DOCUMENTATION

Documentation IUTO

Réalisé le 24 Mai 2025

Rédigé par : MICHEL Thibaud & ROCHON Guillaume

Révisé par : MICHEL Thibaud & ROCHON Guillaume

Validé par : MICHEL Thibaud & ROCHON Guillaume

Table des matières

INTRODUCTION

Cette documentation décrit la mise en place et la configuration complète d'une infrastructure informatique pour l'IUT d'Orléans. Elle couvre l'installation et la configuration de divers services essentiels, tels qu'un Active Directory, un serveur de fichiers, un serveur d'impression, des outils de sauvegarde, des solutions de gestion (GLPI, Zabbix), des services collaboratifs (OwnCloud, Kanboard), ainsi que la sécurisation du réseau via un pare-feu Stormshield et des switchs configurés avec VLAN.

Objectifs :

- Centraliser la gestion des utilisateurs et des ressources avec Active Directory.
- Offrir des services partagés (fichiers, impressions) sécurisés et optimisés.
- Assurer la supervision et la maintenance avec GLPI et Zabbix.
- Faciliter la collaboration via OwnCloud et Kanboard.
- Sécuriser l'accès et le trafic réseau avec des VLAN et un pare-feu.

Public visé :
Cette documentation s'adresse aux administrateurs système et réseaux, ainsi qu'aux techniciens en charge de la maintenance de l'infrastructure. Elle fournit des guides détaillés, des scripts et des captures d'écran pour chaque étape.

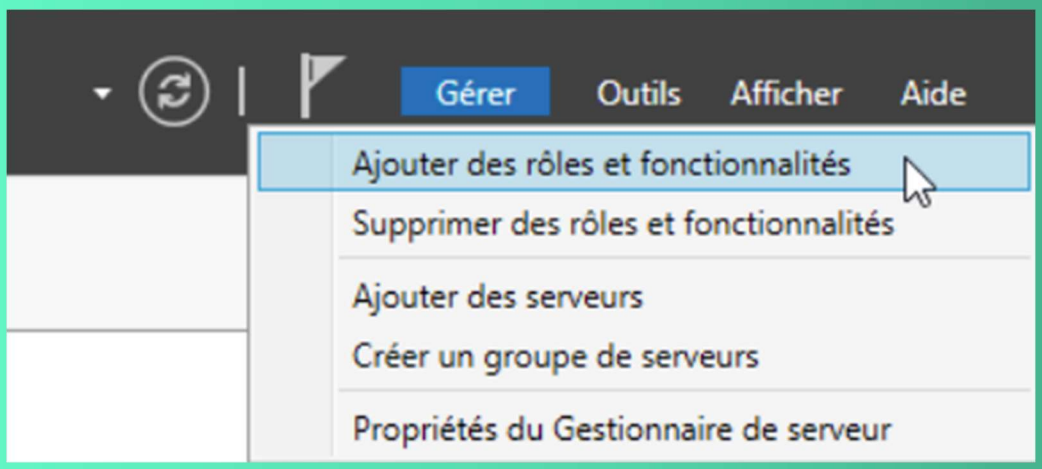
Structure :
Les sections sont organisées par service, avec des sous-parties dédiées à l'installation, la configuration et les tests. Des scripts automatisent les tâches répétitives, et des procédures de vérification garantissent le bon fonctionnement.

Cette infrastructure répond aux besoins pédagogiques et administratifs de l'IUT, en combinant performance, sécurité et facilité de gestion.

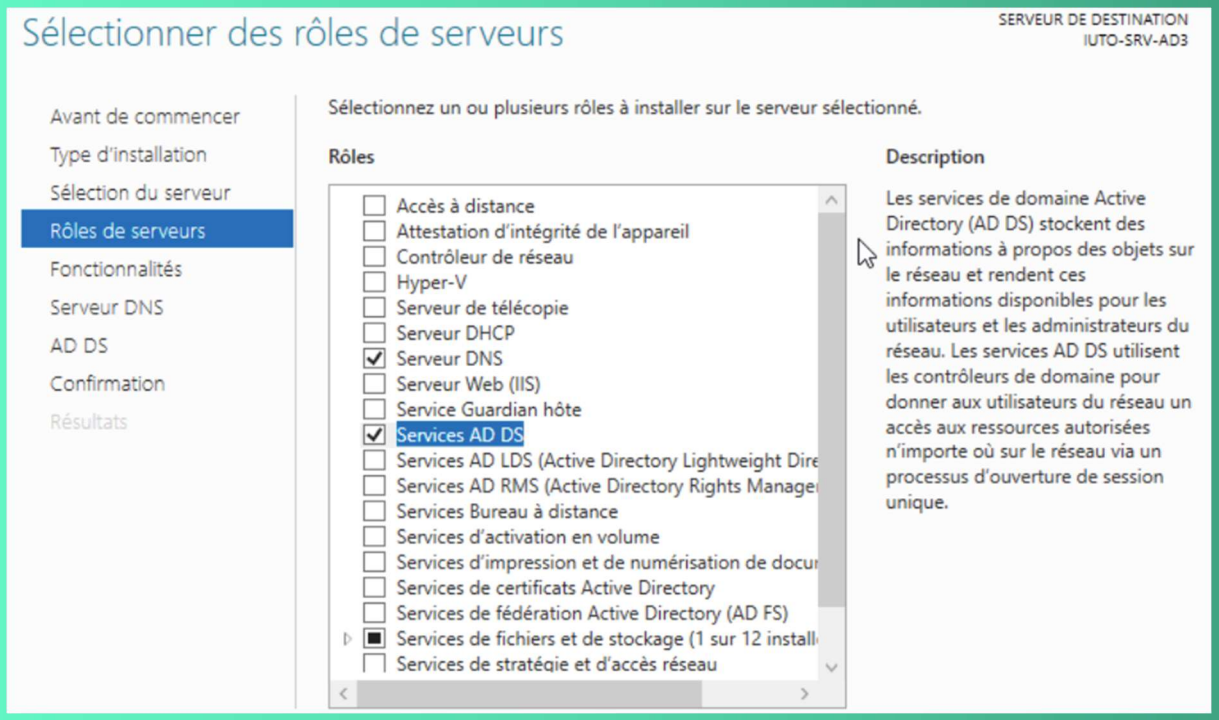
CONFIGURATION D'UN ACTIVE DIRECTORY

Installation du service :

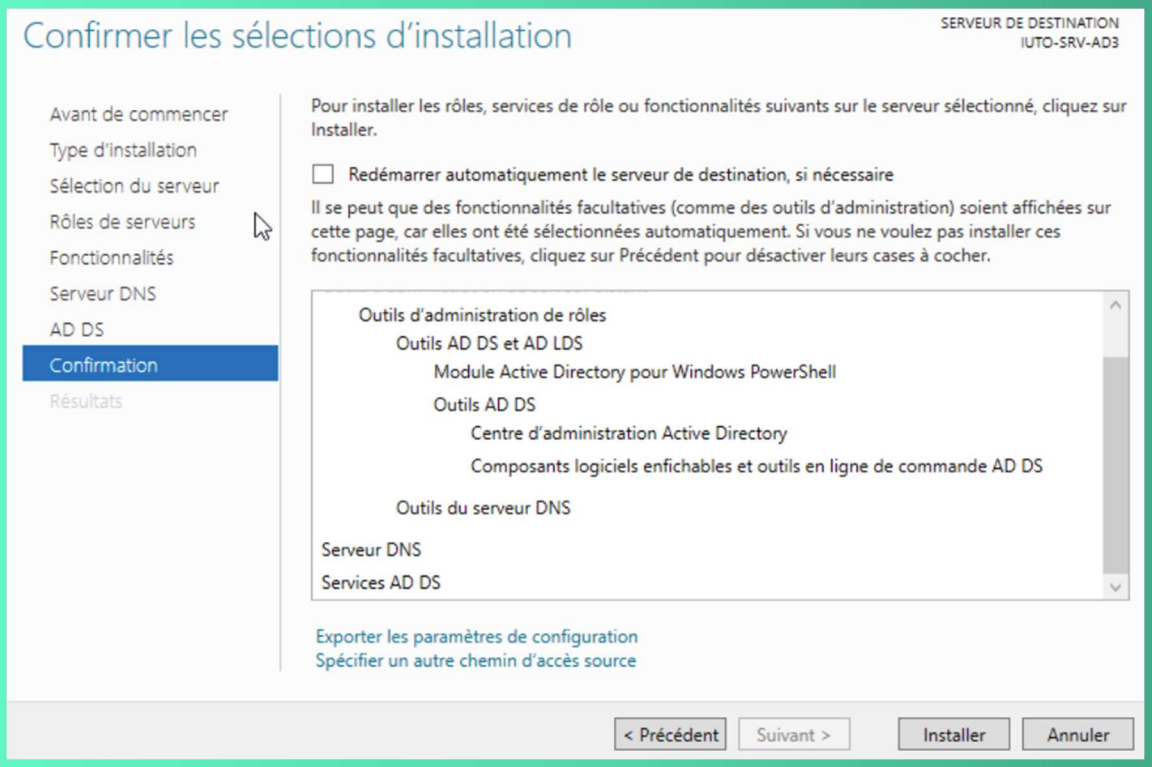
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur 'Gérer' et 'Ajouter des rôles et fonctionnalités'.



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

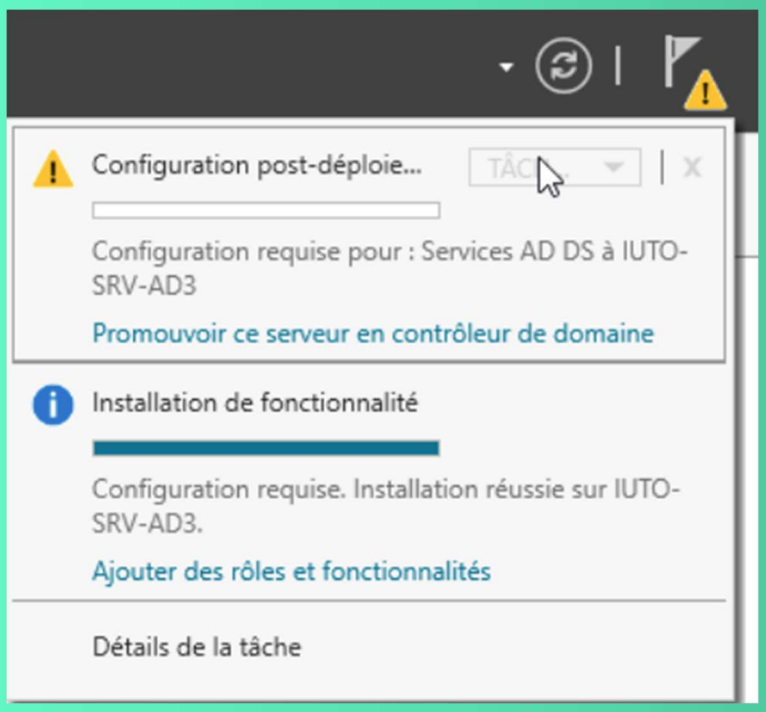


Dans l'onglet 'Confirmation', installer les services



Promouvoir l'AD en tant que contrôleur de domaine :

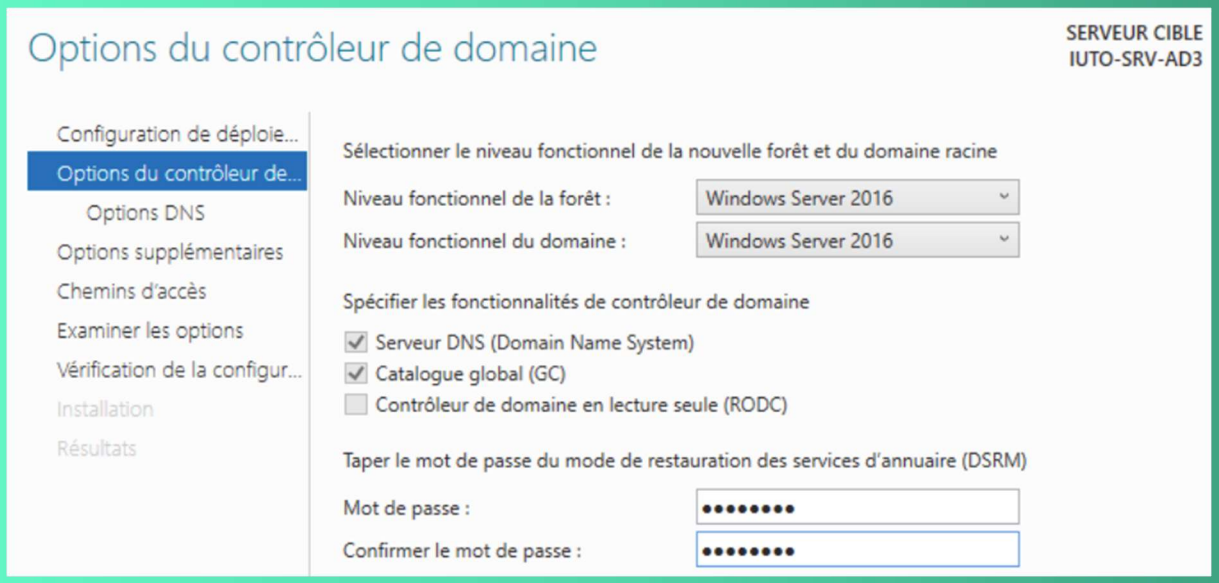
Pour promouvoir l'AD en tant que contrôleur de domaine, il faut cliquer sur le drapeau en haut et cliquer sur 'Promouvoir ce serveur en contrôleur de domaine'.



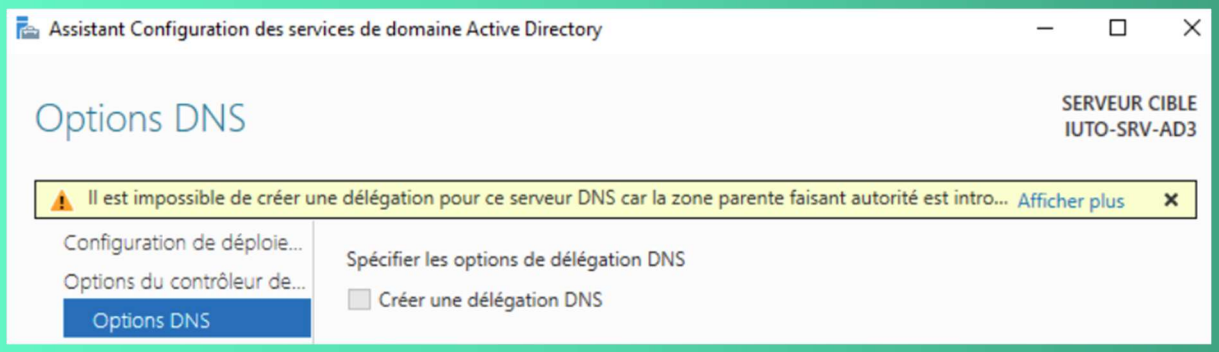
Configuration du contrôleur de domaine :

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

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

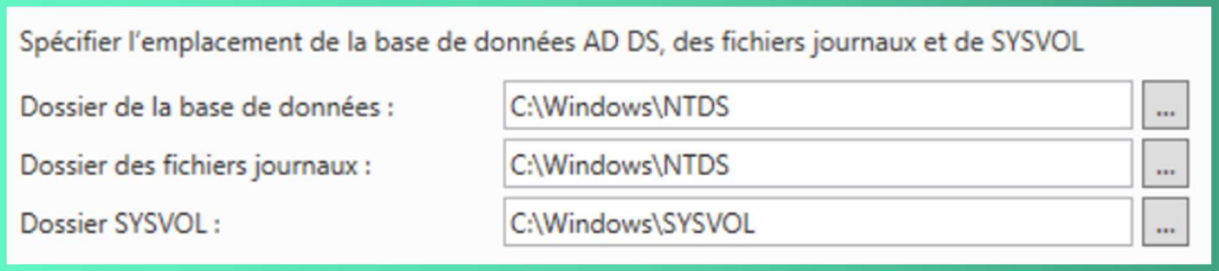


Ne pas créer de délégation DNS car l'AD est aussi serveur DNS

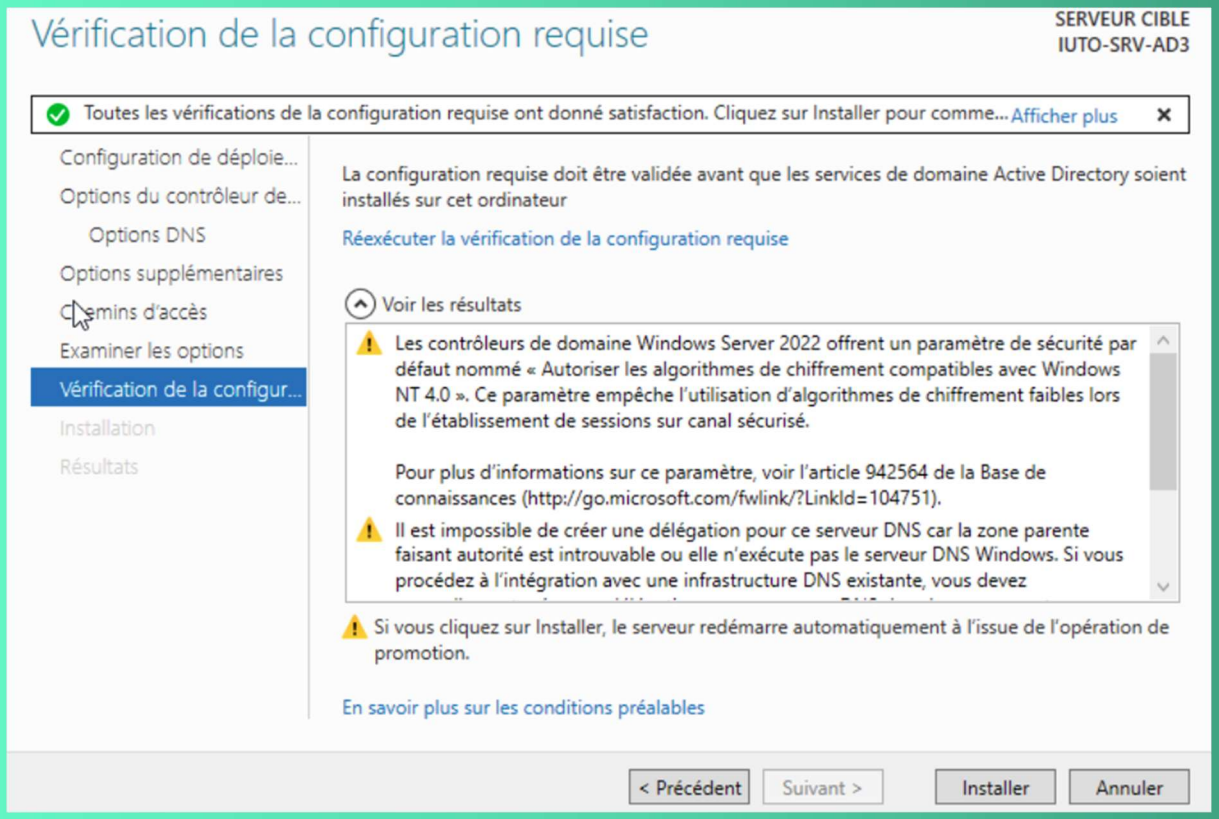


Vérifier le nom de domaine NetBIOS

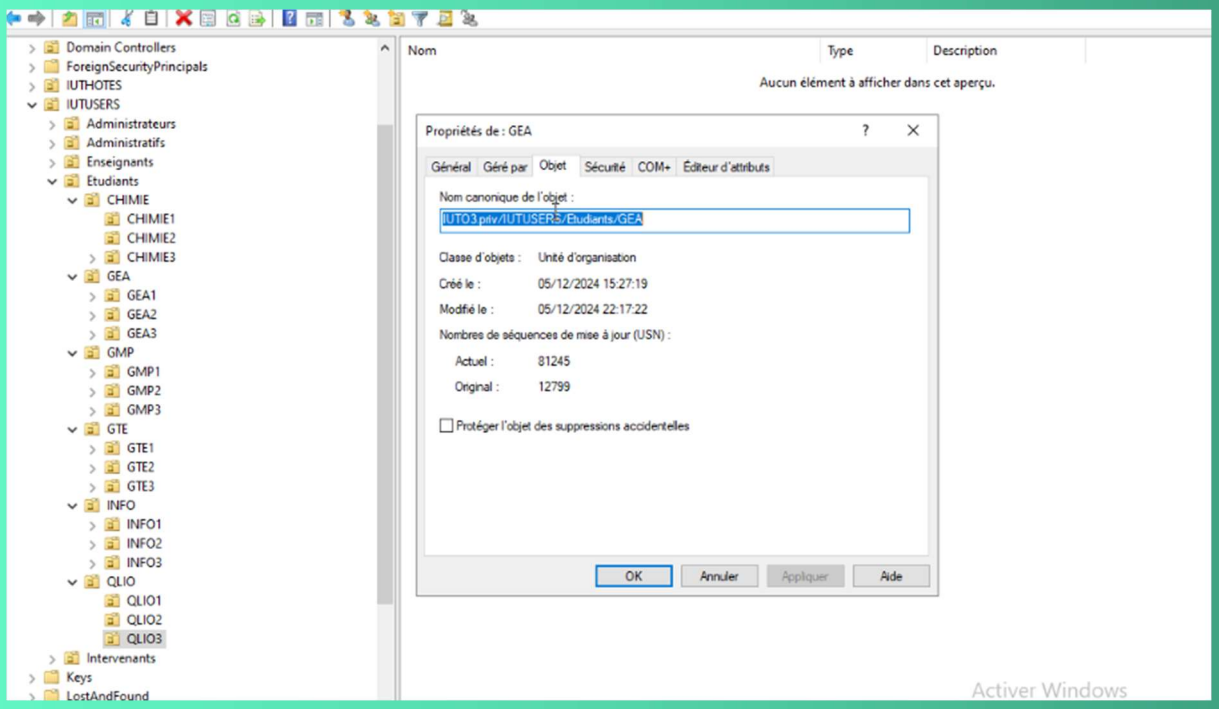
Ne pas modifier les chemins d'accès



Installation de la configuration contrôleur de domaine



Création de l'arborescence utilisateurs :



Intégration des étudiants dans l'unité d'organisation TMP :

Pour intégrer les étudiants de l'IUT d'Orléans dans l'AD, nous avons utilisé un script

```
# Spécifiez le chemin vers le fichier CSV
$CSVFile = "C:\Users\Administrateur\Desktop\import.csv"

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

# Initialiser le compteur pour suivre les utilisateurs créés avec succès
$Compteur = 0

foreach ($Utilisateur in $CSVData) {
  # Récupérer les informations utilisateur
  $UtilisateurPrenom = $Utilisateur.prenom
  $UtilisateurNom = $Utilisateur.nom
  $UtilisateurLogin = $Utilisateur.id
  $UtilisateurEmail = $Utilisateur.email
  $UtilisateurMotDePasse = $Utilisateur.password
  $UtilisateurFormation = $Utilisateur.formation

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

  # Générer SamAccountName unique
  $SamAccountName = $UtilisateurLogin
  $Suffix = 1
  while (Get-ADUser -Filter { SamAccountName -eq $SamAccountName }) {
    $SamAccountName = "${UtilisateurLogin}${Suffix}"
    $Suffix++
  }

  # Générer UserPrincipalName unique
  $UserPrincipalName = "$SamAccountName@IUTO3.priv"
  while (Get-ADUser -Filter { UserPrincipalName -eq $UserPrincipalName }) {
    $UserPrincipalName = "${SamAccountName}-${Suffix}@IUTO3.priv"
    $Suffix++
  }

  # Générer DisplayName unique
  $DisplayName = "$UtilisateurNom $UtilisateurPrenom"
  $Suffix = 1
  while (Get-ADUser -Filter { DisplayName -eq $DisplayName }) {
    $DisplayName = "$UtilisateurNom $UtilisateurPrenom-$Suffix"
    $Suffix++
  }

  Try {
    # Créer l'utilisateur
    New-ADUser -Name $DisplayName `
          -DisplayName $DisplayName `
          -GivenName $UtilisateurPrenom `
          -Surname $UtilisateurNom `
          -SamAccountName $SamAccountName `
          -UserPrincipalName $UserPrincipalName `
          -EmailAddress $UtilisateurEmail `
          -Title $UtilisateurFormation `
          -Path "OU=TMP,DC=IUTO3,DC=priv" `
          -AccountPassword (ConvertTo-SecureString -AsPlainText -Force $UtilisateurMotDePasse) `
          -Enabled $true `
          -PasswordNeverExpires $true `
          -CannotChangePassword $true
    Write-Output "Création de l'utilisateur : $SamAccountName ($UtilisateurNom $UtilisateurPrenom)"
    $Compteur++ # Incrementer le compteur
  } catch {
    Write-Error "Erreur lors de la création de l'utilisateur $SamAccountName : $_.Exception.Message"
  }
}

# Afficher le nombre total d'utilisateurs créés
Write-Output "Nombre total d'utilisateurs crees : $Compteur"

# Attente de 5 secondes avant de fermer la fenêtre
Start-Sleep -Seconds 5
```

Intégration des étudiants de l'unité d'organisation TMP dans leur promotion :

Pour intégrer les étudiants de l'IUT d'Orléans précédemment dans TMP pour vérifier leur bonne intégration, nous avons utilisé un autre script pour ranger les étudiants dans leur promotion.

```
# Spécifiez le chemin vers l'UO source (TMP)
$SourceOU = "OU=TMP,DC=IUTO3,DC=priv"

# Dossier racine des formations
$RacineOU = "OU=Etudiants,OU=IUTUSERS,DC=IUTO3,DC=priv"

# Liste des formations possibles
$Formations = @("GEA", "GTE", "GMP", "QLIO", "INFO", "CHIMIE")
$Niveaux = @("1", "2", "3")

# Récupérer les utilisateurs de l'UO TMP
Try {
  $Utilisateurs = Get-ADUser -Filter * -SearchBase $SourceOU -Properties Title | Where-Object { $_.Title -ne $null }
  Write-Output "Nombre d'utilisateurs récupérés dans TMP : $($Utilisateurs.Count)"
} catch {
```

```
    Write-Error "Erreur lors de la recuperation des utilisateurs de l'UO TMP : $_"
    exit
}

# Déplacer chaque utilisateur dans la bonne UO en fonction de sa formation et son niveau
foreach ($Utilisateur in $Utilisateurs) {
    # Extraction de la formation et du niveau à partir du champ "Title" (ex: GSA1, INFO2)
    if ($Utilisateur.Title -match "^([A-Z]+)([1-3]*)") {
        $Formation = $Matches[1]  # Ex : GSA, INFO
        $Niveau = $Matches[2]     # Ex : 1, 2, 3

        # Vérifier si la formation et le niveau sont valides
        if ($Formations -contains $Formation -and $Niveaux -contains $Niveau) {
            # Construire le chemin cible de l'UO
            $TargetOU = "OU=$Formation$Niveau,OU=$Formation,$RacineOU"

            # Déplacer l'utilisateur dans l'UO cible
            try {
                Move-ADObject -Identity $Utilisateur.DistinguishedName -TargetPath $TargetOU
                Write-Output "Utilisateur $($Utilisateur.SamAccountName) déplacé dans $TargetOU"
            } catch {
                Write-Warning "Impossible de déplacer l'utilisateur $($Utilisateur.SamAccountName) dans $TargetOU : $_"
            }
        } else {
            Write-Warning "Formation ou niveau invalide pour l'utilisateur $($Utilisateur.SamAccountName) : $($Utilisateur.Title)"
        }
    } else {
        Write-Warning "Le format de la formation/niveau est invalide pour l'utilisateur $($Utilisateur.SamAccountName) : $($Utilisateur.Title)"
    }
}

# Résumé
Write-Output "Traitement terminé pour les utilisateurs de l'UO TMP."
```

Intégration des enseignants dans l’unité d’organisation TMP :

```
# Spécifiez le chemin vers le fichier CSV
$CSVFile = "C:\Users\Administrateur\Desktop\cvsenseignants.csv"

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

# Initialiser le compteur pour suivre les utilisateurs créés avec succès
$Compteur = 0

foreach ($Utilisateur in $CSVData) {
    # Récupérer les informations utilisateur
    $UtilisateurPrenom = $Utilisateur.prenom
    $UtilisateurNom = $Utilisateur.nom
    $UtilisateurLogin = $Utilisateur.id
    $UtilisateurEmail = $Utilisateur.email
    $UtilisateurMotDePasse = $Utilisateur.password
    $UtilisateurFormation = $Utilisateur.formation

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

    # Générer SamAccountName unique
    $SamAccountName = $UtilisateurLogin
    $Suffix = 1
    while (Get-ADUser -Filter { SamAccountName -eq $SamAccountName }) {
        $SamAccountName = "$($UtilisateurLogin)$Suffix"
        $Suffix++
    }

    # Générer UserPrincipalName unique
    $UserPrincipalName = "$SamAccountName@ltUTO3.priv"
    while (Get-ADUser -Filter { UserPrincipalName -eq $UserPrincipalName }) {
        $UserPrincipalName = "$($SamAccountName)-$Suffix@ltUTO3.priv"
        $Suffix++
    }

    # Générer DisplayName unique
    $DisplayName = "$UtilisateurNom $UtilisateurPrenom"
    $Suffix = 1
    while (Get-ADUser -Filter { DisplayName -eq $DisplayName }) {
        $DisplayName = "$UtilisateurNom $UtilisateurPrenom-$Suffix"
        $Suffix++
    }

    try {
        # Creer l'utilisateur
        New-ADUser -Name $DisplayName `
                   -DisplayName $DisplayName `
                   -GivenName $UtilisateurPrenom `
                   -Surname $UtilisateurNom `
                   -SamAccountName $SamAccountName `
                   -UserPrincipalName $UserPrincipalName `
                   -EmailAddress $UtilisateurEmail `
                   -Title $UtilisateurFormation `
                   -Path "OU=TMP,DC=ltUTO3,DC=priv" `
                   -AccountPassword (ConvertTo-SecureString -AsPlainText -Force $UtilisateurMotDePasse) `
                   -Enabled $true `
                   -PasswordNeverExpires $true `
                   -CannotChangePassword $true
        Write-Output "Creation de l'utilisateur : $SamAccountName ($UtilisateurNom $UtilisateurPrenom)"
        $Compteur++ # Incrementer le compteur
    } catch {
        Write-Error "Erreur lors de la création de l'utilisateur $SamAccountName : $_.Exception.Message"
    }
}

# Afficher le nombre total d'utilisateurs créés
Write-Output "Nombre total d'utilisateurs crees : $Compteur"

# Attente de 5 secondes avant de fermer la fenêtre
Start-Sleep -Seconds 5
```

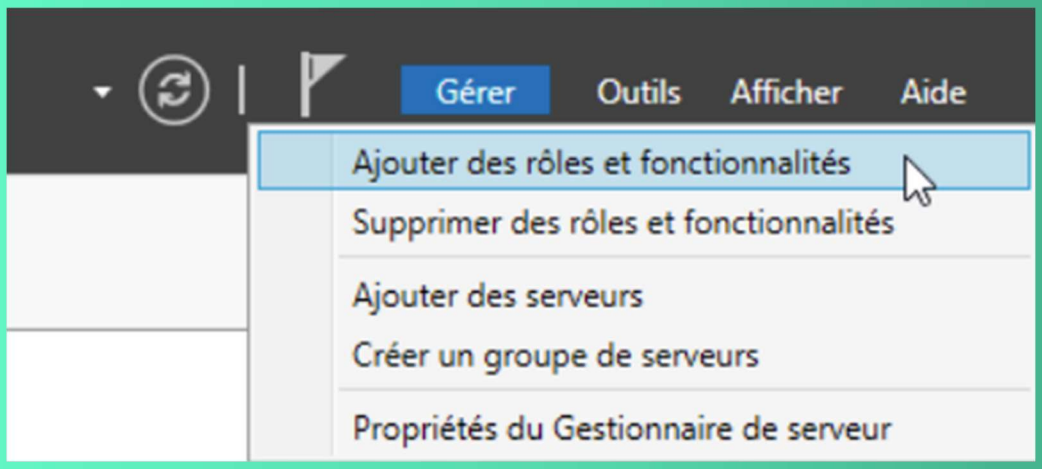
Intégration des enseignants dans l’unité d’organisation enseignants et des intervenants dans l’UO intervenants :

```
# Variables de base
$domain = "ltUTO3.priv"
$TMP_OU = "OU=TMP,DC=ltUTO3,DC=priv"
$Enseignants_OU = "OU=Enseignants,OU=ltUTUSERS,DC=ltUTO3,DC=priv"
$Intervenants_OU = "OU=Intervenants,OU=ltUTUSERS,DC=ltUTO3,DC=priv"

# Importer le module Active Directory (si non automatique)
Import-Module ActiveDirectory

# Récupérer les utilisateurs dans l'OU TMP
$Users = Get-ADUser -Filter * -SearchBase $TMP_OU -Properties Title

if ($Users) {
    foreach ($User in $Users) {
        # Vérifier l'attribut Title
        if ($User.Title -like "*pro*") {
            #Déplacer vers Intervenants
            Write-Host "Déplacement de l'utilisateur $($User.SamAccountName) -> Intervenants"
            Move-ADObject -Identity $User.DistinguishedName -TargetPath $Intervenants_OU
        } else {
            #Déplacer vers Enseignants
            Write-Host "Déplacement de l'utilisateur $($User.SamAccountName) -> Enseignants"
            Move-ADObject -Identity $User.DistinguishedName -TargetPath $Enseignants_OU
        }
    }
} else {
    Write-Host "Aucun utilisateur trouvé dans l'OU TMP."
}

Write-Host "Traitement terminé."
```

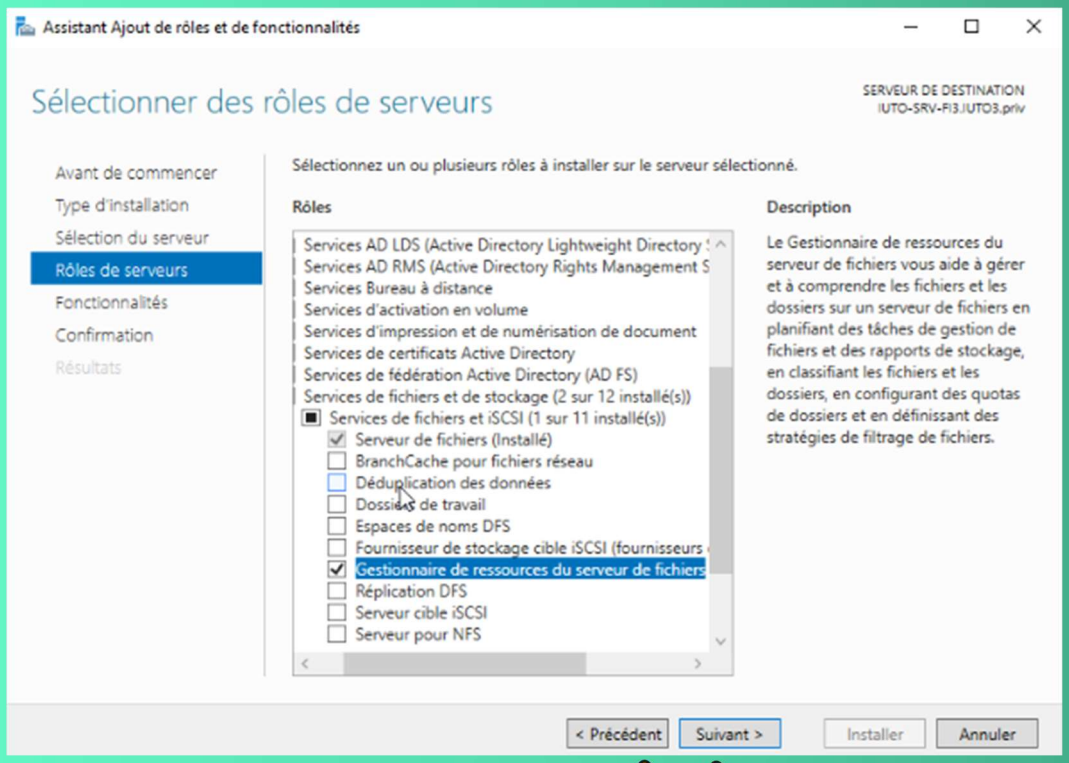
CONFIGURATION DU SERVEUR DE FICHIER

Installation du service :

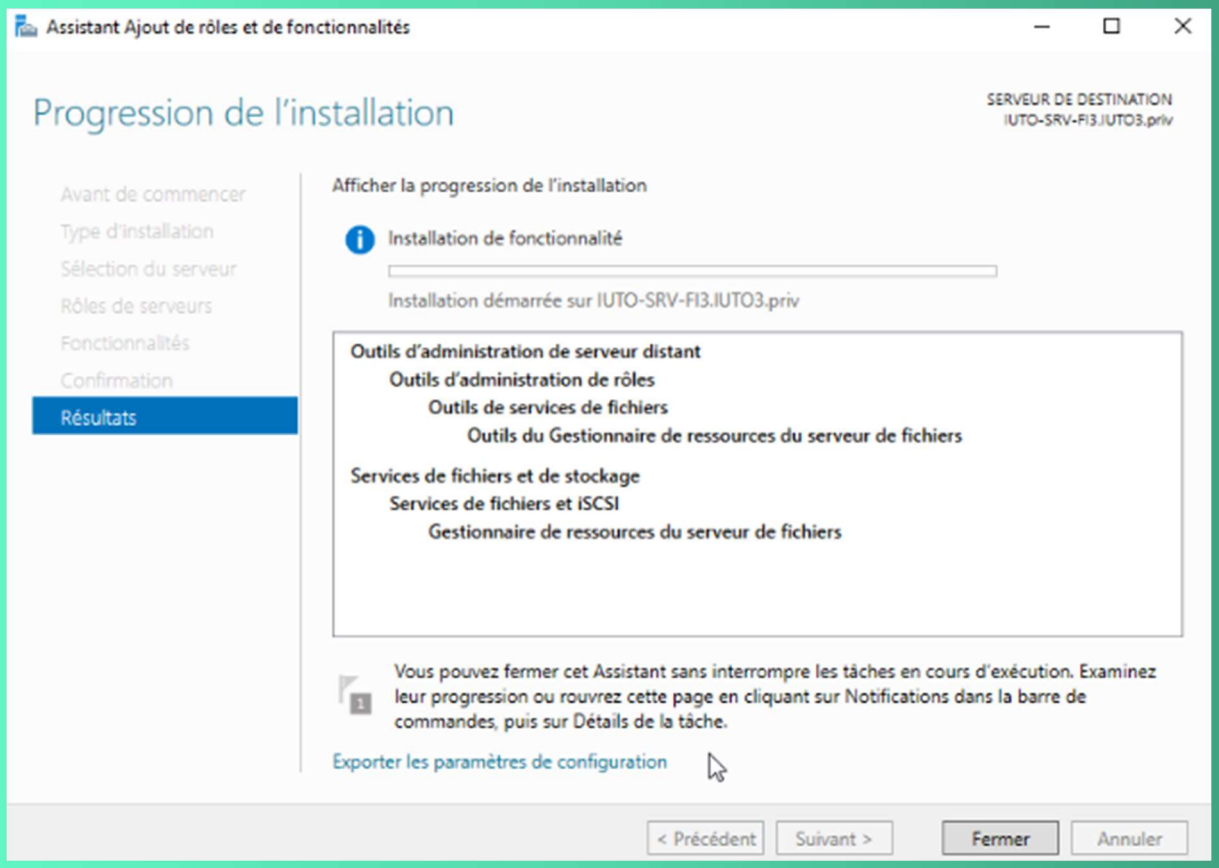
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur ‘Gérer’ et ‘Ajouter des rôles et fonctionnalités’.



Dans l’onglet ‘Rôles de serveurs’, cocher ‘Services de fichiers et iSCSi’ et ‘Gestionnaire de ressources serveur de fichiers’.



Installer le service

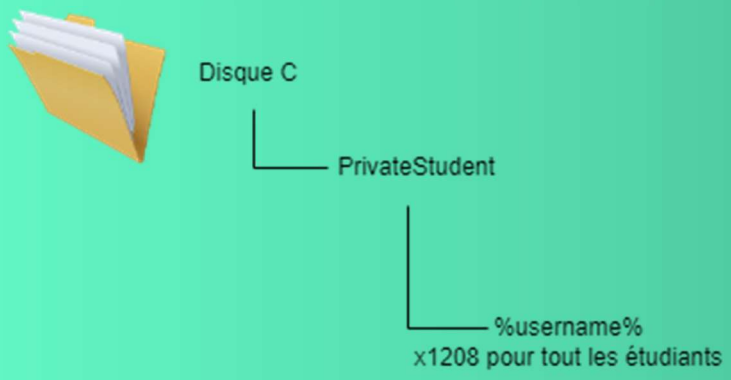


CRÉATION DES DOSSIERS PRIVÉS DES ÉTUDIANTS :

Arborescence des fichiers privés des étudiants :

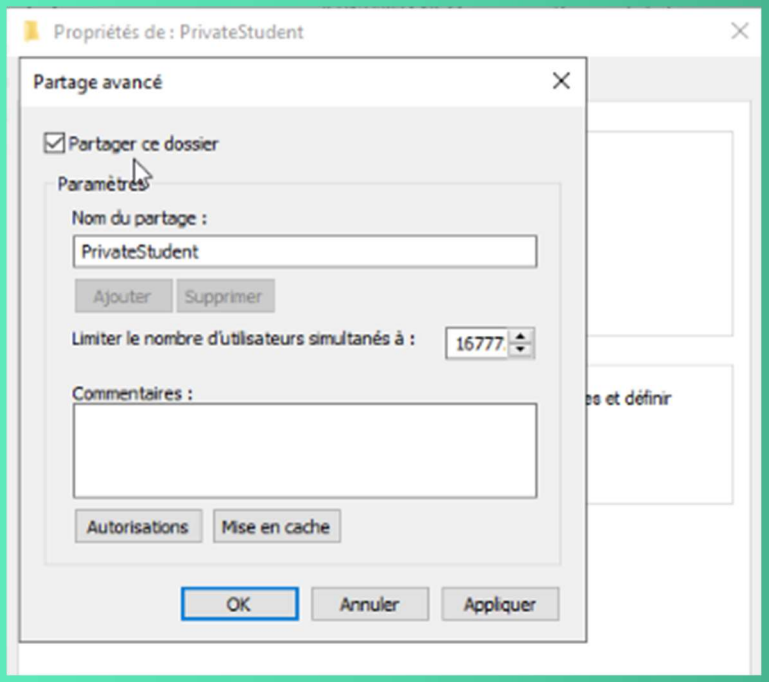
Le dossier PrivateStudent est situé sur le disque C:\PrivateStudent sur le serveur de fichier.

Tous les dossiers privés des étudiants seront enregistrés ici.

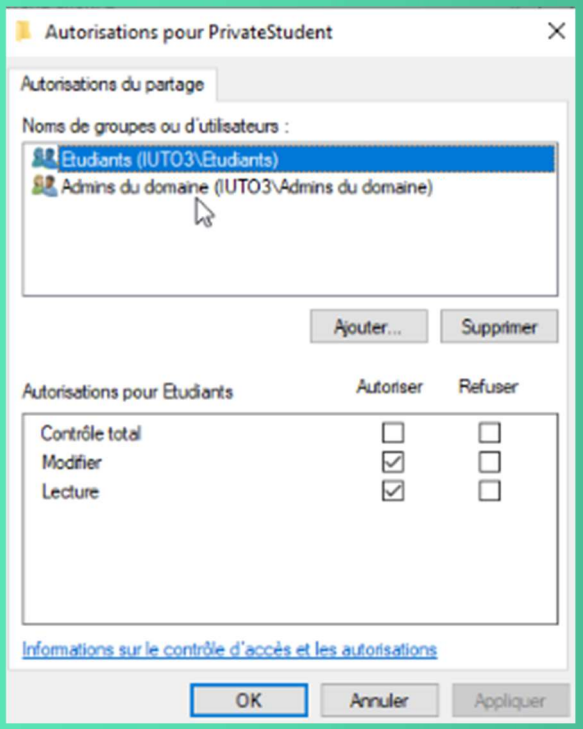


Partage du dossier :

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

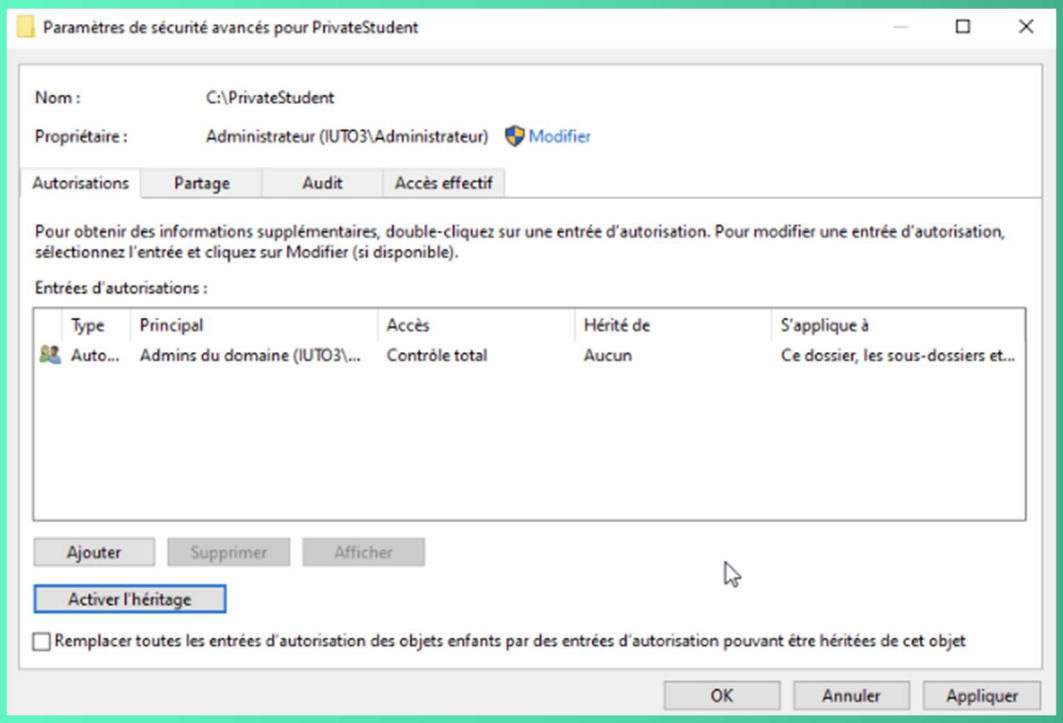


Ajouter l'autorisation contrôle total au groupe 'Admins du domaine' et Lecture et Modifier au groupe 'Etudiants'.

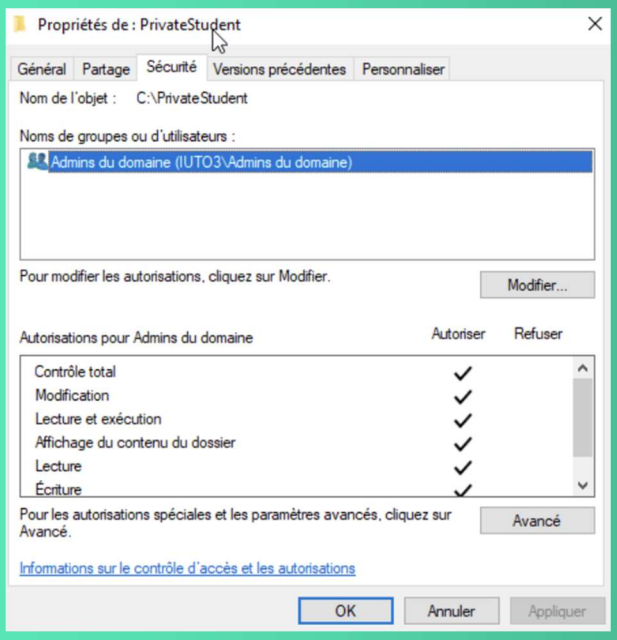


Permissions NTFS :

Il faut désactiver l'héritage dans les paramètres de sécurités avancés du dossier PrivateStudent



Ensuite, pour configurer le permissions NTFS, il faut aller dans l'onglet sécurité puis sur modifier et ajouter le groupe admins du domaine en contrôle total



Script de création des dossiers pour chaque utilisateur + permission NTFS :

A exécuter sur l'AD

ScriptDossierPrivateStudent

Script d'ajout des quotas :

ScriptQuota

Test des quotas :

Nous avons créé un fichier texte de 1Go avec la commande :

fsutil file createnew C:\chemin\vers\fichier.txt 1073741824

Puis ensuite essayé de le copier dans les répertoires private et cela ne fonctionne pas.

Les quotas de 1Go ont donc bien été appliqués

CRÉATION DU DOSSIER PRIVÉS DES ENSEIGNANTS :

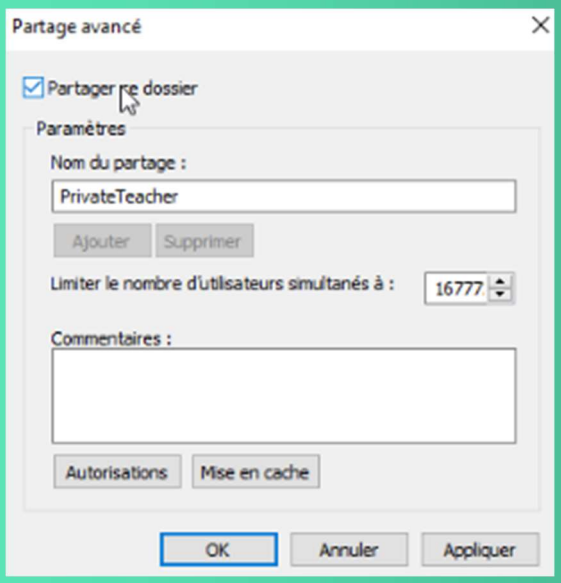
Arborescence des fichiers privés des enseignants :

Le dossier PrivateTeacher est situé sur le disque C:\PrivateTeacher sur le serveur de fichier.

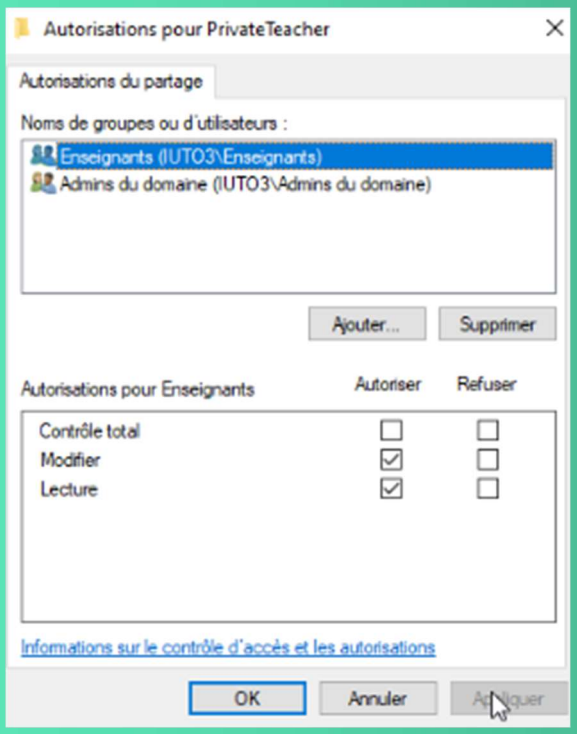
Tous les dossiers privés des enseignants seront enregistrés ici.

Partage du dossier :

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

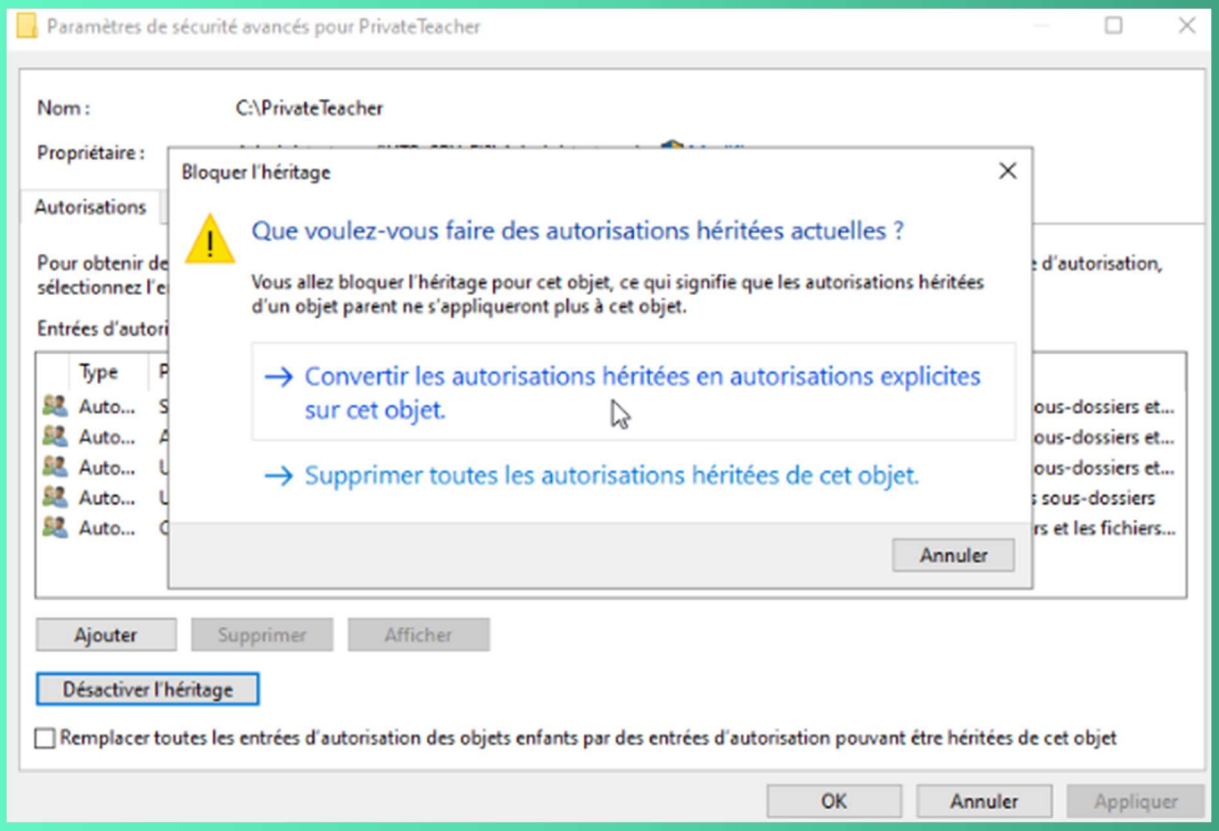


Ajouter l'autorisation contrôle total au groupe 'Admins du domaine' et Lecture et Modifier au groupe 'Enseignants'.

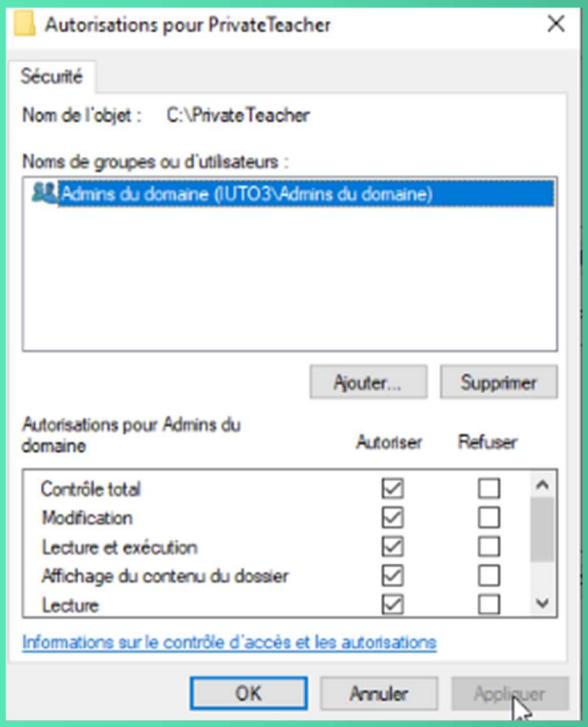


Permissions NTFS :

Il faut désactiver l'héritage dans les paramètres de sécurités avancés du dossier PrivateTeacher



Pour configurer le permissions NTFS, il faut aller dans l'onglet sécurité puis sur modifier et ajouter le groupe 'Admins du domaine' en contrôle total.



Script de création des dossiers pour chaque enseignant + permission NTFS :

Scriptdossierprivateteacher

Script d'ajout des quotas :

ScriptQuota

CRÉATION DU DOSSIER PROMOTIONS POUR LE PARTAGE ENTRE ENSEIGNANTS/ÉLÈVES :

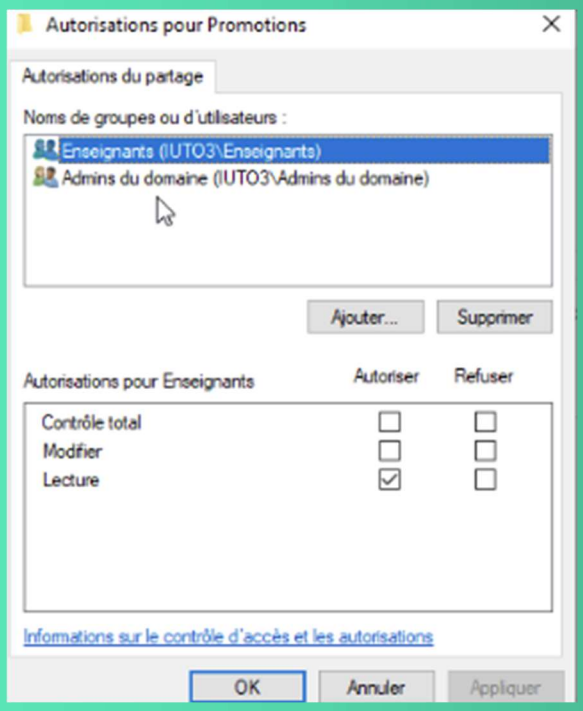
Arborescence du dossier Promotions :

Le dossier Promotions est situé sur le disque C:\Promotions sur le serveur de fichier.

Tous les dossiers Enoncé et Dépôt travail des étudiants seront enregistrés ici.

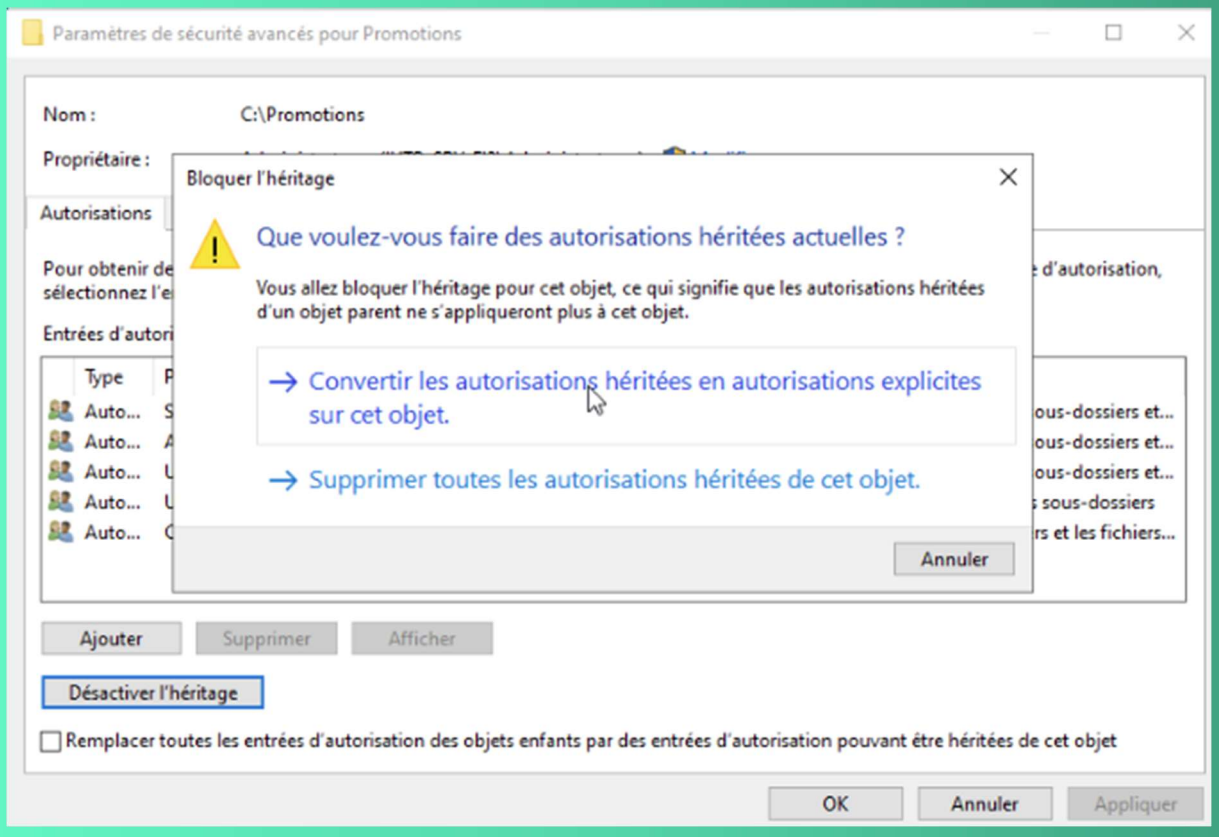
Partage du dossier :

Partager le dossier Promotions avec contrôle total sur le groupe 'Admins du domaine' et Lecture sur le groupe 'Enseignants'

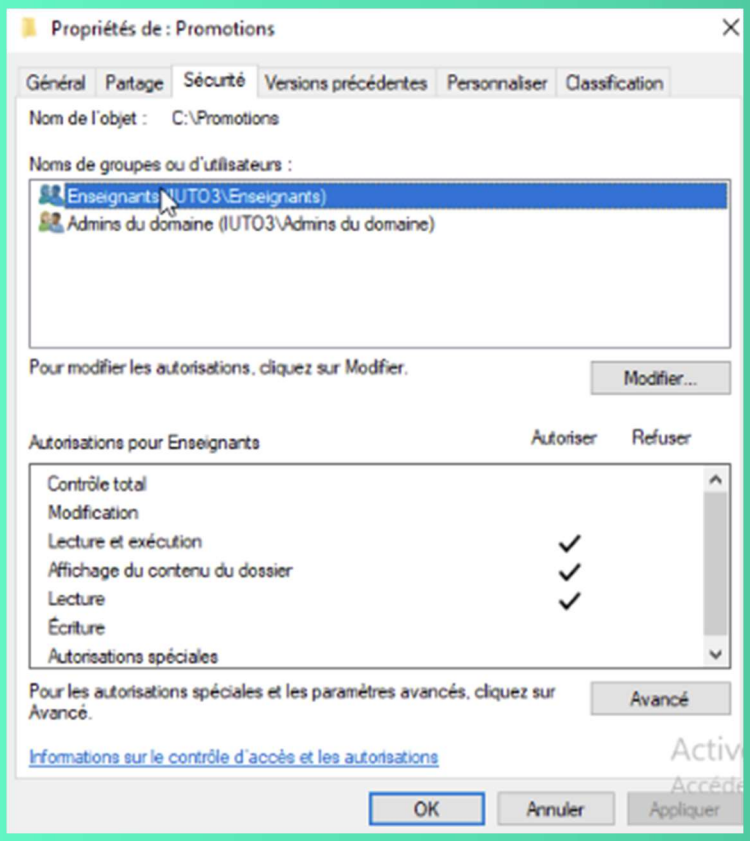


Permissions NTFS :

Il faut désactiver l'héritage dans les paramètres de sécurités avancés du dossier Promotions



Pour configurer le permissions NTFS, il faut aller dans l'onglet sécurité puis sur modifier et ajouter le groupe 'Admins du domaine' en contrôle total. Et Enseignants en Lecture et Exécution



Executer ce script pour partager et deployer les autorisations NTFS de tous les dossiers Enonce et Depot Travail

Script de création des dossiers NTFS + partage :

ScriptdossierpromotionsNTFS

ScriptdossierpromotionsPartage

Création du script pour ajouter les lecteurs réseaux aux utilisateurs :

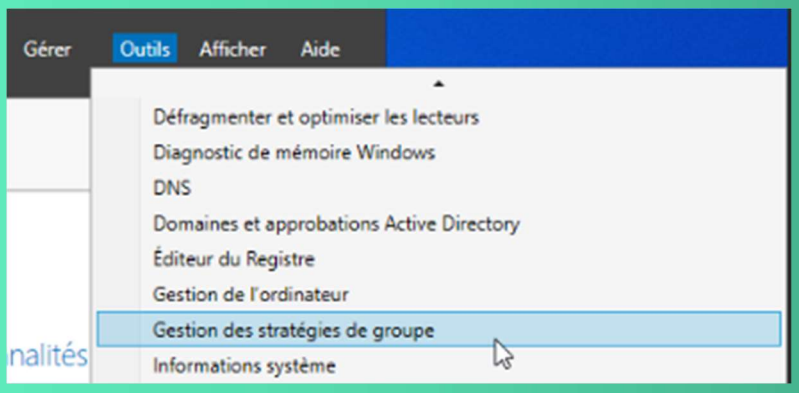
Script qui génère les lecteurs réseaux :

ScriptLecteurReseauEtudiants

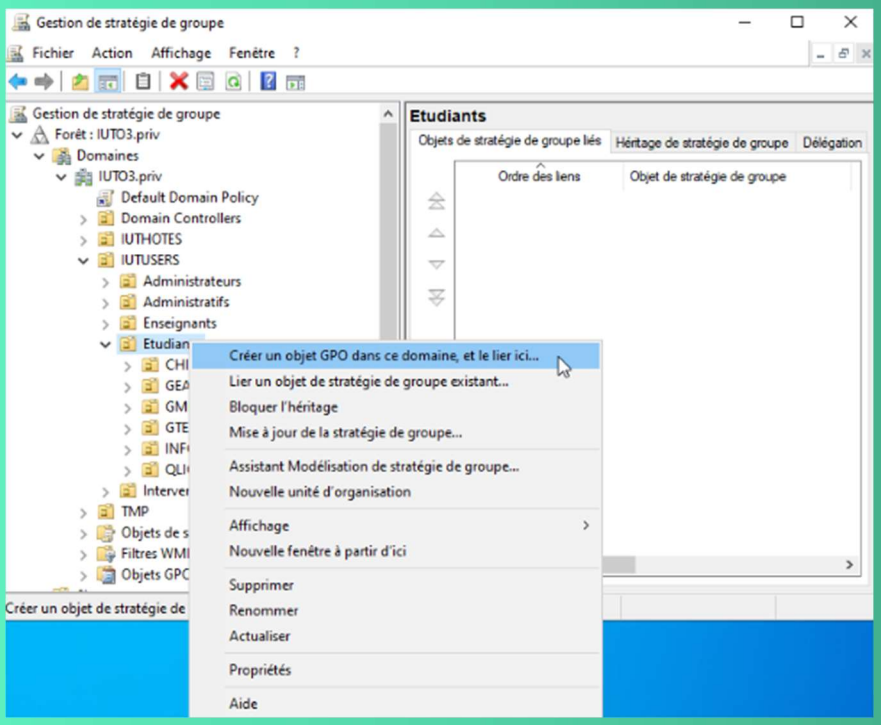
ScriptLecteurReseauEnseignants

Configurer la GPO pour ajouter les lecteurs réseaux :

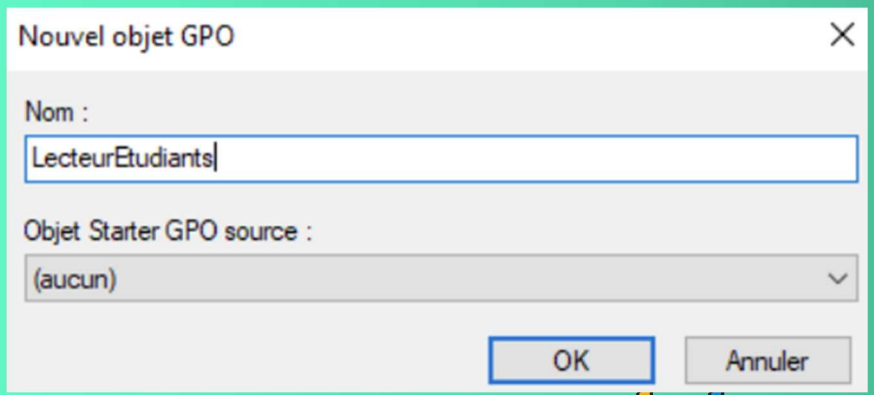
Pour installer le service, lancer le gestionnaire de serveur, puis cliquer sur ‘Outils’ et ‘Gestion des stratégies de groupe.



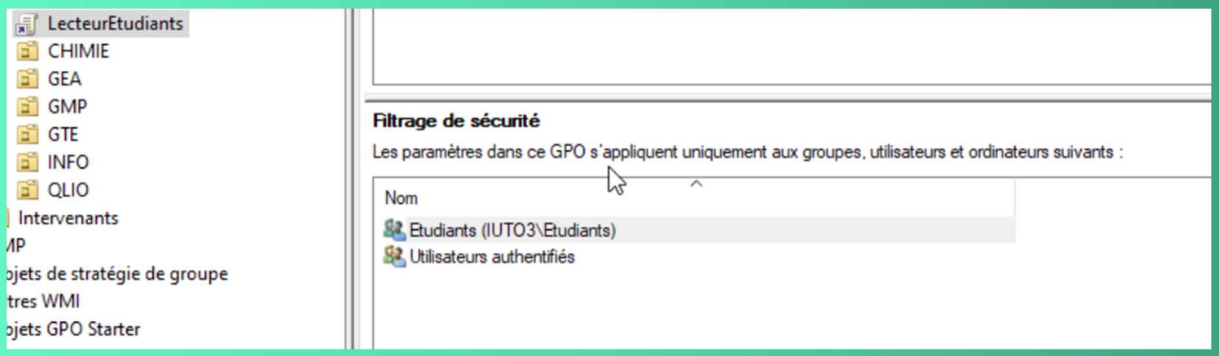
Pour créer une GPO et l’ajouter à l’UO étudiants en suivant ce chemin ‘Forêt : IUTO3.priv, Domaines, IUTO3.priv, IUTUSERS, Etudiants’ puis faire un clic droit puis ‘Créer un objet GPO dans ce domaine, et le lier ici…’.



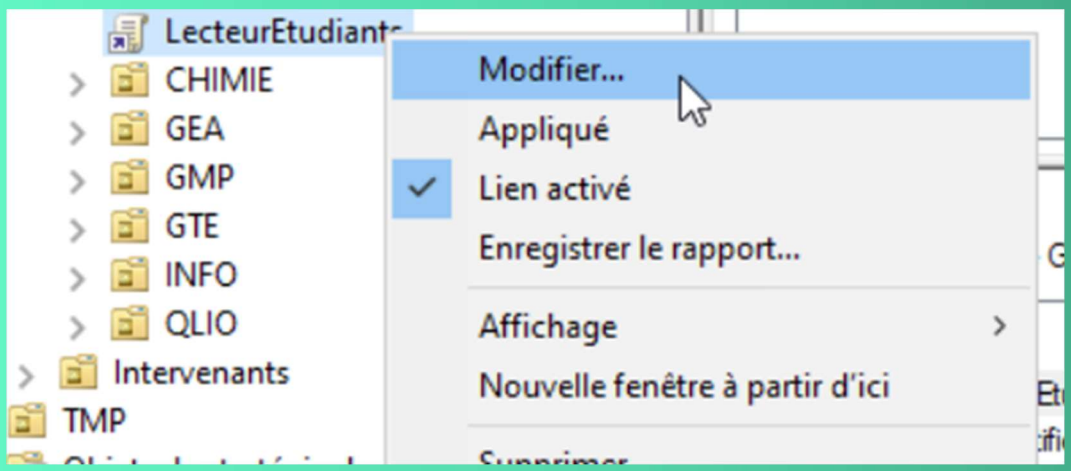
Choisir le nom de sa GPO



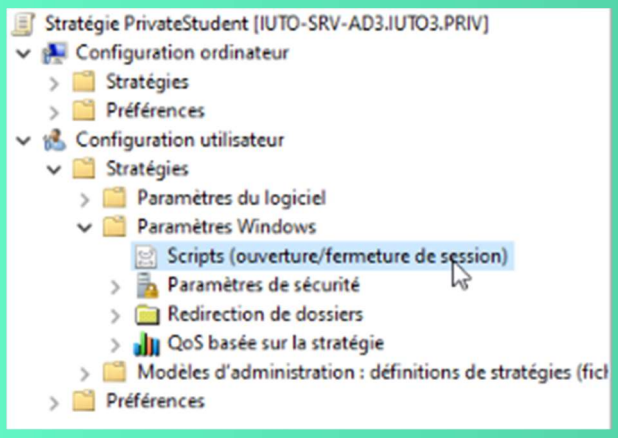
Ajouter le groupe d'utilisateurs 'Etudiants'



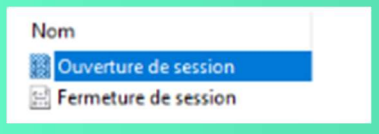
Puis faire un clic droit sur la GPO que l'on vient de créer 'Appliqué' puis 'Modifier…'



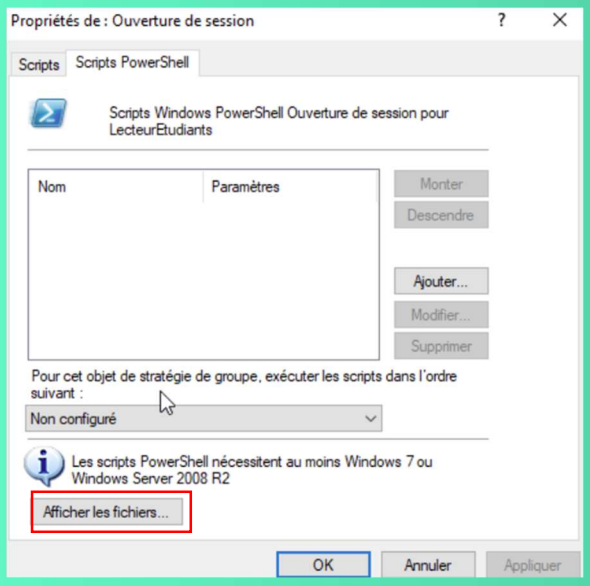
Ensuite, cliquer sur 'Configuration utilisateur' puis 'Stratégies', 'Paramètres Windows' et 'Scripts'



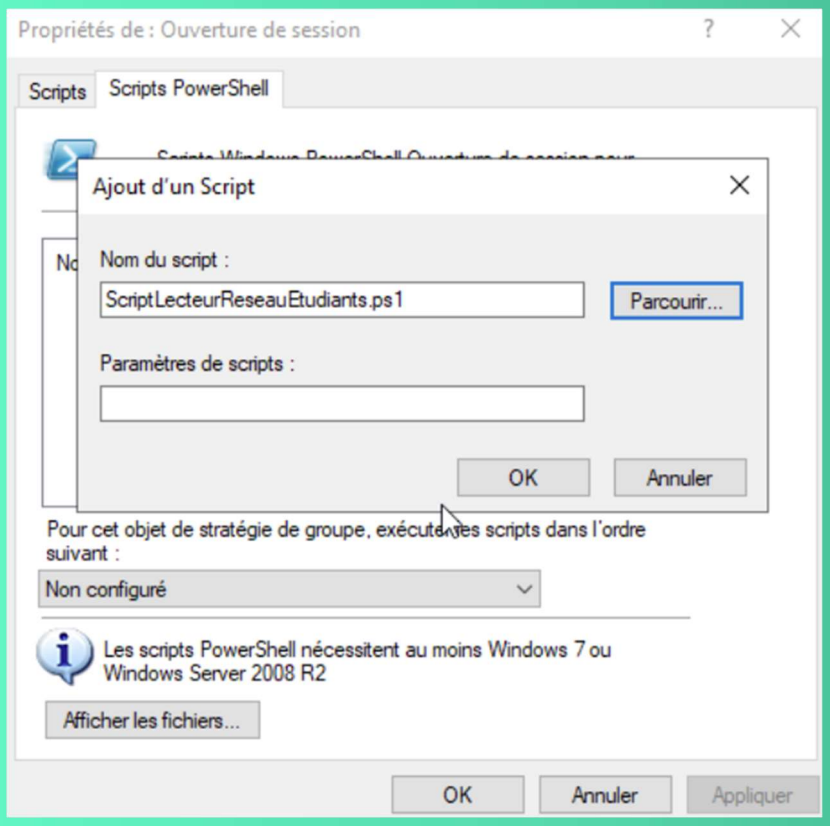
Pour ajouter le script à l'ouverture de la session, cliquer sur 'Ouverture de session'



Cliquer sur 'Afficher les fichiers…' et coller son script powershell dedans



Pour finir, cliquer sur ‘Ajouter’ puis ‘Parcourir…’ pour ajouter son script que l’on vient de coller



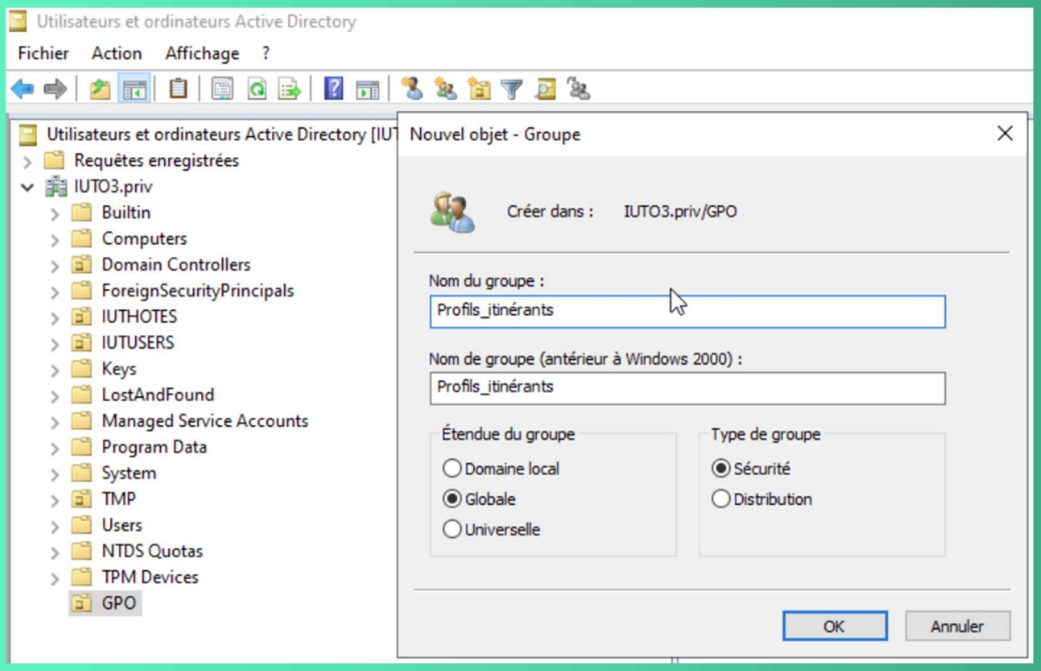
PROFILS ITINÉRANTS

Préparer le contrôleur de domaine (AD et GPO) :

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

Création d'une OU pour les GPO :

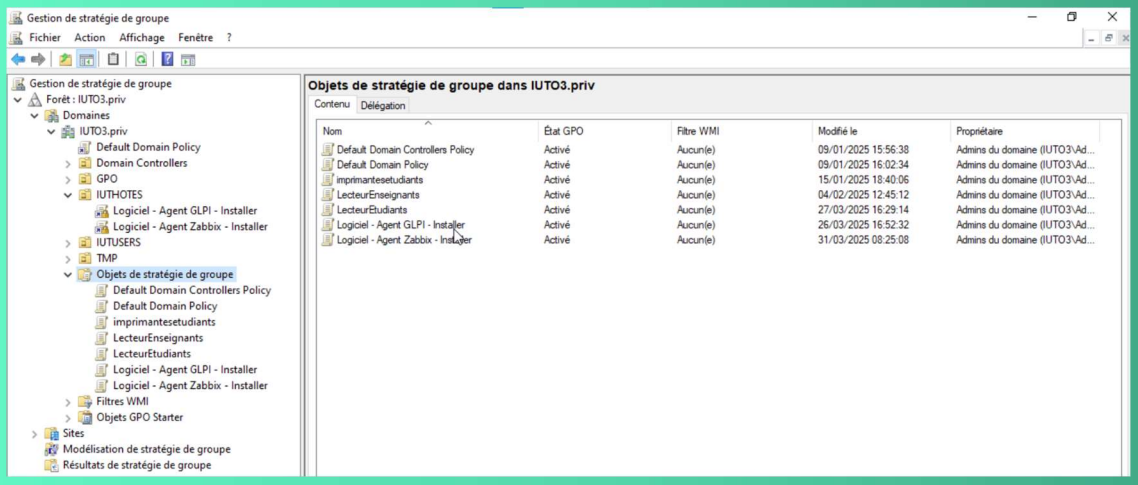
Nous avons créé une Unité d'Organisation nommée GPO puis créer un groupe global nommée 'Profils_itinérants'



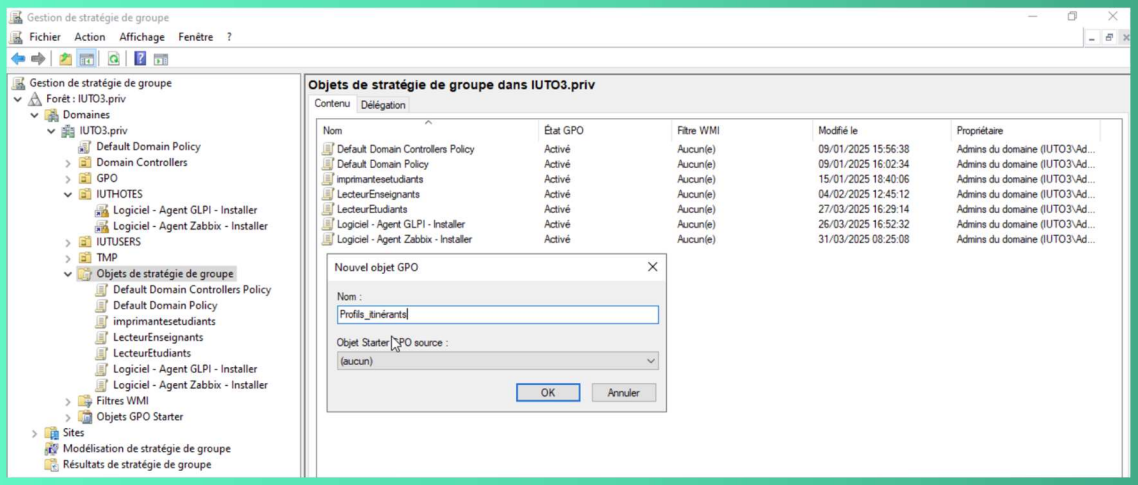
Afin d'éviter des possibles problèmes « un jour » nous allons mettre en place une GPO

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

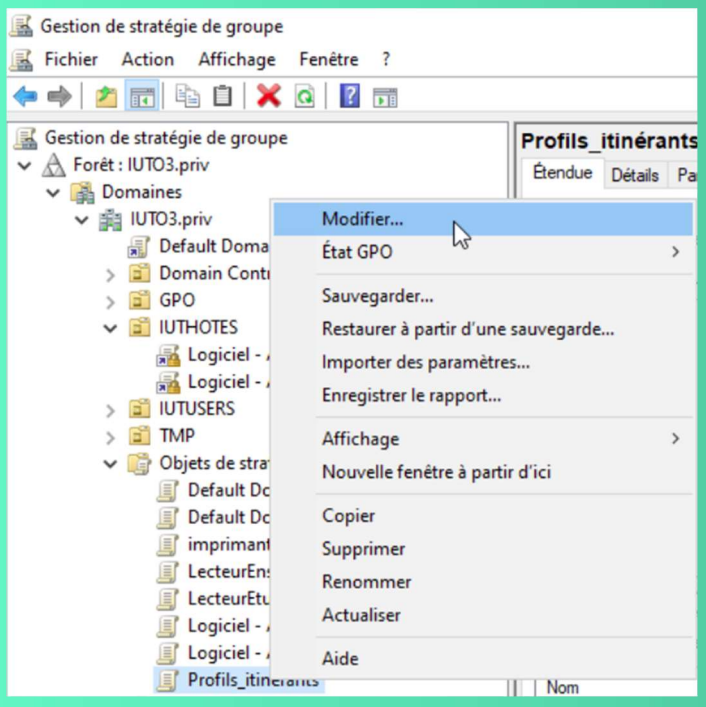
Pour cela, ouvrez votre console de gestion des stratégies de groupe.



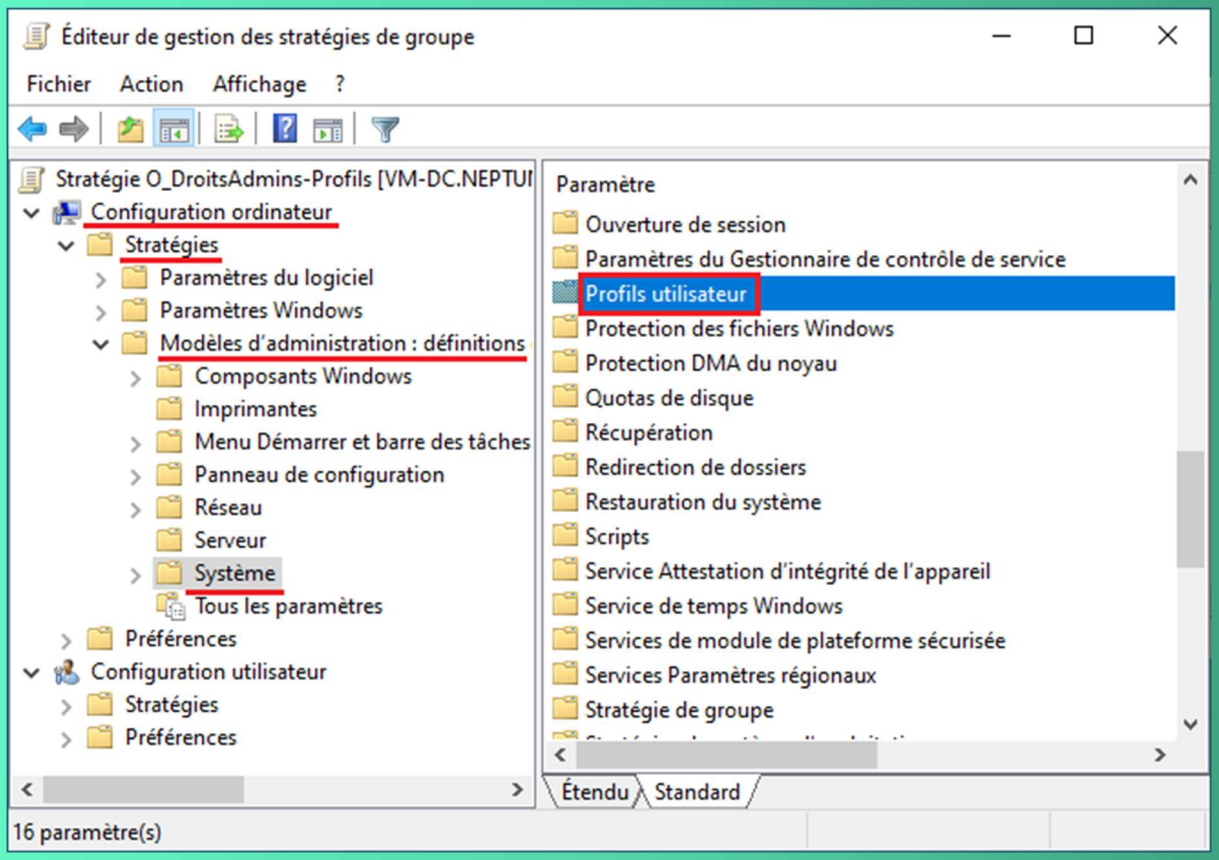
Dans la partie « Objets de stratégie de groupe », faites un clic droit puis « Nouveau ». Ensuite nommer la GPO



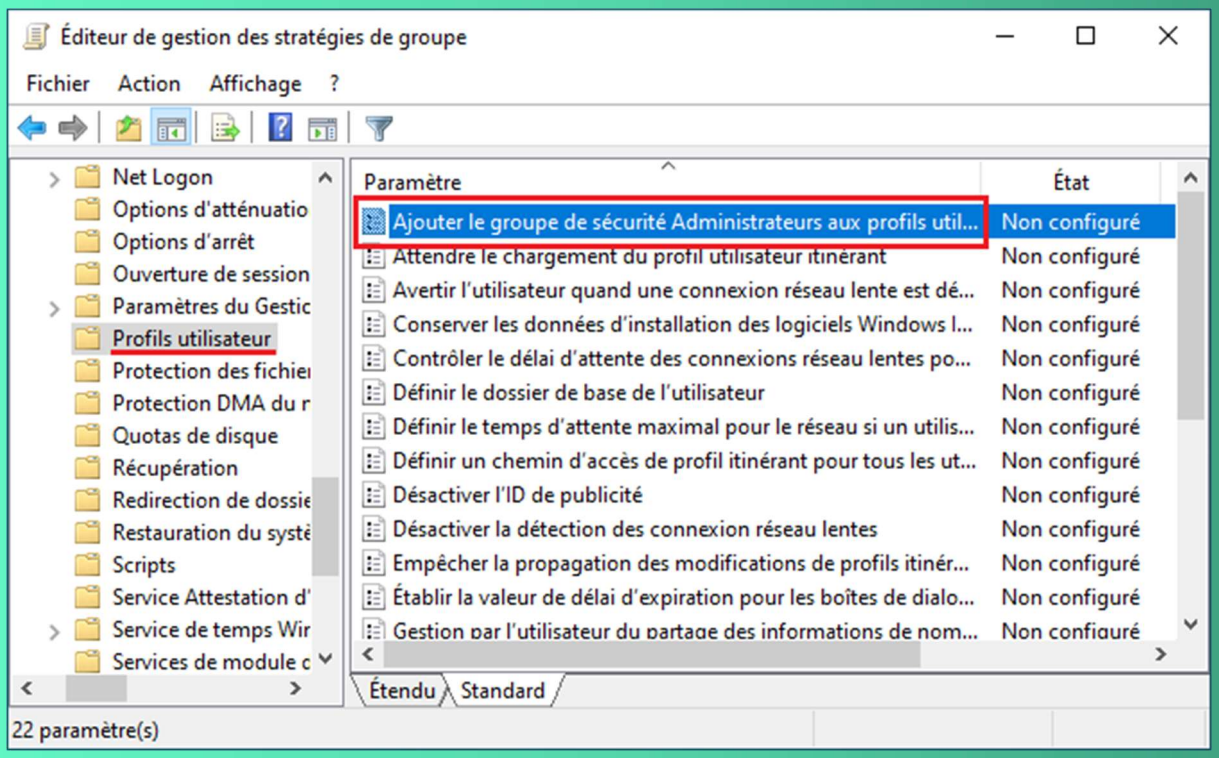
Ensuite faites un clic droit sur son nom puis « Modifier ».



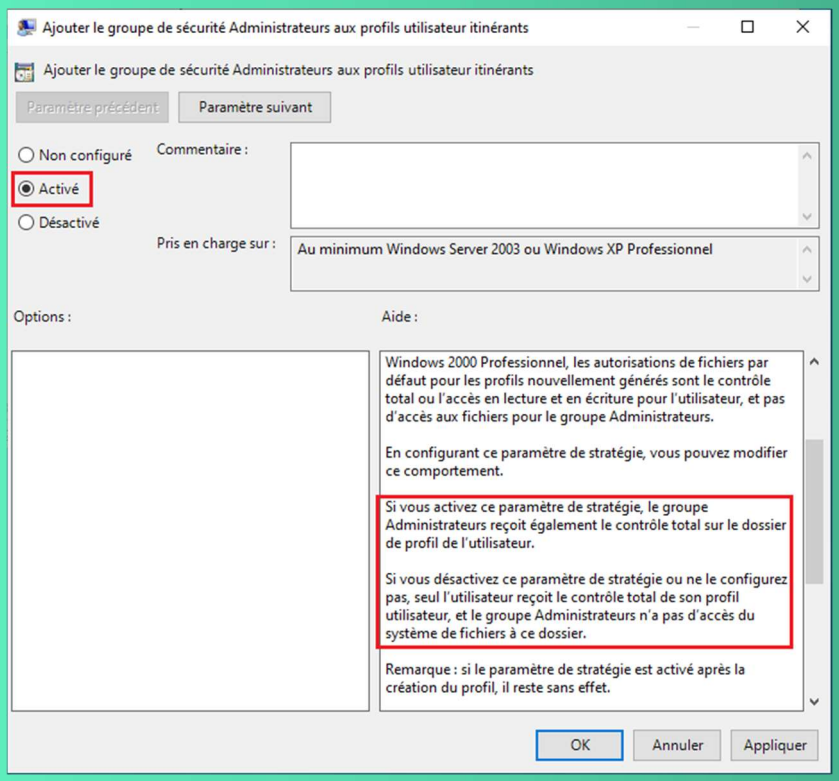
Dans l'éditeur de GPO, allez dans Configuration ordinateur > Stratégies > Modèles d'administration > Système > Profils utilisateur.



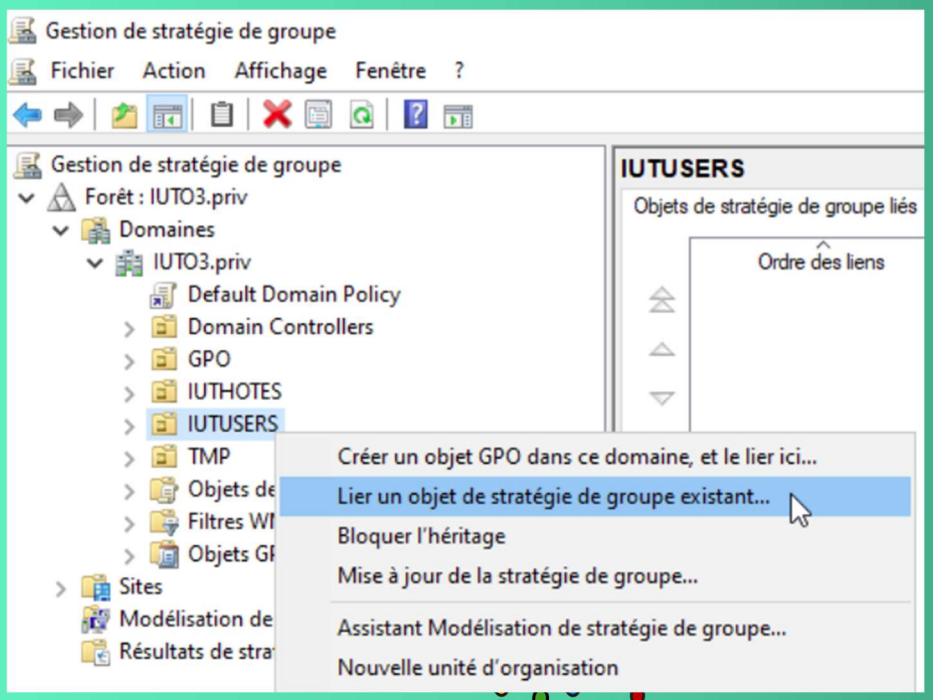
Recherchez sur la droite le paramètre nommé « Ajouter le groupe de sécurité Administrateurs aux profils utilisateur itinérants » et double-cliquez dessus.



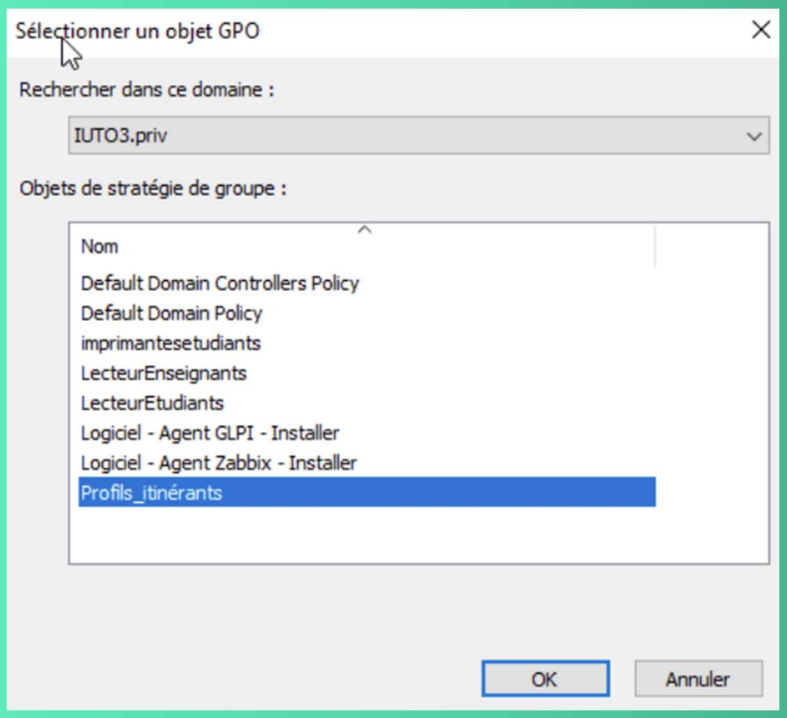
Si on regarde un peu dans la partie « Aide », il y a des infos intéressantes nous précisant ce qu'il se passe si on active ce paramètre, si au contraire on le désactive ou ne le configure pas. Nous voulons que les admins puissent accéder aux profils dont nous allons l'activer. Cochez la case « Activé » et cliquez sur OK.



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 ».



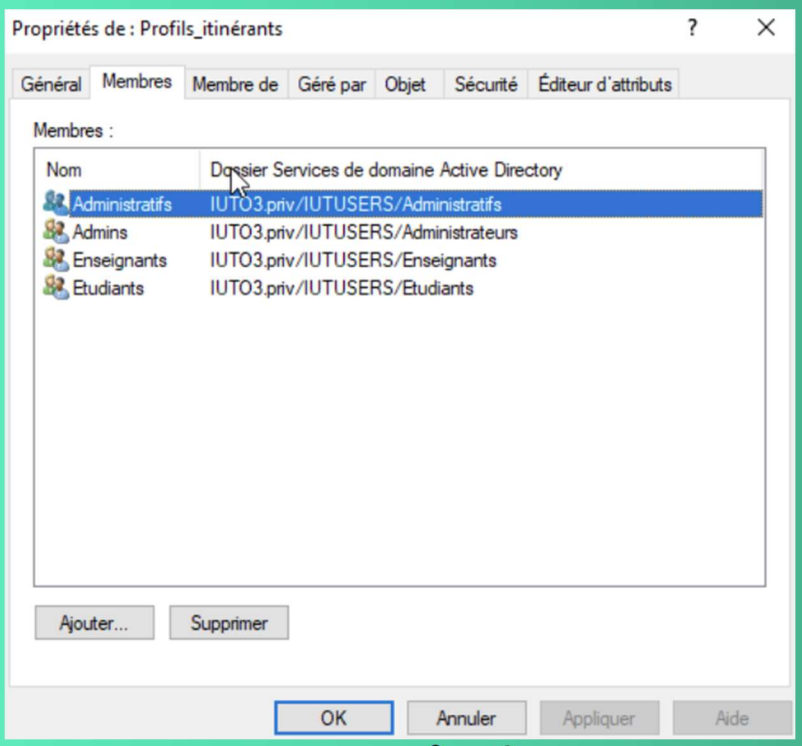
Choisissez dans la liste la GPO que vous venez de créer et cliquez sur OK.



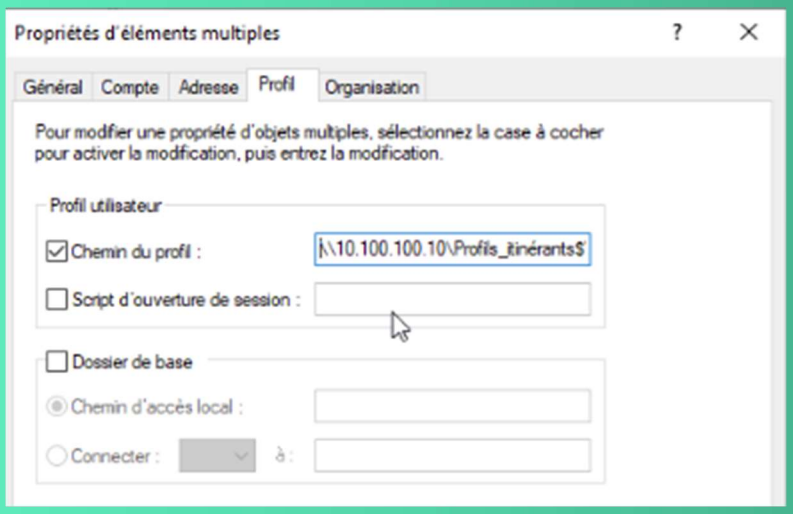
C'est tout ce qu'il y a à faire côté serveur AD pour le moment, passons à l'étape suivante.

Définir un profil itinérant pour un utilisateur AD :

Retournons dans notre AD, faire un clic droit sur les utilisateurs que vous souhaitez ajouter dans notre groupe puis faire un clic droit et 'ajouter à un groupe'



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



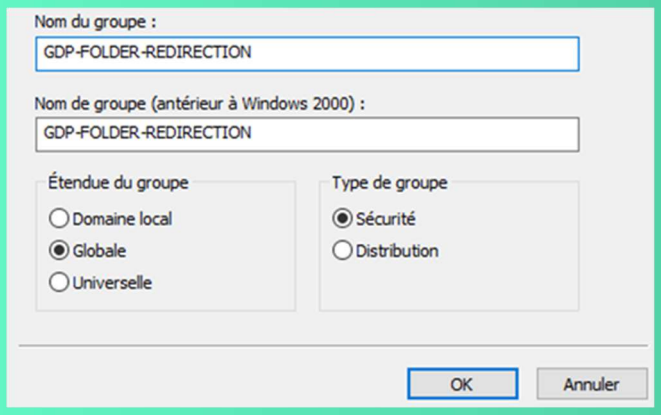
Il faut renseigner ici le chemin réseau du partage contenant les profils, suivi du nom du dossier de profil qui sera créé pour l'utilisateur lui-même et qui devra donc être unique. Pour éviter les problèmes, je vous conseille de nommer le dossier de profil comme le login de l'utilisateur (un login dans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

\\10.100.100.10\Profils_itinerants$\%username%

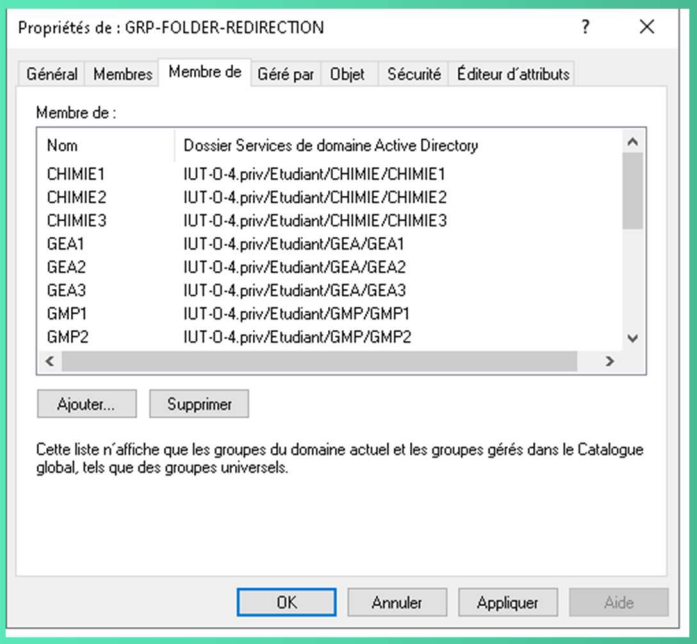
Cliquez sur Appliquer pour valider l'attribution d'un chemin de profil. La variable prendra automatiquement le login de l'utilisateur en cours de modification. Cliquez sur OK quand vous avez terminé. Il ne nous reste plus qu'à connecter l'utilisateur sur son PC pour voir ce que ça donne.

Redirection des dossiers :

Création du groupe :

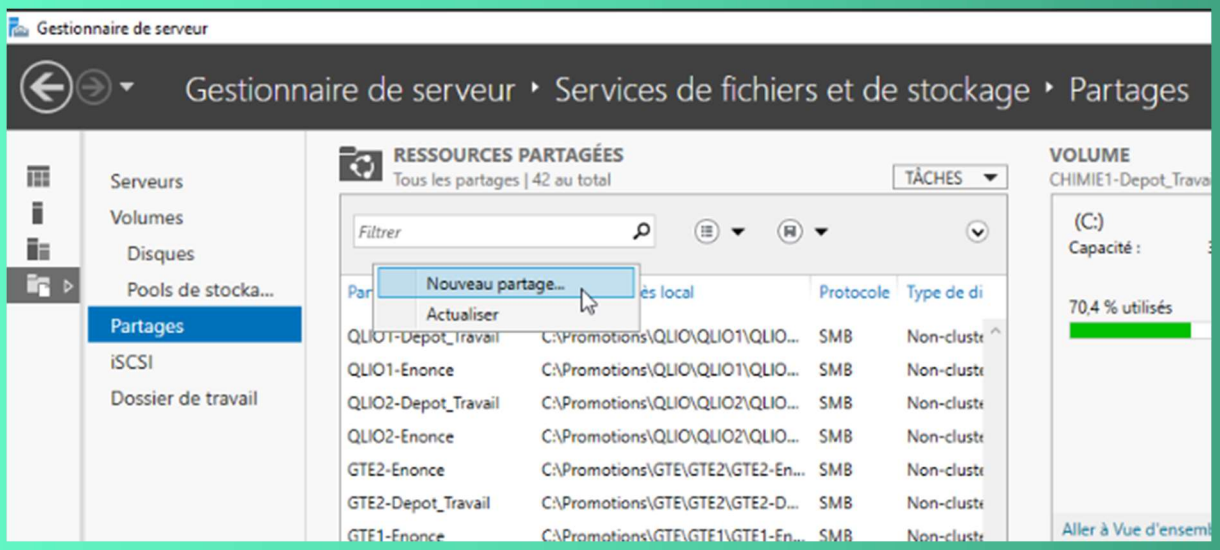


Ajout des groupes de chaque section classe dans le groupe de redirection de dossier :



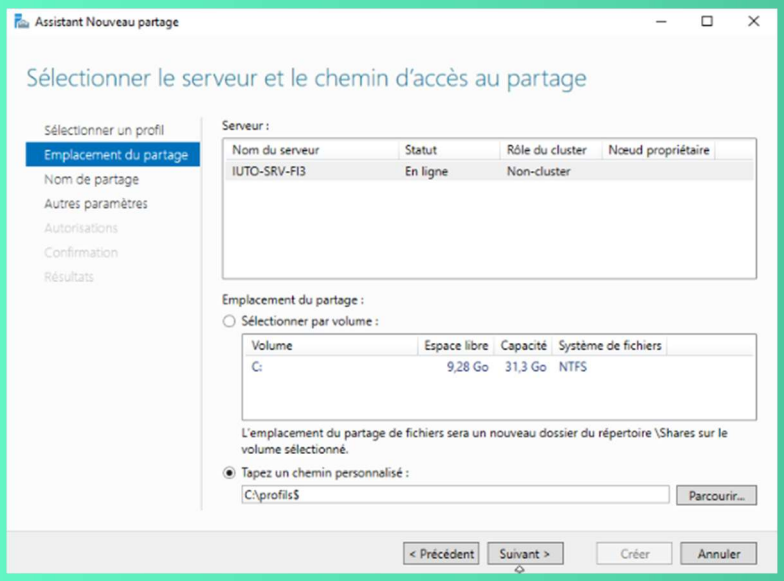
Le partage et attribution des droits :

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

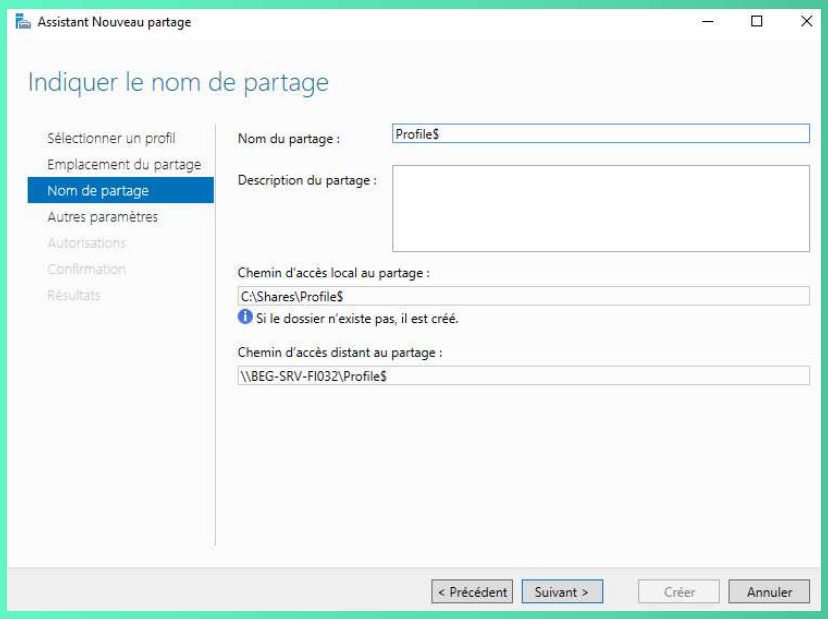


Pour faire de l'hébergement de fichiers comme nous le souhaitons, sélectionnez "Partage SMB - Rapide".

Sélectionner l’emplacement du partage



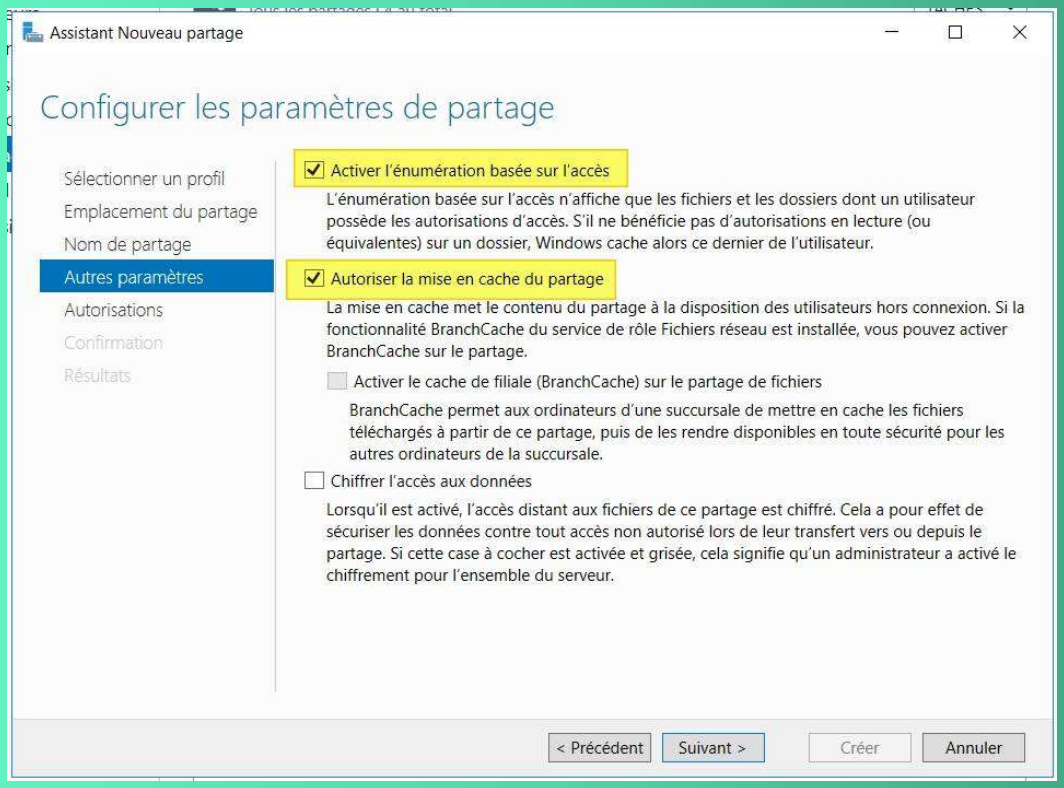
Donnez un nom à votre partage, par exemple : PrProfilsofiles$. Ce partage étant sensible et qu'il n'y a pas lieu d'y accéder en direct, notamment via la découverte réseau, je vous recommande de mettre un "$" à la fin du nom pour qu'il soit masqué un minimum.



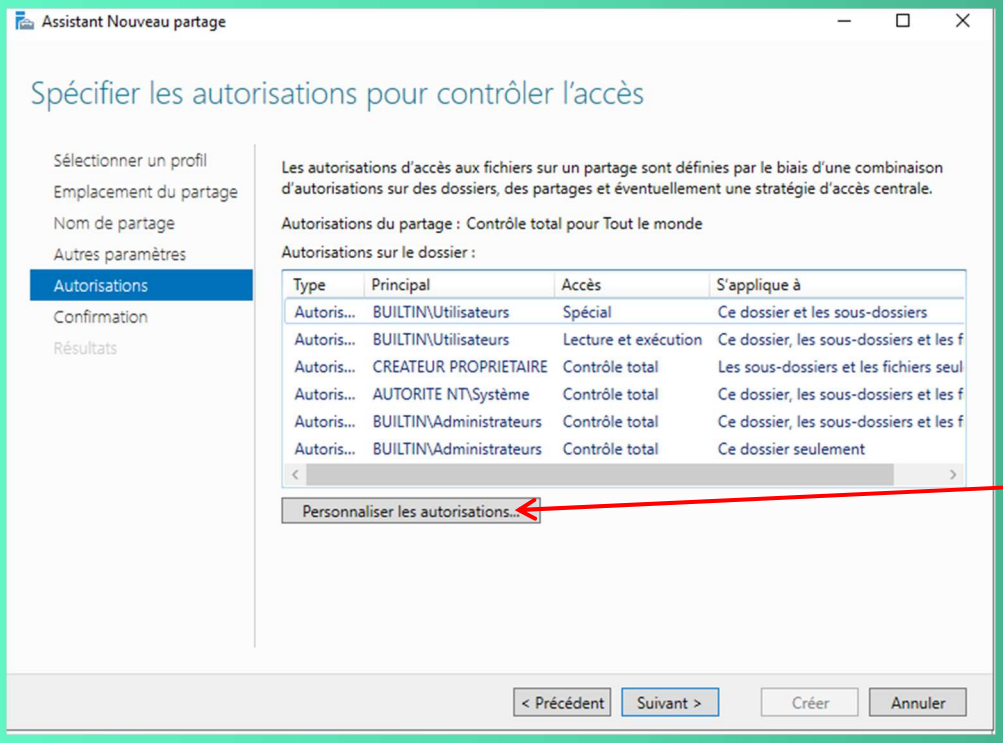
Deux options sont à activer sur cette page :

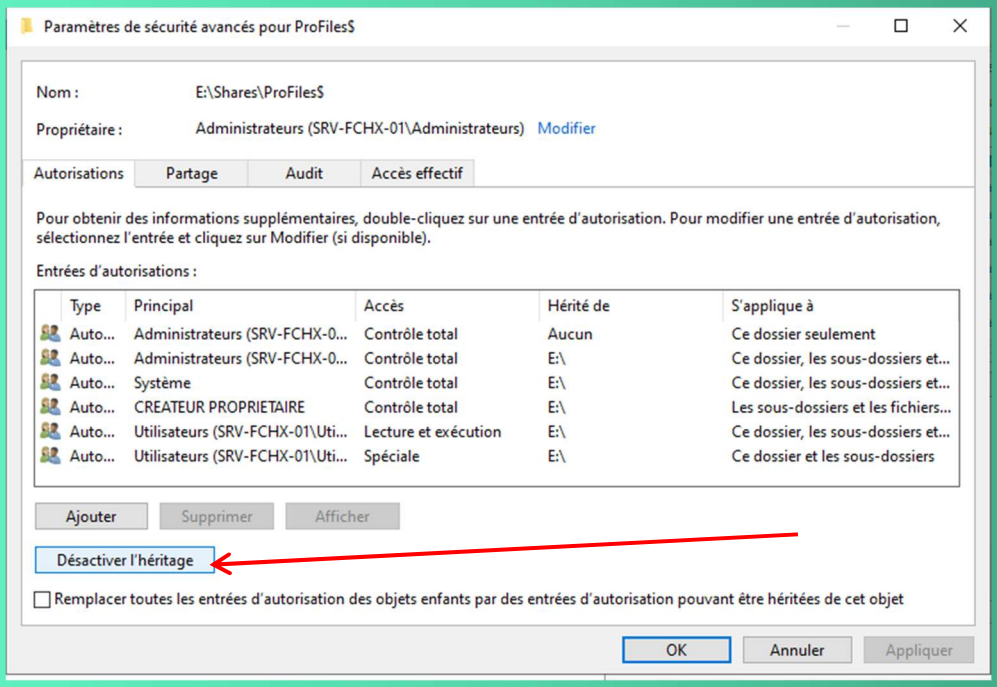
Activer l'énumération basée sur l'accès : l'utilisateur ayant les droits que sur son dossier "perso" alors il verra uniquement son dossier s'il parcoure le partage - l'affichage dans l'explorateur se base sur les droits de l'utilisateur.

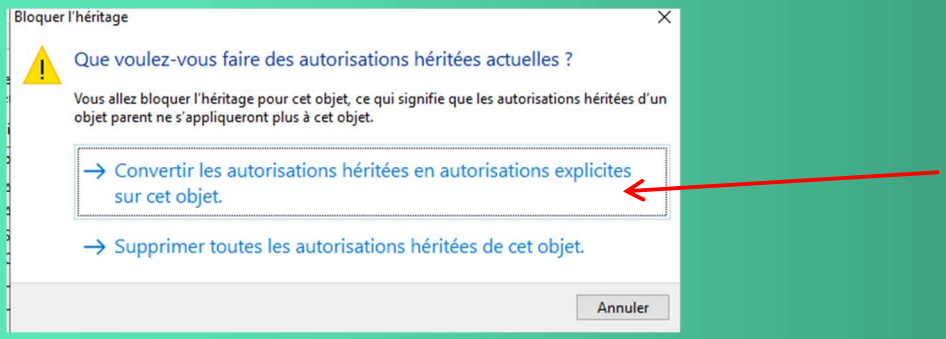
Autoriser la mise en cache du partage : cette option permettra à l'utilisateur d'utiliser la synchronisation des fichiers hors connexion sur ce partage pour que ses données soient synchronisées sur son poste. Sans cela, ce sera refusé par le serveur.



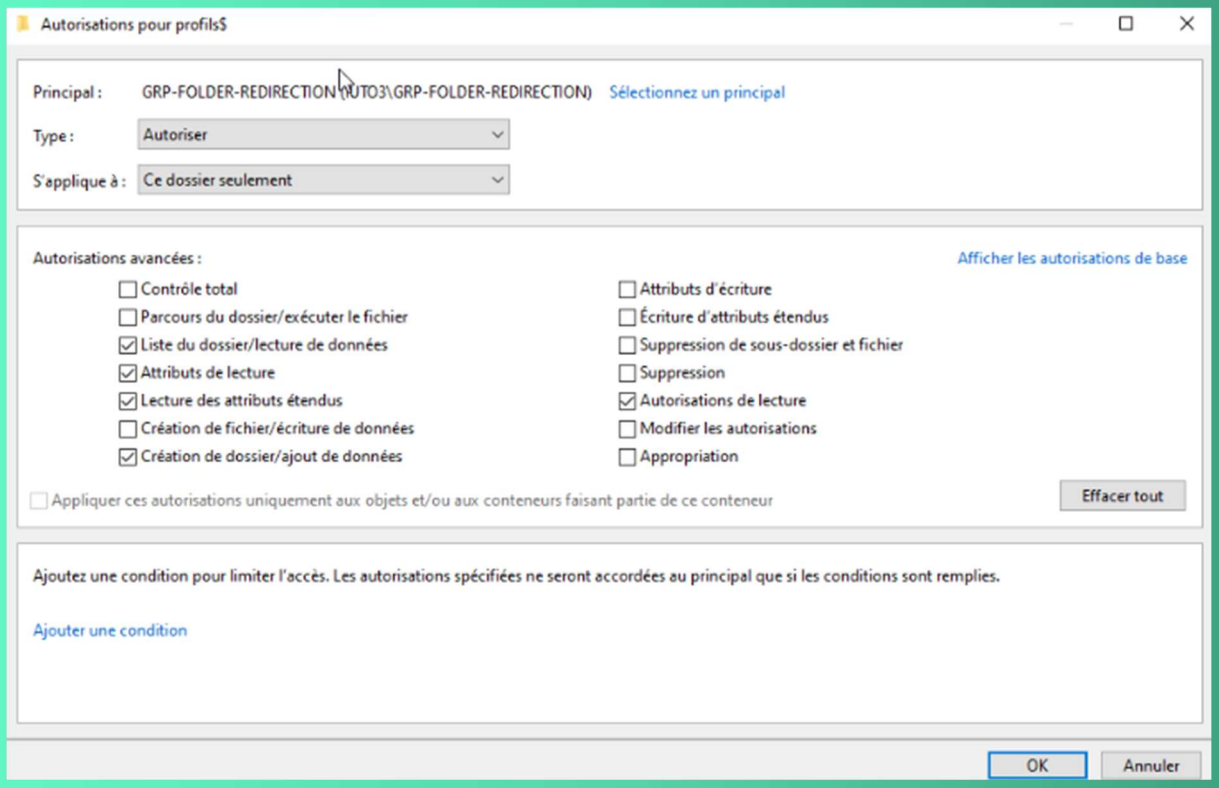
Il faut maintenant passer à l'étape la plus délicate : les autorisations NTFS. Nous allons donner les bons droits sur le partage afin que, lorsqu'un utilisateur se connecte, un dossier de profil puisse être généré (le nom sera son identifiant AD) et qu'il puisse écrire dans ce dossier. Il aura les droits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



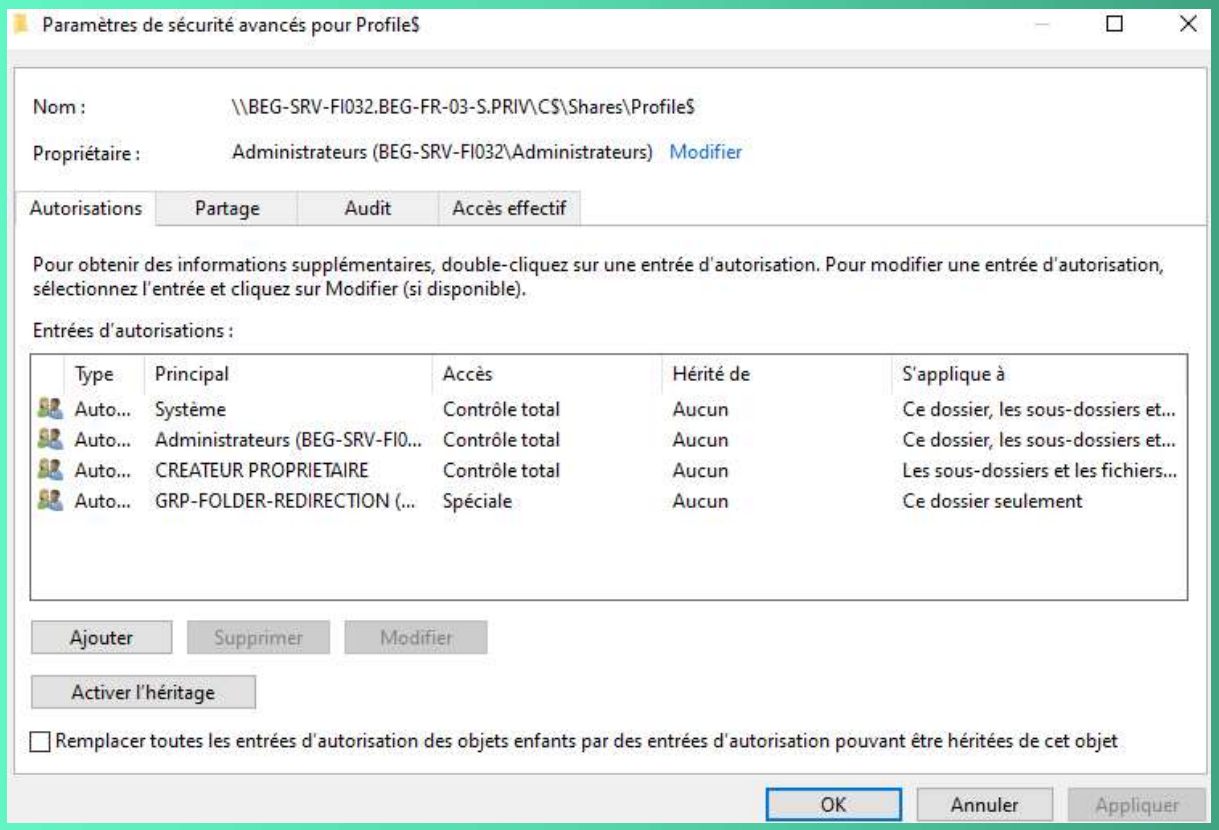

Paramètres de sécurité avancés pour ProFiles$
Nom : E:\Shares\ProFiles$
Propriétaire : Administrateurs (SRV-FCHX-01\Administrateurs) Modifier
Autorisations Partage Audit Accès effectif
Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'autorisation. Pour modifier une entrée d'autorisation, sélectionnez l'entrée et cliquez sur Modifier (si disponible).
Entrées d'autorisations :
Type Principal Accès Hérité de S'applique à
Auto... Administrateurs (SRV-FCHX-0... Contrôle total Aucun Ce dossier seulement
Auto... Administrateurs (SRV-FCHX-0... Contrôle total E:\ Ce dossier, les sous-dossiers et...
Auto... Système Contrôle total E:\ Ce dossier, les sous-dossiers et...
Auto... CREATEUR PROPRIETAIRE Contrôle total E:\ Les sous-dossiers et les fichiers...
Auto... Utilisateurs (SRV-FCHX-01\Uti... Lecture et exécution E:\ Ce dossier, les sous-dossiers et...
Auto... Utilisateurs (SRV-FCHX-01\Uti... Spéciale E:\ Ce dossier et les sous-dossiers
Ajouter Supprimer Afficher
Désactiver 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


Bloquer l'héritage
Que voulez-vous faire des autorisations héritées actuelles ?
Vous allez bloquer l'héritage pour cet objet, ce qui signifie que les autorisations héritées d'un objet parent ne s'appliqueront plus à cet objet.
Convertir les autorisations héritées en autorisations explicites sur cet objet.
Supprimer toutes les autorisations héritées de cet objet.
Annuler

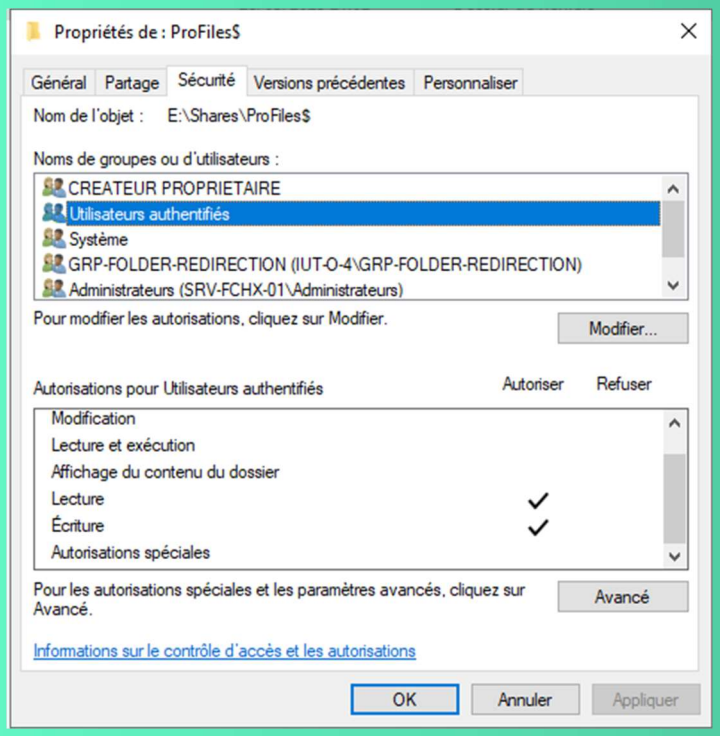
Maintenant, ajoutez des autorisations pour le groupe "GRP-FOLDER-REDIRECTION" et configurez comme ceci :



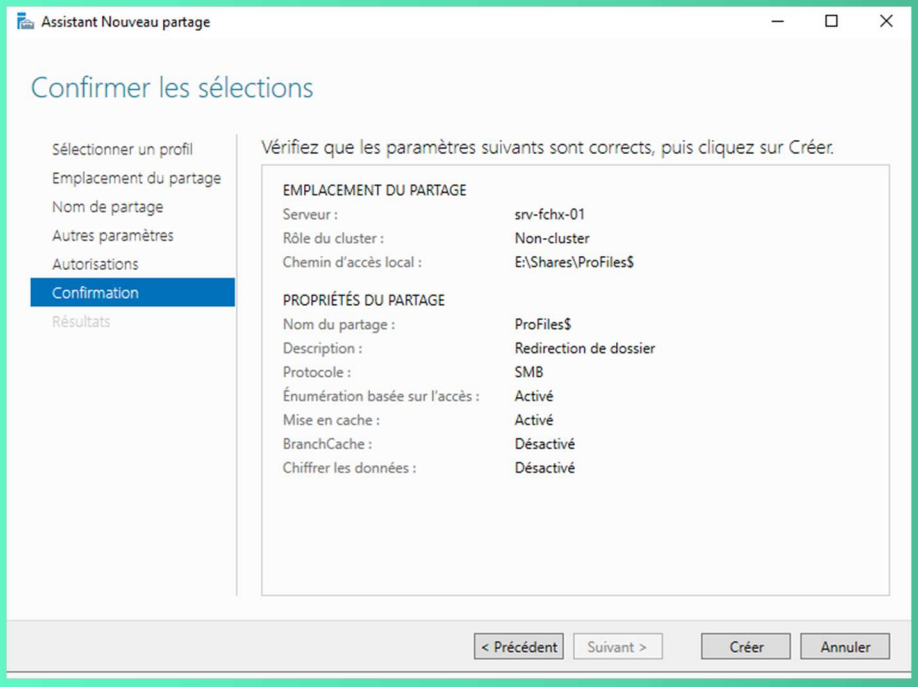
Au final, vous devez avoir les droits identiques à ceux ci-dessous (attention au champ "S'applique à") :



Par la suite j'aurais ajouté les utilisateurs authentifier en Lecture \ Ecriture :

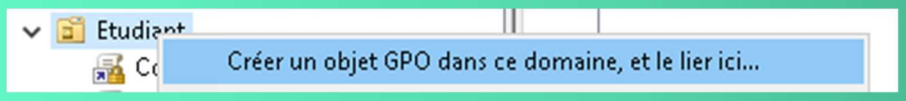


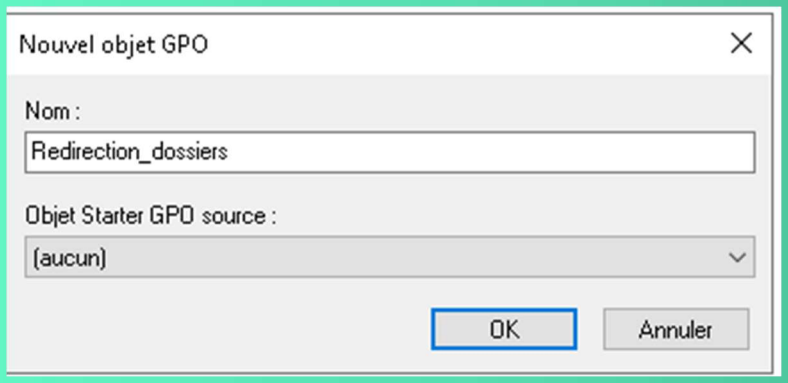
On confirme les paramètres du partage :



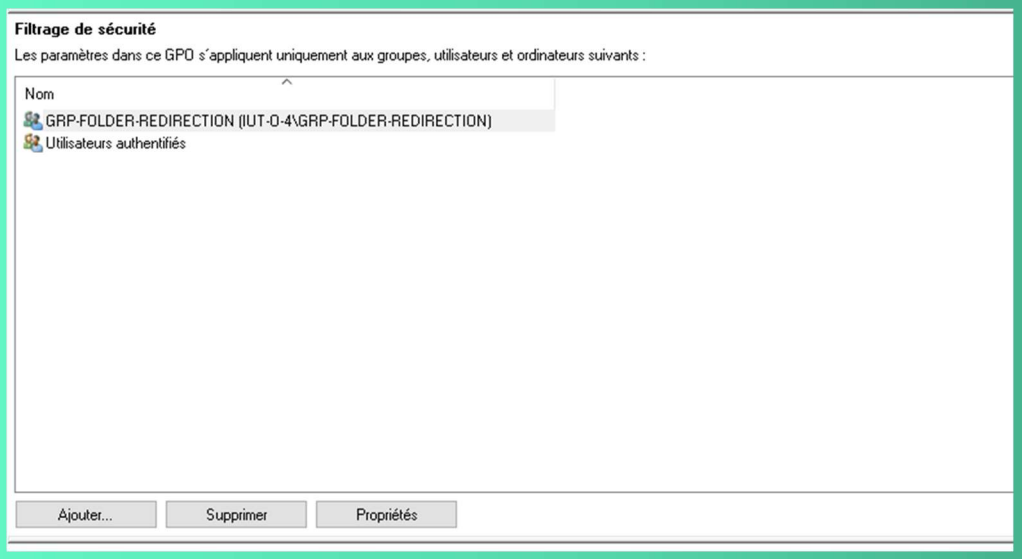
La GPO de redirection de dossiers :

Crée la GPO a l'endroit voulu :

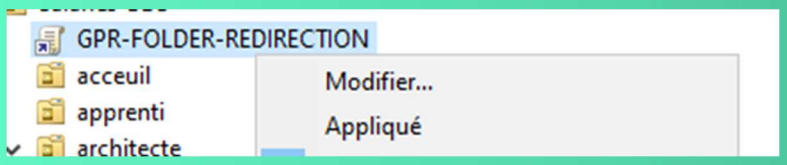




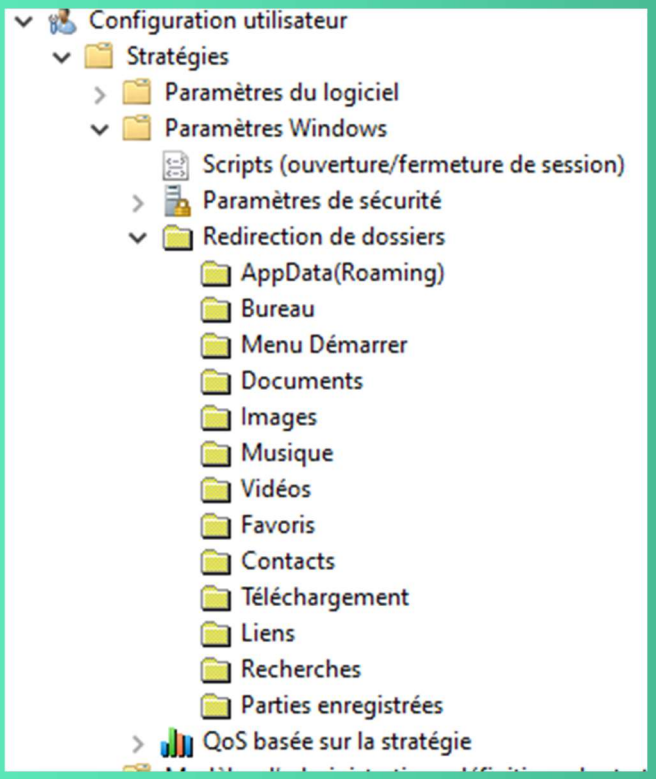
Ajout du GRP-FOLDER dans les sécurités de la GPO :



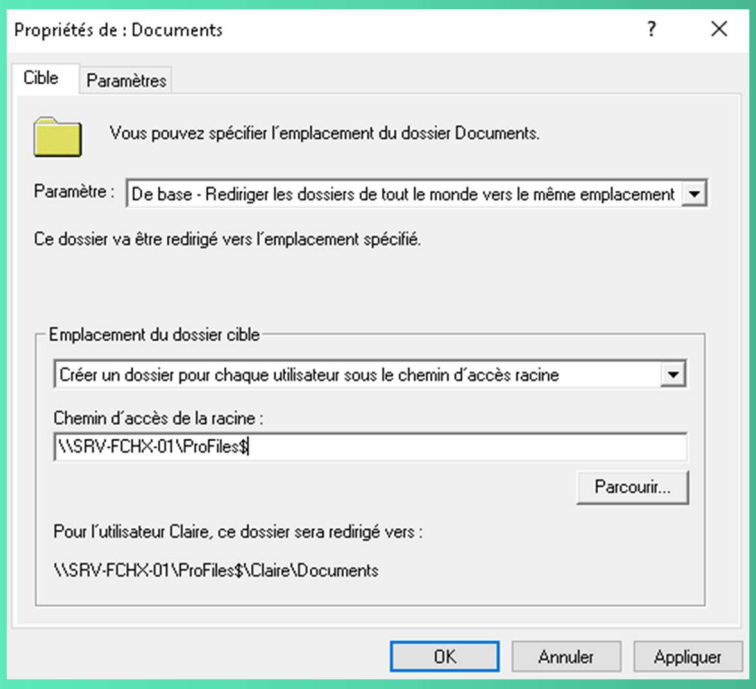
Faire un clic droit Modifier :



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 (faite un clic droit sur GPO)



Par exemple pour document, faite un clic droit sur « Document » et bien mettre c'est paramètre avec le lien de partage

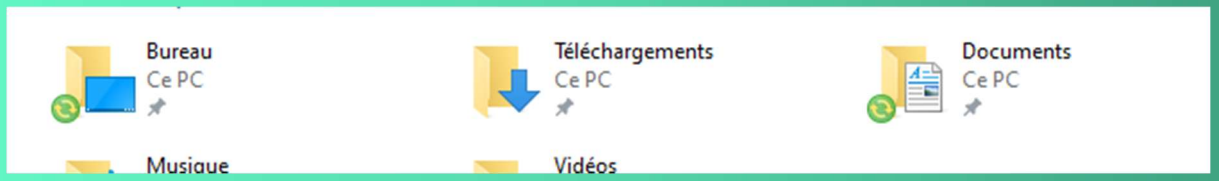


Sur l'AD faire :

```
U:\>gpupdate /force
Mise à jour de la stratégie...
```

Test de redirection de dossiers :

Résultat si jamais ça ne fonctionne pas redémarrer le PC



Si il y a un erreur de synchronisation lancer REGEDIT en admin dans :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CSC

Clic droit dans le volet de droite > **Nouveau > Valeur DWORD 32 bits**

Nomme-la : FormatDatabase

Double-clique dessus :

- **Base** : choisis **Décimale**
- **Données de la valeur** : mets 1

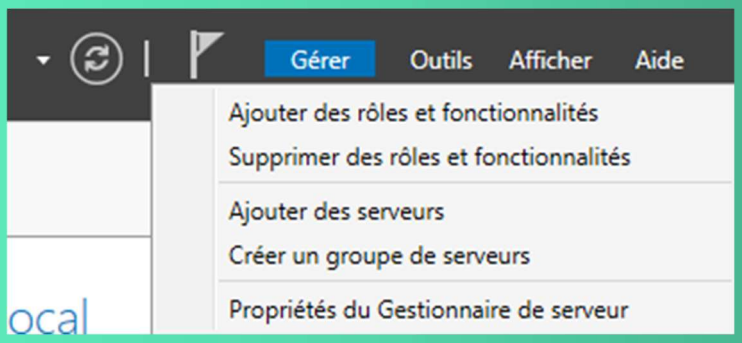
Clique sur OK

Redémarre le PC

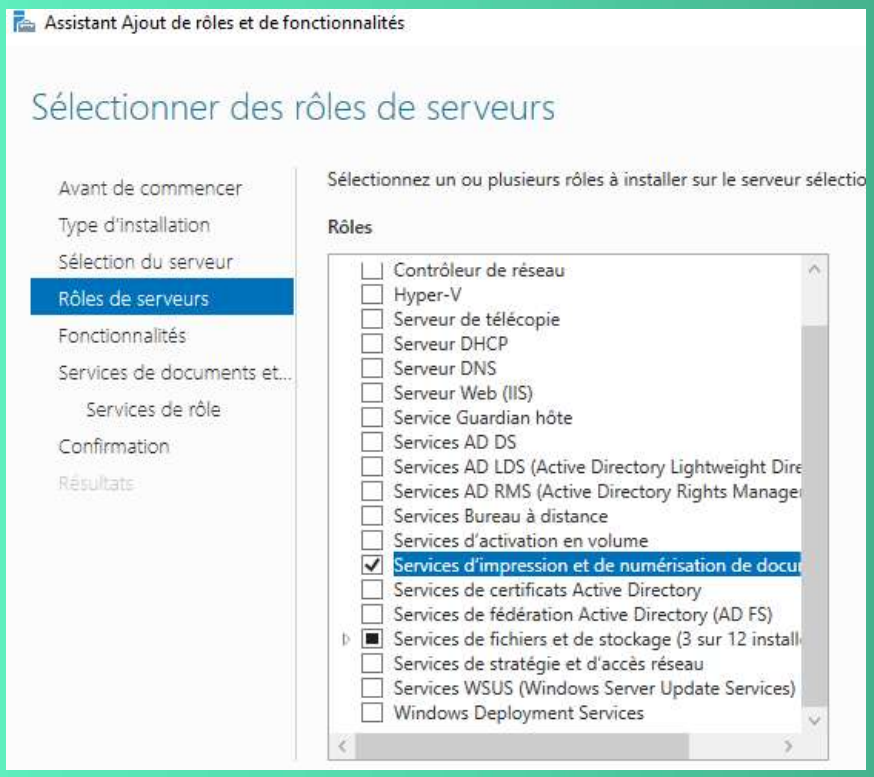
CONFIGURATION DU SERVEUR D'IMPRESSION

INSTALLATION DU SERVICE :

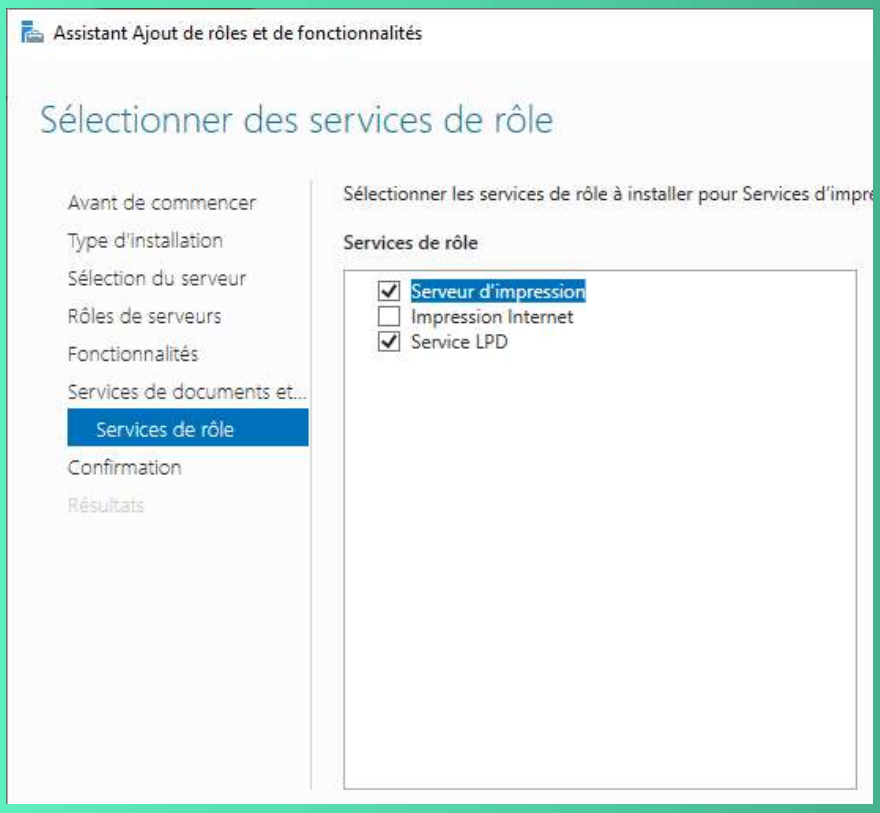
Les ressources de votre serveur d'impression seront à définir en fonction du nombre d'utilisateurs et du nombre d'imprimantes à gérer. Pour commencer l'installation, connectez-vous à votre serveur Accédez au gestionnaire de serveur, cliquez sur 'Gérer' puis sur 'Ajouter des rôles et fonctionnalités'.



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

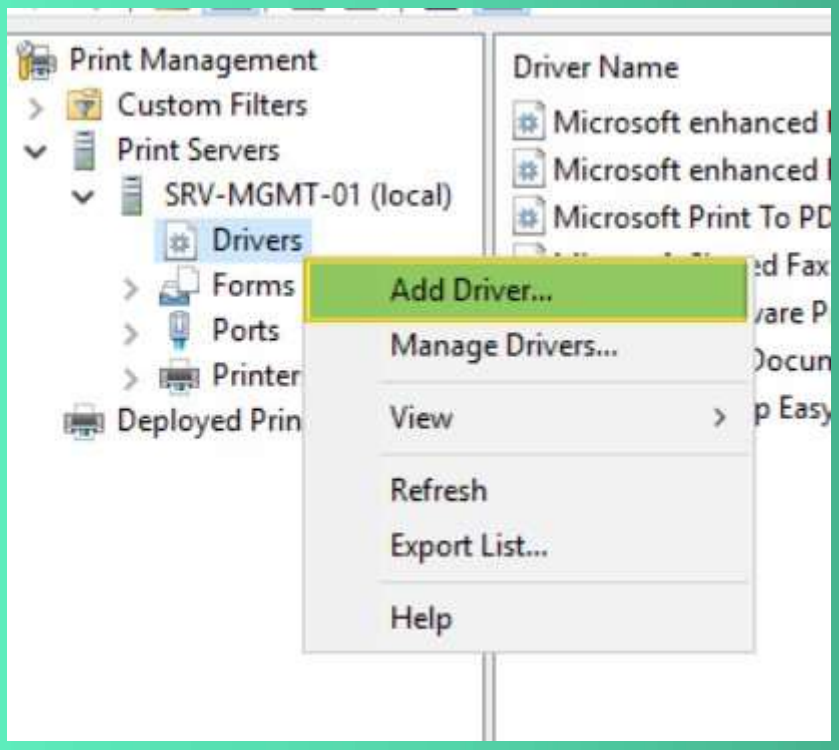


Au niveau des rôles du service d'impression, cochez à minima "Server d'Impression" qui est le serveur d'impression de base. Si vous envisagez de réaliser des impressions depuis des périphériques Unix ou Android, cochez également "LPD Service" afin d'installer ce service complémentaire qui sera utile dans ce cas. Poursuivez jusqu'au lancement de l'installation...

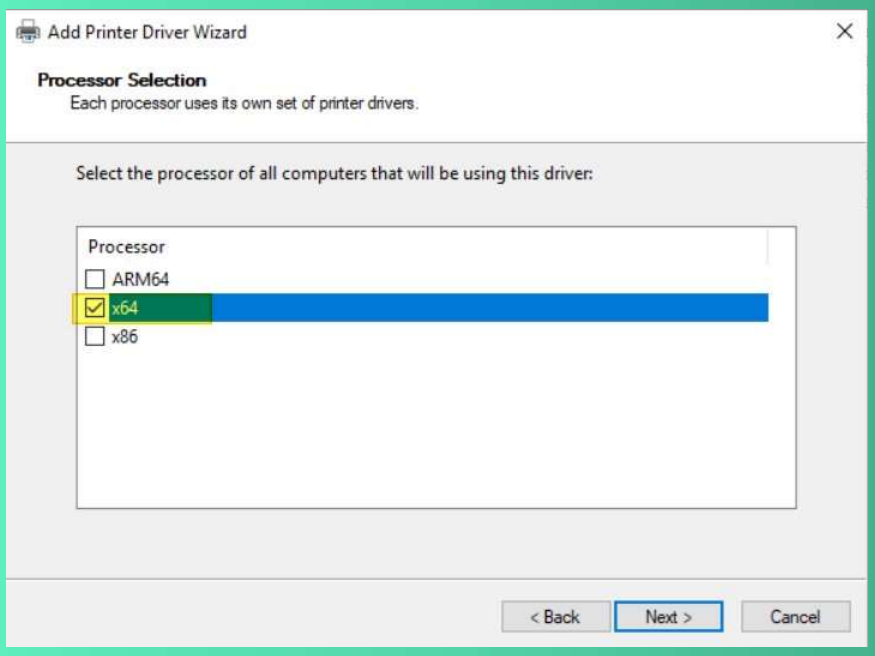


Ajouter un pilote d'impression :

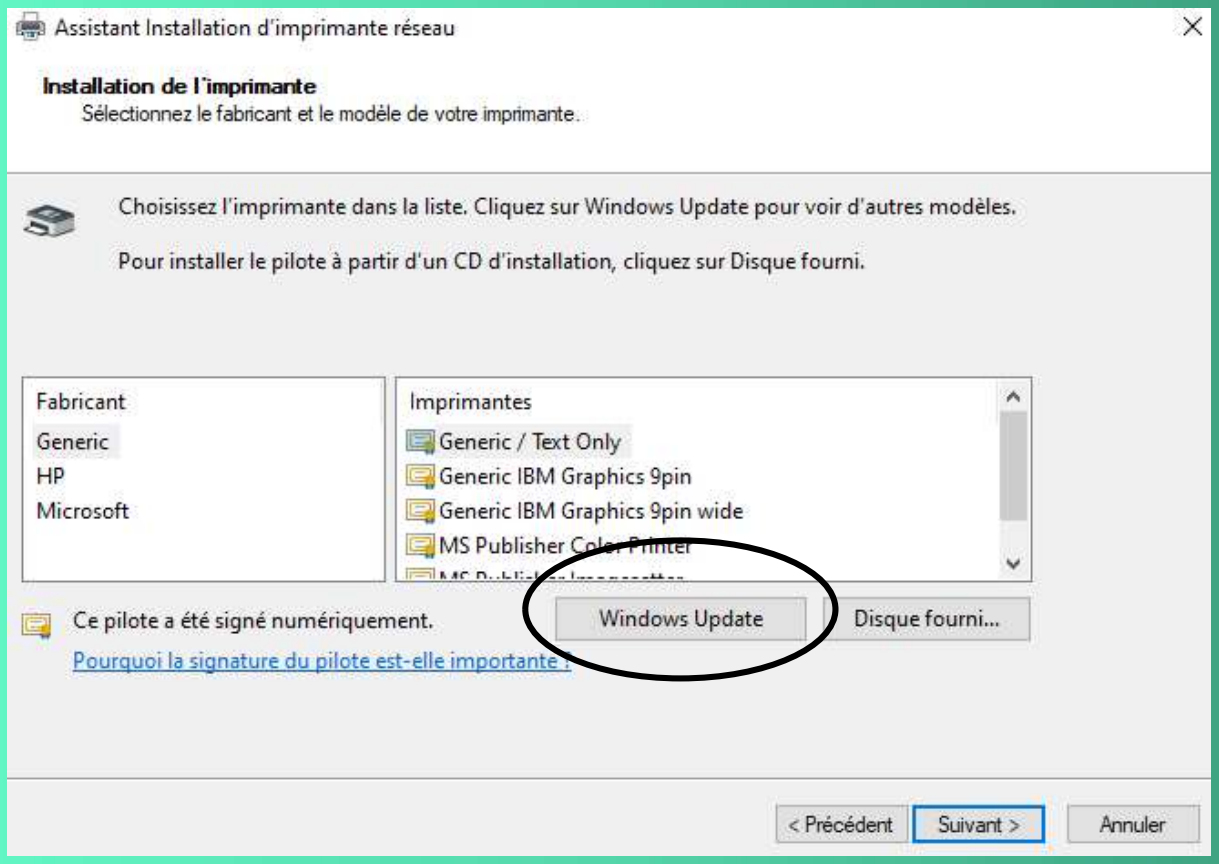
Pour commencer, nous allons donc importer notre pilote sur le serveur d'impression. Ce qui s'effectue de cette manière : Serveurs d'impression > nom de votre serveur > clic droit sur "Pilotes" et "Ajouter un pilote".



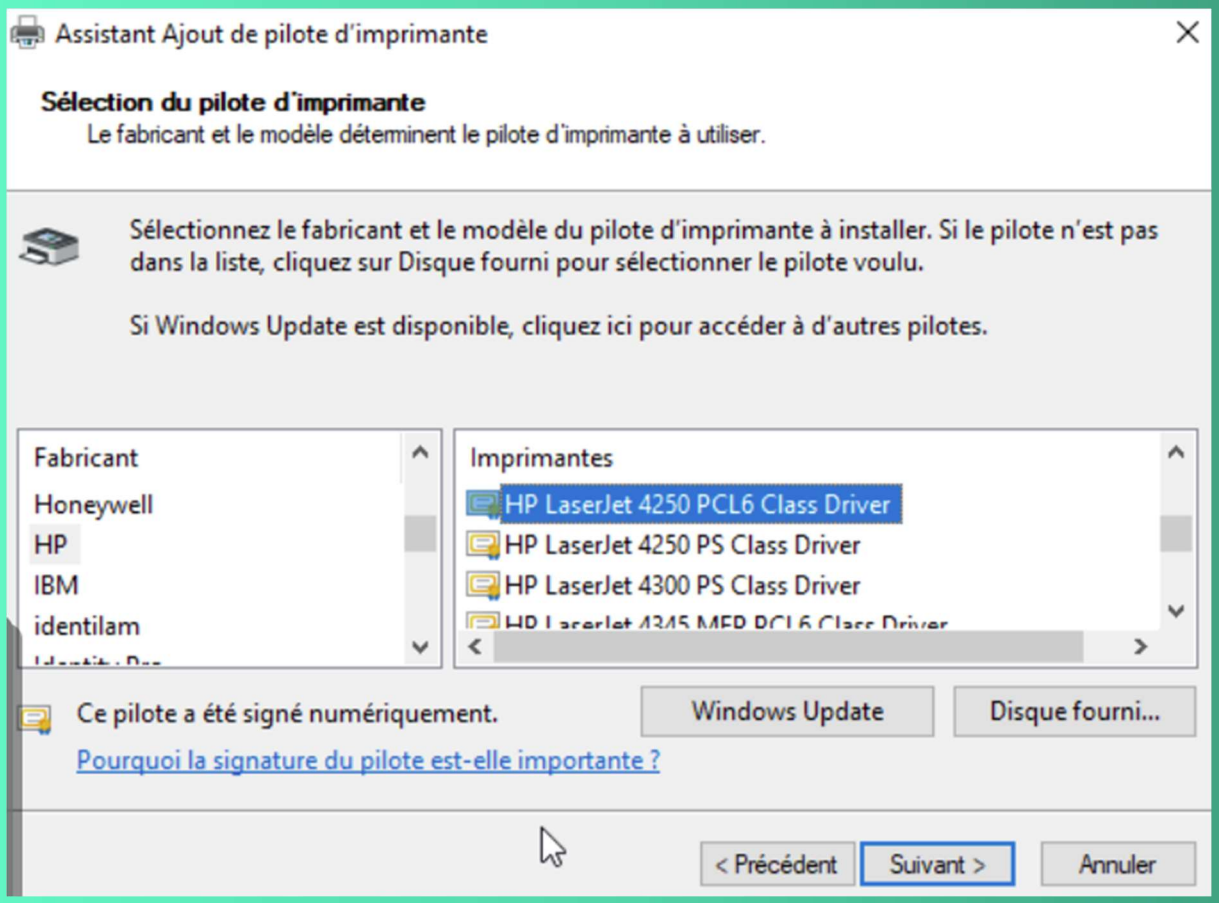
Sélectionnez les architectures processeurs compatibles avec le pilote que vous souhaitez importer.



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

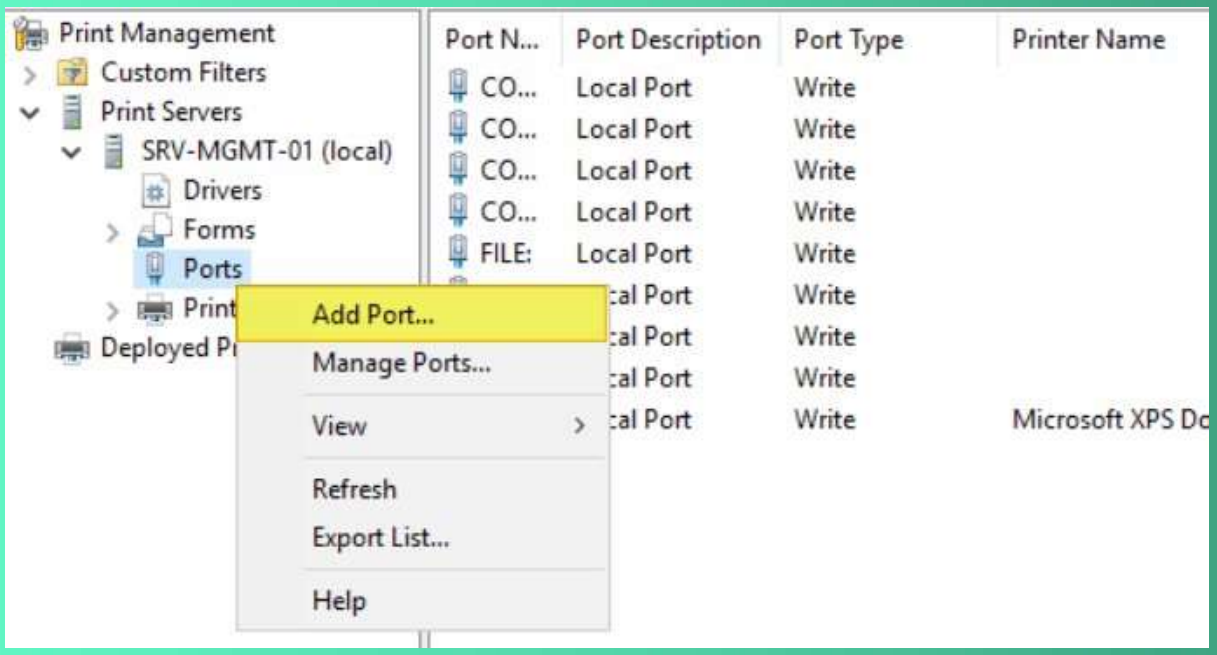


Ensuite, choisir le bon pilote, avec la marque et ensuite le modèle

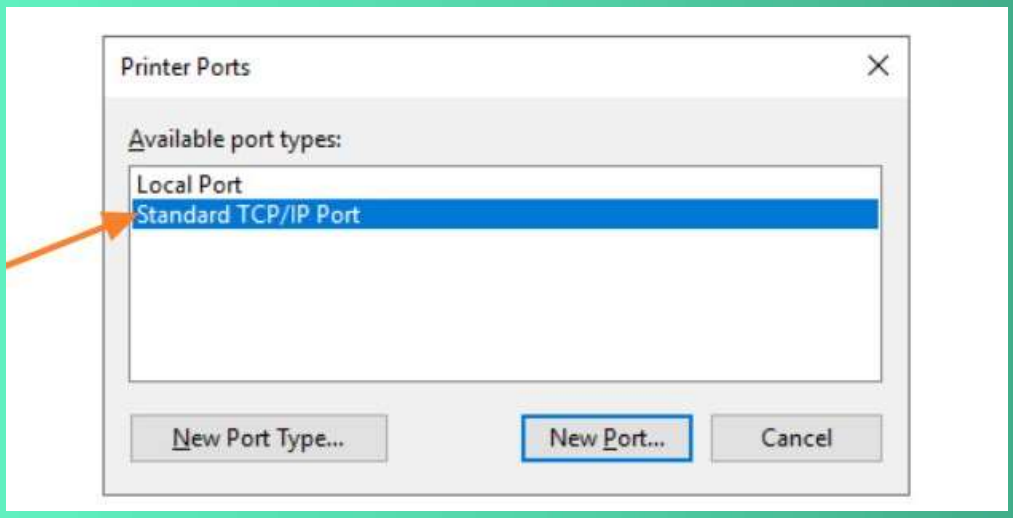


Créer un port TCP/IP :

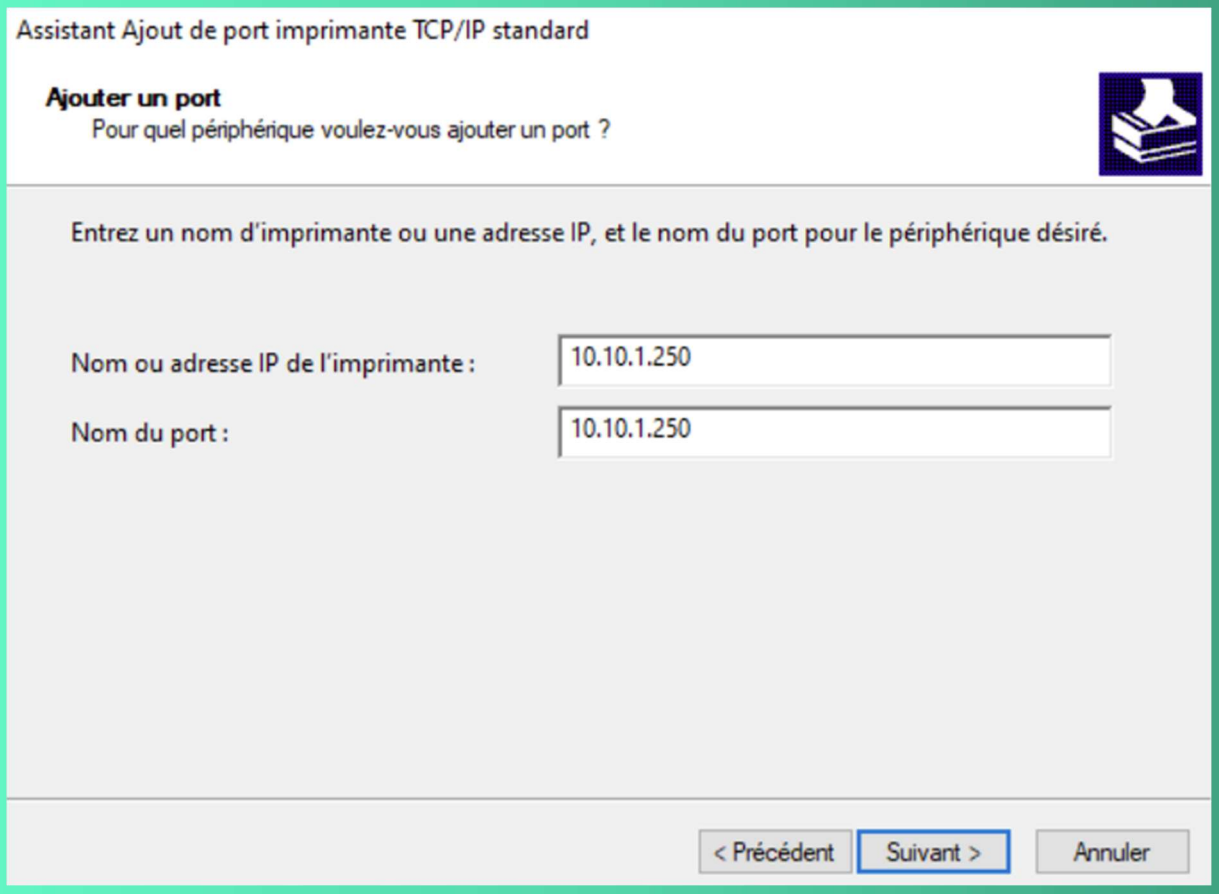
Sur le même principe que pour ajouter un pilote, la création d'un port s'effectue via un clic droit sur "Ports" puis "Ajouter un Port".



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

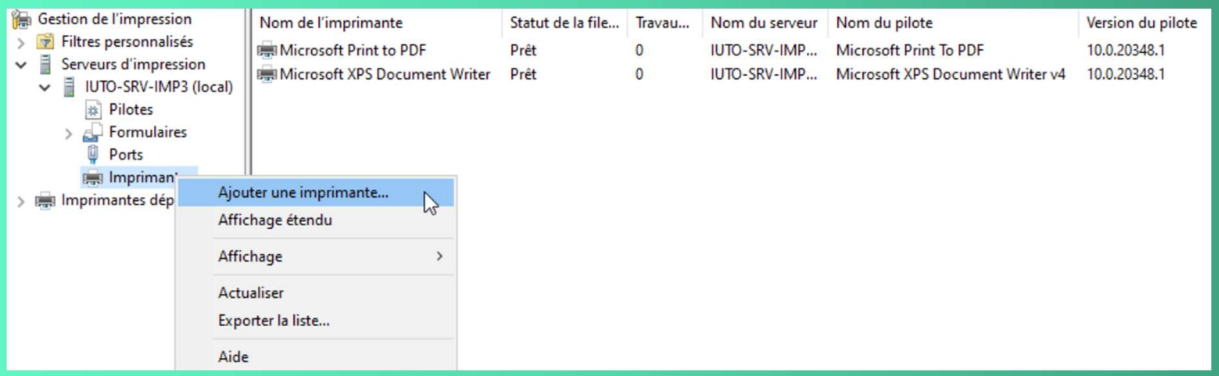


Remplissez le premier champ, nommé "Nom ou adresse IP de l'imprimante" en indiquant l'adresse IP de votre imprimante. Ensuite, donnez un nom à ce port en remplissant le champ "Nom du port", par exemple indiquez le nom de l'imprimante suivi de l'adresse IP, ce qui sera pratique visuellement dans la console.

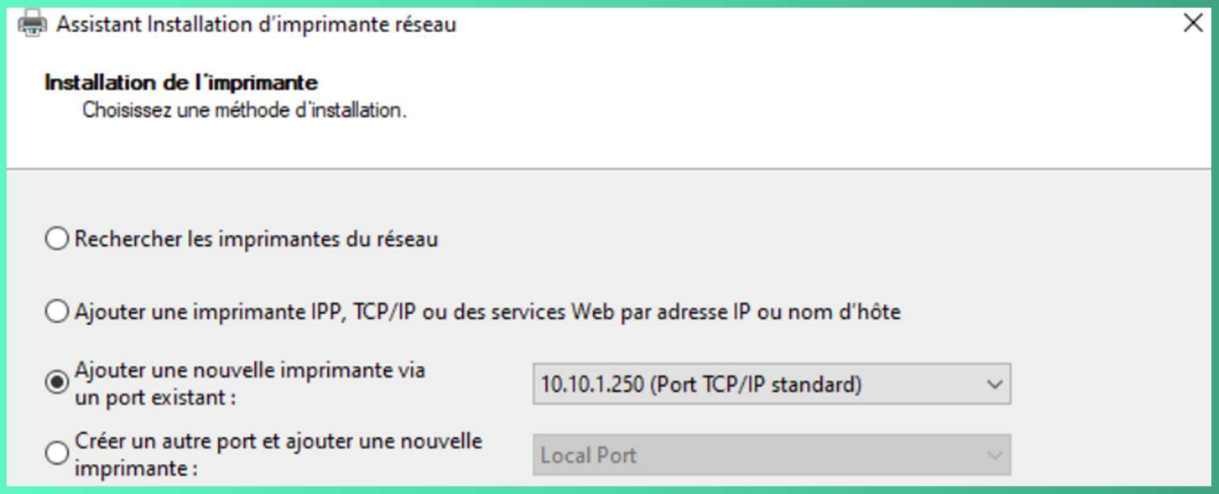


Ajouter l'imprimante à partager :

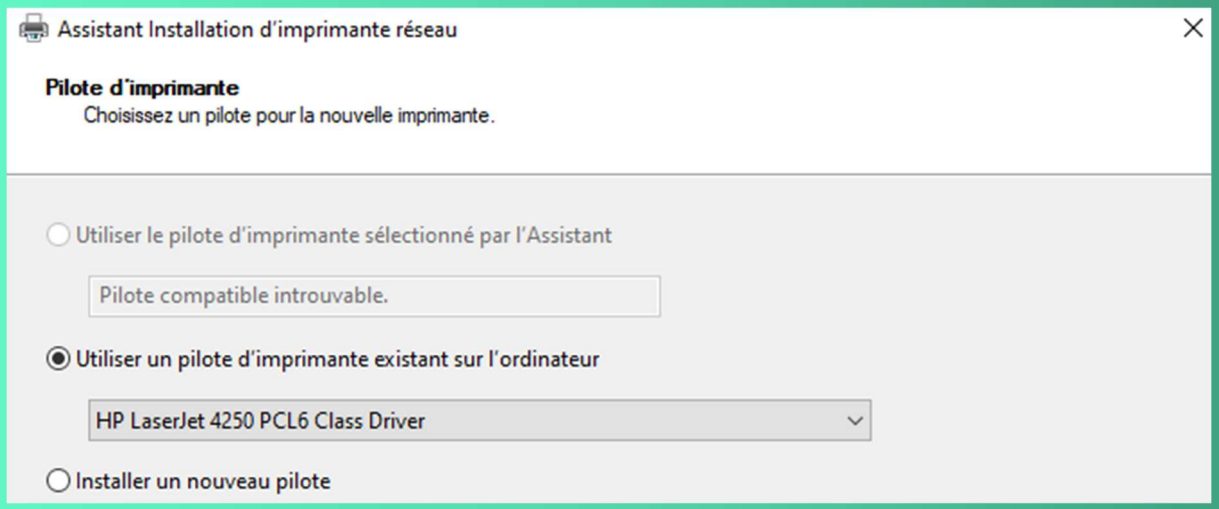
Pour ajouter l'imprimante, effectuez un clic droit sur "Imprimantes" et cliquez sur "Ajouter une imprimante".



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



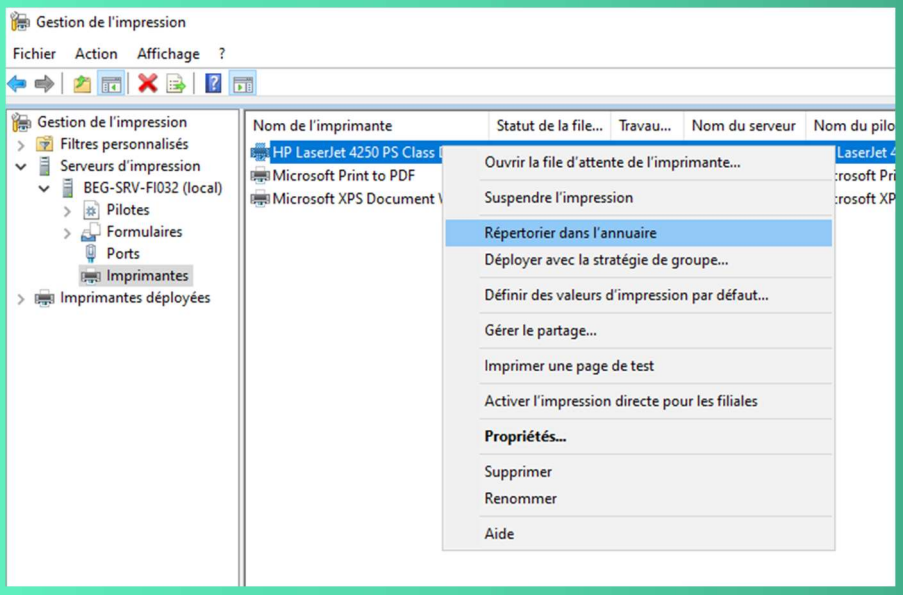
Sélectionner 'utiliser un pilote d'imprimante existant sur l'ordinateur



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

Répertorier l'imprimante dans l'annuaire :

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

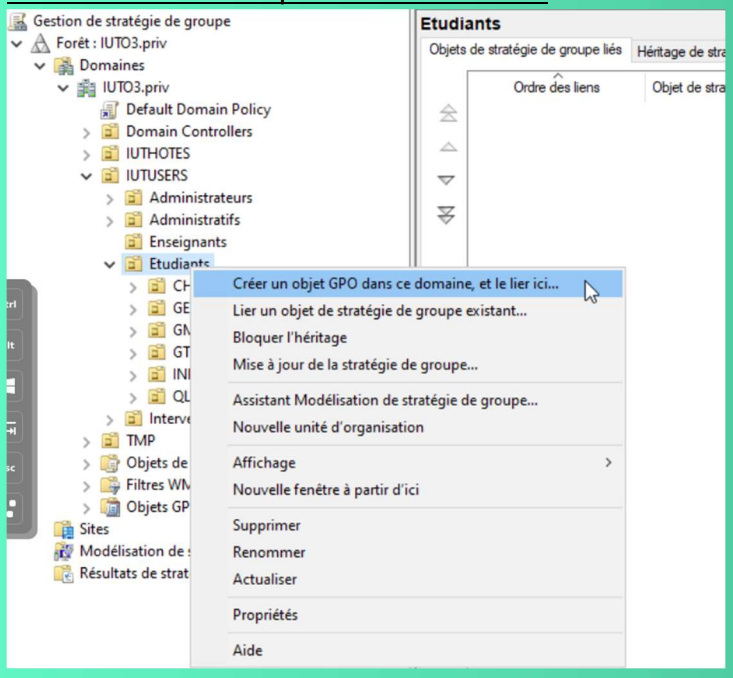


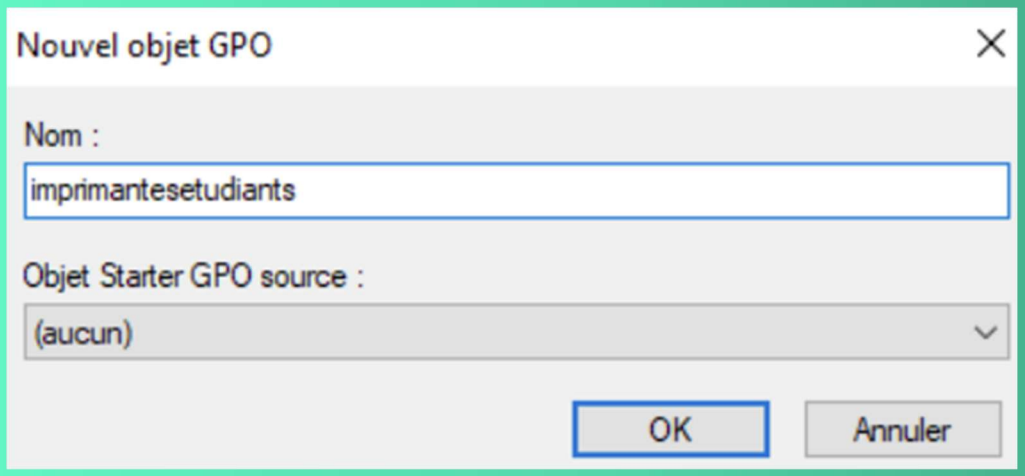
Ensuite, j'ai ajouté 2 autres imprimantes nommée IUTO-CHI003-IMP3 et IUTO-CHI101-IMP3

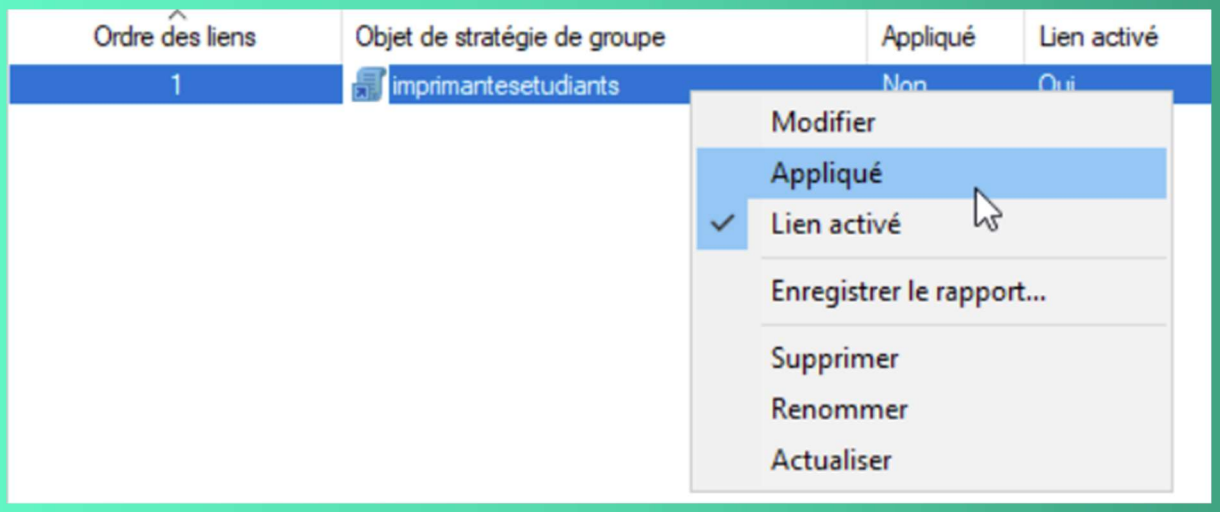
Et doublé ces imprimantes pour séparer les profs et les étudiants

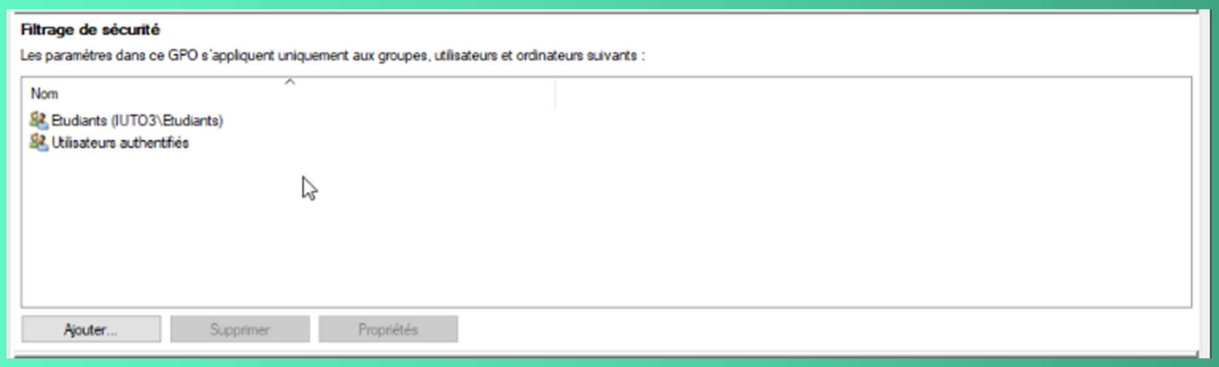
Nom de l'imprimante	Statut de la file...	Travau...	Nom du serveur	Nom du pilote	Version du pilote
IUTO-CHI001-IMPETUD3	Prêt	0	IUTO-SRV-IMP...	HP LaserJet 4250 PCL6 Class Driver	10.0.17119.1
IUTO-CHI001-IMPPROF3	Erreur	2	IUTO-SRV-IMP...	HP LaserJet 4250 PCL6 Class Driver	10.0.17119.1
IUTO-CHI003-IMPETUD3	Prêt	0	IUTO-SRV-IMP...	HP LaserJet 4250 PCL6 Class Driver	10.0.17119.1
IUTO-CHI003-IMPPROF3	Prêt	0	IUTO-SRV-IMP...	HP LaserJet 4250 PCL6 Class Driver	10.0.17119.1
IUTO-CHI101-IMPETUD3	Prêt	0	IUTO-SRV-IMP...	HP LaserJet 4250 PCL6 Class Driver	10.0.17119.1
IUTO-CHI101-IMPPROF3	Prêt	0	IUTO-SRV-IMP...	HP LaserJet 4250 PCL6 Class Driver	10.0.17119.1

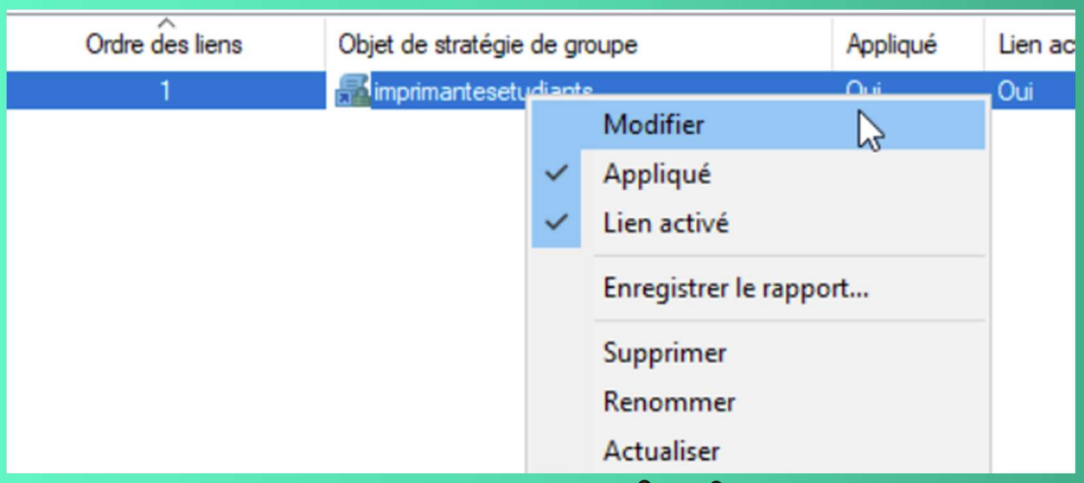
Création de la GPO pour les étudiants :

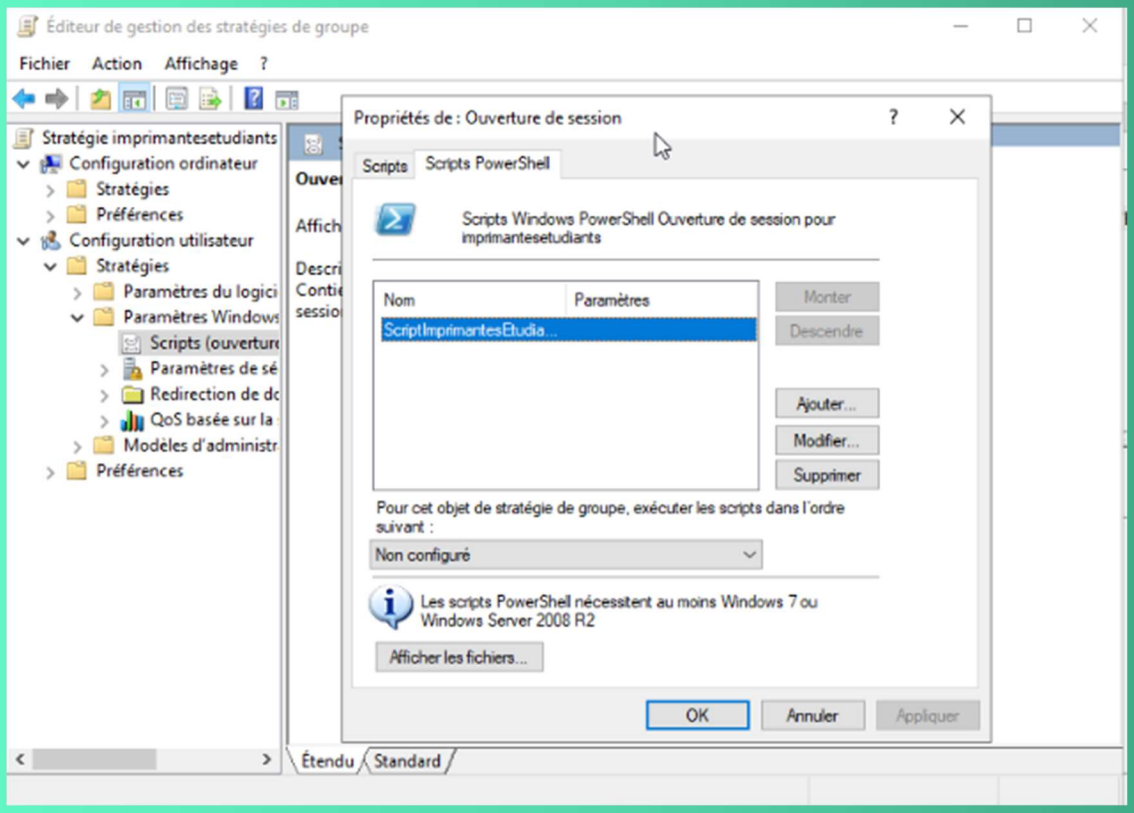


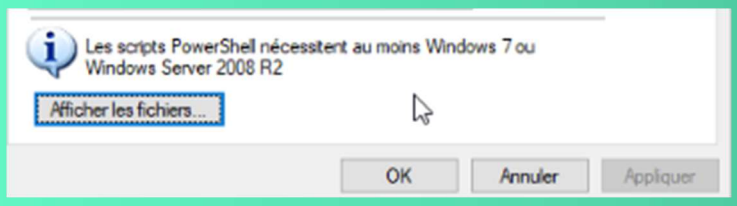

Nouvel objet GPO
Nom :
imprimantesetudiants
Objet Starter GPO source :
(aucun)
OK
Annuler


Ordre des liens
Objet de stratégie de groupe
Appliqué
Lien activé
1
imprimantesetudiants
Modifier
Appliqué
Lien activé
Enregistrer le rapport...
Supprimer
Renommer
Actualiser

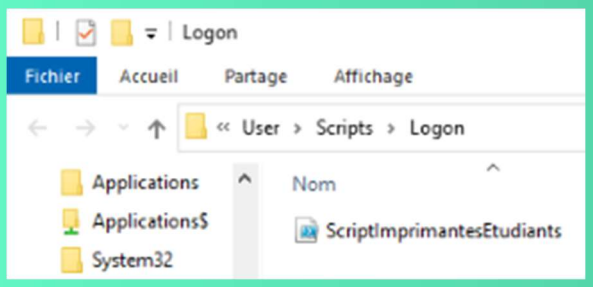

Filtrage de sécurité
Les paramètres dans ce GPO s'appliquent uniquement aux groupes, utilisateurs et ordinateurs suivants :
Nom
Etudiants (IUTO3\Etudiants)
Utilisateurs authentifiés
Ajouter...
Supprimer
Propriétés


Ordre des liens
Objet de stratégie de groupe
Appliqué
Lien ac
1
Oui
Oui
Modifier
Appliqué
Lien activé
Enregistrer le rapport...
Supprimer
Renommer
Actualiser

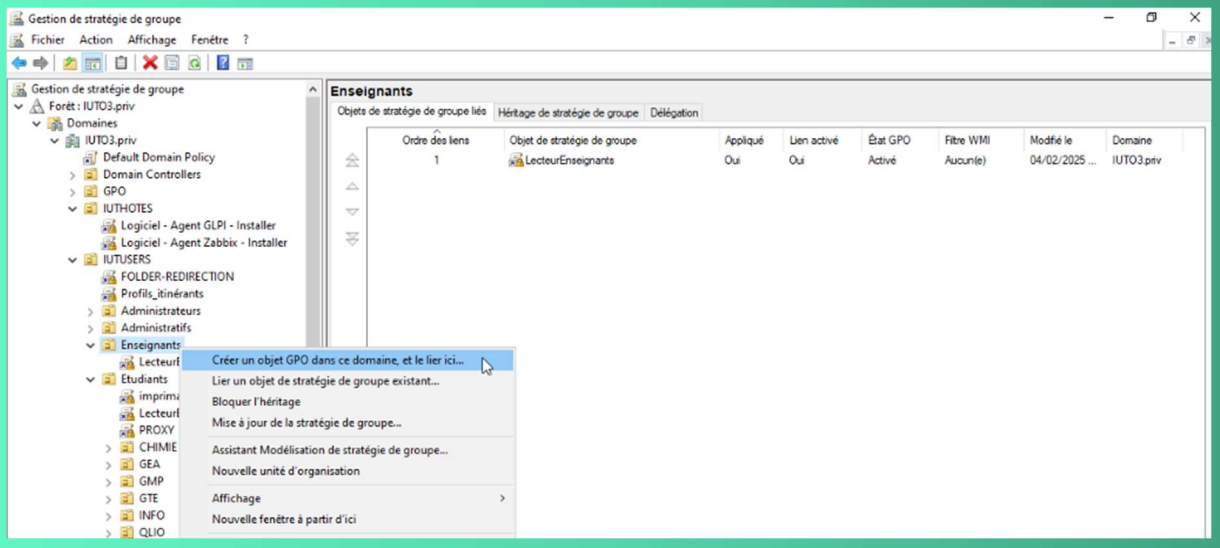


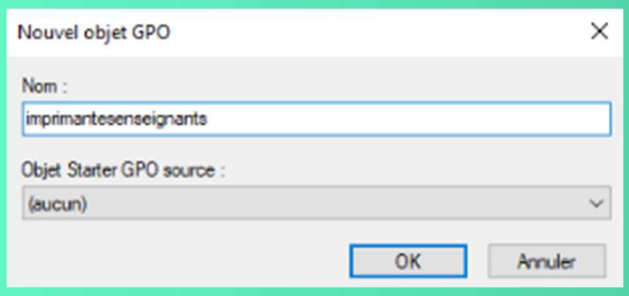


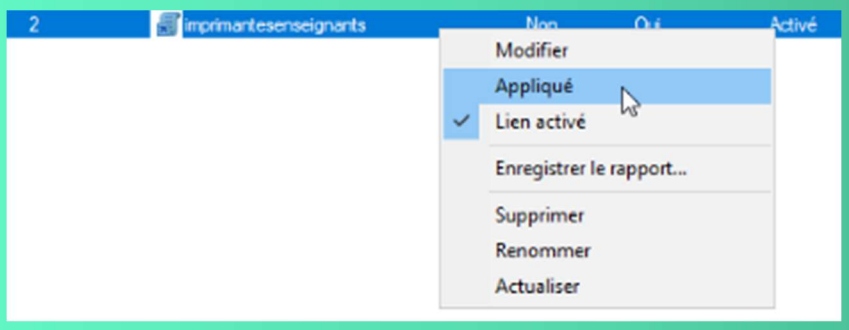
Copier son script à cet endroit

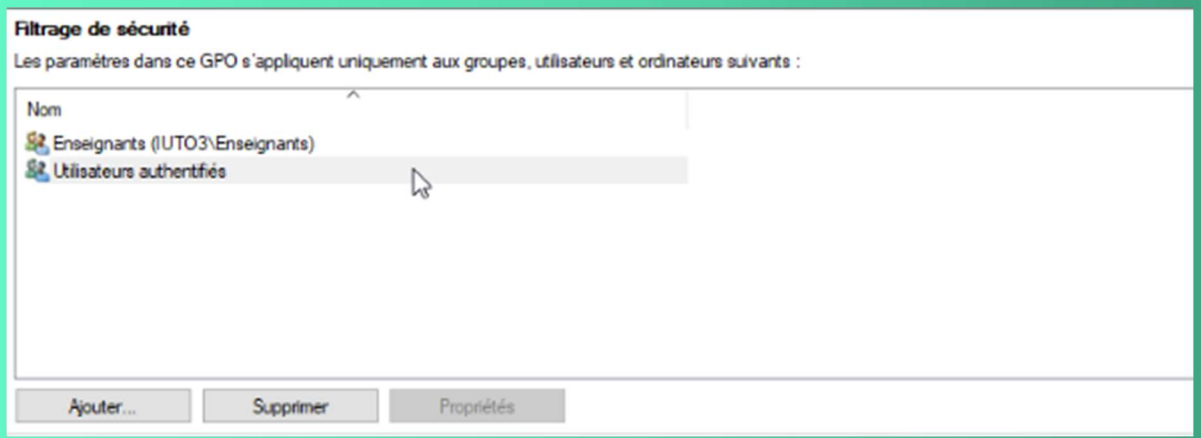


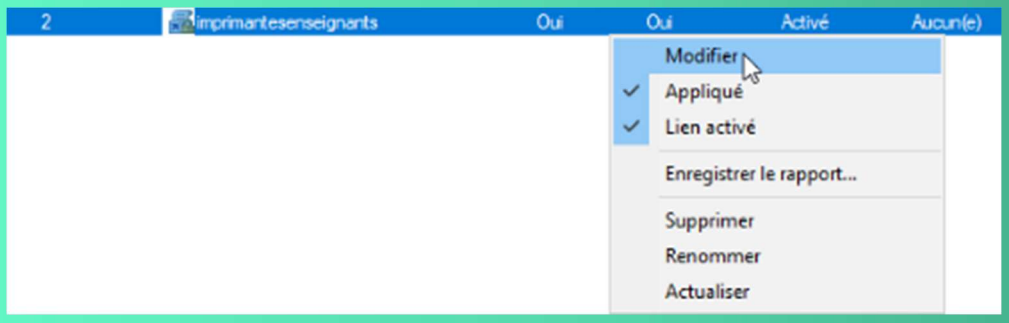
Création de la GPO pour les enseignants :

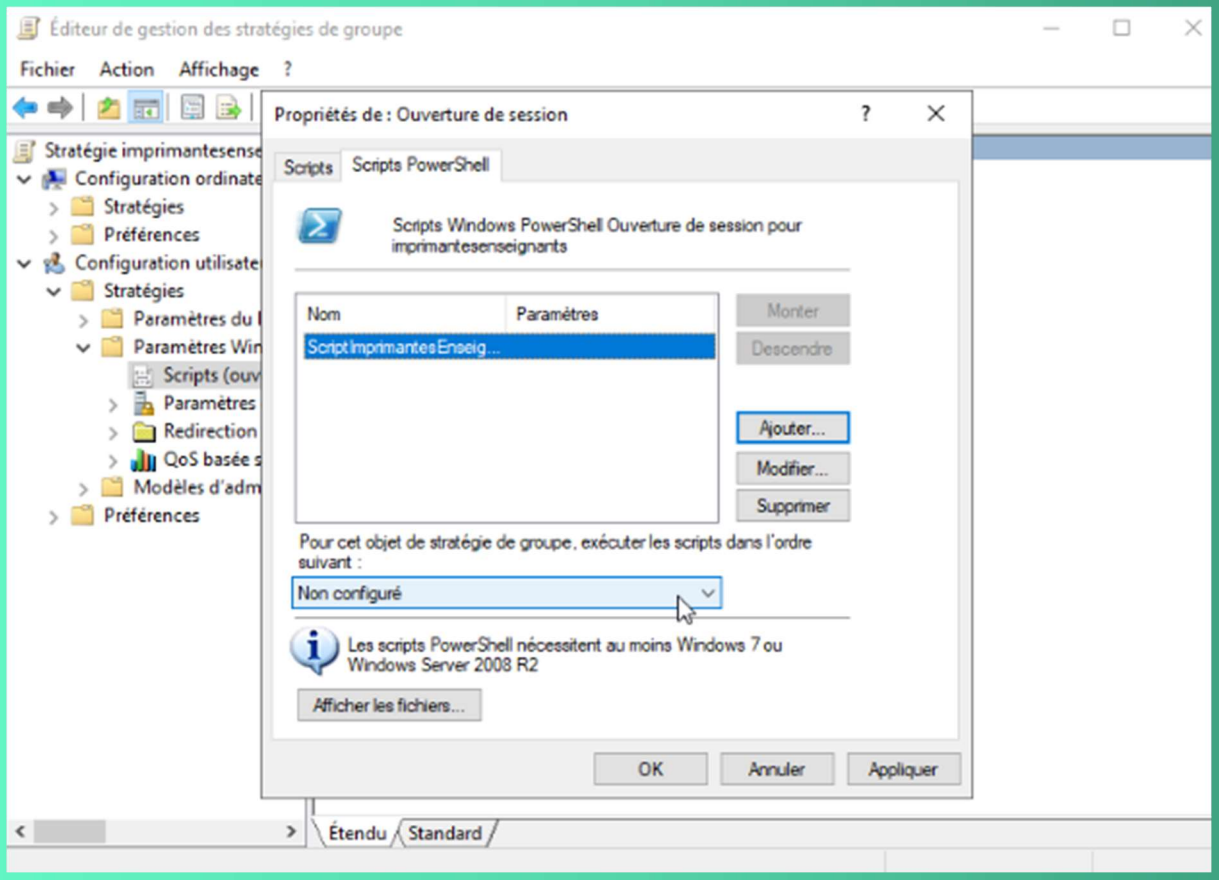

Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : IUTO3.priv
Domaines
IUTO3.priv
Default Domain Policy
Domain Controllers
GPO
IUTHOTES
Logiciel - Agent GLPI - Installer
Logiciel - Agent Zabbix - Installer
IUTUSERS
FOLDER-REDIRECTION
Profils_itinérants
Administrateurs
Administratifs
Enseignants
Étudiants
CHIMIE
GEA
GMP
GTE
INFO
QLIO
Enseignants
Objets de stratégie de groupe liés
Héritage de stratégie de groupe
Délégation
Ordre des liens
Objet de stratégie de groupe
Appliqué
Lien activé
État GPO
Filtre WMI
Modifié le
Domaine
1
LecteurEnseignants
Oui
Oui
Activé
Aucun(e)
04/02/2025 ...
IUTO3.priv
Créer un objet GPO dans ce domaine, et le lier ici...
Lier un objet de stratégie de groupe existant...
Bloquer l'héritage
Mise à jour de la stratégie de groupe...
Assistant Modélisation de stratégie de groupe...
Nouvelle unité d'organisation
Affichage
Nouvelle fenêtre à partir d'ici

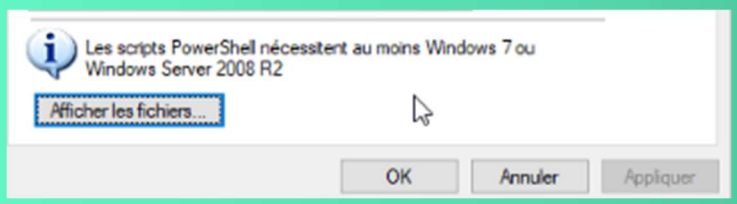

Nouvel objet GPO
Nom :
imprimantesenseignants
Objet Starter GPO source :
(aucun)
OK
Annuler


2
imprimantesenseignants
Activé
Modifier
Appliqué
Lien activé
Enregistrer le rapport...
Supprimer
Renommer
Actualiser


Filtrage de sécurité
Les paramètres dans ce GPO s'appliquent uniquement aux groupes, utilisateurs et ordinateurs suivants :
Nom
Enseignants (IUTO3\Enseignants)
Utilisateurs authentifiés
Ajouter...
Supprimer
Propriétés





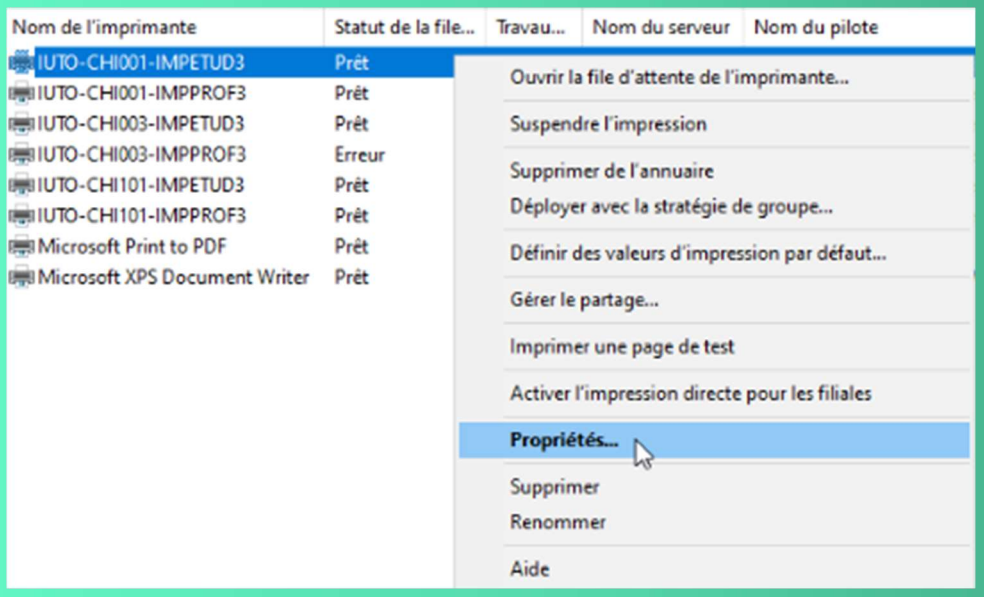


Et copier coller le script ici

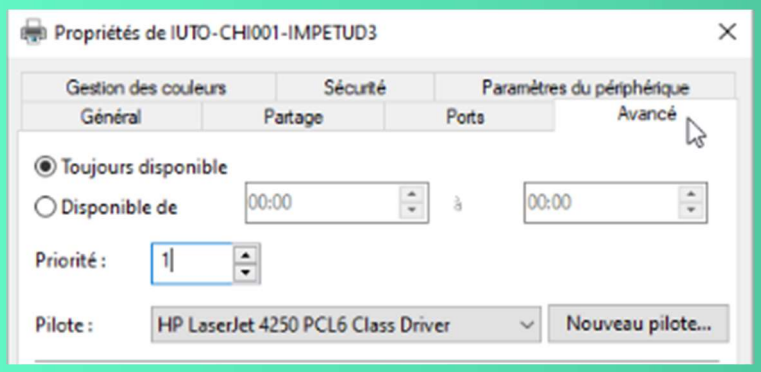
Modifier la priorité des files d'attente :

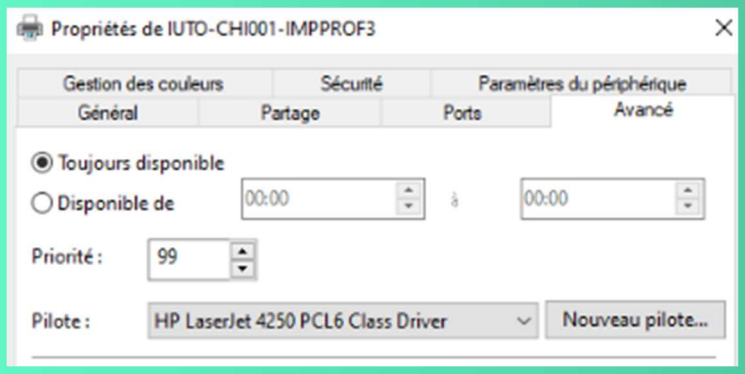
Nous allons configurer la priorité des files d'attentes pour faire en sorte que les enseignants soit prioritaires

Pour ce faire, clic droit sur l'imprimante puis priorités



Puis dans l'onglet avancé, configurer la priorité des étudiants à 1 et celle des enseignants à 99





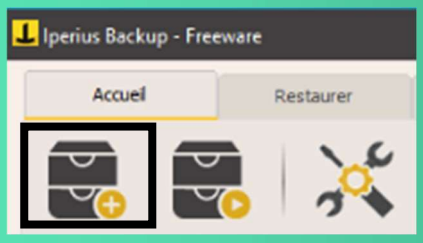
INSTALLATION DE IPERIUS

Pour installer Iperius, il faut aller sur le site officiel et télécharger l'éxécutable version 8.5.5:

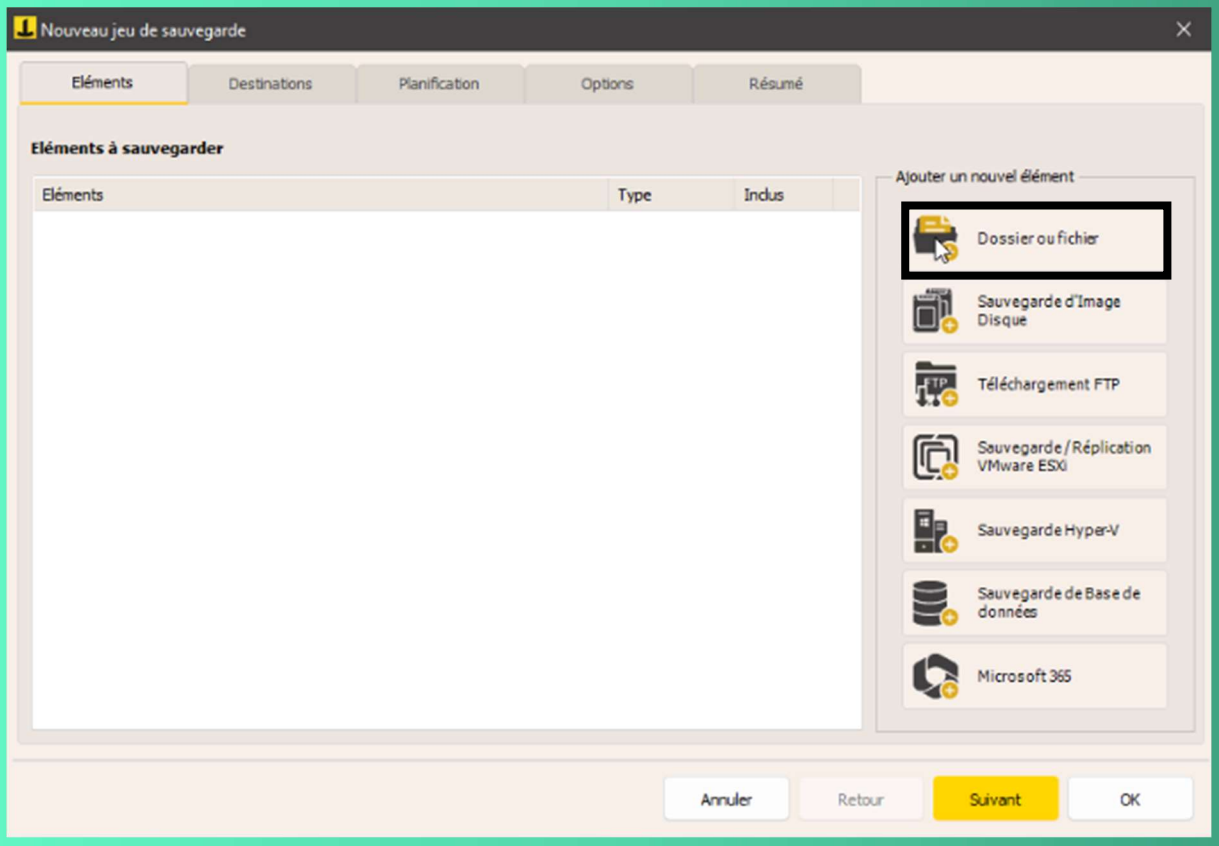
https://www.iperiusbackup.fr/

Créer une sauvegarde :

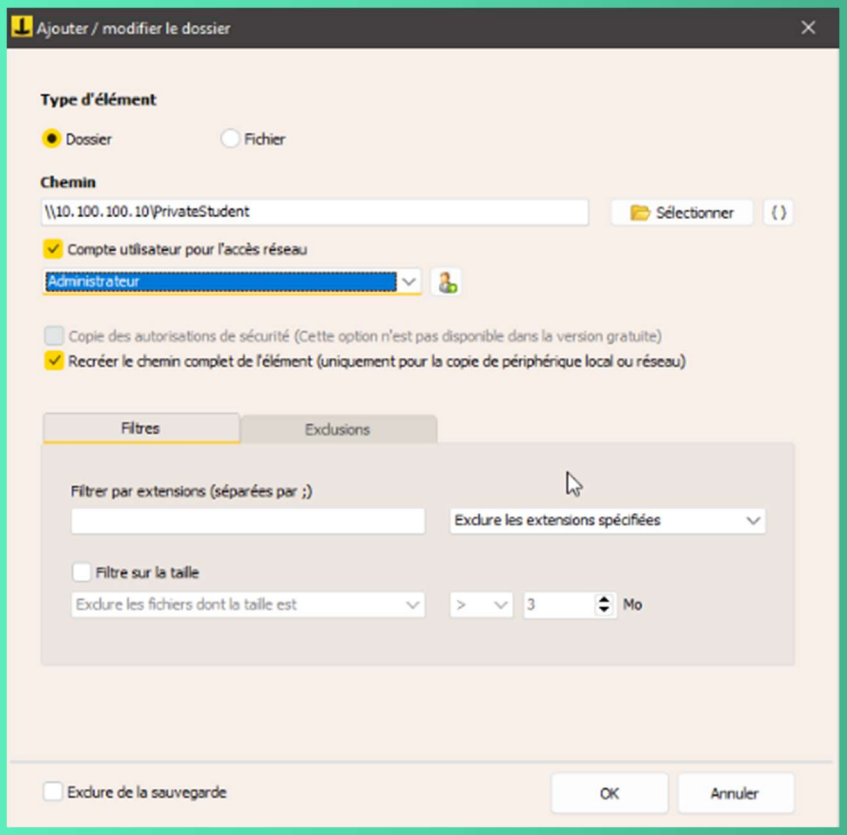
Pour créer une sauvegarde sur Iperius, il faut cliquer sur 'créer un nouveau jeu de sauvegarde'



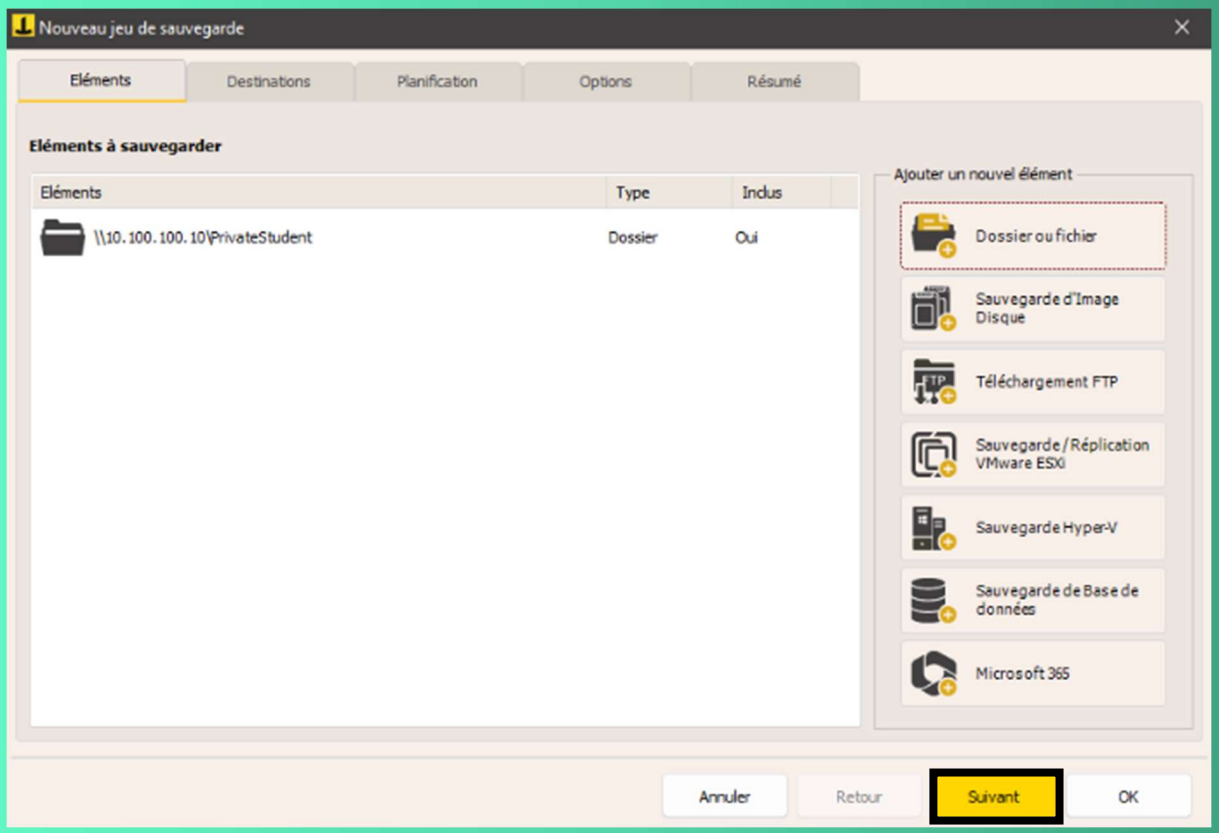
Ensuite, sélectionner le nouvel élément de sauvegarde en fonction de ce que nous voulons sauvegarder. Dans notre cas, nous avons sauvegardé un dossier :



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

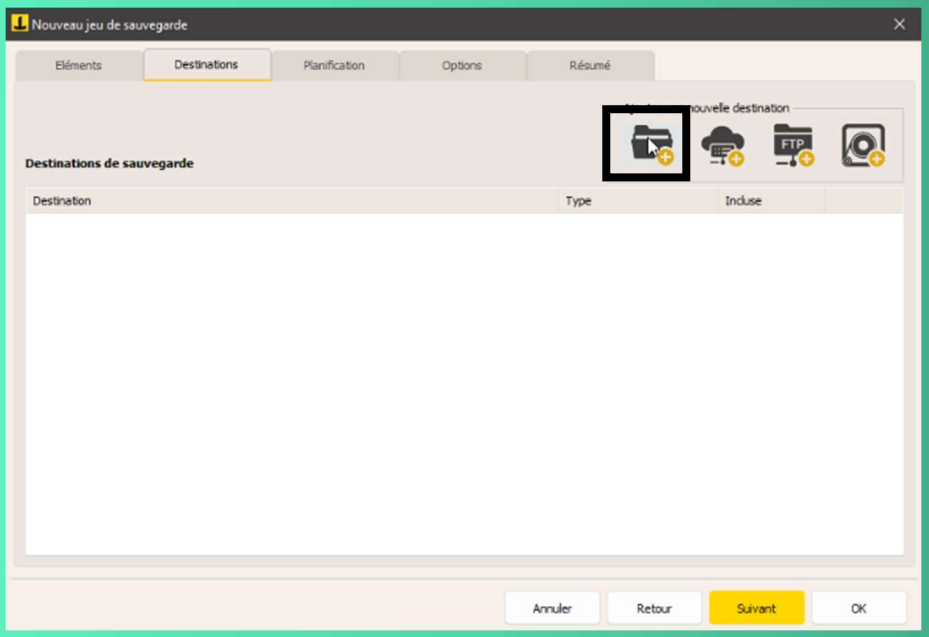


Maintenant que le chemin de notre dossier private à sauvegarder est créé, cliquer sur ‘suivant’

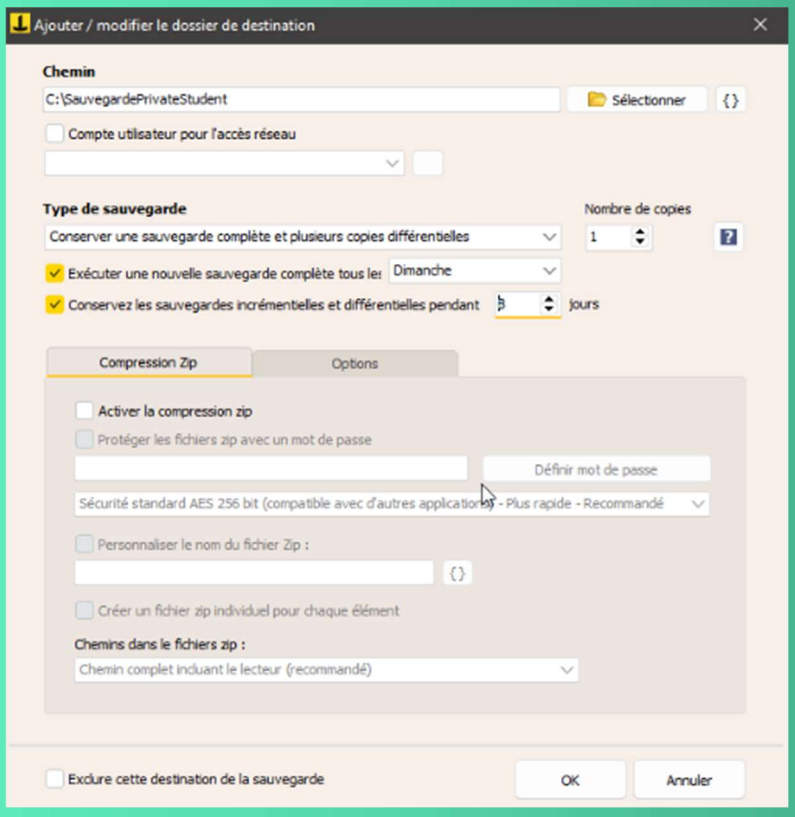


Choisir le dossier de sauvegarde :

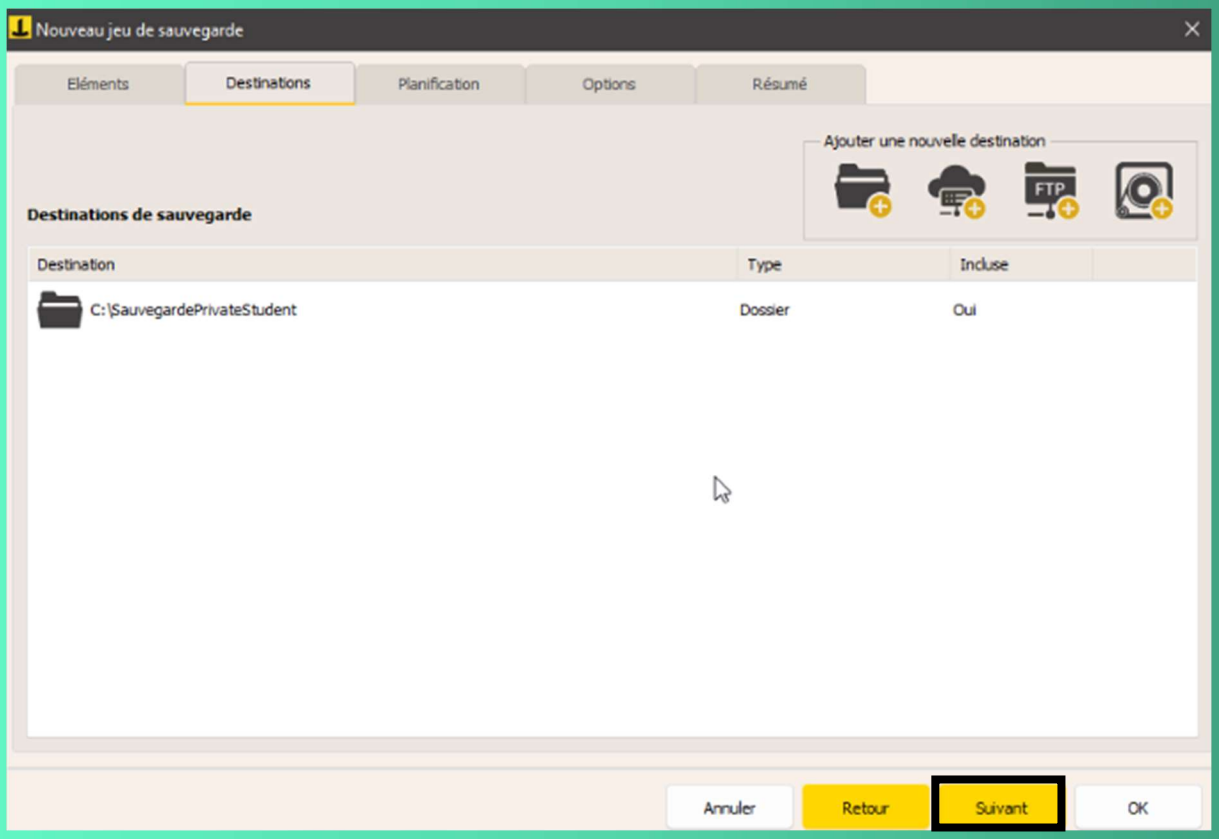
Pour choisir un dossier ou la sauvegarde sera enregistrer, cliquer sur ‘Ajouter un dossier de destination’, il est aussi possible de faire une sauvegarde sur le cloud, sur un serveur FTP ou alors une bande



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

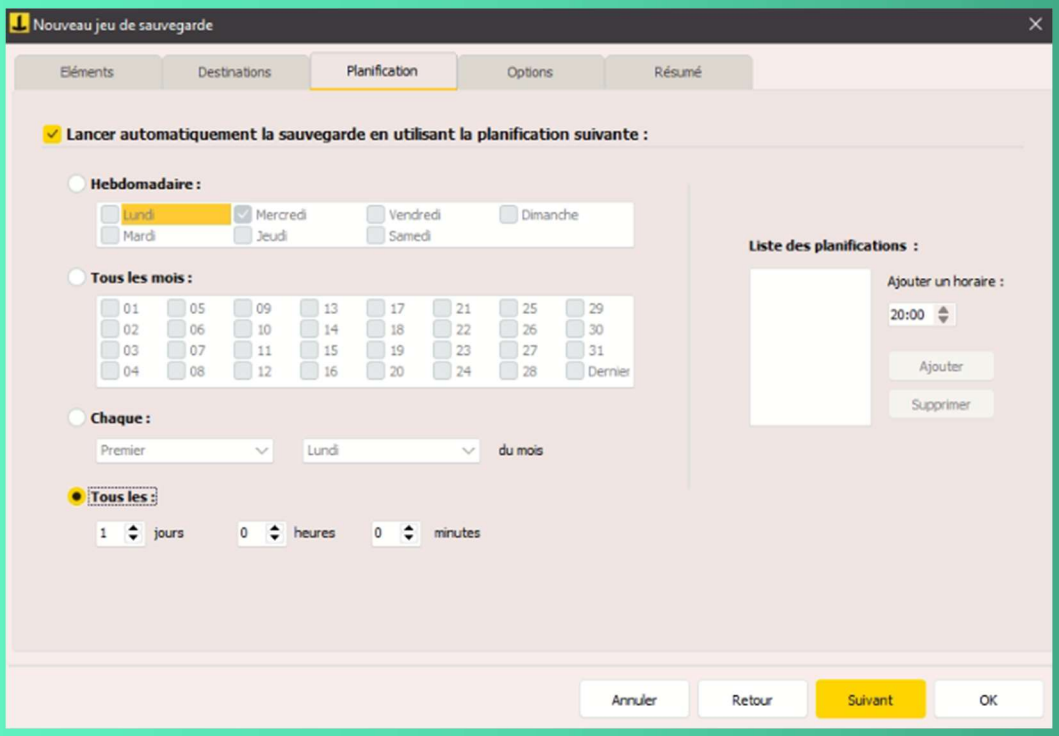


Maintenant que le chemin du dossier de sauvegarde est créé, cliquer sur ‘suivant’



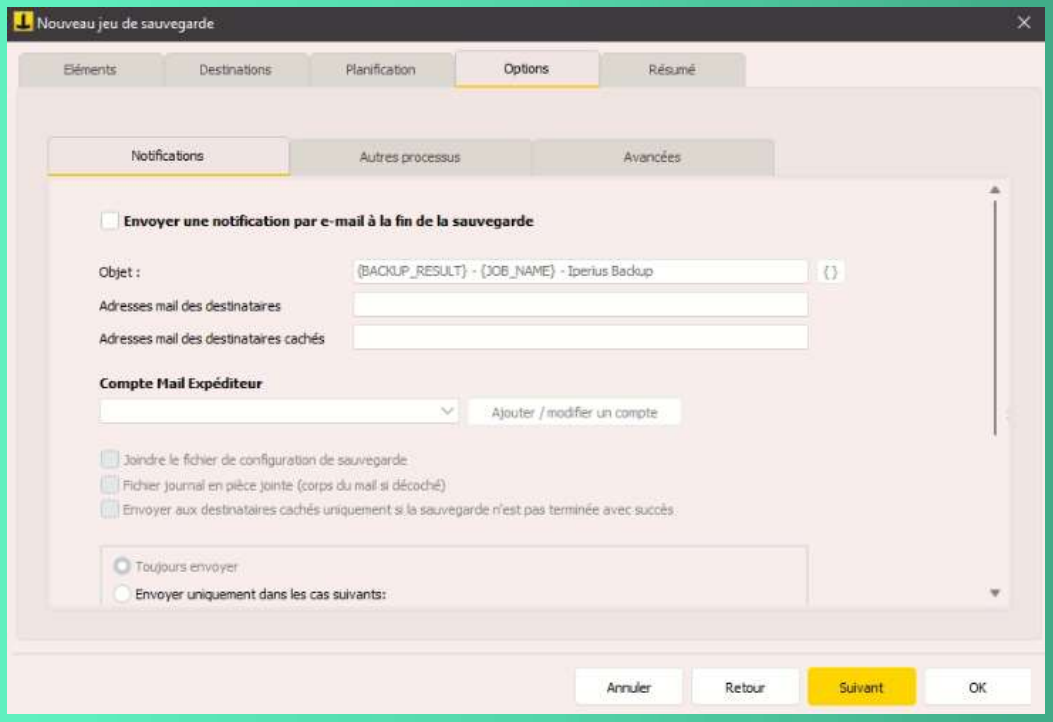
Planification :

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



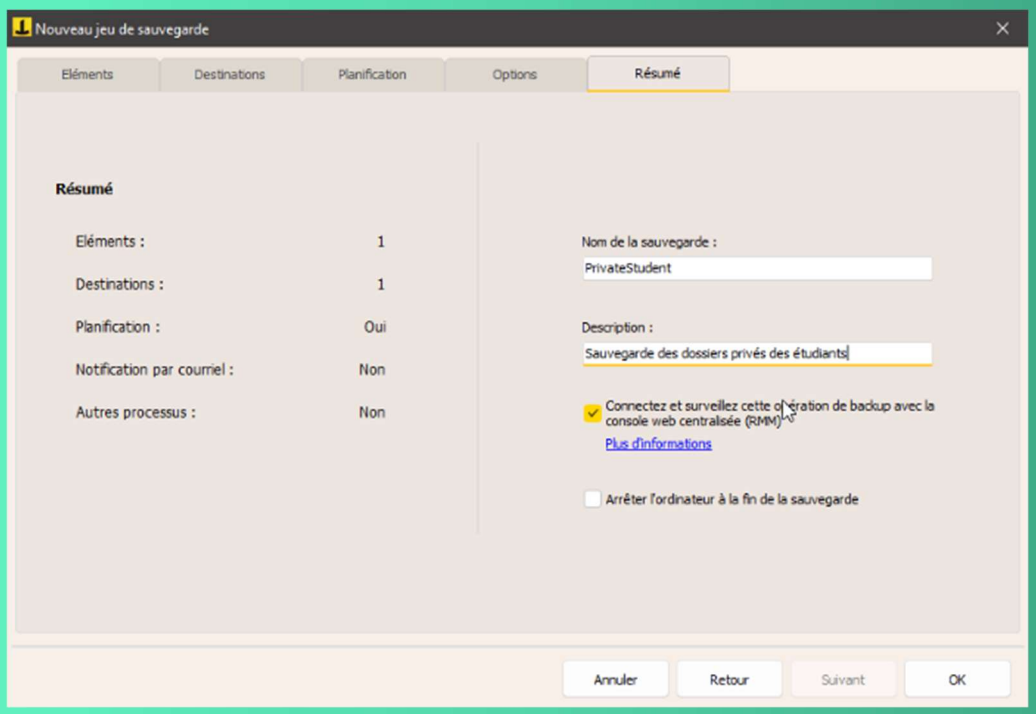
Options :

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



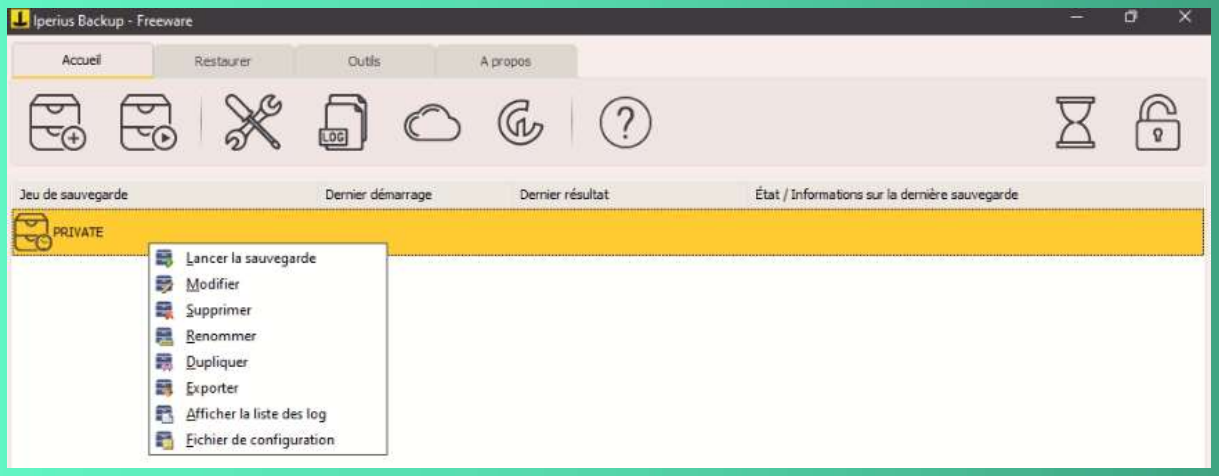
Résume :

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



Test de la sauvegarde :

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



Faire de même pour les dossiers PrivateTeacher et Promotions

INSTALLATION DE GLPI

Installer le socle LAMP :

La première grande étape consiste à installer les paquets du socle LAMP : Linux Apache2 MariaDB PHP. Sous Debian 12, qui est la dernière version stable de Debian, PHP 8.2 est distribué par défaut dans les dépôts officiels.

Commençons par installer ces trois paquets :

apt install apache2 php mariadb-server

Puis, nous allons installer toutes les extensions nécessaires au bon fonctionnement de GLPI.

apt install php-xml php-common php-json php-mysql php-mbstring php-curl php-gd php-intl php-zip php-bz2 php-imap php-apcu

Ces commandes vont permettre de récupérer les versions de ces extensions pour PHP 8.2.

Si vous envisagez d'associer GLPI avec un annuaire LDAP comme l'Active Directory, vous devez installer l'extension LDAP de PHP. Sinon, ce n'est pas nécessaire et vous pouvez le faire par la suite, si besoin.

apt install php-ldap

Nous venons d'installer Apache2, MariaDB, PHP et un ensemble d'extensions.

Préparer une base de données pour GLPI :

Nous allons préparer MariaDB pour qu'il puisse héberger la base de données de GLPI. La première action à effectuer, c'est d'exécuter la commande ci-dessous pour effectuer le minimum syndical en matière de sécurisation de MariaDB.

Mysql_secure_installation

```
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
 ... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Ensuite, nous allons créer une base de données dédiée pour GLPI et celle-ci sera accessible par un utilisateur dédié. Hors de question d'utiliser le compte root de MariaDB : une base de données = un utilisateur.

Connectez-vous à votre instance MariaDB :

Mysql -u root -p

Puis, nous allons exécuter les requêtes SQL ci-dessous pour créer la base de données "glpi" ainsi que l'utilisateur "gt" avec le mot de passe "MotDePasseRobuste" (que vous changez, bien sûr). Cet utilisateur aura tous les droits sur cette base de données (et uniquement sur celle-ci).

CREATE DATABASE glpi;

GRANT ALL PRIVILEGES ON glpi.* TO gt@localhost IDENTIFIED BY "Azerty45";

FLUSH PRIVILEGES;

EXIT

Télécharger GLPI et préparer son installation :

La prochaine étape consiste à télécharger l'archive ".tgz" qui contient les sources d'installation de GLPI. A partir du GitHub de GLPI, récupérez le lien vers la dernière version. Ici, c'est la version GLPI 10.0.10 qui est installée.

wget https://github.com/glpi-project/glpi/releases/download/10.0.17/glpi-10.0.17.tgz

Puis, nous allons exécuter la commande ci-dessous pour décompresser l'archive .tgz dans le répertoire "/var/www/", ce qui donnera le chemin d'accès "/var/www/glpi" pour GLPI.

tar -xzvf glpi-10.0.17.tgz -C /var/www/

Nous allons définir l'utilisateur "www-data" correspondant à Apache2, en tant que propriétaire sur les fichiers GLPI.

chown www-data /var/www/glpi/ -R

Ensuite, nous allons devoir créer plusieurs dossiers et sortir des données de la racine Web (/var/www/glpi) de manière à les stocker dans les nouveaux dossiers que nous allons créer. Ceci va permettre de faire une installation sécurisée de GLPI, qui suit les recommandations de l'éditeur.

Commencez par créer le répertoire "/etc/glpi" qui va recevoir les fichiers de configuration de GLPI. Nous donnons des autorisations à www-data sur ce répertoire car il a besoin de pouvoir y accéder.

mkdir /etc/glpi

chown www-data /etc/glpi

Puis, nous allons déplacer le répertoire "config" de GLPI vers ce nouveau dossier :

mv /var/www/glpi/config /etc/glpi

Répétons la même opération avec la création du répertoire "/var/lib/glpi" :

mkdir /var/lib/glpi

chown www-data /var/lib/glpi/

Dans lequel nous déplaçons également le dossier "files" qui contient la majorité des fichiers de GLPI : CSS, plugins, etc.

mv /var/www/glpi/files /var/lib/glpi

Terminons par la création du répertoire "/var/log/glpi" destiné à stocker les journaux de GLPI. Toujours sur le même principe :

mkdir /var/log/glpi

chown www-data /var/log/glpi

Créer les fichiers de configuration :

Nous devons configurer GLPI pour qu'il sache où aller chercher les données. Autrement dit, nous allons déclarer les nouveaux répertoires fraichement créés.

Nous allons créer ce premier fichier :

nano /var/www/glpi/inc/downstream.php

Afin d'ajouter le contenu ci-dessous qui indique le chemin vers le répertoire de configuration :

```
<?php

define('GLPI_CONFIG_DIR', '/etc/glpi/');

if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {

require_once GLPI_CONFIG_DIR . '/local_define.php';

}
```

Ensuite, nous allons créer ce second fichier :

nano /etc/glpi/local_define.php

Afin d'ajouter le contenu ci-dessous permettant de déclarer deux variables permettant de préciser les chemins vers les répertoires "files" et "log" que l'on a préparé précédemment.

```
<?php

define('GLPI_VAR_DIR', '/var/lib/glpi/files');

define('GLPI_LOG_DIR', '/var/log/glpi');
```

Voilà, cette étape est terminée.

Préparer la configuration apache2 :

Passons à la configuration du serveur web Apache2. Nous allons créer un nouveau fichier de configuration qui va permettre de configurer le VirtualHost dédié à GLPI. Dans mon cas, le fichier s'appelle "IUTO3.priv.conf" en référence au nom de domaine choisi pour accéder à GLPI : IUTO3.priv. L'idéal étant d'avoir un nom de domaine (même interne) pour accéder à GLPI afin de pouvoir positionner un certificat SSL par la suite.

nano /etc/apache2/sites-available/IUTO3.priv.conf

Ce qui donne la configuration suivante (selon le modèle officiel de la documentation) :

```
<VirtualHost *:80>
        ServerName 10.100.100.240
        DocumentRoot /var/www/glpi/public
```

```
        # If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving multiple applications),
        # you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target the GLPI directory itself.
        # Alias "/glpi" "/var/www/glpi/public"
        <Directory /var/www/glpi/public>
                Require all granted
                RewriteEngine On
                # Redirect all requests to GLPI router, unless file exists.
                RewriteCond %{REQUEST_FILENAME} !-f
                RewriteRule ^(.*)$ index.php [QSA,L]
        </Directory>
</VirtualHost>
```

Puis, nous allons activer ce nouveau site dans Apache2 :

```
a2ensite IUTO3.priv.conf
```

Nous en profitons également pour désactiver le site par défaut car il est inutile :

```
a2dissite 000-default.conf
```

Nous allons aussi activer le module "rewrite" (pour les règles de réécriture) car on l'a utilisé dans le fichier de configuration du VirtualHost (RewriteCond / RewriteRule).

```
a2enmod rewrite
```

Il ne reste plus qu'à redémarrer le service Apache2 :

```
systemctl restart apache2
```

Utilisation de PHP8.2-FPM avec apache2 :

Pour utiliser PHP en tant que moteur de scripts avec Apache2, il y a deux possibilités : utiliser le module PHP pour Apache2 (libapache2-mod-php8.2) ou utiliser PHP-FPM.

Il est recommandé d'utiliser PHP-FPM car il est plus performant et se présente comme un service indépendant. Dans l'autre mode, chaque processus Apache2 exécute son propre moteur de scripts PHP.

Si vous souhaitez utiliser PHP-FPM, suivez les étapes ci-dessous. Sinon, passez à la suite mais veillez à configurer l'option "session.cookie_httponly" évoquée ci-dessous.

Nous allons commencer par installer PHP8.2-FPM avec la commande suivante :

```
apt install php8.2-fpm
```

Puis, nous allons activer deux modules dans Apache et la configuration de PHP-FPM, avant de recharger Apache2 :

a2enmod proxy_fcgi setenvif

a2enconf php8.2-fpm

systemctl reload apache2

Pour configurer PHP-FPM pour Apache2, nous n'allons pas éditer le fichier "/etc/php/8.2/apache2/php.ini" mais plutôt ce fichier :

nano /etc/php/8.2/fpm/php.ini

Dans ce fichier, recherchez l'option "session.cookie_httponly" et indiquez la valeur "on" pour l'activer, afin de protéger les cookies de GLPI.

; Whether or not to add the httpOnly flag to the cookie, which makes it

; inaccessible to browser scripting languages such as JavaScript.

; https://php.net/session.cookie-httponly

session.cookie_httponly = on

Enregistrez le fichier quand c'est fait. Par la suite, vous pourriez être amené à effectuer d'autres modifications, notamment pour augmenter la taille des uploads sur GLPI, etc.

Pour appliquer les modifications, nous devons redémarrer PHP-FPM :

systemctl restart php8.2-fpm.service

Pour finir, nous devons modifier notre VirtualHost pour préciser à Apache2 que PHP-FPM doit être utilisé pour les fichiers PHP :

nano /etc/apache2/sites-available/IUTO3.priv.conf

<FilesMatch \.php$>

SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"

</FilesMatch>

```
 GNU nano 7.2                        /etc/apache2/sites-available/IUTO3.priv.conf
<VirtualHost *:80>
ServerName 10.100.100.240
DocumentRoot /var/www/glpi/public
# If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving multiple applications),
# you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target the GLPI directory itself.
# Alias "/glpi" "/var/www/glpi/public"
<Directory /var/www/glpi/public>
Require all granted
RewriteEngine On
# Redirect all requests to GLPI router, unless file exists.
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*)$ index.php [QSA,L]
</Directory>
<FilesMatch \.php$>
SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"
</FilesMatch>
</VirtualHost>
```

Quand c'est fait, relancer Apache2 :

Systemctl restart apache2

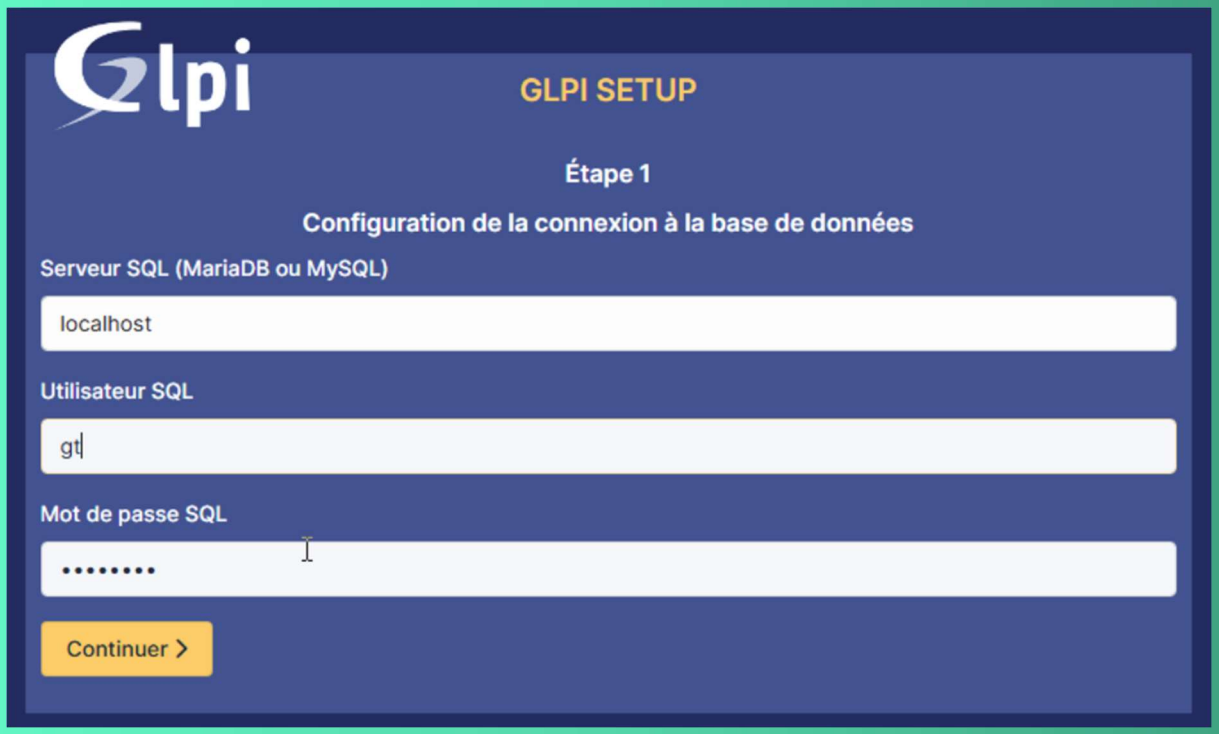
Installation de GLPI :

Pour effectuer l'installation de GLPI, nous devons utiliser un navigateur Web afin d'accéder à l'adresse du GLPI. Il s'agit de l'adresse déclarée dans le fichier de configuration Apache2 (ServerName). Si vous avez suivi toutes les étapes correctement, vous devriez arriver sur cette page. Nous allons commencer par choisir la langue.

Puisqu'il s'agit d'une nouvelle installation, nous cliquons sur "Installer".

Etape importante : GLPI vérifie la configuration de notre serveur pour déterminer si tous les prérequis sont respectés. Tout est bon, donc nous pouvons continuer.

A l'étape suivante, nous devons renseigner les informations pour se connecter à la base de données. Nous indiquons "localhost" en tant que serveur SQL puisque MariaDB est installé en local, sur le même serveur que GLPI. Puis, nous indiquons notre utilisateur "gt" et le mot de passe associé.



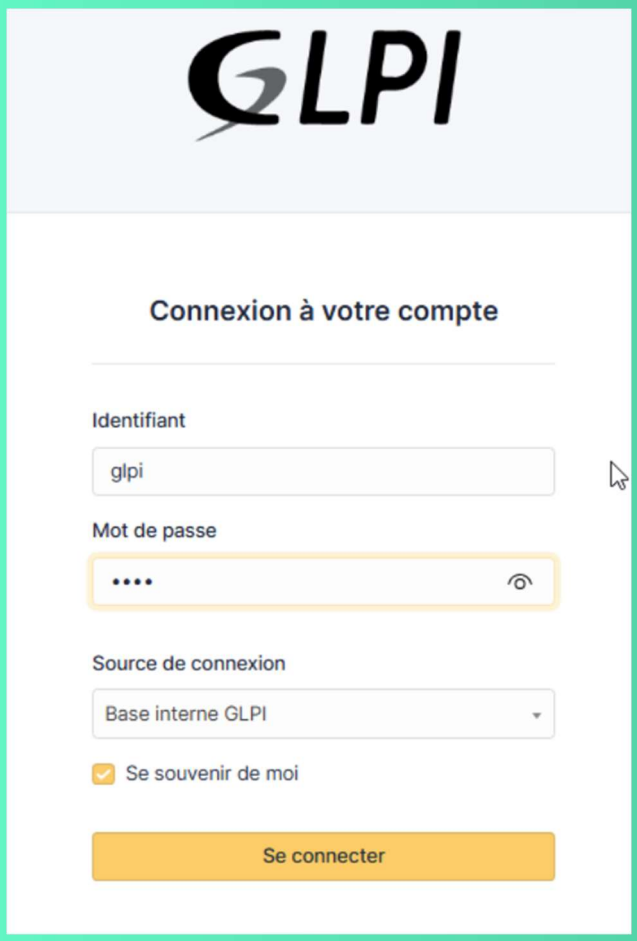
Après avoir cliqué sur "Continuer", nous devons choisir la base de données "glpi" créée précédemment.

Poursuivez...

Suivez les dernières étapes qui n'ont pas de réel impact. Le plus dur est fait !

Félicitations, vous venez d'installer GLPI ! Comme le précise la dernière étape, le compte administrateur par défaut est "glpi/glpi" !

Nous allons donc nous connecter avec le compte "glpi" et le mot de passe "glpi".



Même si l'installation est terminée, nous avons encore quelques actions à réaliser pour la finaliser :

- Changer le mot de passe de tous les comptes par défaut (cliquez sur les liens situés dans l'encadré orange) (mdp Azerty45)

- Supprimer le fichier "install.php" puisqu'il n'est plus nécessaire et représente un risque (relancer l'installation)

rm /var/www/glpi/install/install.php

Voilà, c'est fait. Désormais, votre GLPI est prêt à être utilisé et configuré (création d'utilisateurs, de catégories, de tickets, etc...).

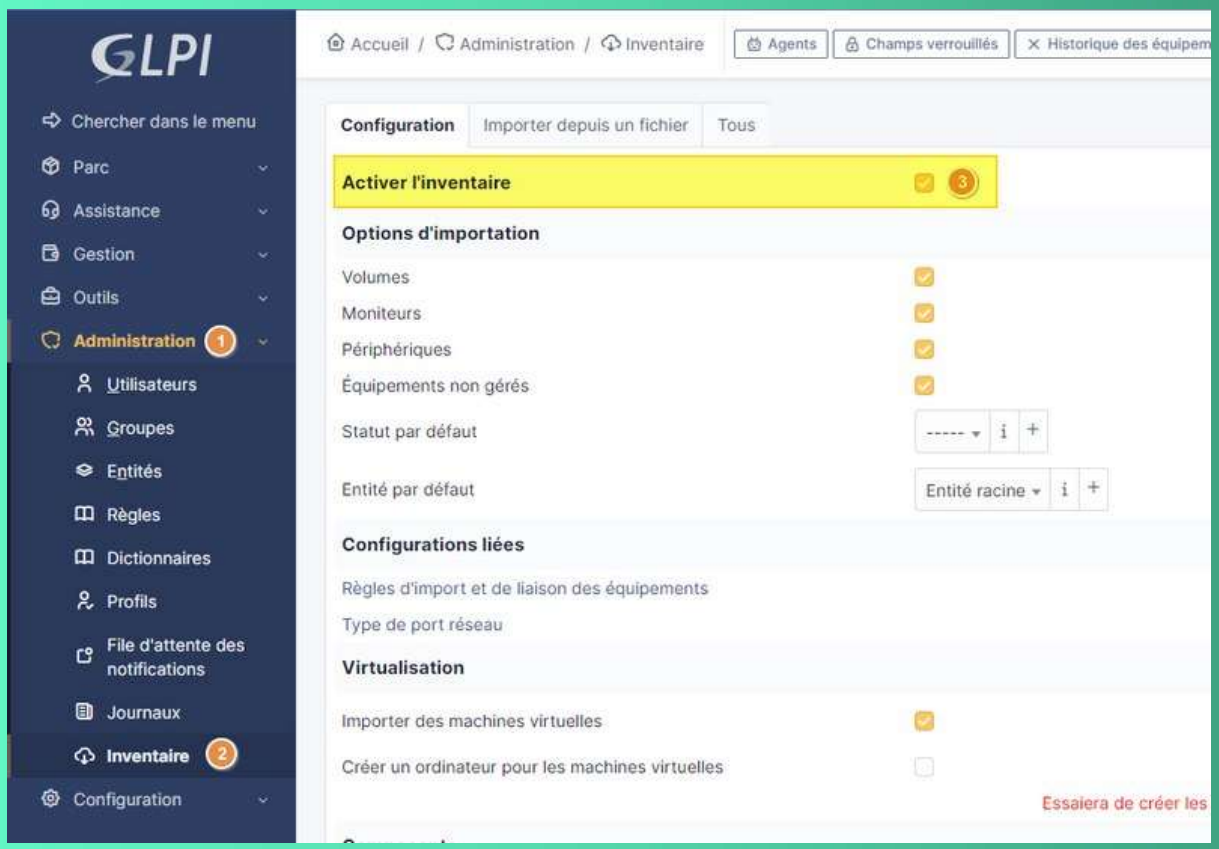
Activer l'inventaire dans GLPI 10 :

Cliquez sur "Administrateur" dans le menu latéral (1)

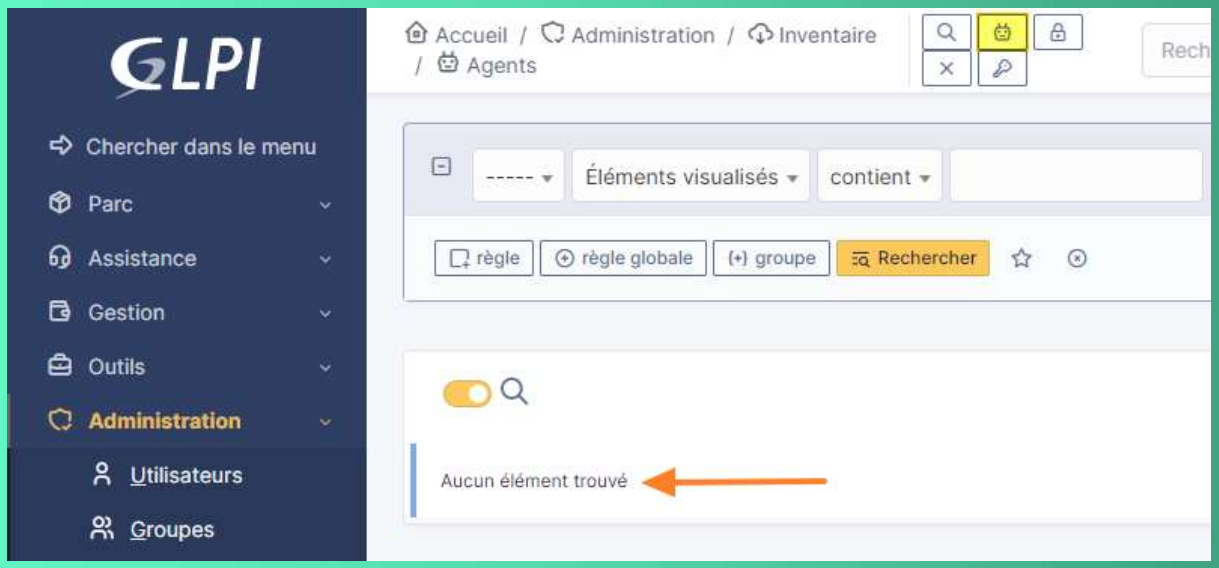
Cliquez sur "Inventaire" (2)

Cochez l'option "Activer l'inventaire" (3)

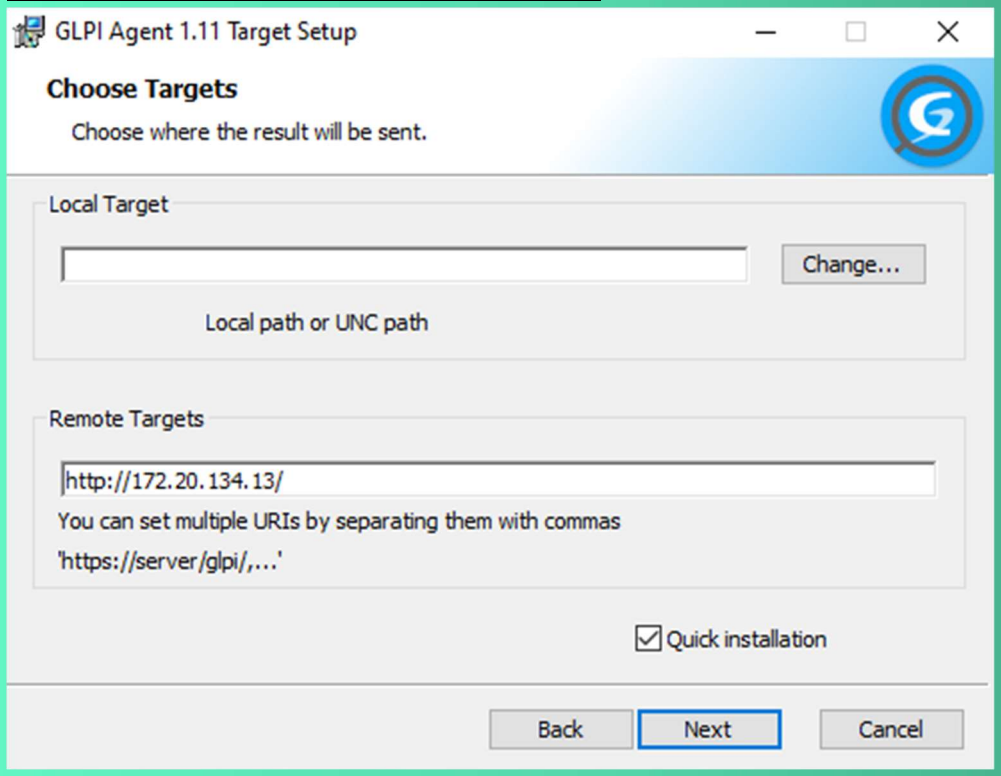
Enregistrez la modification en cliquant sur le bouton "Sauvegarder" en bas de page



Pour le moment, aucun agent n'est enregistré sur notre serveur GLPI. Nous pouvons le vérifier en cliquant sur l'icône qui ressemble à un robot en haut de l'interface. Nous pouvons lire la mention suivante : "Aucun élément trouvé".



Installer l'agent GLPI sur un client :



Créer une GPO pour déployer l'agent GLPI (sans script) :

Pour déployer l'agent GLPI par GPO, il y a plusieurs méthodes envisageables... Notamment celles-ci :

- Utiliser le script VBS "glpi-agent-deployment.vbs" mis à disposition par GLPI et l'exécuter en tant que script de démarrage de Windows
- Exécuter "msiexec.exe" avec les bons arguments pour cibler le package MSI de l'agent GLPI et spécifier l'URL de notre serveur GLPI, etc...
- Modifier le package MSI de l'Agent GLPI avec ORCA pour inclure l'URL de notre serveur, etc... et l'installation via la fonction "Installation de logiciel"

- Installer le package MSI de l'Agent GLPI via la fonction native "Installation de logiciel" des GPO et le configurer à l'aide de valeurs dans le Registre Windows

Nous allons partir sur la dernière méthode : elle me semble à la fois facile à mettre en œuvre et suffisamment flexible.

Télécharger et partager le package MSI de l'agent GLPI :

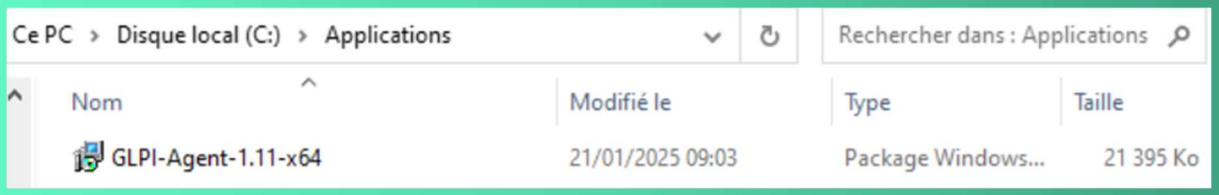
La première étape consiste à télécharger l'agent GLPI au format MSI, à partir du GitHub officiel mentionné en début d'article.

https://github.com/glpi-project/glpi-agent/releases/

J'ai installé cette version de client :

https://github.com/glpi-project/glpi-agent/releases/download/1.11/GLPI-Agent-1.11-x64.msi

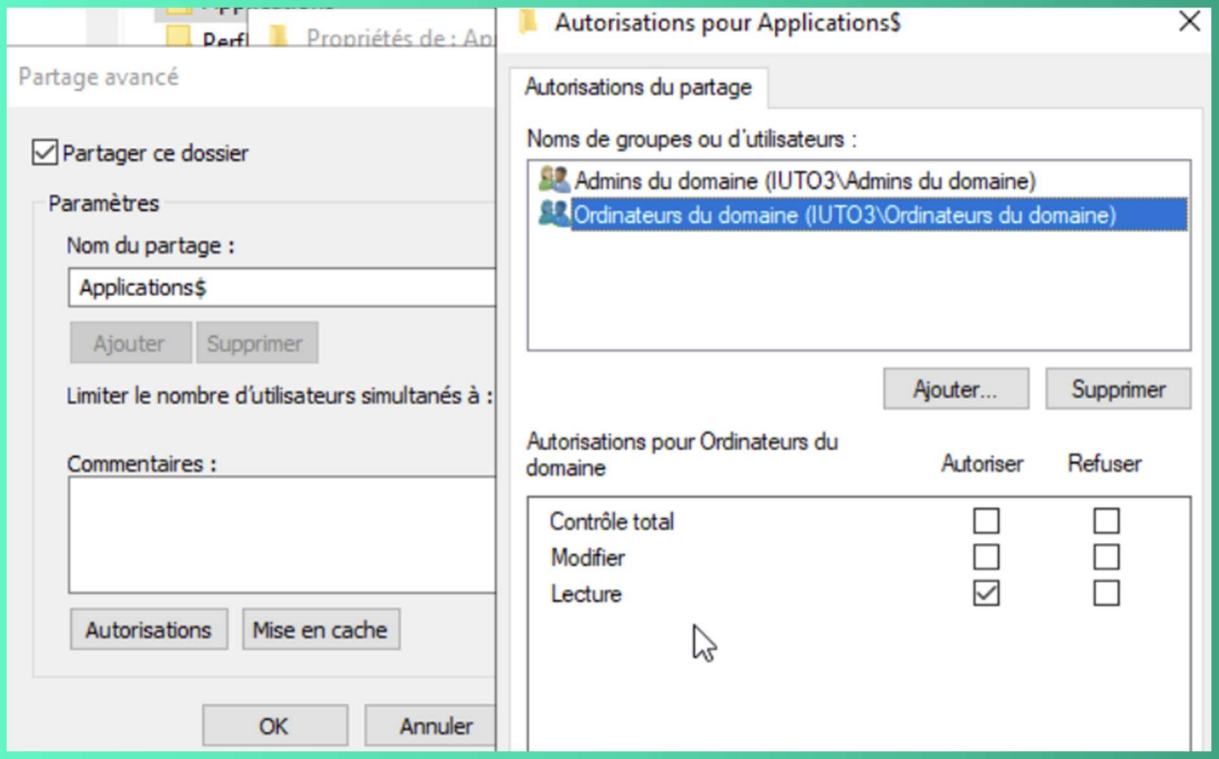
Dans mon cas, l'agent GLPI sera stocké dans "C:\Applications" du serveur "IUTO-SRV-AD3.IUTO3.priv".



Ce répertoire est partagé en tant que "Applications$" et les permissions de partage sont définies comme suit :

Groupe "Ordinateurs du domaine" en lecture seule

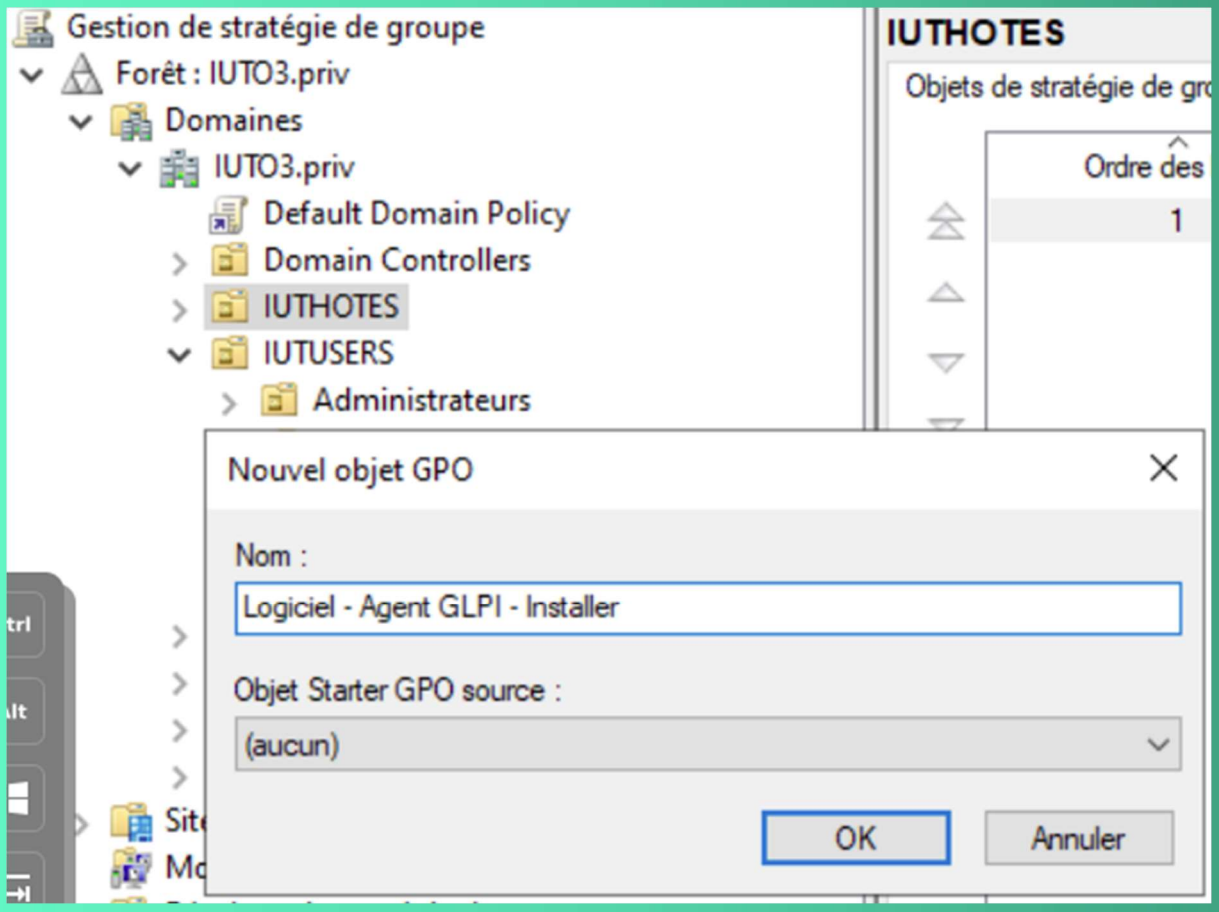
Groupe "Admins du domaine" en contrôle total



Installer l'agent GLPI par GPO :

Passons à la création de la stratégie de groupe pour déployer l'agent GLPI. Ouvrez la console "Gestion de stratégie de groupe" et créez une nouvelle GPO.

En ce qui me concerne, la GPO s'appelle "Logiciel - Agent GLPI - Installer" et elle est liée à l'OU "PC" qui contient mes postes de travail Windows. Attention, si vous liez la GPO à la racine de votre domaine Active Directory, l'agent GLPI sera déployé sur toutes les machines (postes de travail et serveurs).



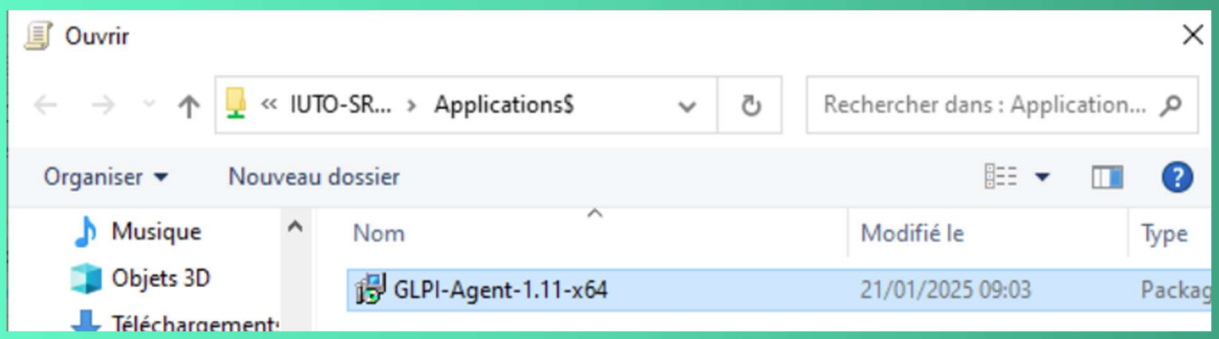
Une fois la GPO créée, vous allez devoir l'éditer via un clic droit sur son nom puis "Modifier". Parcourez les paramètres de cette façon :

Configuration ordinateur > Stratégies > Paramètres du logiciel > Installation de logiciel

Ici, effectuez un clic droit puis : Nouveau > Package. Une fenêtre va s'ouvrir afin de vous permettre de sélectionner le package MSI à déployer. Vous devez préciser le chemin réseau (chemin UNC) vers le package MSI.

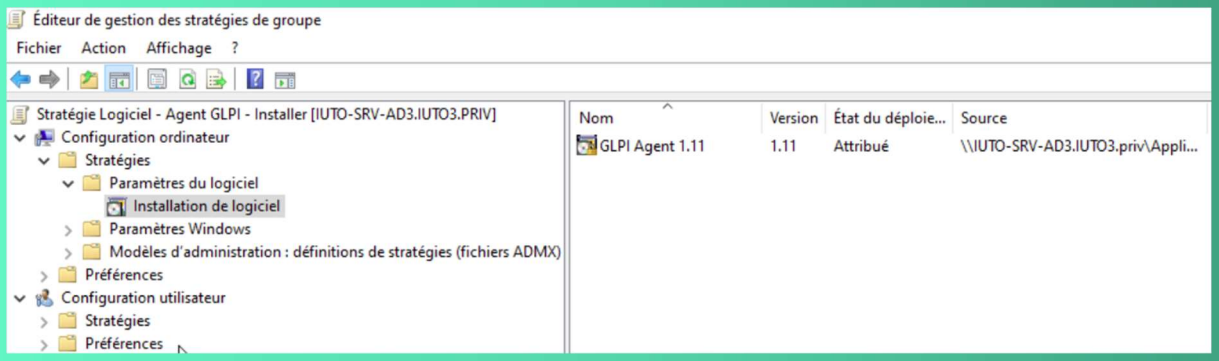
Pour ma part, cela donne le chemin suivant :

\\IUTO-SRV-AD3.IUTO3.priv\Applications$\GLPI-Agent-1.11-x64



A la question "Sélectionnez le type de déploiement", choisissez "Attribué" et poursuivez.

Voilà, l'agent GLPI est prêt à être déployé par GPO :



Le problème, c'est que l'agent GLPI sera déployé sans aucune configuration. De ce fait, il ne pourra pas se synchroniser sur notre serveur GLPI et les machines ne vont pas remonter dans l'inventaire....

Configurer l'agent GLPI avec le Registre Windows :

Pour répondre à cette problématique, nous allons configurer l'agent GLPI par GPO en jouant directement sur les valeurs situées dans la clé de Registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\GLPI-Agent

Effectivement, l'agent GLPI stocke sa configuration dans le Registre Windows, ce qui permet de la modifier facilement.

Ainsi, nous allons configurer deux valeurs :

server : pour indiquer l'URL du serveur GLPI (vers une page spécifique)

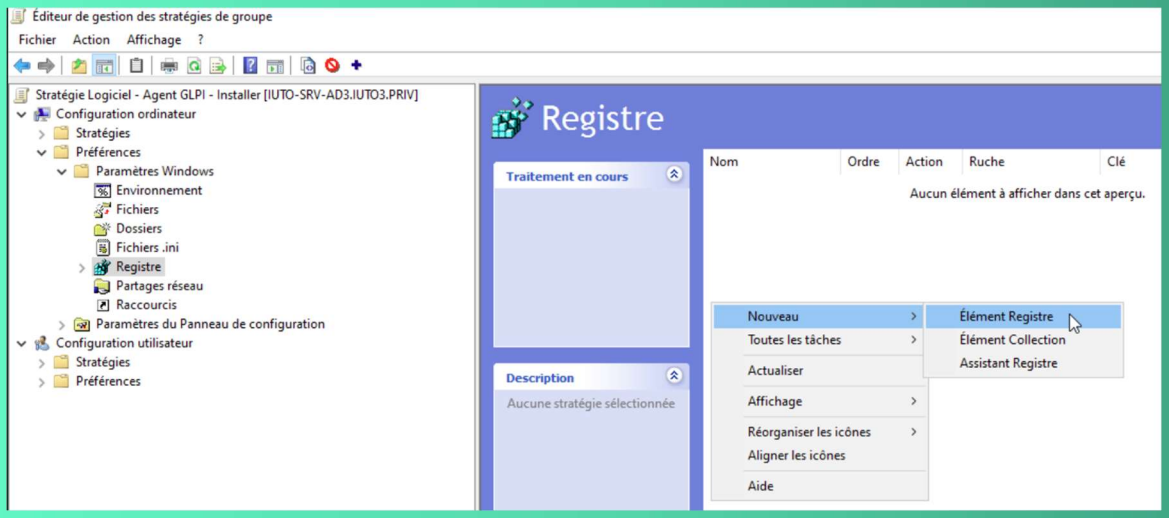
tag : pour indiquer un tag spécifique à associer à ces machines (le tag est utile pour la classification, surtout si vous avez plusieurs clients sur le même GLPI

Pour définir des valeurs de Registre par GPO, procédez de cette façon (toujours dans la même GPO, même si ce n'est pas obligatoire) :

Parcourez les paramètres de GPO de façon à atteindre cet emplacement :

Configuration ordinateur > Préférences > Paramètres Windows > Registre

Ici, effectuez un clic droit puis cliquez sur : Nouveau > Elément Registre.



Commencez par configurer la valeur "server".

Action : mettre à jour Ruche :

HKEY_LOCAL_MACHINE

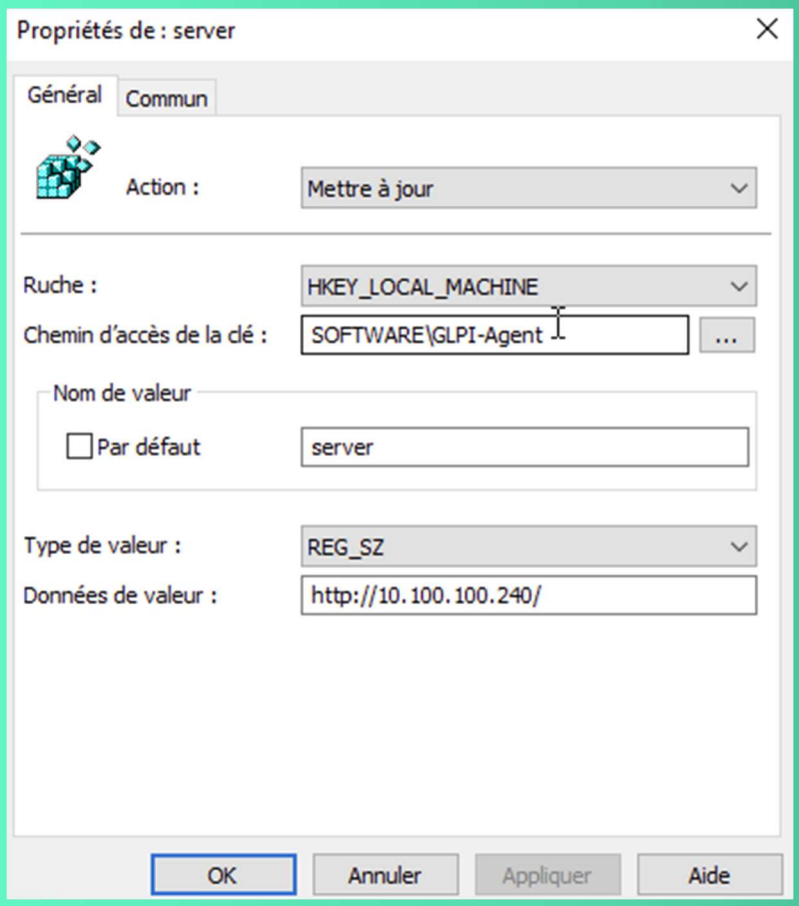
Chemin d'accès de la clé : SOFTWARE\GLPI-Agent

Nom de valeur : server

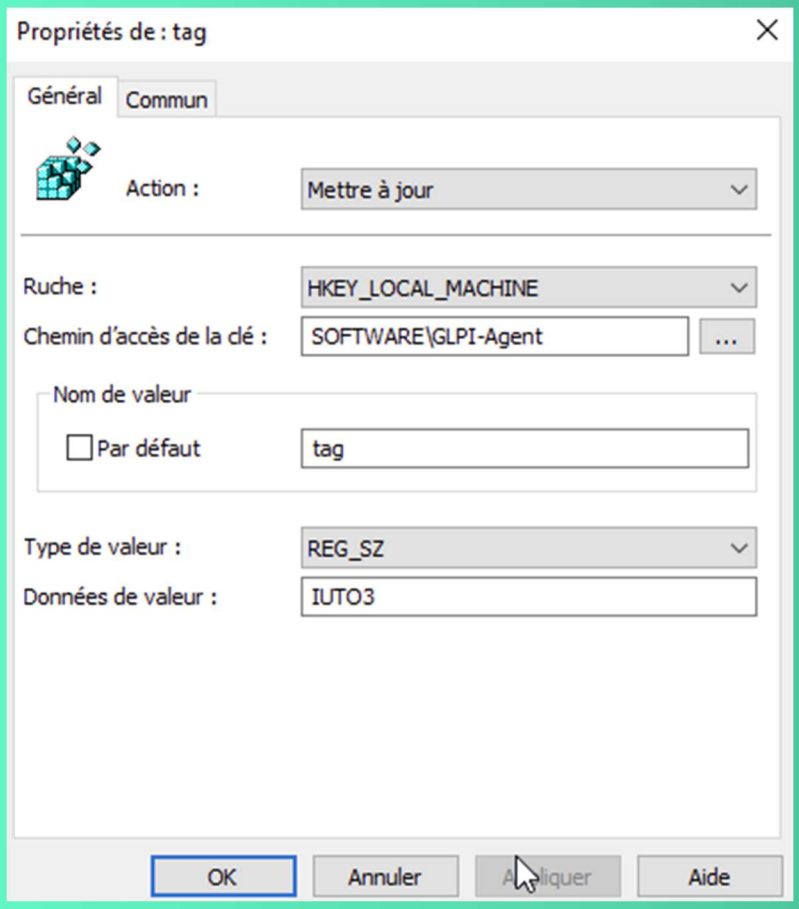
Type de valeur : REG_SZ

Données de valeur : http://10.100.100.240/

Veillez à ajuster l'URL vers votre serveur GLPI. Ce qui donne :



Répétez l'opération pour la valeur "tag" en indiquant la valeur que vous voulez pour le tag :



Ce qui donne ce résultat :

Nom	Ordre	Action	Ruche	Clé	Nom de vale
server	1	Mettre ...	HKEY_LOCAL_MAC...	SOFTWARE\GLPI-Agent	server
tag	2	Mettre ...	HKEY_LOCAL_MAC...	SOFTWARE-GLPI	tag

Voilà, la GPO est entièrement prête : l'agent GLPI sera installé et configuré ! Pour faire évoluer la configuration de vos agents GLPI par la suite, il vous suffira de modifier les valeurs de Registre ! Plutôt pratique. Sachez toutefois qu'il faut redémarrer l'agent GLPI (ou la machine, en fait) pour prendre en compte les modifications. Ici, il s'agit d'une fresh install de l'agent GLPI, donc ce sera pris en compte directement.

Déployer GLPI sur Linux :

Le script de déploiement et de configuration de GLPI se trouve sur l'AD

//IUTO-SRV-AD3/Script_Linux/install_glpi.sh

Procédure à réaliser sur la machine linux

Apt install smbclient dos2unix

Smbclient //IUTO-SRV-AD3/Script_Linux -U Administrateur -W IUTO3 -c 'get install_glpi.sh /tmp/install_glpi.sh'

Chmod +x /tmp/install_glpi.sh

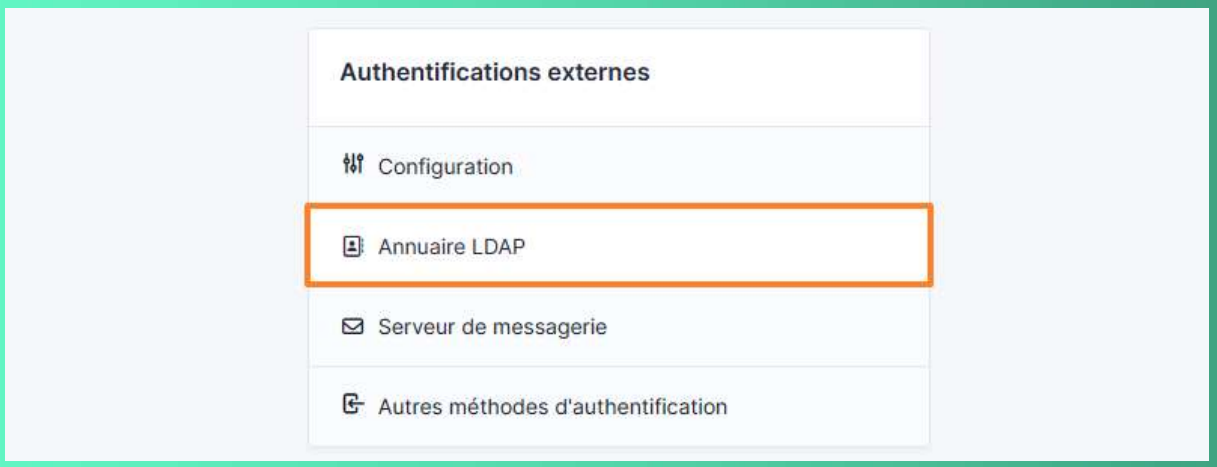
Dos2unix /tmp/install_glpi.sh

Bash /tmp/install_glpi.sh

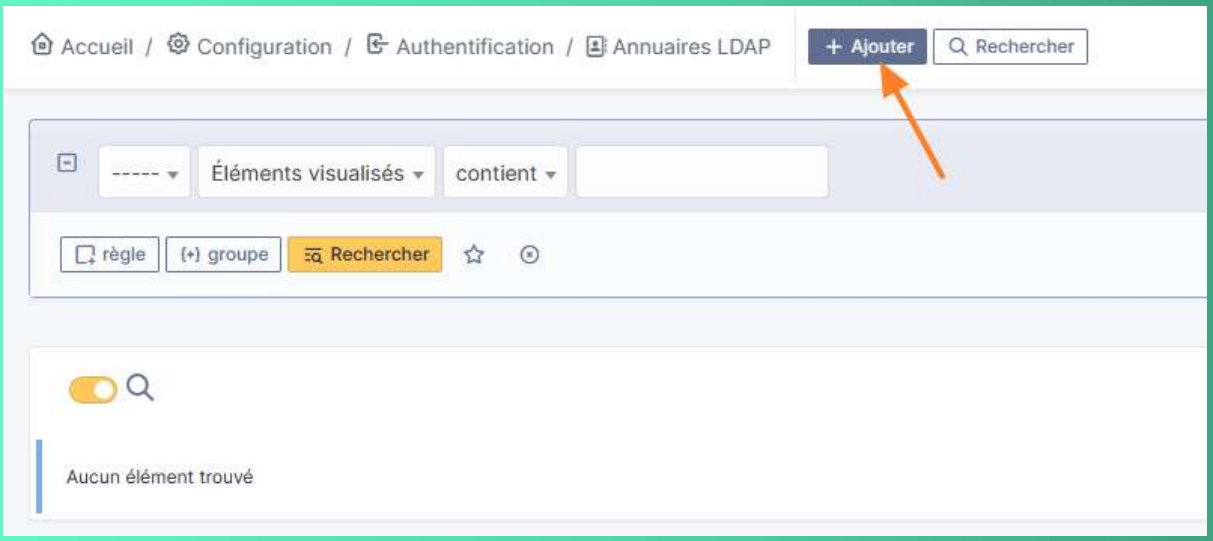
Activer l’authentification LDAP dans GLPI 10 :

Désormais, nous allons ajouter notre annuaire Active Directory à GLPI. Connectez-vous à GLPI avec un compte administrateur, puis dans le menu "Configuration", cliquez sur "Authentification".

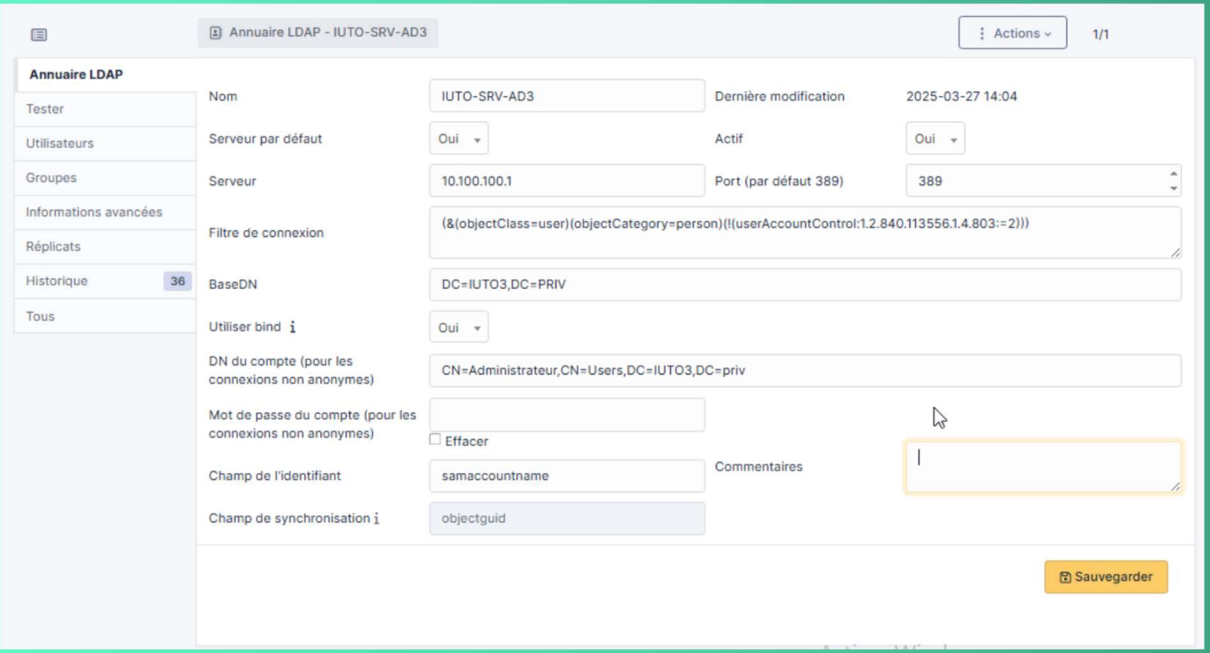
Au centre de l'écran, cliquez sur "Annuaire LDAP".



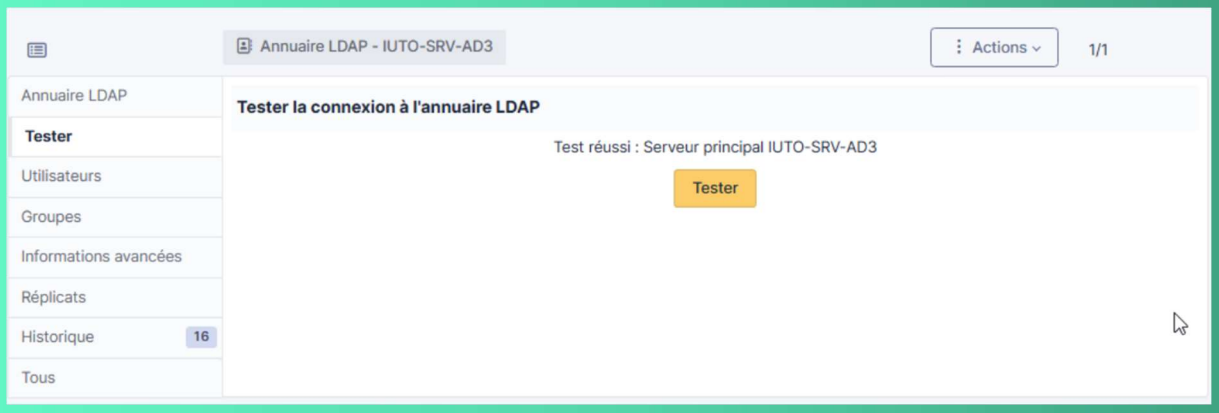
Puis, cliquez sur le bouton "Ajouter".



Quand votre configuration est prête, cliquez sur "Ajouter".



Dans la foulée, GLPI va effectuer un test de connexion LDAP et vous indiquer s'il est parvenu, ou non, à se connecter à votre annuaire. Si ce n'est pas le cas (comme moi, la première fois), cliquez sur le nom de votre annuaire, vérifiez la configuration, puis retournez dans "Tester" sur la gauche afin de lancer un nouveau test. Pour ma part, le problème venait du champ "Serveur" : j'avais mis le nom DNS du serveur à la place de l'adresse IP, mais cela ne fonctionnait pas. Pourtant, mon serveur GLPI parvient bien à résoudre le nom DNS.



Tester la connexion Active Directory :

Installation des Plugins :

IP Report :

wget https://github.com/pluginsGLPI/addressing/archive/refs/heads/master.zip

```
root@IUTO-SRV-GLPI:~# wget https://github.com/pluginsGLPI/addressing/archive/refs/heads/master.zip
--2025-01-28 08:31:19--  https://github.com/pluginsGLPI/addressing/archive/refs/heads/master.zip
Résolution de github.com (github.com)… 140.82.121.3
Connexion à github.com (github.com)|140.82.121.3|:443… connecté.
requête HTTP transmise, en attente de la réponse… 302 Found
Emplacement : https://codeload.github.com/pluginsGLPI/addressing/zip/refs/heads/master [suivant]
--2025-01-28 08:31:24--  https://codeload.github.com/pluginsGLPI/addressing/zip/refs/heads/master
Résolution de codeload.github.com (codeload.github.com)… 140.82.121.9
Connexion à codeload.github.com (codeload.github.com)|140.82.121.9|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : non indiqué [application/zip]
Sauvegarde en : « master.zip »

master.zip                      [ <=>                                   ] 141,08K  --.-KB/s    ds 0,06s

2025-01-28 08:31:24 (2,38 MB/s) - « master.zip » sauvegardé [144466]
```

mv master.zip /var/www/glpi/plugins/

cd /var/www/glpi/plugins/

unzip master.zip -d /var/www/glpi/plugins/

rm master.zip

mv addressing-master ipreport

Vérifier les permissions :

chown -R www-data:www-data /var/www/glpi/plugins/ipreport

chmod -R 755 /var/www/glpi/plugins/ipreport

Account Inventory :

Wget https://github.com/InfotelGLPI/accounts/archive/refs/heads/master.zip

mv master.zip /var/www/glpi/plugins/

cd /var/www/glpi/plugins/

unzip master.zip -d /var/www/glpi/plugins/

rm master.zip

Vérifier les permissions :

chown -R www-data:www-data /var/www/glpi/plugins/accounts-master/

chmod -R 755 /var/www/glpi/plugins/accounts-master/

Plugin Fields :

wget https://github.com/pluginsGLPI/fields/archive/refs/heads/main.zip

mv main.zip /var/www/glpi/plugins/

cd /var/www/glpi/plugins/

unzip main.zip -d /var/www/glpi/plugins/

mv /var/www/glpi/plugins/fields-main /var/www/glpi/plugins/fields

rm main.zip

Vérifier les permissions :

chown -R www-data:www-data /var/www/glpi/plugins/fie

chmod -R 755 /var/www/glpi/plugins/fields

Activer le plugin dans GLPI :

- Connectez-vous à l'interface web de GLPI en tant qu'administrateur.
- Allez dans **Configuration** > **Plugins**.
- Le plugin **Fields** devrait apparaître dans la liste.
- Cliquez sur **Installer**, puis sur **Activer**.

Tablette :

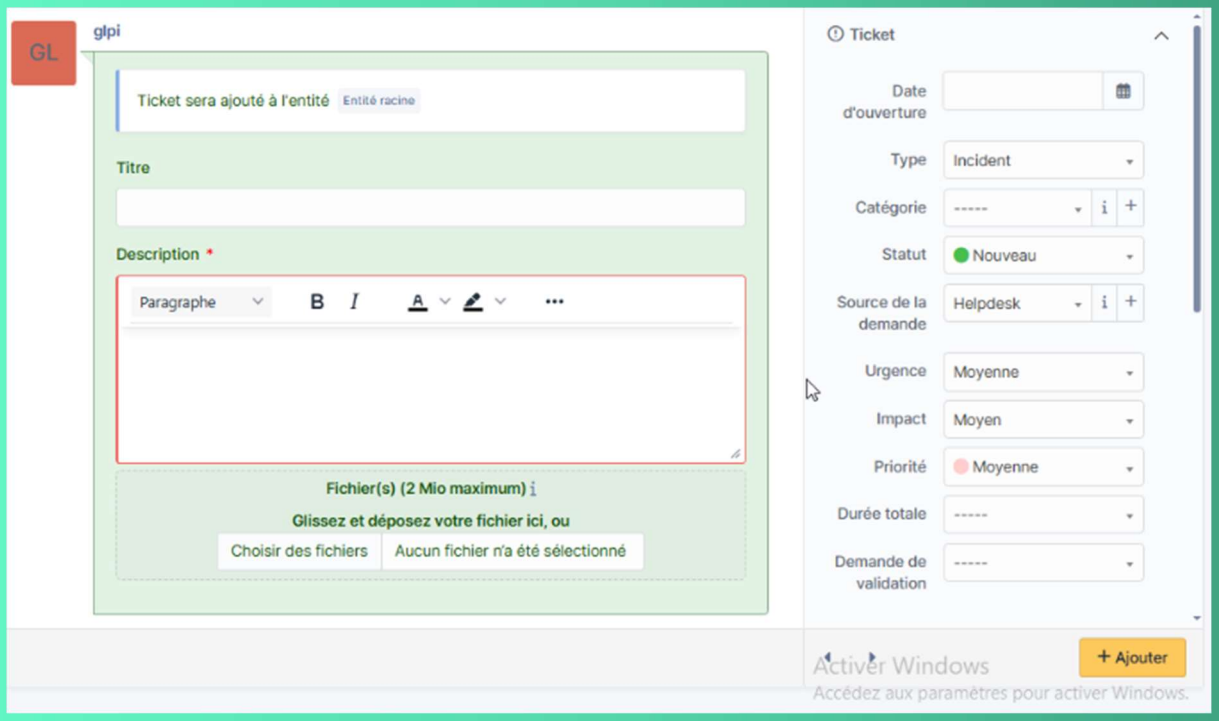
Advanced settings < Open list servers < add server

http://172.20.134.13/

glpi

Azerty45

Comment créer un ticket :



Titre : Titre du ticket

Description : Description du problème / de la demande

Date d'ouverture : Date à laquelle le ticket a été ouvert

Type : Incident / Demande

Catégorie : Catégorie du problème

Statut : Nouveau / En cours (Attribué) / En cours (Planfié) / En attente / Résolu / Clos

Source de la demande : Comment a été fait le ticket

Urgence : Très haute / Haute / Moyenne / Basse / Très basse

Impact : Très haut / Haut / Moyen / Bas / Très bas

Priorité : Majeure / Très haute / Haute / Moyenne / Basse / Très basse

Durée totale : Tamps passé sur le ticket

Demande de validation : Si une validation est nécessaire pour cloturer le ticket

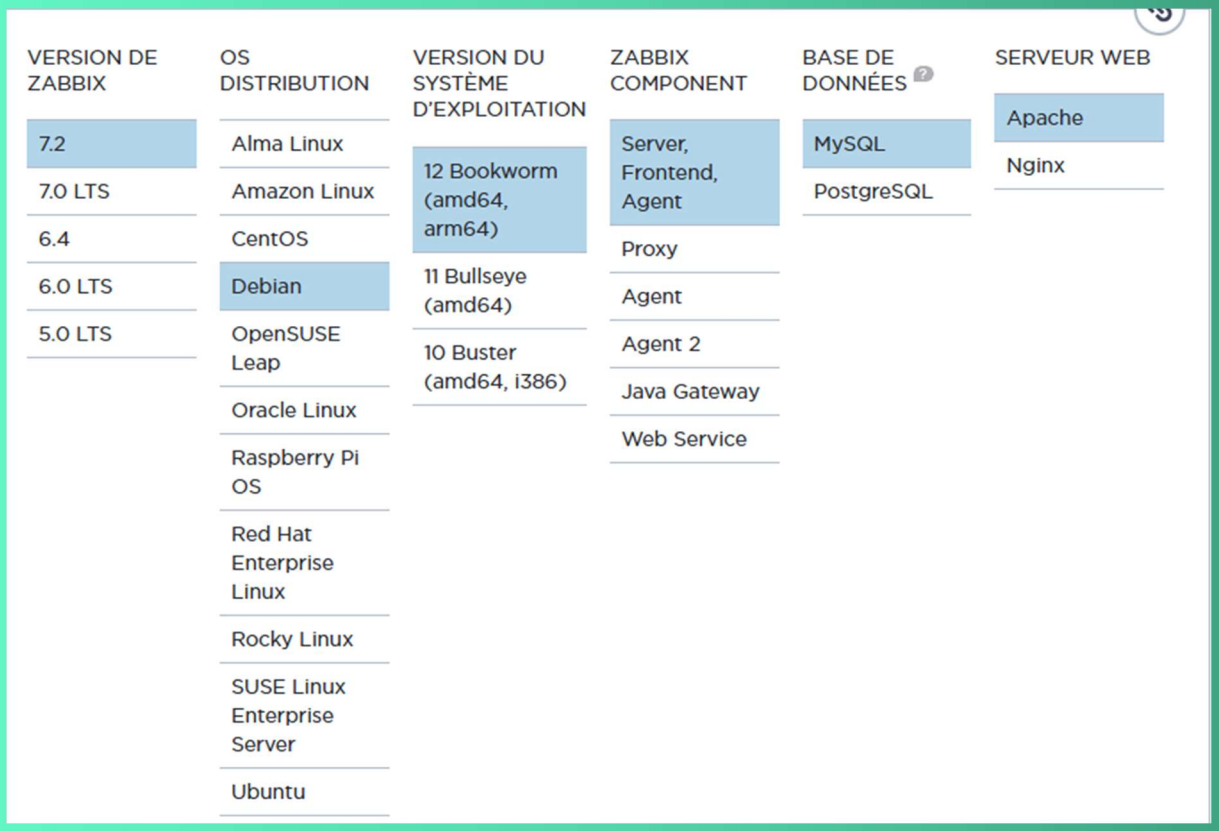
Demandeur : L'utilisateur qui a ouvert le ticket

Attribué à : Le technicien / Groupe en charge de la résolution du ticket

INSTALLATION DE ZABBIX

La documentation se trouve en partie sur le site de Zabbix : https://www.zabbix.com/fr/download

Choisir la plateforme



Installer le depot de Zabbix :

wget https://repo.zabbix.com/zabbix/7.2/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.2+debian12_all.deb

dpkg -i zabbix-release_latest_7.2+debian12_all.deb

apt update && apt upgrade

Installer Zabbix server, frontend, agent

apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent

Mise en place du dépôt MariaDB :

apt install apt-transport-https curl

mkdir -p /etc/apt/keyrings

curl -o /etc/apt/keyrings/mariadb-keyring.pgp 'https://mariadb.org/mariadb_release_signing_key.pgp'

Copier ceci dans le fichier /etc/apt/sources.list.d/mariadb.sources

MariaDB 11.4 repository list - created 2024-12-12 08:51 UTC

https://mariadb.org/download/

X-Repolib-Name: MariaDB

Types: deb

deb.mariadb.org is a dynamic mirror if your preferred mirror goes offline. See https://mariadb.org/mirrorbits/ for details.

URIs: https://deb.mariadb.org/11.4/debian

URIs: https://mirrors.ircam.fr/pub/mariadb/repo/11.4/debian

Suites: bookworm

Components: main

Signed-By: /etc/apt/keyrings/mariadb-keyring.pgp

Installer mariadb avec les commandes

Apt install && apt upgrade -y

Apt install mariadb-server

Créer la base de données :

Mysql -uroot -p

create database zabbix character set utf8mb4 collate utf8mb4_bin;

create user gt@localhost identified by 'password';

grant all privileges on zabbix.* to gt@localhost;

set global log_bin_trust_function_creators = 1;

quit;

Importer le schéma de zabbix server :

zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -gt -p zabbix

Desactiver log_bin_trust_function_creators apres avoir importer le schéma :

mysql -root -p

set global log_bin_trust_function_creators =0 ;

quit ;

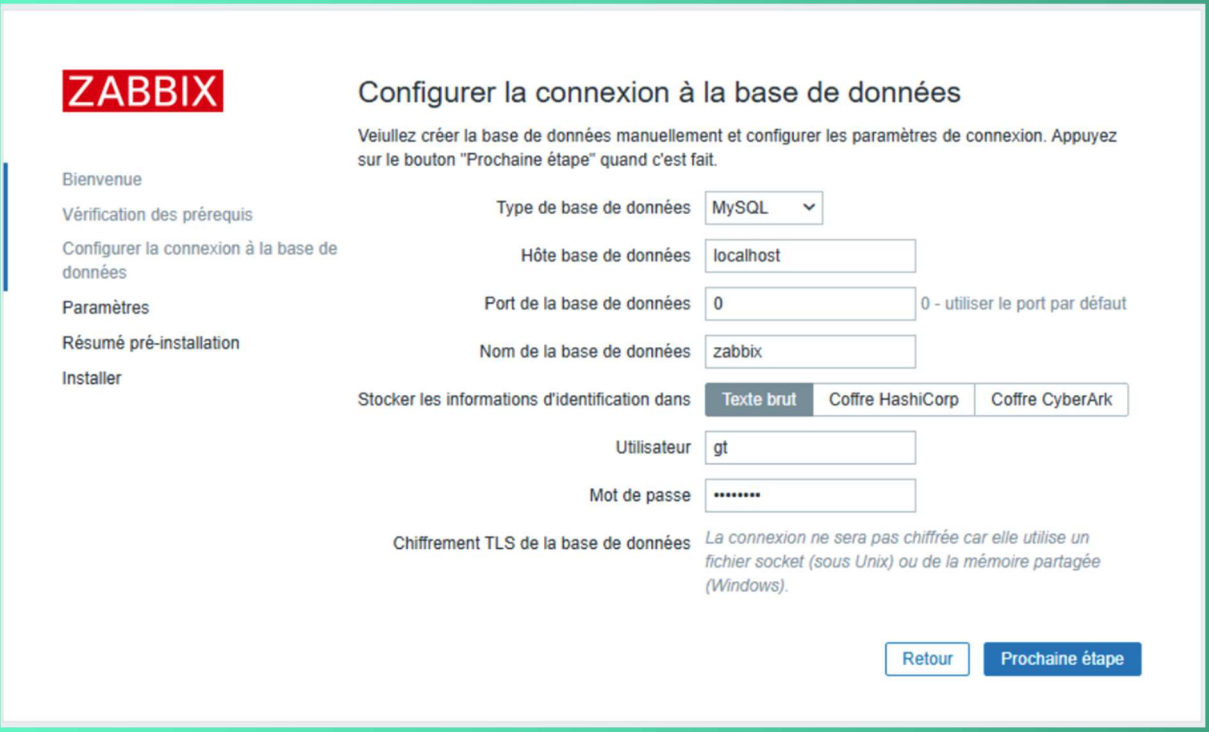
Configurer la base de données pour Zabbix server :

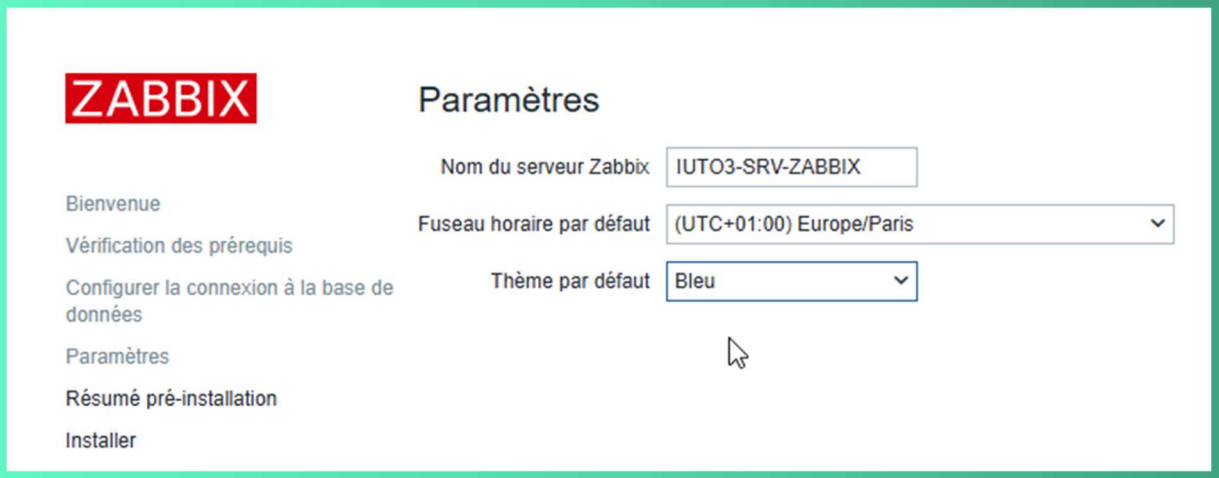
Modifier me fichier /etc/zabbix/zabbix_server.conf

DBPassword=password

Démarrez les processus serveur et agent Zabbix :

Systemctl restart zabbix-server zabbix-agent apache2





Pour se connecter, le Username est Admin et le password est zabbix

Déploiement de Zabbix sur Linux

Le script se trouve sur l'AD au chemin :

//IUTO-SRV-AD3/Script_Linux/install_zabbix.sh

Procédure à réaliser sur la machine linux

Apt install smbclient dos2unix

Smbclient //IUTO-SRV-AD3/Script_Linux -U Administrateur -W IUTO3 'get install_zabbix.sh /tmp/install_zabbix.sh'

Chmod +x /tmp/install_zabbix.sh

Dos2unix /tmp/install_zabbix.sh

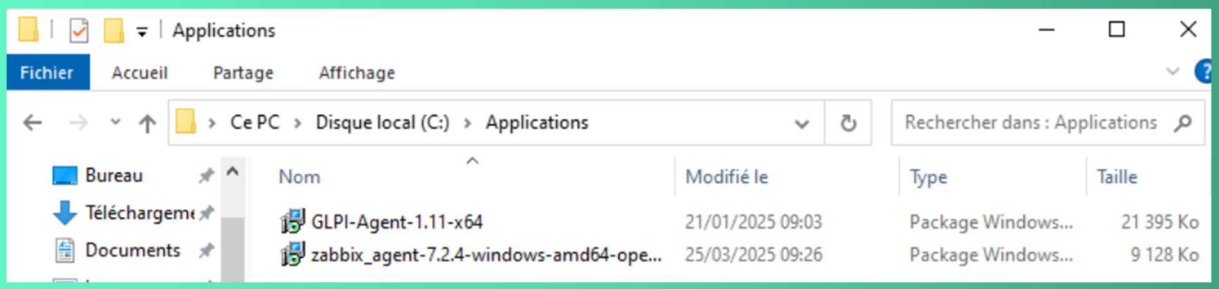
Bash /tmp/install_zabbix.sh

DÉPLOIEMENT DE ZABBIX VIA GPO

Télécharger et partager le package MSI de l'agent ZABBIX :

Agent zabbix 7.2.4 installé : https://www.zabbix.com/fr/download_agents

Dans mon cas, l'agent ZABBIX sera stocké dans "C:\Applications" du serveur "IUTO-SRV-AD3.IUTO3.priv".



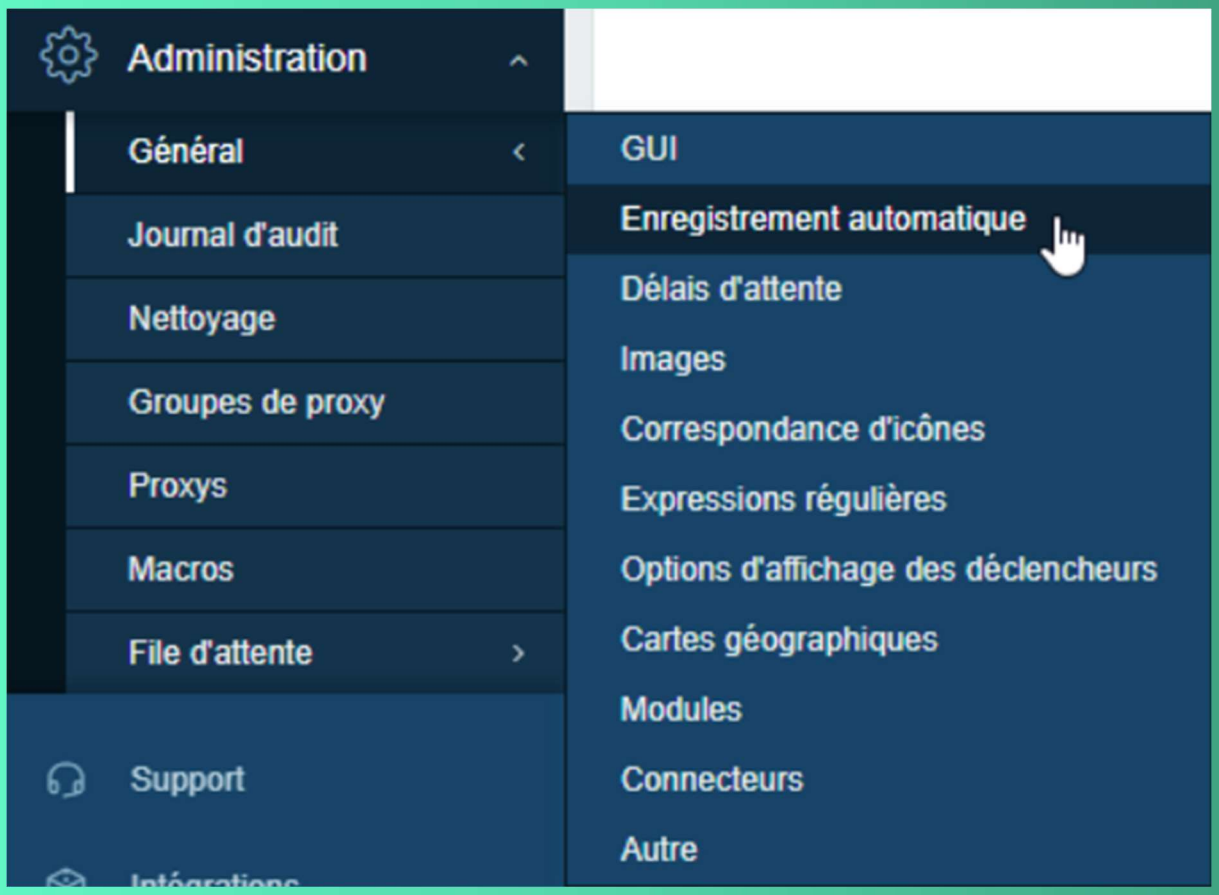
Ce répertoire est partagé en tant que "Applications$" et les permissions de partage sont définies comme suit :

Groupe "Ordinateurs du domaine" en lecture seule

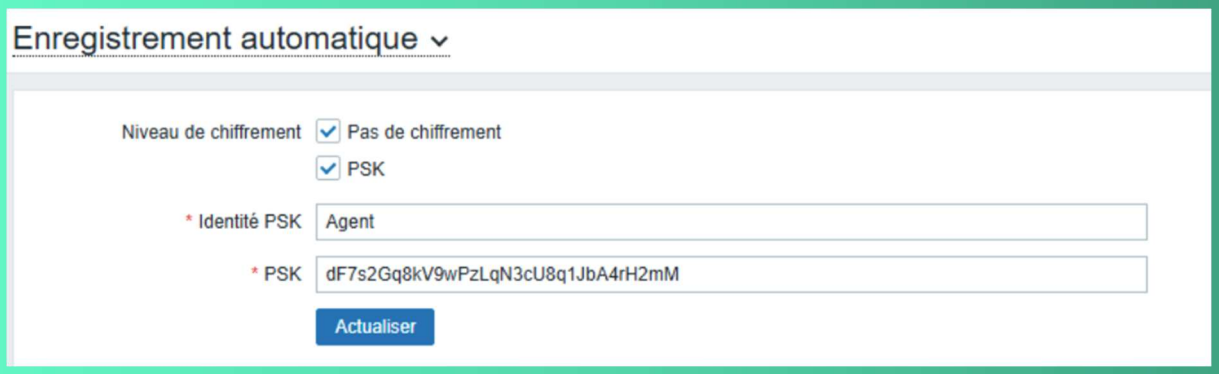
Groupe "Admins du domaine" en contrôle total

Avant de faire le script, on modifie les opiotns de Zabbix, car nous allons mettre en place le chiffrement par PSK

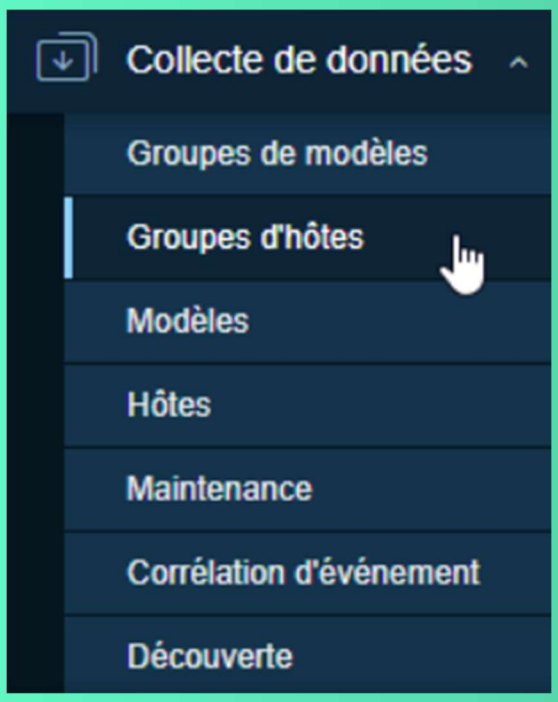
Dans Administration et Général :



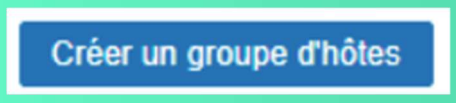
Pour générer un PSK sur linux : openssl rand -hex 32



On ajoute ensuite un groupe pour les serveurs windows

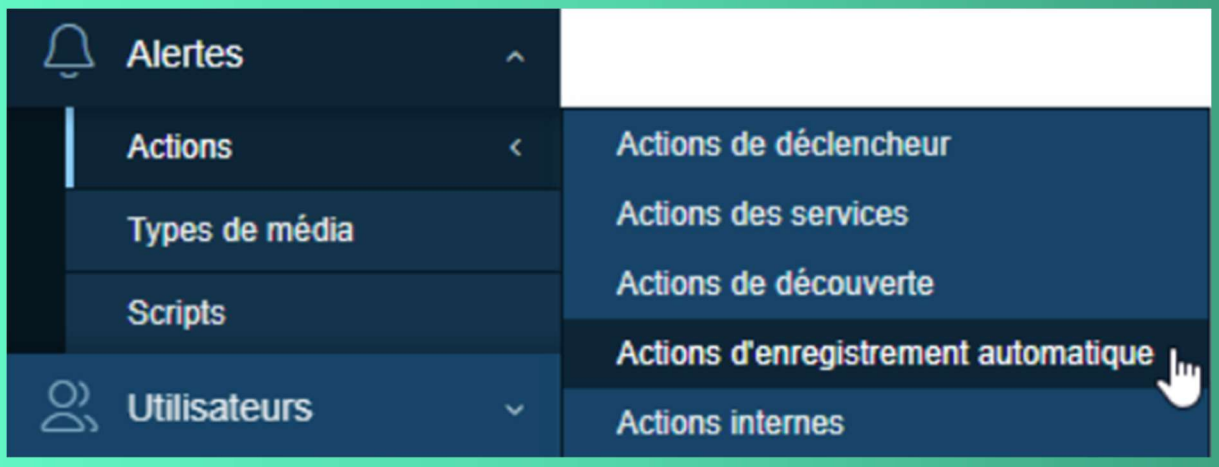


En haut à droite, on clique sur « Créer un groupe d'hôtes »

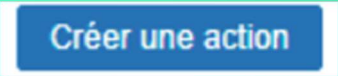


On active ensuite l'auto registration

On se rend dans « Alertes » puis « Actions »

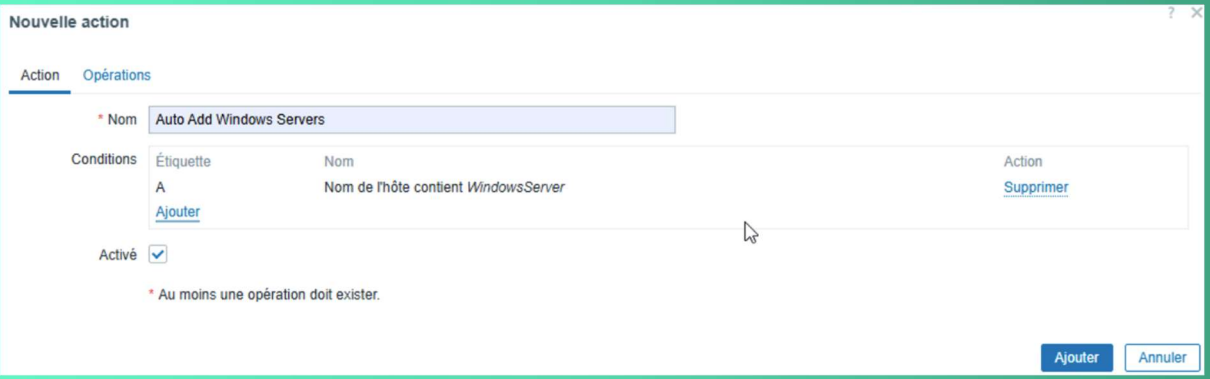


En haut à droite, on clique

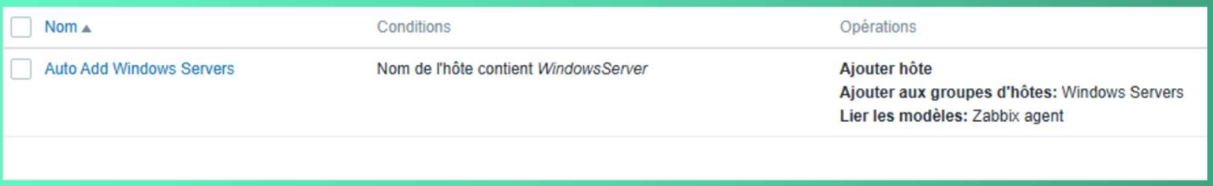


On définit un nom puis on clique sur "Ajouter".

On définit la métadonnée que l'on a mis dans le script.

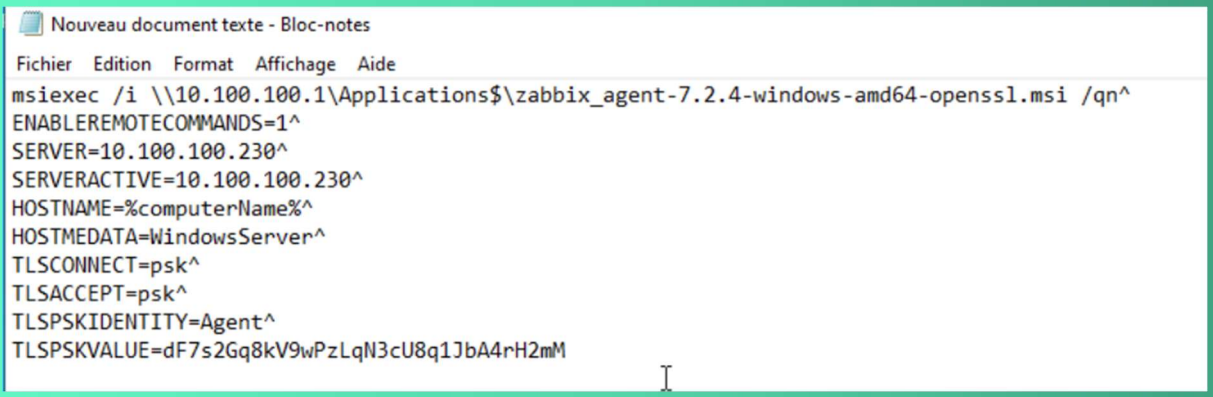


Ensuite, dans la catégorie "Opérations", on ajoute l'hôte, on lui définit un groupe et un modèle.



Script d'installation

On crée ce script dans le dossier Zabbix du partage



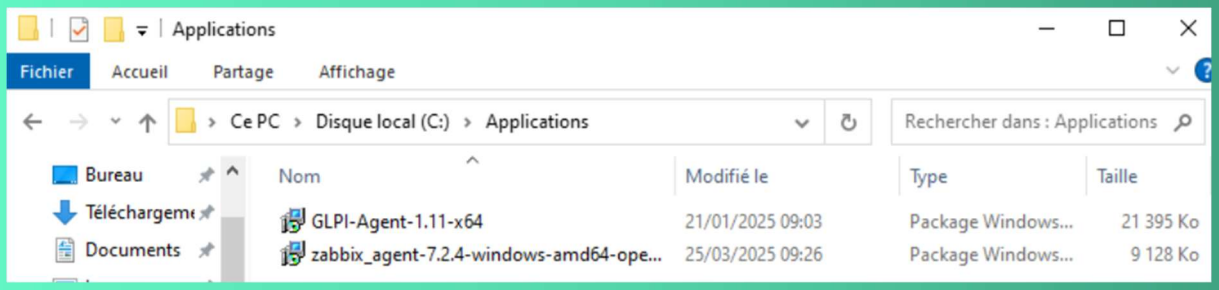
Création de la GPO

DÉPLOIEMENT DE ZABBIX VIA GPO

Télécharger et partager le package MSI de l'agent ZABBIX :

Agent zabbix 7.2.4 installé : https://www.zabbix.com/fr/download_agents

Dans mon cas, l'agent ZABBIX sera stocké dans "C:\Applications" du serveur "IUTO-SRV-AD3.IUTO3.priv".



Ce répertoire est partagé en tant que "Applications$" et les permissions de partage sont définies comme suit :

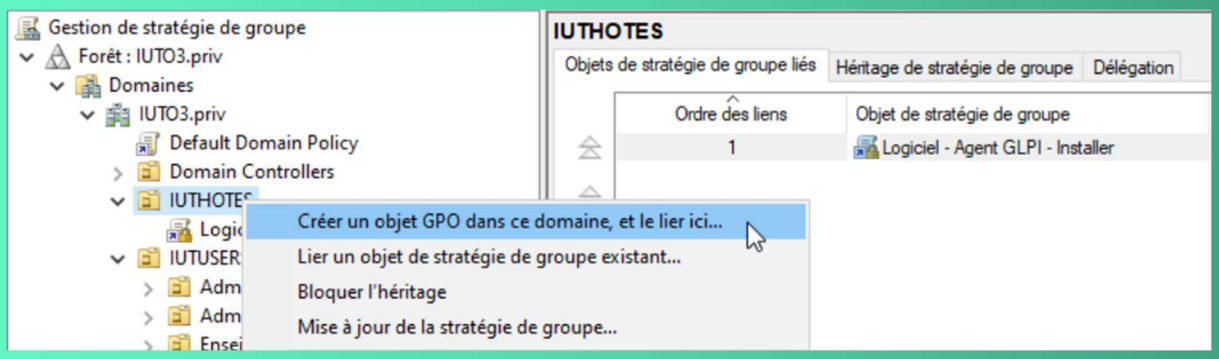
Groupe "Ordinateurs du domaine" en lecture seule

Groupe "Admins du domaine" en contrôle total

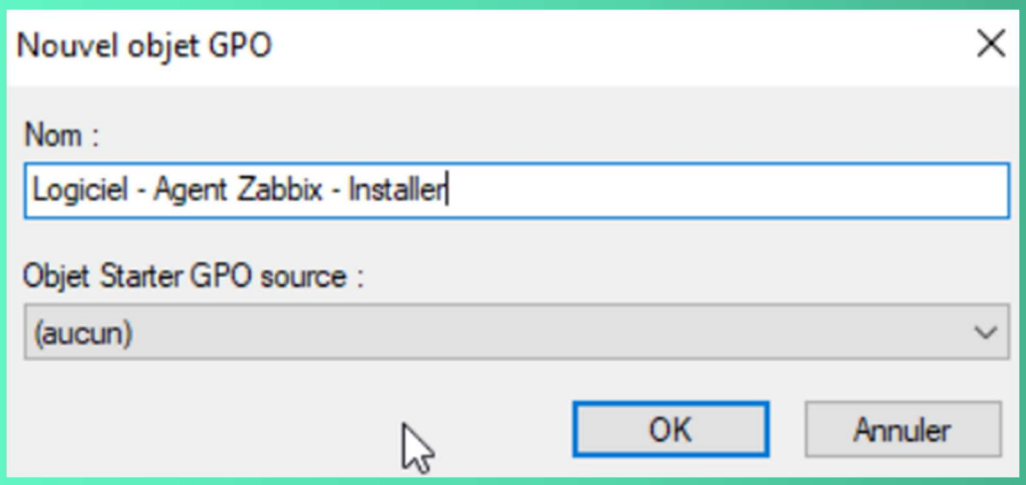
Installer l'agent GLPI par ZABBIX :

Passons à la création de la stratégie de groupe pour déployer l'agent ZABBIX. Ouvrez la console "Gestion de stratégie de groupe" et créez une nouvelle GPO.

En ce qui me concerne, la GPO s'appelle "Logiciel - Agent ZABBIX - Installer" et elle est liée à l'OU "PC" qui contient mes postes de travail Windows. Attention, si vous liez la GPO à la racine de votre domaine Active Directory, l'agent ZABBIX sera déployé sur toutes les machines (postes de travail et serveurs).



Entrer le nom de la GPO



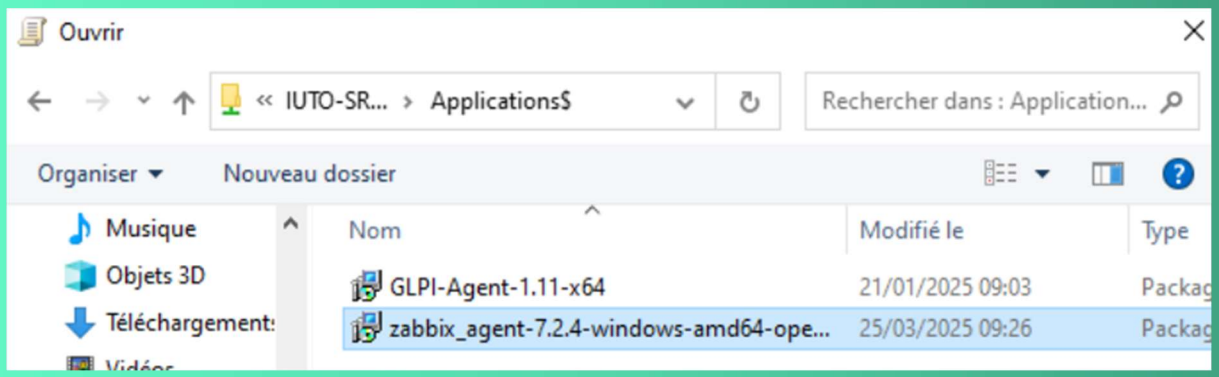
Une fois la GPO créée, vous allez devoir l'éditer via un clic droit sur son nom puis "Modifier". Parcourez les paramètres de cette façon :

Configuration ordinateur > Stratégies > Paramètres du logiciel > Installation de logiciel

Ici, effectuez un clic droit puis : Nouveau > Package. Une fenêtre va s'ouvrir afin de vous permettre de sélectionner le package MSI à déployer. Vous devez préciser le chemin réseau (chemin UNC) vers le package MSI.

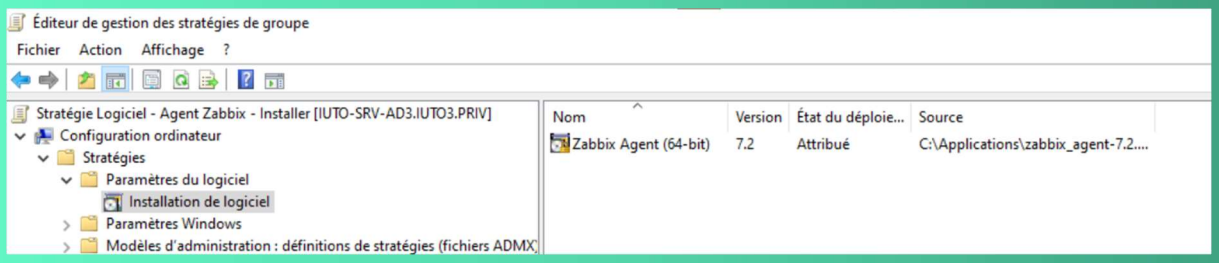
Pour ma part, cela donne le chemin suivant :

\\IUTO-SRV-AD3.IUTO3.priv\Applications$\zabbix_agent-7.2.4-windows-amd64-openssl



A la question "Sélectionnez le type de déploiement", choisissez "Attribué" et poursuivez.

Voilà, l'agent ZABBIX est prêt à être déployé par GPO :



Le problème, c'est que l'agent ZABBIX sera déployé sans aucune configuration. De ce fait, il ne pourra pas se synchroniser sur notre serveur ZABBIX.

Configurer l'agent ZABBIX avec le Registre Windows :

Pour répondre à cette problématique, nous allons configurer l'agent GLPI par GPO en jouant directement sur les valeurs situées dans la clé de Registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\GLPI-Agent

Effectivement, l'agent GLPI stocke sa configuration dans le Registre Windows, ce qui permet de la modifier facilement.

Ainsi, nous allons configurer deux valeurs :

server : pour indiquer l'URL du serveur GLPI (vers une page spécifique)

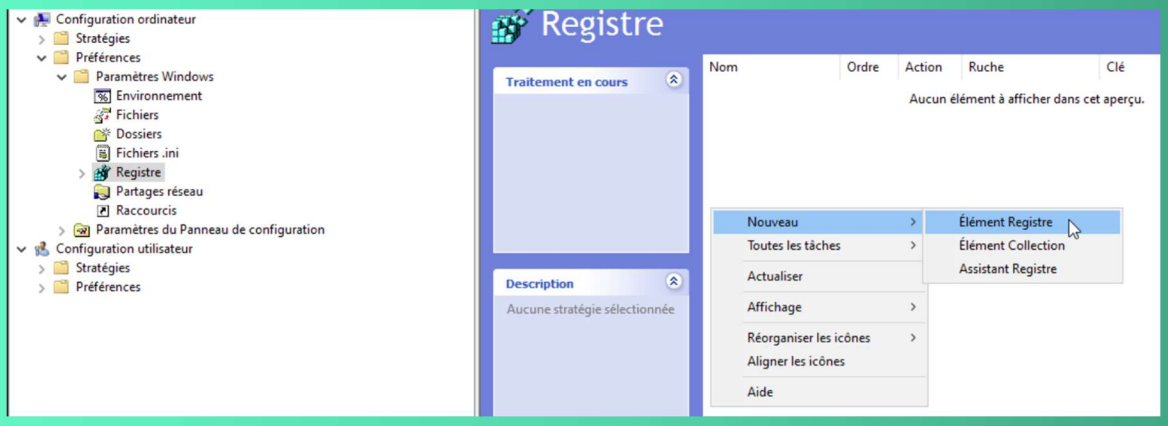
tag : pour indiquer un tag spécifique à associer à ces machines (le tag est utile pour la classification, surtout si vous avez plusieurs clients sur le même GLPI

Pour définir des valeurs de Registre par GPO, procédez de cette façon (toujours dans la même GPO, même si ce n'est pas obligatoire) :

Parcourez les paramètres de GPO de façon à atteindre cet emplacement :

Configuration ordinateur > Préférences > Paramètres Windows > Registre

Ici, effectuez un clic droit puis cliquez sur : Nouveau > Elément Registre.



Configurer la clé 1 : Adresse du serveur Zabbix :

Action : Mettre à jour

Ruche : HKEY_LOCAL_MACHINE

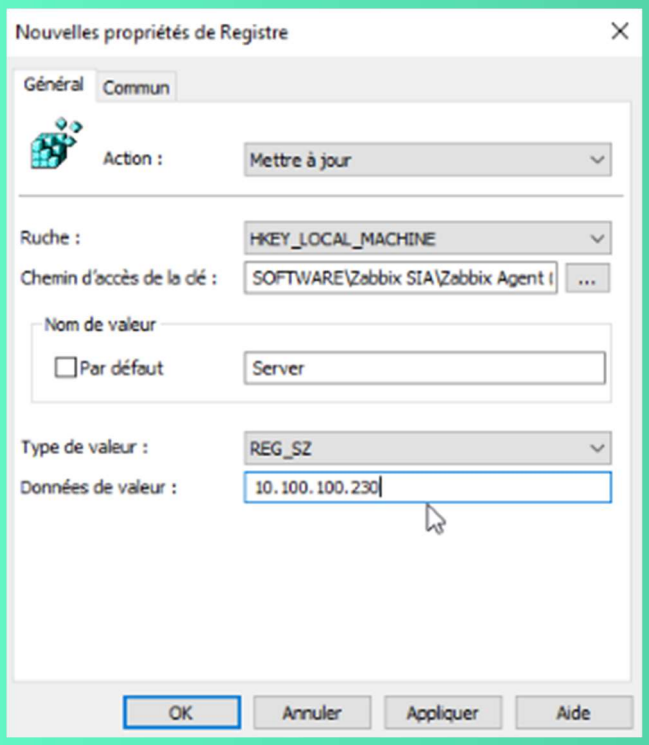
Chemin d'accès de la clé : SOFTWARE\Zabbix SIA\Zabbix Agent 2 (64-bit)

Nom de valeur : Server

Type de valeur : REG_SZ (déjà sélectionné)

Données de valeur : 10.100.100.230

Clique sur **OK**.



Configurer la clé 2 : Mode actif :

Action : Mettre à jour

Ruche : HKEY_LOCAL_MACHINE

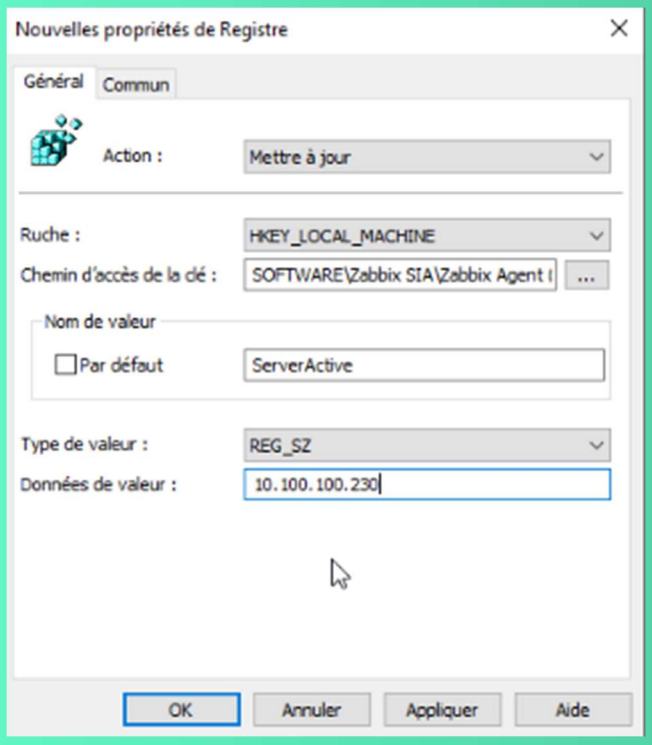
Chemin d'accès de la clé : SOFTWARE\Zabbix SIA\Zabbix Agent 2 (64-bit)

Nom de valeur : ServerActive

Type de valeur : REG_SZ (déjà sélectionné)

Données de valeur : 10.100.100.230

Clique sur **OK**.



<u>Configurer la clé 3 : Nom de l'hôte basé sur l'ordinateur :</u>

Action : Mettre à jour

Ruche : HKEY_LOCAL_MACHINE

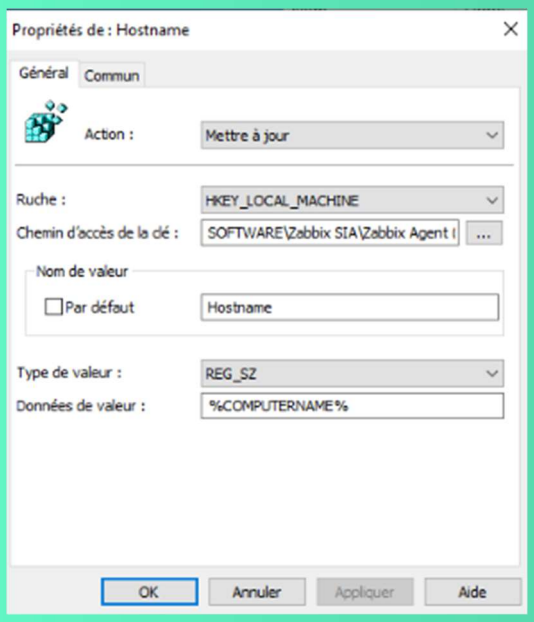
Chemin d'accès de la clé : SOFTWARE\Zabbix SIA\Zabbix Agent 2 (64-bit)

Nom de valeur : Hostname

Type de valeur : REG_SZ (déjà sélectionné)

Données de valeur : %COMPUTERNAME%

Clique sur **OK**.

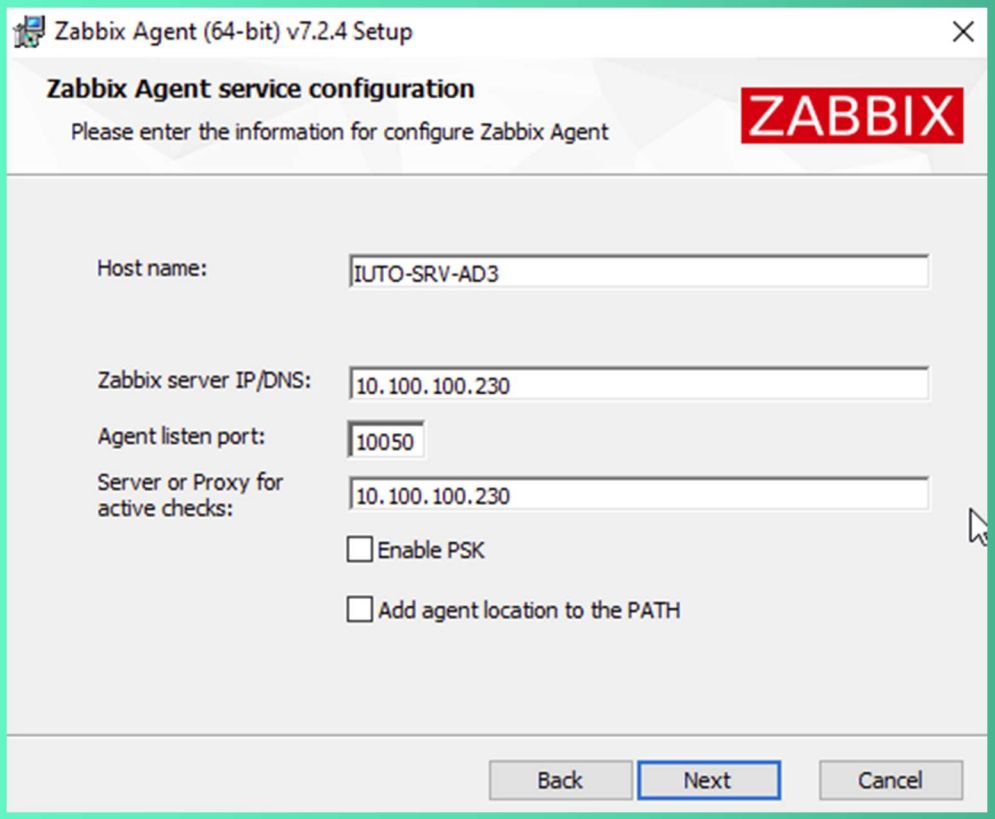


Installation d’un agent manuellement :

Va sur la page officielle :

👉 https://www.zabbix.com/download_agents

Executer le .msi



Serveur or proxy 10.100.100.230

INSTALLATION DE OWNCLOUD

Mise à jour du système :

apt update && apt upgrade -y

Installation des dépôts de PHP8.1 :

apt install -y apt-transport-https lsb-release ca-certificates curl gnupg2

curl -fsSL https://packages.sury.org/php/apt.gpg | gpg --dearmor -o /etc/apt/keyrings/sury.gpg

echo "deb [signed-by=/etc/apt/keyrings/sury.gpg] https://packages.sury.org/php/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/php.list

apt update

apt upgrade

Installation des paquets nécessaires :

apt install -y php7.4 php7.4-cli php7.4-common php7.4-mysql php7.4-xml php7.4-mbstring php7.4-curl php7.4-zip php7.4-gd php7.4-intl php7.4-bcmath php7.4-imap php7.4-opcache php7.4-readline php7.4-ldap

Configuration de MariaDB :

Mysql -u root

CREATE DATABASE owncloud;

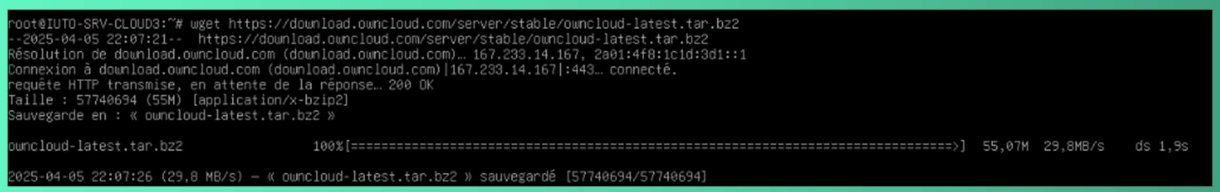
CREATE USER 'owncloduser'@'localhost' IDENTIFIED BY 'Azerty45';

GRANT ALL PRIVILEGES ON owncloud.* TO 'owncloduser'@'192.168.3.100' IDENTIFIED BY 'Azerty45';

FLUSH PRIVILEGES;EXIT;

Télécharger OwnCloud :

wget https://download.owncloud.com/server/stable/owncloud-latest.tar.bz2



Extraire et déplacer OwnCloud :

tar -xjf owncloud-latest.tar.bz2

mv owncloud /var/www/owncloud

chown -R www-data:www-data /var/www/owncloud

chmod -R 755 /var/www/owncloud

Créer un VirtualHost Apache :

nano /etc/apache2/sites-available/owncloud.conf

Voici le contenu :

```
<VirtualHost *:80>
    ServerAdmin admin@localhost
    DocumentRoot /var/www/owncloud
    ServerName 192.168.3.100

    <Directory /var/www/owncloud/>
        Options +FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/owncloud_error.log
    CustomLog ${APACHE_LOG_DIR}/owncloud_access.log combined
</VirtualHost>
```

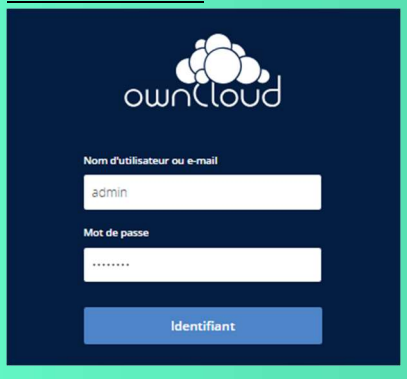
Activer la conf :

a2ensite owncloud.conf

a2enmod rewrite headers env dir mime

systemctl reload apache2

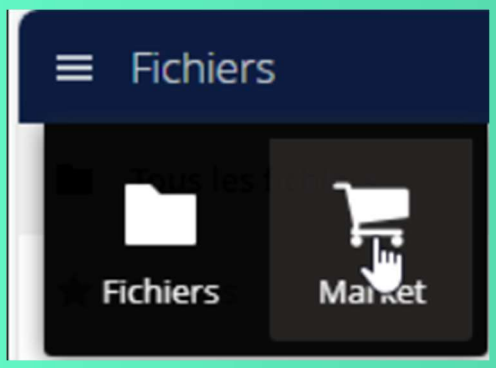
Accès au site :



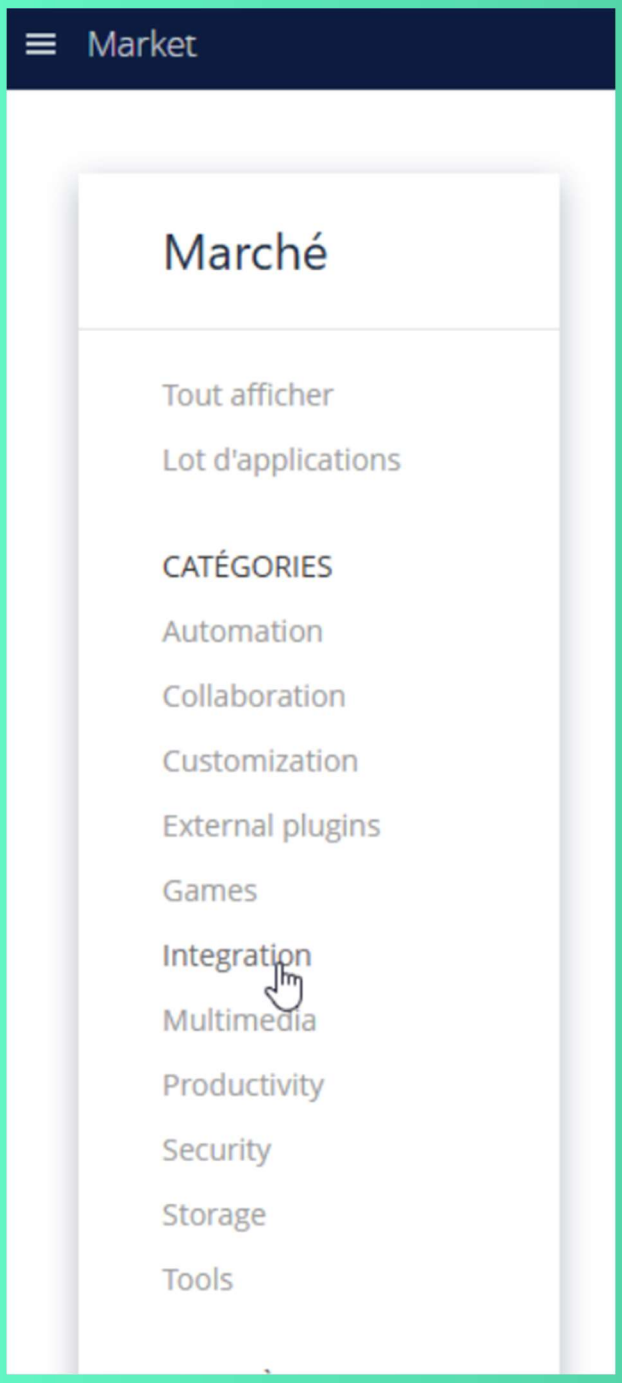
Intégration LDAP :

Pour réaliser l'intégration LDAP, il faut installer un module

Cliquer sur les 3 barres en haut à gauche et sélectionner Market



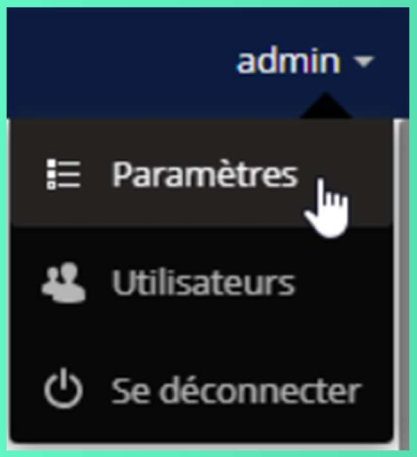
Dans le menu, sélectionner Intégration



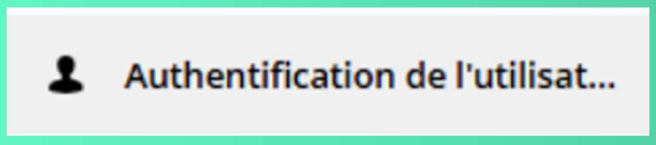
Selectionner LDAP integration et installer

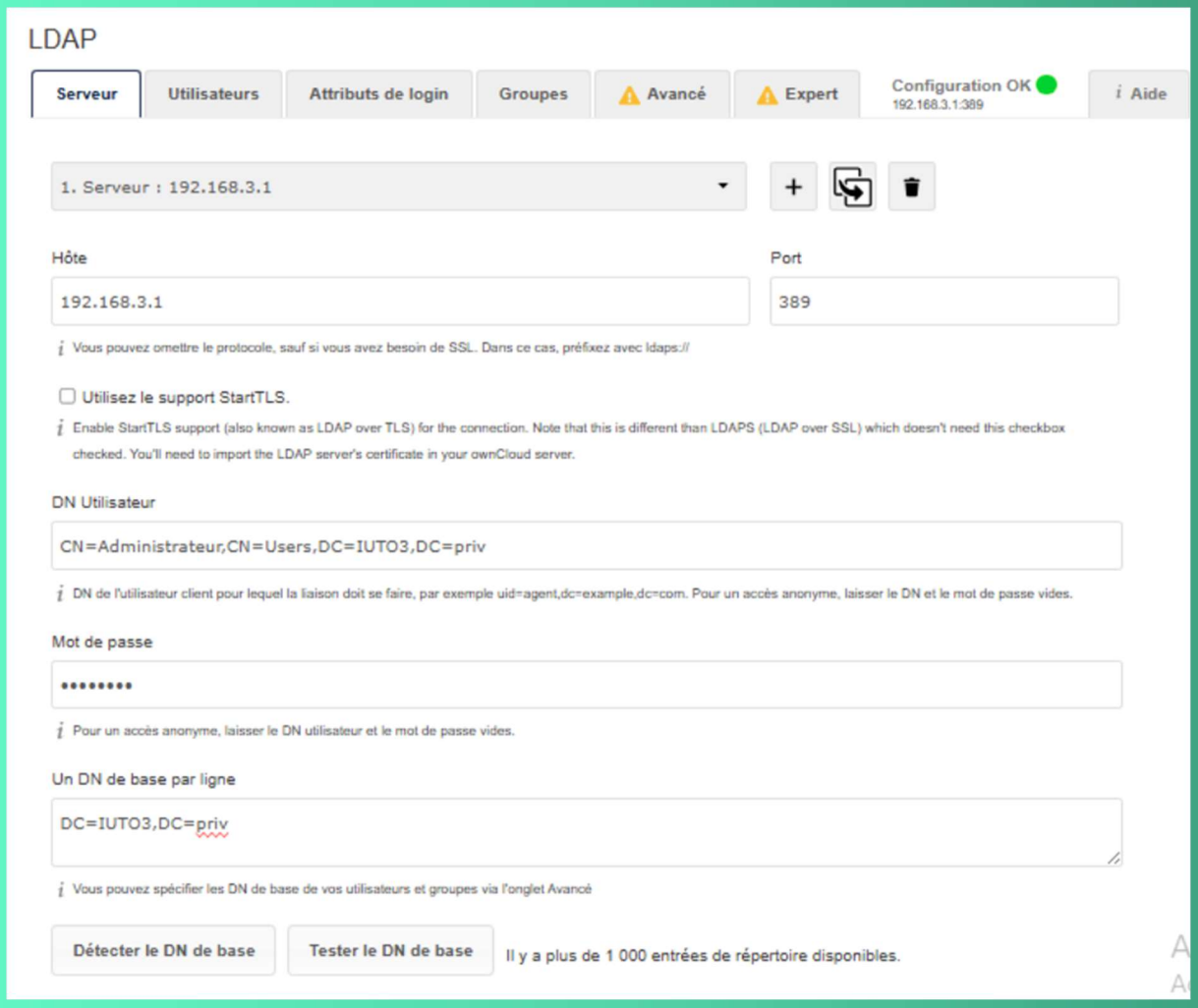
Configurer l'authentification LDAP :

Cliquer sur son profil en haut à droite puis sur Paramètres



Ensuite, cliquer sur Authentification de l'utilisateur




LDAP
Serveur
Utilisateurs
Attributs de login
Groupes
Avancé
Expert
Configuration OK
192.168.3.1:389
Aide
1. Serveur : 192.168.3.1
Hôte
192.168.3.1
Port
389
Vous pouvez omettre le protocole, sauf si vous avez besoin de SSL. Dans ce cas, préfixez avec ldaps://
Utilisez le support StartTLS.
Enable StartTLS support (also known as LDAP over TLS) for the connection. Note that this is different than LDAPS (LDAP over SSL) which doesn't need this checkbox checked. You'll need to import the LDAP server's certificate in your ownCloud server.
DN Utilisateur
CN=Administrateur,CN=Users,DC=IUTO3,DC=priv
DN de l'utilisateur client pour lequel la liaison doit se faire, par exemple uid=agent,dc=example,dc=com. Pour un accès anonyme, laisser le DN et le mot de passe vides.
Mot de passe
••••••••
Pour un accès anonyme, laisser le DN utilisateur et le mot de passe vides.
Un DN de base par ligne
DC=IUTO3,DC=priv
Vous pouvez spécifier les DN de base de vos utilisateurs et groupes via l'onglet Avancé
Détecter le DN de base
Tester le DN de base
Il y a plus de 1 000 entrées de répertoire disponibles.

INSTALLATION DU SERVEUR MAIL

PREREQUIS

Sur l'AD :

Ajouter un enregistrement A dans le DNS

Nom : IUTO-SRV-MAIL3

Adresse IP : 10.100.100.200

✅ Coche **Créer un pointeur (enregistrement PTR)**

Ajouter un enregistrement MX dans le DNS

Nom : (laisse vide pour s'appliquer à IUTO3.priv)

Nom de l'hôte de courrier : IUTO-SRV-MAIL3.IUTO3.priv.

Priorité : 10

Vérifications depuis le serveur de mail :

Apt install dnsutils

nslookup IUTO-SRV-MAIL3.IUTO3.priv

nslookup -type=MX IUTO3.priv

Enable default official Debian/Ubuntu apt repositories :

iRedMail needs official Debian/Ubuntu apt repositories, please enable them in /etc/apt/sources.list.

Install packages required by iRedMail installer:

Apt install -y gzip dialog

Download the latest release of iRedMail :

Visit Download page to get the latest stable release of iRedMail.

Wget https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.3.tar.gz

Tar zxf 1.7.3.tar.gz

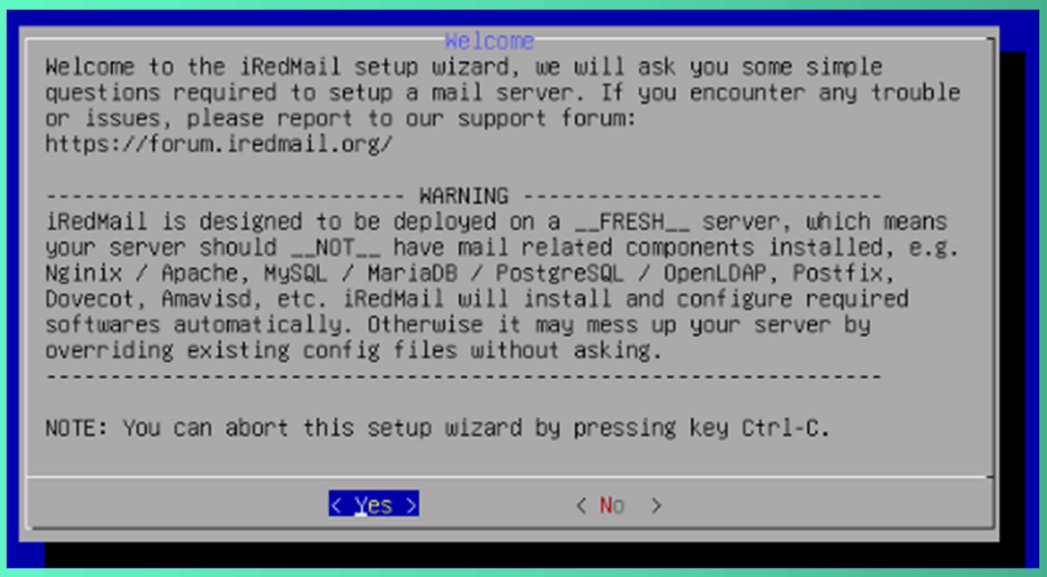
Start iRedMail installer

Cd iRedMail-1.7.3

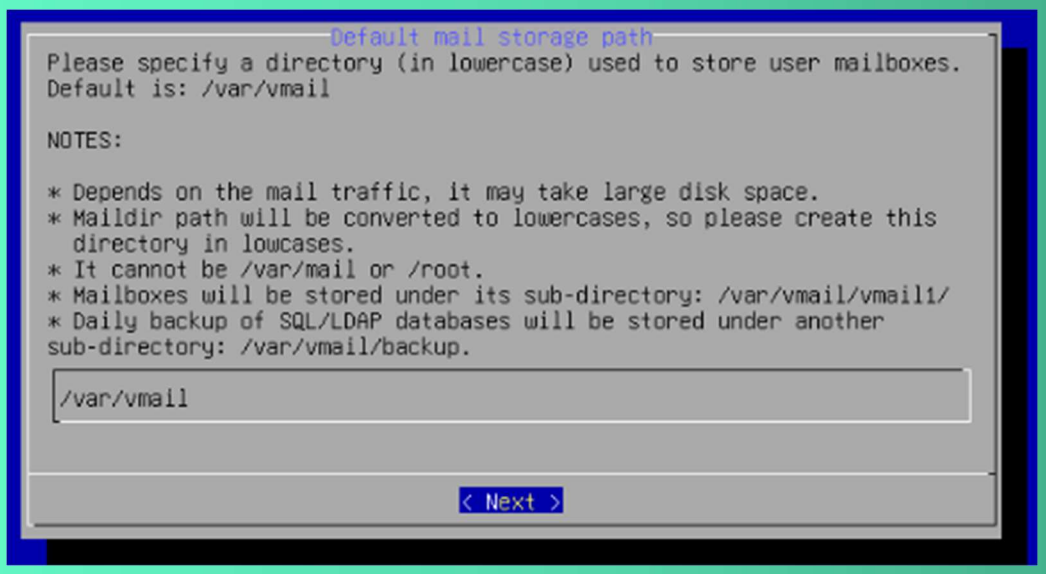
Bash iRedMail.sh

Screenshots of installation :

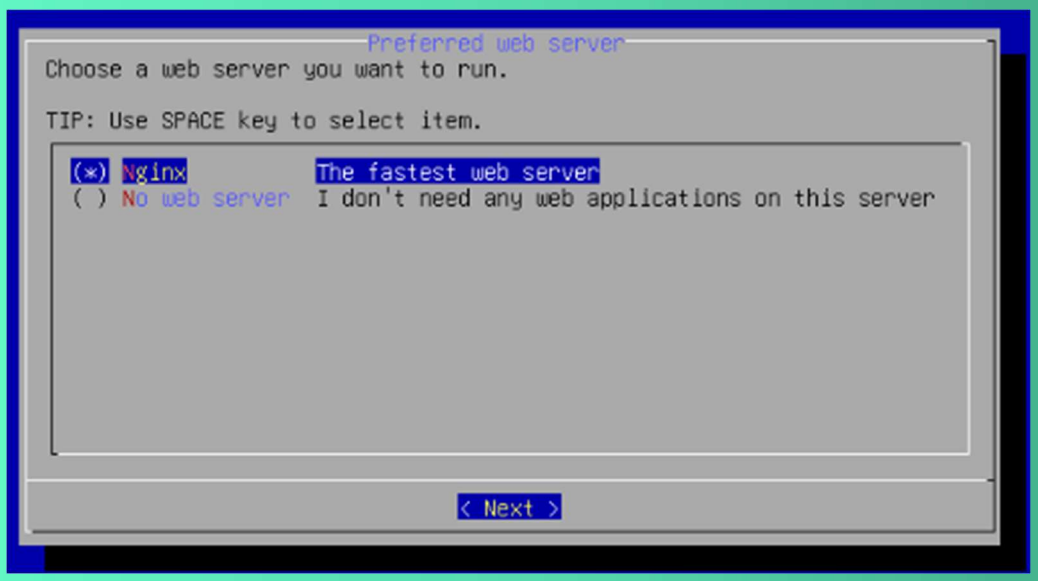
Welcome and thanks for your use



Specify location to store all mailboxes. Default is /var/vmail/.

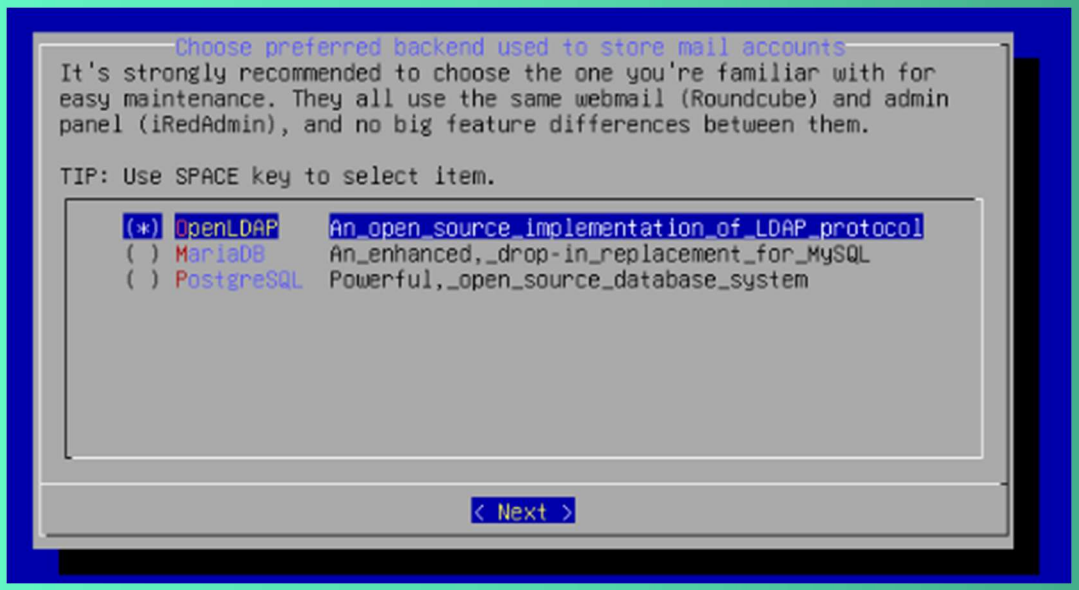


Choose your web server

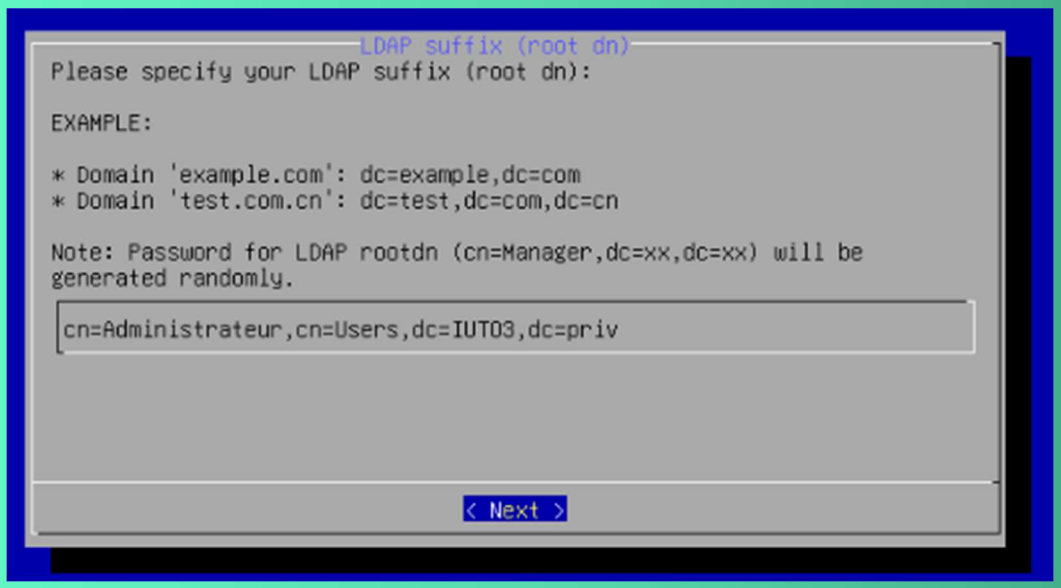


Choose backend used to store mail accounts. You can manage mail accounts with iRedAdmin, our web-based iRedMail admin panel.

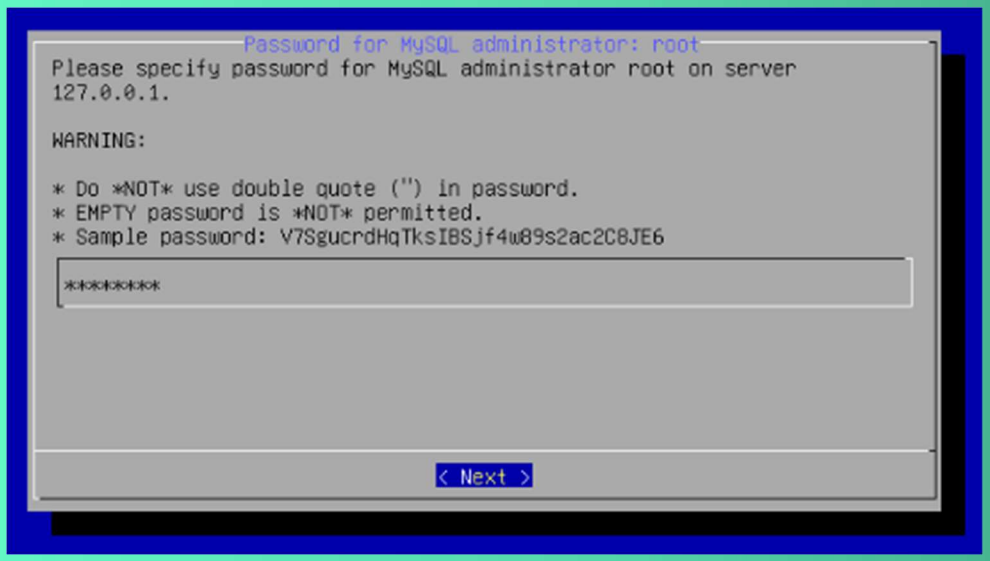
Selectionner OpenLDAP meme pour une intégration LDAP sur AD Windows



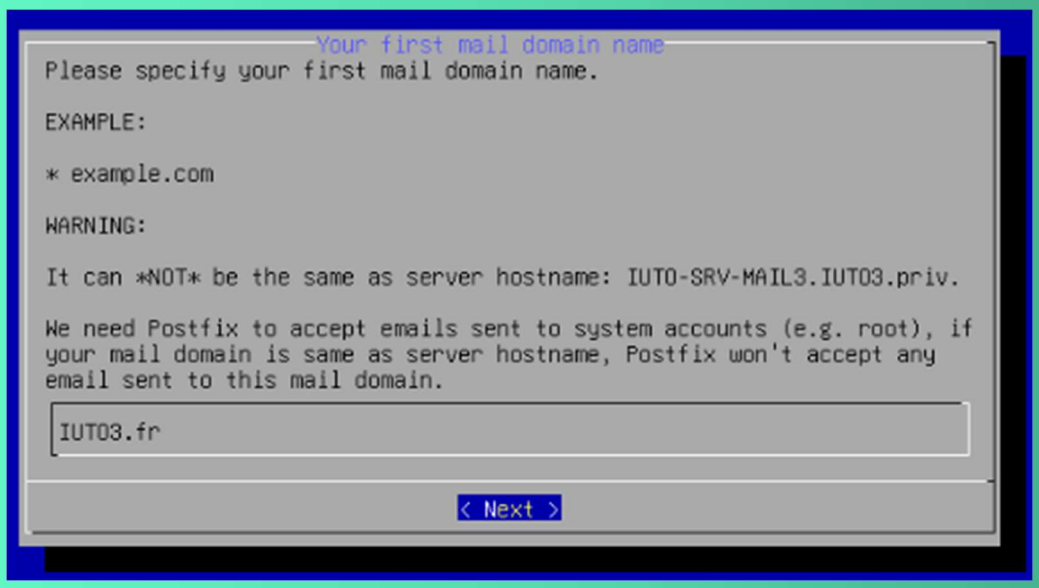
If you choose to store mail accounts in OpenLDAP, iRedMail installer will ask to set the LDAP suffix.



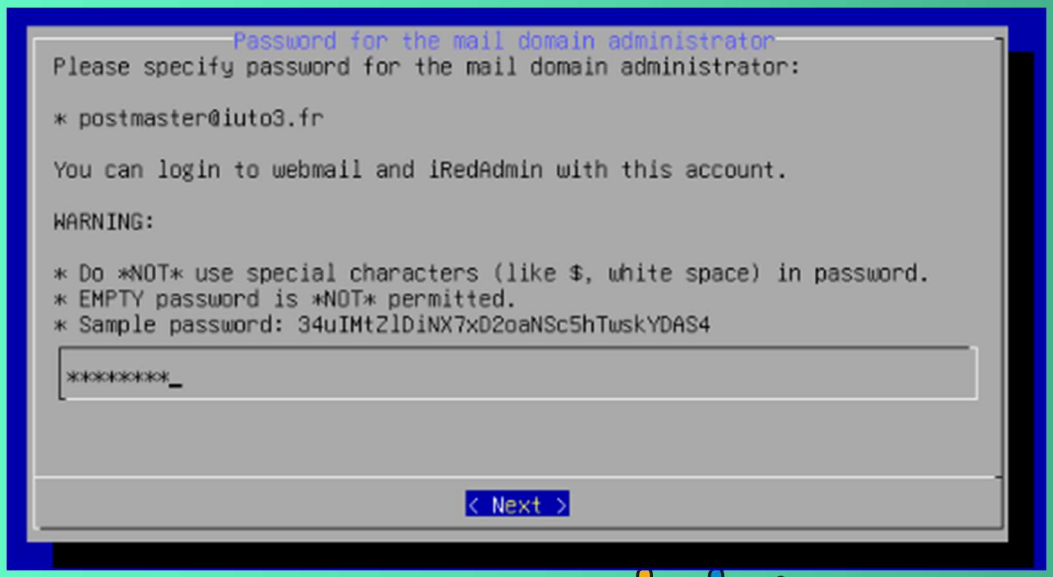
Set password for mySQL Administrator : Azerty45



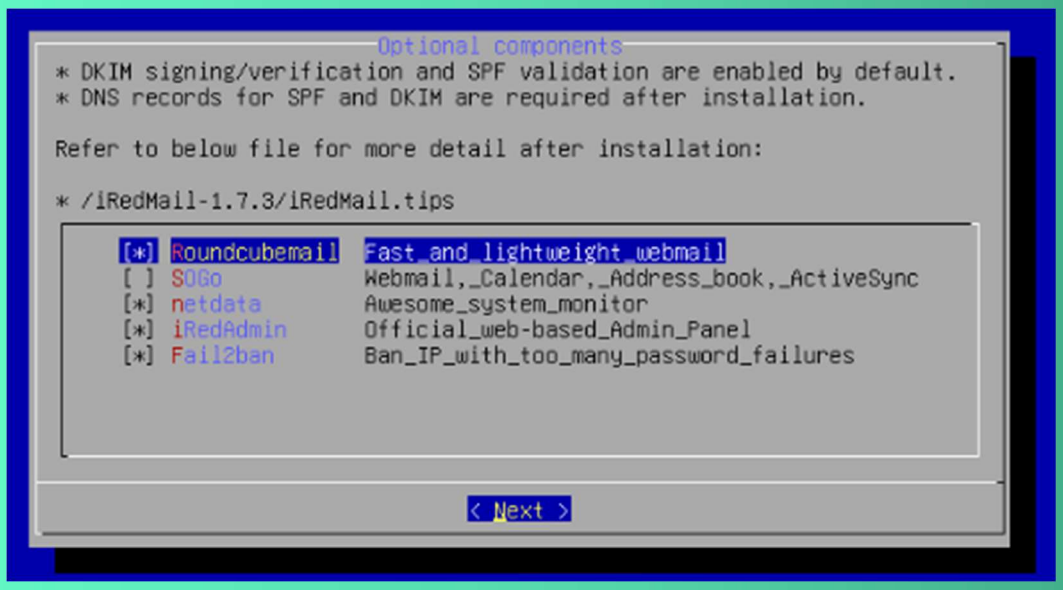
Add your first mail domain name

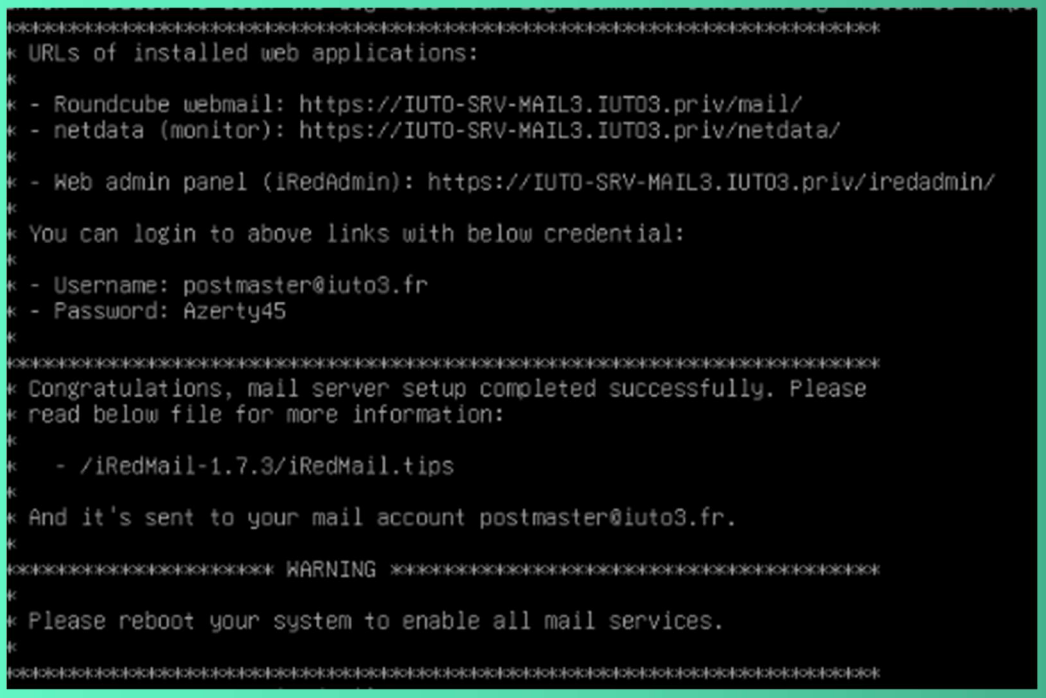


Set password of admin account of your first mail domain.



Choose optional components





Integrate Microsoft Active Directory with Postfix

Ldapsearch -x -H ldap://IUTO-SRV-AD3.IUTO3.priv -D'cn=Administrateur,cn=Users,dc=iuto3,dc=priv' -W -b 'dc=iuto3,dc=priv'

Enable LDAP query with AD in Postfix :

Disable unused iRedMail special settings :

```
postconf -e virtual_alias_maps=''
postconf -e sender_bcc_maps=''
postconf -e recipient_bcc_maps=''
postconf -e relay_domains=''
postconf -e relay_recipient_maps=''
postconf -e sender_dependent_relayhost_maps=''
```

Add your mail domain name in smtpd_sasl_local_domain and virtual_mailbox_domains :

```
postconf -e smtpd_sasl_local_domain='iuto.fr'
postconf -e virtual_mailbox_domains='iuto.fr'
```

Change transport maps setting:

```
postconf -e transport_maps='hash:/etc/postfix/transport'
```

Enable AD query. **Note**: We will create these 3 files later.

Verify SMTP senders

```
postconf -e smtpd_sender_login_maps='proxy:ldap:/etc/postfix/ad_sender_login_maps.cf'
```

Verify local mail users

```
postconf -e virtual_mailbox_maps='proxy:ldap:/etc/postfix/ad_virtual_mailbox_maps.cf'
```

Verify local mail lists/groups.

```
postconf -e virtual_alias_maps='proxy:ldap:/etc/postfix/ad_virtual_group_maps.cf'
```

Create/edit file: /etc/postfix/transport.

```
iuto3.fr dovecot
```

Note: the name dovecot used here is a Postfix transport defined in /etc/postfix/master.cf, used to deliver received emails to local user mailboxes.

Run postmap so that postfix can read it:

```
postmap hash:/etc/postfix/transport
```

Create file: /etc/postfix/ad_sender_login_maps.cf

```
server_host     = IUTO-SRV-AD3.IUTO3.priv
server_port     = 389
version         = 3
bind            = yes
start_tls       = no
bind_dn         = cn=Administrateur,cn=Users,dc=IUTO3,dc=priv
bind_pw         = Azerty45
search_base     = OU=IUTUSERS,dc=IUTO3,dc=priv
scope           = sub
query_filter    = (&(objectclass=person)(mail=%s))
```

```
result_attribute= mail
debuglevel     = 0
```

Create file: /etc/postfix/ad_virtual_mailbox_maps.cf:

```
server_host     = IUTO-SRV-AD3.IUTO3.priv
server_port     = 389
version         = 3
bind            = yes
start_tls       = no
bind_dn         = cn=Administrateur,cn=Users,dc=IUTO3,dc=priv
bind_pw         = Azerty45
search_base     = OU=IUTUSERS,dc=IUTO3,dc=priv
scope           = sub
query_filter    = (&(objectclass=person)(mail=%s))
result_attribute= mail
result_format   = %d/%u/Maildir/
debuglevel      = 0
```

Note: We hard-code user's mailbox path in result_format = parameter, it will be something like example.com/username/Maildir/.

Create file: /etc/postfix/ad_virtual_group_maps.cf:

```
server_host     = ad.example.com
server_port     = 389
version         = 3
bind            = yes
start_tls       = no
bind_dn         = cn=Administrateur,cn=Users,dc=IUTO3,dc=priv
bind_pw         = Azerty45
search_base     = OU=IUTUSERS,dc=IUTO3,dc=priv
scope           = sub
query_filter    = (&(objectClass=group)(mail=%s))
special_result_attribute = member
leaf_result_attribute = mail
result_attribute= mail
debuglevel      = 0
```

Also, we need to remove iRedAPD related settings in Postfix:

Open Postfix config file /etc/postfix/main.cf

Remove setting check_policy_service inet:127.0.0.1:7777.

```
# Recipient restrictions
smtpd_recipient_restrictions =
    reject_non_fqdn_recipient
    reject_unlisted_recipient
   #check_policy_service inet:127.0.0.1:7777
    permit_mynetworks
    permit_sasl_authenticated
    reject_unauth_destination
    check_policy_service inet:127.0.0.1:12340
```

Ligne 199/358

Verify LDAP query with AD in Postfix :

We can now use command line tool postmap to verify AD integration in postfix. Before testing, we have to create two testing mail accounts first:

Query mail user account with below command:

postmap -q aladjadi@iuto.fr ldap:/etc/postfix/ad_virtual_mailbox_maps.cf

example.com/user/Maildir/

```
root@IUTO-SRV-MAIL3:/etc/postfix# postmap -q aladjadi@iuto.fr ldap://etc/postfix/ad_virtual_mailbox_maps.cf
iuto.fr/aladjadi/Maildir/
```

Verify sender login check:

postmap -q user@example.com ldap:/etc/postfix/ad_sender_login_maps.cf

user@example.com

```
root@IUTO-SRV-MAIL3:/etc/postfix# postmap -q aladjadi@iuto.fr ldap://etc/postfix/ad_sender_login_maps.cf
aladjadi@iuto.fr
```

Verify mail group

postmap -q testgroup@example.com ldap:/etc/postfix/ad_virtual_group_maps.cf

user@example.com

Enable Active Directory integration in Dovecot :

we have to modify Dovecot config file /etc/dovecot/dovecot-ldap.conf like below :

hosts = 10.100.100.1 :389
ldap_version = 3

```
auth_bind      = yes
dn           =  cn=Administrateur,cn=Users,dc=IUTO3,dc=priv
dnpass         = Azerty45
base          = OU=IUTUSERS,dc=IUTO3,dc=PRIV
scope          = subtree
deref          = never

iterate_attrs   = mail=user
iterate_filter  = (&(objectClass=person)(mail=*))

user_filter        = (&(objectClass=person)(|(mail=%u)(otherMailbox=%u)))
pass_filter        = (&(objectClass=person)(mail=%u))
pass_attrs         = userPassword=password
default_pass_scheme  = CRYPT
user_attrs         =
mail=master_user,mail=user,=home=/var/vmail/vmail1/%Ld/%Ln/,=mail=maildir:~/Maildir/Restart
```

dovecot service to make it work.

Systemctl restart dovecot

Now use command telnet to verify AD query after restarted Dovecot service :

telnet localhost 143 # <- Type this

* OK [...] Dovecot ready.

. login user@example.com password_of_user # <- Type this. Do not miss the dot in the beginning

. OK [...] Logged in

Enable Active Directory integration in Roundcube webmail for Global LDAP Address Book :

Edit roundcube config file config/config.inc.php, comment out the LDAP address book setting added by iRedMail, and add new setting for AD like below:

- on RHEL/CentOS/Debian/Ubuntu and OpenBSD:
  it's /opt/www/roundcubemail/config/config.inc.php
- on FreeBSD: it's /usr/local/www/roundcubemail/config/config.inc.php

```
 GNU nano 7.2                                                /opt/www/roundcubemail/config/config.inc.php
$config['ldap_public']["global_ldap_abook"] = array(
    'name'              => 'Global LDAP Address Book',
    'hosts'             => array('10.100.100.1'),
    'port'              => 389,
    'use_tls'           => false,
    'ldap_version'      => '3',
    'network_timeout'   => 10,
    'user_specific'     => false,

    // Search mail users under same domain.
    'base_dn'       => 'OU=IUTUSERS,dc=IUTO3,dc=priv',
    'bind_dn'       => 'cn=Administrateur,cn=Users,dc=IUTO3,dc=priv',
    'bind_pass'     => 'Azerty45'

    'hidden'        => false,
    'searchonly'    => false,
    'writable'      => false,

    'search_fields' => array('mail', 'cn','sAMAccountName','displayName','sn','givenName'),

    // mapping of contact fields to directory attributes
    'fieldmap' => array(
        'name'          => 'cn',
        'displayname'   => 'displayName'
        'surname'       => 'sn',
        'firstname'     => 'givenName',
        'jobtitle'      => 'title',
        'department'    => 'department',
        'company'       => 'company',
        'email'         => 'mail:*',
        'phone:work'    => 'telephoneNumber',
        'phone:home'    => 'homePhone',
        'phone:mobile'  => 'mobile',
        'phone:workfax' => 'facsimileTelephoneNumber',
        'phone:pager'   => 'pager',
        'phone:other'   => 'ipPhone',
        'street:work'   => 'streetAddress',
        'zipcode:work'  => 'postalCode',
        'locality:work' => 'l',
        'region:work'   => 'st',
        'country:work'  => 'c',
        'notes'         => 'description',
        'photo'         => 'jpegPhoto',
        'website'       => 'wWWHomePage',
    ),
    'sort'          => 'cn',
```

INSTALLATION DE FOG

Installer FOG depuis le github officiel : https://github.com/FOGProject

wget https://github.com/FOGProject/fogproject/archive/refs/heads/working-1.6.zip

unzip working-1.6.zip

cd fogproject-working-1.6/bin

./installfog.sh

```
root@IUTO-SRV-FOG3:~/fogproject-working-1.6/bin# ./installfog.sh
Installing LSB_Release as needed
 * Attempting to get release information.....................Done

 ==================================
 ===         ====     =====       ====
 ===  =========  ==  ===   ==    ===
 ===  ========  ====  ==  ====  ===
 ===  ========  ====  ==  =========
 ===       ====  ====  ==  =========
 ===  ========  ====  ==  ===    ===
 ===  ========  ====  ==  ====  ===
 ===  =========  ==  ===   ==    ===
 ===  ==========    =====      ====
 ==================================
 ===== Free Opensource Ghost ======
 ==================================
 ============ Credits =============
 = https://fogproject.org/Credits =
 ==================================
 == Released under GPL Version 3 ==
 ==================================

  Version: 1.6.0-beta.2167 Installer/Updater

 What version of Linux would you like to run the installation for?

         1) Redhat Based Linux (Redhat, Alma, Rocky, CentOS, Mageia)
         2) Debian Based Linux (Debian, Ubuntu, Kubuntu, Edubuntu)
         3) Alpine Linux

 Choice: [2] 2
```

Suivre ces étapes :

What type of installation would you like to do? [N/s (Normal/Storage)] N

f you are not sure, select No. [y/N] N

Would you like to use the FoG server for DHCP service? [y/N] n

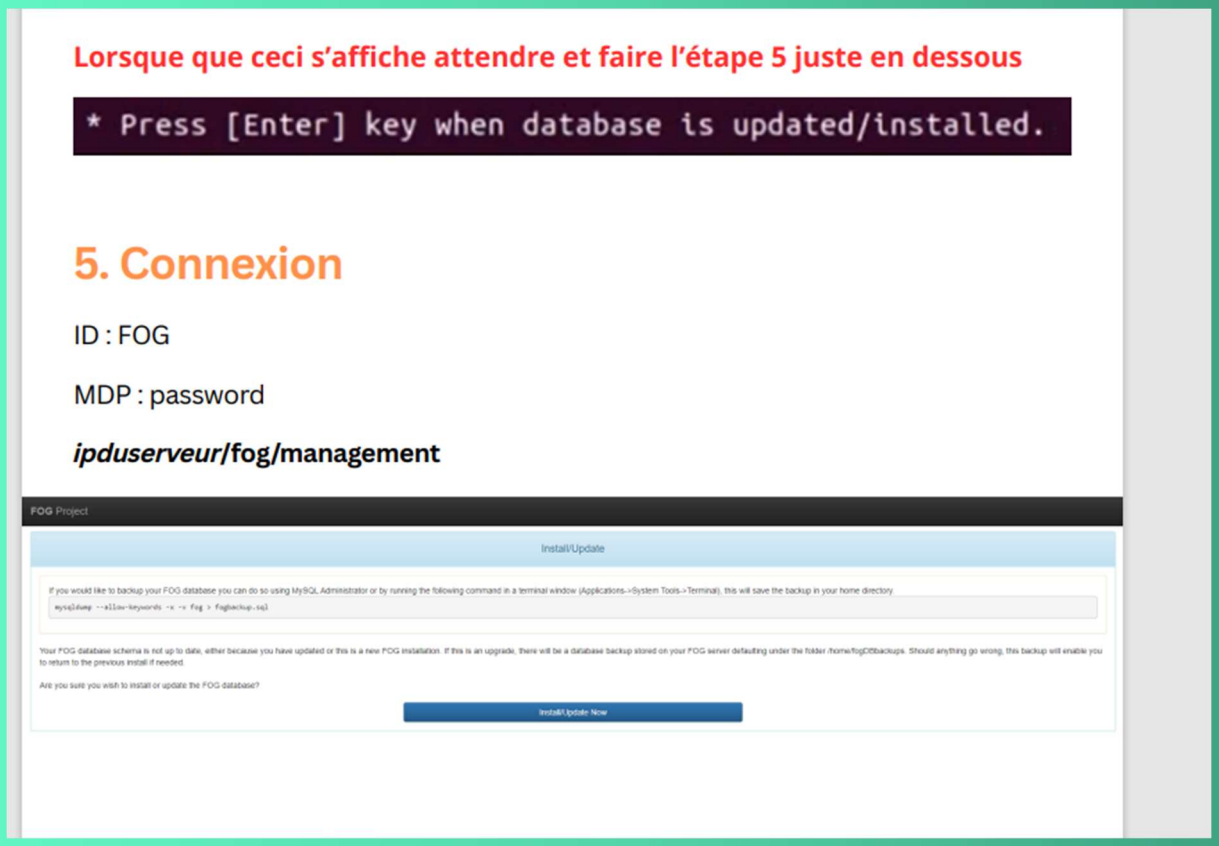
This version of FoG has internationalization support, would you like to install the additional language packs? (y/N] N

Would you like to enable secure HTTPS on your FOG server? [y/N] N

Would you like too change it? If you are not sure, select No [y/N] N

Are you ok with sending this information? [Y/n] Y

Are you sure you wish to continue (Y/N) Y



https://10.100.100.220/fog/management

INSTALLATION DE KANBOARD

Installer les dépendances nécessaires :

Mettez à jour vos paquets et installez Apache, PHP et MySQL avec les commandes suivantes :

Version : Php8.2 / MariaDB10.11

apt update

apt install apache2 php php-cli php-mbstring php-xml php-curl php-mysql mariadb-server php-ldap git php-sqlite3 php-gd

Redémarrez Apache pour appliquer les changements :

systemctl restart apache2

Télécharger et configurer Kanboard :

Allez dans le répertoire web de votre serveur Apache et clonez le dépôt de Kanboard depuis GitHub :

cd /var/www

git clone https://github.com/kanboard/kanboard.git kanboard

chown -R www-data:www-data kanboard

Kanboard nécessite une base de données pour stocker les informations relatives aux projets et tâches.

Créez la base de données dans MySQL/MariaDB et un utilisateur pour Kanboard :

mysql -u root -p

CREATE DATABASE kanboard;

CREATE USER 'gt'@'localhost' IDENTIFIED BY 'Azerty45';

GRANT ALL PRIVILEGES ON kanboard.* TO 'gt'@'localhost';

FLUSH PRIVILEGES;

EXIT;

Configurer Kanboard pour la connexion à la base de données :

Allez dans le répertoire de Kanboard et copiez le fichier de configuration par défaut :

cd /var/www/kanboard

cp config.default.php config.php

Ensuite, ouvrez config.php pour y indiquer les informations de votre base de données :

nano config.php

Assurez-vous que tous les fichiers ont les bonnes permissions :

sudo chown -R www-data:www-data /var/www/html/kanboard

sudo chmod -R 755 /var/www/html/kanboard

Configurer Apache pour Kanboard :

Créez un fichier de configuration Apache pour Kanboard :

nano /etc/apache2/sites-available/kanboard.conf

Ajoutez les lignes suivantes :

```
<VirtualHost *:80>
    ServerName 10.100.100.220
    DocumentRoot /var/www/kanboard
    <Directory /var/www/kanboard>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

Activez le site et redémarrez Apache :

sudo a2ensite kanboard.conf

sudo a2enmod rewrite

sudo systemctl restart apache2

Configurer l'authentification LDAP :

Configurer LDAP dans Kanboard :

Ouvrez le fichier config.php pour activer et configurer l'authentification LDAP. Ajoutez les paramètres LDAP suivants dans le fichier :

```
// Activer LDAP
define('LDAP_ENABLED', true);
define('LDAP_SERVER', 'ldap://ldap.votre-serveur.com'); // Adresse de votre serveur LDAP
define('LDAP_PORT', 389); // Port LDAP (389 pour non sécurisé, 636 pour sécurisé)
define('LDAP_BASE_DN', 'OU=IUTUSERS,DC=IUTO3,DC=PRIV'; // Base DN (remplacez par le vôtre)
define('LDAP_USER_DN', 'CN=Users,DC=example,DC=com'); // Groupe d'utilisateurs LDAP
define('LDAP_USER_FILTER', '(&(objectClass=user)(sAMAccountName=%s))'); // Filtre de recherche
LDAP BIND TYPE : USER ;
define('LDAP_BIND_DN', 'CN=bind_user,CN=Users,DC=example,DC=com'); // Utilisateur pour se
connecter au LDAP
```

define('LDAP_BIND_PASSWORD', 'mot_de_passe'); // Mot de passe pour se connecter au LDAP
define('LDAP_VERSION', 3); // Version du protocole LDAP (3 pour Active Directory)
define('LDAP_TLS', false); // Activer TLS si nécessaire (true pour sécurisé)

Modifiez ces valeurs pour qu'elles correspondent à votre serveur LDAP. Par exemple, si vous utilisez Active Directory, le BASE DN pourrait ressembler à DC=example,DC=com, et le USER DN pourrait être CN=Users,DC=example,DC=com.

Désactiver l'authentification interne (facultatif) :

Si vous souhaitez désactiver l'authentification interne et utiliser uniquement LDAP, ajoutez la ligne suivante dans config.php :

define('AUTH_METHOD', 'ldap'); // Utiliser uniquement LDAP pour l'authentification

Vérification et tests :

Redémarrez Apache pour appliquer les changements :

sudo systemctl restart apache2

Accédez à Kanboard depuis votre navigateur. Allez à http://localhost (ou l'adresse IP de votre serveur) pour accéder à l'interface de Kanboard.

Testez la connexion LDAP :
Utilisez les identifiants d'un utilisateur LDAP valide pour vous connecter. Si tout est configuré correctement, Kanboard devrait authentifier les utilisateurs via votre serveur LDAP.

INSTALLATION DE SQUID

Installation de Squid :

apt install squid –y

Configuration de SQUID :

Dans le ‘’/etc/squid/squid.conf’’ écrire

```
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535      # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
# http_port 10.100.100.236:3128
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
# acl networklan src 10.0.0.0/8
http_access deny all
http_port 3128
# http_access allow networklan
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|?) 0 0% 0
refresh_pattern (Release|Packages(.gz)*)$ 0 20% 2880
refresh_pattern . 0 20% 4320
cache_mem 256 MB
maximum_object_size 512 MB
```

Ensuit il faut activer et lancer le serveur :

systemctl enable squid
systemctl start squid

Blocage de site/domaine :
nano /etc/squid/squid.conf

```
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl networklan src 10.0.0.0/8

# ACL de blocage de sites
acl blockYoutube dstdomain .youtube.com
acl blockFacebookFR dstdomain .facebook.fr
acl blockFacebookCOM dstdomain .facebook.com

# Refuser l'accès aux sites interdits
http_access deny blockYoutube
http_access deny blockFacebookFR
http_access deny blockFacebookCOM

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
```

ACL de blocage de sites
acl blockYoutube dstdomain .youtube.com
acl blockFacebookFR dstdomain .facebook.fr
acl blockFacebookCOM dstdomain .facebook.com

Refuser l'accès aux sites interdits
http_access deny blockYoutube
http_access deny blockFacebookFR
http_access deny blockFacebookCOM

Blocage par Mots-Clef :

Créez le fichier "block_keywords.conf" dans "/etc/squid" :
nano /etc/squid/block_keywords.conf

Il faut saisir les mots interdis

adult
sexe
porn

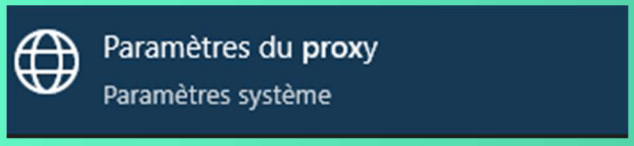
Ensuite il faut modifier le fichier squid.conf
nano /etc/squid.conf

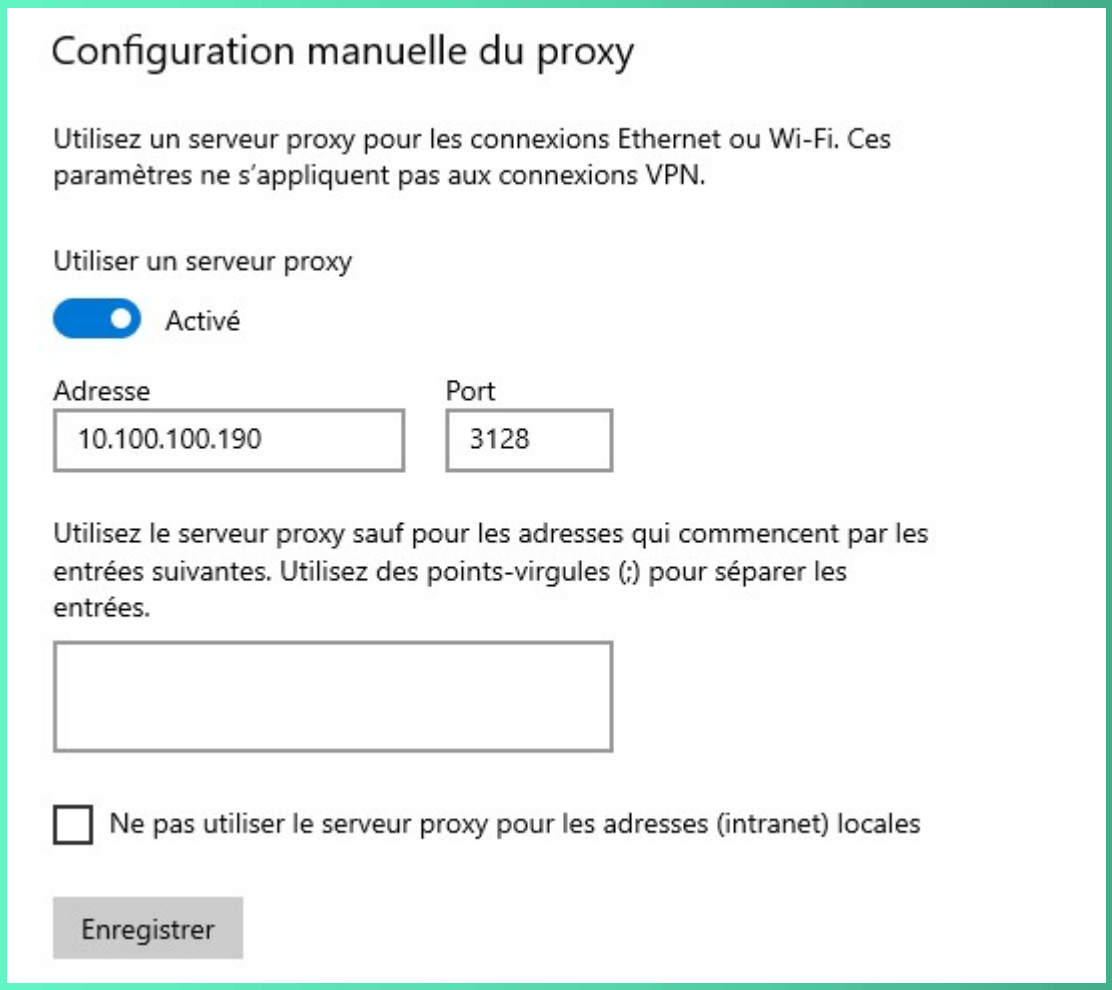
acl block_keywords url_regex -i "/etc/squid/block_keywords.conf" http_access deny block_keywords

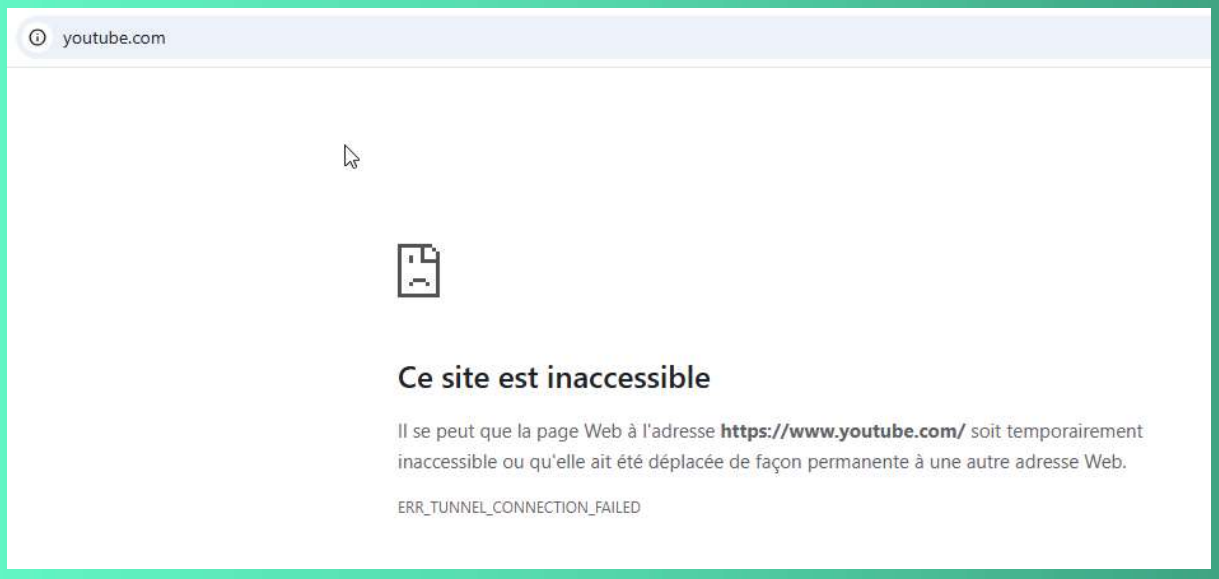
```
# ACL de blocage de sites
acl blockYoutube dstdomain .youtube.com
acl blockFacebookFR dstdomain .facebook.fr
acl blockFacebookCOM dstdomain .facebook.com

# ACL de blocage par mot clef
acl block_keywords url_regex -i "/etc/squid/block_keywords.conf"
http_access deny block_keywords

# Refuser l'accès aux sites interdits
http_access deny blockYoutube
http_access deny blockFacebookFR
http_access deny blockFacebookCOM
```

systemctl enable squid
systemctl restart squid

Test sur client :

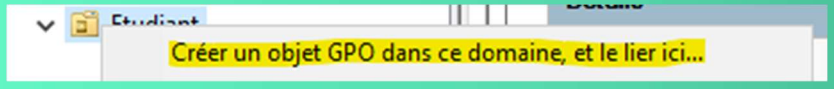




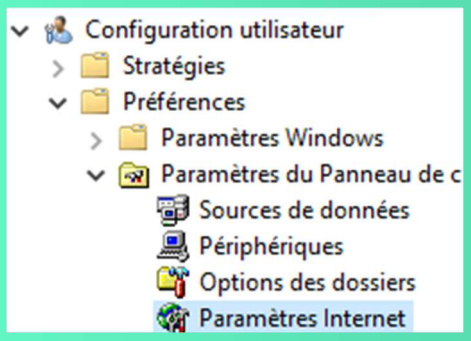


<u>Déploiement du proxy par GPO :</u>

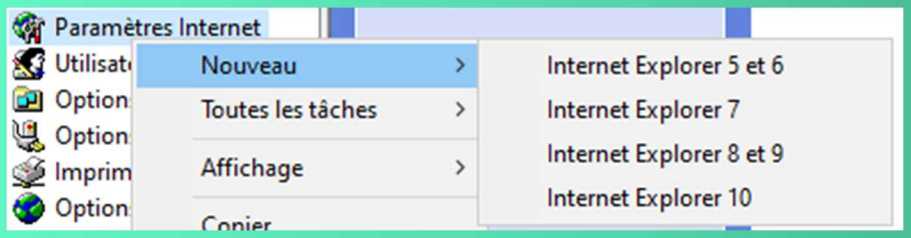
Dans le gestionnaire de stratégie de groupe sur les ‘’IUTuser’’ dans ‘’Étudiant’’



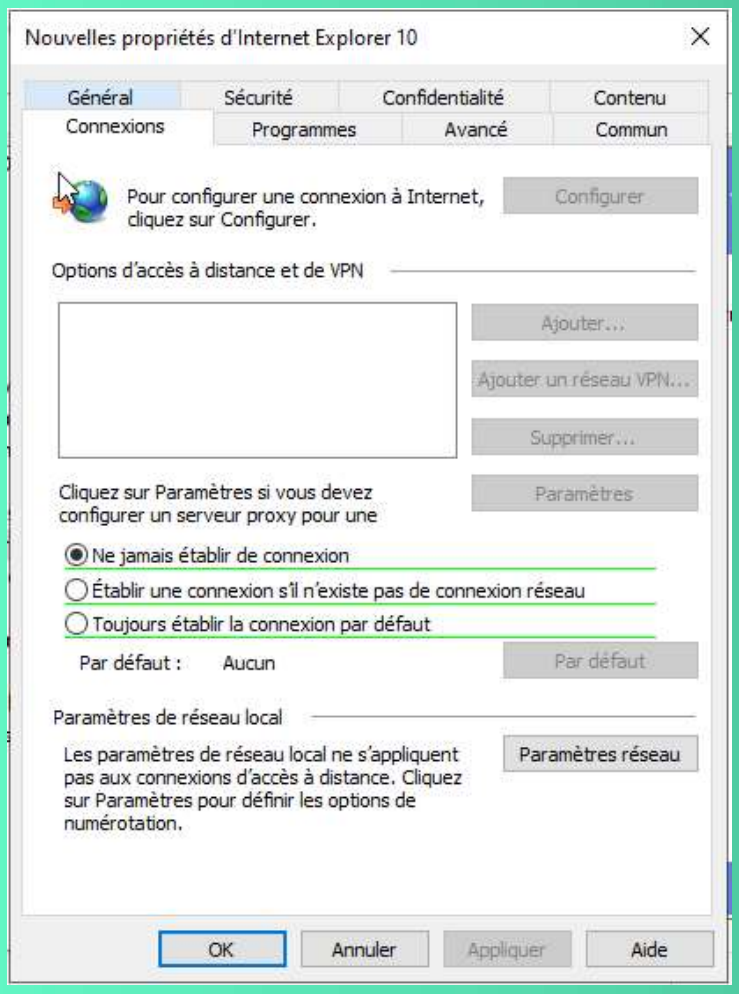
Clique droit « Modifier »



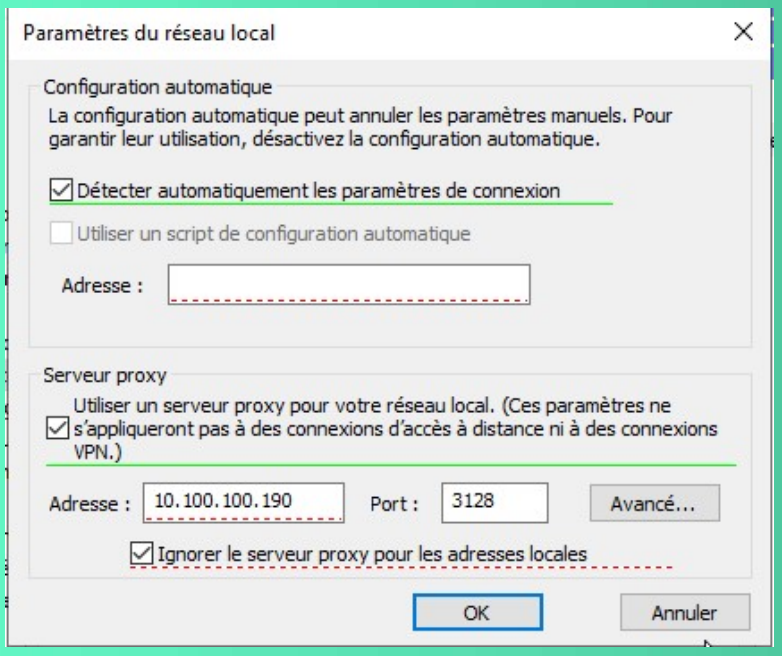
Choisir Explorer 10



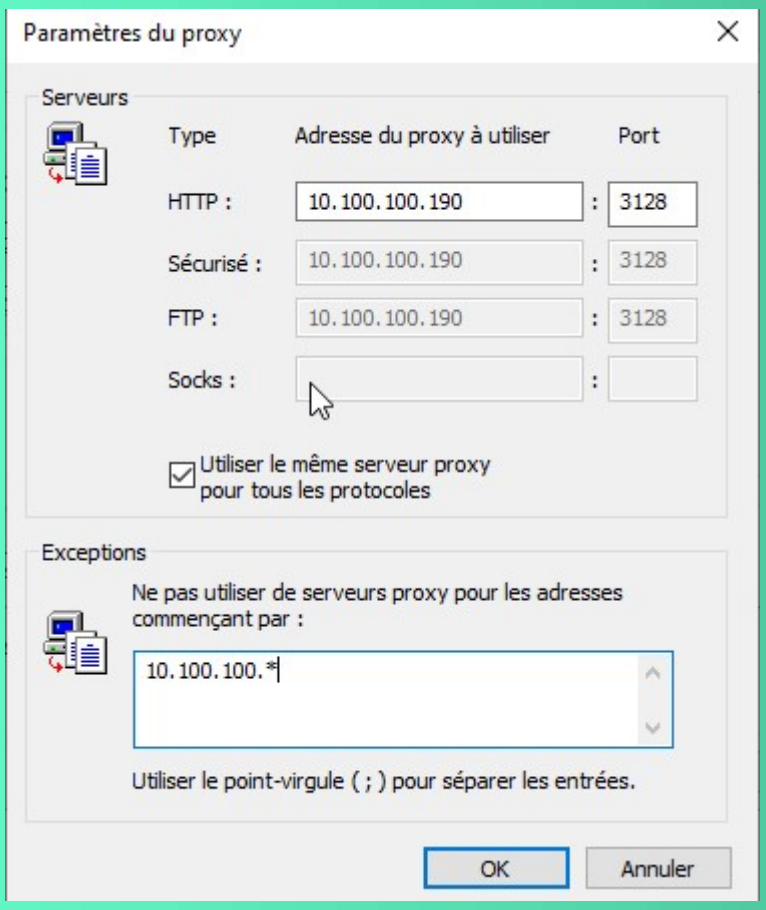
Dans « Connexions »



Ensuite « Paramètres réseaux »

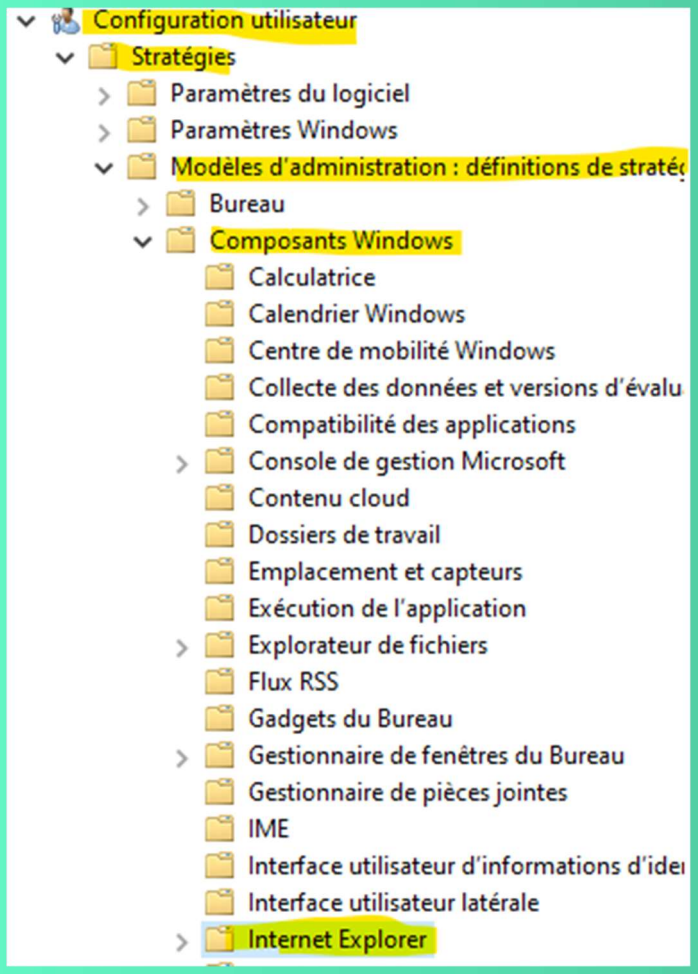

Paramètres du réseau local
Configuration automatique
La configuration automatique peut annuler les paramètres manuels. Pour garantir leur utilisation, désactivez la configuration automatique.
Détecter automatiquement les paramètres de connexion
Utiliser un script de configuration automatique
Adresse :
Serveur proxy
Utiliser un serveur proxy pour votre réseau local. (Ces paramètres ne s'appliqueront pas à des connexions d'accès à distance ni à des connexions VPN.)
Adresse : 10.100.100.190
Port : 3128
Avancé...
Ignorer le serveur proxy pour les adresses locales
OK
Annuler

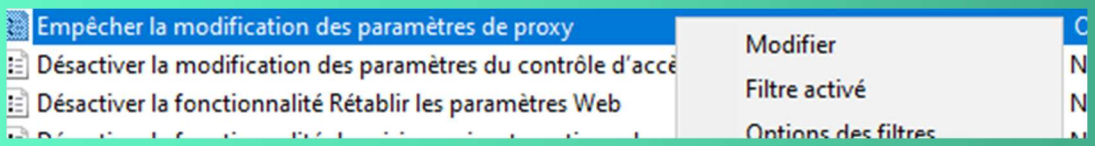
Puis « Avancé… »

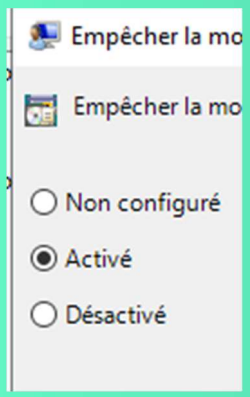

Paramètres du proxy
Serveurs
Type
Adresse du proxy à utiliser
Port
HTTP : 10.100.100.190 : 3128
Sécurisé : 10.100.100.190 : 3128
FTP : 10.100.100.190 : 3128
Socks :
Utiliser le même serveur proxy pour tous les protocoles
Exceptions
Ne pas utiliser de serveurs proxy pour les adresses commençant par :
10.100.100.*
Utiliser le point-virgule (;) pour séparer les entrées.
OK
Annuler

Blocage des paramètres proxy aux utilisateurs :

Modifier la meme GPO





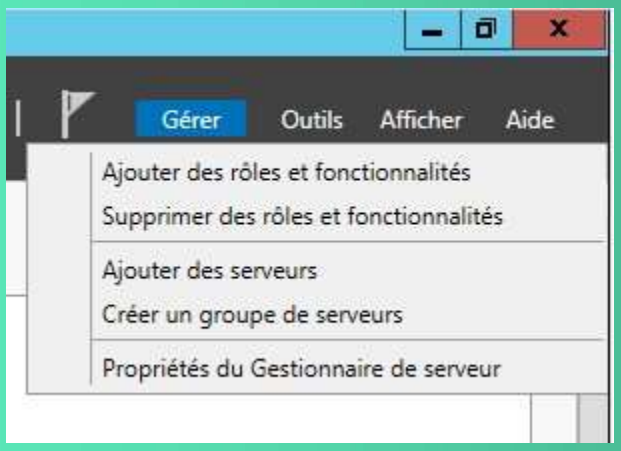


MISE EN PLACE D'UN RODC

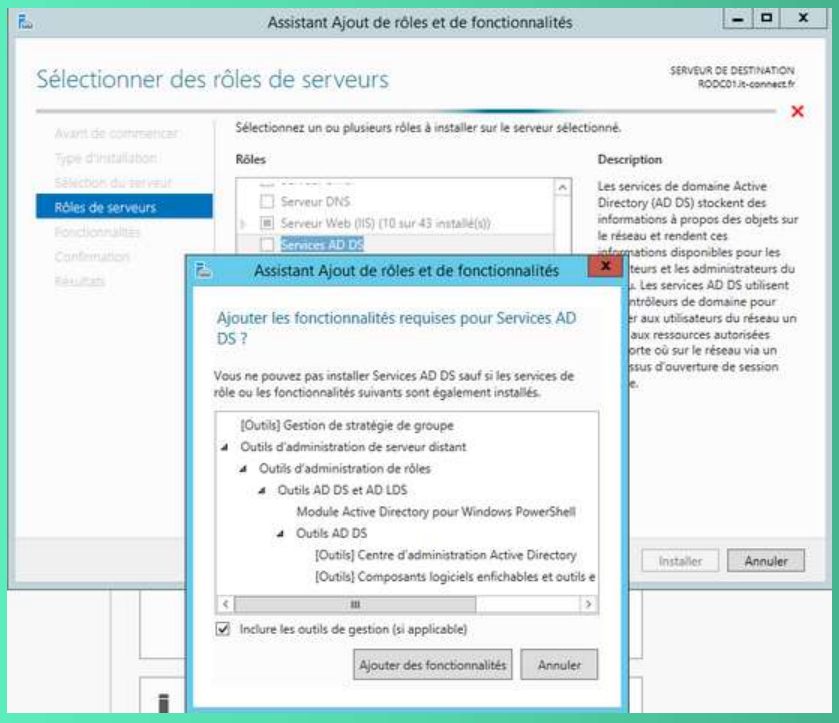
Installation du service :

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 IUTO3.PRIV en niveau fonctionnel Windows Server 2022.

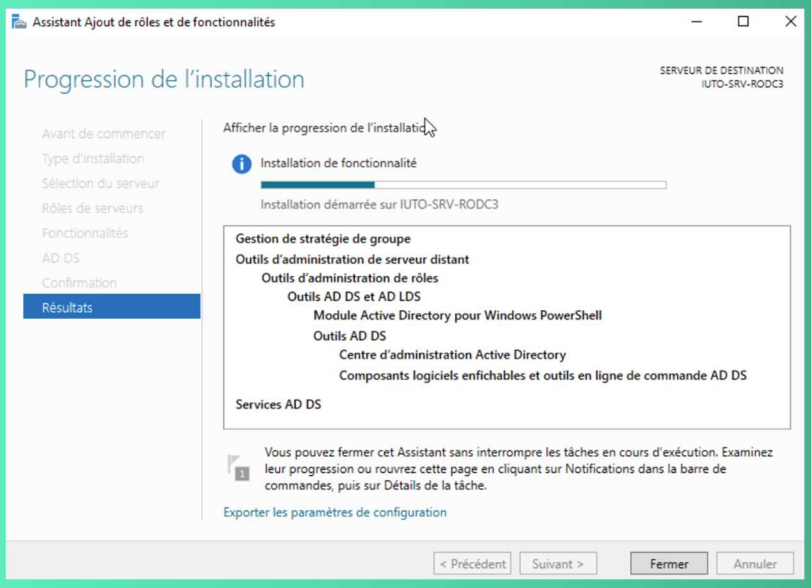
Sur le futur RODC, ouvrez le gestionnaire de serveur puis cliquez sur « Gérer » et « Ajouter des rôles et fonctionnalités ».



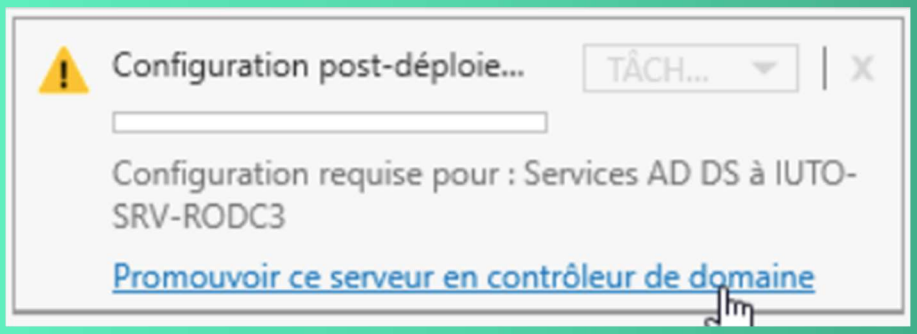
Dans la liste, sélectionnez « Services AD DS », confirmez l'ajout des fonctionnalités requises pour ce rôle et poursuivez.



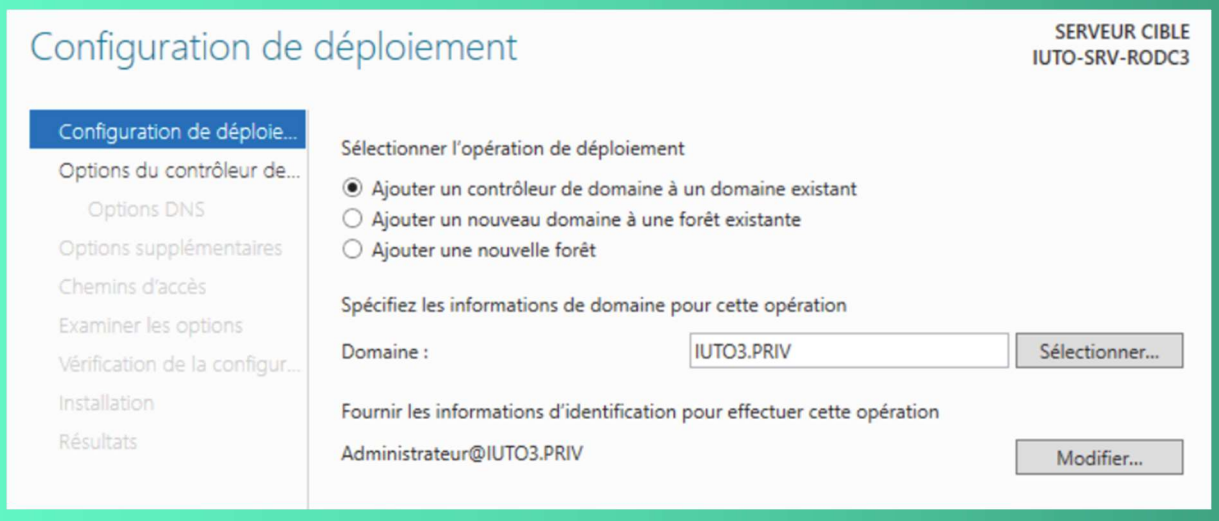
Confirmez que vous souhaitez installer les sélections en cliquant sur « Installer ».



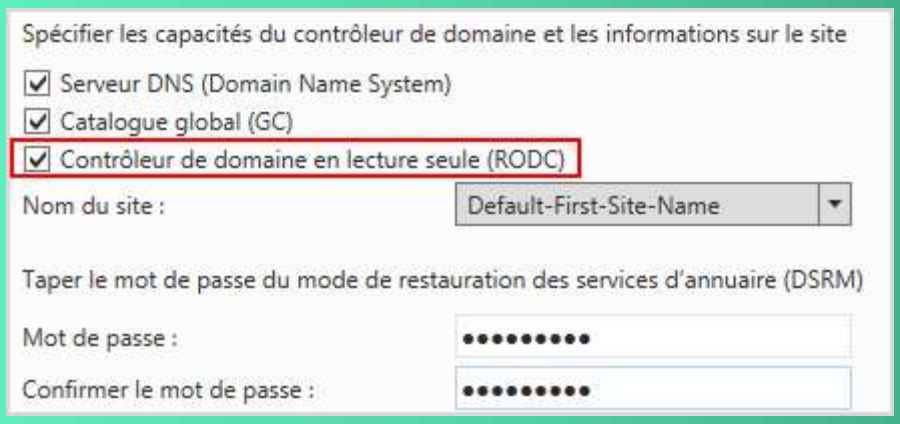
Ensuite, retournez au sein du gestionnaire de serveur, cliquez sur l'icône en « forme de triangle jaune où il y a un point d'exclamation » puis « Promouvoir ce serveur en contrôleur de domaine ».



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



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



Les options RODC doivent être définies :

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

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

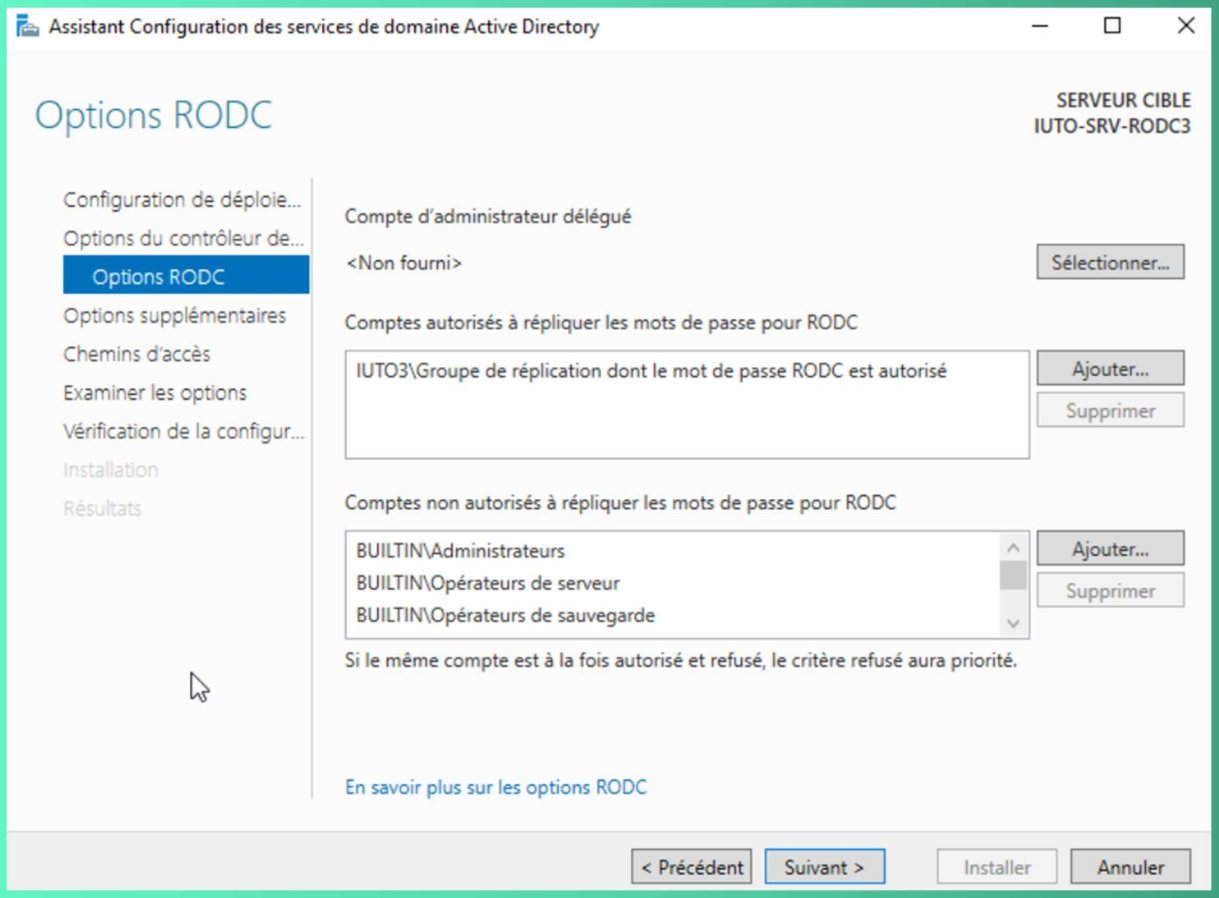
- Groupe de réplication dont le mot de passe RODC est autorisé
- Groupe de réplication dont le mot de passe RODC est refusé

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

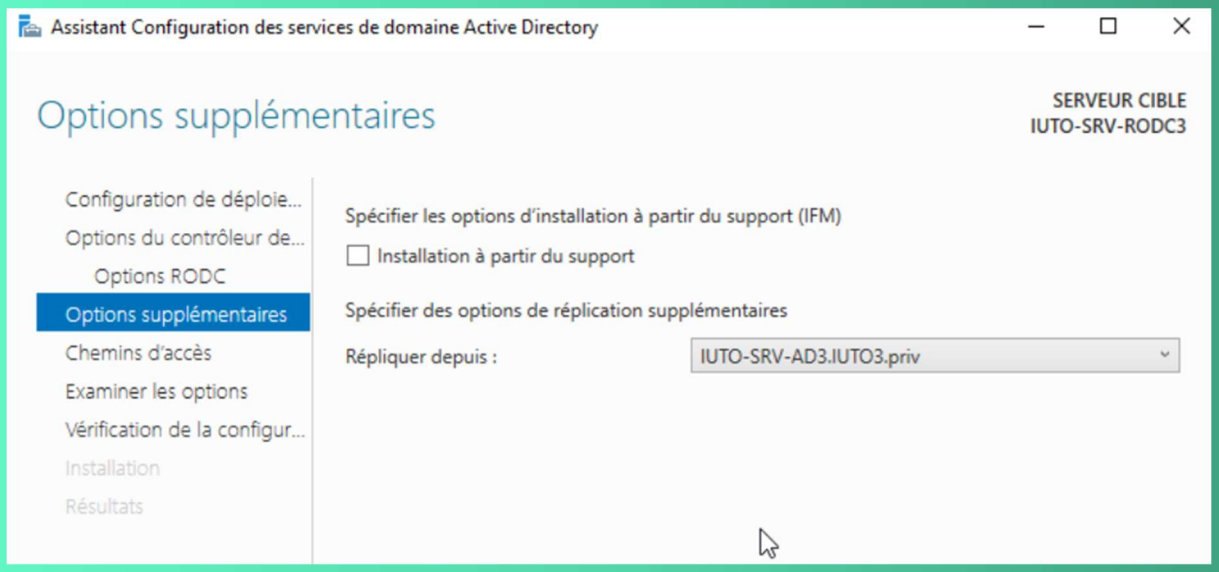
- Comptes autorisés à répliquer les mots de passe pour RODC : Ajouter des utilisateurs ou groupes pour lesquels vous souhaitez autoriser la réplication. Le mieux, c'est de laisser uniquement le groupe « Groupe de réplication dont le mot de passe RODC est autorisé » et dans l'Active Directory d'ajouter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

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

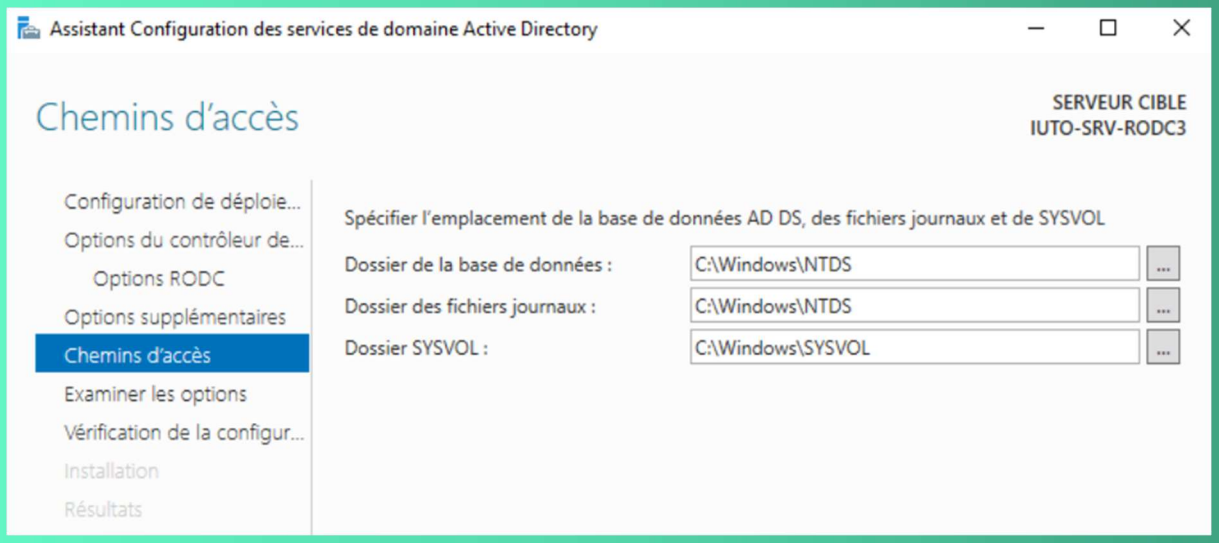
Cliquez sur « Suivant » pour continuer l'installation.



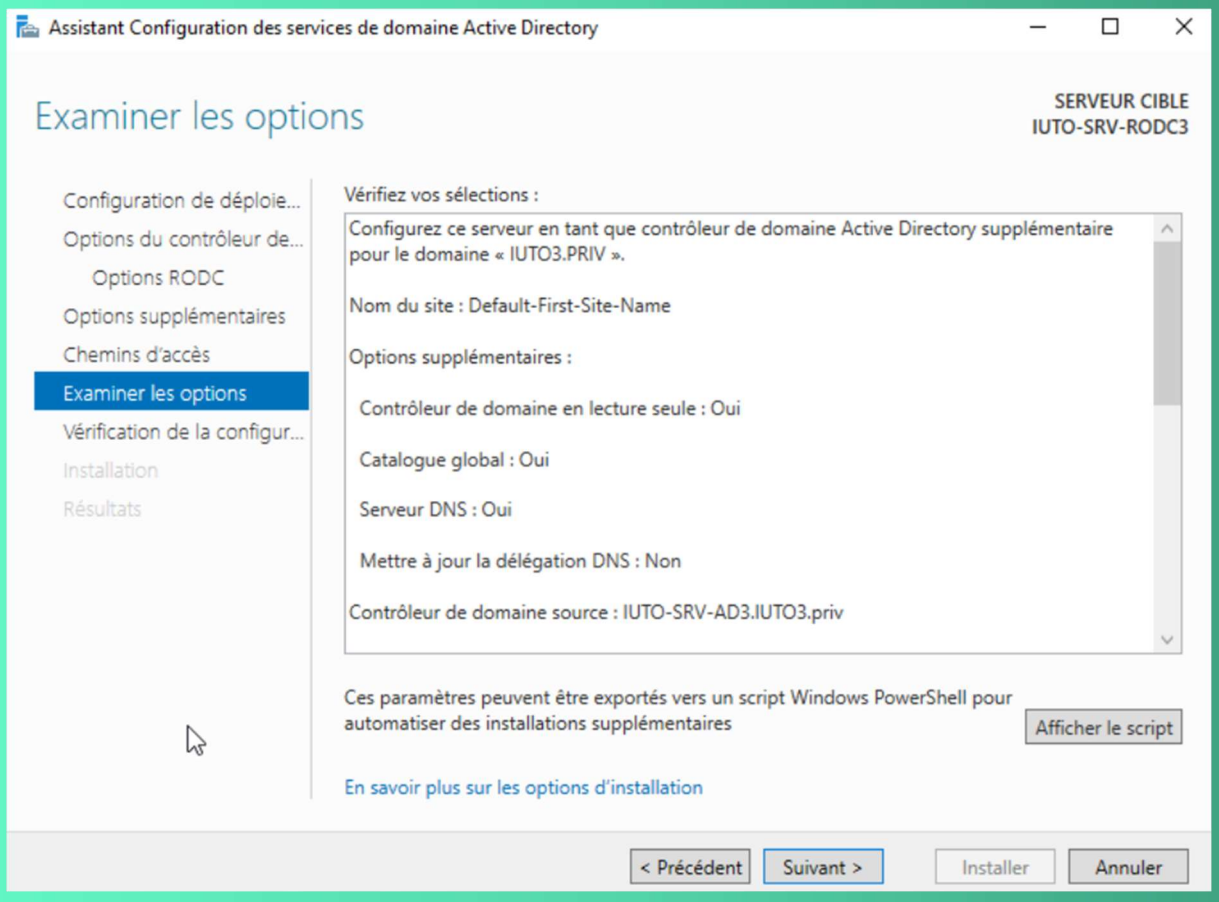
Indiquez un contrôleur de domaine standard depuis lequel répliquer les informations autorisées (ou installer à partir d'un support si vous disposez d'un support prêt – utile pour économiser de la bande passante même lors de la mise en place). Cliquez sur « Suivant ».



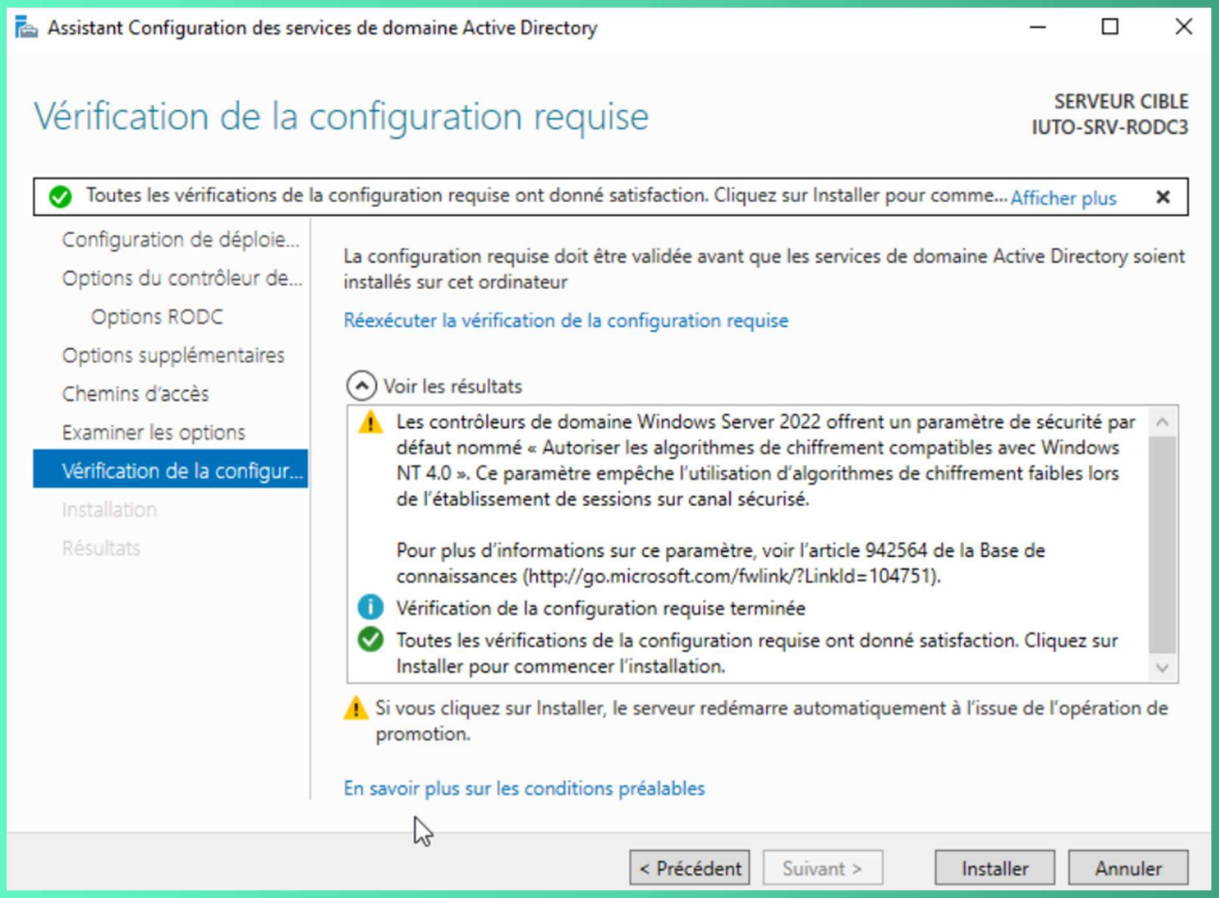
Indiquez l'emplacement de la base de données, des fichiers journaux et de SYSVOL (peuvent être placés sur des disques différents). Cliquez sur « Suivant ».



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



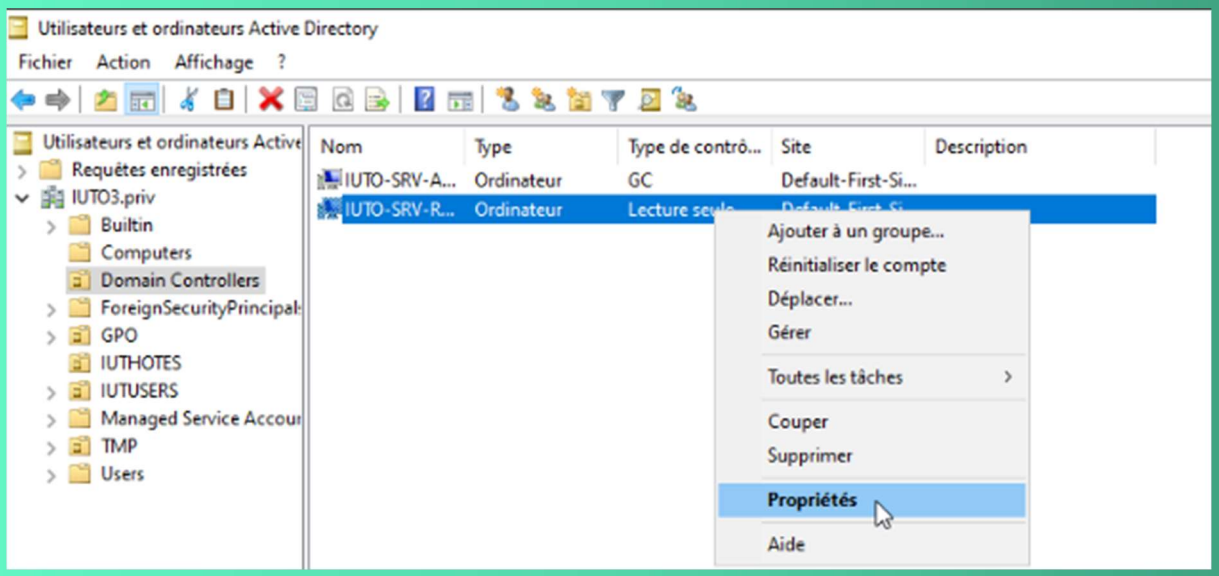
Après que la configuration soit vérifiée, cliquez sur « Installer » et patientez un instant. Le serveur va redémarrer automatiquement à la fin de l'installation.



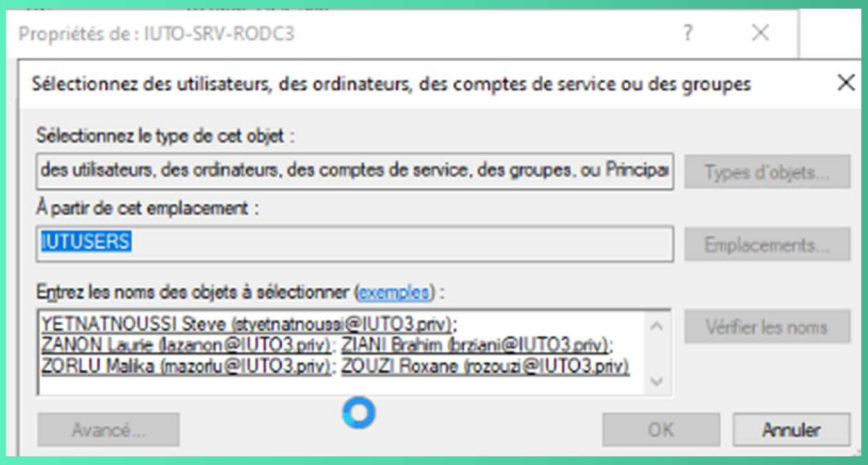
L'installation du RODC est désormais terminée.

Réplication des mots de passes

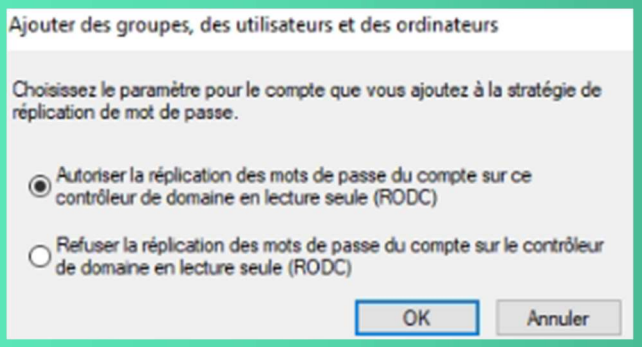
Sur un contrôleur de domaine standard (lecture/écriture), ouvrez la console « Utilisateurs et ordinateurs Active Directory », positionnez-vous sur l'unité d'organisation « Domain Controllers ». Sur la droite, faites clic droit sur l'objet ordinateur correspondant à votre serveur RODC puis « Propriétés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

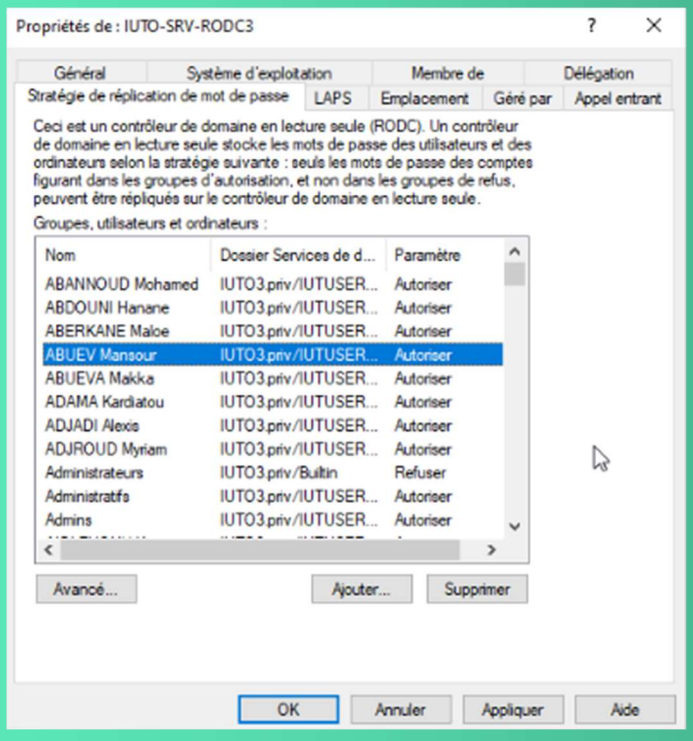


Cliquez ensuite sur l'onglet « Stratégie de réplication de mot de passe » qui concerne donc la stratégie de réplication des mots de passe. La fenêtre affiche les utilisateurs et groupes pour lesquels vous autorisez ou refusez explicitement la réplication des mots de passe.



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





Intégration des serveurs LINUX dans le domaine

Pré-requis :

Vérification de la connexion à l'AD

Vous devez avoir un accès réseau à votre Debian pour joindre le contrôleur de domaine (DC) « ping 'nom du domaine' »

```
root@IUTO-SRV-ZABBIX:~# ping iuto3.priv
PING iuto3.priv (10.100.100.1) 56(84) bytes of data.
64 bytes from 10.100.100.1 (10.100.100.1): icmp_seq=1 ttl=128 time=0.724 ms
64 bytes from 10.100.100.1 (10.100.100.1): icmp_seq=2 ttl=128 time=0.757 ms
64 bytes from 10.100.100.1 (10.100.100.1): icmp_seq=3 ttl=128 time=0.755 ms
64 bytes from 10.100.100.1 (10.100.100.1): icmp_seq=4 ttl=128 time=0.686 ms
64 bytes from 10.100.100.1 (10.100.100.1): icmp_seq=5 ttl=128 time=0.838 ms
^C
--- iuto3.priv ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.686/0.752/0.838/0.050 ms
```

Configurer le « nano /etc/hosts » pour inclure le contrôleur de domaine.

```
  GNU nano 7.2
127.0.0.1       IUTO-SRV-ZABBIX
127.0.1.1       IUTO-SRV-ZABBIX.IUTO3.priv      IUTO-SRV-ZABBIX

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Synchroniser L'horloge :

Mettre à jour :

« apt update & apt upgrade »

« apt install ntpsec »

« « systemctl start ntp »

Installer les paquets nécessaires :

Mise à système et installer les dépendances :

« apt update »

« apt install sssd sssd-tools realmd adcli krb5-user samba-common-bin packagekit »

Configuration de Kerberos :

Vous pouvez laisser par défault car nous allons le configure dans le dossier :

« nano /etc/krb5.conf »

```
  GNU nano 7.2                                                  /etc/krb5.conf *
[libdefaults]
        default_realm = IUTO-SRV-ZABBIX3.IUTO3.priv

# The following krb5.conf variables are only for MIT Kerberos.
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
        rdns = false


# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        IUTO3.priv = {
                kdc = IUTO-SRV-AD3.IUTO3.priv
                admin_server = IUTO-SRV-AD3.IUTO3.priv
        }
```

```
[domain_realm]
        .iuto3.priv = IUTO3.priv
        iuto3.priv = IUTO3.priv_
```

Connexion à l'AD :

Modification de « etc/resolv.conf » :

Vous devez écrire « nameserver '@IP de votre srv AD' »

```
  GNU nano 7.2                                                  /etc/resolv.conf
nameserver 10.100.100.1
```

Joindre la machine au domaine AD :

« adcli join -D IUTO3.priv -U Administrateur -v »

```
root@IUTO-SRV-ZABBIX:~# adcli join -D IUTO3.priv -U Administrateur -v
```

Puis taper votre mot de passe.

```
root@IUTO-SRV-ZABBIX:~# adcli join -D IUTO3.priv -U Administrateur -v
 * Using domain name: IUTO3.priv
 * Calculated computer account name from fqdn: IUTO-SRV-ZABBIX
 * Calculated domain realm from name: IUTO3.PRIV
 * Discovering domain controllers: _ldap._tcp.IUTO3.priv
 * Sending NetLogon ping to domain controller: iuto-srv-ad3.iuto3.priv
 * Received NetLogon info from: IUTO-SRV-AD3.IUTO3.priv
 * Wrote out krb5.conf snippet to /tmp/adcli-krb5-IwjHrv/krb5.d/adcli-krb5-conf-cQfCwz
Password for Administrateur@IUTO3.PRIV:
```

```
root@IUTO-SRV-ZABBIX:~# adcli join -D IUTO3.priv -U Administrateur -v
 * Using domain name: IUTO3.priv
 * Calculated computer account name from fqdn: IUTO-SRV-ZABBIX
 * Calculated domain realm from name: IUTO3.PRIV
 * Discovering domain controllers: _ldap._tcp.IUTO3.priv
 * Sending NetLogon ping to domain controller: iuto-srv-ad3.iuto3.priv
 * Received NetLogon info from: IUTO-SRV-AD3.IUTO3.priv
 * Wrote out krb5.conf snippet to /tmp/adcli-krb5-IwjHrv/krb5.d/adcli-krb5-conf-cQfCwz
Password for Administrateur@IUTO3.PRIV:
 * Authenticated as user: Administrateur@IUTO3.PRIV
 * Using GSS-SPNEGO for SASL bind
 * Looked up short domain name: IUTO3
 * Looked up domain SID: S-1-5-21-3546124178-3557249819-3756094561
 * Using fully qualified name: IUTO-SRV-ZABBIX
 * Using domain name: IUTO3.priv
 * Using computer account name: IUTO-SRV-ZABBIX
 * Using domain realm: IUTO3.priv
 * Calculated computer account name from fqdn: IUTO-SRV-ZABBIX
 * Generated 120 character computer password
 * Using keytab: FILE:/etc/krb5.keytab
 * A computer account for IUTO-SRV-ZABBIX$ does not exist
 * Found well known computer container at: CN=Computers,DC=IUTO3,DC=priv
 * Calculated computer account: CN=IUTO-SRV-ZABBIX,CN=Computers,DC=IUTO3,DC=priv
 * Encryption type [3] not permitted.
 * Encryption type [1] not permitted.
 * Created computer account: CN=IUTO-SRV-ZABBIX,CN=Computers,DC=IUTO3,DC=priv
 * Sending NetLogon ping to domain controller: iuto-srv-ad3.iuto3.priv
 * Received NetLogon info from: IUTO-SRV-AD3.IUTO3.priv
 * Set computer password
 * Retrieved kvno '2' for computer account in directory: CN=IUTO-SRV-ZABBIX,CN=Computers,DC=IUTO3,DC=priv
 * Checking RestrictedKrbHost/IUTO-SRV-ZABBIX
 *    Added RestrictedKrbHost/IUTO-SRV-ZABBIX
 * Checking host/IUTO-SRV-ZABBIX
 *    Added host/IUTO-SRV-ZABBIX
 * Discovered which keytab salt to use
 * Added the entries to the keytab: IUTO-SRV-ZABBIX$@IUTO3.PRIV: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: host/IUTO-SRV-ZABBIX@IUTO3.PRIV: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: RestrictedKrbHost/IUTO-SRV-ZABBIX@IUTO3.PRIV: FILE:/etc/krb5.keytab
root@IUTO-SRV-ZABBIX:~#
```

Configurer le fichier ldap :

Dans le dossier « nano /Etc/ldap/ldap.conf »

Puis écrivez « TLS_REQCERT try »

```
  GNU nano 7.2                                                /etc/ldap/ldap.conf *
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE   dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-provider.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
TLS_REQCERT try_
```

Vérification de l'intégration :

Une fois la machine jointe au domaine, vous pouvez vérifier avec la commande « realm list »

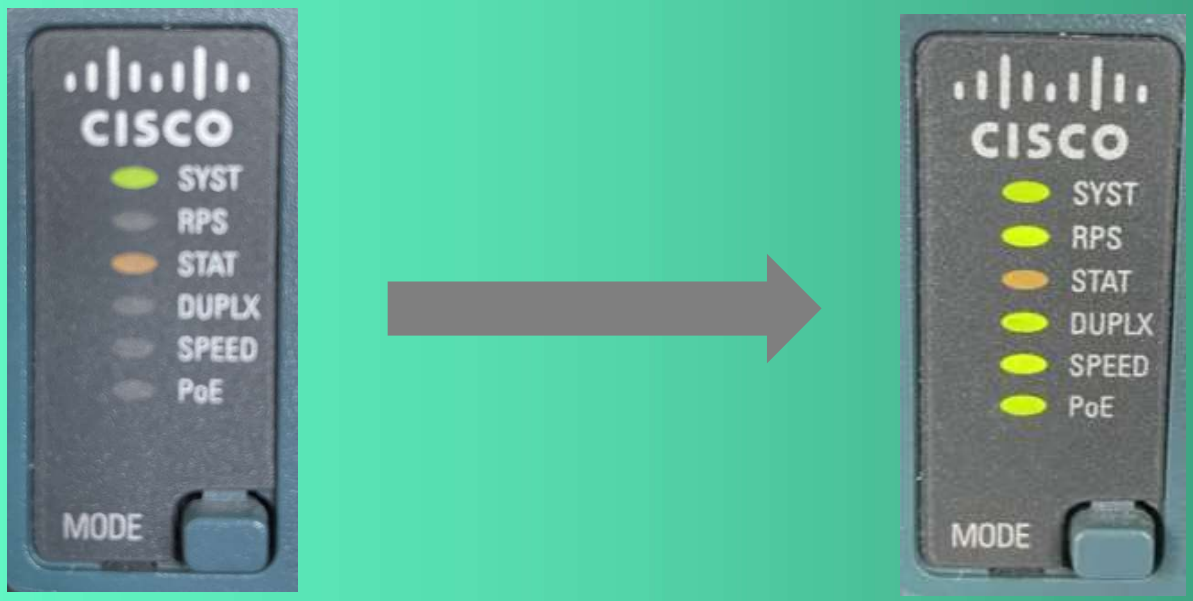
Vous pouvez également vous rendre sur votre AD et vérifier que le poste est bien remonté, taper la commande suivante dans votre cmd : « dsa.msc »

On peut apercevoir que nos deux machines linux sont bien remonté dans notre AD.

CONFIGURATION DU SWITCH

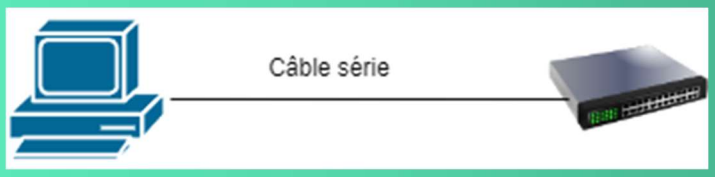
Procédure de réinitialisation :

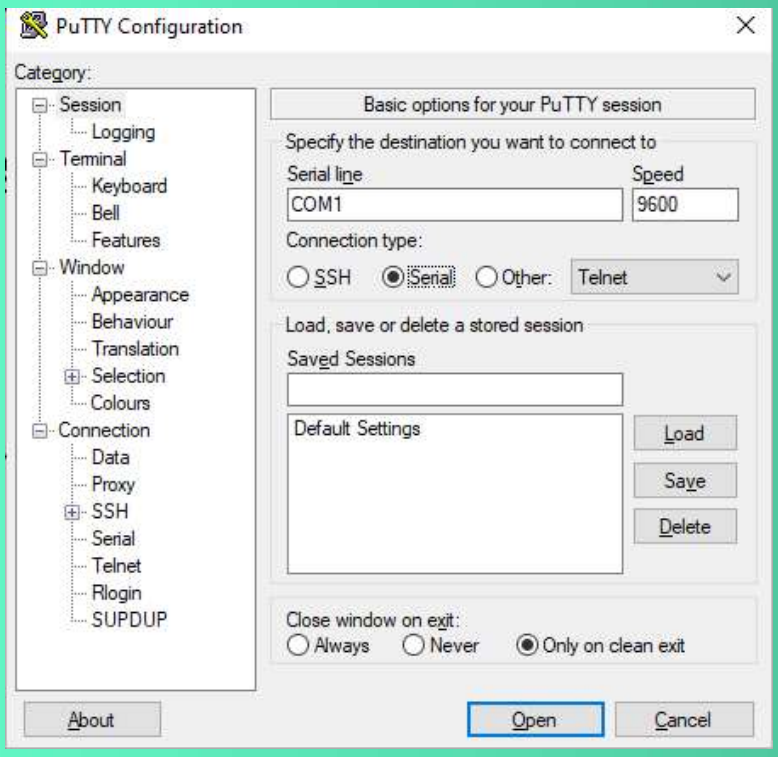
Pour réinitialiser le switch aux paramètres d'usine, il faut appuyer sur le bouton mode et maintenez-le enfoncé, les voyants LED du commutateur commencent à clignoter au bout de 3 secondes. Maintenez toujours le bouton mode enfoncé, les LED cessent de clignoter après 7 secondes supplémentaires puis le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

```
IUTO-SWCHI-03(config)#hostname IUTO-SWCHI-03
```

Nous avons ajouté comme mot de passe ‘AzertyGT45’

```
IUTO-SWCHI-03(config)#enable password AzertyGT45
IUTO-SWCHI-03(config)#service password-encryption
```

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

```
IUTO-SWCHI-03(config-line)#line vty 0
IUTO-SWCHI-03(config-line)#password AzertyGT
```

Et ajouter une adresse IP

```
IUTO-SWCHI-03(config)#interface vlan 99
IUTO-SWCHI-03(config-if)#ip address 10.10.0.254 255.0.0.0
```

Pour enregistrer la configuration, il faut entrer cette commande :

```
IUTO-SWCHI-03#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuration des VLANS :

Des contraintes sont à respectées :

Les ports 1 à 24 seront réservés à la DATA

Les ports 25 à 30 seront réservés aux TELIP

Les ports 31 et 36 sont réservés à la VISIO

Les ports 37 et 42 sont réservés aux WIFI

Le port 47 est réservé pour le lien avec le cœur de réseau

Le port 48 est réservés au ADMIN, dédié à la gestion du commutateur

Création des VLANS :

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

Nous devons créer 4 VLAN différents, le VLAN 10 nommée DATA, le VLAN 20 nommée TELIP, le VLAN 30 nommée VISIO ainsi que le VLAN 40 nommée WIFI

```
IUTO-SWCHI-03(config)#vlan 10
IUTO-SWCHI-03(config-vlan)#name DATA
IUTO-SWCHI-03(config-vlan)#exit
IUTO-SWCHI-03(config)#Vlan 20
IUTO-SWCHI-03(config-vlan)#name TELIP
IUTO-SWCHI-03(config-vlan)#exit
IUTO-SWCHI-03(config)#vlan 30
IUTO-SWCHI-03(config-vlan)#name VISIO
IUTO-SWCHI-03(config-vlan)#exit
IUTO-SWCHI-03(config)#vlan 40
IUTO-SWCHI-03(config-vlan)#name WIFI
IUTO-SWCHI-03(config-vlan)#exit
IUTO-SWCHI-03(config)#vlan 99
IUTO-SWCHI-03(config-vlan)#name ADMIN
```

Ajout des ports dans leur VLAN respectif :

Ajouter le port 1 à 24 dans le VLAN 10 en mode access réservés à la DATA :

```
IUTO-SWCHI-03(config)#interface range fastEthernet 0/1-24
IUTO-SWCHI-03(config-if-range)#switchport mode access
IUTO-SWCHI-03(config-if-range)#switchport access vlan 10
```

Ajouter le port 25 à 30 dans le VLAN 20 en mode access réservés aux TELIP :

```
IUTO-SWCHI-03(config)#interface range fastEthernet 0/25-30
IUTO-SWCHI-03(config-if-range)#switchport mode access
IUTO-SWCHI-03(config-if-range)#switchport access vlan 20
```

Ajouter le port 31 et 36 dans le VLAN 30 en mode access réservés à la VISIO :

```
IUTO-SWCHI-03(config)#interface range fastEthernet 0/31-36
IUTO-SWCHI-03(config-if-range)#switchport mode access
IUTO-SWCHI-03(config-if-range)#switchport access vlan 30
```

Ajouter le port 37 et 42 dans le VLAN 40 en mode access réservés à la WIFI :

```
IUTO-SWCHI-03(config)#interface range fastEthernet 0/37-42
IUTO-SWCHI-03(config-if-range)#switchport mode access
IUTO-SWCHI-03(config-if-range)#switchport access vlan 40
```

Sur le port 47, nous allons activer le mode trunk et y autoriser le VLAN 10, 20, 30 et 40

```
IUTO-SWCHI-03(config)#interface fastEthernet 0/47
IUTO-SWCHI-03(config-if)#switchport mode trunk
IUTO-SWCHI-03(config-if)#switchport trunk allowed vlan 10,20,30,40
```

Ajouter le port 48 dans le VLAN 99 en mode access réservés à ADMIN :

```
IUTO-SWCHI-03(config)#interface fastEthernet 0/48
IUTO-SWCHI-03(config-if)#switchport mode access
IUTO-SWCHI-03(config-if)#switchport access vlan 99
```

Pour vérifier que les interfaces soit dans les bon VLAN, entre la commande ‘show vlan’

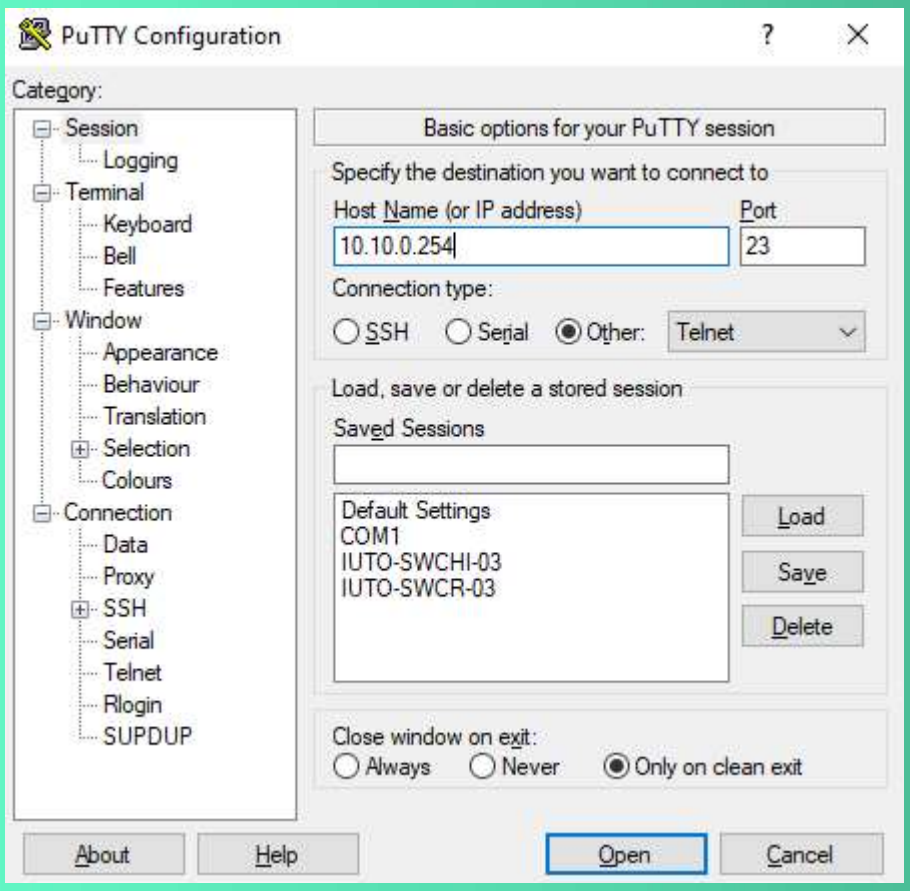
```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/43, Fa0/44, Fa0/45, Fa0/46
                                                Fa0/47, Gi0/1, Gi0/2, Gi0/3
                                                Gi0/4
10   DATA                             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
20   TELIP                            active    Fa0/25, Fa0/26, Fa0/27, Fa0/28
                                                Fa0/29, Fa0/30
30   VISIO                            active    Fa0/31, Fa0/32, Fa0/33, Fa0/34
                                                Fa0/35, Fa0/36
40   WIFI                             active    Fa0/37, Fa0/38, Fa0/39, Fa0/40
                                                Fa0/41, Fa0/42
99   ADMIN                            active    Fa0/48
```

Pour enregistrer la configuration, il faut entrer cette commande :

```
IUTO-SWCHI-03#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Comment se connecter à distance :

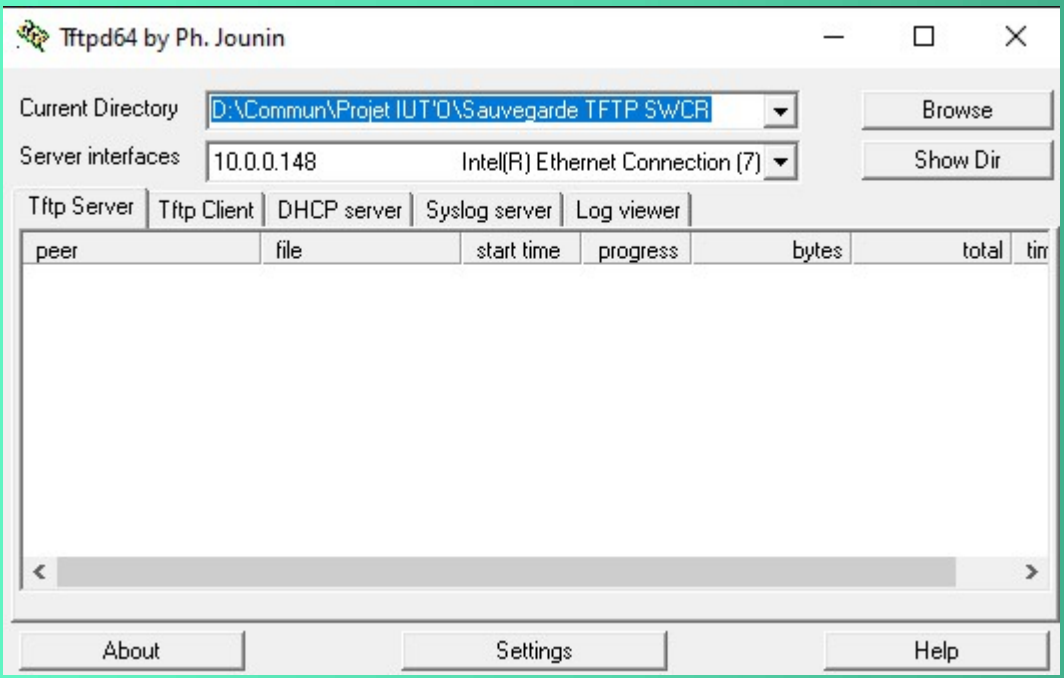
Pour se connecter à distance, il faut connecter le PC au switch avec un câble RJ 45 et ensuite en utilisant le logiciel PuTTY en utilisant son adresse IP.



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 ou sera enregistrer le fichier ainsi que l'interface réseau.



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

```
IUTO-SWCHI-03#copy startup-config tftp:
Address or name of remote host []? 10.0.0.148
Destination filename [iuto-swchi-03-confg]? vv
!!
4854 bytes copied in 0.033 secs (147091 bytes/sec)
```

Restauration d'une sauvegarde :

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

```
IUTO-SWCHI-03#copy tftp running-config
Address or name of remote host [10.0.0.148]?
Source filename [iuto-swchi-03-confg]? iuto-swchi-032-confg
Destination filename [running-config]?
Accessing tftp://10.0.0.148/iuto-swchi-032-confg...
Loading iuto-swchi-032-confg from 10.0.0.148 (via Vlan99): !
[OK - 4820 bytes]
```

Résumer de la configuration :

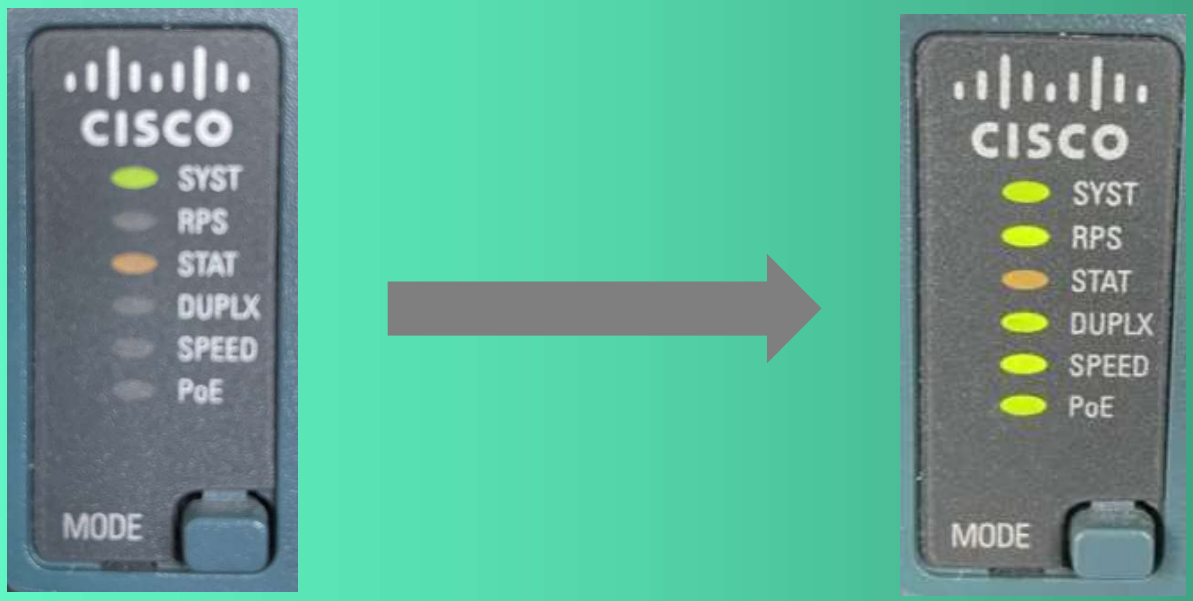
Mdp vty 0 = AzertyGT

Mdp en = AzertyGT45

CONFIGURATION DU SWITCH

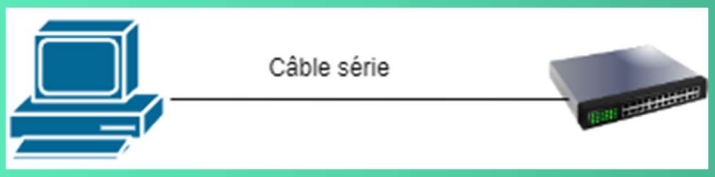
Procédure de réinitialisation :

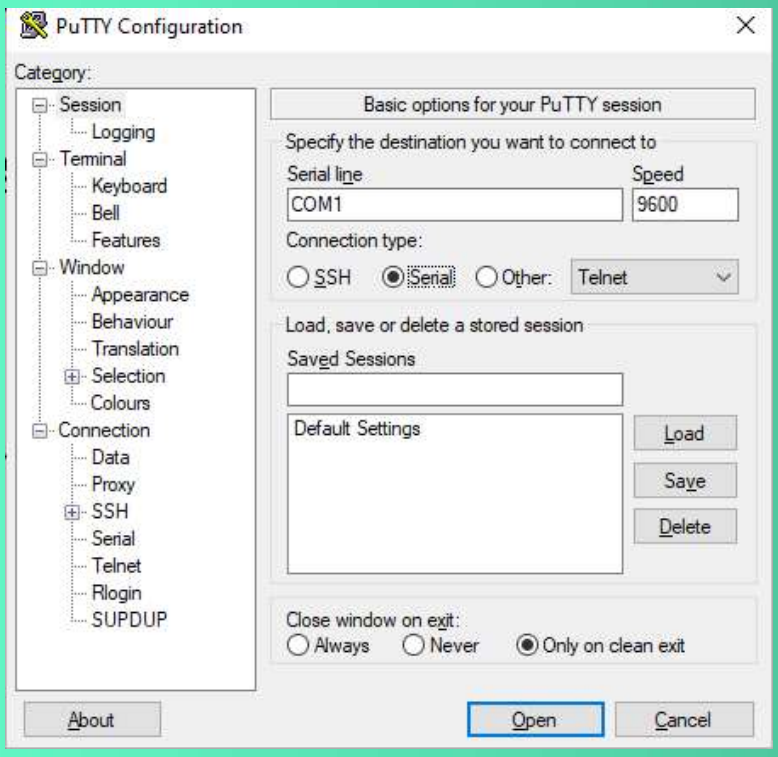
Pour réinitialiser le switch aux paramètres d'usine, il faut appuyer sur le bouton mode et maintenez-le enfoncé, les voyants LED du commutateur commencent à clignoter au bout de 3 secondes. Maintenez toujours le bouton mode enfoncé, les LED cessent de clignoter après 7 secondes supplémentaires puis le 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 IUTO-SWCR-03
```

Nous avons ajouté comme mot de passe ‘Azerty45’

```
IUTO-SWCR-03(config)#enable password AzertyGT45
IUTO-SWCR-03(config)#service password-encryption
```

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

```
IUTO-SWCR-03(config-line)#line vty 0
IUTO-SWCR-03(config-line)#password AzertyGT
```

Et ajouter une adresse IP

```
IUTO-SWCR-03(config)#interface vlan 1
IUTO-SWCR-03(config-if)#ip address 10.0.0.251 255.0.0.0
```

Pour enregistrer la configuration, il faut entrer cette commande :

```
IUTO-SWCR-03#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 l'IUTO 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

```
IUTO-SWCR-03(config)#vlan 10
IUTO-SWCR-03(config-vlan)#name DATA
IUTO-SWCR-03(config-vlan)#exit
IUTO-SWCR-03(config)#vlan 20
IUTO-SWCR-03(config-vlan)#name TELIP
IUTO-SWCR-03(config-vlan)#exit
IUTO-SWCR-03(config)#vlan 30
IUTO-SWCR-03(config-vlan)#name VISIO
IUTO-SWCR-03(config-vlan)#exit
IUTO-SWCR-03(config)#vlan 40
IUTO-SWCR-03(config-vlan)#name WIFI
IUTO-SWCR-03(config-vlan)#exit
```

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

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

Ajout des ports dans leur VLAN respectif :

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

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

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

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

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

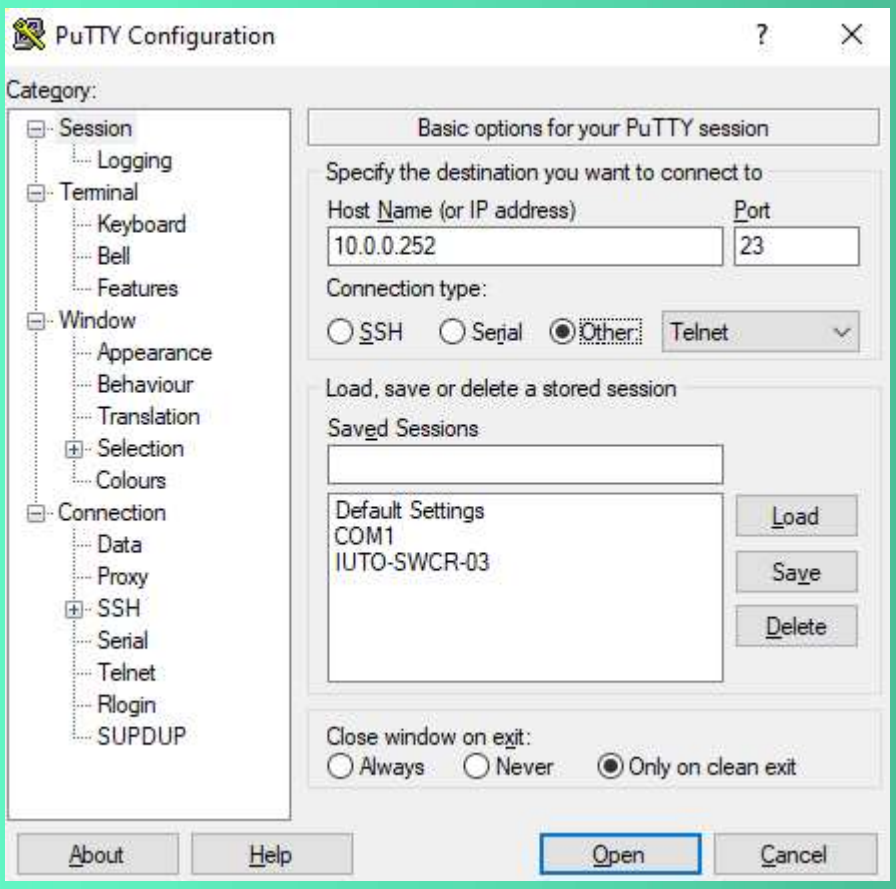
```
BEG-SW-031(config)#interface range fastEthernet 0/22-23
BEG-SW-031(config-if-range)#switchport mode access
BEG-SW-031(config-if-range)#switchport access vlan 30
BEG-SW-031(config-if-range)#shutdown
```

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

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

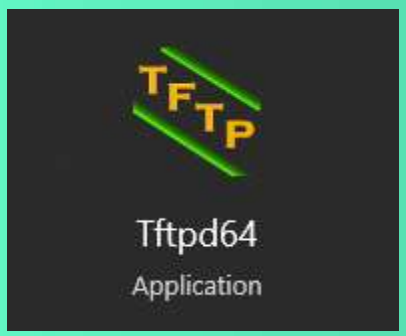
Comment se connecter à distance :

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

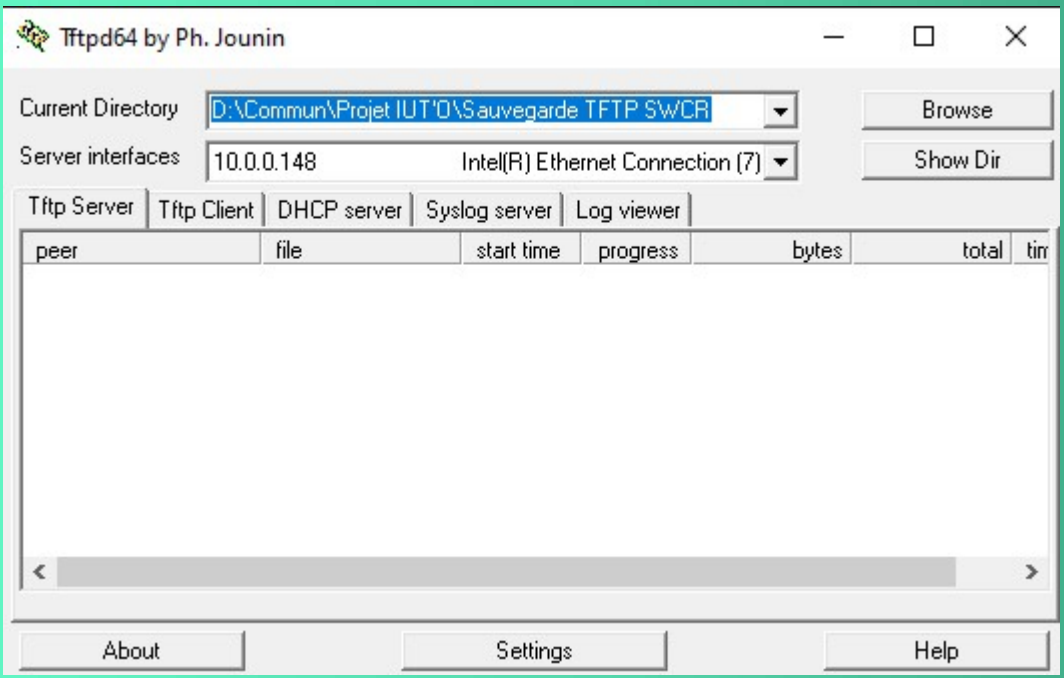


Sauvegarde TFTP :

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



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



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

```
IUTO-SWCR-03#copy startup-config tftp
Address or name of remote host []? 10.0.0.148
Destination filename [iuto-swcr-03-confg]?
!!
2192 bytes copied in 1.015 secs (2160 bytes/sec)
```

Restauration d'une sauvegarde :

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

```
IUTO-SWCR-03#copy tftp running-config
Address or name of remote host [10.0.0.148]?
Source filename [iuto-swcr-03-fonctionnel-config]? iuto-swcr-03-fonctionnel-confg
Destination filename [running-config]?
Accessing tftp://10.0.0.148/iuto-swcr-03-fonctionnel-confg...
Loading iuto-swcr-03-fonctionnel-confg from 10.0.0.148 (via Vlan1): !
[OK - 2192 bytes]
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 5 seconds)
```

Résumer de la configuration :

Mdp vty 0 = AzertyGT

Mdp en = AzertyGT45

CONFIGURATION EXTERNE

Réinitialisation du boitier :

Appuyez et maintenez enfoncé le petit point situé à droite du boîtier à l'aide d'un stylo pendant 5 à 10 secondes, jusqu'à ce que les voyants "Online" et "Status" se mettent à clignoter.

Attendez 5 minutes :

Résultat lorsque tout est correct :

CONNEXION WEB :

Connexion à distance :

Brancher un câble RJ45 sur l'un des ports LAN et un autre câble sur le port WAN du réseau de la salle

Ouvrez un navigateur et saisissez :

https://10.0.0.254/admin

Attention, votre adresse IP doit impérativement être en /24 dans la configuration de base

Login : admin
Password : admin

CONFIGURATION DU STORMSHIELD :

Une fois connecté, vous serez dirigé vers l'interface du Stormshield, où vous pourrez accéder à toutes les options de configuration et de gestion de votre pare-feu

Obtenez les droits de modification :

Cliquez sur les 2 boutons situés sous l'inscription "admin" en haut à droite

Configuration du nom du firewall :

Accédez à **"CONFIGURATION"** en haut de l'écran, puis naviguez dans le menu de gauche en cliquant sur **"Configuration"**, **"Système"**, **"Configuration"** et **"Configuration générale"**

Dans **"Configuration générale"**, modifiez le champ **"Nom du Firewall"**

Vous pouvez également modifier la langue du firewall et le clavier en sélectionnant **"Français"**

Confirmez la modification

Configuration de l'heure (NTP) :

Accédez à **"CONFIGURATION"** en haut de l'écran, puis naviguez dans le menu de gauche en cliquant sur **"Configuration"**, **"Système"**, **"Configuration"** et **"Configuration générale"**

Dans les **"Paramètres de date et d'heure"**, cochez la case **"Maintenir le firewall à l'heure (NTP)"** et, dans la section **"Fuseau horaire"**, sélectionnez **"Europe/Paris"**

Dans la liste des serveurs NTP, cliquez sur **"+ Ajouter"**

Ajoutez ensuite les deux serveurs NTP de Stormshield suivants :

ntp1.stormshieldcs.eu

ntp2.stormshieldcs.eu

Confirmez la modification

Modification du password admin :

Accédez à **"CONFIGURATION"** en haut de l'écran, puis naviguez dans le menu de gauche en cliquant sur **"Configuration"**, **"Système"**, **"Administrateurs"** et **"Compte Admin"**

Dans **"Authentification"** saisissez l'ancien mot de passe, qui est **"admin"** (mot de passe par défaut)

Saisissez le nouveau mot de passe : **"Azerty45GT"**

Confirmez la modification

Nouveaux identifiants de connexion :

Login : admin

Password : Azerty45GT

Mise en place de la règle de NAT :

Accédez à **"CONFIGURATION"** en haut de l'écran, puis naviguez dans le menu de gauche en cliquant sur **"Configuration"**, **"Politique de sécurité"**, **"Filtrage et NAT"**

Tout en haut, l'option **"(1) Block all"** est sélectionnée. Modifiez-la en **"(10) Pass all"**

Confirmez la modification

Dans la section **"NAT"**, cliquez sur **"+ Nouvelle règle"**, puis dans le menu déroulant, sélectionnez **"Nouvelle règle de partage d'adresse source (masquerading)"**

Sur la nouvelle règle cliquez sur le **"Port src"**. Dans la section **Général**, pour le champ **"Port machine source translatée"**, sélectionnez **"Firewall_out"** faire **OK**

Ensuite, cliquez sur **"Source"**. Dans la section **"Trafic après translation"**, sous **Général**, pour le champ **"Port source translaté"**, choisissez **"none"** faire **OK**

N'oubliez pas de mettre l'état en mode **"On"**

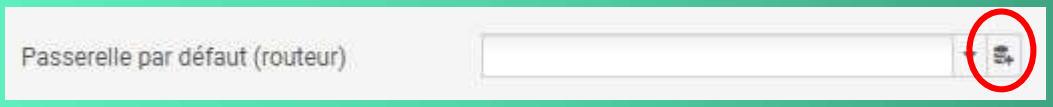
Confirmez la modification

Configuration de la passerelle :

Accédez à **"CONFIGURATION"** en haut de l'écran, puis naviguez dans le menu de gauche en cliquant sur **"Configuration"**, **"Réseau"**, **"Routage"** et **"Routes statiques IPV4"**

Dans **"Configuration générale (routeur)"**, modifiez le champ **"Passerelle par défaut"**

Faites un clic droit sur le logo **"Ajout d'objet"**



Entrez le nom du nouvel objet, puis l'adresse IPv4, qui sera **172.20.2.254** dans notre cas.

Confirmez la modification

Configuration des adresses IP :

Accédez à **"CONFIGURATION"** en haut de l'écran, puis naviguez dans le menu de gauche en cliquant sur **"Configuration"**, **"Système"**, **"Réseau"** et **"Interfaces"**

Retrait des interfaces des bridges :

Maintenez l'interface sélectionnée et faites-la glisser vers la zone libre (blanche) située juste en dessous

Suppression du bridge :

Effectuez un clic droit sur le bridge, puis sélectionnez "SUPPRIMER"

Dans cet exemple, le réseau LAN est configuré en 10.0.0.0/8 et le réseau WAN en 172.20.0.0/16

Configuration de l'interface IN (port LAN) :

I. Double-cliquez sur l'interface IN
II. Dans la section **"Paramètres généraux"**, choisissez **"Interne"**
III. Dans la section **"Plan d'adressage"**, sélectionnez **"Dynamique / Statique"**
IV. Cliquez sur **"+ Ajouter"**
V. Entrez l'adresse IP suivante : **10.0.0.254/8**

Configuration de l'interface OUT (port WAN) :

I. Double-cliquez sur l'interface OUT
II. Dans la section **"Paramètres généraux"**, choisissez **"Externe"**
III. Dans la section **"Plan d'adressage"**, sélectionnez **"Dynamique / Statique"**
IV. Cliquez sur **"+ Ajouter"**
V. Entrez l'adresse IP suivante : **172.20.203.100/16**

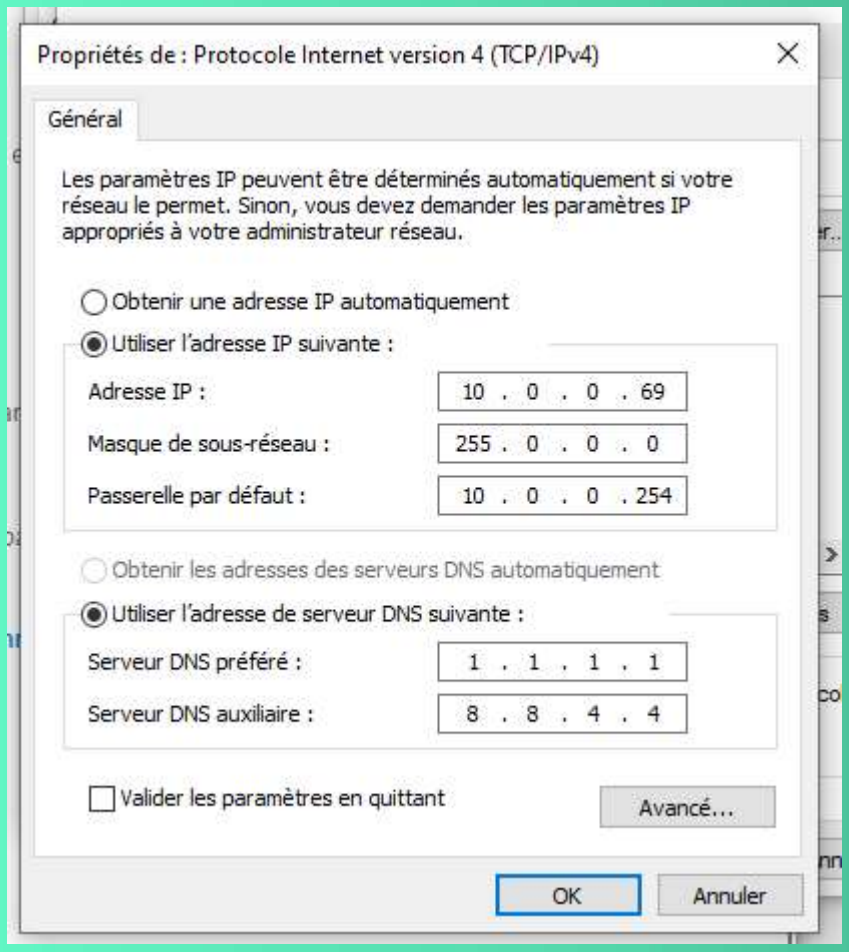
Confirmez la modification

Configuration du PROXY :

Accédez à **"CONFIGURATION"** en haut de l'écran, puis naviguez dans le menu de gauche en cliquant sur **"Configuration"**, **"Security Policy"** et **"Filtering"**

Confirmez la modification

Configuration de mon pc

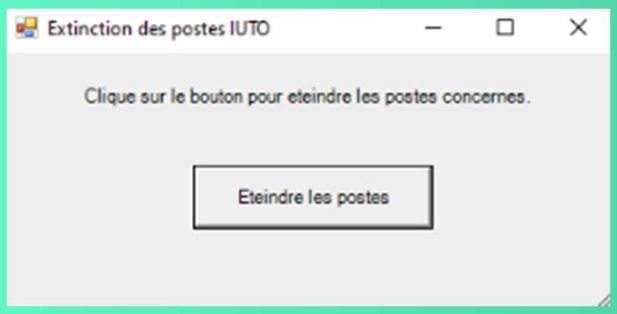


ÉTEINDRE AUTOMATIQUEMENT LES POSTES CLIENTS

J'ai réalisé deux scripts pour éteindre automatiquement des postes à partir de leur nom

Shutdown-IUTO-GUI.ps1 :

Ce script génère un bouton qui demande la confirmation pour éteindre les postes concernés



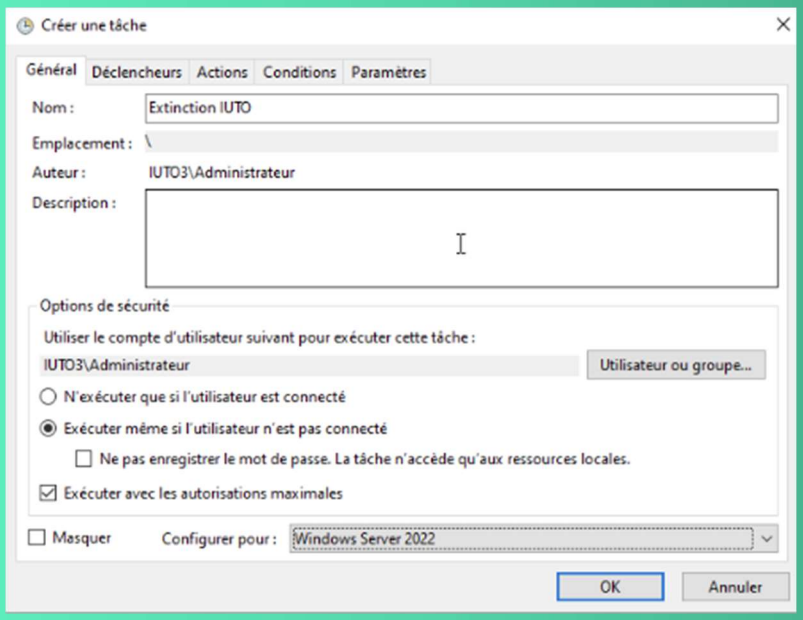
Shutdown-IUTO-AUTO.ps1 :

Ce script va nous servir à éteindre automatiquement les machines à une certaine heure

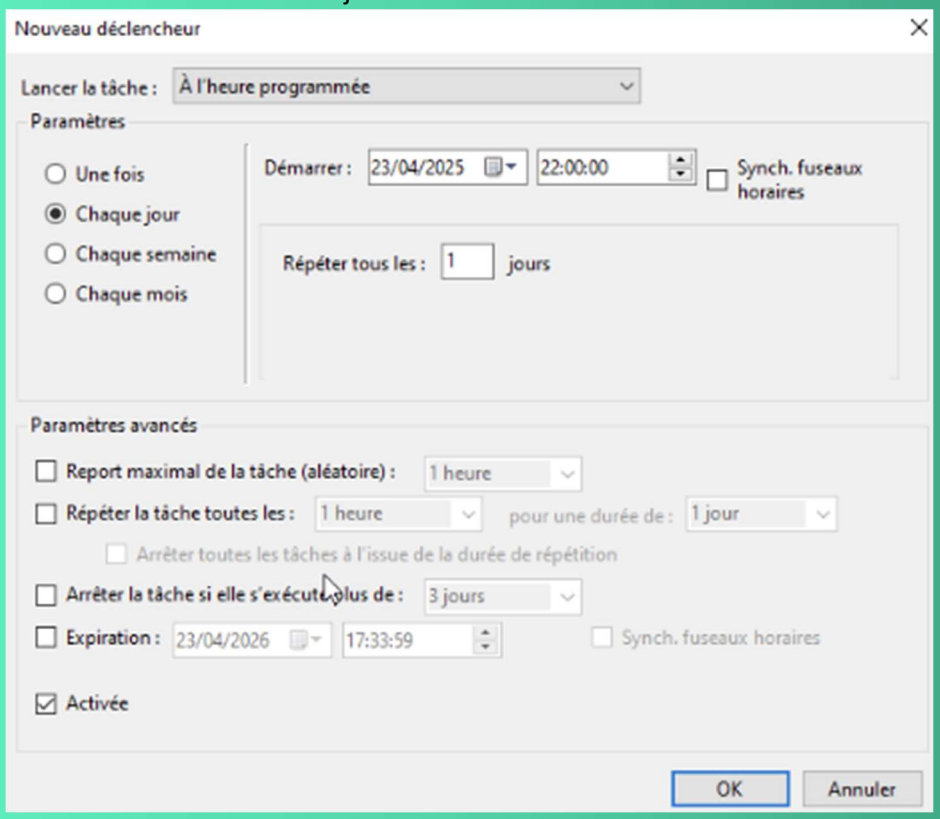
Automatiser l'exécution du script :

1. Ouvrir le panificateur de taches (taskschd.msc)
2. Cliquer sur "Créer une tâche"

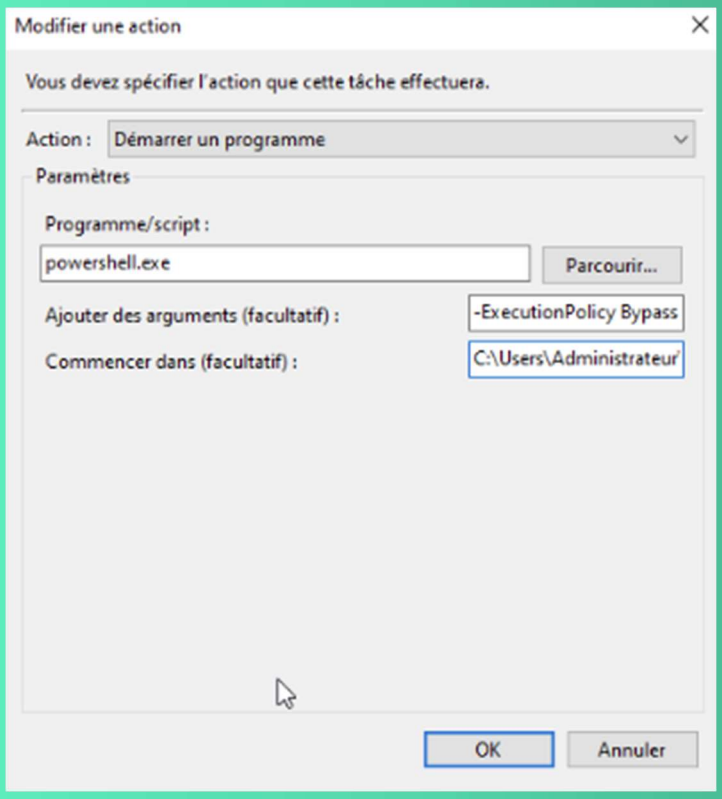
3. Onglet Général:
    a. Nom: Extinction IUTO
    b. Exécuter avec les autorisations maximales et même si l'utilisateur n'est pas connecté et sélectionner Configurer pour : Windows Server 2022



4. Onglet Déclencheurs:
    a. Nouveau > Début: “Tous les jours” > Heure



5. Onglet Actions:
    a. Action: Démarrer un programme
    b. Programme/script: powershell.exe
    c. Ajouter des arguments: -ExecutionPolicy Bypass -File “C:\Users\Administrateur\Desktop\Shutdown-IUTO-AUTO.ps1



6. Onglet Conditions:
    a. Tu peux cocher/décocher selon besoin
7. Onglet Paramètres:
    a. Coche “Exécuter la tâche dès que possible si un démarrage est manqué”