickets Kerberos aux clients.

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

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

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

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

Stratégie avancée de réPLICATION de mot de passe pour BEG-SRV-RODC032

Utilisation de la stratégie Stratégie résultante

Afficher les utilisateurs et ordinateurs qui répondent aux critères suivants :

Comptes dont les mots de passe sont stockés sur ce contrôleur de domaine en les :

Utilisateurs et ordinateurs : Objets récupérés : 122

Nom	Dossier Services de do...	Type	Dernière modification d...	Le mot de p...
AUMIS Barthelemy	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:20	N'expire j...
AZZOUG Malik	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:26	N'expire j...
BAHANI Issam	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:19	N'expire j...
BARNIER Clement	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:20	N'expire j...
BASSOUMBA Franc...	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:19	N'expire j...
BEG-SRV-RODC032	BEG-FR-03-S.PRIV/D...	Ordinateur	03/10/2024 23:16:40	N'expire j...
BELARBI Valentin	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:22	N'expire j...
BILLOT Adèle	BEG-FR-03-S.PRIV/BEG-FR...	Utilisateur	20/09/2024 14:40:21	N'expire j...
BLANDIN Remi	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:24	N'expire j...
BOLIVARD Theresa	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:26	N'expire j...
BOUCHETTE Corali...	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:26	N'expire j...
BOUSSON Romain	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:20	N'expire j...
BREUGNOT Irvin	BEG-FR-03-S.PRIV/B...	Utilisateur	20/09/2024 14:40:25	N'expire j...

Exporter... Préremplir les mots de passe... Aide Fermer

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

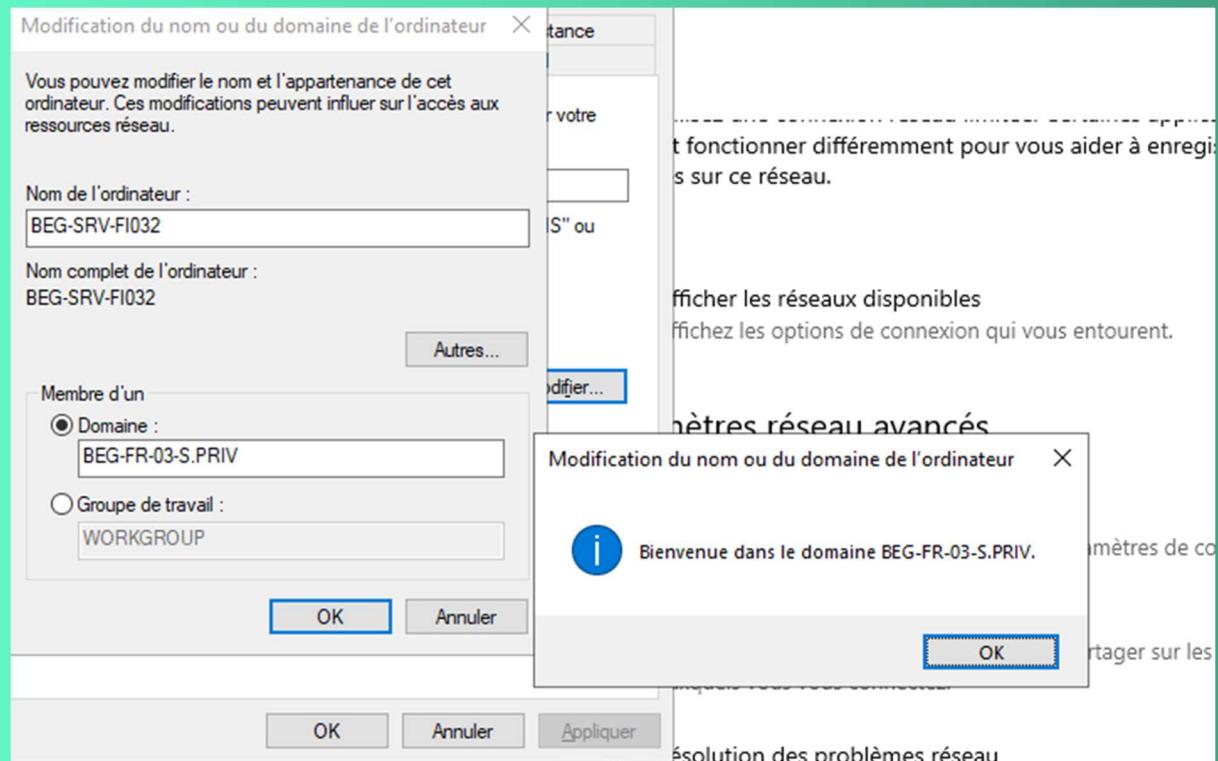
CHANGER LE SID D'UNE MACHINE

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

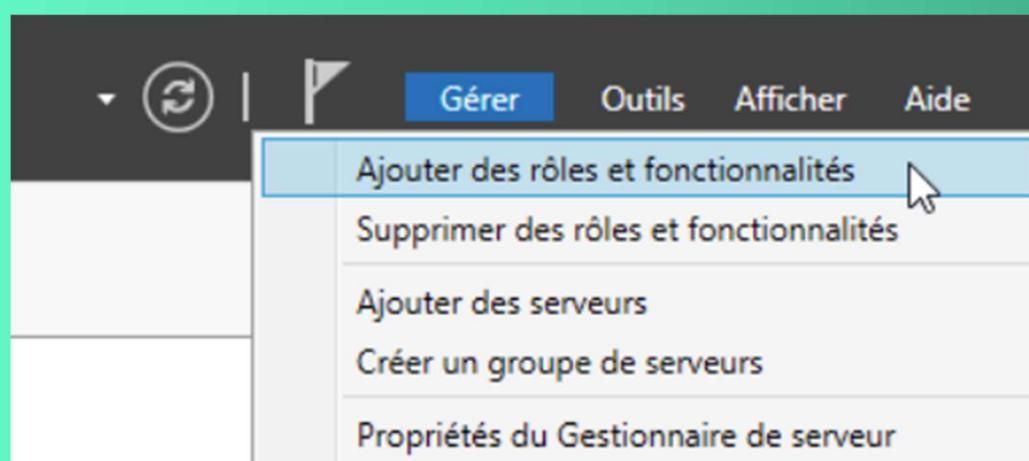
```
C:\Windows\System32\sysprep\sysprep.exe /oobe /generalize /shutdown
```

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

SÉRVEUR 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

<input type="checkbox"/> Services de certificats Active Directory	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.
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 installé(s))	
<input checked="" type="checkbox"/> Services de fichiers et iSCSI (1 sur 11 installé(s))	
<input checked="" type="checkbox"/> Serveur de fichiers (Installé)	
<input type="checkbox"/> BranchCache pour fichiers réseau	
<input type="checkbox"/> Déduplication des données	
<input type="checkbox"/> Dossiers de travail	
<input type="checkbox"/> Espaces de noms DFS	
<input type="checkbox"/> Fournisseur de stockage cible iSCSI (fournis par le serveur)	
<input checked="" type="checkbox"/> Gestionnaire de ressources du serveur de fichiers	
<input type="checkbox"/> Réplication DFS	
<input type="checkbox"/> Serveur cible iSCSI	
<input type="checkbox"/> Serveur pour NFS	
<input type="checkbox"/> Service Agent VSS du serveur de fichiers	
<input checked="" type="checkbox"/> Services de stockage (Installé)	
<input type="checkbox"/> Services de stratégie et d'accès réseau	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	
<input type="checkbox"/> 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

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

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

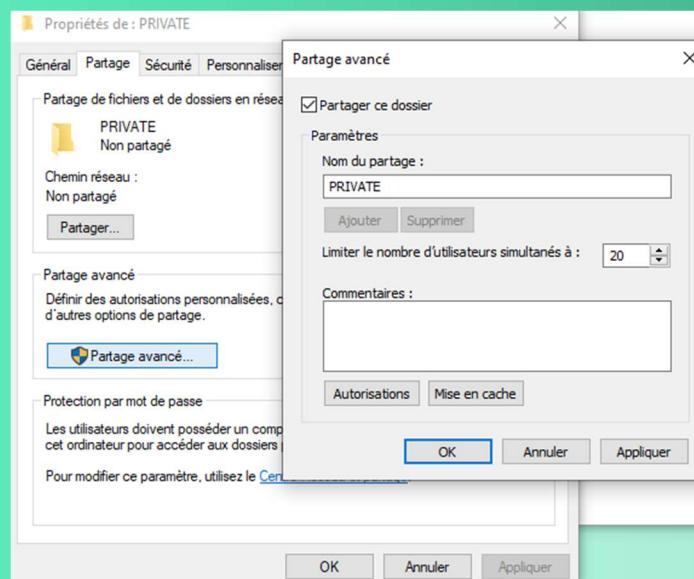
< Précédent Suivant > Fermer Annuler

CRÉATION DES DOSSIERS

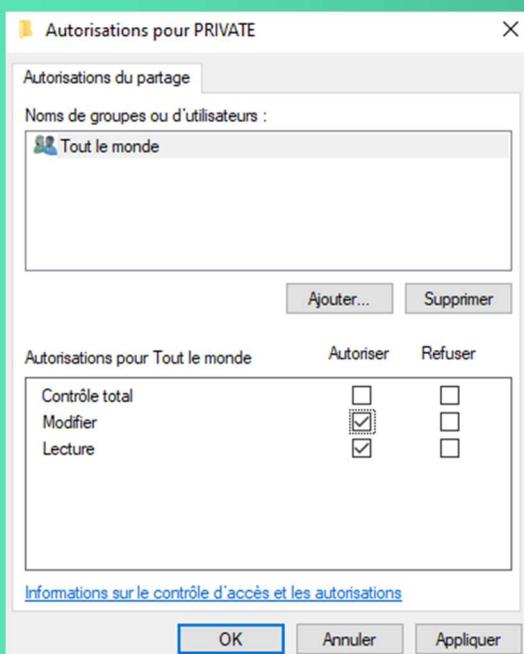
PRIVATE

Partage du dossier :

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

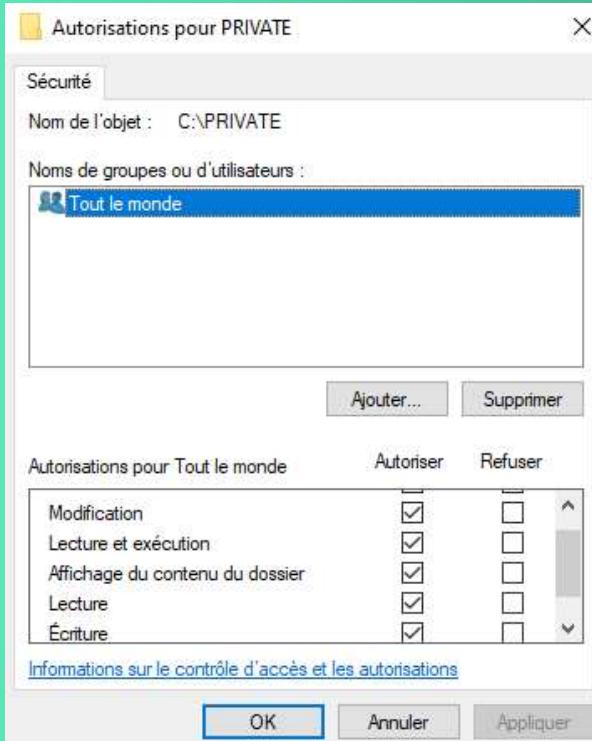


Ensuite, cliquer sur ‘Autorisations’ et sélectionner tout le monde en lecture et modifier

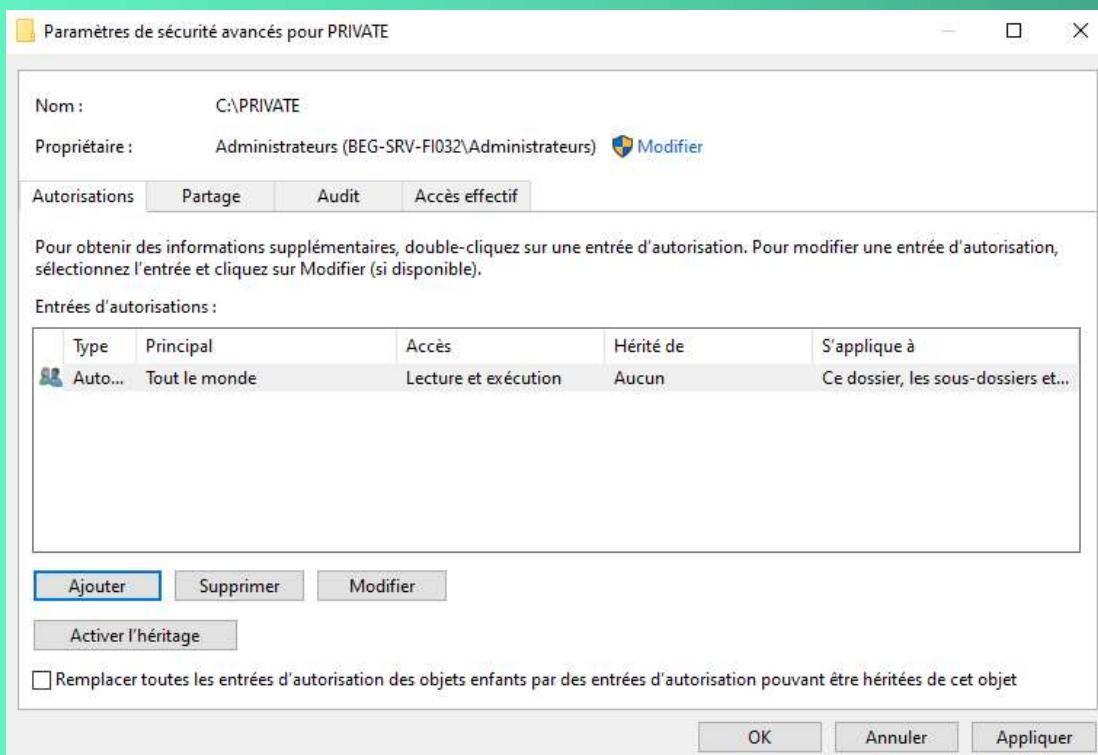


Permissions NTFS :

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



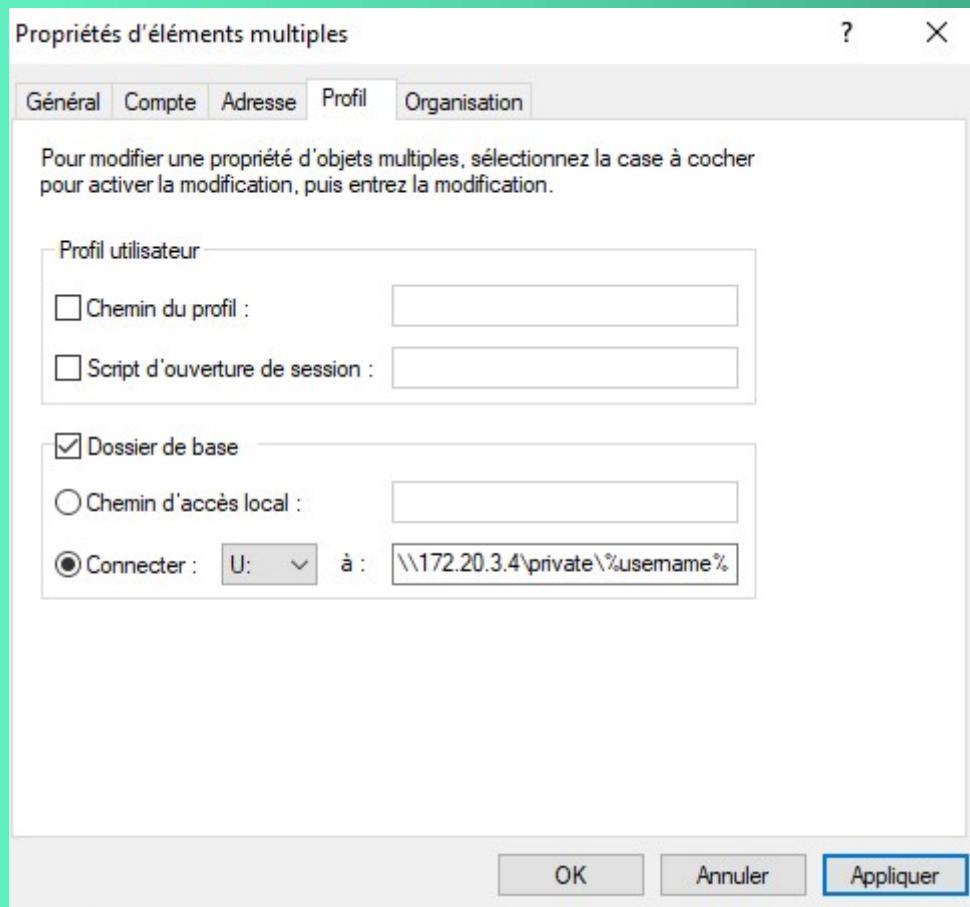
Ensuite il faut désactiver l'héritage dans les paramètres de sécurité avancés du dossier PRIVATE



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



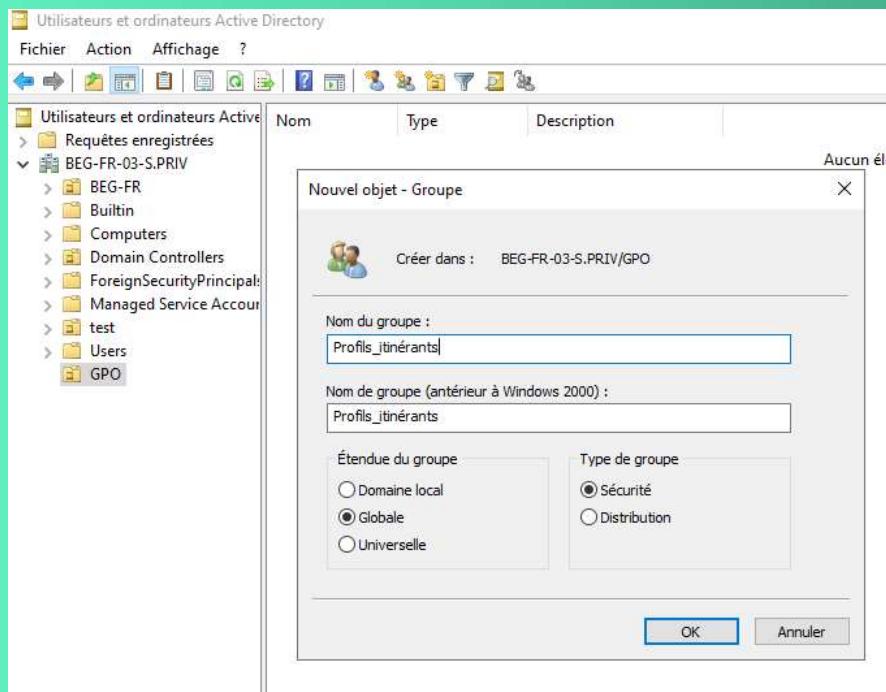
PROFILS ITINÉRANTS

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.

Nom	État GPO	Filtre WMI	Modifié le	Propriétaire
Default Domain Controllers Policy	Activé	Aucun(e)	06/09/2024 16:31:04	Admins du domaine (BEG...)
Default Domain Policy	Activé	Aucun(e)	06/09/2024 16:34:42	Admins du domaine (BEG...)
imprimante	Activé	Aucun(e)	25/09/2024 15:20:22	Admins du domaine (BEG...)
imprimantes	Activé	Aucun(e)	20/09/2024 17:15:10	Admins du domaine (BEG...)

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

Nouvel objet GPO

Nom : Profils_itinérants

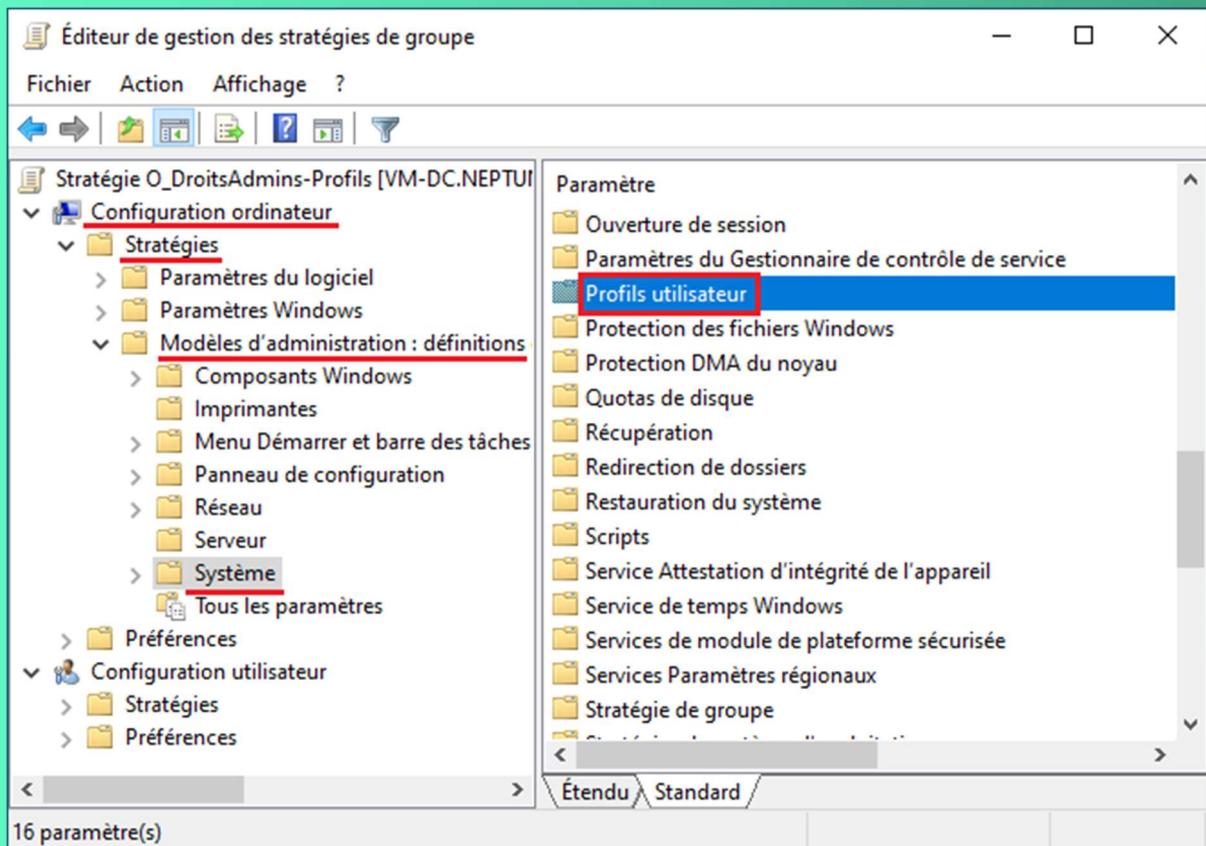
Objet Starter GPO source : (aucun)

OK Annuler

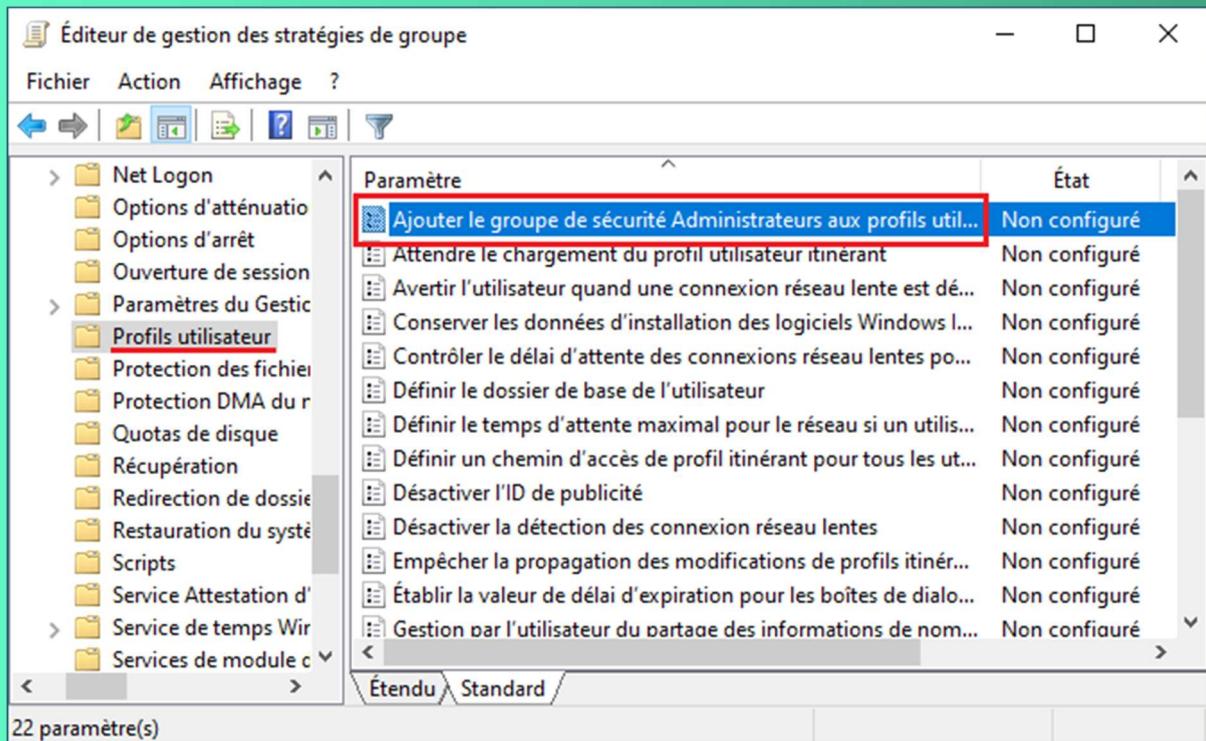
Ensuite faites un clic droit sur son nom puis « Modifier ».

- Modifier...
- État GPO
- Sauvegarder...
- Restaurer à partir d'une sauvegarde...
- Importer des paramètres...
- Enregistrer le rapport...

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

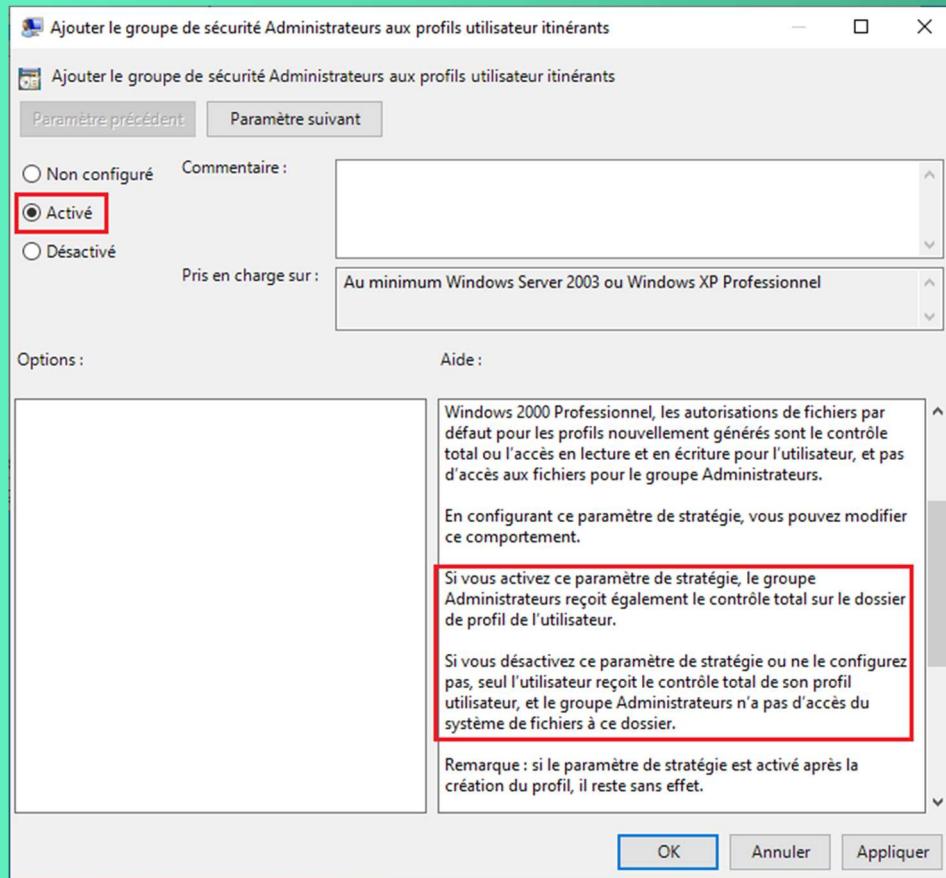


Recherchez sur la droite le paramètre nommé « Ajouter le groupe de sécurité Administrateurs aux profils utilisateur itinérants » et double-cliquez dessus.

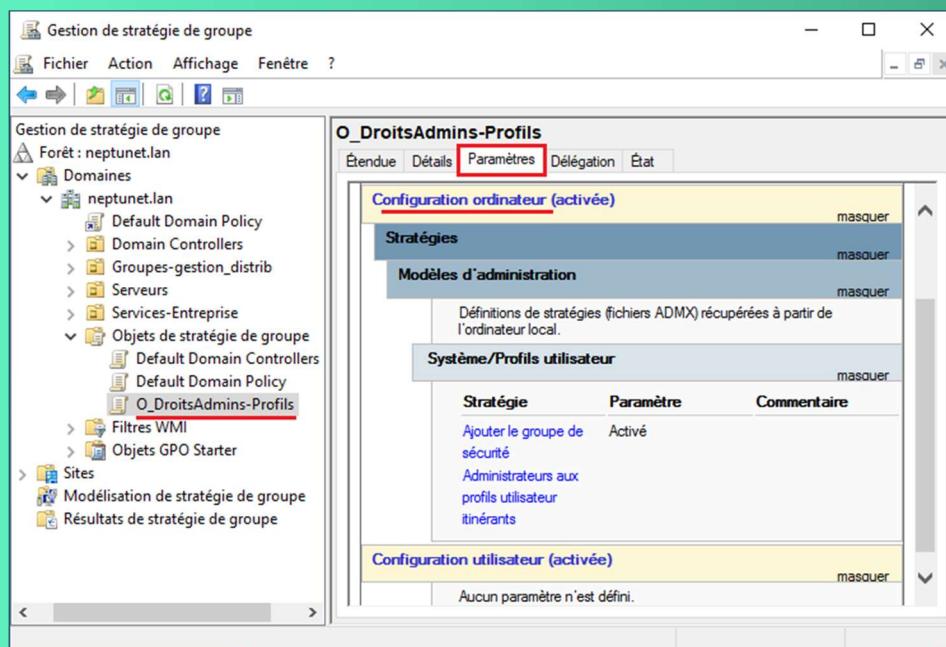


Si on regarde un peu dans la partie « Aide », il y a des infos intéressantes nous précisant ce qu'il se passe si on active ce paramètre, si au contraire on le désactive ou ne le configure pas. Nous voulons

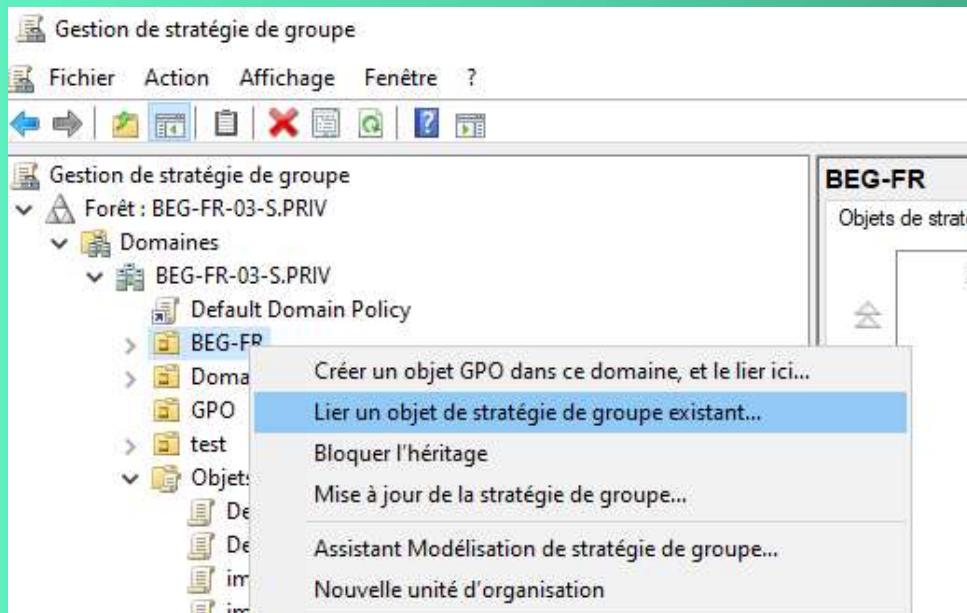
que les admins puissent accéder aux profils dont nous allons l'activer. Cochez la case « Activé » et cliquez sur OK.



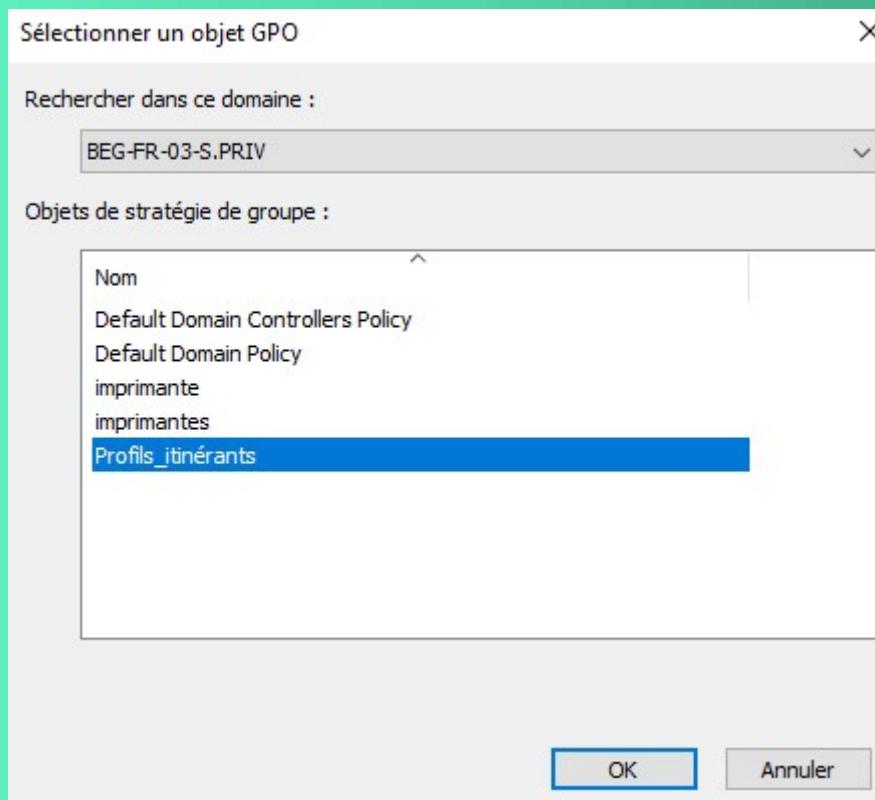
Vous pouvez fermer l'éditeur de stratégies et revenir sur la console de gestion des GPO. Si on jette un coup d'œil dans les paramètres de la GPO que l'on vient de créer, on voit bien ce qu'on a mis en place.



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 :

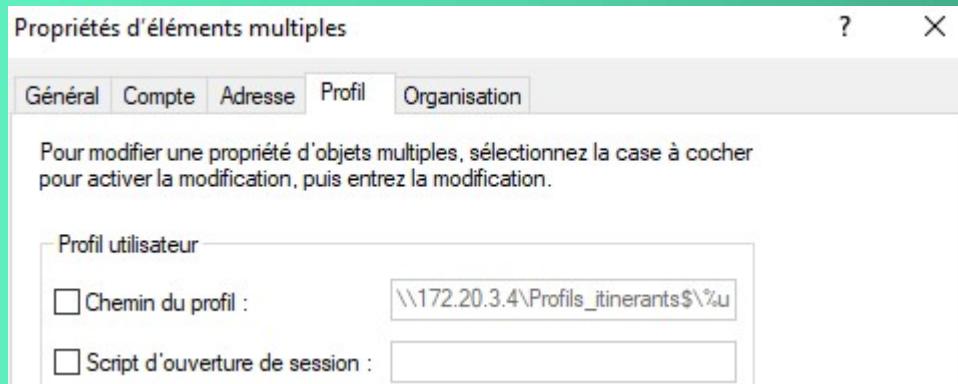
Retournons dans notre AD, faire un clic droit sur les utilisateurs que l'ont souhaite ajouté dans notre groupe puis faire un clic droit et 'ajouter à un groupe'

The screenshot shows the Windows Server 2012 Active Directory Users & Computers interface. On the left is a tree view of the directory structure under 'Utilisateurs et ordinateurs Active'. A context menu is open over a list of user accounts on the right. The menu items include: Ajouter à un groupe... (highlighted in blue), Désactiver le compte, Activer le compte, Déplacer..., Ouvrir la page de démarrage, Envoyer un message, Toutes les tâches >, Couper, Supprimer, Propriétés, and Aide.

Nom	Type	Description
GPO	Unité d'organis...	
Imprimantes	Unité d'organis...	
Admin	Utilisateur	
AUMIS Barth...	Utilisateur	
AZZOUG Ma...	Utilisateur	
BAHANI Issa...	Utilisateur	
BARNIER Cle...	Utilisateur	
BASSOUMB...	Utilisateur	
BELARBI Val...	Utilisateur	
BILLOT Adele	Utilisateur	
BLANDIN Re...	Utilisateur	
BOLIVARD T...	Utilisateur	
BOUCHETTE...	Utilisateur	
BOUSSON R...	Utilisateur	
BREUGNOT I...	Utilisateur	
BRUNEAU C...	Utilisateur	
CAILLOT Ste...	Utilisateur	
CAMBERVEL...	Utilisateur	
CAMUS PETI...	Utilisateur	
CANY Charl...	Utilisateur	
CARREAU C...	Utilisateur	
CHATELIN E...	Utilisateur	
CHOLLET Ro...	Utilisateur	
CLAIRET Juli...	Utilisateur	
CLEMENTE E...	Utilisateur	
COLOMIER ...	Utilisateur	
COUSIN Gab...	Utilisateur	

This screenshot shows the 'Membre de:' properties dialog box for a group object. It lists three entries: 'Nom' (Name) is 'Dossier Services de domaine Active Directory'; 'Profils_itinérants' (highlighted in blue) is 'BEG-FR-03-S.PRIV/GPO'; and 'Utilisateurs du do...' (Users of the do...) is 'BEG-FR-03-S.PRIV/Users'.

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



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

[\\172.20.3.4\Profils_itinerants\\$\%username%](\\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 :

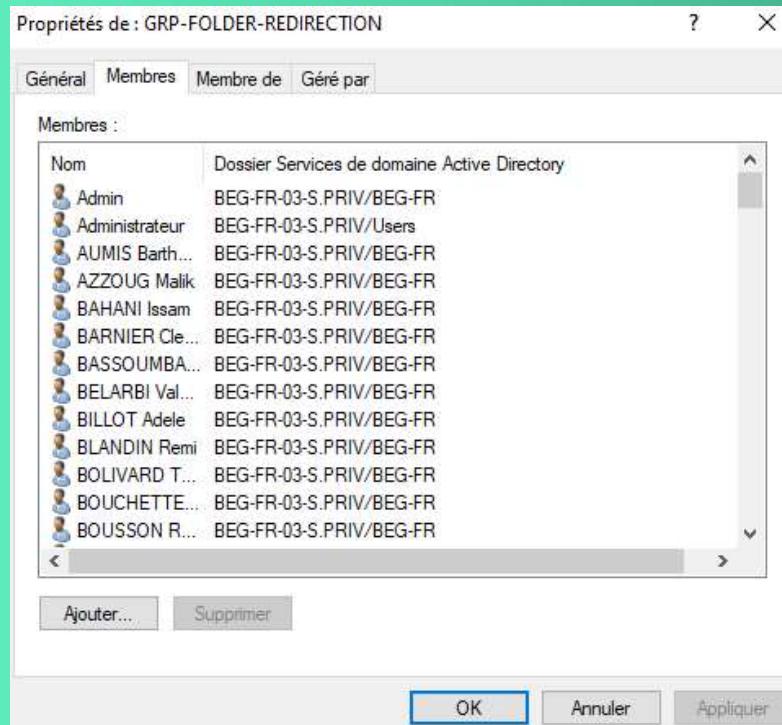
Nous allons créer le groupe de sécurité "GRP-FOLDER-REDIRECTION" avec la commande suivante :
 New-ADGroup -Name "GRP-FOLDER-REDIRECTION" -SamAccountName "GRP-FOLDER-REDIRECTION"
 ` -GroupCategory Security -GroupScope DomainLocal ` -Description "Utilisateurs ayant un profil
 redirigé"

```
Administrator : 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 :

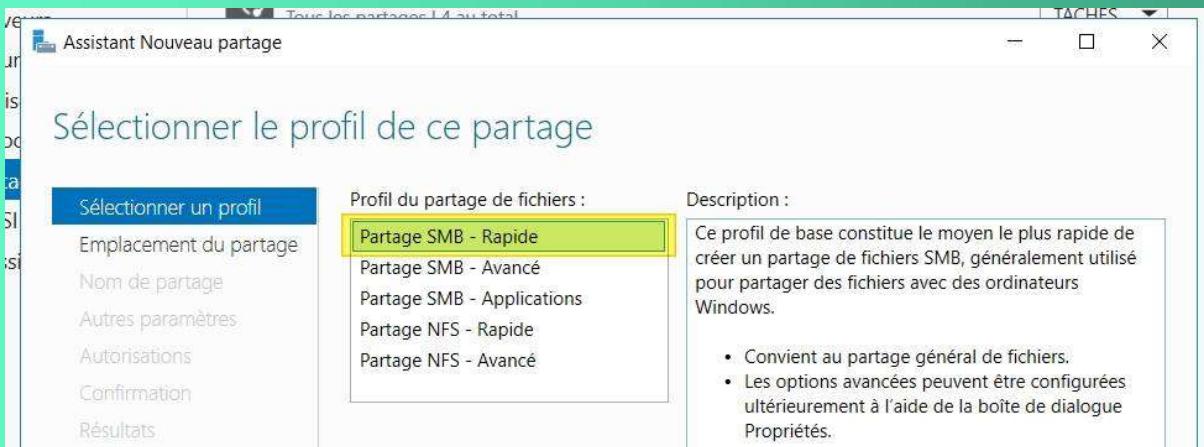


Le partage et attribution des droits :

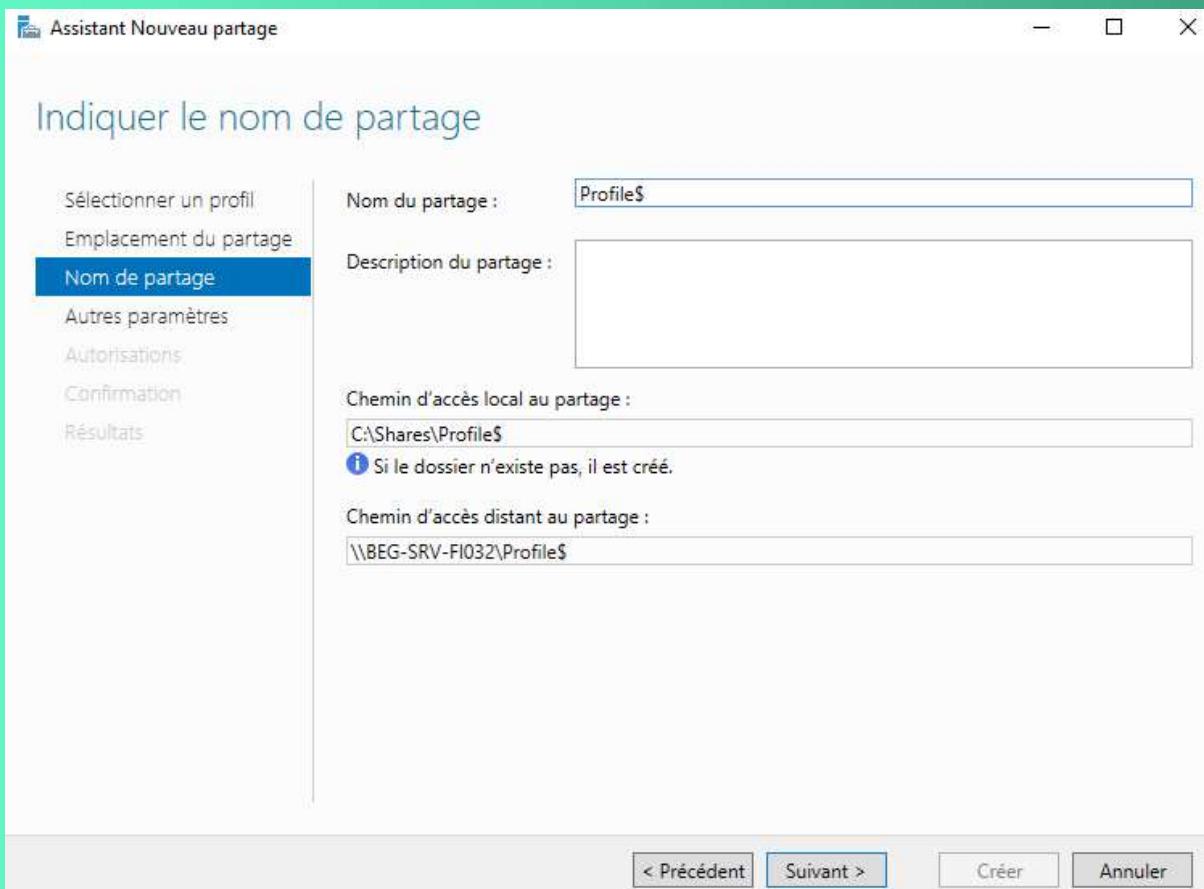
Dans la console "Gestionnaire de serveur", accédez à "Services de fichiers et de stockage" (vous devez installer la fonctionnalité) et ensuite créez un nouveau partage, comme ceci :

Partager	Chemin d'accès local	Protocole	Type de disponibilité
▲ BEG-SRV-AD032 (3)			
BEG	C:\BEG	SMB	Non-cluster
NETLOGON	C:\Windows\SYSVOL\sysvol\BEG...	SMB	Non-cluster
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Non-cluster
▲ BEG-SRV-FI032 (3)			
print\$	C:\Windows\system32\spool\driv...	SMB	Non-cluster
PRIVATE	C:\PRIVATE	SMB	Non-cluster
SauvegardeAD	C:\SauvegardeAD	SMB	Non-cluster

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



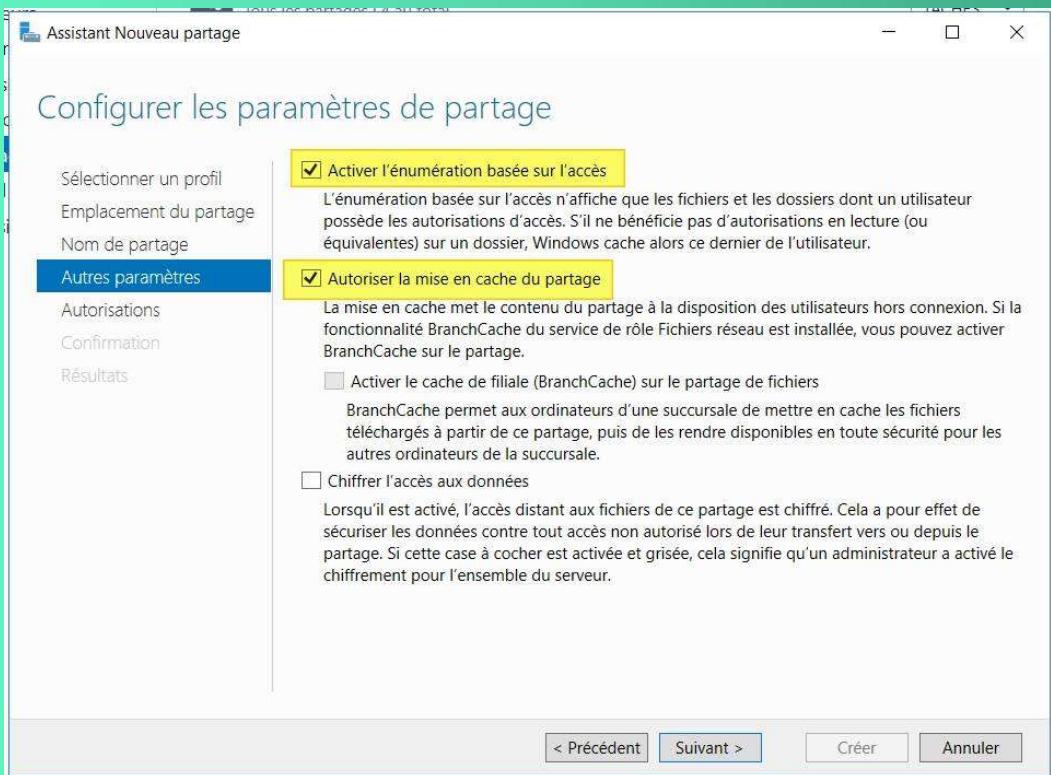
Donnez un nom à votre partage, par exemple : PrProfilsofiles\$. Ce partage étant sensible et qu'il n'y a pas lieu d'y accéder en direct, notamment via la découverte réseau, je vous recommande de mettre un "\$" à la fin du nom pour qu'il soit masqué un minimum.



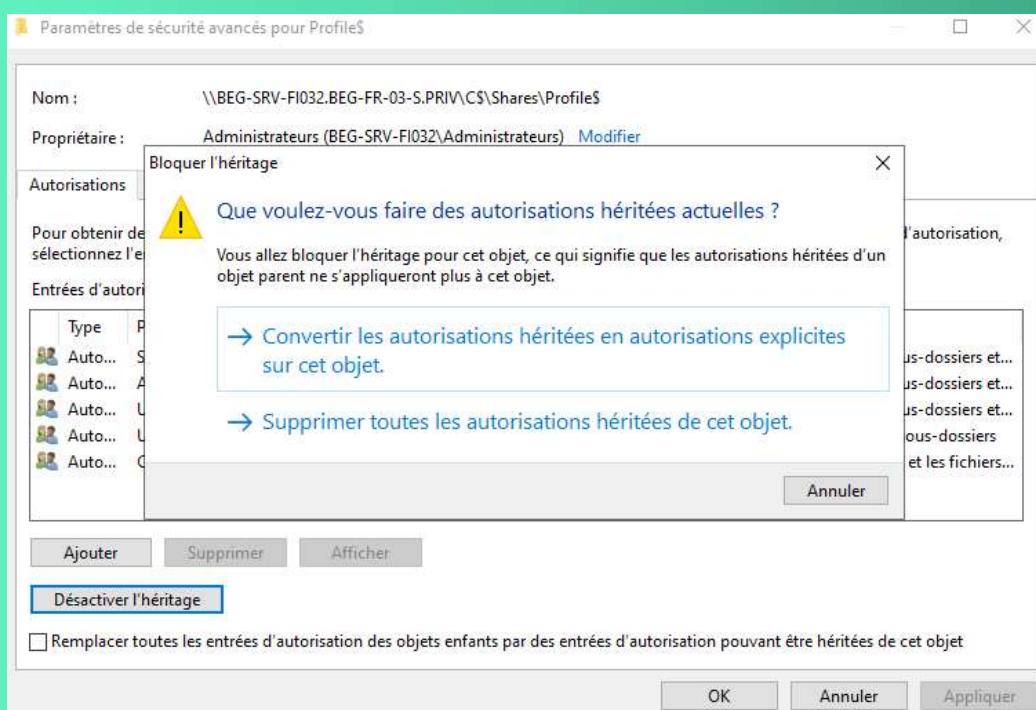
Deux options sont à activer sur cette page :

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 configuez 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
- Parcours du dossier/exécuter le fichier
- Liste du dossier/lecture de données
- Attributs de lecture
- Lecture des attributs étendus
- Création de fichier/écriture de données
- Crédit 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\C\$\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 :

The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console. On the left, under 'Forêt : BEG-FR-03-S.PRIV', a new GPO named 'FOLDER_REDIRECTION' is being created. On the right, the 'FOLDER_REDIRECTION' GPO properties window is open, showing the 'Liaisons' (Links) tab where 'BEG-FR' is listed. Below it, the 'Filtrage de sécurité' (Security Filtering) section shows that the GPO applies only to the group 'GRP-FOLDER-REDIRECTION'.

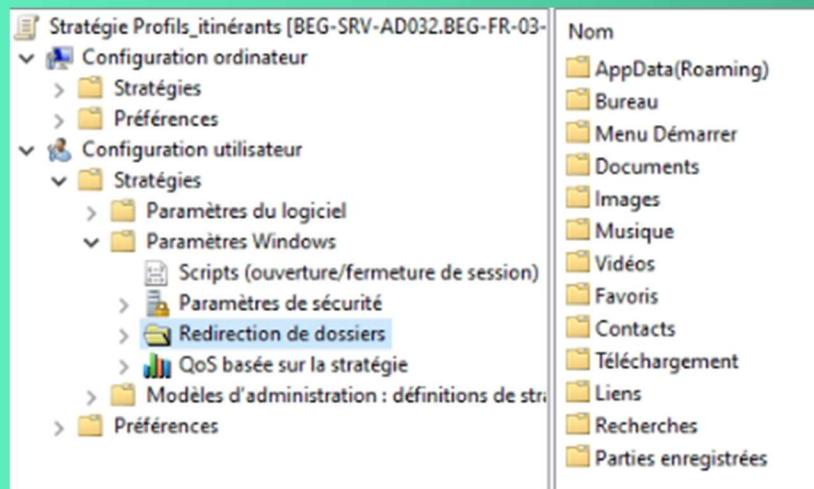
Suite à une mise à jour publiée par Microsoft (MS16-072), il y a eu des changements au niveau de la sécurité et pour que la redirection de profils fonctionne, vous devez ajouter le groupe "Utilisateurs authentifiés" en "Lecture" dans l'onglet "Délégation" :

The screenshot shows the 'Délégation' tab in the 'FOLDER_REDIRECTION' GPO properties window. It lists several groups and users with their permissions. The 'Utilisateurs authentifiés' group is highlighted with a yellow background and has 'Lecture' (Read) permission assigned.

Nom	Autorisations acceptées	Hérité
Administrateurs de l'entreprise (IT-CONNECT\Administrateurs ...)	Modifier les paramètres, supprimer, modifier la sécurité	Non
Admins du domaine (IT-CONNECT\Admins du domaine)	Modifier les paramètres, supprimer, modifier la sécurité	Non
ENTERPRISE DOMAIN CONTROLLERS	Lecture	Non
GRP-FOLDER-REDIRECTION (IT-CONNECT\GRP-FOLDER-REDIREC ...)	Lecture (à partir du filtrage de sécurité)	Non
Système	Modifier les paramètres, supprimer, modifier la sécurité	Non
Utilisateurs authentifiés	Lecture	Non

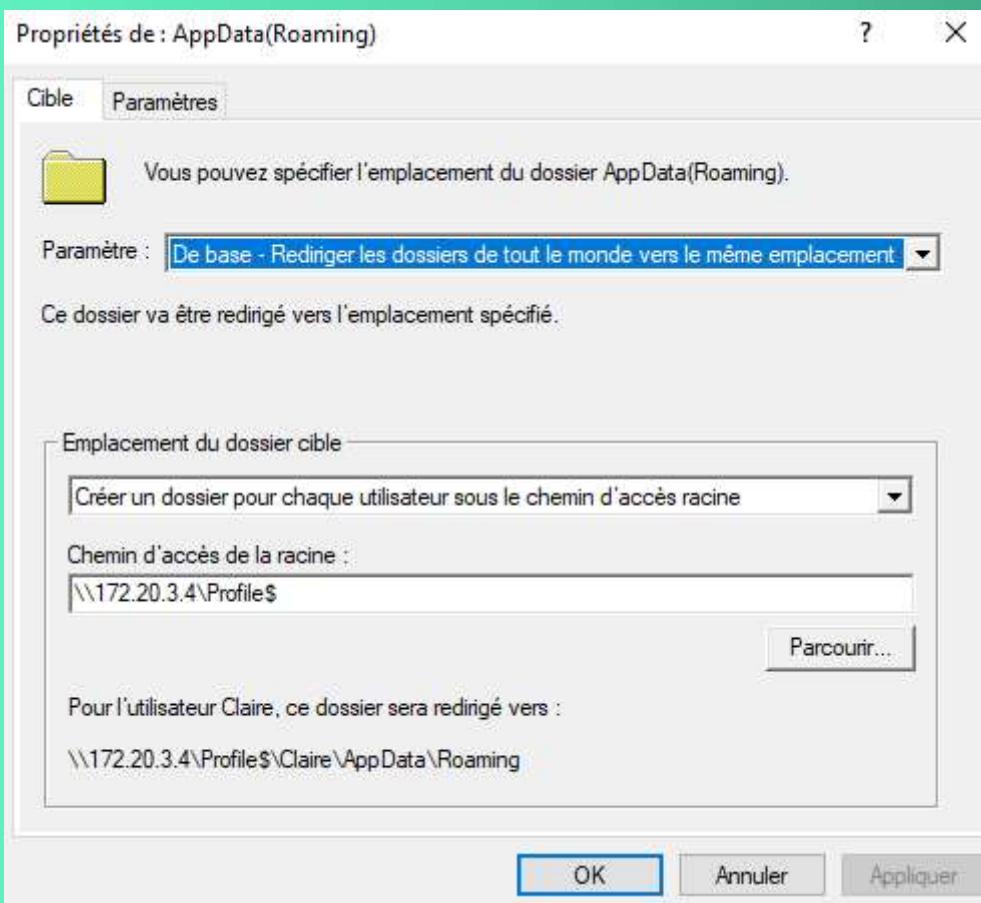
Ensuite, modifiez la GPO pour configurer la redirection de dossiers. Ce paramètre s'applique directement au niveau de l'utilisateur : Configuration utilisateur > Stratégies > Paramètres Windows > Redirection de dossiers

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



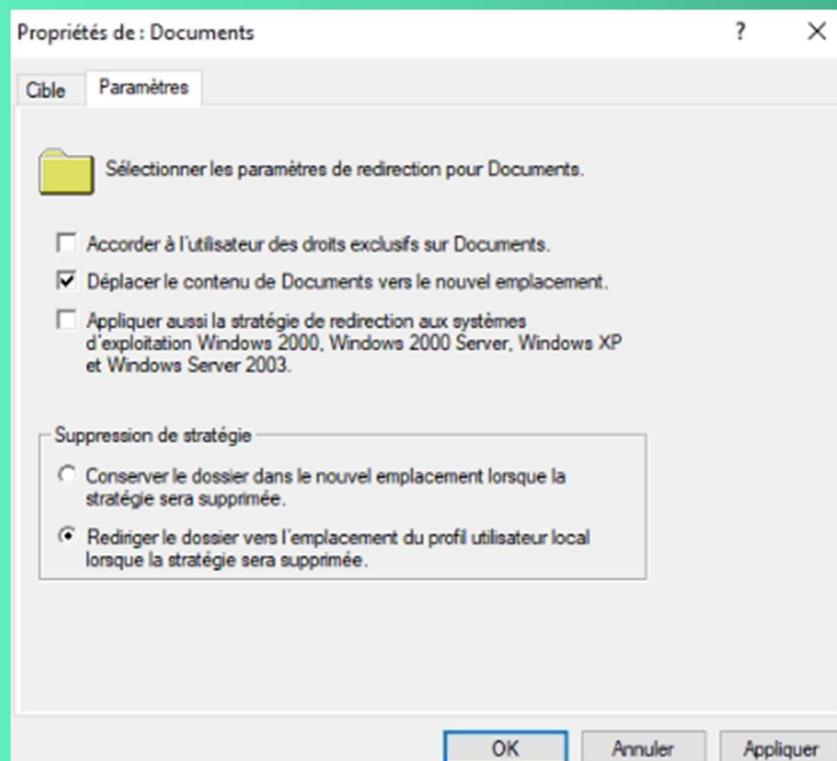
Choisissez l'option "Créer un dossier pour chaque utilisateur le chemin d'accès racine", ce qui rejoins ce que je disais précédemment : à la racine du partage des profils, un dossier va être créé pour l'utilisateur et dans ce dossier, il y aura un dossier "Documents".

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



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

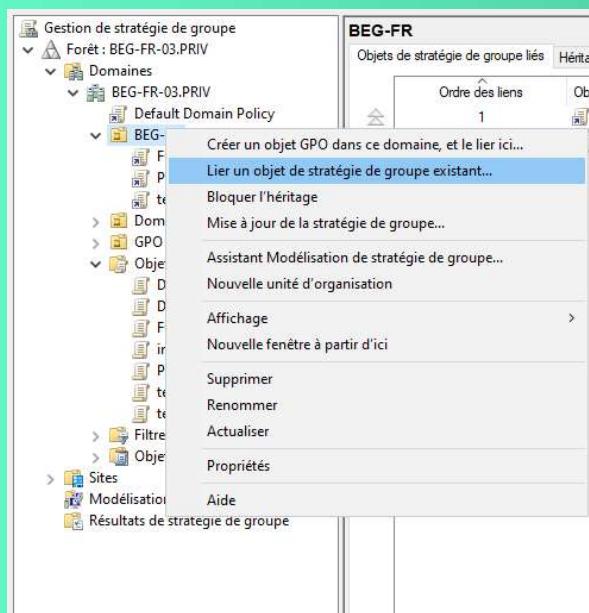
Si vous souhaitez empêcher le compte administrateur d'accéder au dossier et qu'il y ait seulement l'utilisateur qui puisse accéder, alors cochez l'option "Accorder à l'utilisateur des droits exclusifs sur Documents".



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

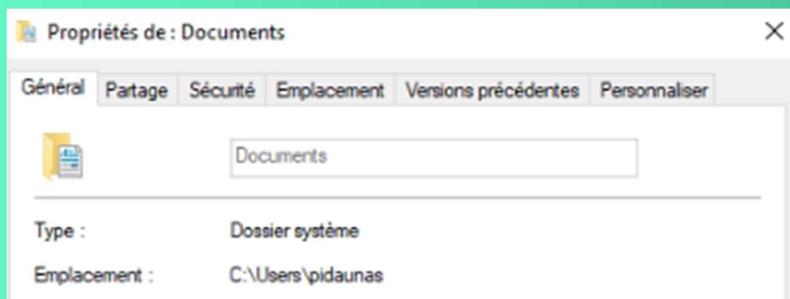
Vous pouvez valider, fermer l'éditeur de GPO et pensez à lier votre GPO sur votre domaine avant de passer à la phase de tests.

Mettre dans "Gestion de stratégie de groupe" la GPO "FOLDER_REDIRECTION"



Test de redirection de dossiers :

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



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

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

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

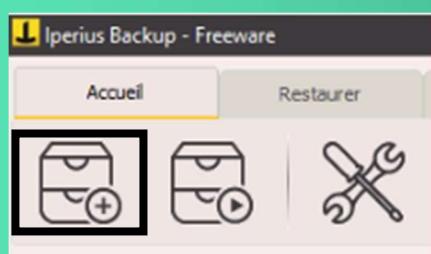
CONFIGURATION DE IPERIUS

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

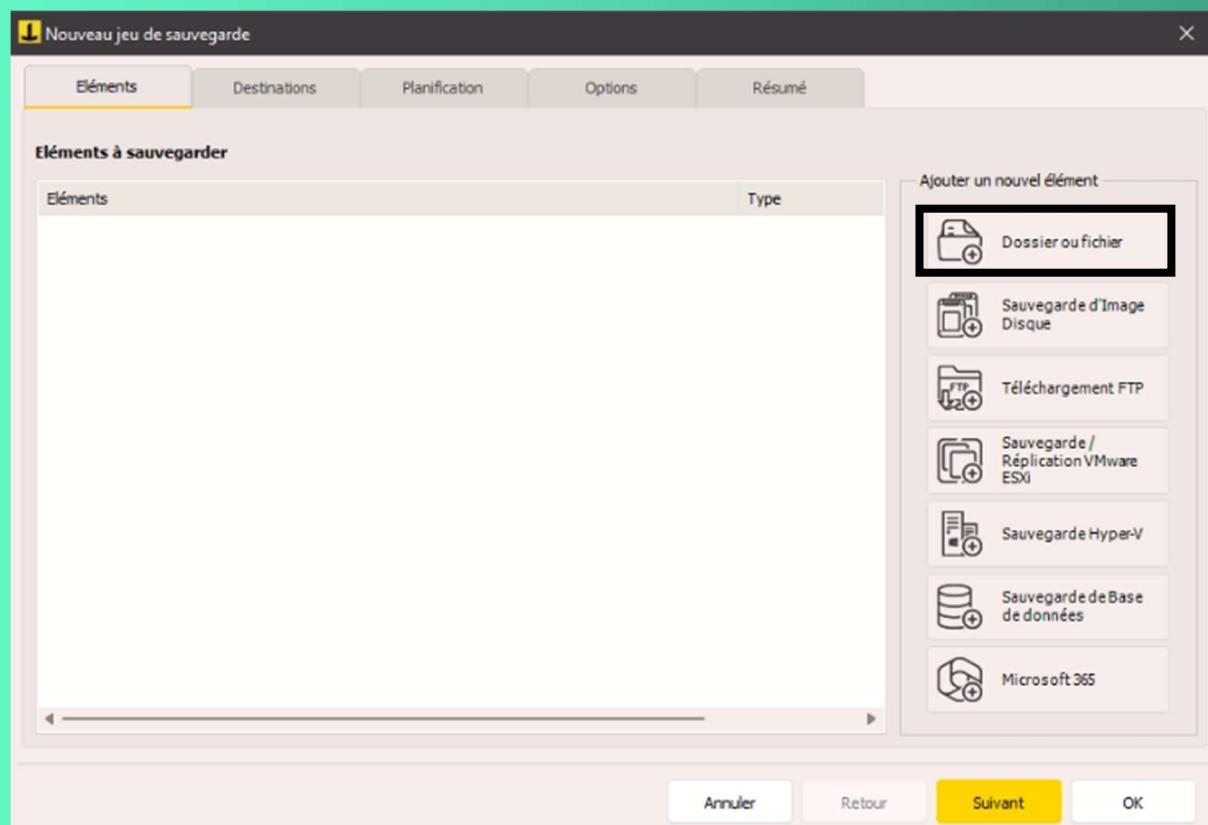
<https://www.iperiusbackup.fr/>

Créer une sauvegarde :

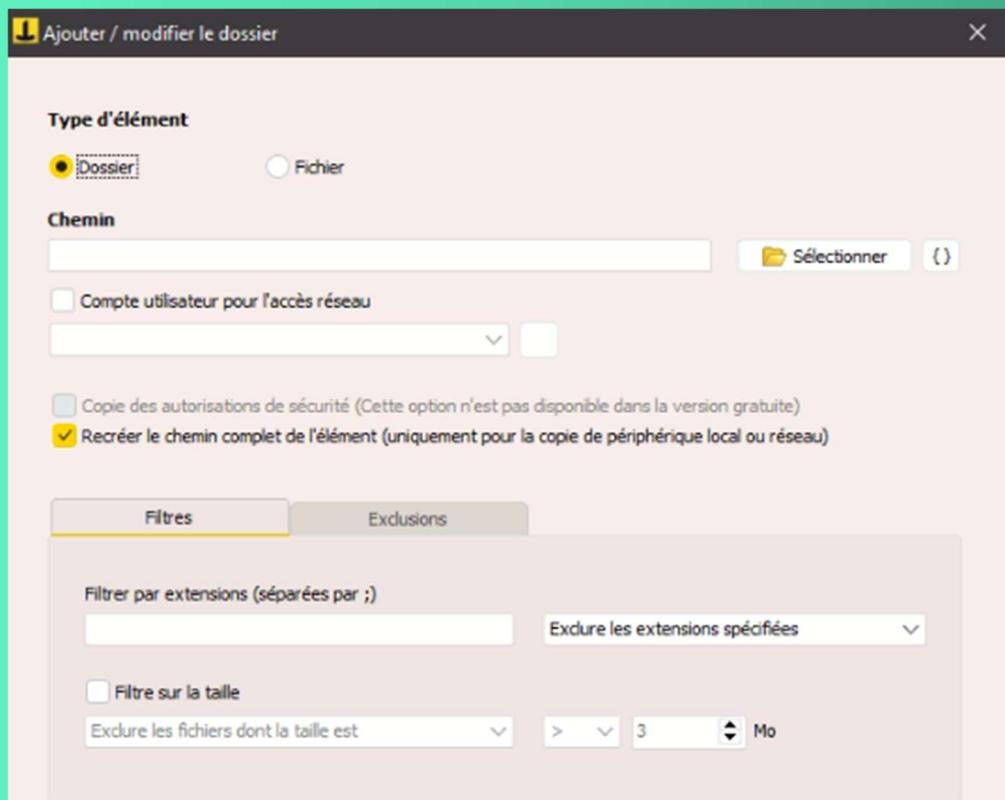
Pour créer une sauvegarde sur Iperius, il faut cliquer sur 'créer un nouveau jeu de sauvegarde'



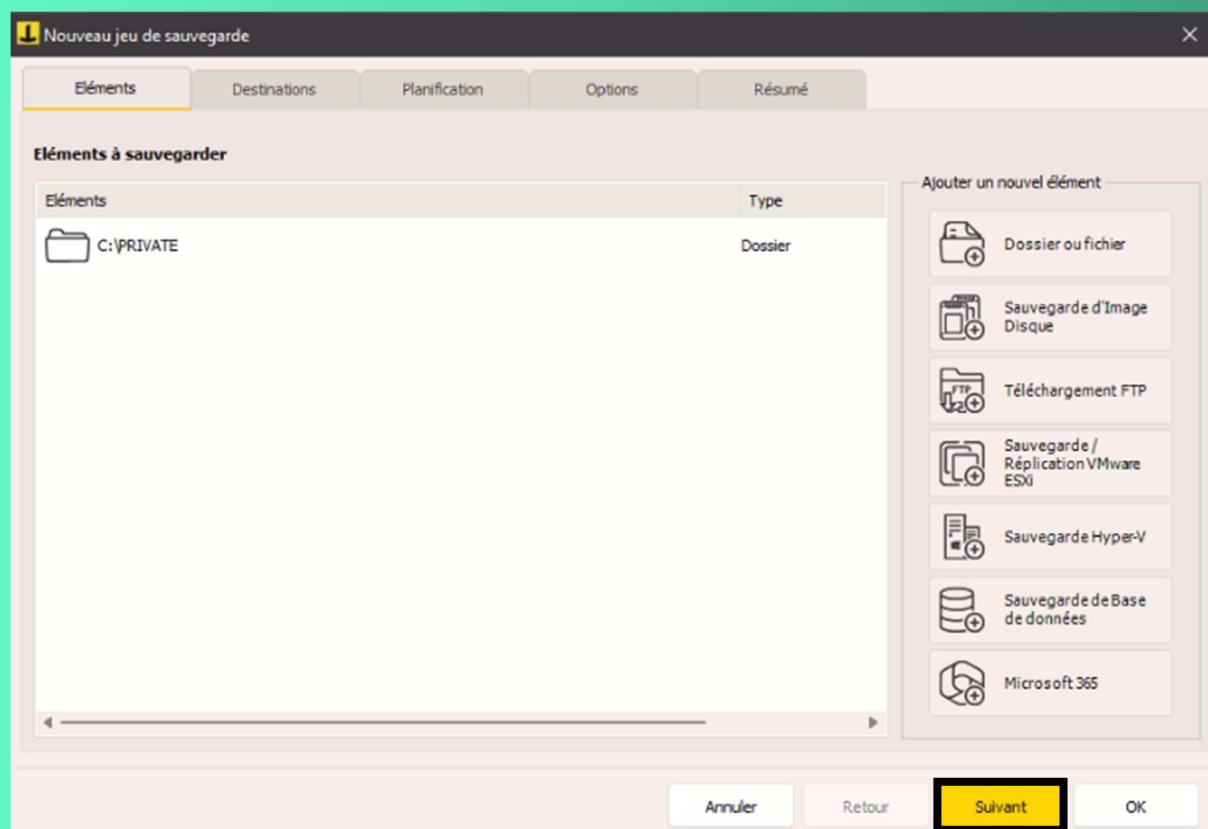
Ensuite, sélectionner le nouvel élément de sauvegarde en fonction de ce que nous voulons sauvegarder. Dans notre cas, nous avons sauvegardé un dossier :



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

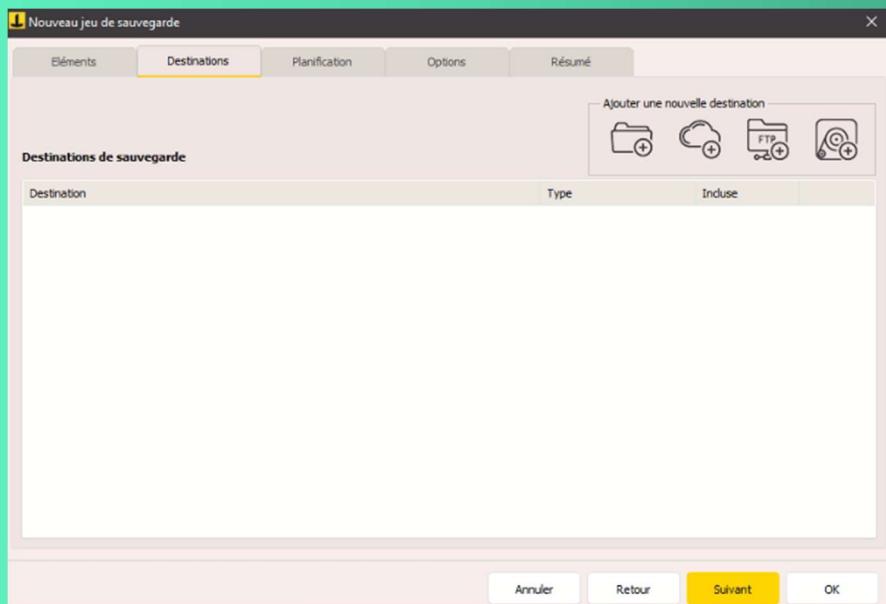


Maintenant que le chemin de notre dossier private à sauvegarder est créé, cliquer sur ‘suivant’

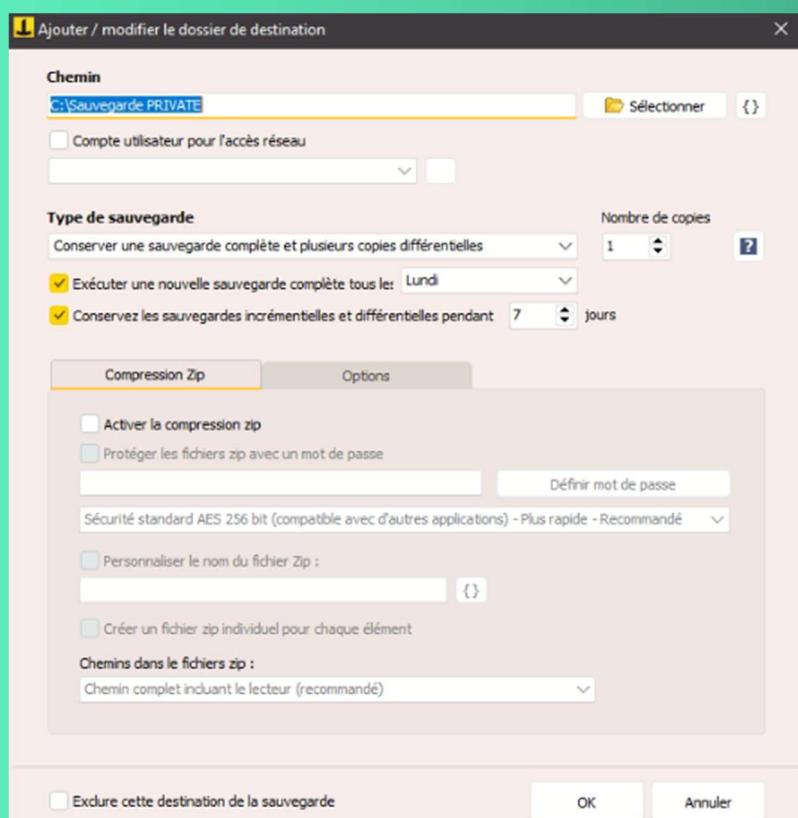


Choisir le dossier de sauvegarde :

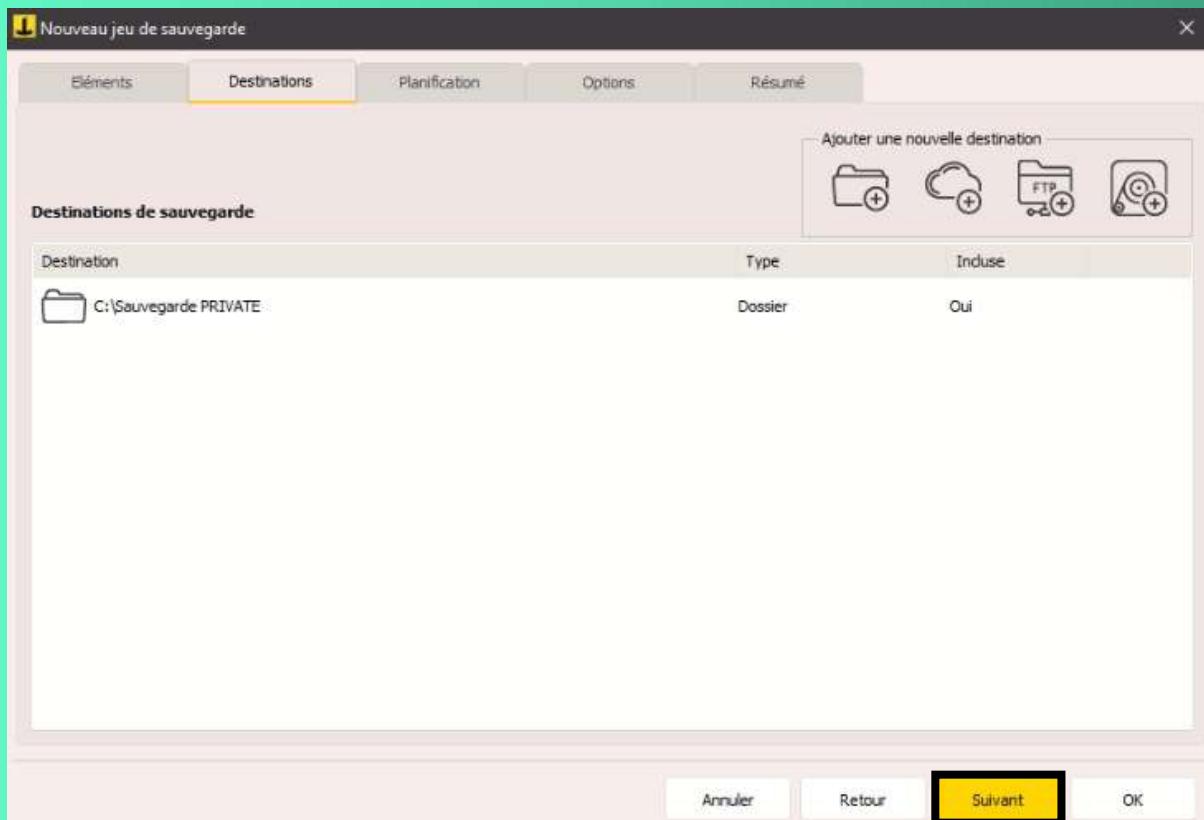
Pour choisir un dossier ou la sauvegarde sera enregistrer, cliquer sur ‘Ajouter un dossier de destination’, il est aussi possible de faire une sauvegarde sur le cloud, sur un serveur FTP ou alors une bande



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

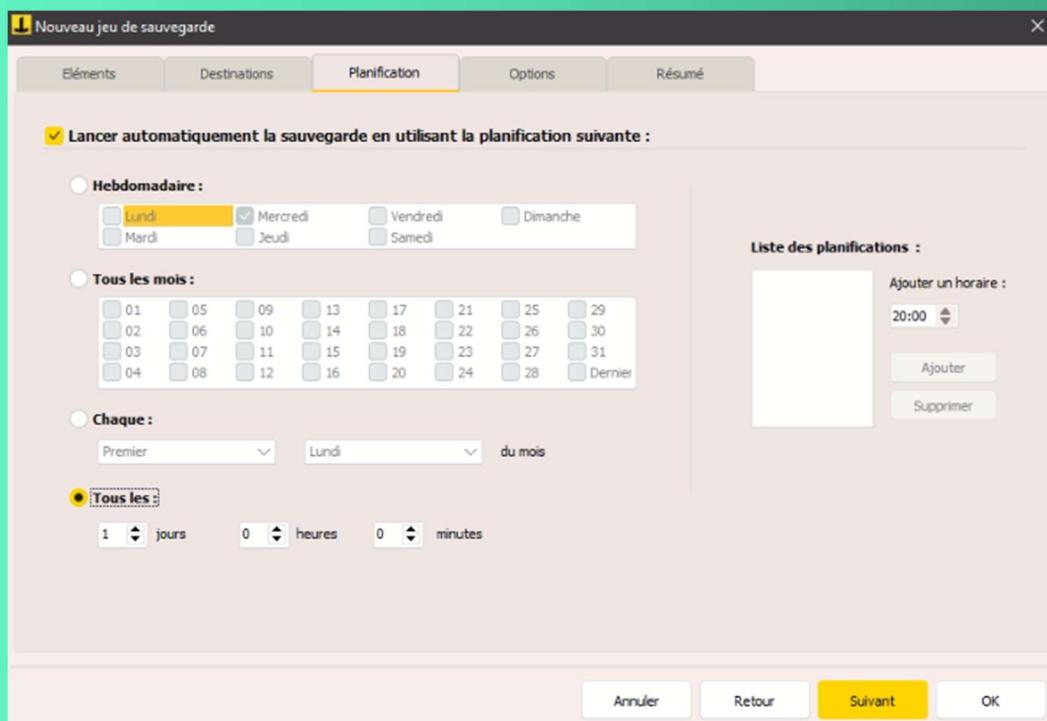


Maintenant que le chemin du dossier de sauvegarde est créé, cliquer sur ‘suivant’



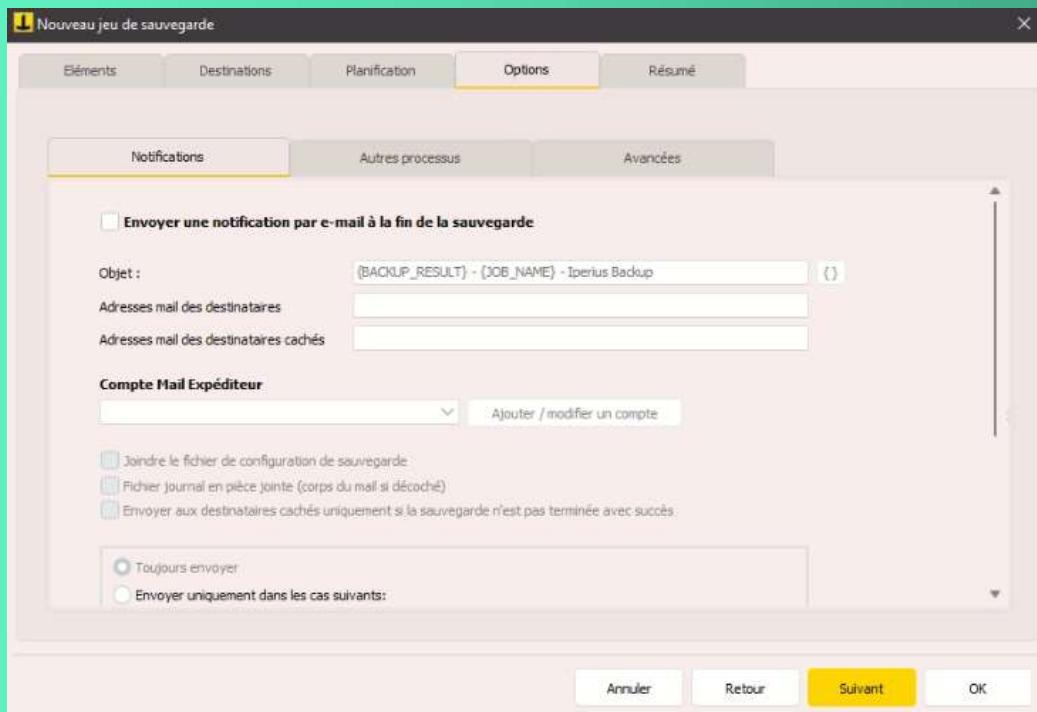
Planification :

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



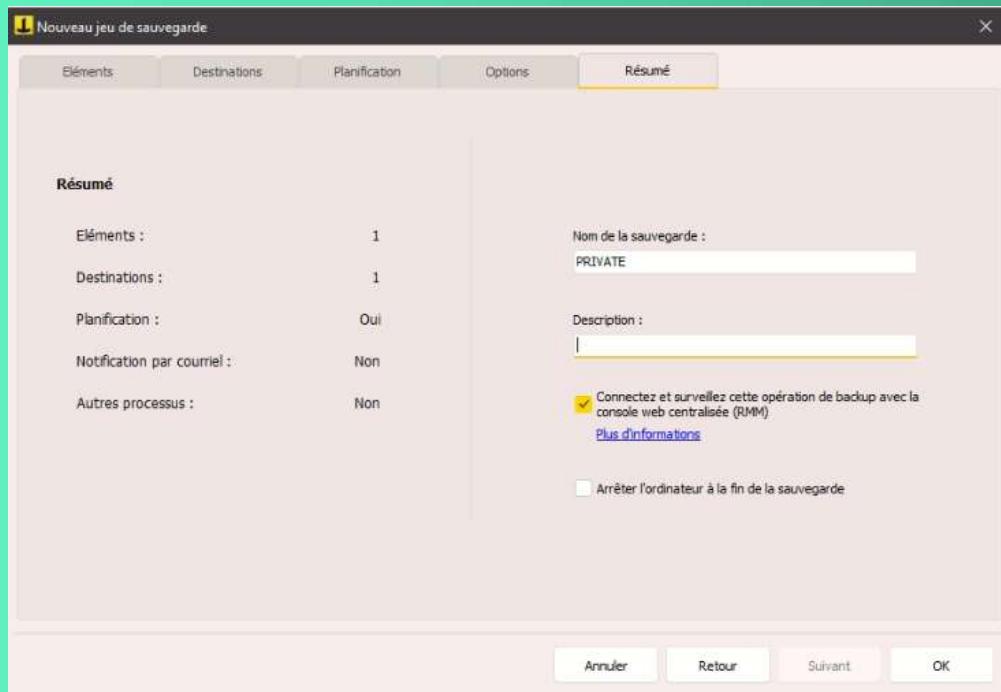
Options :

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



Résumé :

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



Test de la sauvegarde :

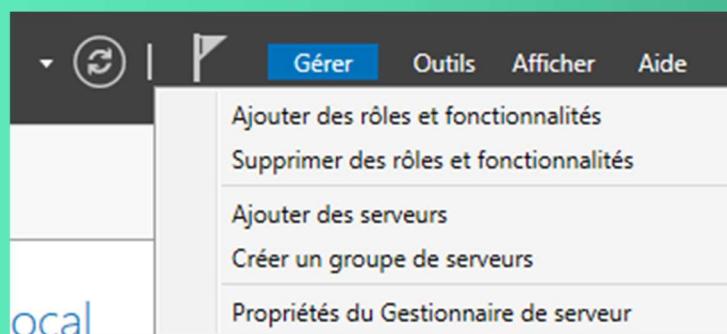
Pour tester la sauvegarde, faire un clic droit et 'lancer la sauvegarde'

CONFIGURATION DU SERVEUR

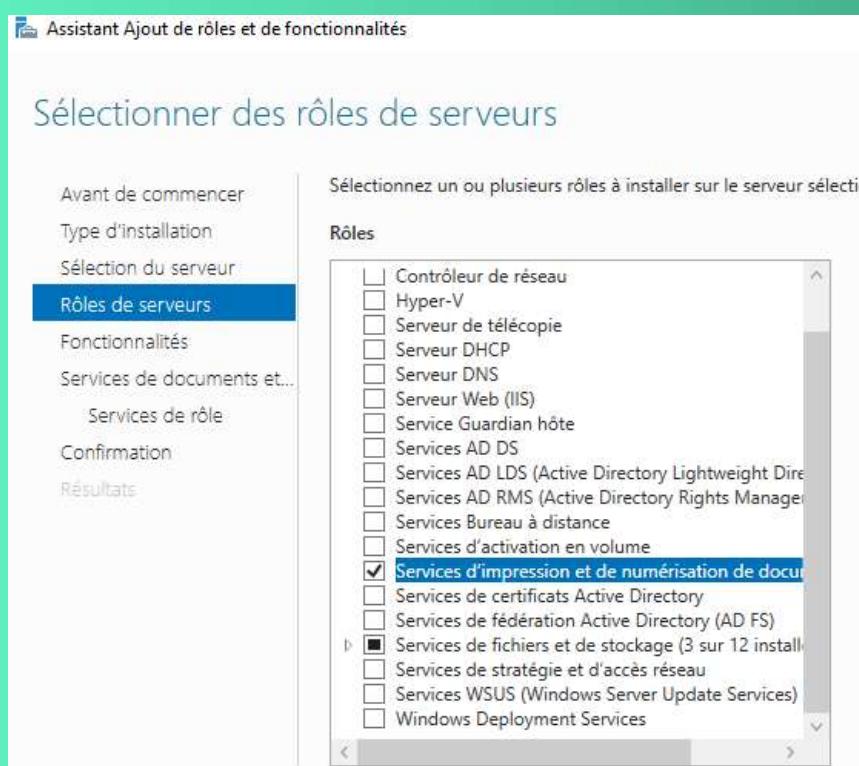
D'IMPRESSION

Installation du service :

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

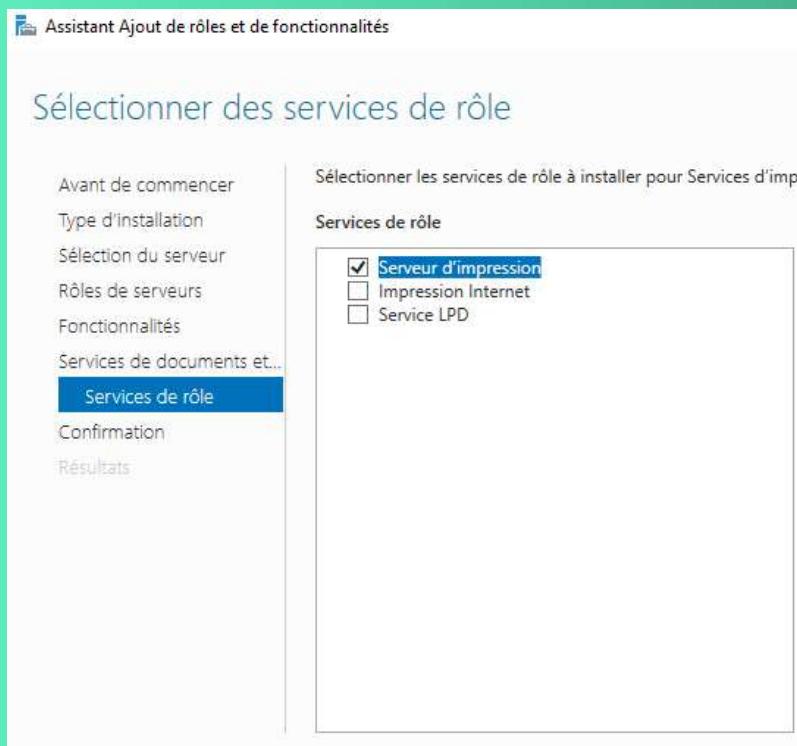


Passez les premières étapes, sélectionnez le rôle 'Services d'impression et de numérisation de documents'



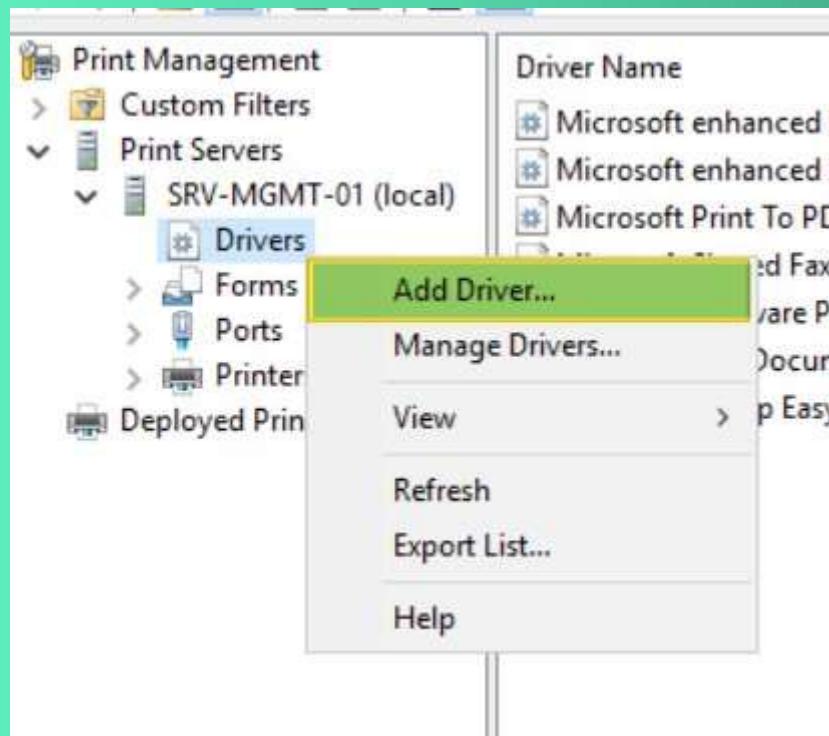
Au niveau des rôles du service d'impression, cochez à minima "Server d'Impression" qui est le serveur d'impression de base. Si vous envisagez de réaliser des impressions depuis des périphériques

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

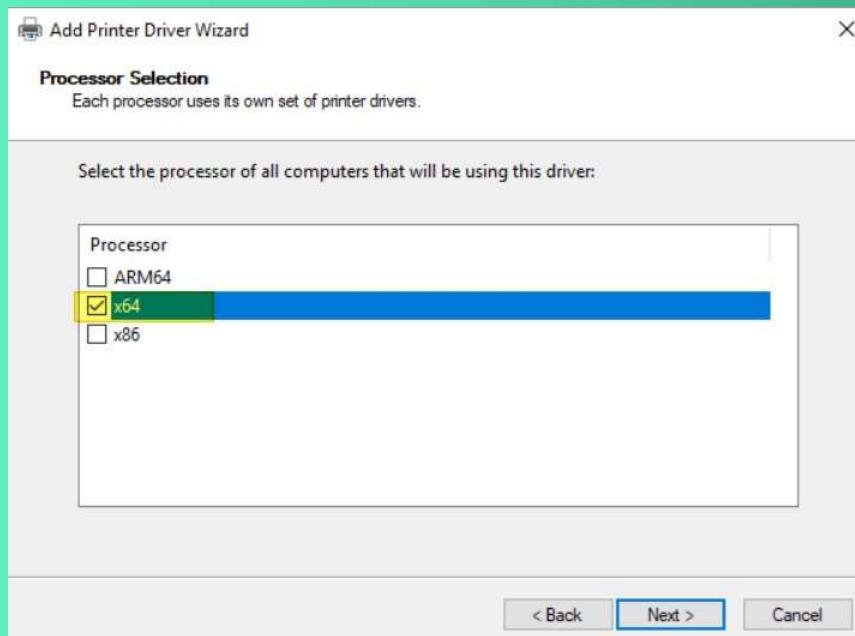


Ajouter un pilote d'impression :

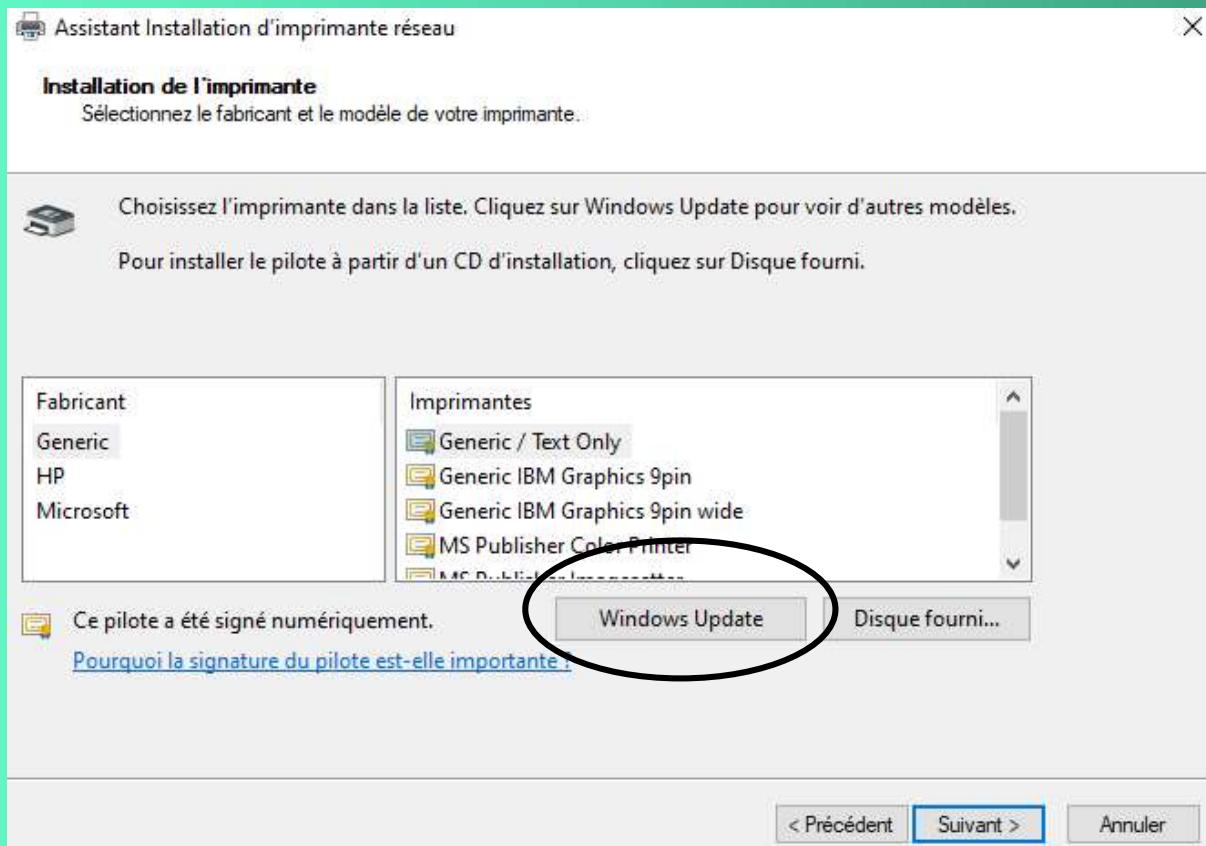
Pour commencer, nous allons donc importer notre pilote sur le serveur d'impression. Ce qui s'effectue de cette manière : Serveurs d'impression > nom de votre serveur > clic droit sur "Pilotes" et "Ajouter un pilote".



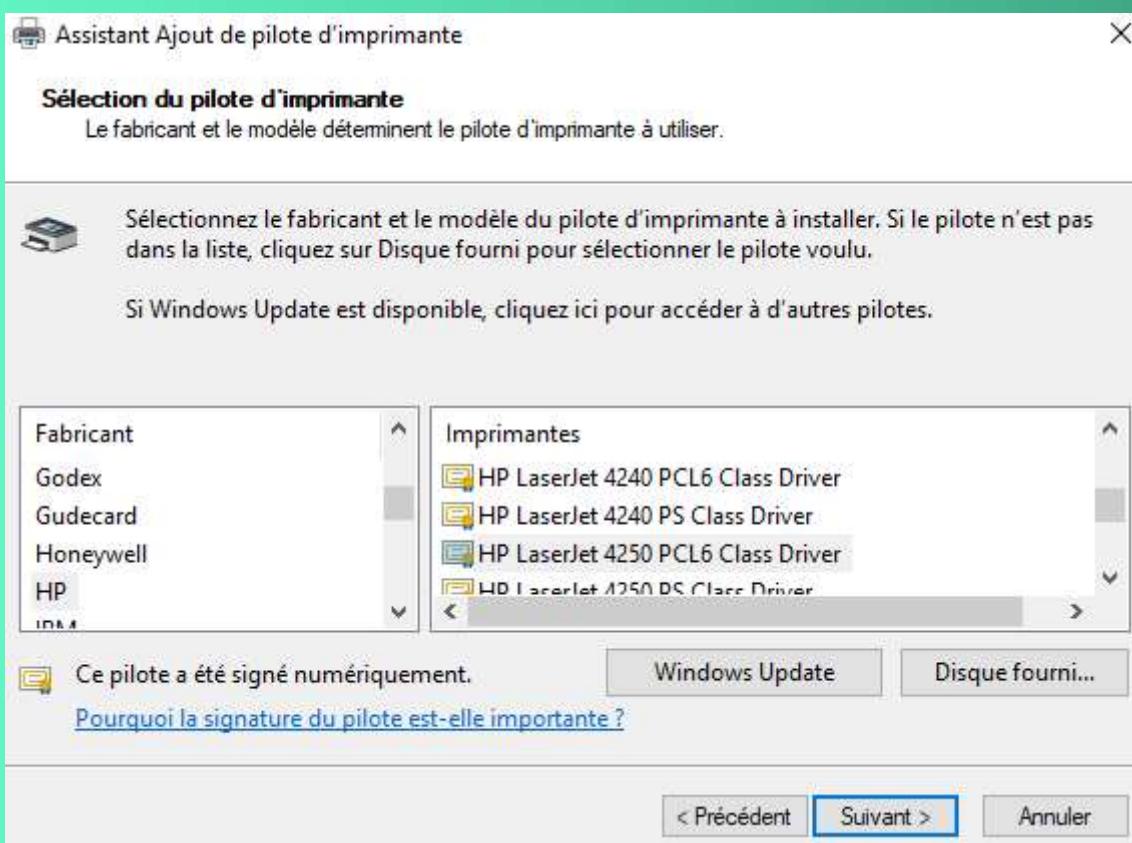
Sélectionnez les architectures processeurs compatibles avec le pilote que vous souhaitez importer.



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

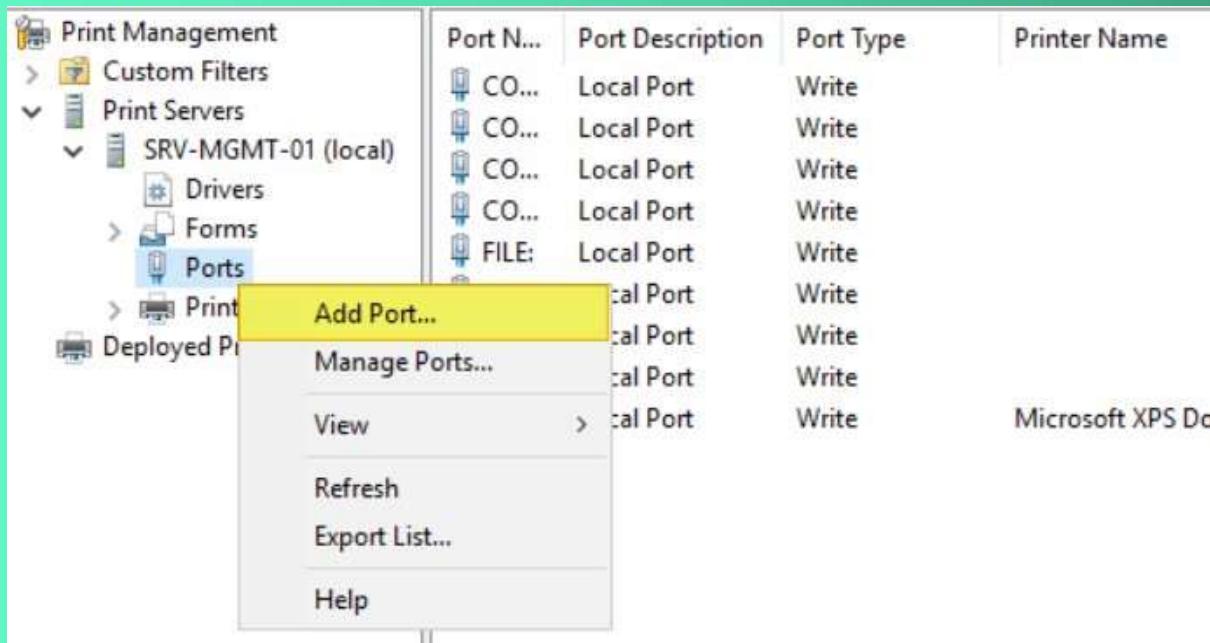


Ensuite, choisir le bon pilote, avec la marque et ensuite le modèle



Créer un port TCP/IP :

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



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



Remplissez le premier champ, nommé "Nom ou adresse IP de l'imprimante" en indiquant l'adresse IP de votre imprimante. Ensuite, donnez un nom à ce port en remplaçant 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 :

172.20.5.220

Nom du port :

172.20.5.220

< Précédent

Suivant >

Annuler

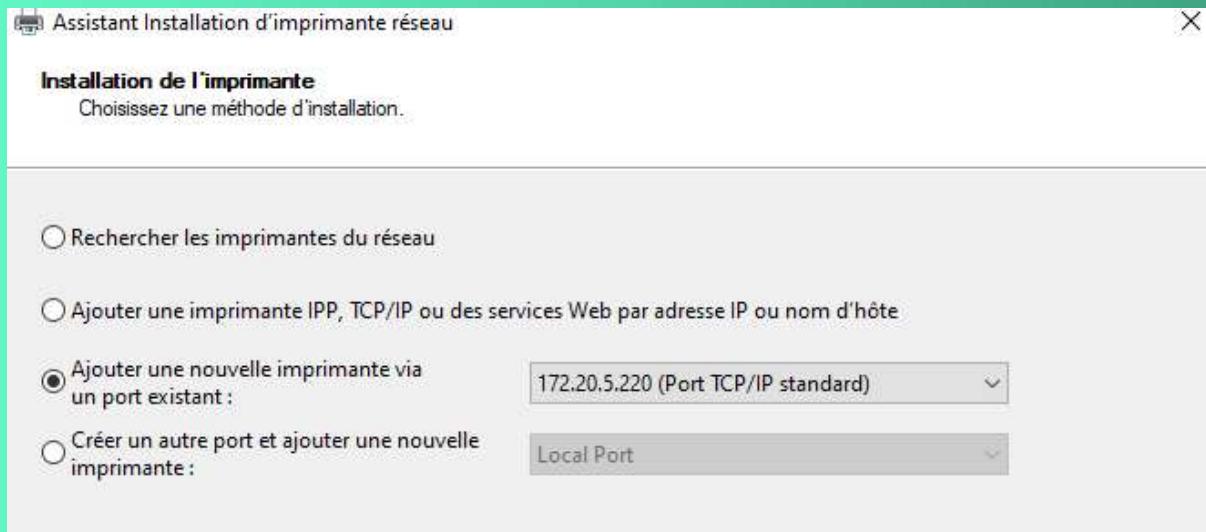
Ajouter l'imprimante à partager :

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

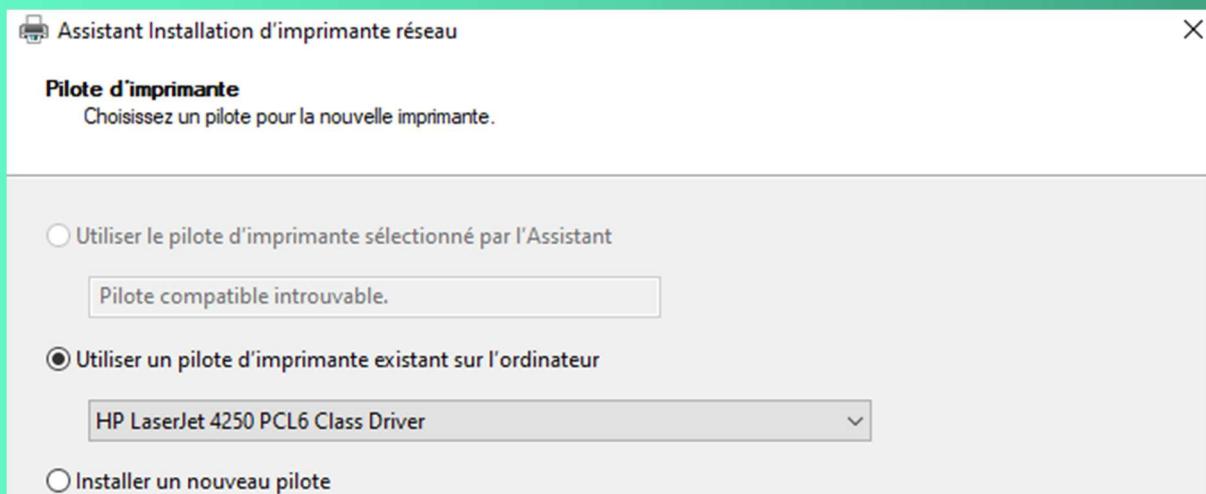
The screenshot shows the Windows Print Management console. On the left, there's a tree view with nodes like 'Gestion de l'impression', 'Filtres personnalisés', 'Serveurs d'impression' (with 'BEG-SRV-FI032 (local)' expanded), 'Pilotes', 'Formulaires', 'Ports', and 'Imprimantes'. A context menu is open over the 'Imprimantes' node, with 'Ajouter une imprimante...' highlighted in blue. The main pane displays a table of printers:

Nom de l'imprimante	Statut de la file...	Trava...	Nom du serveur	Nom du pilote
Microsoft Print to PDF	Prêt	0	BEG-SRV-FI032...	Microsoft Print T
Microsoft XPS Document Writer	Prêt	0	BEG-SRV-FI032...	Microsoft XPS D...

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



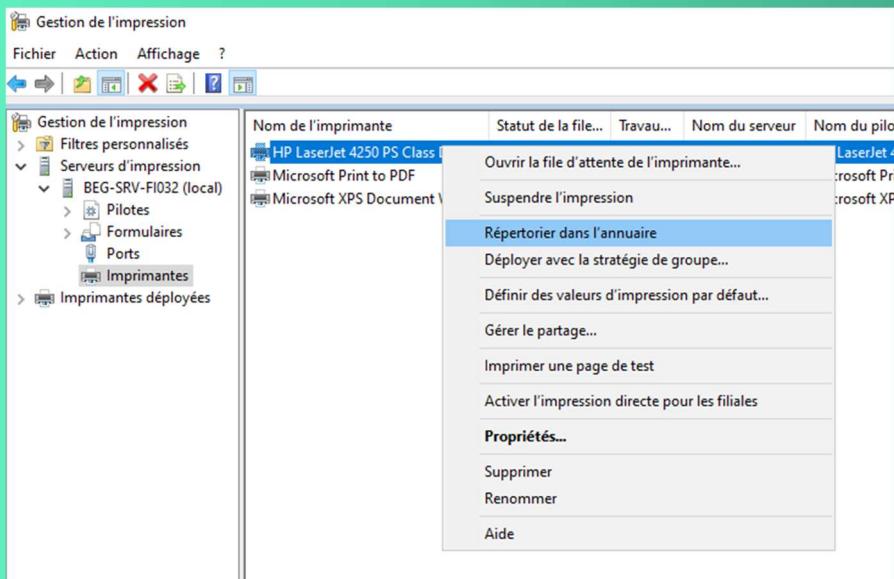
Sélectionner 'utiliser un pilote d'imprimante existant sur l'ordinateur'



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 :

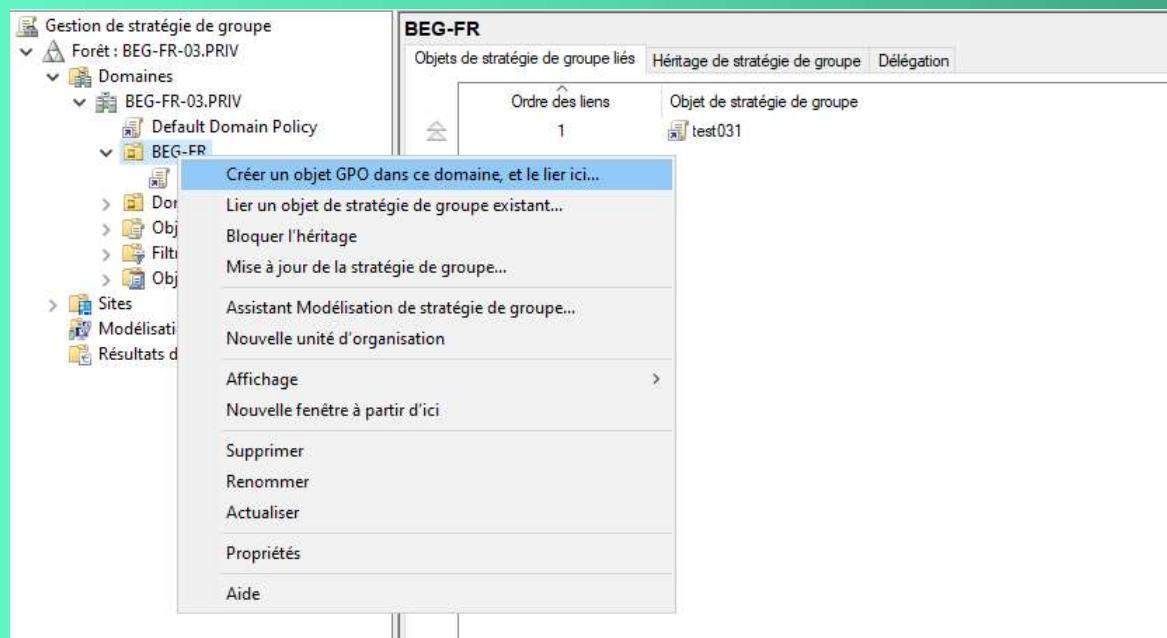
Répertorier l'imprimante dans l'annuaire :

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.

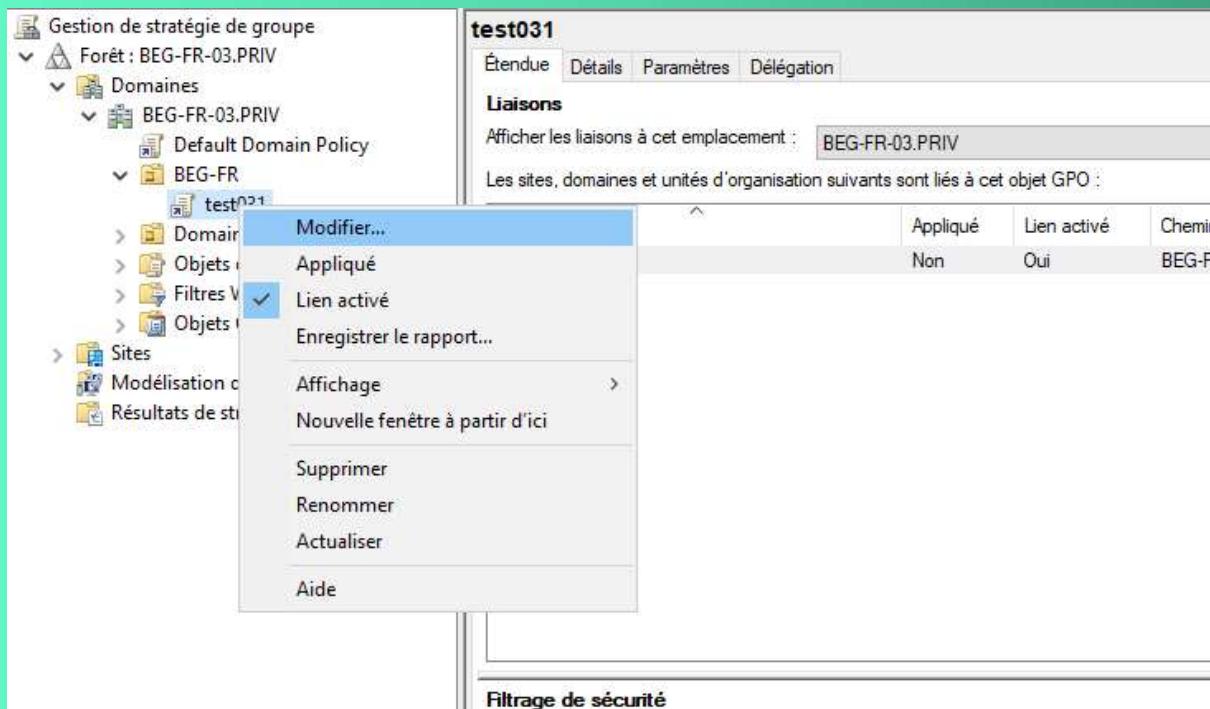


Création de la GPO :

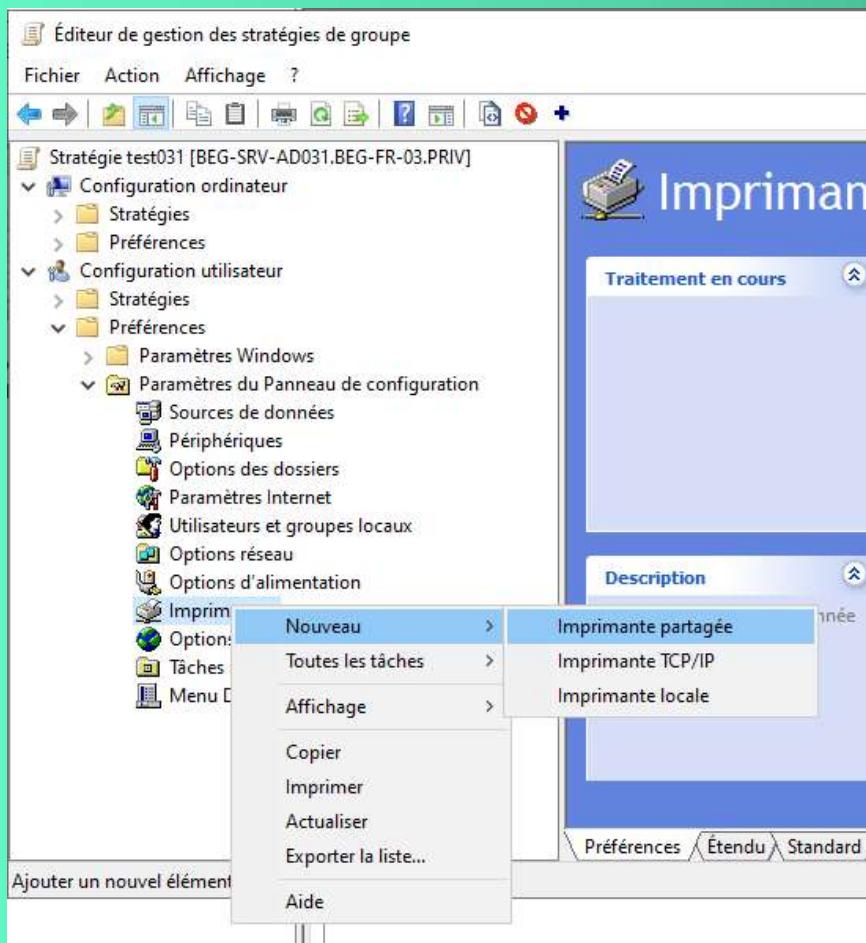
Création d'une GPO nommée 'imprimantes' en faisant clic droit sur une Unité d'Organisation



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

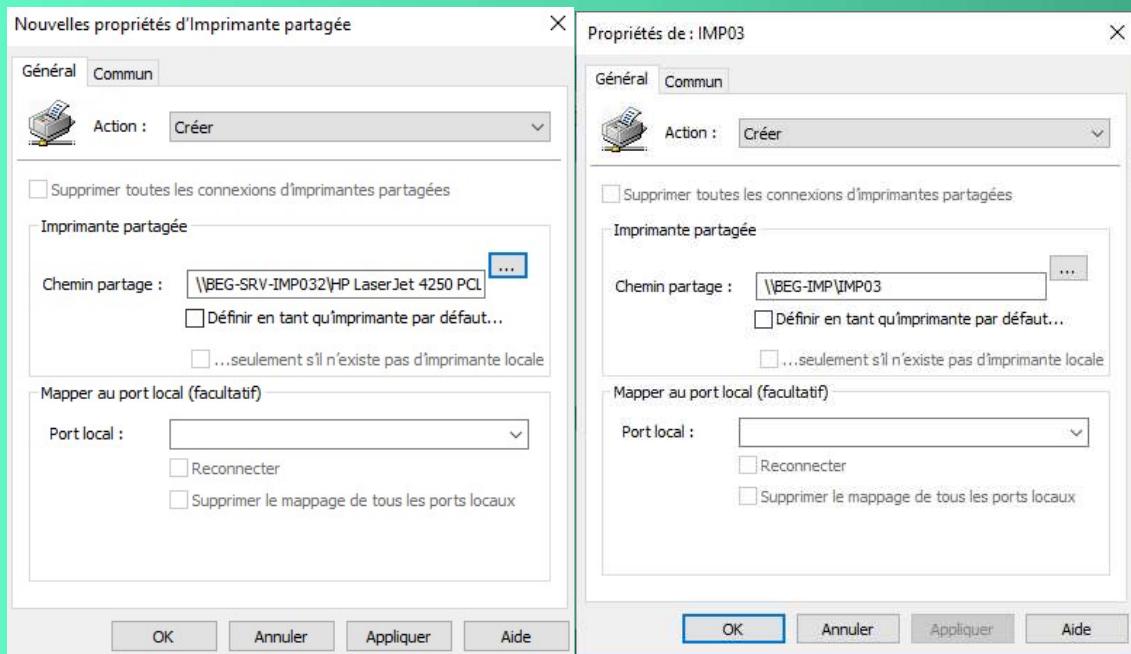


Ensuite, aller dans Configuration utilisateur > Préférences > Paramètres de Panneau de configuration > imprimantes puis faire un clic droit, nouveau et imprimante partagée



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.

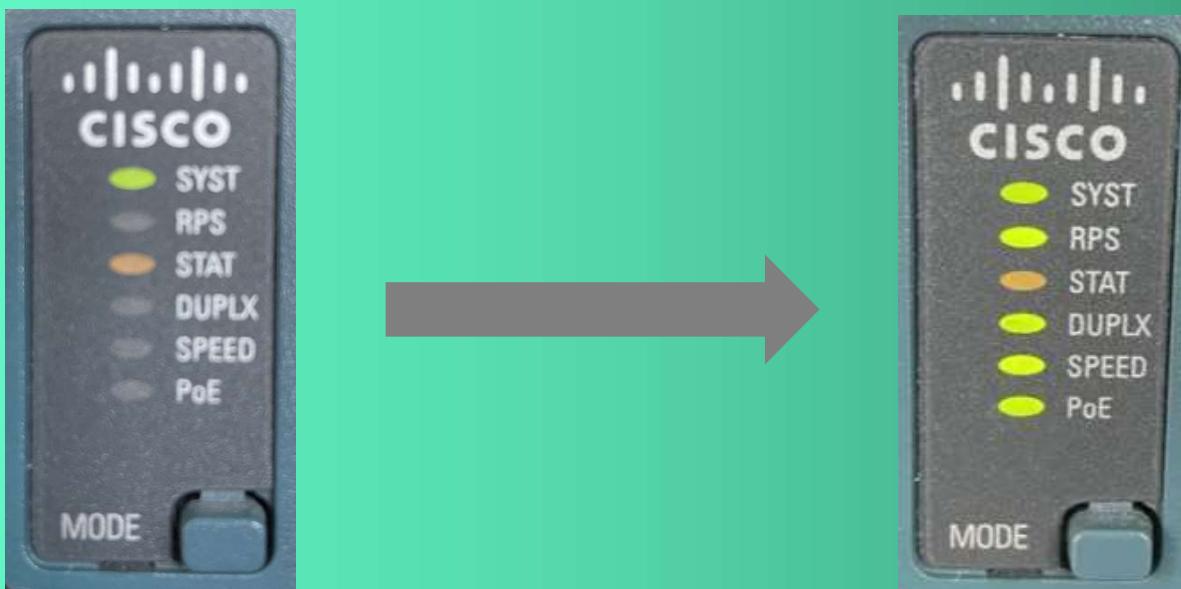
Configuration de l'adresse IP

- ➔ 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

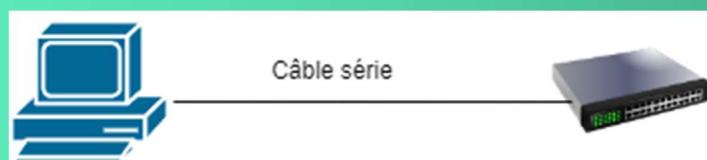
Procédure de réinitialisation :

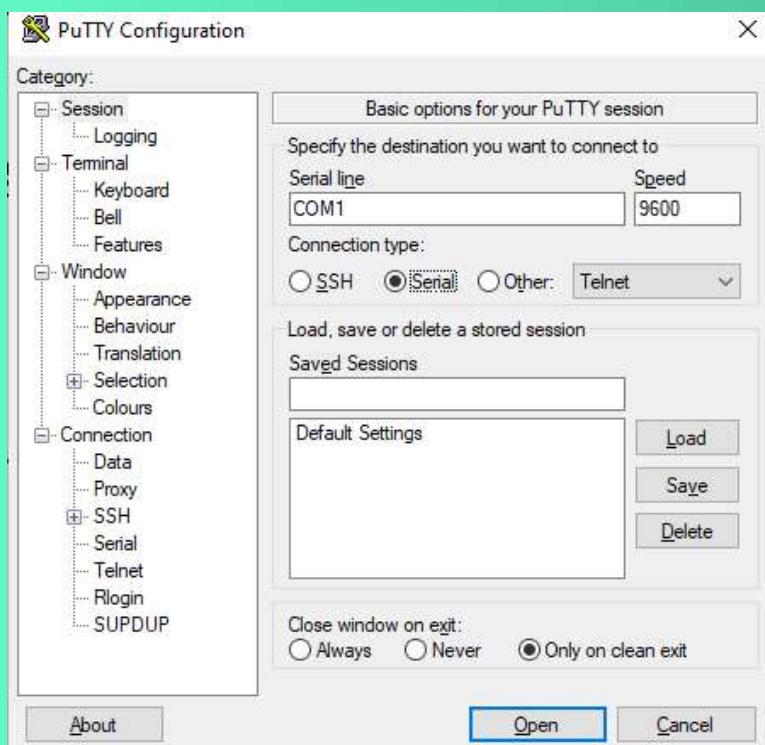
Pour réinitialiser le switch aux paramètres d'usine, il faut appuyer sur le bouton mode et maintenez-le enfoncé, les voyants LED du commutateur commencent à clignoter au bout de 3 secondes. Maintenez toujours le bouton mode enfoncé, les LED cessent de clignoter après 7 secondes supplémentaires puis le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

Mise en place d'une bannière EXEC :

```
BEG-CR-031(config)#banner exec '
Enter TEXT message.  End with the character '''.
                                |
                                |
                                |||
                                .|||.      .|||. .
.::||| | ||||:..:|||| | ||||:.
Cisco Systems

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

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

Créer des VLANs :

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

Mettre le mode TRUNK sur les interfaces voulues :

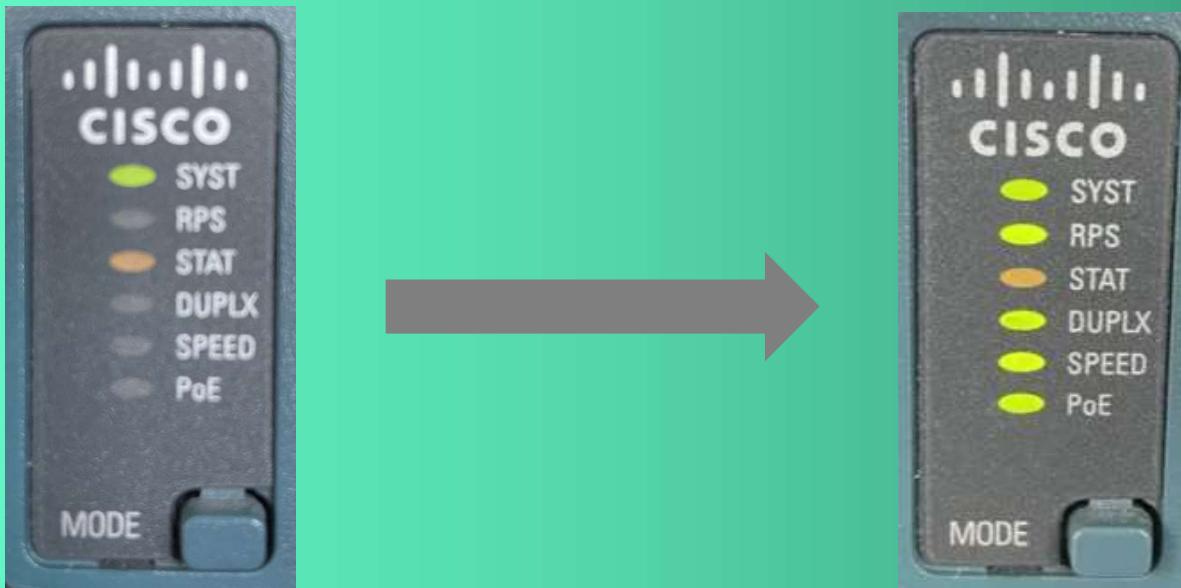
```
interface FastEthernet0/1
  switchport mode access
!
interface FastEthernet0/2
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
  switchport nonegotiate
!
interface FastEthernet0/3
  switchport trunk allowed vlan 10,20,30
  switchport mode trunk
  switchport nonegotiate
!
interface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

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

CONFIGURATION DU SWITCH

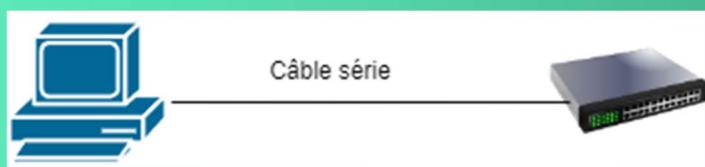
Procédure de réinitialisation :

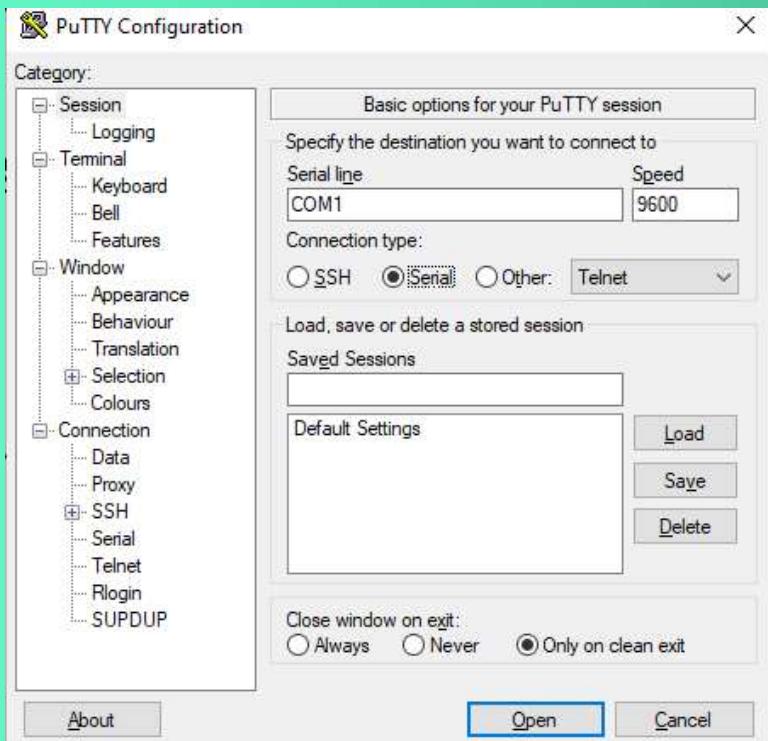
Pour réinitialiser le switch aux paramètres d'usine, il faut appuyer sur le bouton mode et maintenez-le enfoncé, les voyants LED du commutateur commencent à clignoter au bout de 3 secondes. Maintenez toujours le bouton mode enfoncé, les LED cessent de clignoter après 7 secondes supplémentaires puis le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



Se connecter au Switch :

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





Configuration de base du switch :

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

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

Nous avons ajouté comme mot de passe 'Azerty45'

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

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

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

Et ajouter une adresse IP

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

Pour enregistrer la configuration, il faut entrer cette commande :

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

Configuration des VLANS :

Des contraintes sont à respectées :

Le port 1 du switch de BEG est dédié à la gestion du commutateur et utilisé occasionnellement

Les ports 2 à 10 seront réservés à la téléphonie

Les ports 11 à 21 seront réservés aux PC et aux copieurs

Les ports 22 et 23 sont réservés à la visio-conférence et désactivés

Le port 24 est réservé pour le lien avec le cœur de réseau

Création des VLANS :

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

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

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

Pour vérifier que les VLAN sont 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
```

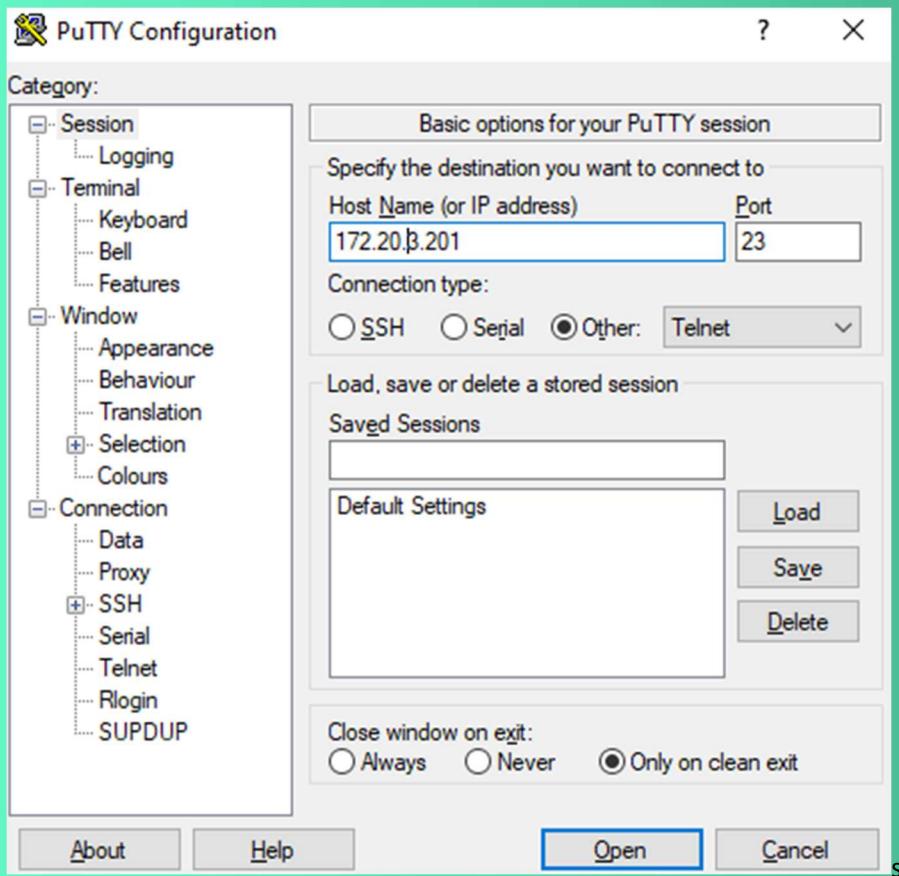
Sur le port 24, nous allons ‘taguer le port’ en activant le mode trunk et y autoriser le VLAN 10, 20 et 30

```
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 :

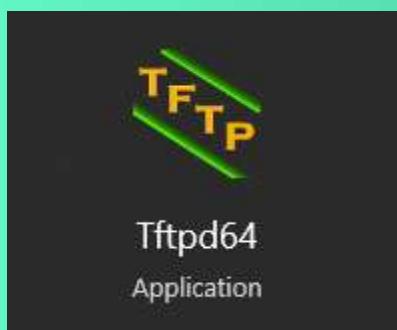
Pour se connecter à distance, il faut connecter le PC au switch avec un câble RJ 45 et ensuite en utilisant le logiciel PuTTY en utilisant son adresse IP.



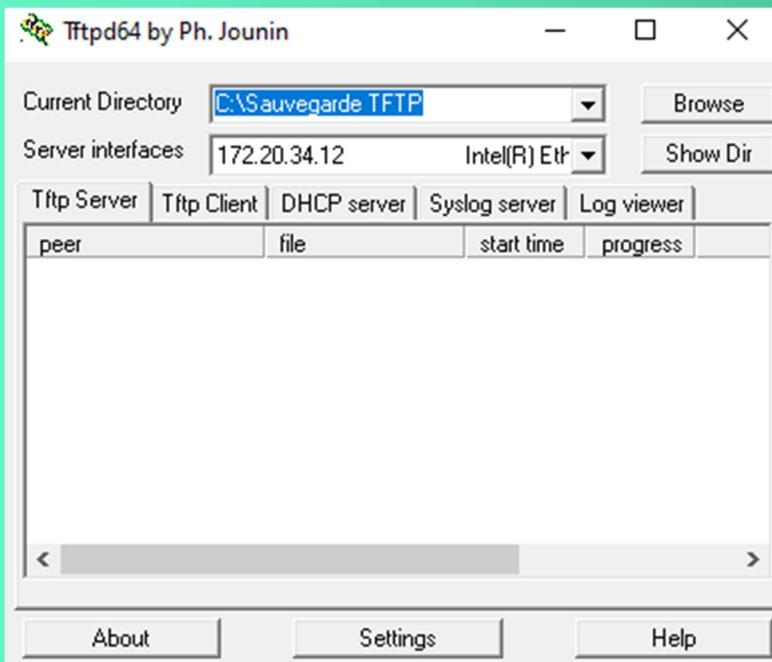


Sauvegarde TFTP :

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 démarrer. Il suffit de le fermer.



Une fois le logiciel ouvert, cette page s'ouvre. Sur cette page vous pourrez modifier le répertoire où 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'

Mise en place de la bannière MOTD

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 = FONCTIONNEL

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

INSTALLATION D'UNE CLE

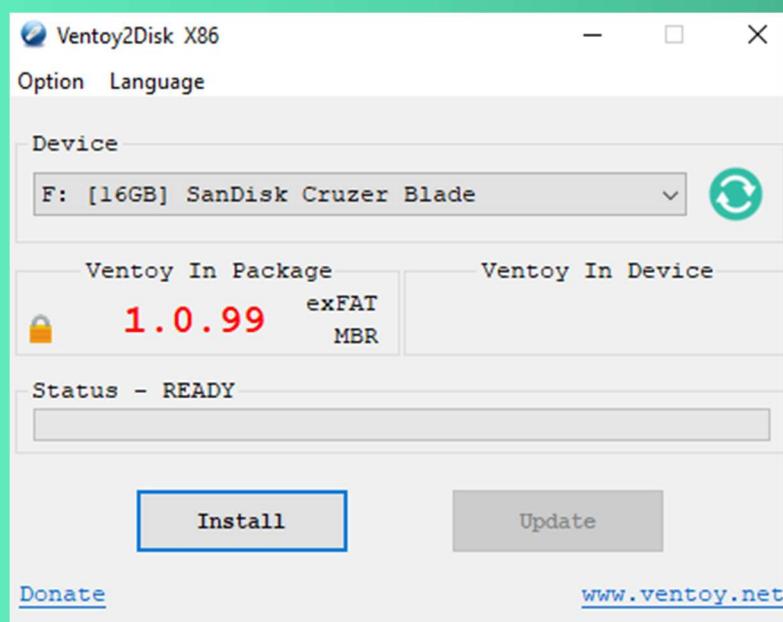
VENTOY

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

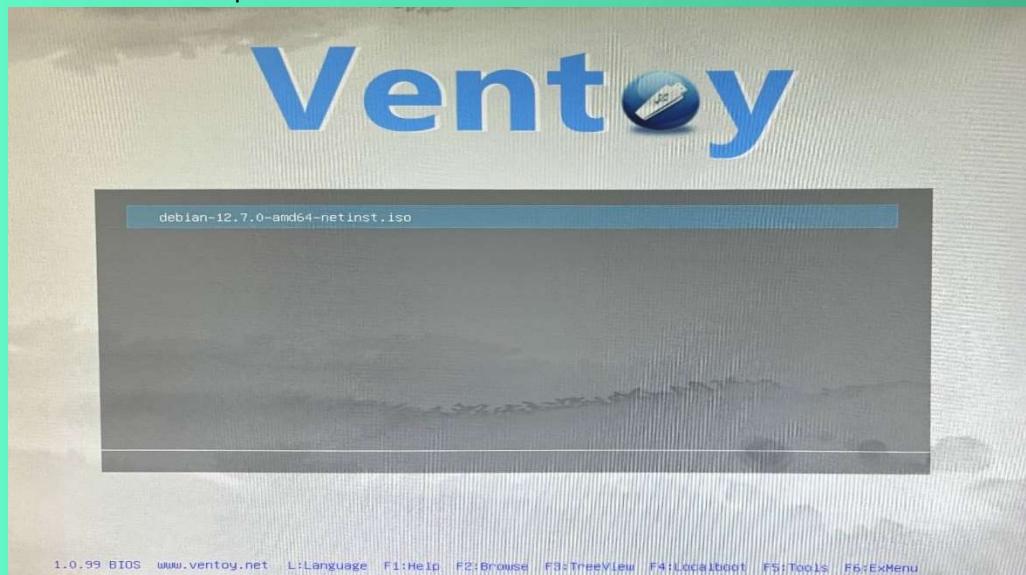
Pour installer ventoy, il faut se rendre sur le site : <https://www.ventoy.net/en/download.html>

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

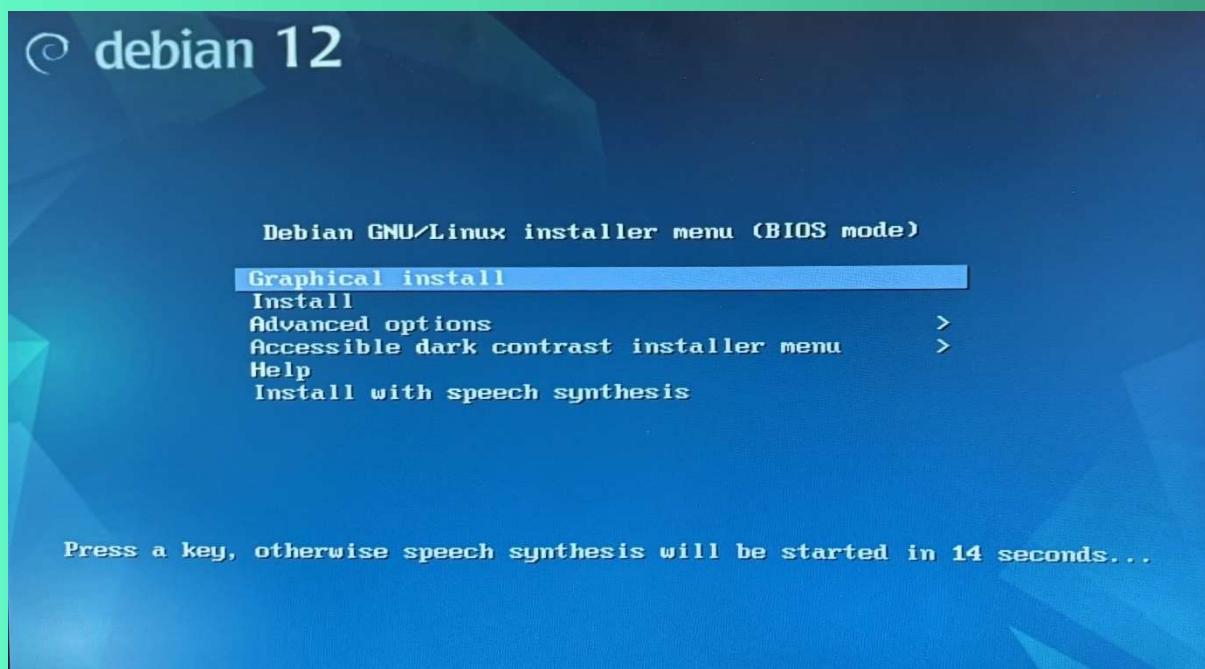
Ensuite, nous avons installé ventoy sur une clé USB en format FAT32



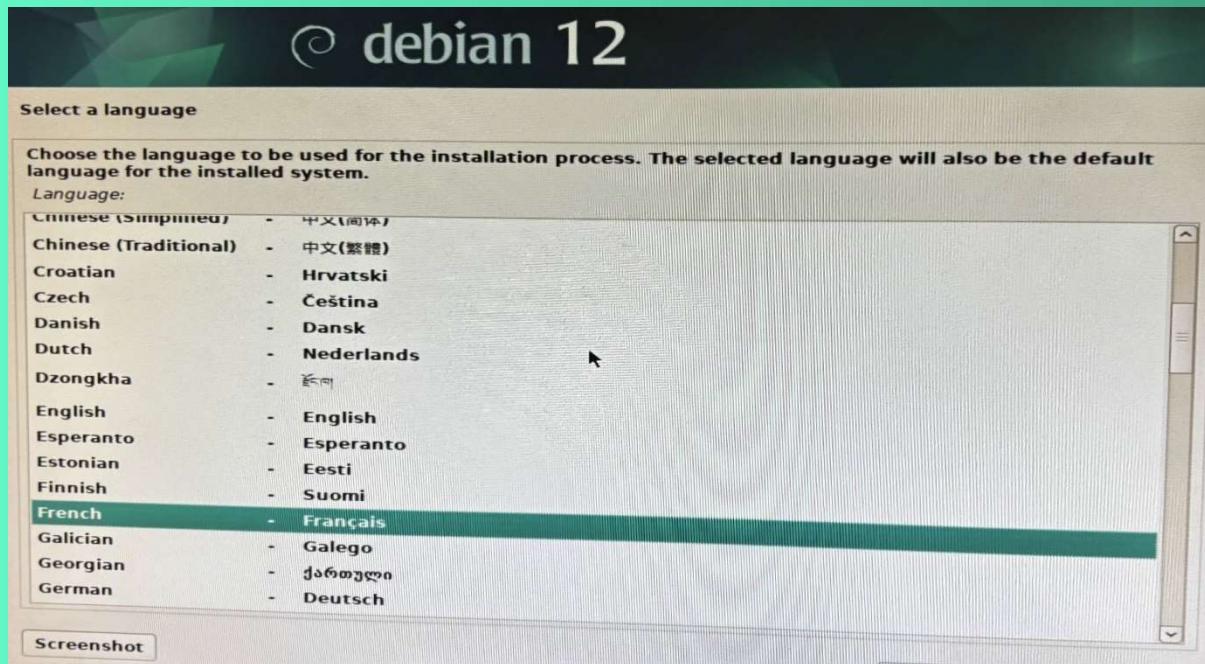
Sélectionner l'ISO que l'on souhaite installer



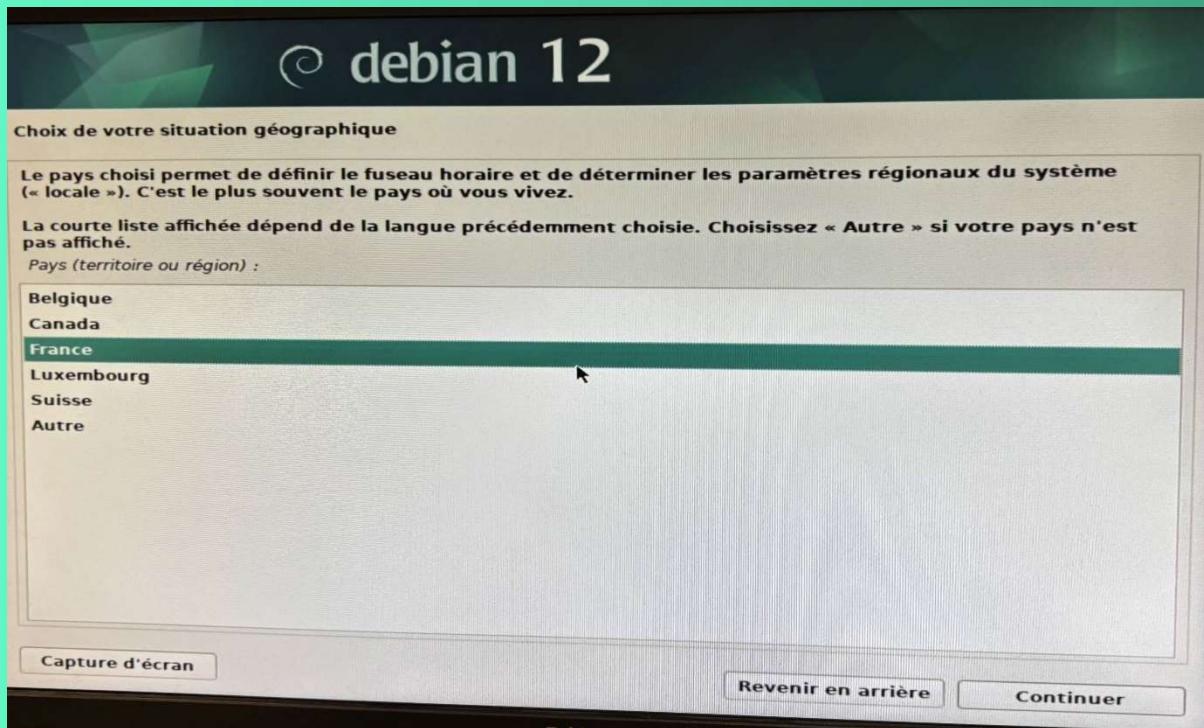
Installation de Debian 12 en version graphique



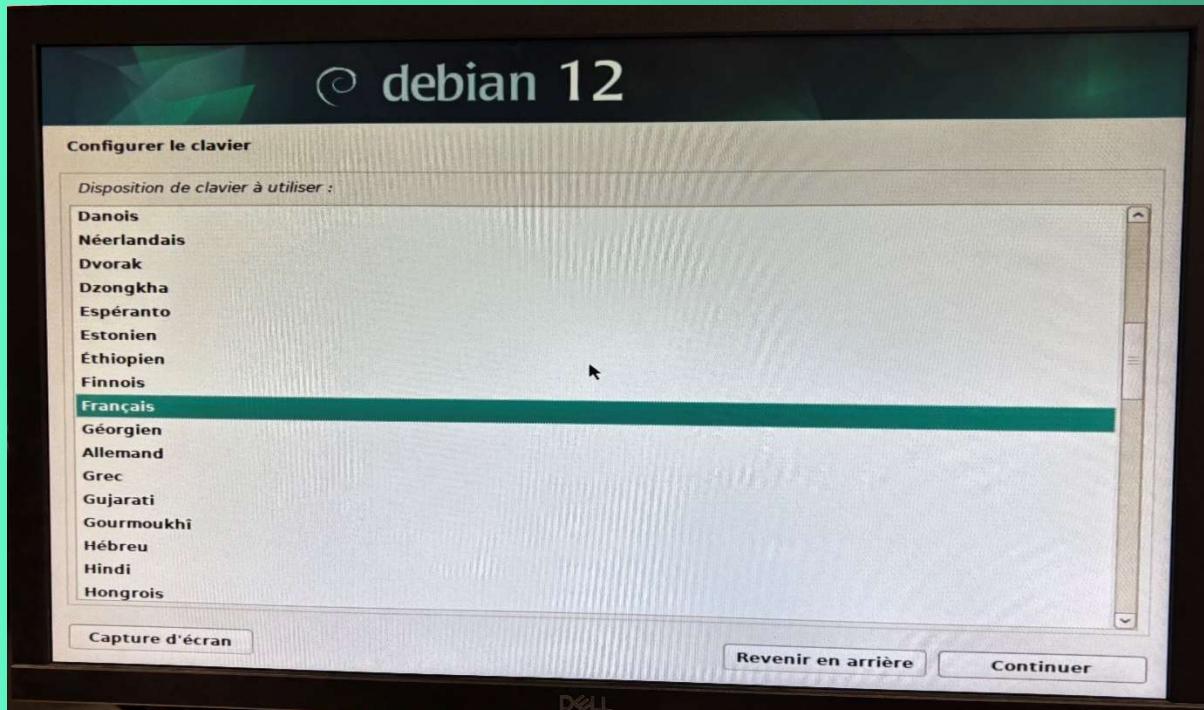
Sélection de la langue qui sera utilisé pour le processus d'installation



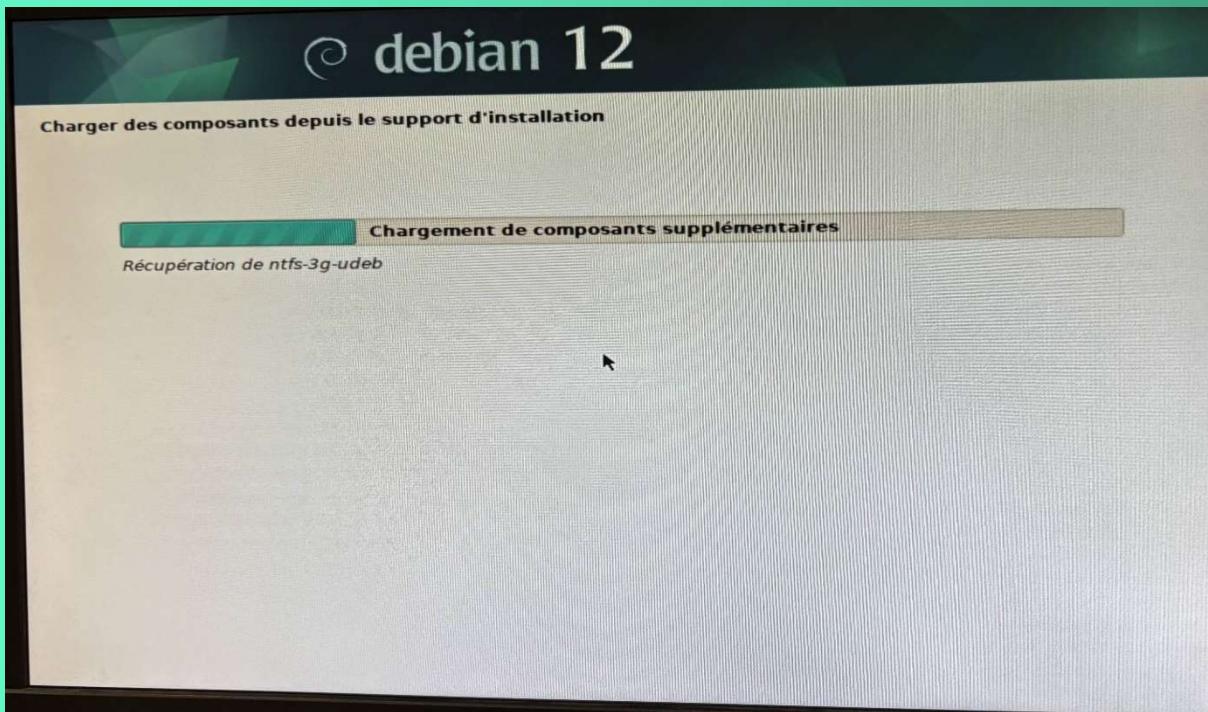
Choisir son pays local permettant de définir le fuseau horaire



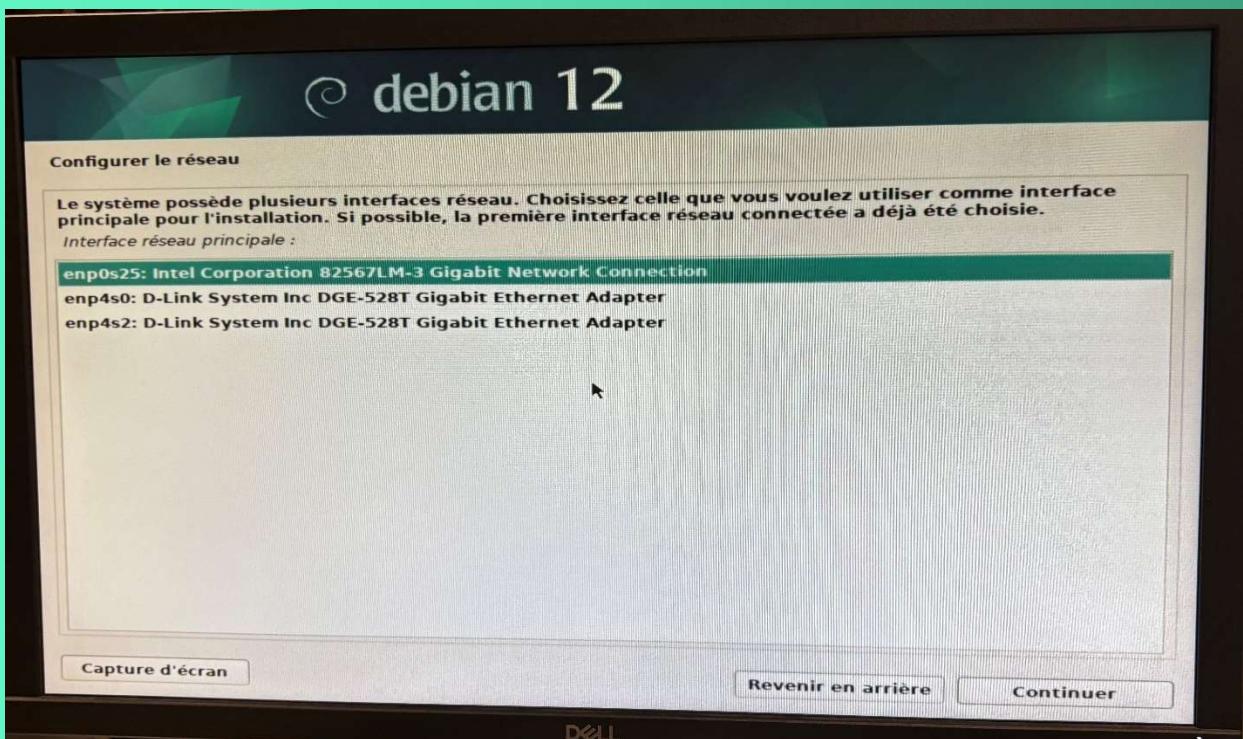
Configurer la langue du clavier



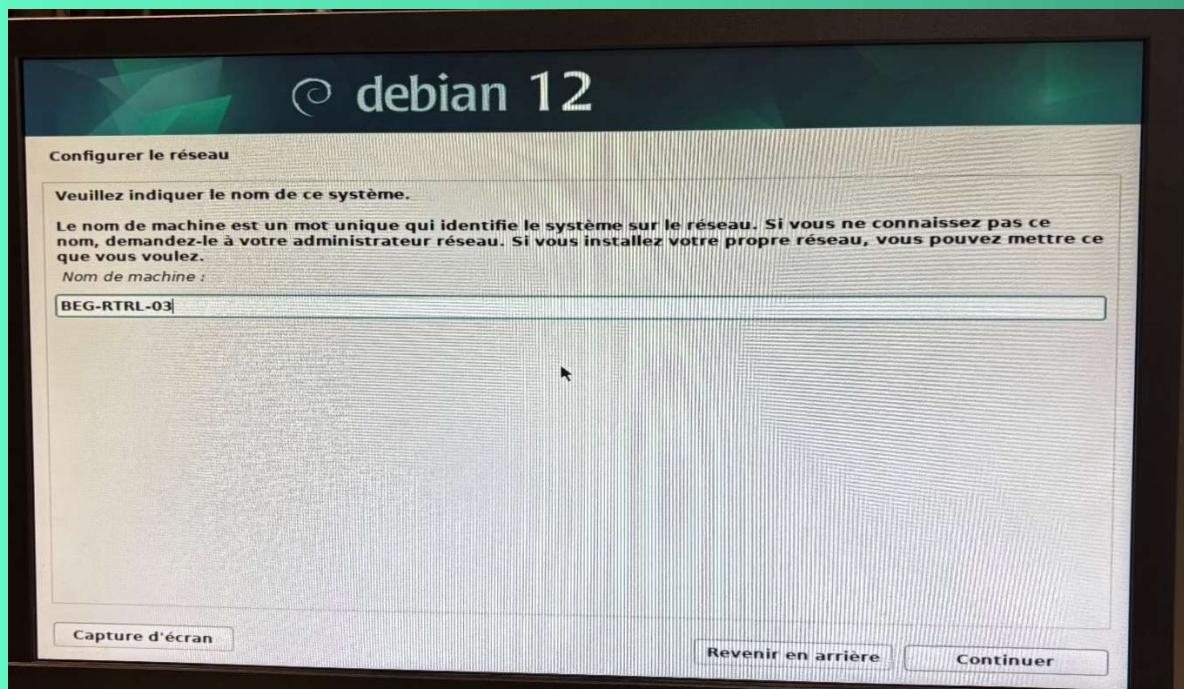
Chargement de composants supplémentaires nécessaires depuis le support d'installation



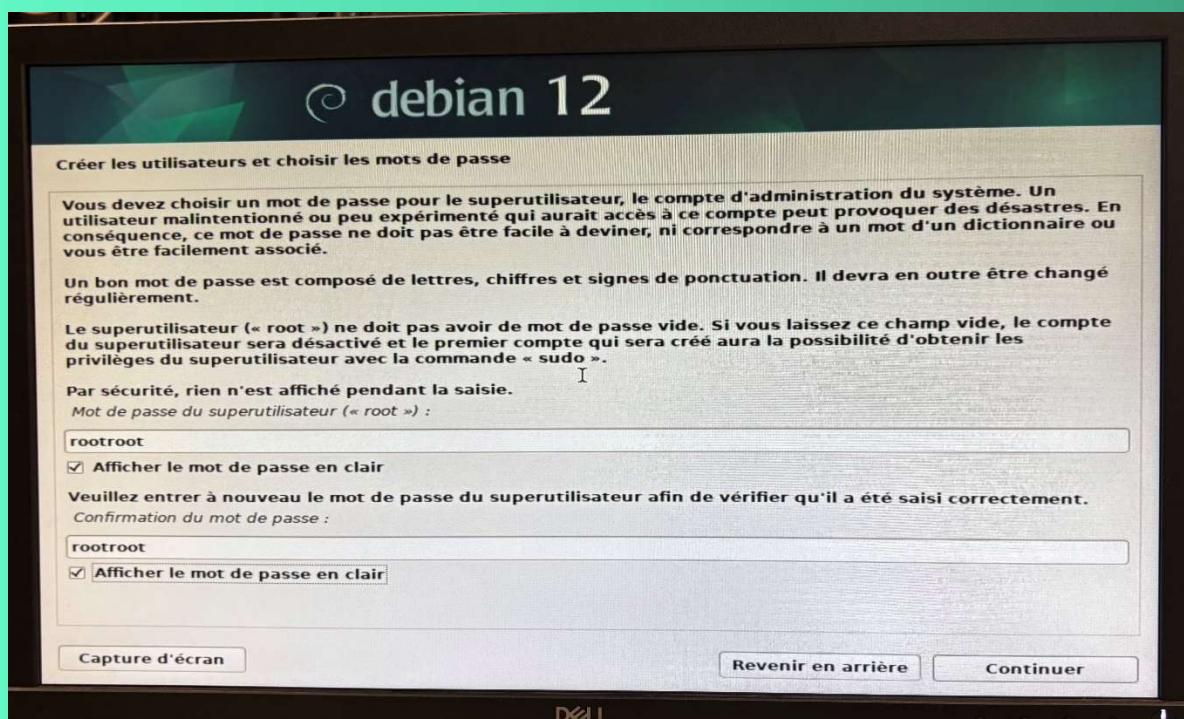
Sélection de la carte réseau principale



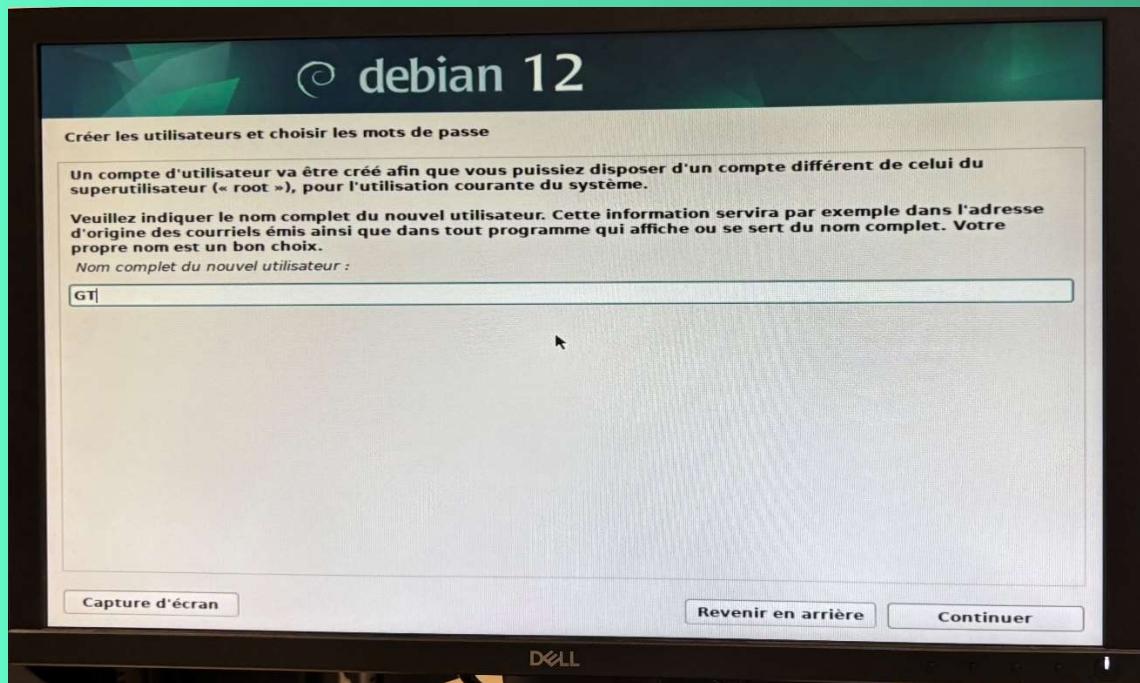
Configuration de nom de la machine



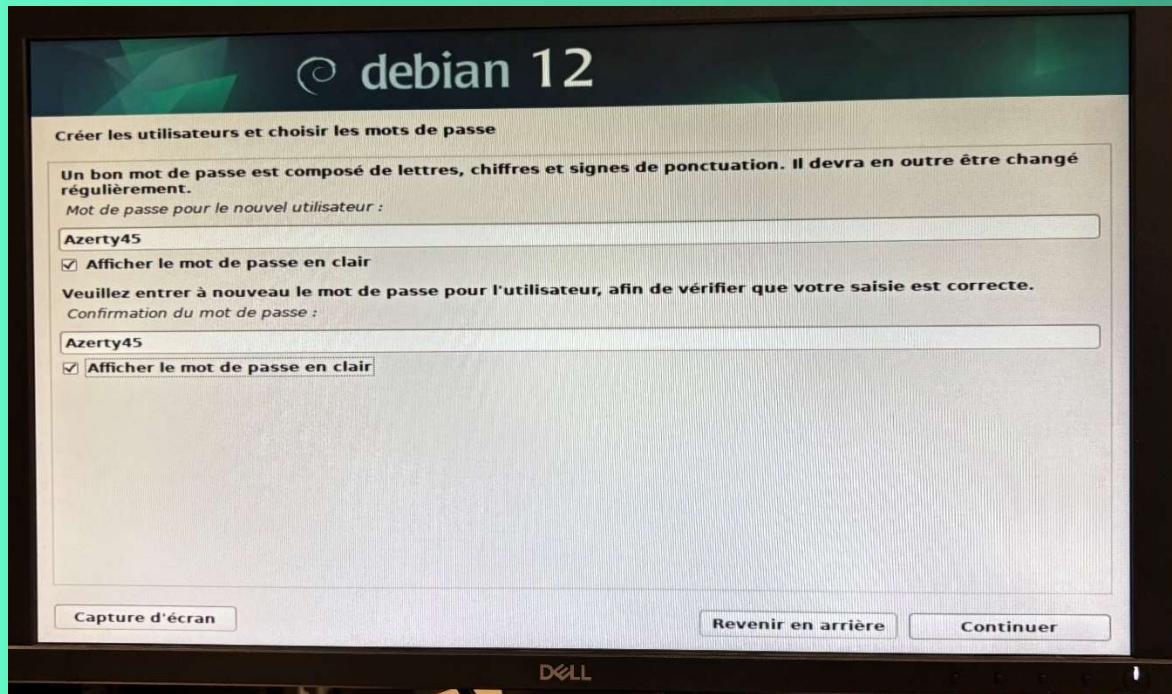
Création du mot de passe pour le compte superutilisateur / d'administration du système



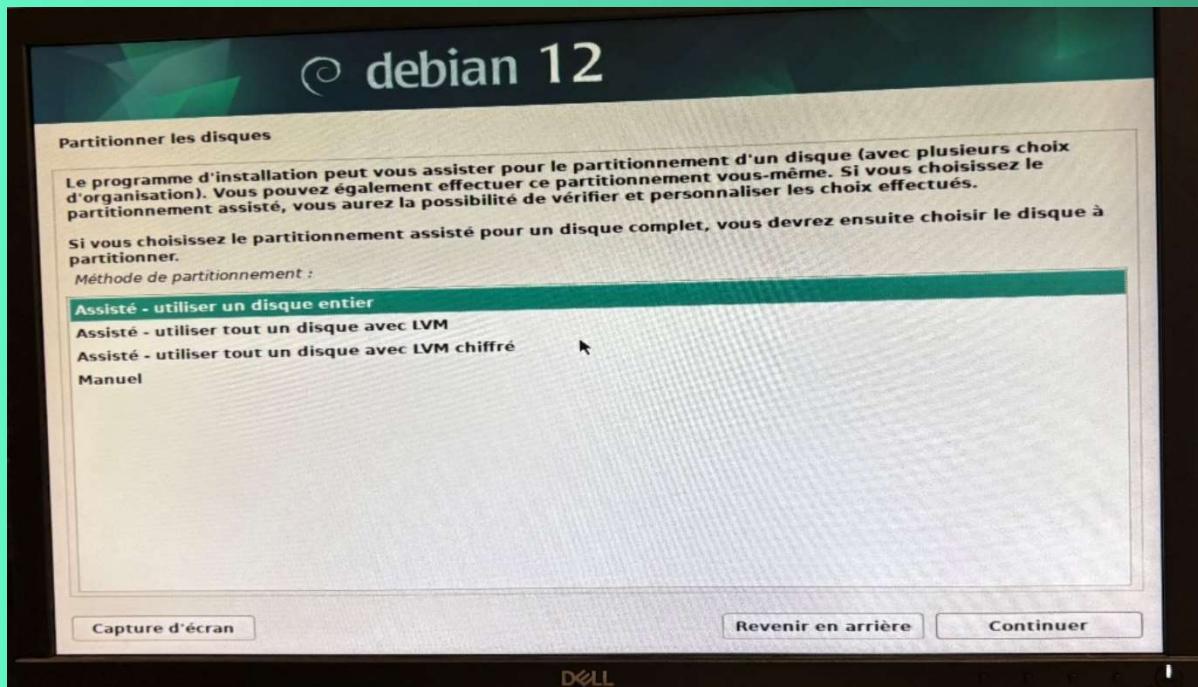
Créer le compte du nouvel utilisateur en choisissant l'identifiant du compte utilisateur



Choisir le mot de passe du compte utilisateur



Méthode de partitionnement



Choisir le disque

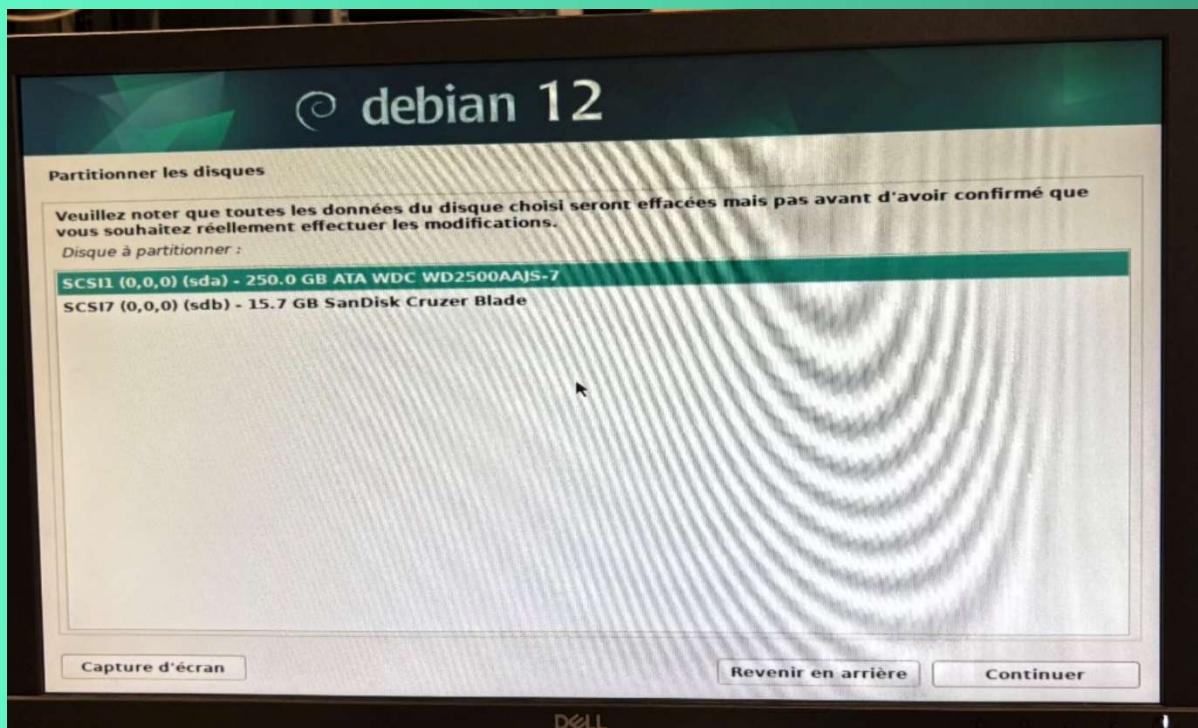
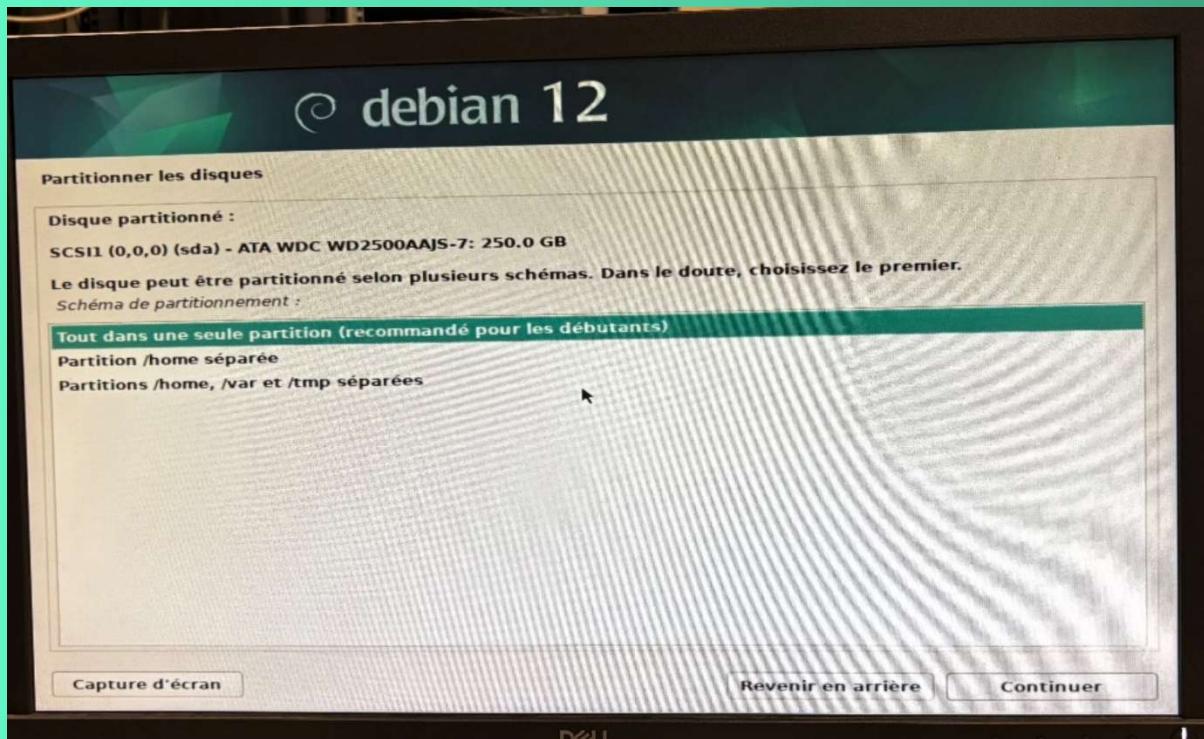
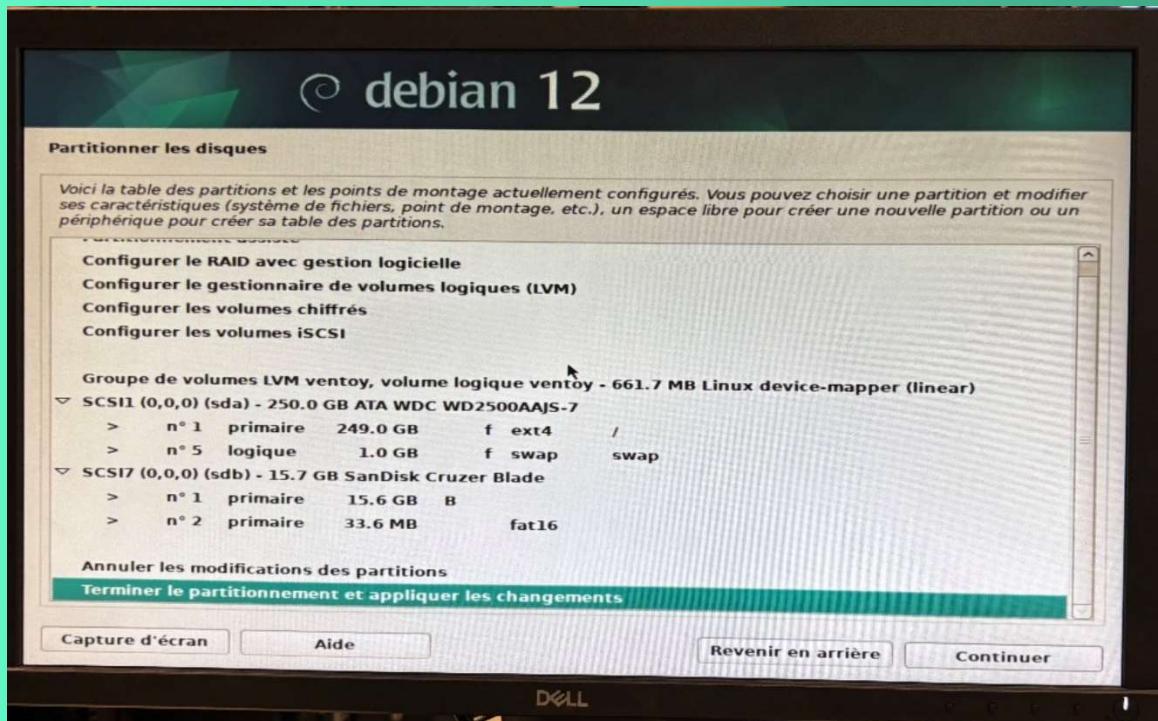


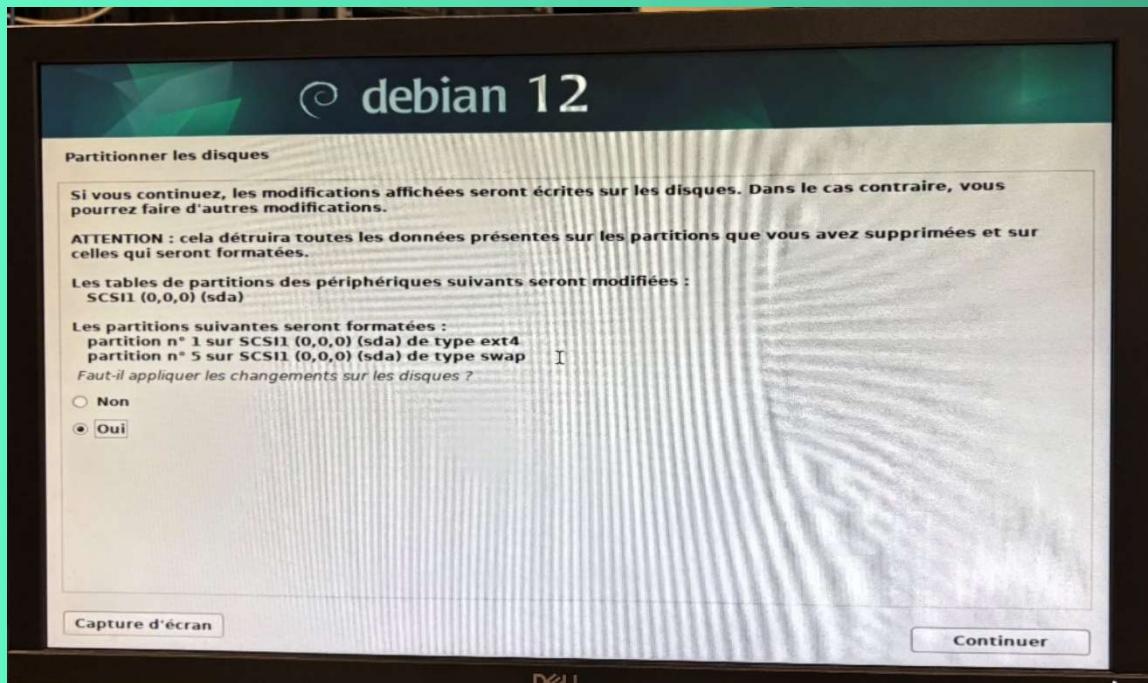
Schéma du partitionnement



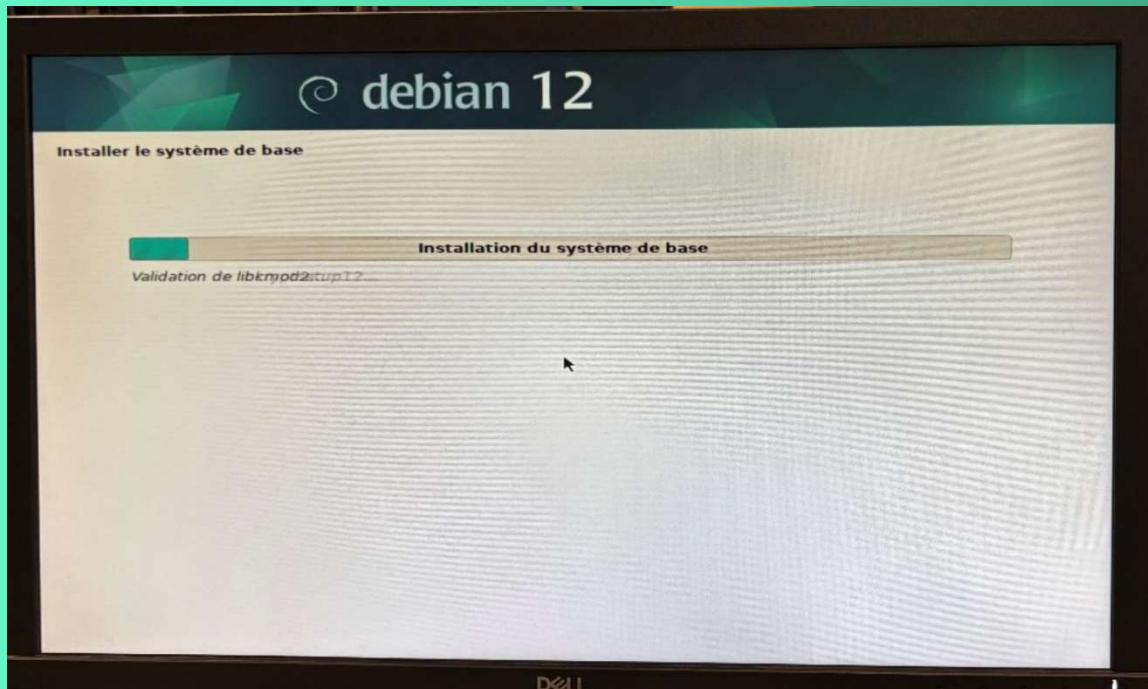
Terminer le partitionnement et appliquer les changements



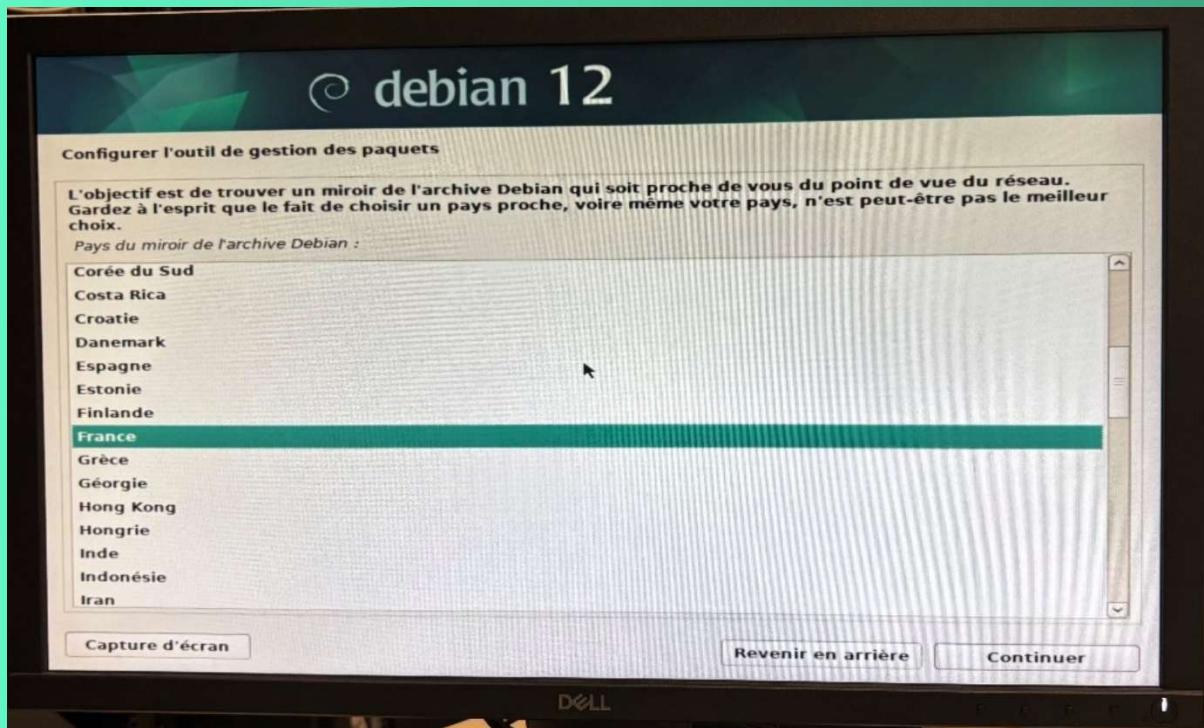
Appliquer les changements sur les disques



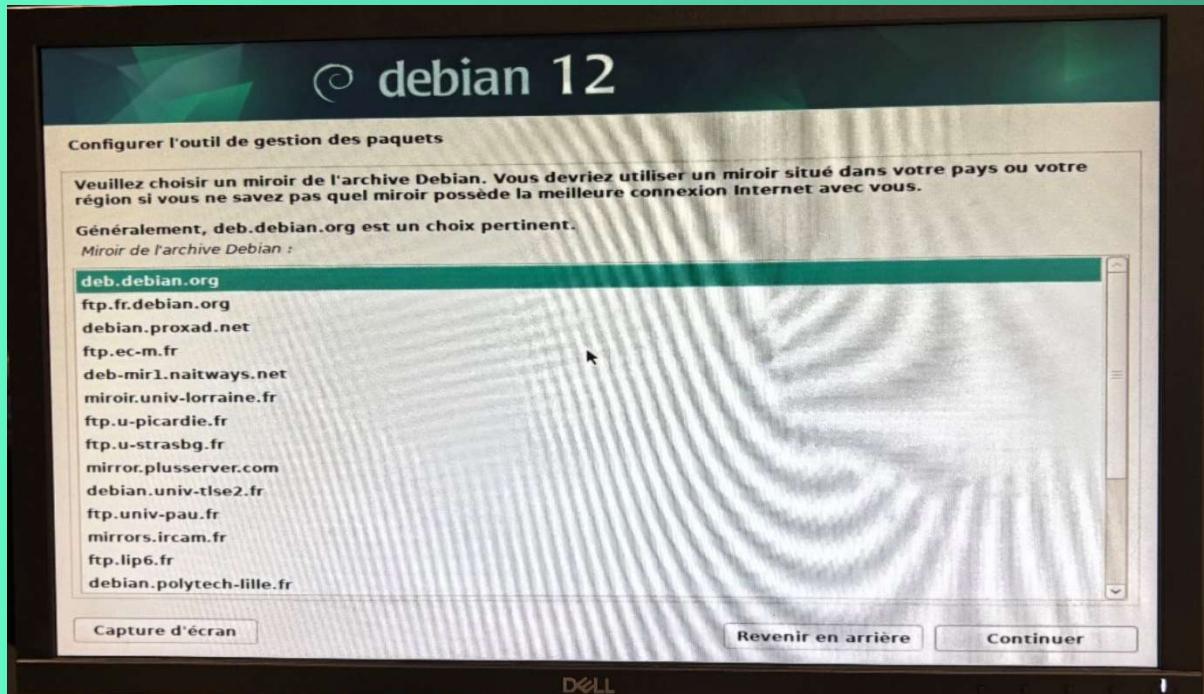
Installation du système de base



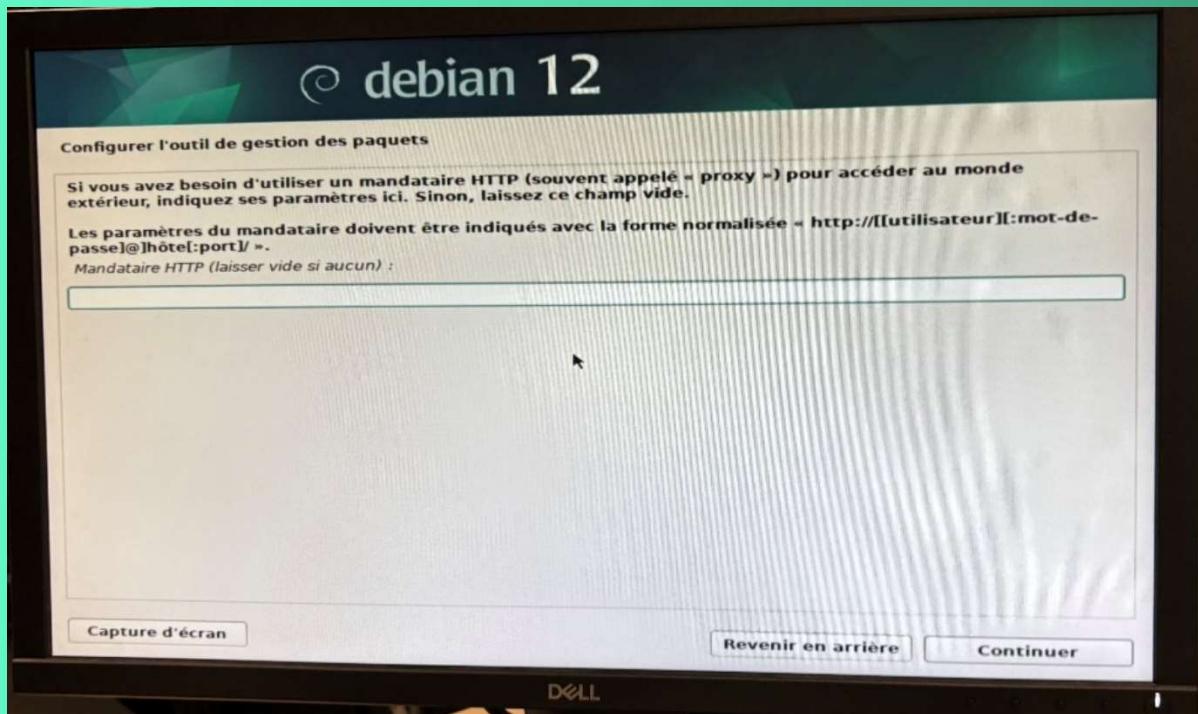
Choisir un miroir de l'archive en prenant le pays le plus proche



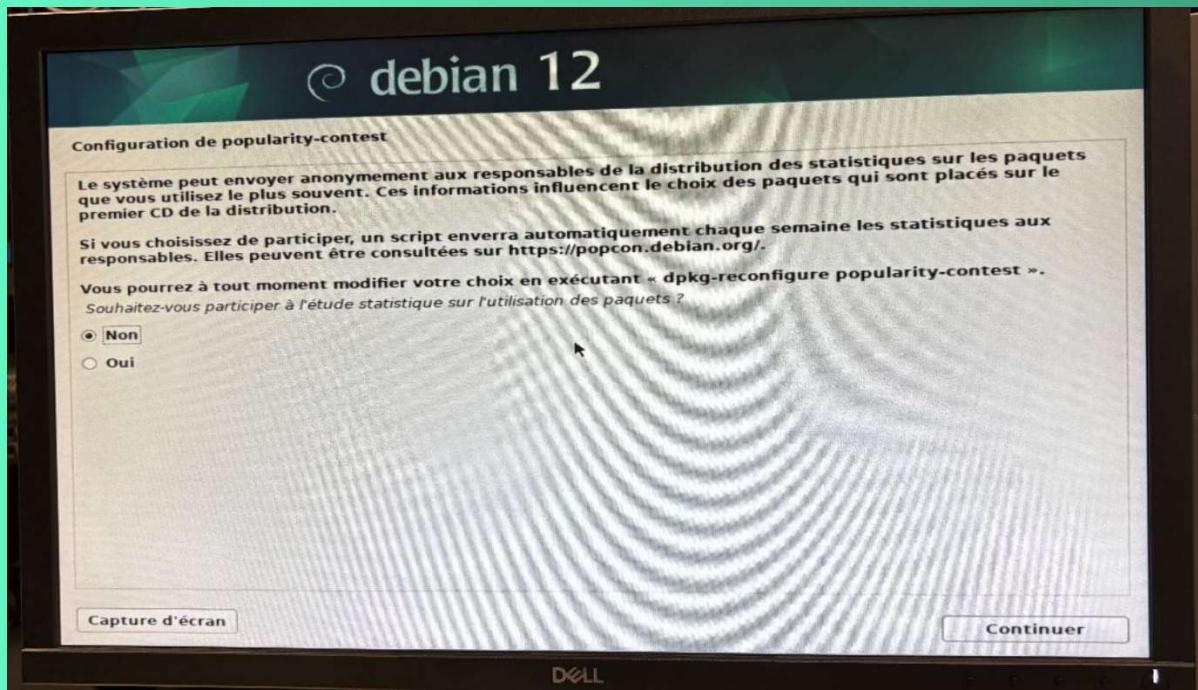
Choisir le miroir de l'archive Debian



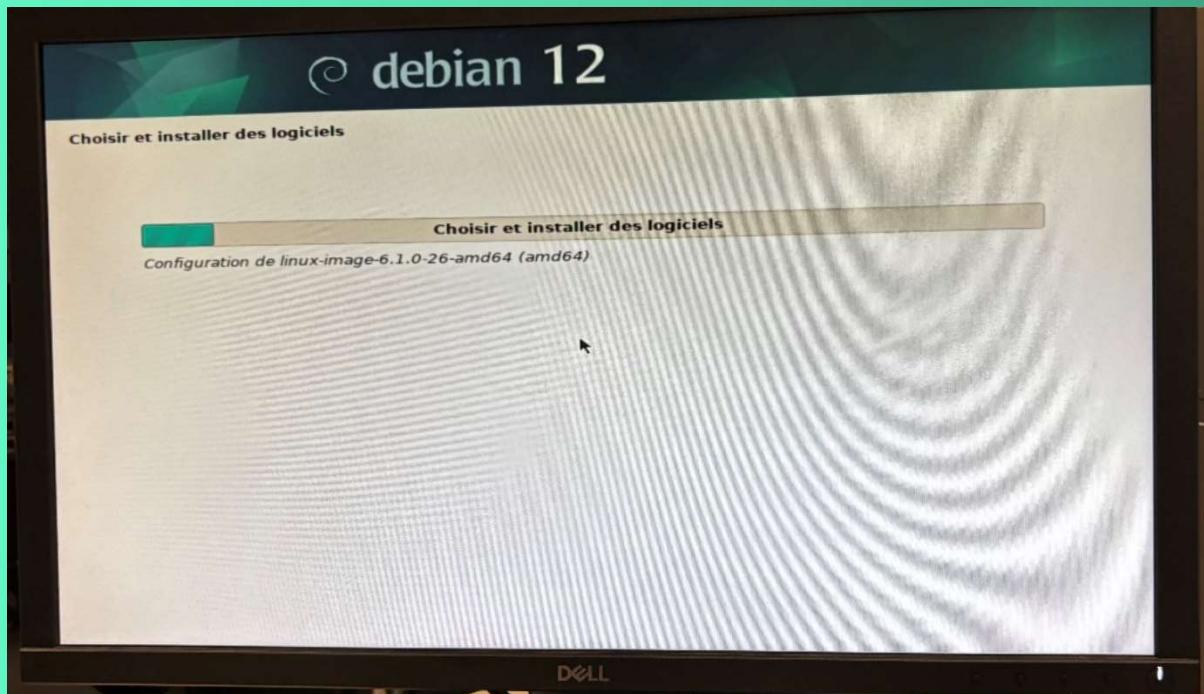
Pas de mandataire http



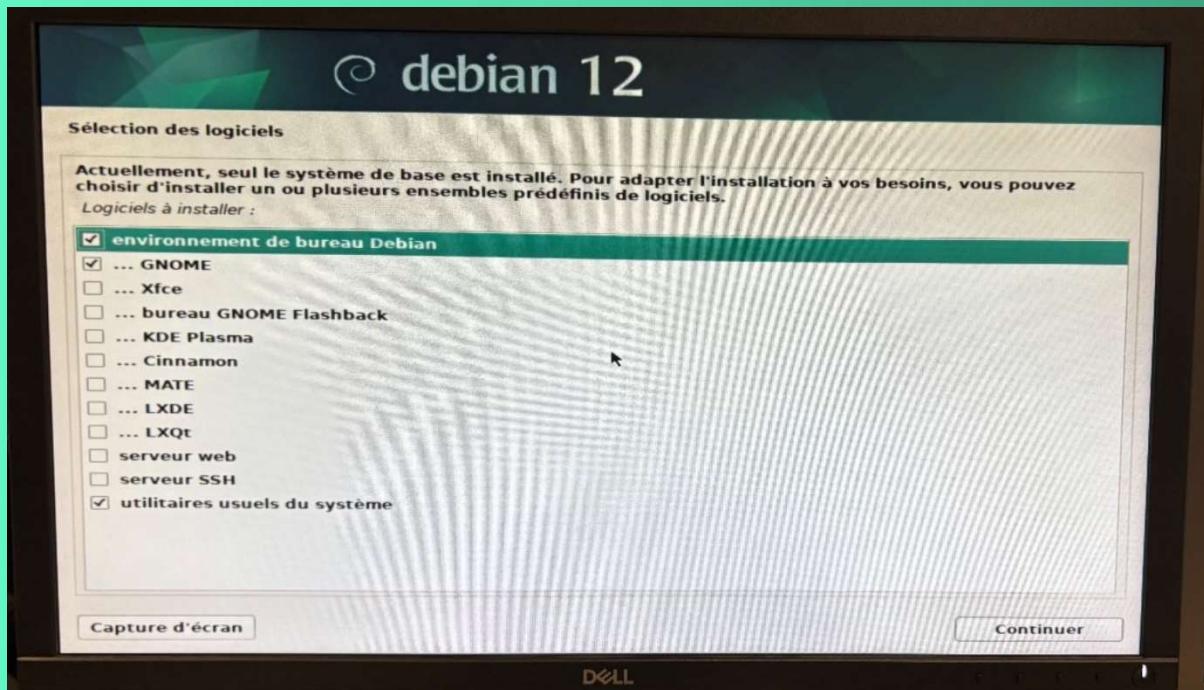
Configurer le popularity-contest



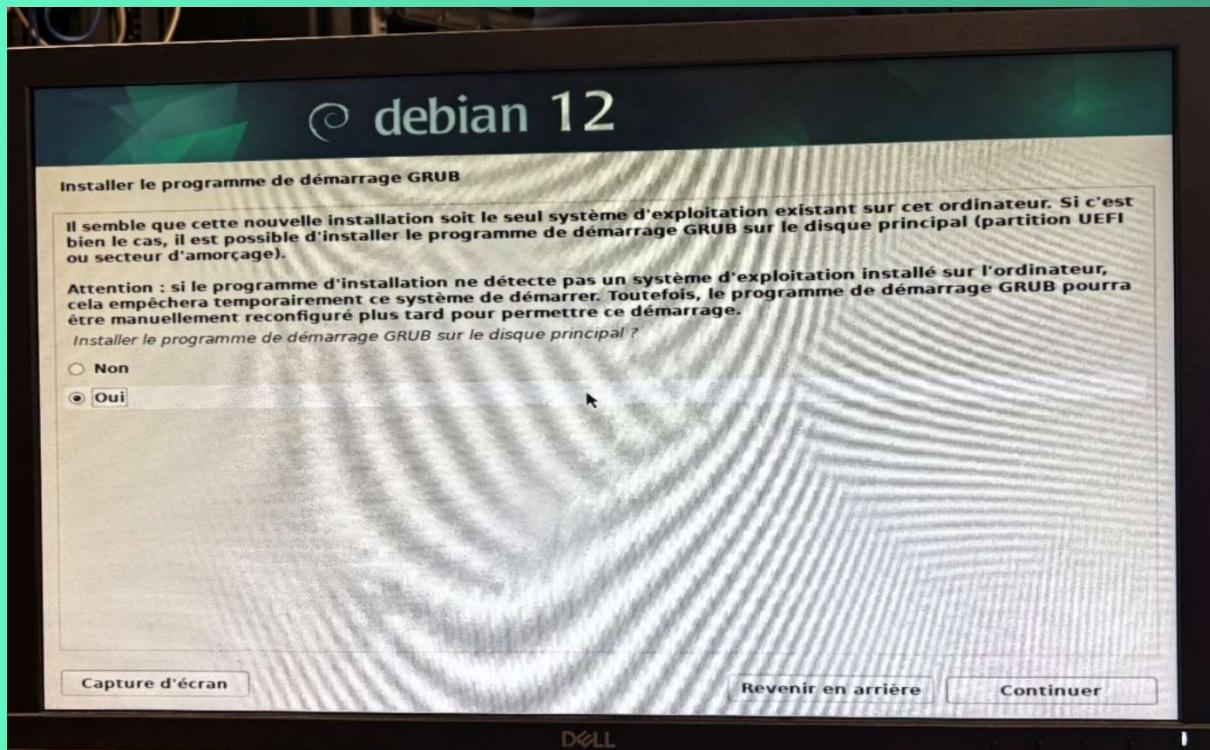
Installation des logiciels



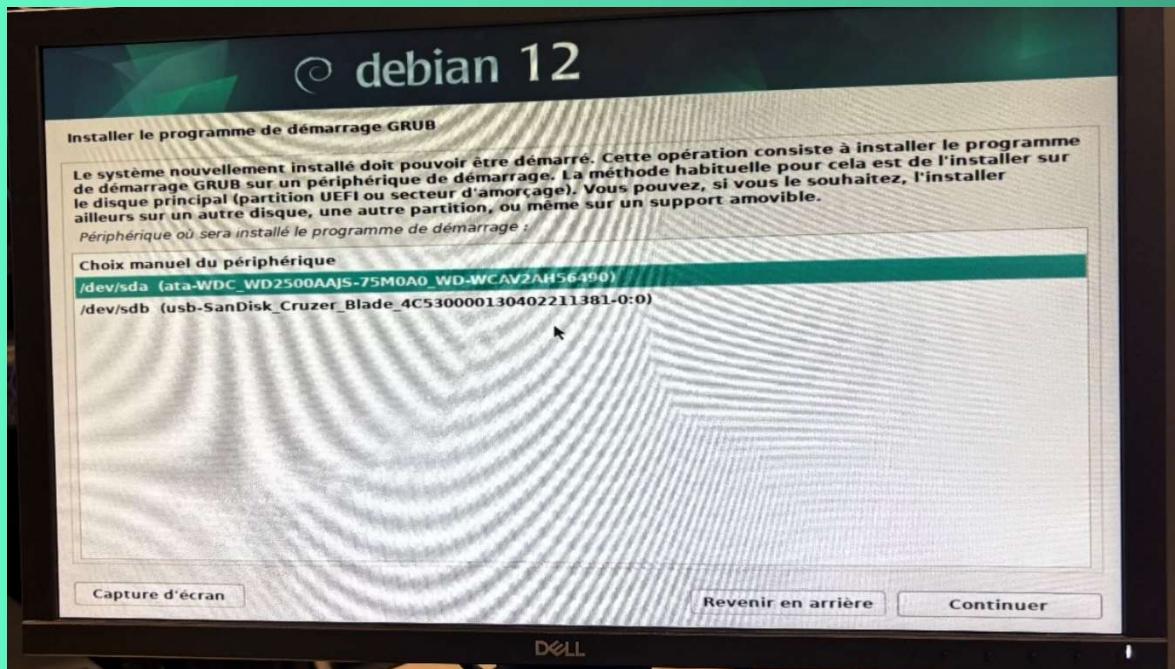
Choix de logiciels prédéfinis



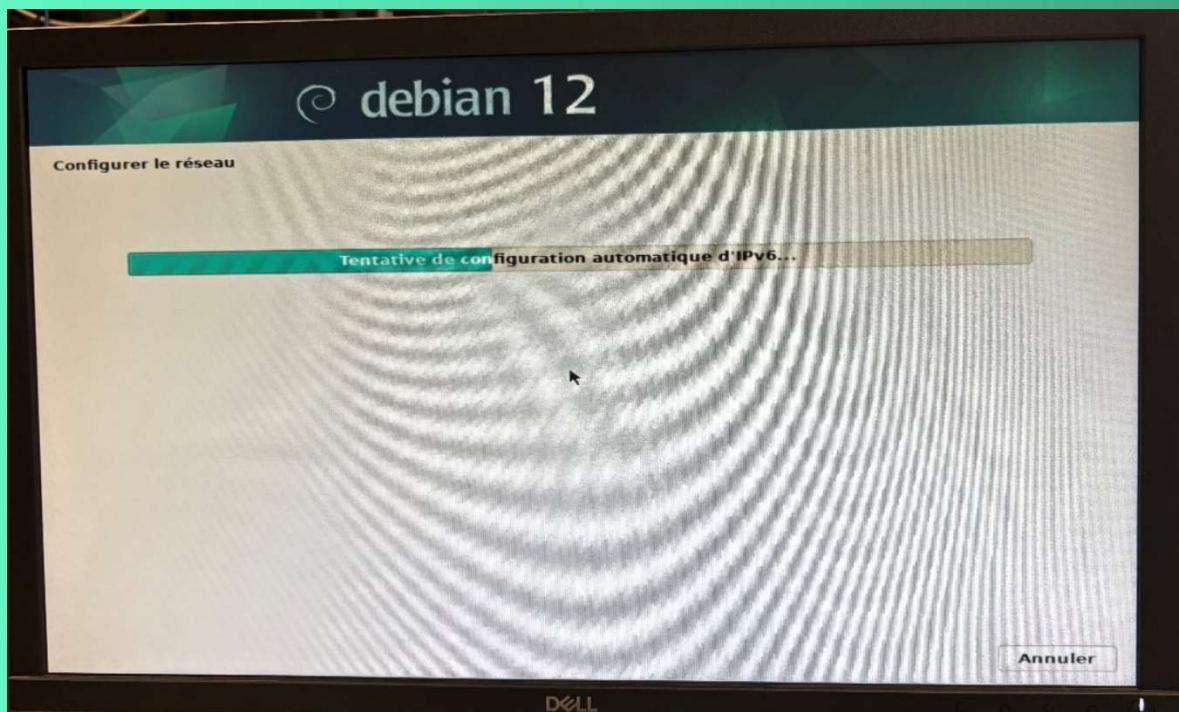
Installer le programme de démarrage GRUB



Installer le périphérique de démarrage



Fin de l'installation



CONFIGURATION DU FIREWALL

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

Configuration des cartes réseaux :

Enp0s25 (lien LAN)

Auto enp0s25

Iface enp0s25 inet static

Adress 172.21.3.254/16

Enp4s0 (lien DMZ)

Auto enp4s0

Iface enp4s0 inet static

Adress 192.168.100.254/24

Enp4s2 (lien INTERNET)

Auto enp4s2

Iface enp4s2 inet static

Adress 172.20.34.212/16

Gateway 172.20.2.254

Tests réalisés :

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

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

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

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

Modifier dans le fichier etc/resolv.conf

Nameserver 8.8.8.8

Nameserver 1.1.1.1

Mise en place du routage

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

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

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

Tests réalisés :

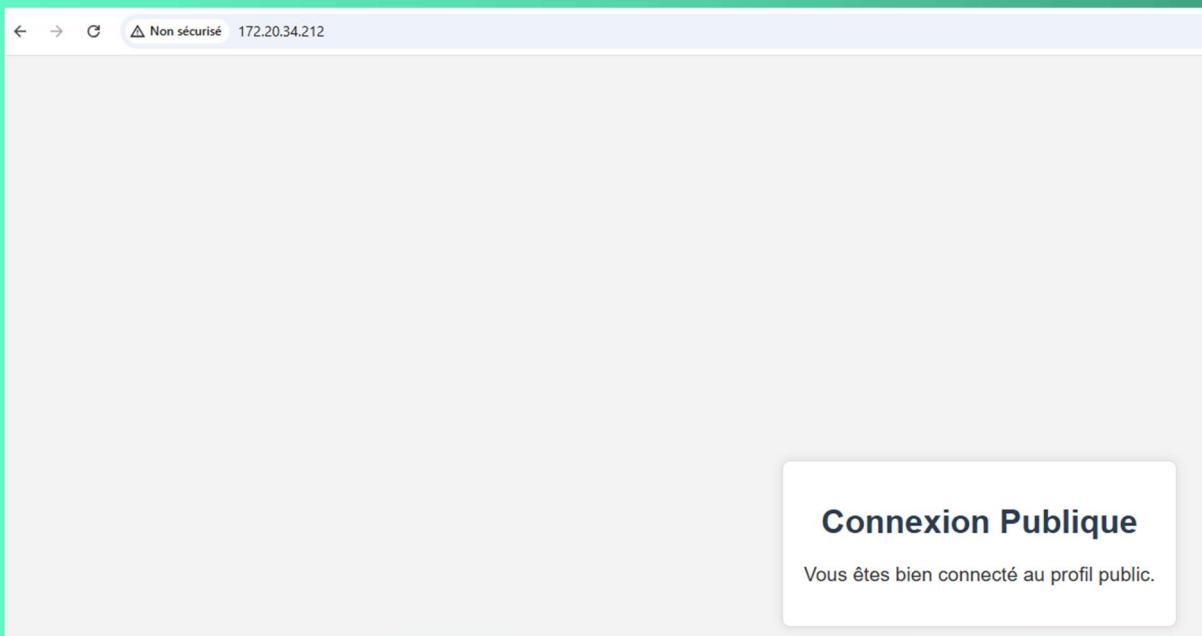
Depuis une machine cliente en 172.20.34.12 à accéder au site internet présent sur le serveur IIS en 192.168.100.10 sur le port 80

Redirection au site web :

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

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

Tests réalisés :



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

Règles iptables

Activer le pare-feu :

```
Iptables -P INPUT DROP
```

```
Iptables -P OUTPUT DROP
```

```
Iptables -P FORWARD DROP
```

Autoriser toutes les connexions déjà établies :

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

Autoriser le SSH pour seulement l'adresse IP 172.20.34.12 :

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

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

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

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

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

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

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

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

Autoriser l'accès 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.

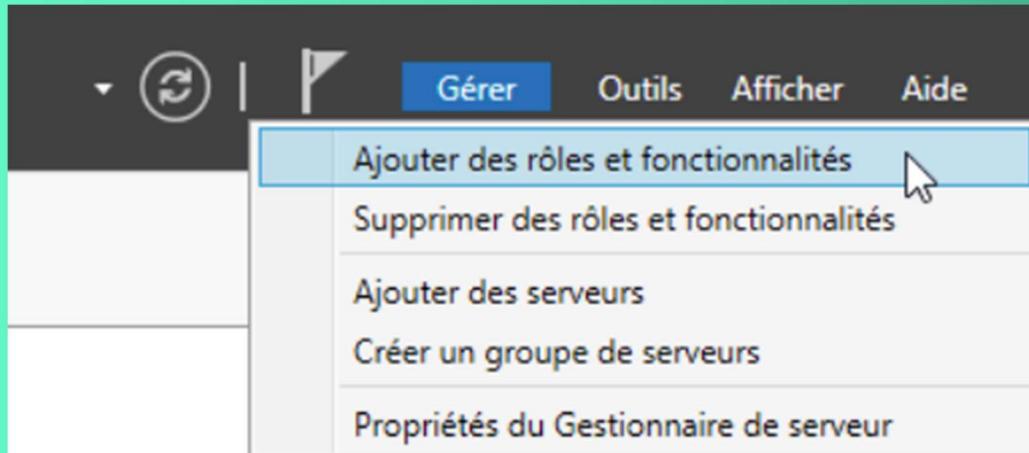
Avec la commande netfilter-persistent save, les règles iptables sont enregistrer dans le fichier :

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

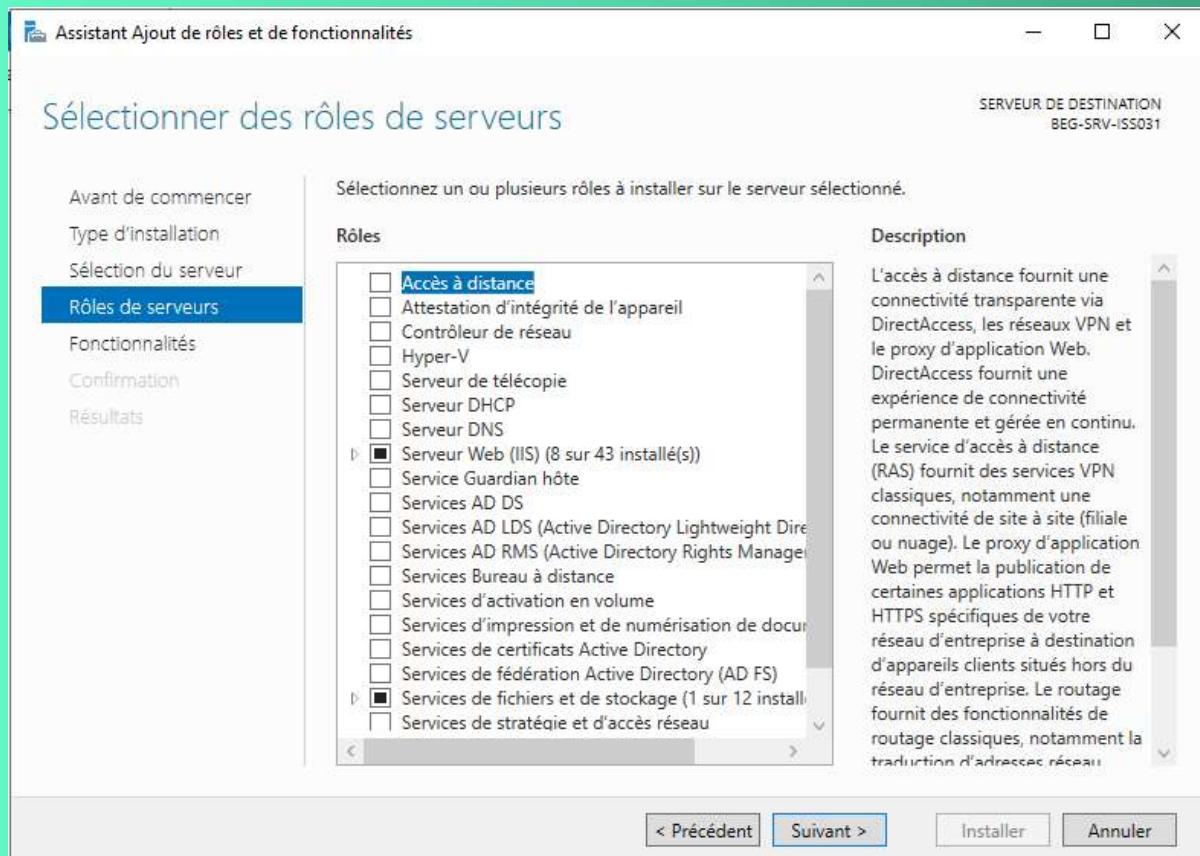
Restart le service avec la commande systemctl restart netfilter-persistent.service

CONFIGURATION D'UN SERVEUR IIS

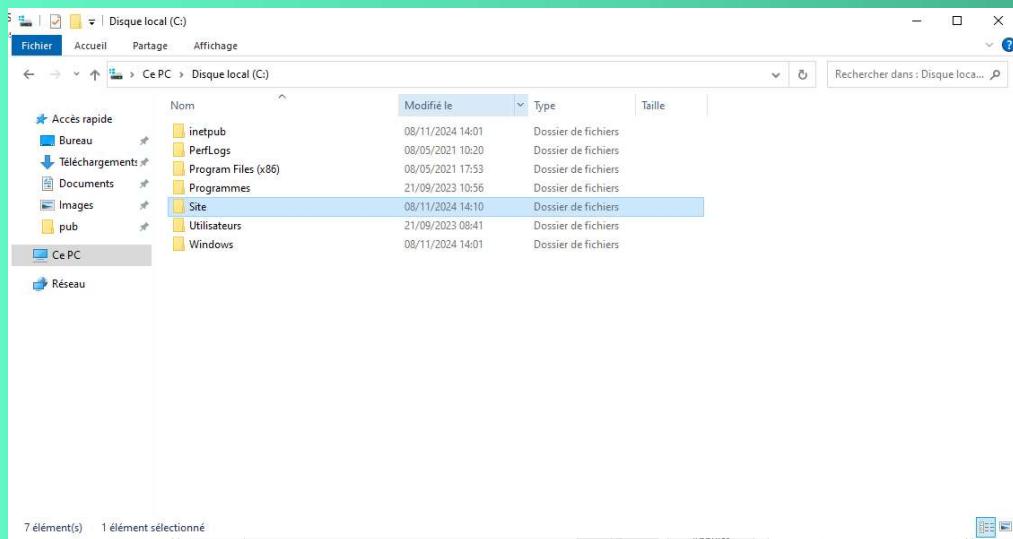
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur ‘Gérer’ et ‘Ajouter des rôles et fonctionnalités’.



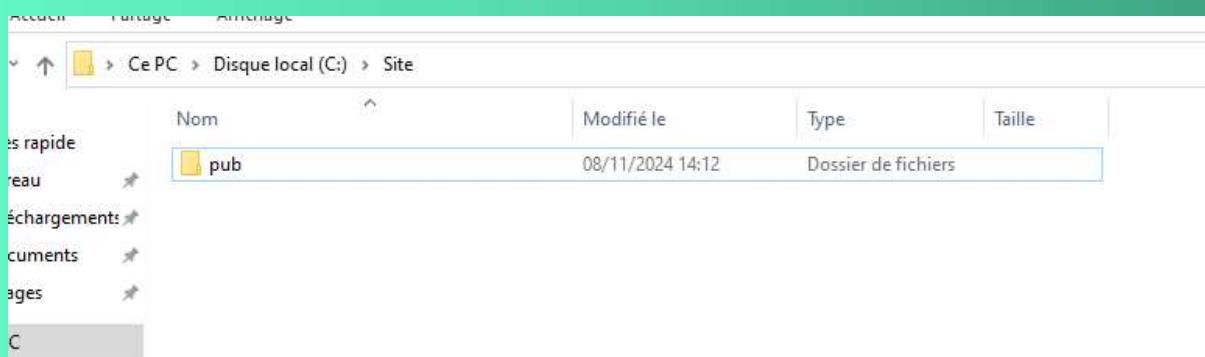
Dans l'onglet ‘Rôles de serveurs’, cocher ‘Serveur Web (IIS)’



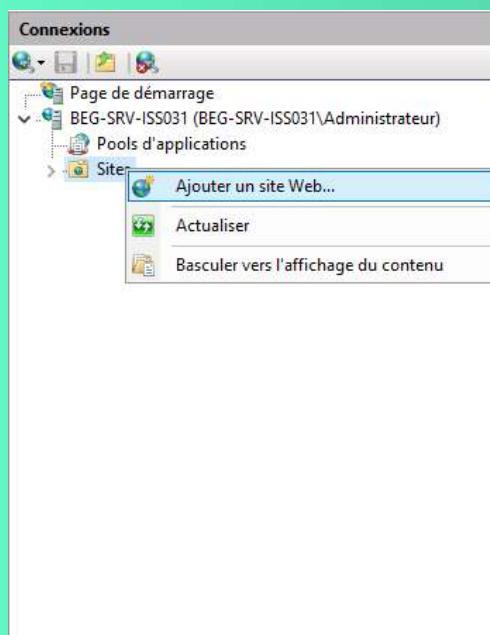
Ensuite, créer un dossier sur notre disque C



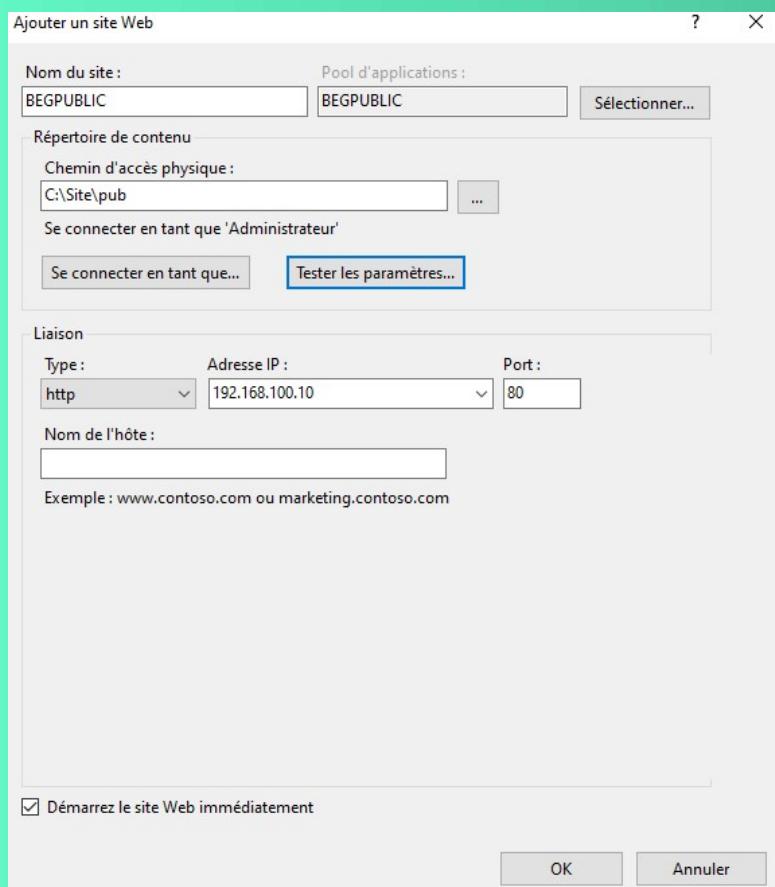
Comme sous-dossiers 'pub' signifiant que le site sera public



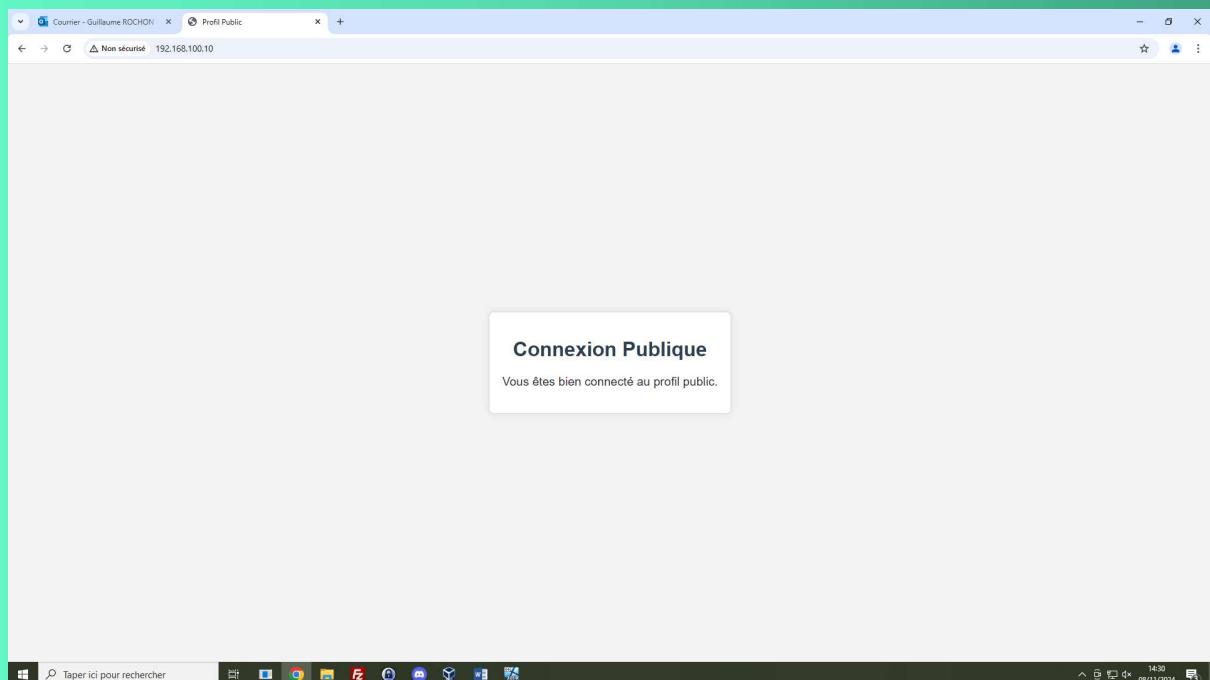
Pour le site « pub » crée un fichier html avec une indication pour vérifier que c'est bon



Tester la connexion à son site web



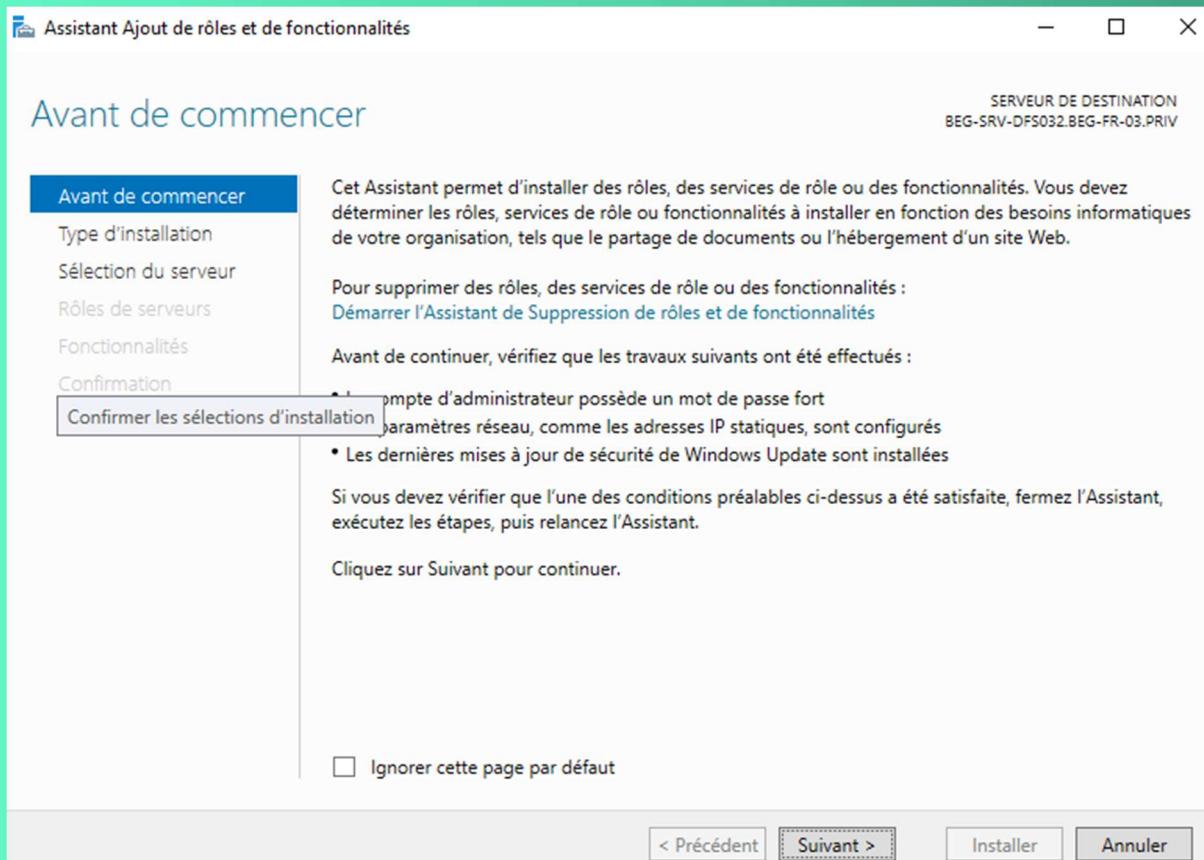
Résultat :



CONFIGURATION D'UN SERVEUR DFS

Installation du service :

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



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

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

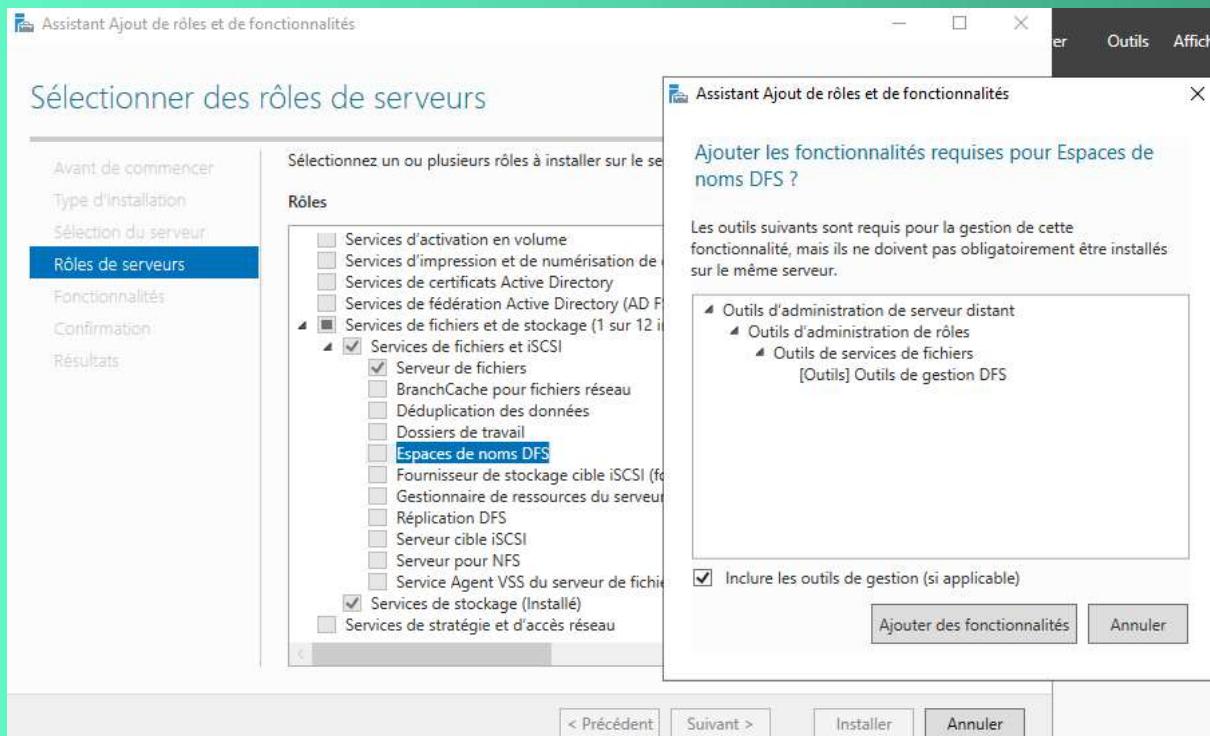
Filtre :		
Nom	Adresse IP	Système d'exploitation
BEG-SRV-DFS032.BEG-F...	172.20.3.9	Microsoft Windows Server 2022 Datacenter

1 ordinateur(s) trouvé(s)

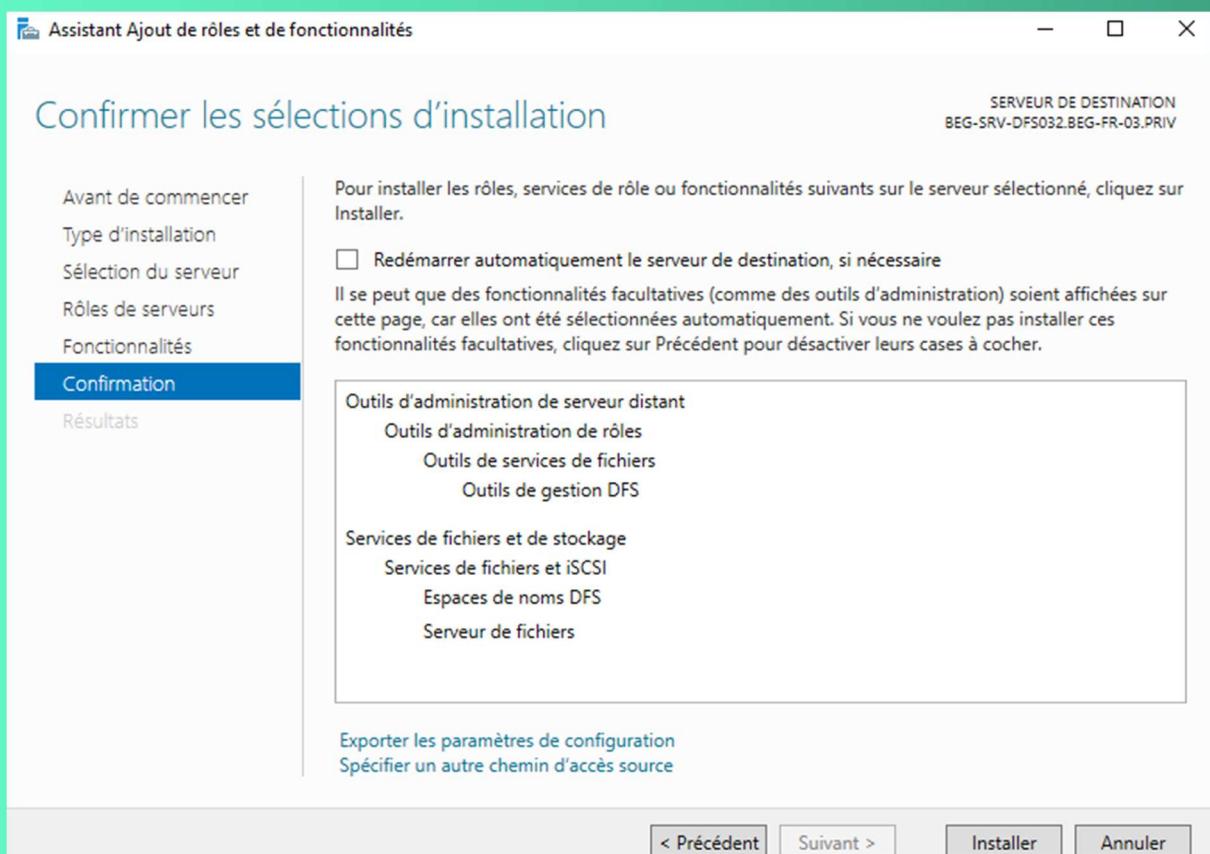
Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète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

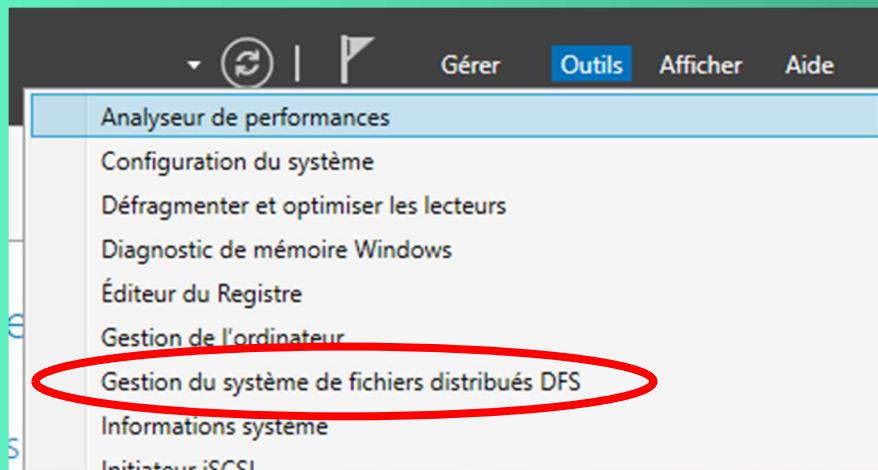


Création d'une racine DFS autonome :

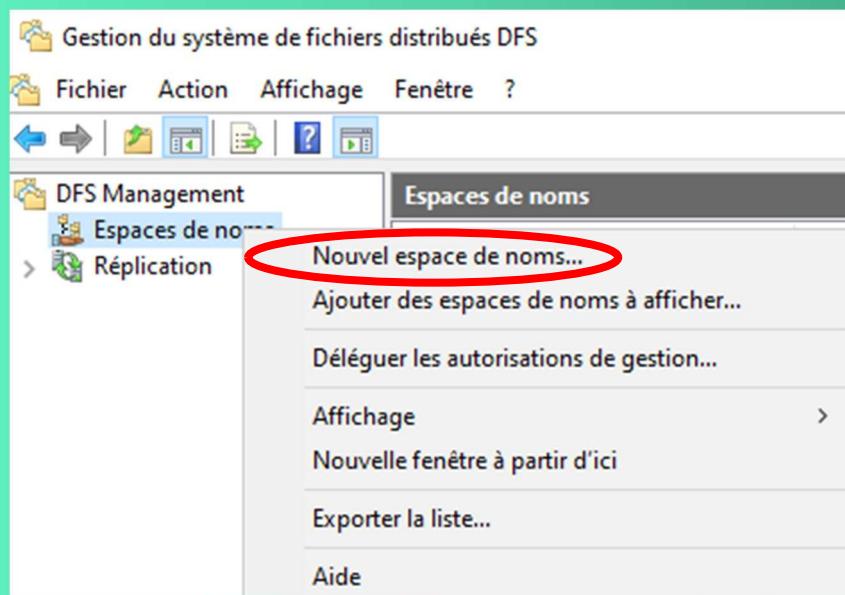
L'infrastructure décrite en début de document nécessite l'utilisation d'une racine de noms de domaine, mais, pour vous montrer la mise en place d'une racine autonome voici la procédure à suivre.

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... ».



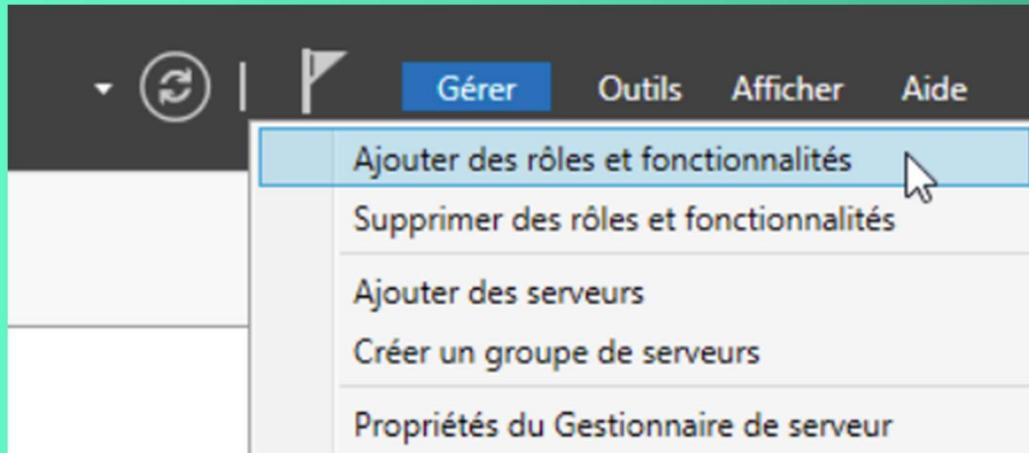
Indiquez le serveur d'espaces de noms qui hébergera donc les espaces de noms, ce serveur n'a pas vocation à héberger lui-même les données. En effet, il sert uniquement de redirecteur entre vos dossiers DFS virtuels et les dossiers partagés physiques qui contiennent les données, des données qui sont stockées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

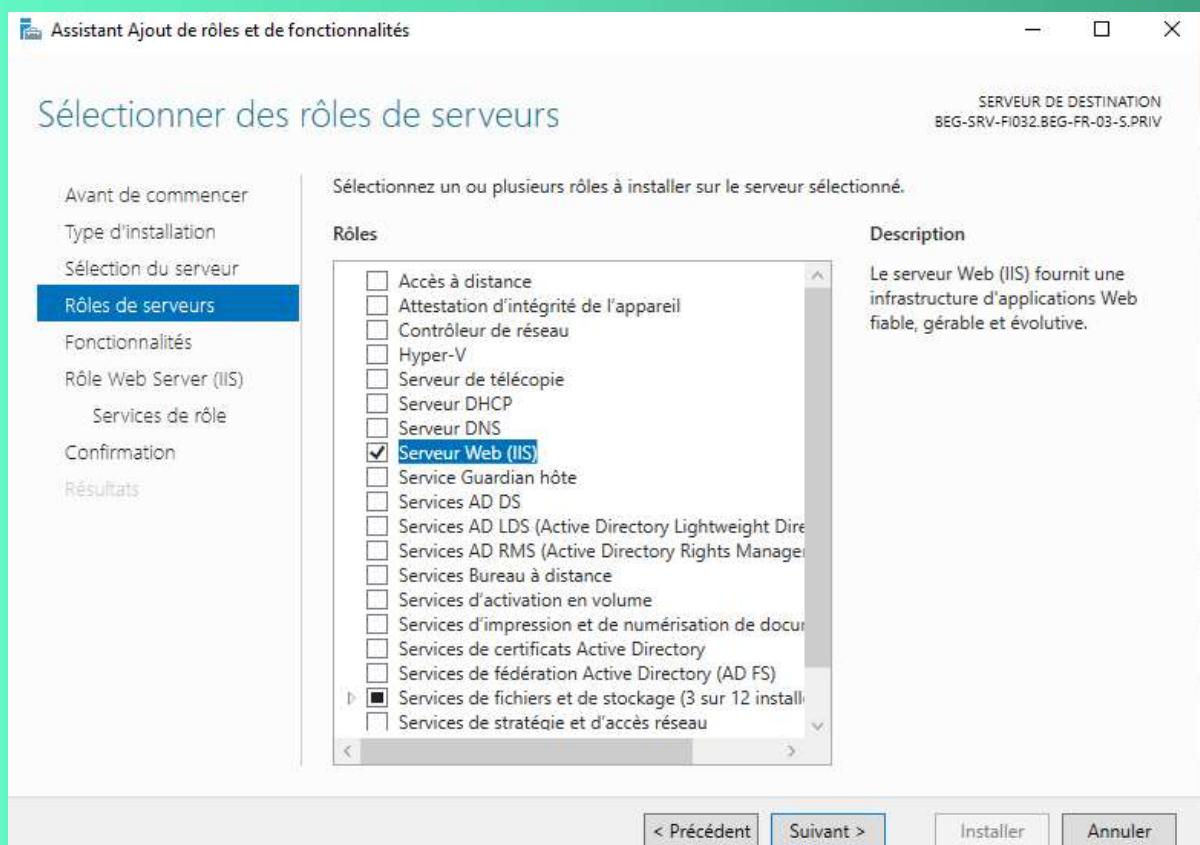
Cliquez sur « Parcourir... » pour rechercher le serveur qui hébergera l'espace de noms en cours de création. Cliquez sur « Suivant » une fois la sélection effectuée.

INSTALLER LE SERVICE IIS ET ROLE FTP

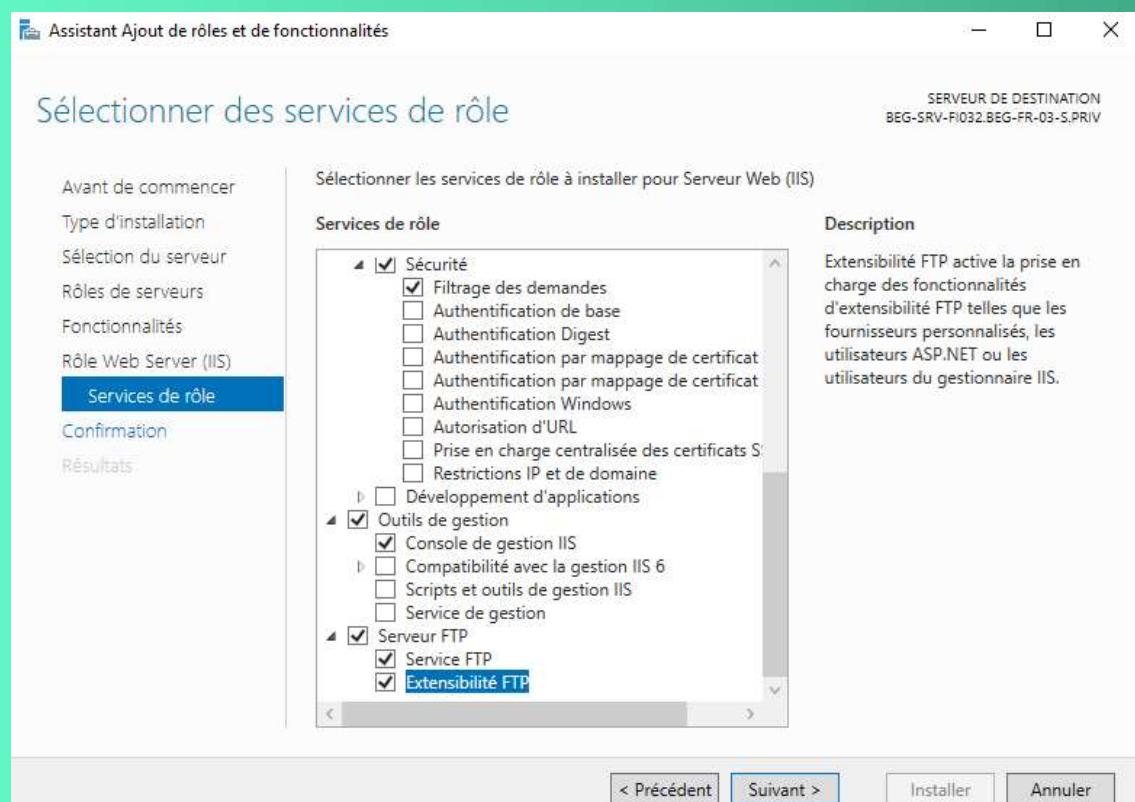
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur ‘Gérer’ et ‘Ajouter des rôles et fonctionnalités’.



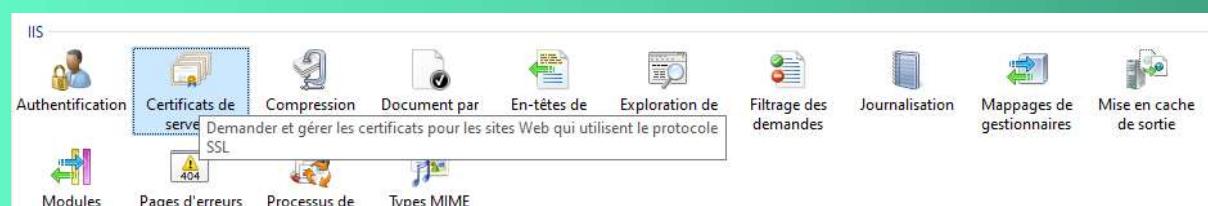
Dans l'onglet ‘Rôles de serveurs’, cocher ‘Serveur Web (IIS)’



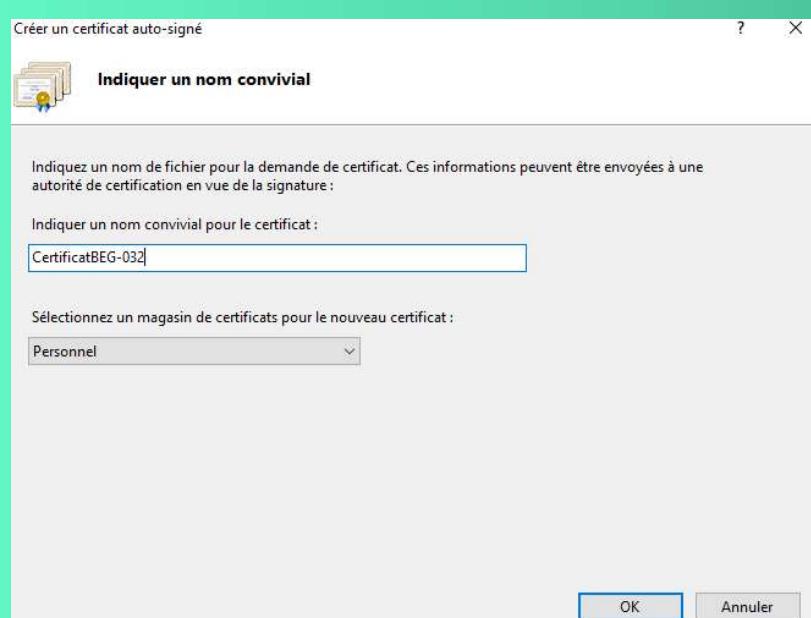
Dans l'onglet 'Services de rôle', cocher 'Service FTP' et 'Extensibilité FTP'



Créer le certificat



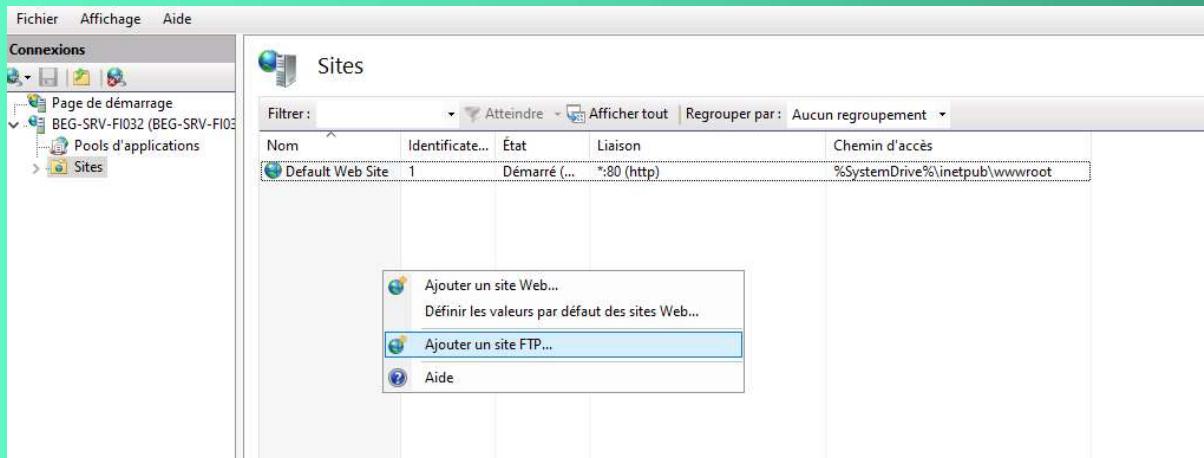
Créer un certificat autosigné



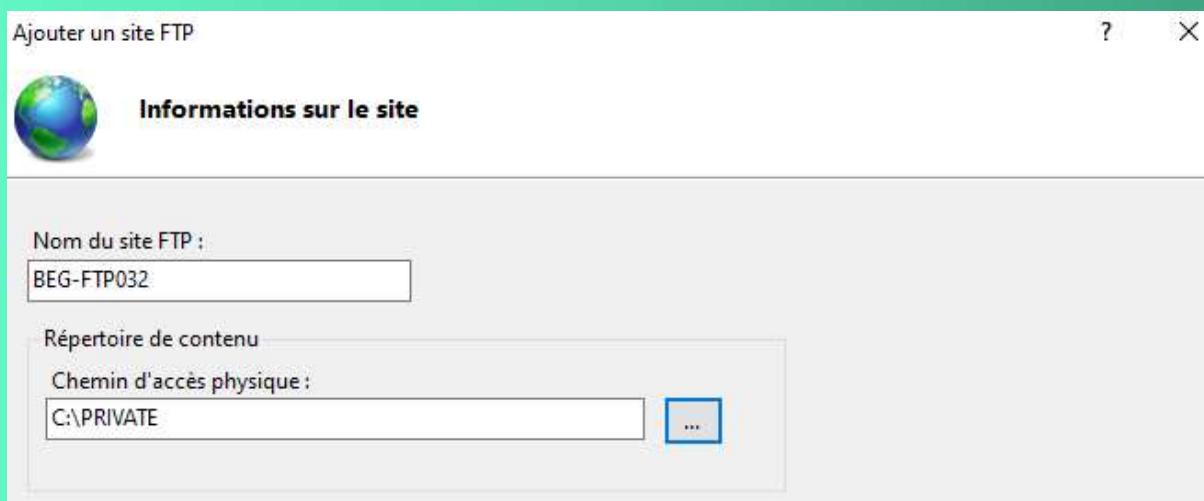
Configurer un site FTP :

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

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

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

Ajouter un site FTP

Informations sur les autorisations et l'authentification

Authentification

Anonyme De base

Autorisation

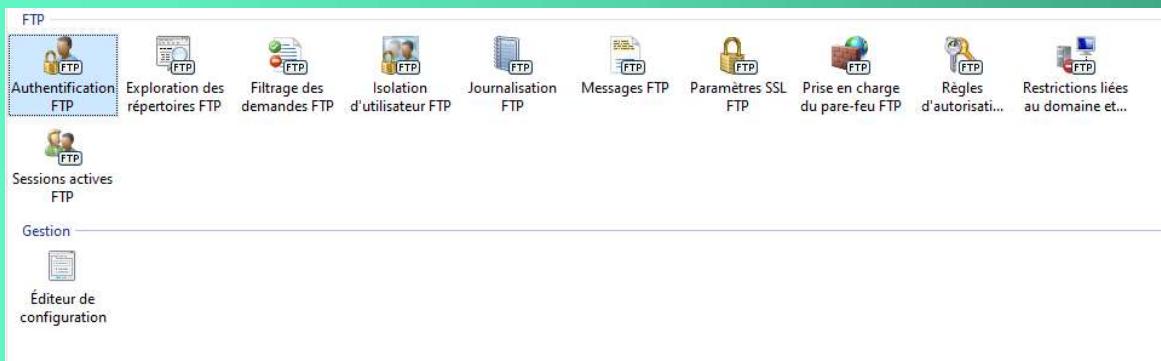
Autoriser l'accès à : Rôles ou groupes d'utilisateurs définis

BEG-FR

Autorisations

Lecture Écriture

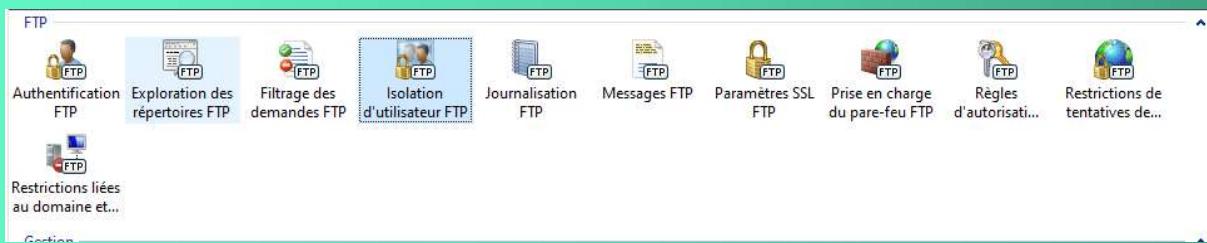
Configurer l'isolation des utilisateurs :



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

Définir les informations d'identification

Nom d'utilisateur :

Mot de passe :

Confirmer le mot de passe :

OK **Annuler**