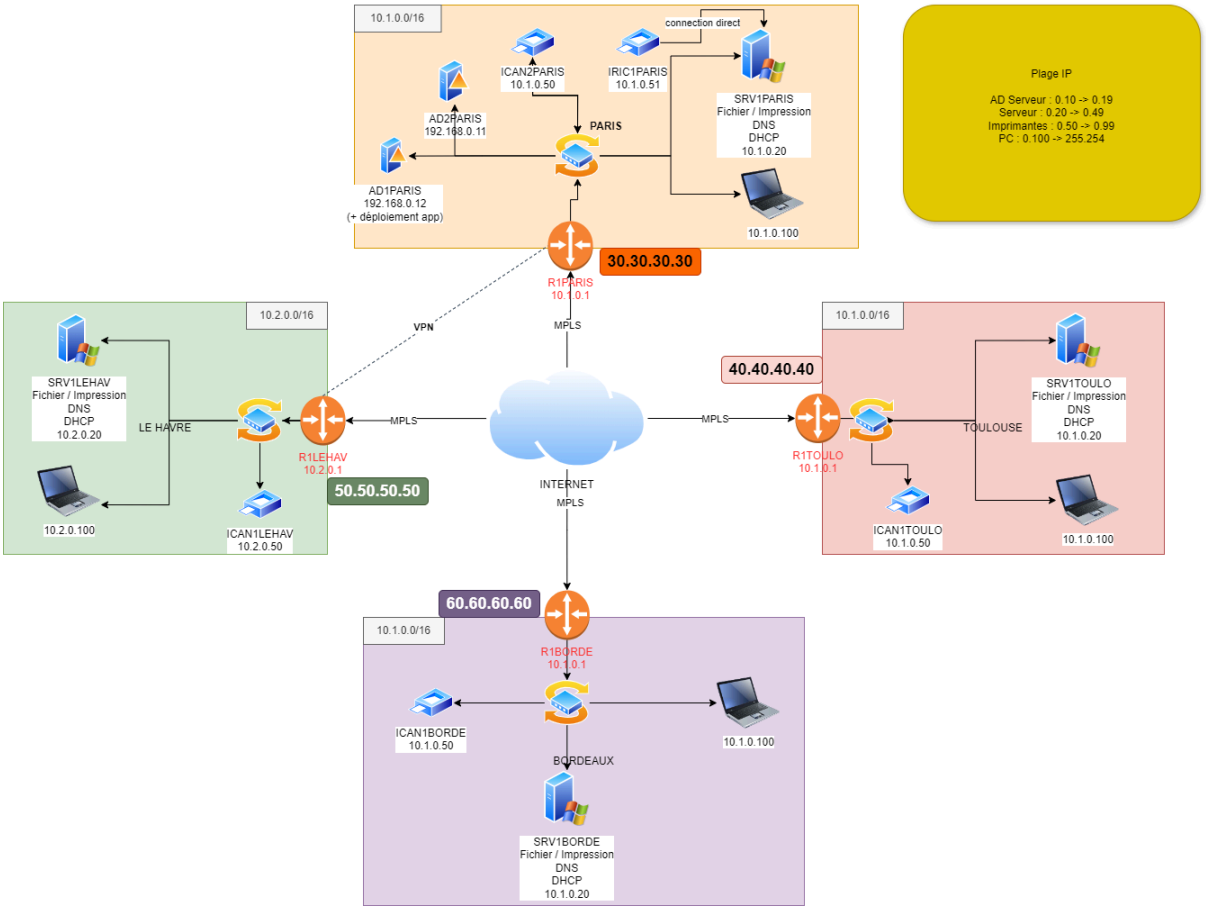
Mise en oeuvre d'une infrastructure Windows Serveur

I - Mise en place et configuration du parc

A - Schéma de l'infrastructure

Voici mon schéma du l'énoncé. On y retrouve les 4 sites et les différents périphériques finaux ainsi que leurs adresses IP.



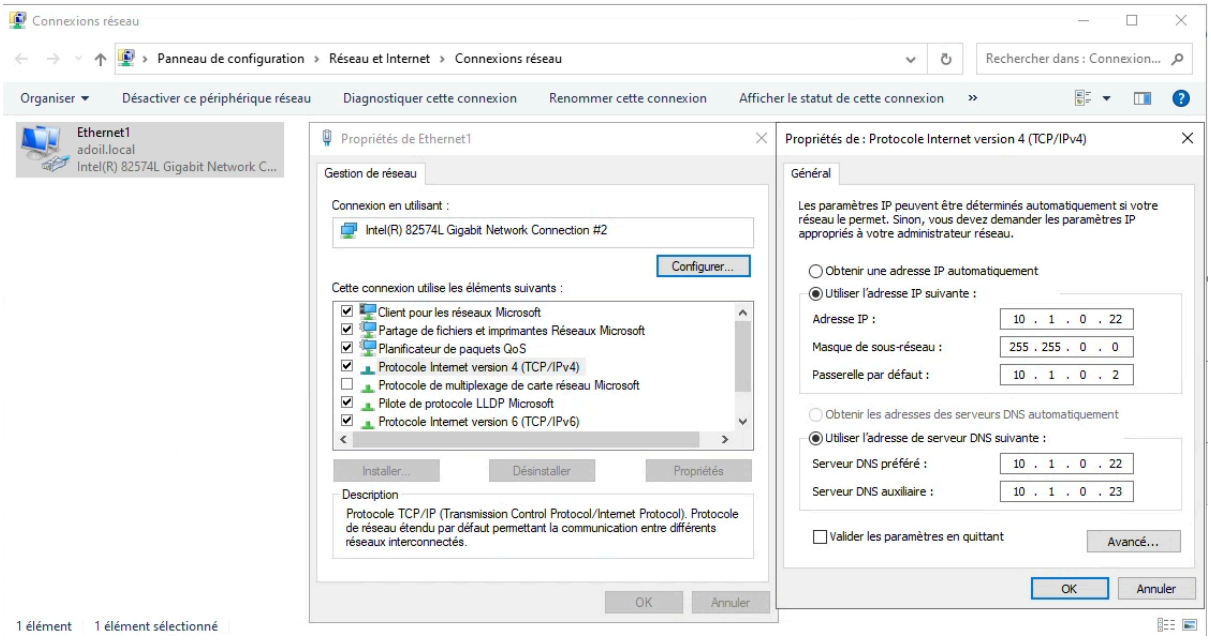
B - Mise en place SRV1PARIS

Pour commencer, je vais préciser que toutes les machines virtuelles (abrégé en VM) sont créées et gérées par VMWare WorkStation Pro 17. L'installation des VM ne sera pas montrée ici, uniquement la configuration.

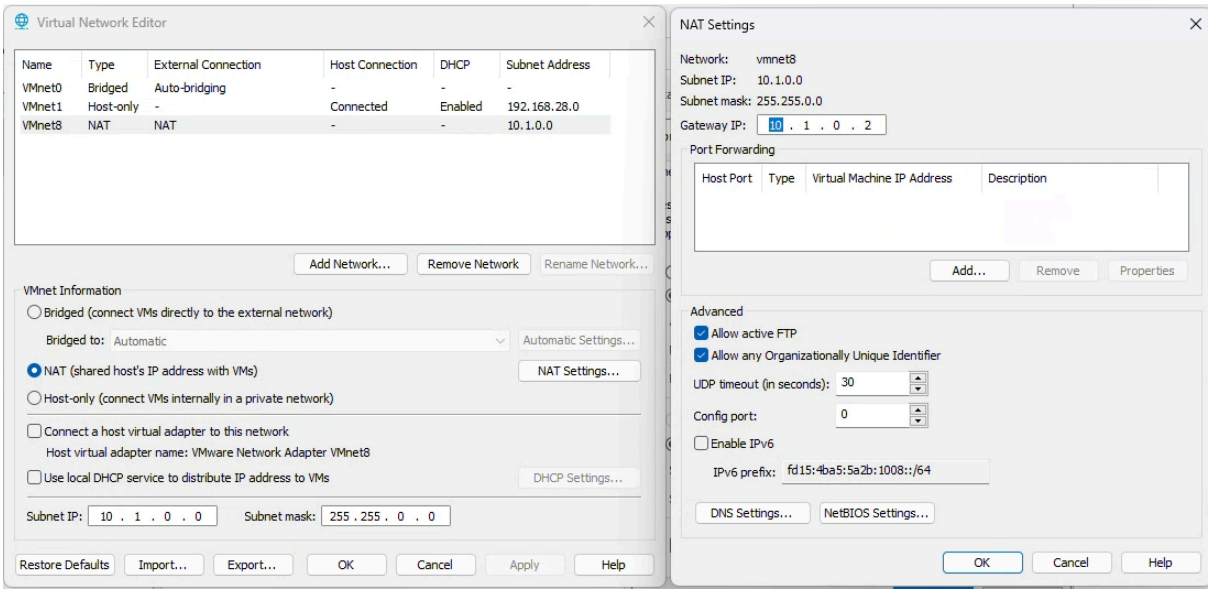
La première étape est la mise en place du DNS sur PARIS.

Il faut tout d'abord penser a mettre une IP Statique sur le serveur (toujours le faire sur les serveurs, l'IP ne doit pas être modifié). Dans notre cas : 10.1.0.22

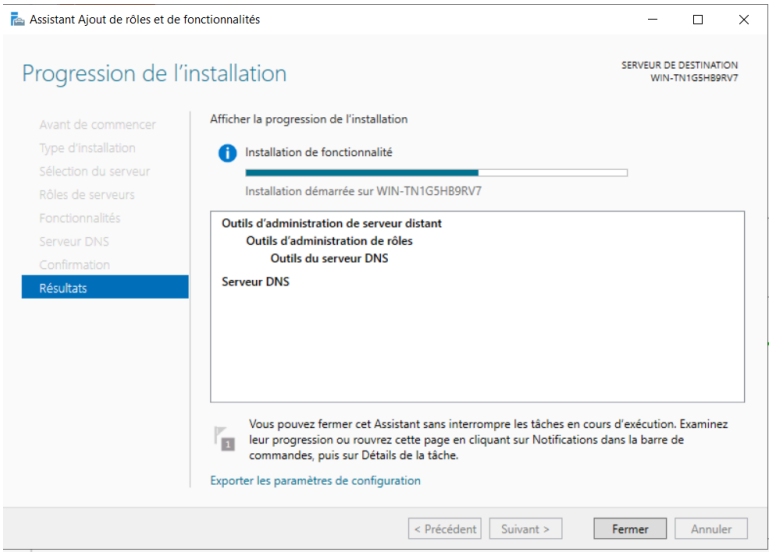
```
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::898f:21f6:7964:ce25%2
   Adresse IPv4. . . . . . . . . . . . . .: 10.1.0.22
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 10.1.0.2
```



La passerelle par défaut est 10.1.0.2 car c'est comme cela que VMWare le gère. D'ailleurs, voici la configuration du réseau via VMWare :

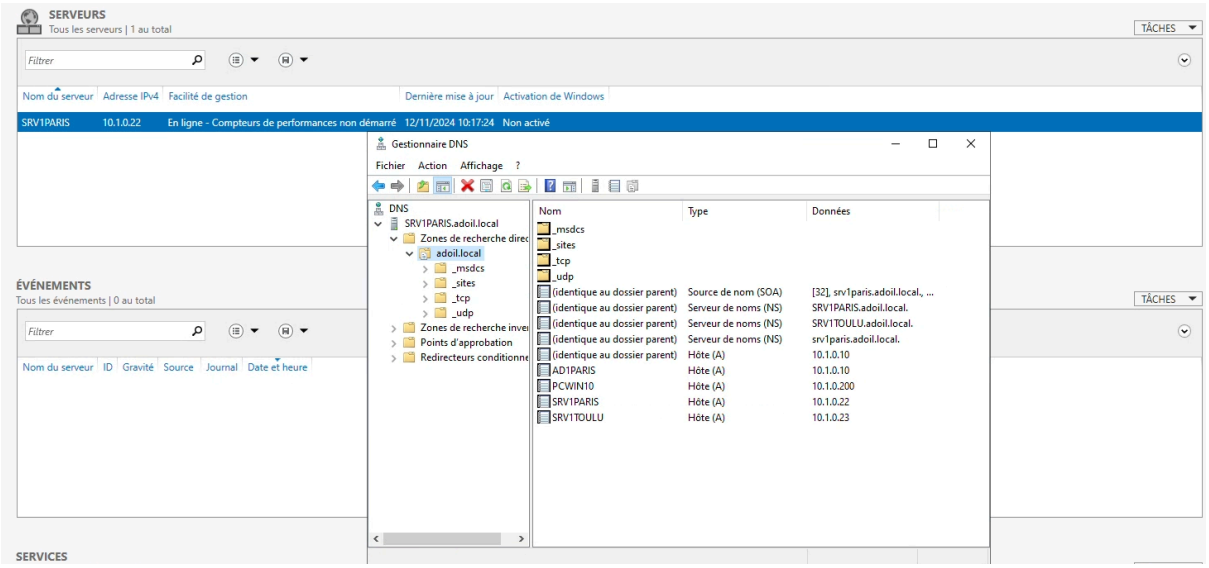


Ensuite on ajoute le rôle DNS grâce au gestionnaire de serveur.

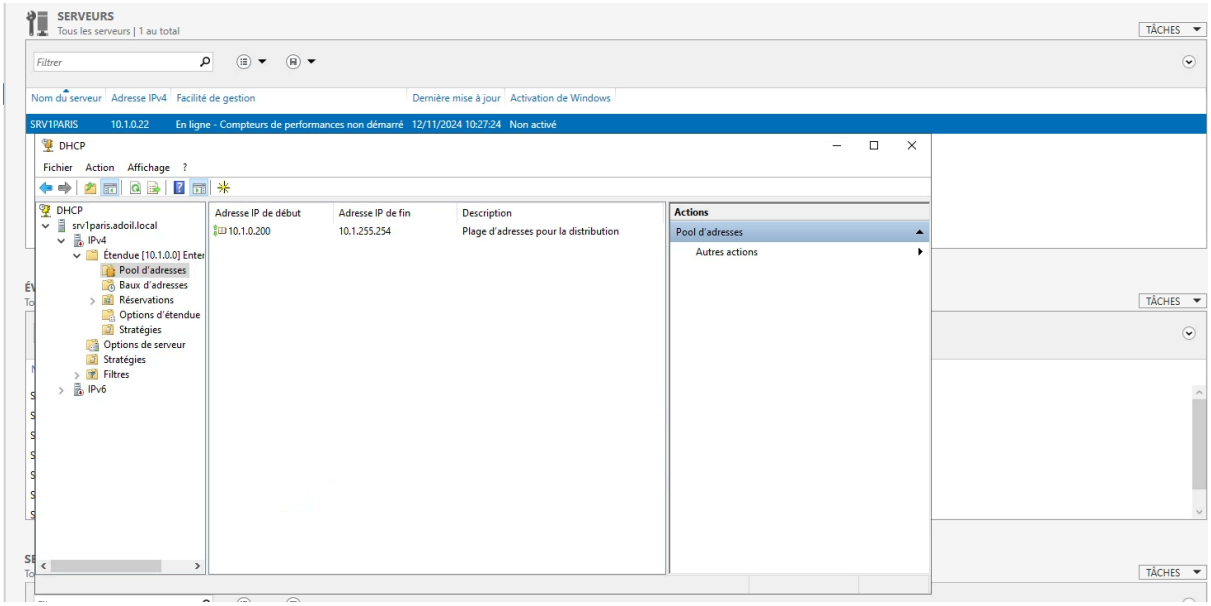


On va ouvrir le gestionnaire DNS pour créer notre première zone de recherche directe et inversée. Le nom de notre domaine sera : adoil.local

Voici le gestionnaire après la création des deux zones.



Puis le rôle DHCP :
On ouvre le gestionnaire DHCP et on crée notre étendue de poste conforme à notre schéma.



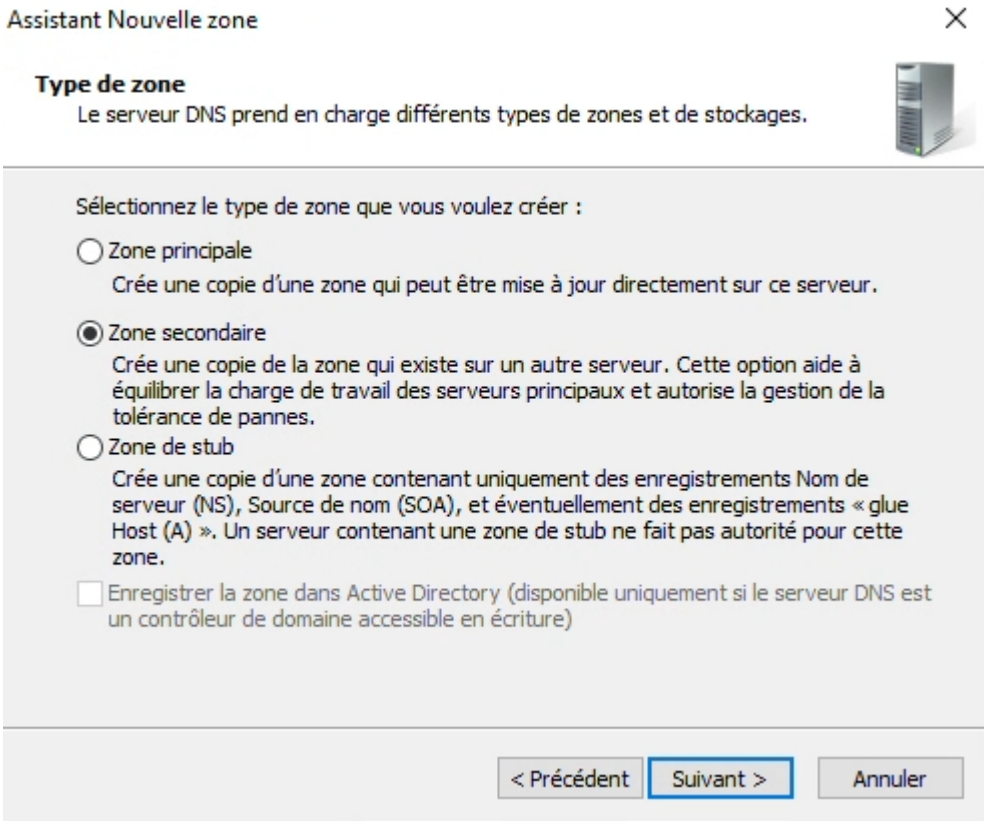
La plage de poste sera donc de 10.1.0.200 à 10.1.255.254

Voici pour notre serveur de Paris (pour l'instant).

C - Mise en place de SRV1TOULO

La mise en place ressemble à celle de Paris. En effet, il sera un DNS Secondaire dans notre cas.

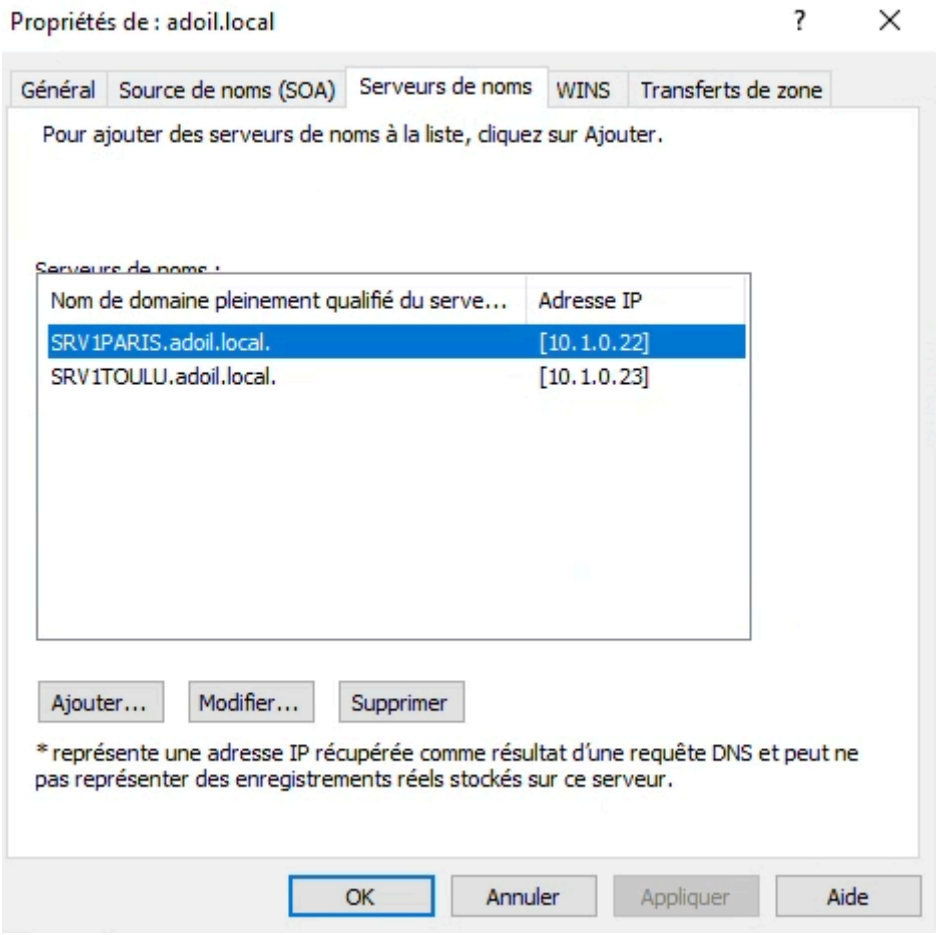
On ajoute donc le rôle DNS (pensez à l'IP Statique, qui sera 10.1.0.23)
Mais cette fois-ci, on crée une plage secondaire et non primaire.



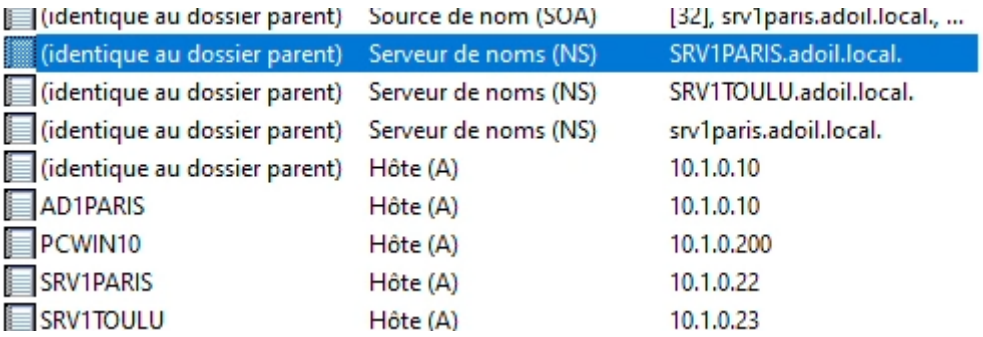
PS : Pensez à rajouter, sur SRV1PARIS, l'adresse IP de SRV1TOULO en tant que DNS Secondaire.

On sélectionne bien notre SRV1PARIS (et le nom de domaine) lors de la création de la plage pour que les deux se lient.

Une fois fait, on retourne donc sur SRV1PARIS pour configurer les serveurs de noms (pensez à bien mettre des noms FQDN)

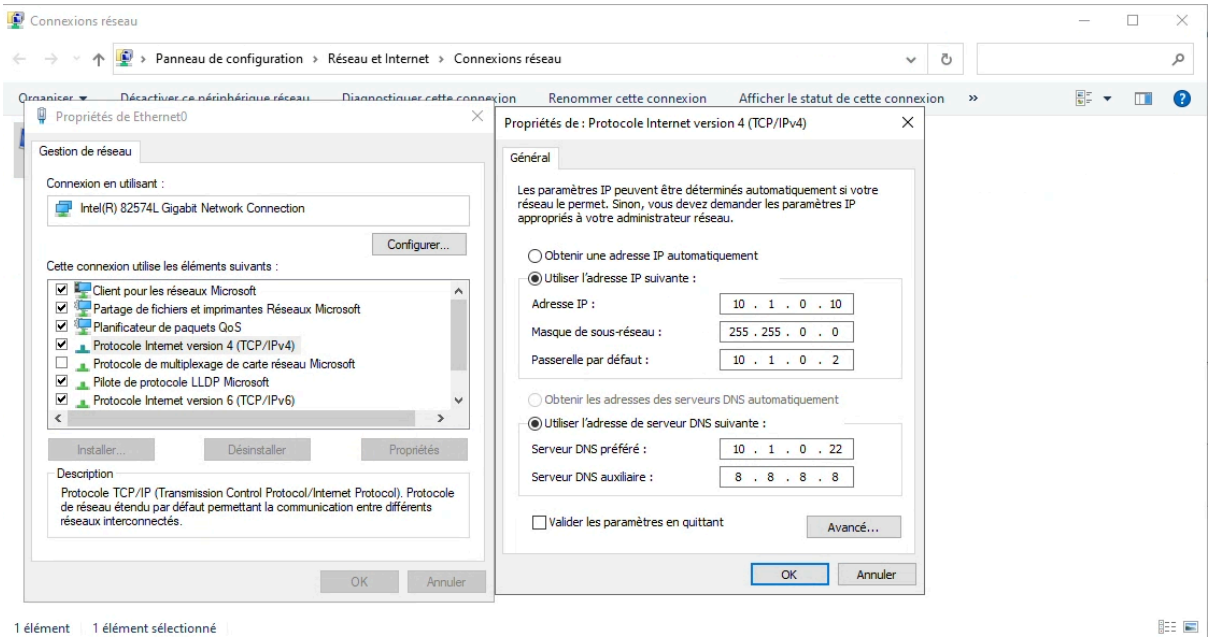


Si la connection s'effectue, le DNS de paris devrait ressembler à ça :

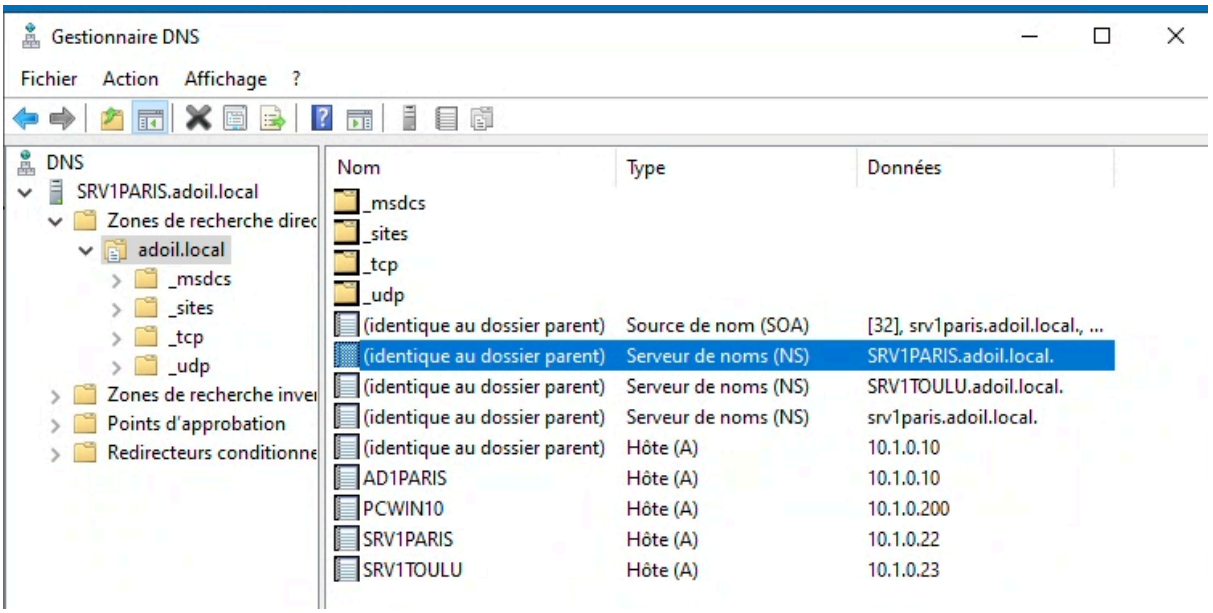


D - Mise en place de AD1PARIS

On installe le rôle AD DS sur cette VM
Pensez à mettre une IP statique : 10.1.0.10 et de bien mettre l'adresse IP du DNS de Paris.



Lorsque cela sera fait, on test si la connection est bonne en allant voir le DNS de Paris :



Les dossiers de l'Active Directory apparaissent donc la liaison est opérationnelle.

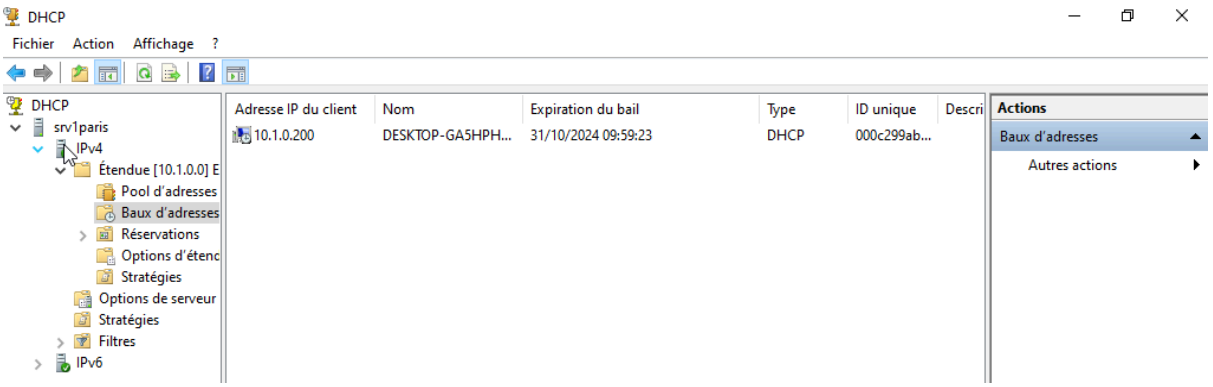
E - Poste Client

La dernière VM sera un poste client basique en Windows 10.

On va le connecter à notre domaine et voir si le DHCP a bien marché.

```
Microsoft Windows [version 10.0.19045.2846]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\SallarZ>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : adoil.local
   Adresse IPv6 de liaison locale. . . . .: fe80::880e:6879:8ba3:5d2c%5
   Adresse IPv4. . . . . . . . . . . . . .: 10.1.0.200
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 10.1.0.2

C:\Users\SallarZ>
```

On peut voir que le poster a bien pris la première adresse IP disponible de la plage.



F - Derniers changements

Maintenant que toutes les liaisons sont ok, il faut mettre tous nos machines dans le domaine ADOIL.local

II - Configuration des solutions

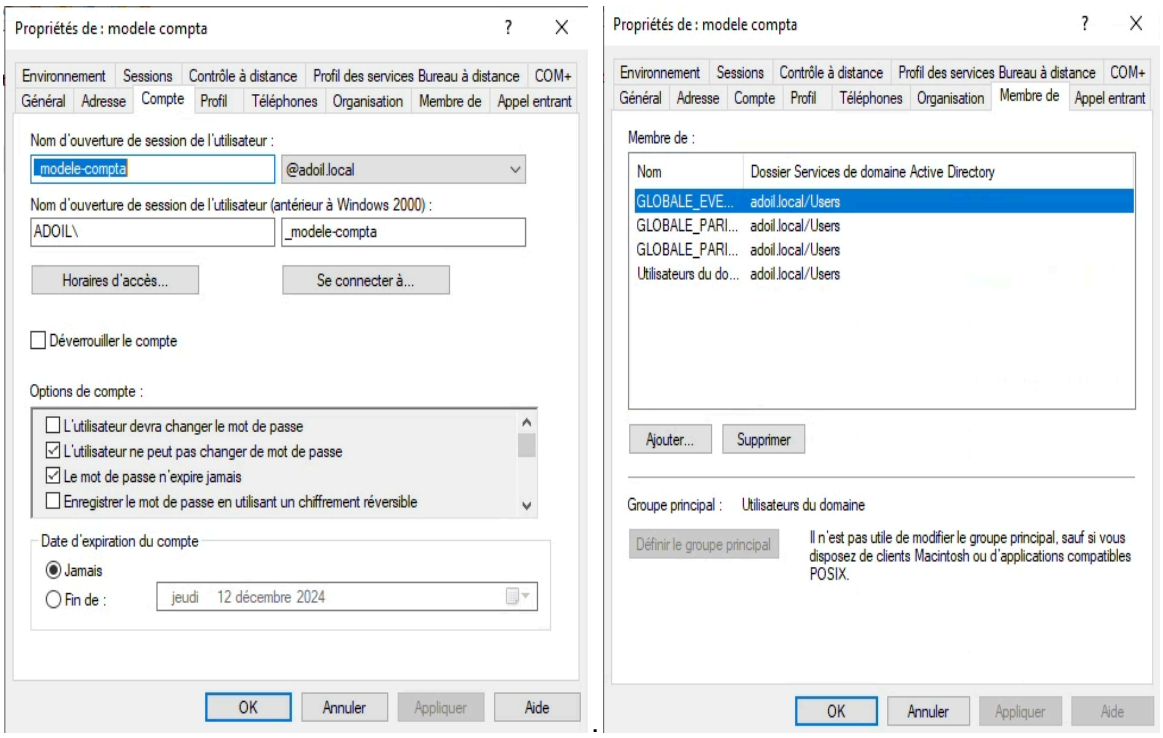
Contrainte n°1 :

"Pour la création des utilisateurs, des modèles seront créés pour les différents types d'utilisateurs : direction, R&D, informatique, communication, comptabilité. Les comptes de login seront de la forme NOM suivi de 1ere lettre du prénom"

Pour ma part, je vais créer les utilisateurs/modèles dans l'Active Directory.

Tout d'abord, je vais créer diverses OU pour mieux ranger les utilisateurs.
Puis créer des groupes globaux pour chaque service (un Read et un Write)

Ensuite je vais créer un utilisateur modèle dans son OU correspondante. (modèle comptabilité dans l'exemple ci-dessous)



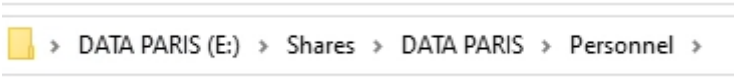
Il faut bien penser à ajouter les divers groupes globaux auxquels le modèle se trouve pour éviter de refaire cette opération à chaque création.

Contrainte n°2 :

"*Chaque utilisateur aura à sa disposition un répertoire de base stocké sur les serveurs de fichiers mappé en U*"

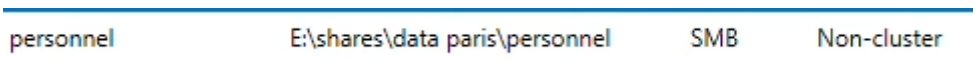
On va créer un disque dur DATAPARIS qui va stocker toutes les données de ce site. (bien sûr, tout est a refaire sur Toulouse)
Pour cela, on utilise VMWare et on ajoute un disque virtuel de 10GO.

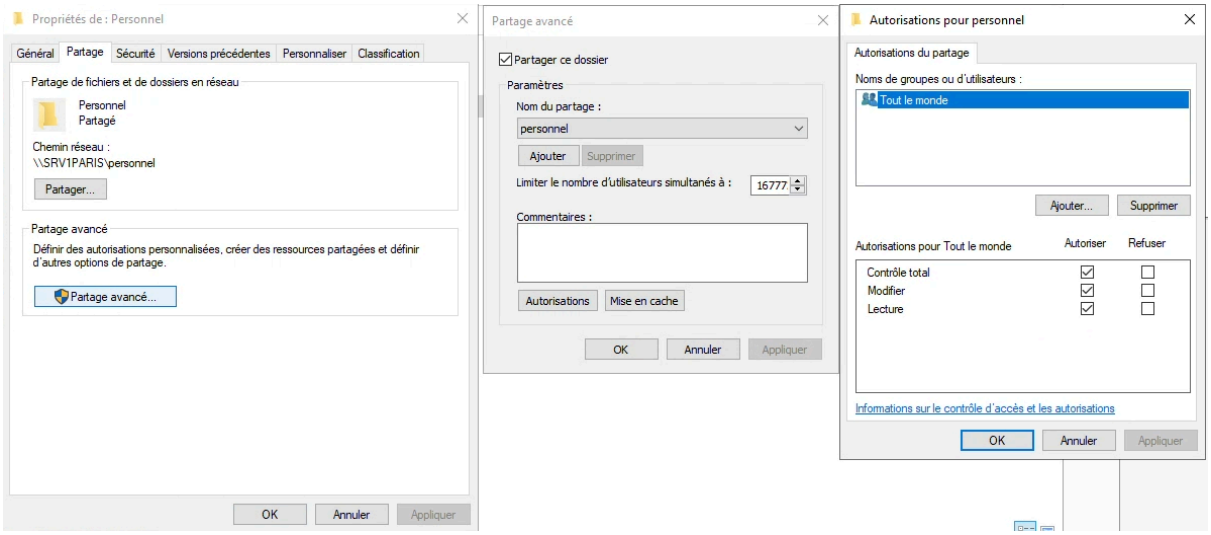
On formate le disque pour qu'il soit utilisable puis on créer dossier "Personnel"



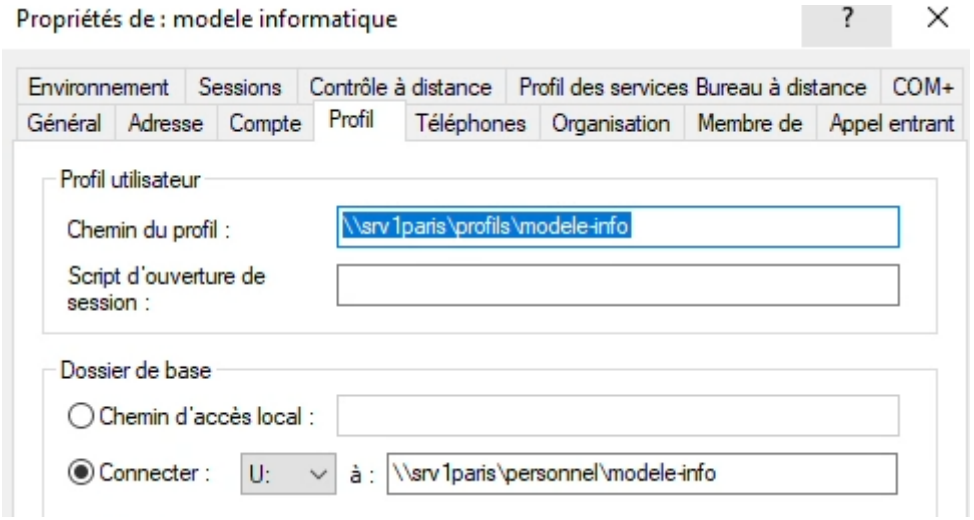
Ensuite on installe le rôle "Services de fichiers et de stockage"

On va ensuite partager le dossier Personnel grâce au services de fichiers



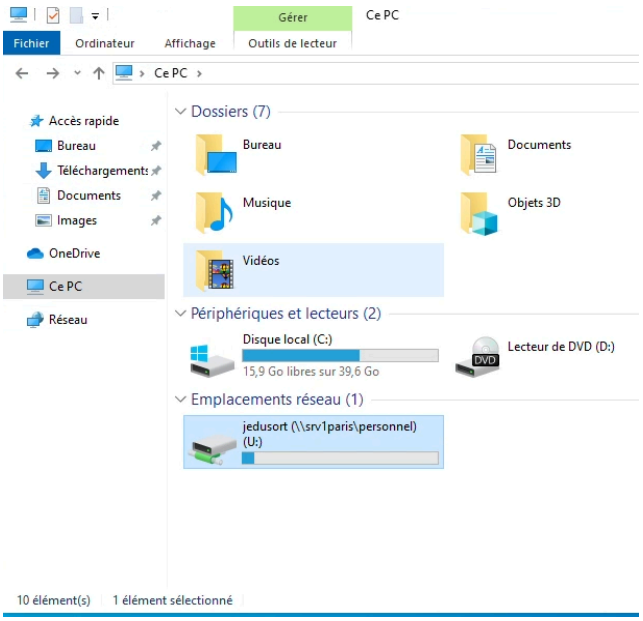


Je crée un utilisateur via modèle.



PS : A la place de modele-info, il faut mettre %USERNAME%

J'ai donc ajouté l'utilisateur Jack DANIEL (danielj) et ouvert sa session, sur laquelle je peux voir le disque et je peux interagir avec.

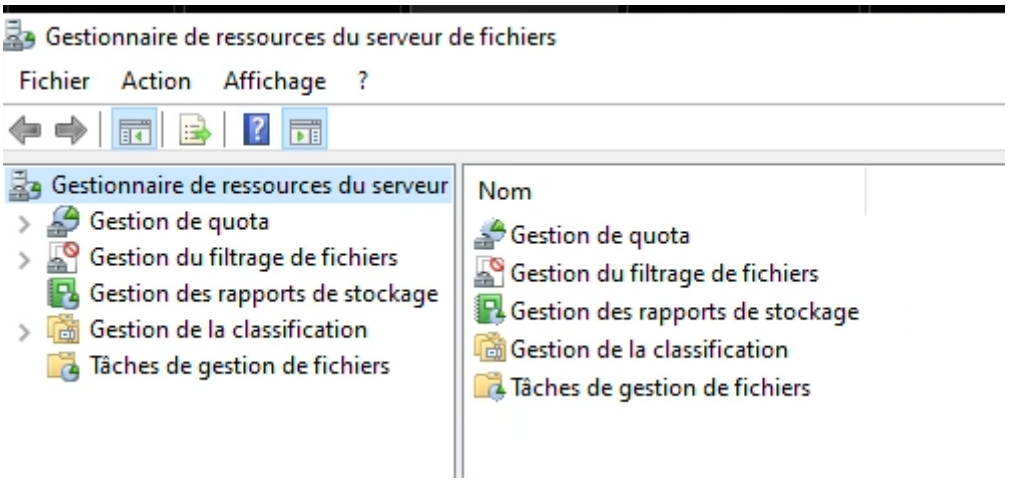


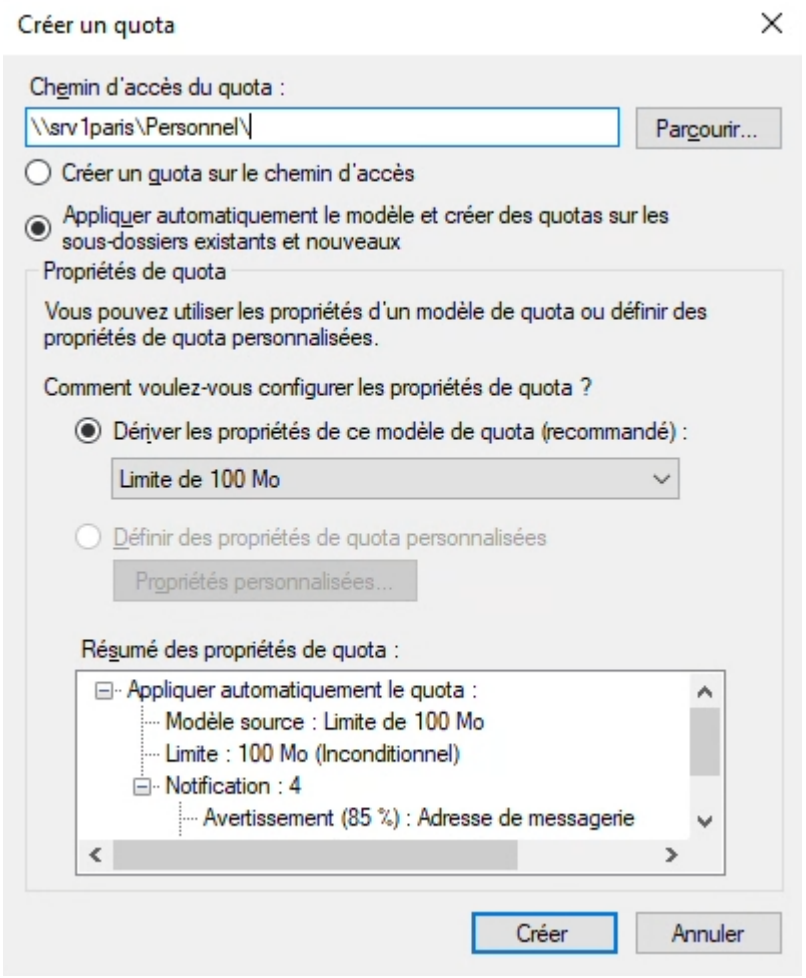
Contrainte n°3 :

"*Les utilisateurs ne pourront pas stocker sur leur lecteur plus de 100MO chacun.*"

Il faut cependant que celui-ci soit de 100M max.

J'installe donc le rôle de gestionnaire de ressources sur le srv1paris et je détermine un quota sur le dossier.





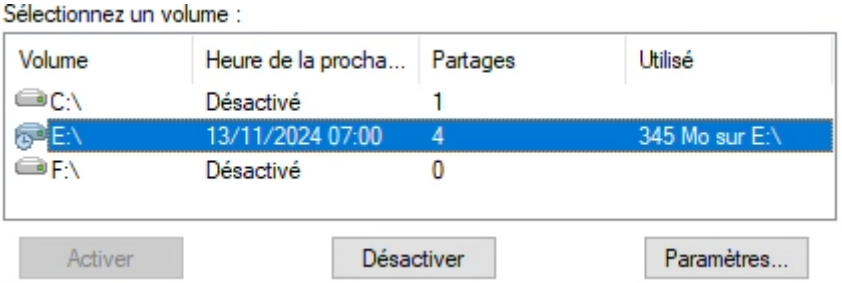
Le volume U: est donc initialisé pour tout les utilisateurs et possède son stockage max.

Contrainte n°4 :

“*Chaque utilisateur pourra restaurer les anciennes versions de ses fichiers.*”

Il faut configurer les clichés instantanés.

Pour cela, il suffit de faire clic droit sur DATAPARIS et “Configurer les clichés instantanés”



On suit l’utilitaire et la restauration de fichier sera OK.

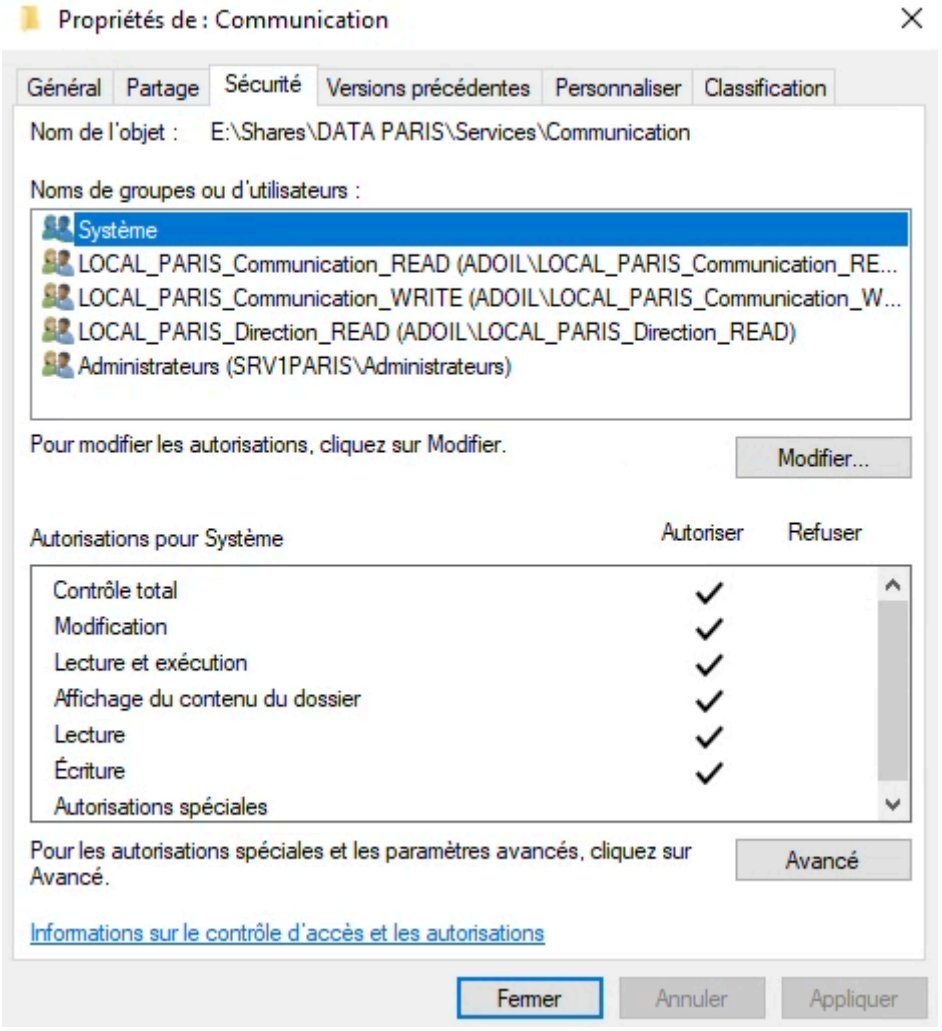
Contrainte n°5 :

“ Chaque service (direction, R&D, informatique, communication, comptabilité) aura à sa disposition un lecteur partagé S: stocké sur les serveurs de fichiers. Ce lecteur sera connecté automatiquement par script. Chaque dossier de service sera limité en taille et ne pourra dépasser 20 GO. Seuls les membres du service pourront accéder à leur répertoire de service. Le service direction pourra visualiser l’ensemble des dossiers. Les utilisateurs ne verront que les dossiers pour lesquels ils ont les droits d’accès.”

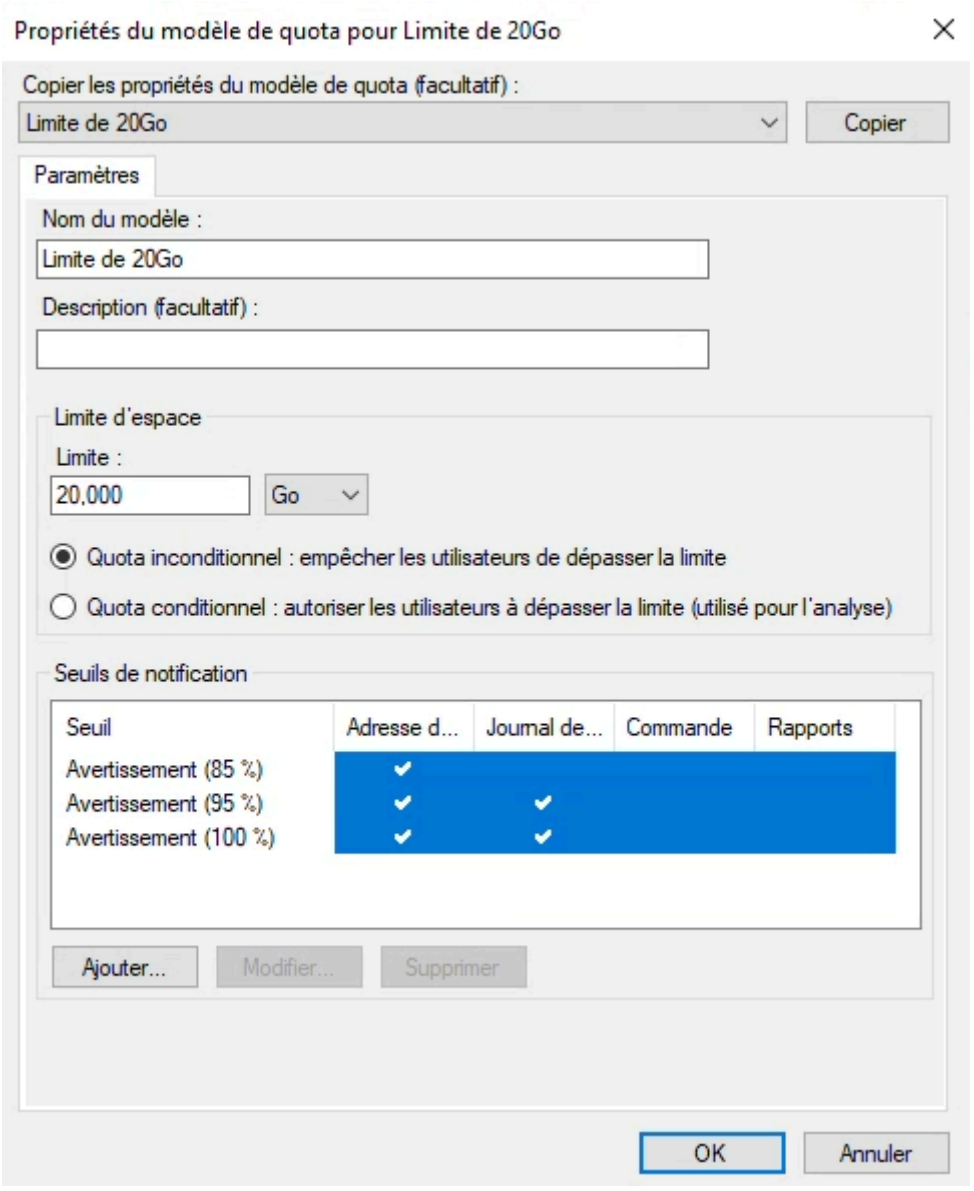
On va commencer par créer des dossiers pour chaque service et configurer des accès pour chaque services.

Dans l’exemple, on va prendre le service “Communication”. On va lui affecter les groupes de domaine local (en effet, le dossier étant une ressource, on utilisera donc des groupes de domaine local)

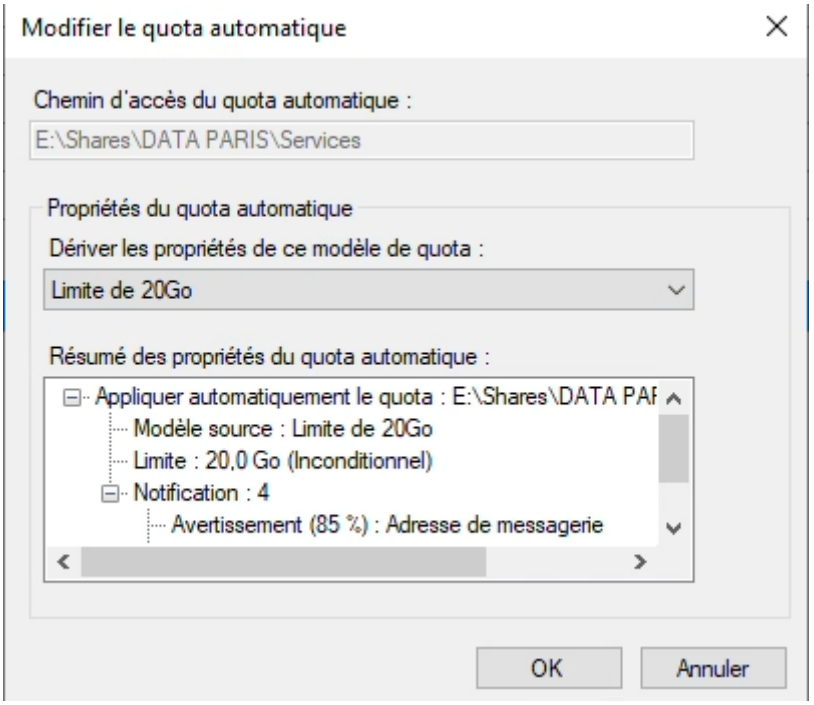
Je lui affecte le groupe LOCAL_PARIS_Communication_READ et LOCAL_PARIS_Communication_READ qui sont assez clair de part leurs noms. De plus, il ne faut pas oublier la direction qui a droit de regard dans chaque fichier.



Une fois l'opération faite pour chaque service, on va utiliser le gestionnaire de ressources pour créer la limite de 20 GO.
D'abord je configure un nouveau modèle de quota car il n'existe pas de limite de 20Go.



Ensuite je l'applique à mon dossier Services



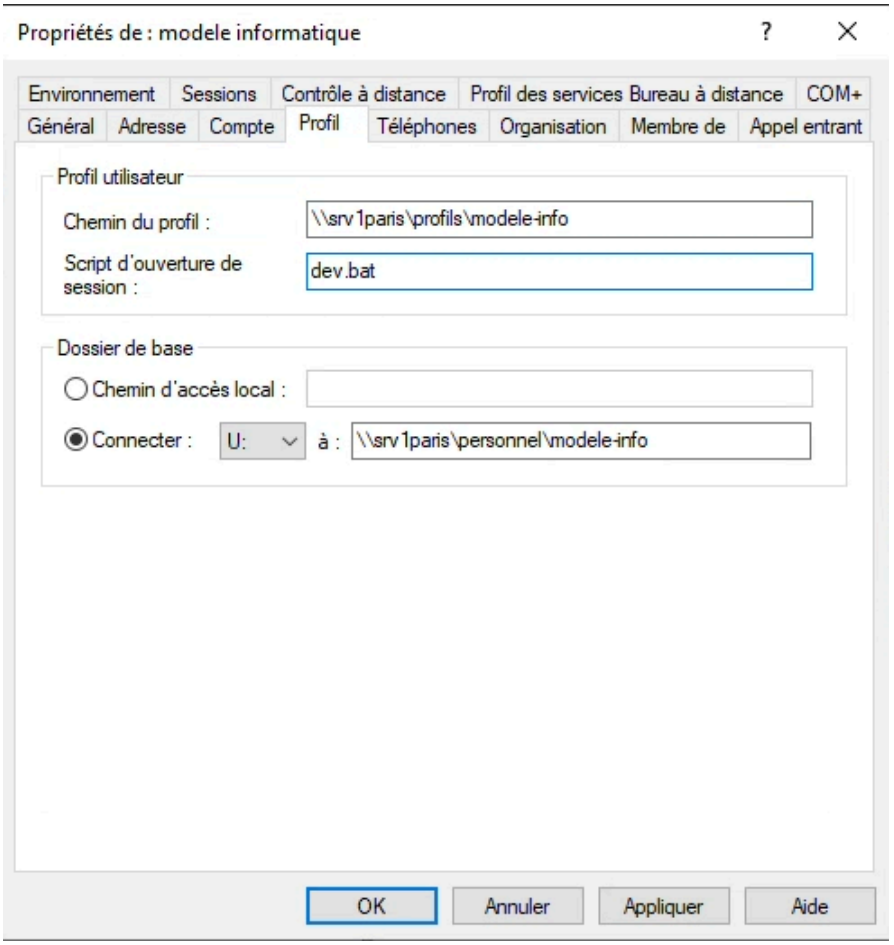
Contrainte n°6 :

" Un lecteur X: leur sera proposé pour échanger des fichiers (stocké sur les serveurs de fichiers). Sur ce lecteur, les utilisateurs pourront déposer des fichiers, lire tous les fichiers, mais seul l'utilisateur qui a créé le fichier pourra le modifier. Ce lecteur sera connecté automatiquement par script."

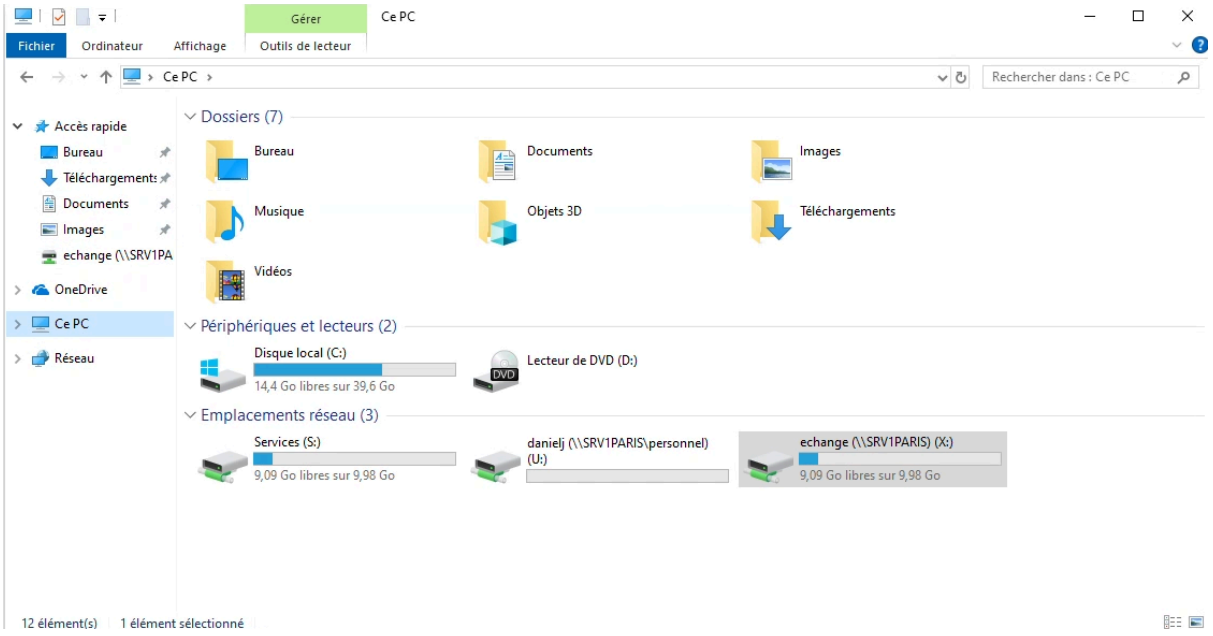
Il faut d'abord désactiver l'héritage puis mettre les droits d'écritures aux utilisateurs et pour finir bien vérifier que le CREATEUR PROPRIETAIRE est dans les groupes.

Ensuite il faut activer le mapping par script. Je place le script suivant dans tous les modèles utilisateurs de Paris.

```
batch
@echo off

:: Map le lecteur X: pour l'échange de fichiers
net use X: \\SRV1PARIS\echange /persistent:yes
```



Lorsqu'on ouvre la session d'un Utilisateurs, on retrouve bien notre disque X:



Il faut ainsi essayer la modification de fichier entre 2 sessions. Dans notre cas, cela marche. L'utilisateur Jack DANIEL peut consulter/écrire les documents mais il ne peut pas les modifier s'il n'est pas le "owner".

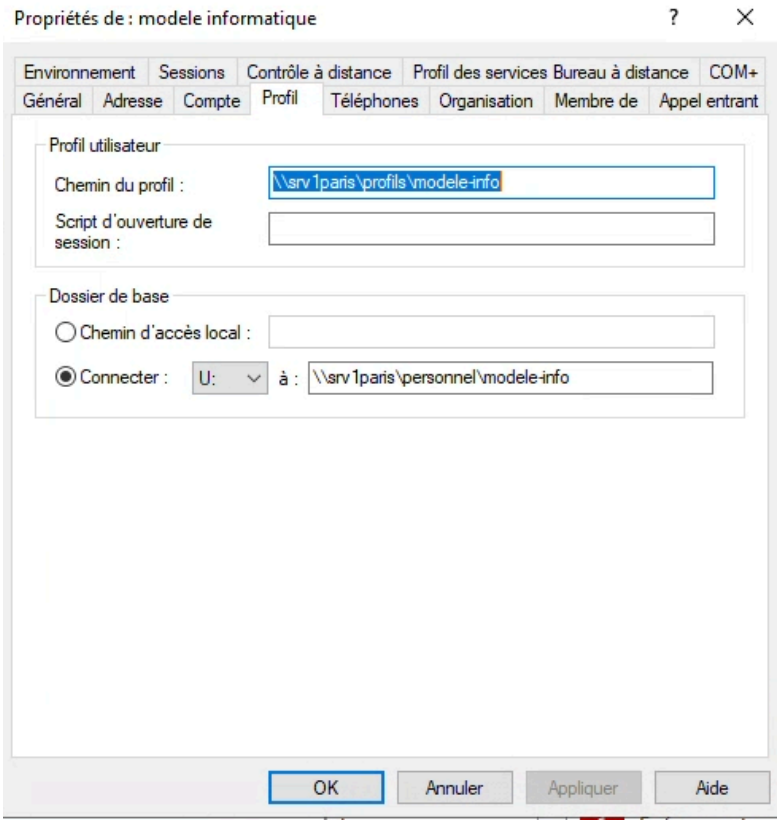
Contrainte n°7 :

“Les profils seront errants, personnels, stockés sur les serveurs de fichiers.”

Maintenant on va rendre les profils errants en créant un dossier Profils sur DATA PARIS. On le partage de la même façon que le dossier “Personnel”.

En remplissant bien les utilisateurs (donc les modèles pour se simplifier la vie), on créer automatiquement les profils (et le Personnel) pour chaque utilisateur

Il faut surtout penser à bien mettre %username% à la place du nom. Car lors de la duplication, il prendra automatiquement le nom du nouvel utilisateur.

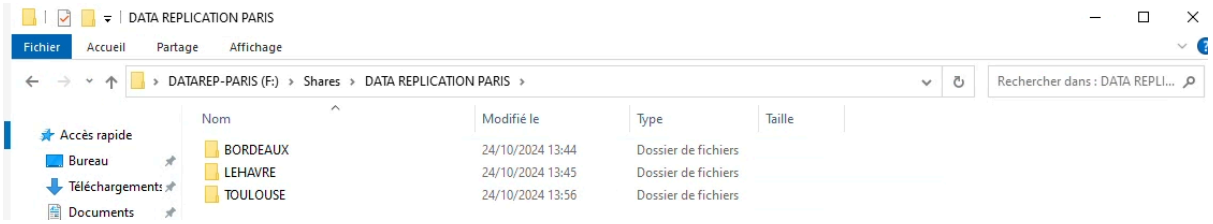


Contrainte n°8 :

“Pour assurer une tolérance de panne, les données des serveurs de fichiers (dossier de base, dossier de service, profiles, échange) seront répliqués sur les serveurs de fichiers de chaque site.”

Il faut ajouter le rôle de serveurs de fichier et Réplication DFS sur les deux serveurs PARIS et TOULOUSE. Il est impossible de la lancer si un serveur ne l’a pas. De plus, il faudra créer un nouveau disque dur virtuel DATARPPARIS et DATARPTOULO.

Dans chaque disque de réplication, il faut créer un espace pour chaque site.

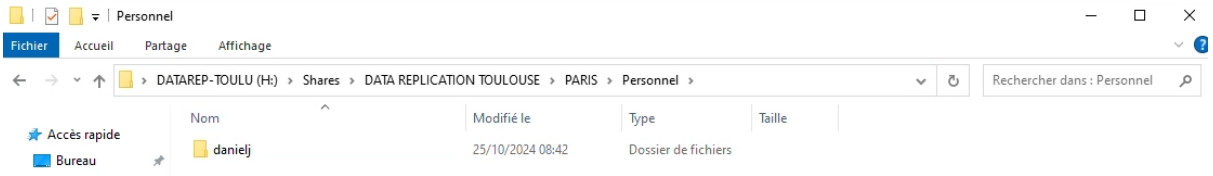


En effet, sur le disque de réplication de Paris, il va falloir répliquer les autres sites dans leurs dossiers (Toulouse)

On crée donc un nouveau groupe de réplication grâce au gestionnaire de fichiers DFS. Il faut en créer 2 :

- DATAPARIS -> DATARPPTOULOUSE
- DATATOULU -> DATARPPARIS

Une fois les deux zones de réplications mis en place, on va vérifier si tous fichiers créer dans un se répliquent dans l'autre. Je vais voir sur le SRV1TOULU si toutes mes données créées sur Paris se sont répliquées.



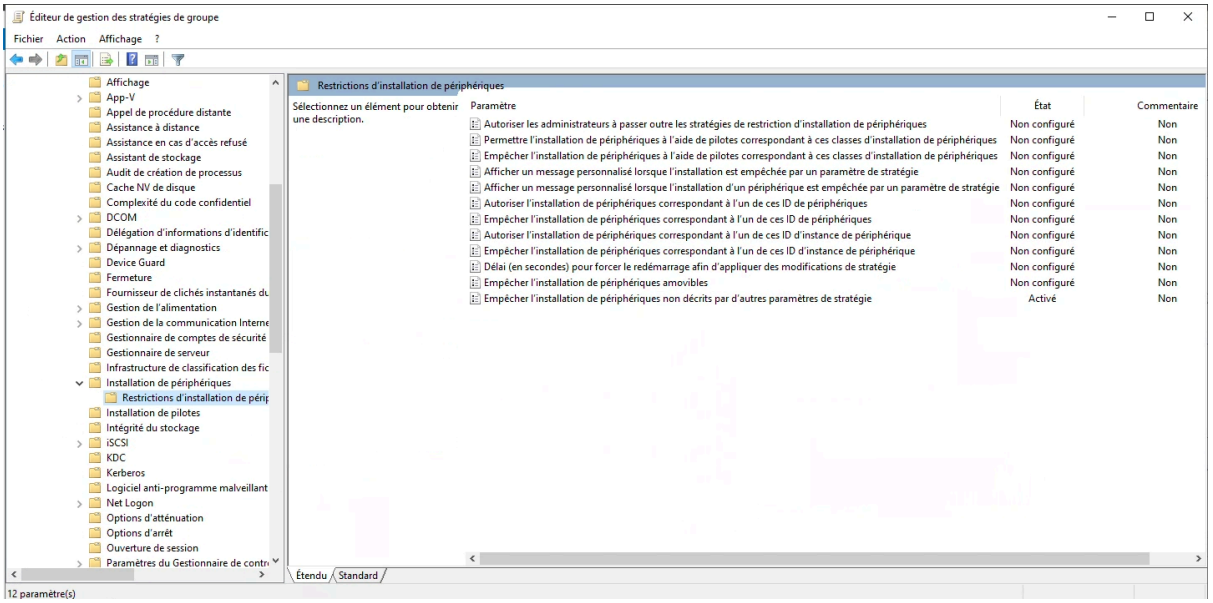
On peut voir que les profils des utilisateurs de Paris sont bien sur le DATARP-TOULOUSE. La réplication est en place.

Contrainte n°9 :

"Les utilisateurs ne pourront pas modifier le paramétrage de l'affichage (définition, pilote)."

On crée une nouvelle GPO puis on va devoir activé 2 stratégies :

- Configuration Ordinateur > Modèles d'administration > Système > Installation de périphériques > Restrictions : pour la restriction des pilotes.



- Configuration > Stratégies > Panneau de Configuration > Affichage : pour les modifications d'affichage.

Lorsqu'on a activé les deux, on assigne cette GPO à tous les utilisateurs. Ainsi, tous les utilisateurs seront concernés peu importe le site.

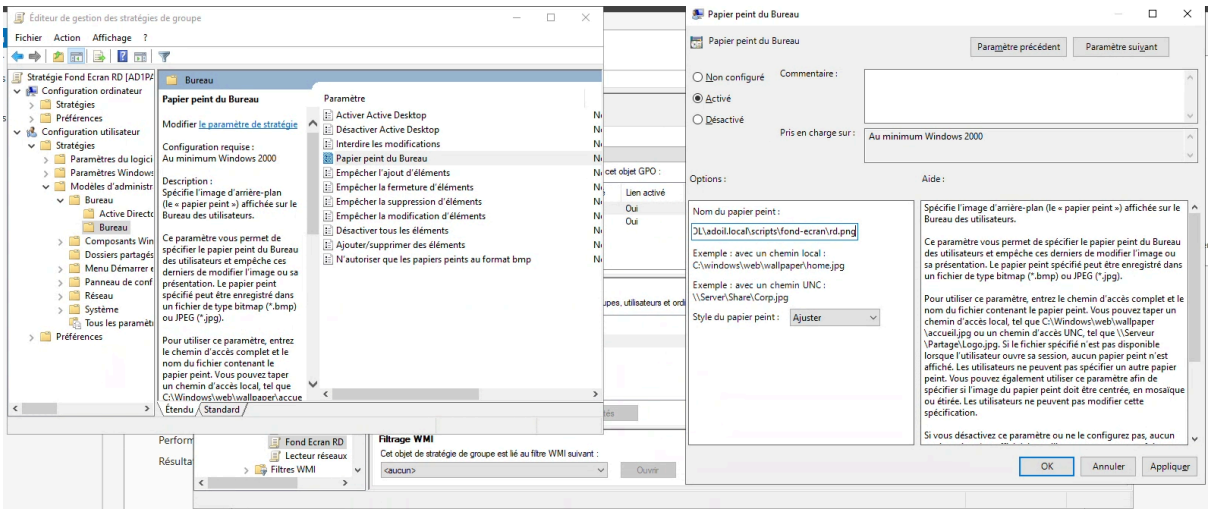
Contrainte n°10 :

" Le fond d'écran indiquera à quel service appartient l'utilisateur."

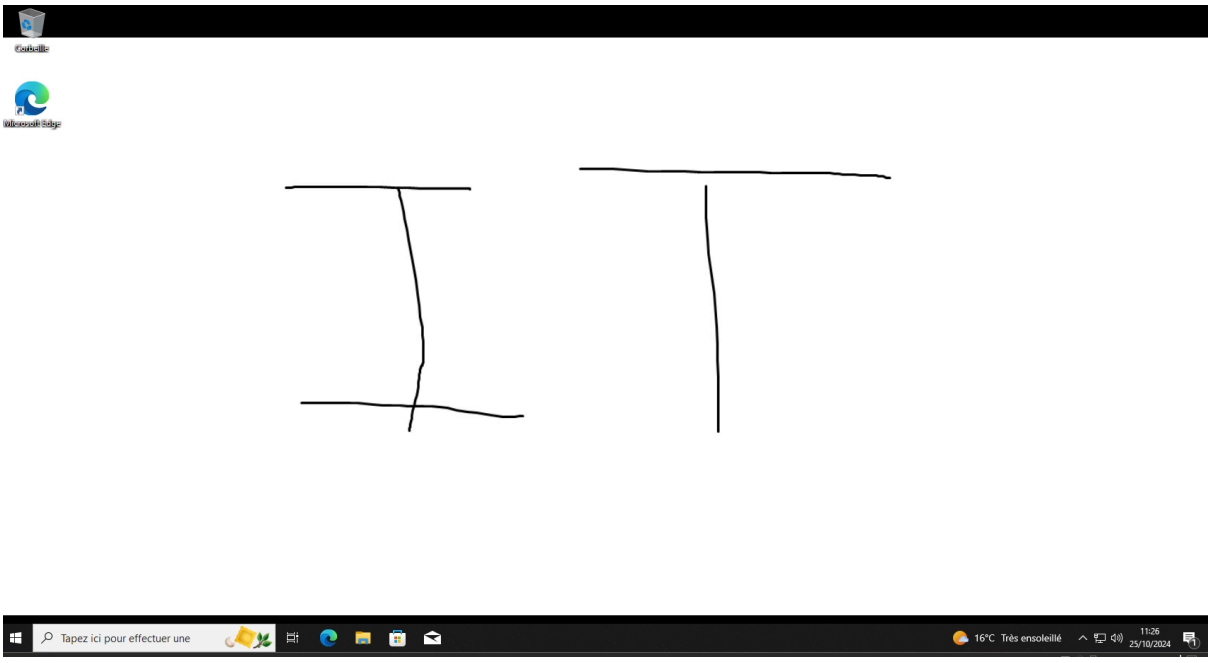
On ouvre l'éditeur de GPO puis on crée une GPO par services. Puis on les assigne à chaque dossier d'utilisateurs (déposer-glisser). Une fois fait, on modifie la GPO avec le chemin suivant : Configuration Utilisateur > Modèle d'Administration > Bureau > Bureau. On y trouve le "Papier Peint du Bureau" qu'on l'on modifie.

Bien-sûr avant cela, j'ai créé plusieurs fonds personnalisés que j'ai déposés dans le SYSVOL du serveur AD.

Puis on valide.



Lorsqu'on l'on a fait ça pour les 5 services. On en a fini avec les fonds d'écrans.



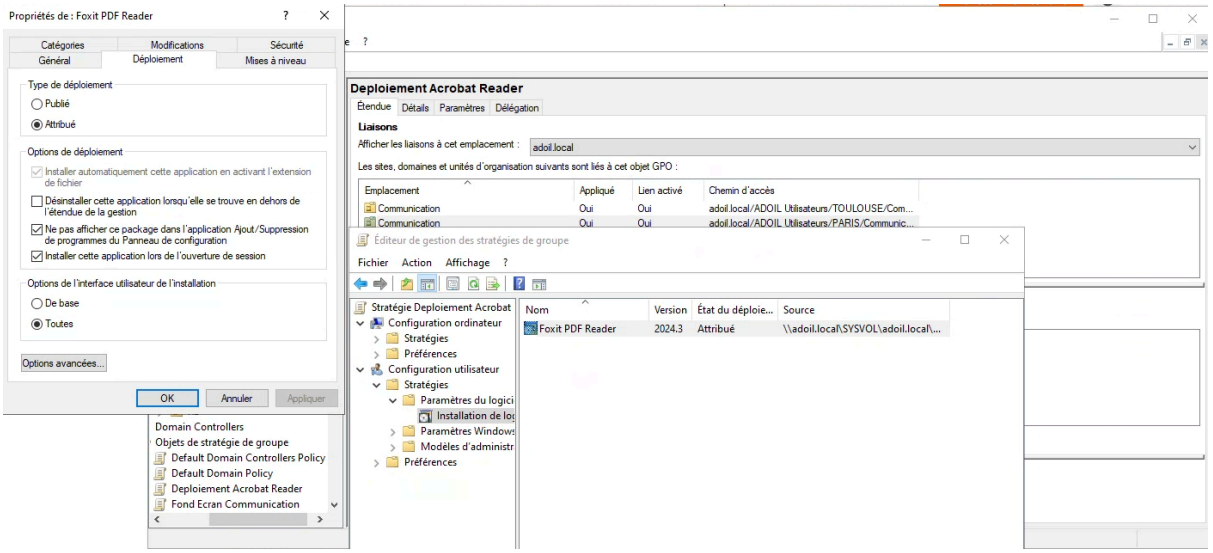
Contrainte n°11 :

"Les personnes du service communication ont besoin d'acrobat reader quel que soit le poste d'où ils se connectent. Le logiciel sera télédistribué et installé sur le poste client s'il n'est pas présent."

On crée une GPO pour déployer Adobe Acrobat Reader (Foxit dans ce cas car MSI d' Acrobat ne fonctionne pas).

- Après avoir créé la GPO, on la modifie puis on suit le chemin : Configuration Utilisateur > Paramètres de logiciel > Installation d'un logiciel > Clic Droit Nouveau.

- Ici il faut renseigner le MSI préalablement placé dans un disque commun aux machines. Dans notre cas \\adoil.local\SYSVOL
- Ensuite modifions la (clic droit) puis Propriétés > Déploiement. Il faut sélectionner les deux dernières coches.
-



- On valide tout et on assigne la GPO aux groupes “Communications” de PARIS et TOULOUSE.
- Pour finir, on se connecte avec un utilisateur du service Communication et on regarde si le logiciel est remonté.

-

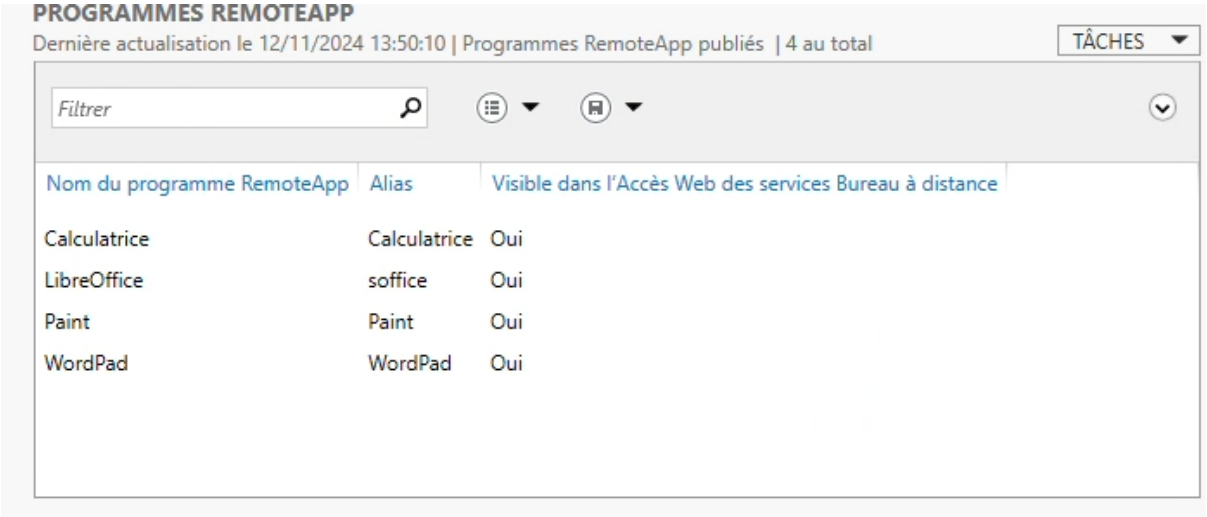
Contrainte n°12 :

“Les comptables utilisent une application développée sous Access, afin d’éviter d’installer Access sur tous les postes, d’homogénéiser les masters des postes clients et de contrôler

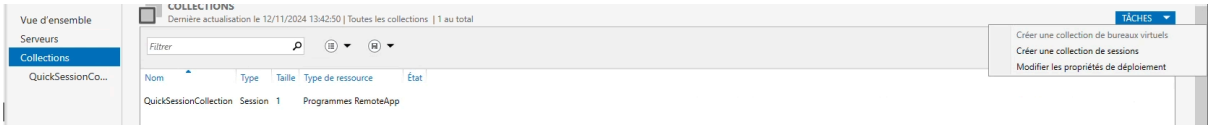
les licences, Access sera disponible pour les comptables grâce aux services « TS Remote App » installé sur un des deux contrôleurs de domaine”

On installe le rôle “Services de Bureau à Distance”
On va ensuite chercher le .msi de LibreOffice puis on utilise l'utilitaire “Installer une application sur un serveur Bureau à Distance” du panneau de configuration, sur lequel on renseigne le chemin du .msi

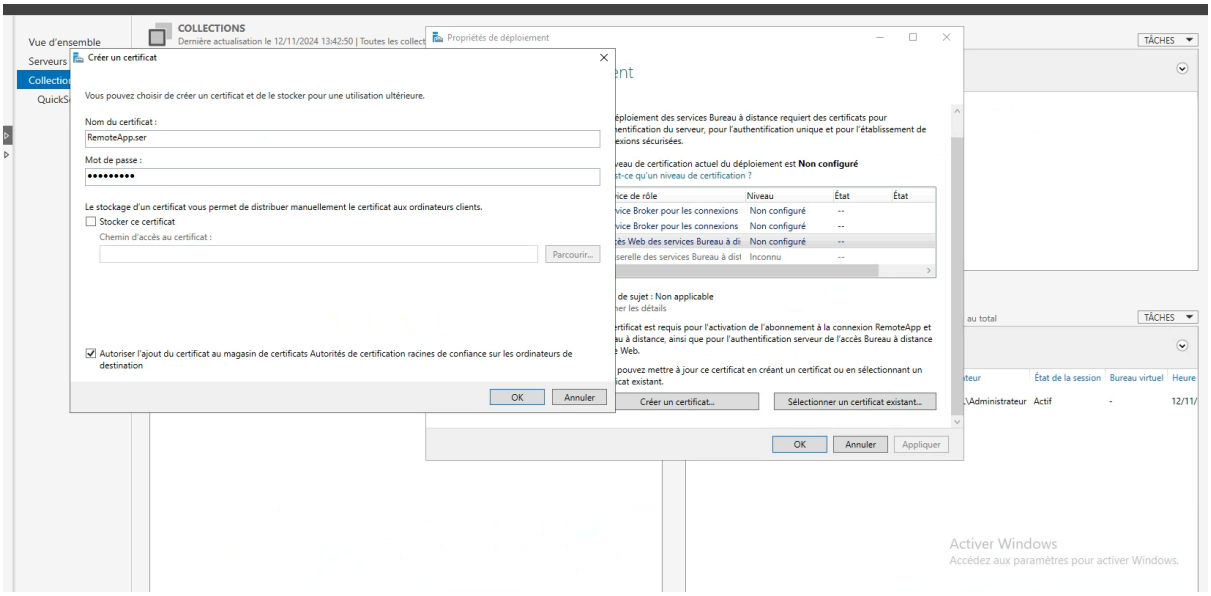
Après avoir fait cela, on va créer une nouvelle tâche “Programme RemoteApp”



La prochaine étape est de gérer les certificats Web pour l’accès. On va modifier les propriétés de déploiement, disponible dans les “Collections”



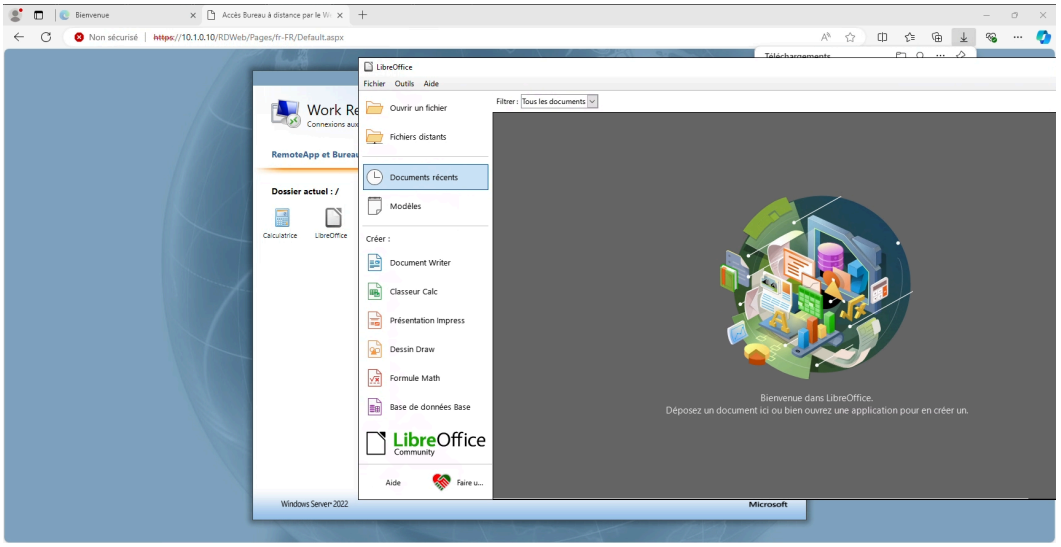
Certificats > Accès Web des services Bureau à Distance > Créer un certificat



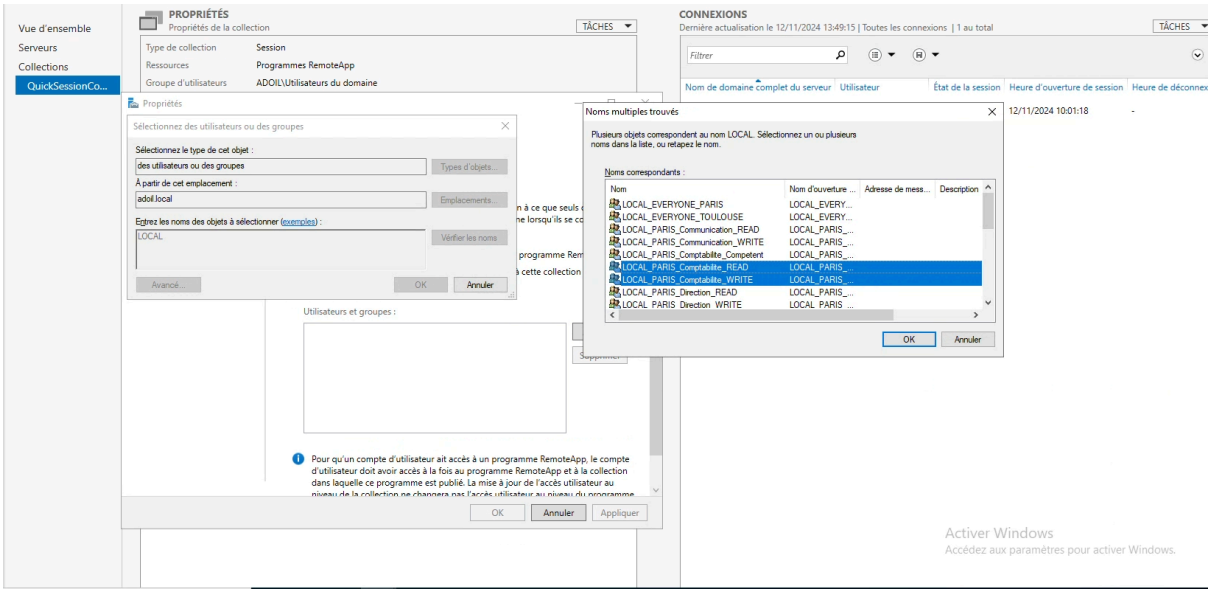
Ensuite on se rend sur un pc client puis on renseigne l’adresse IP du serveur :

10.1.0.10/RDWeb

On se connectera donc avec les identifiants du domaine pour accéder à notre plage de logiciels.



Pour finir, on restreint l’accès qu’aux membres du groupe local Comptabilité.

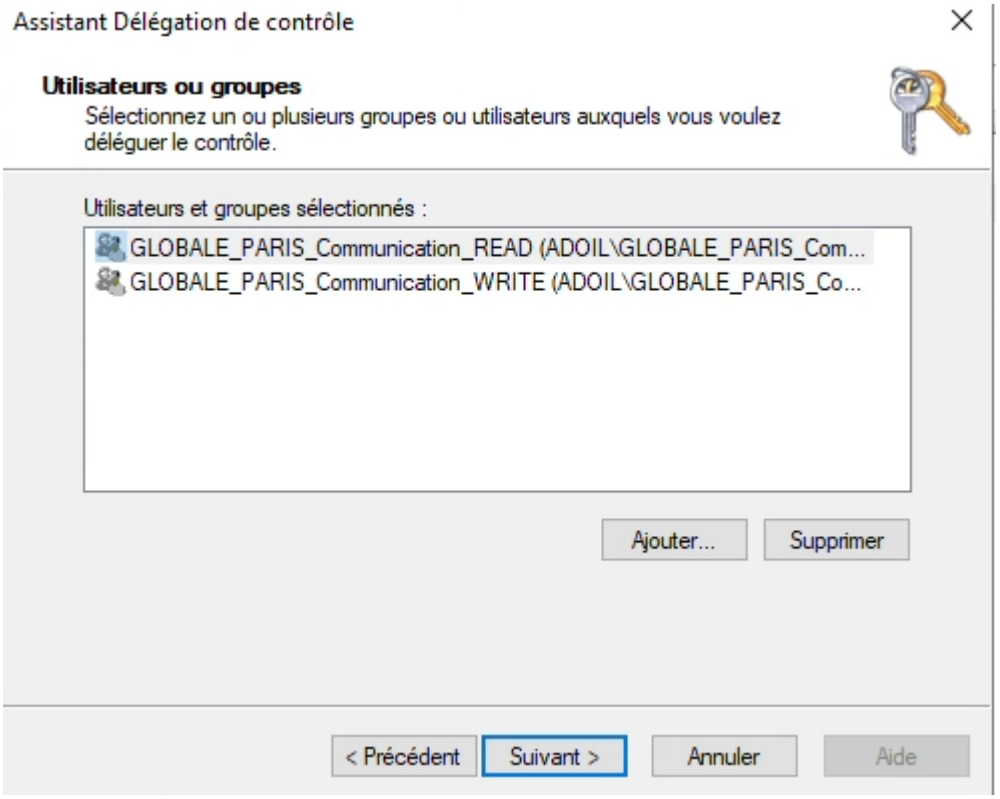


Contrainte n°13 :

“Michel Bonnet, un comptable plus dégourdi que les autres, aura la possibilité de changer les mots de passe de ses collègues comptables. Pour ce faire, on lui mettra en place une

MMC personnalisée, ne montrant que les comptes des comptables et ne permettant que de modifier les mots de passe.”

Il faut d’abord créer Michel BONNET ensuite on va faire une nouvelle OU dans l’OU Comptabilite : Comptable Compétent
Une fois créé, on clic droit sur la nouvelle OU puis Délégation de contrôle. On sélectionne les différents groupes globaux (communication dans notre cas).



-

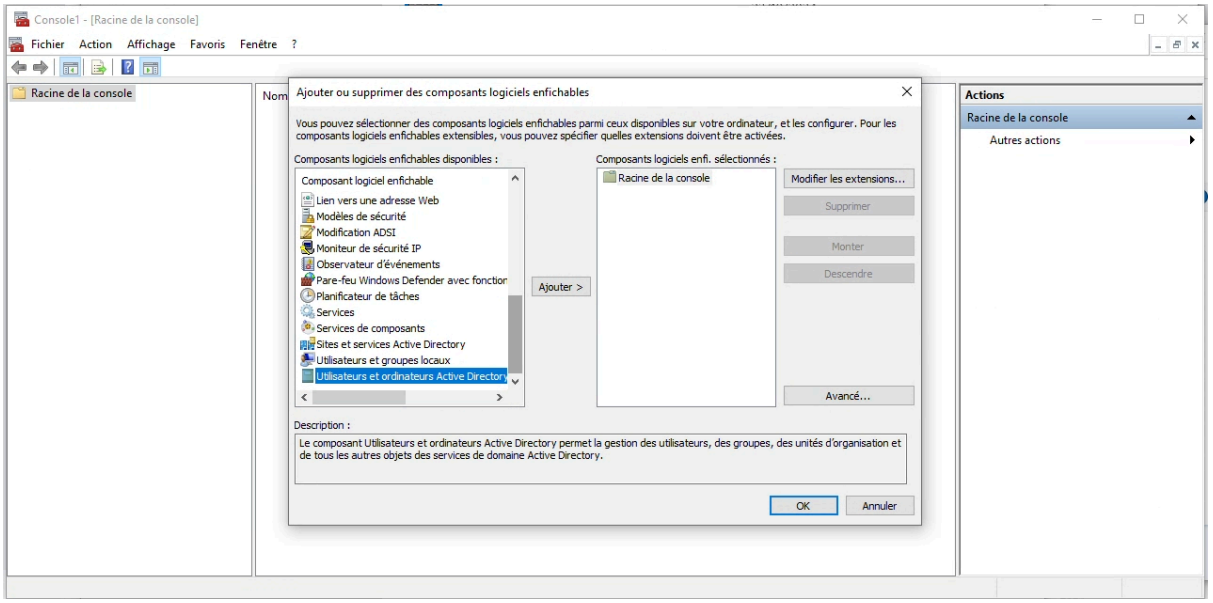
Sur le PCWIN10, il nous faut la fonctionnalité RSAT pour pouvoir créer une console MMC permettant le changement de mot de passe.

Personnellement j’ai utilisé la commande qui permet l’installation sur le poste (executer en administrateur) :

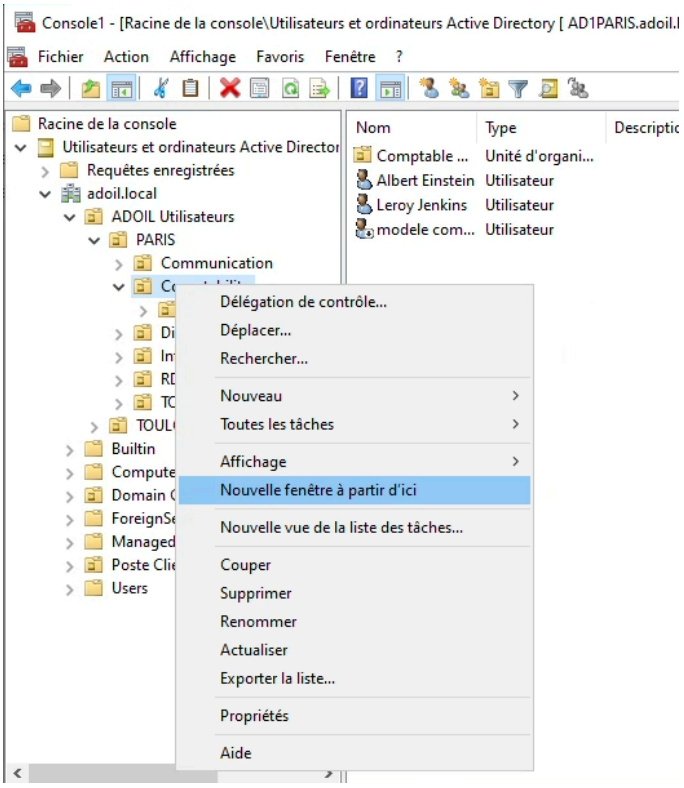
Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"

```
PS C:\Windows\system32> Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"


Path          :
Online        : True
RestartNeeded : False
```

On ouvre la console MMC puis on ajoute un composant logiciel enfichable et on sélectionne “Utilisateurs et ordinateurs Active Directory”



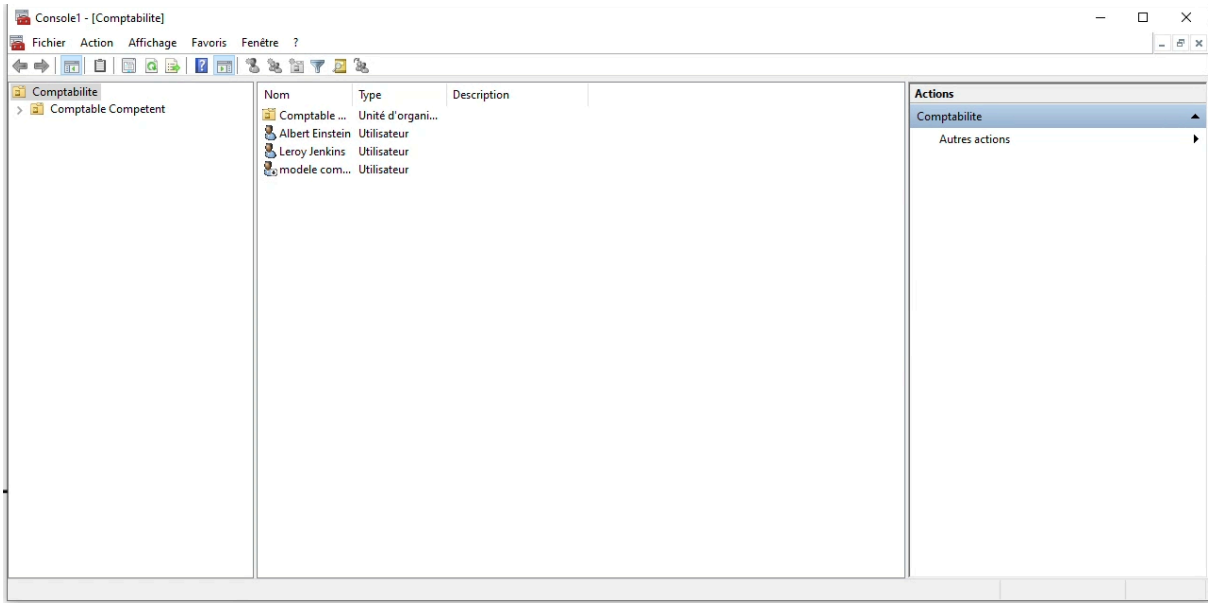
Sur l'AD1PARIS, on va créer une vue personnalisée pour les comptables compétent.



On va donc enregistrer la vue pour pouvoir la déployer sur les postes de comptables compétents.

Soit on lui donne manuellement mais le cas n'est pas très extensible. Soit un créer une GPO qui exécute un script pour lui fournir.

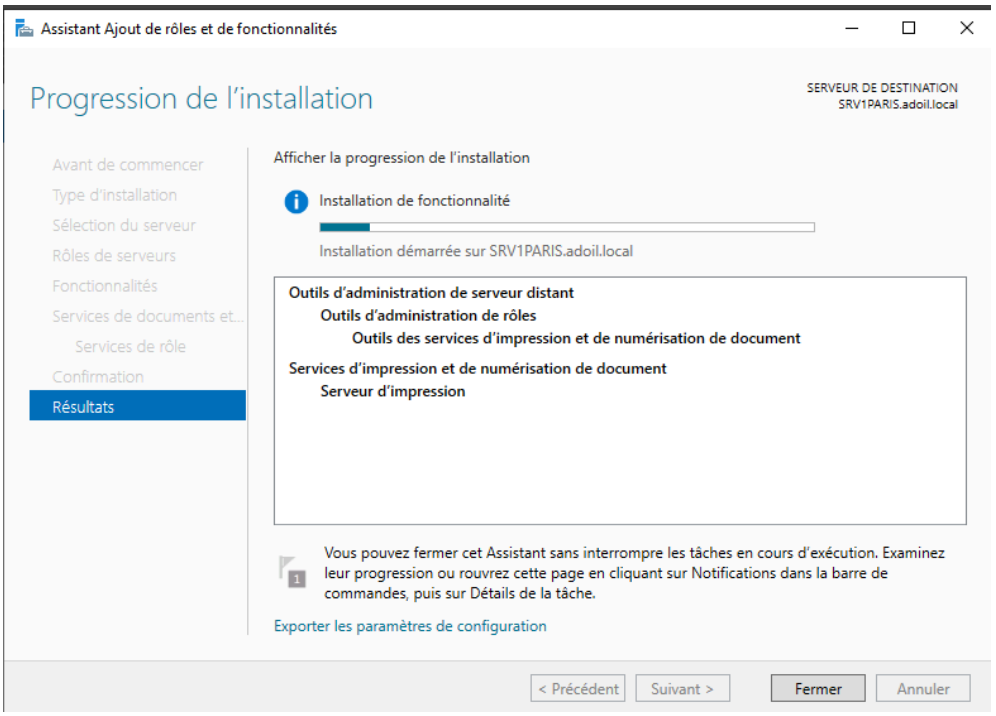
Voici la vue du Comptable :



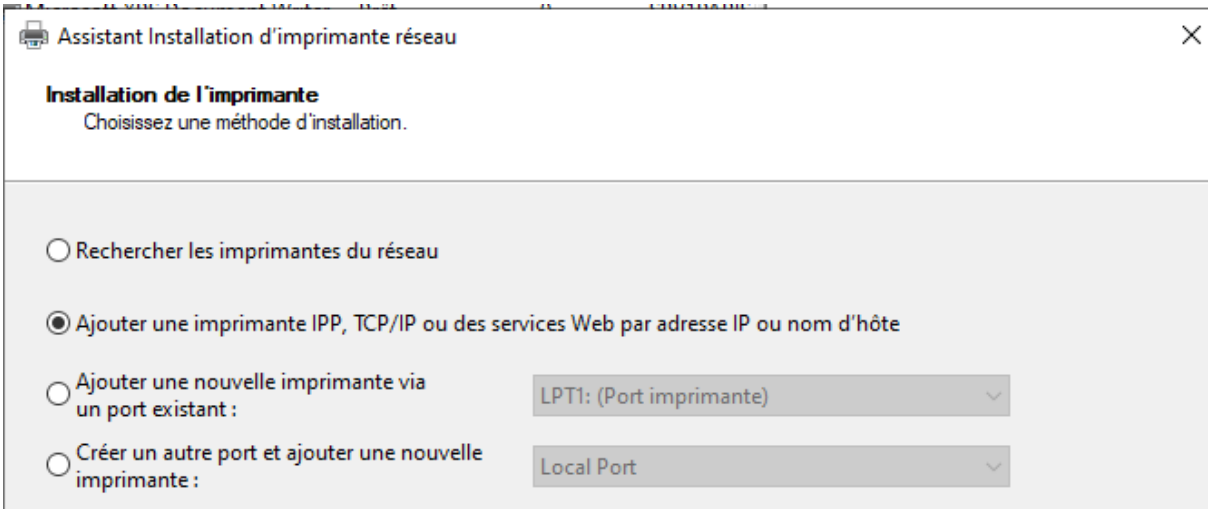
Contrainte n°14 :

“Des imprimantes de marque CANON seront connectées aux serveurs de fichiers. Tous les services pourront les utiliser, mais la direction sera toujours prioritaire sur les tâches d’impressions. Chaque site disposera de son imprimante réseau.”

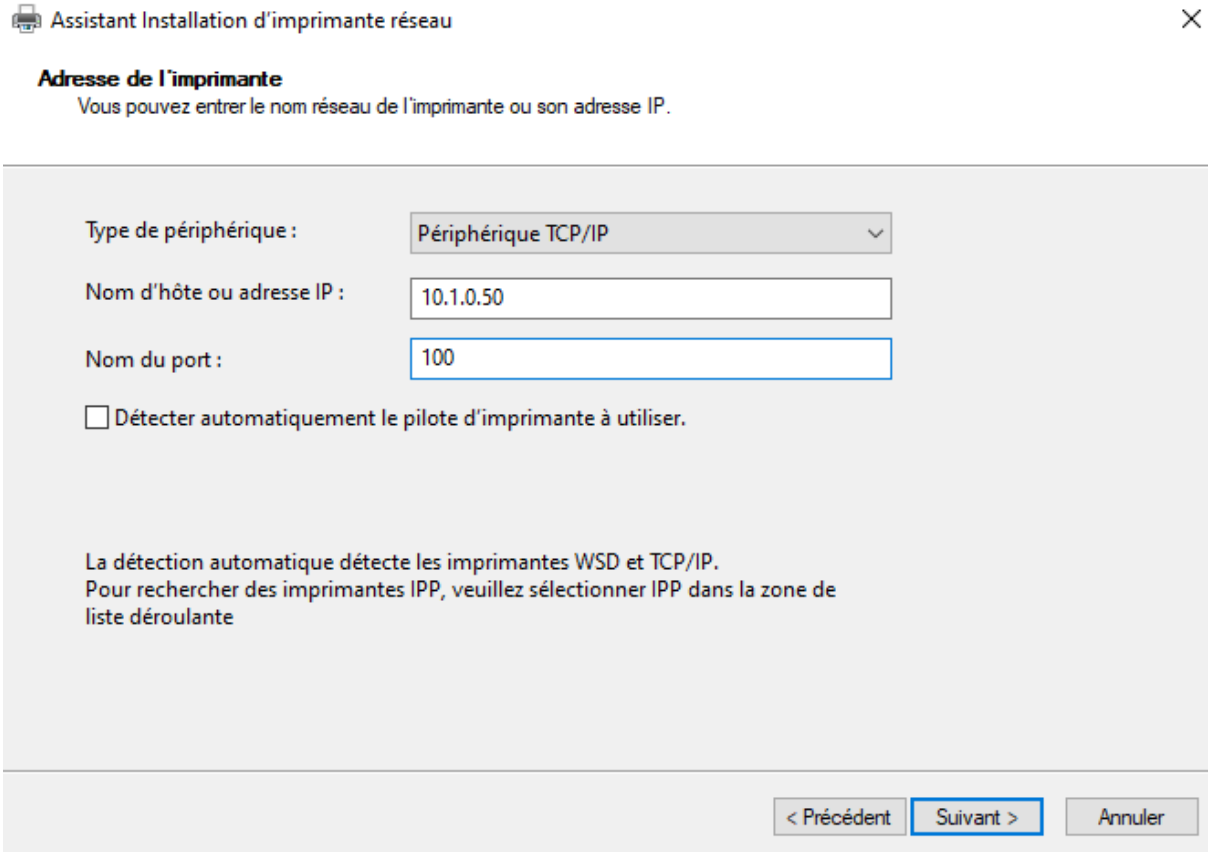
Installation du rôle serveur d’impression

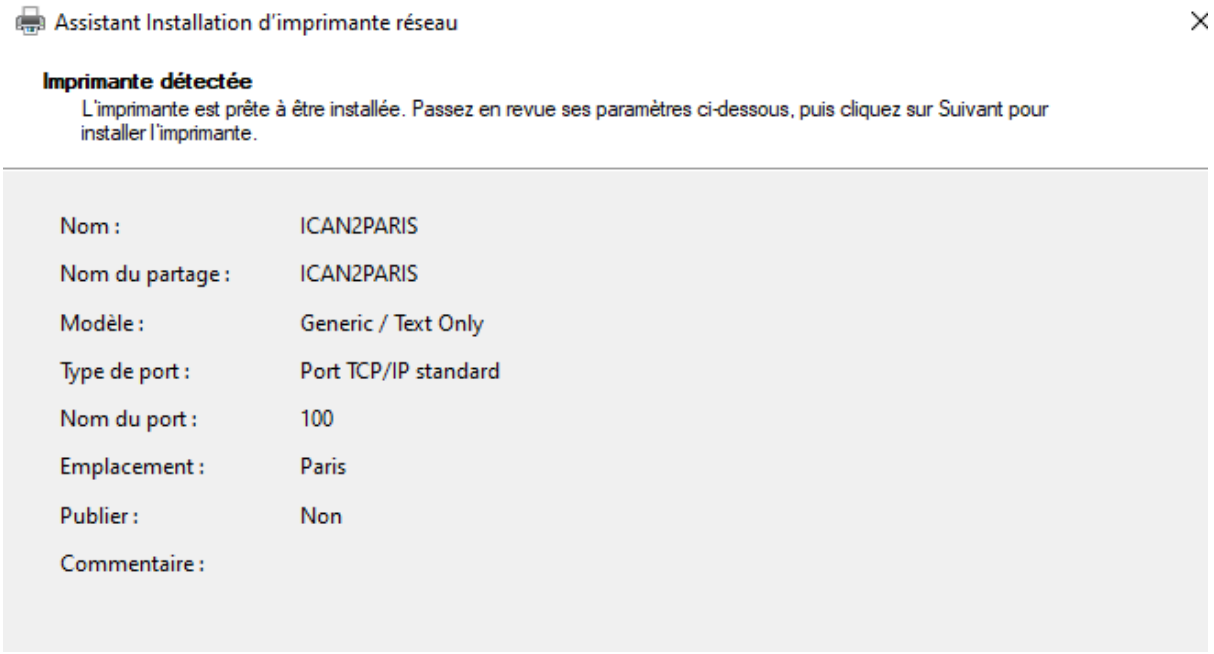


Ouvrir le gestionnaire d’impression puis créer une nouvelle imprimante dans le serveur d’impression



.





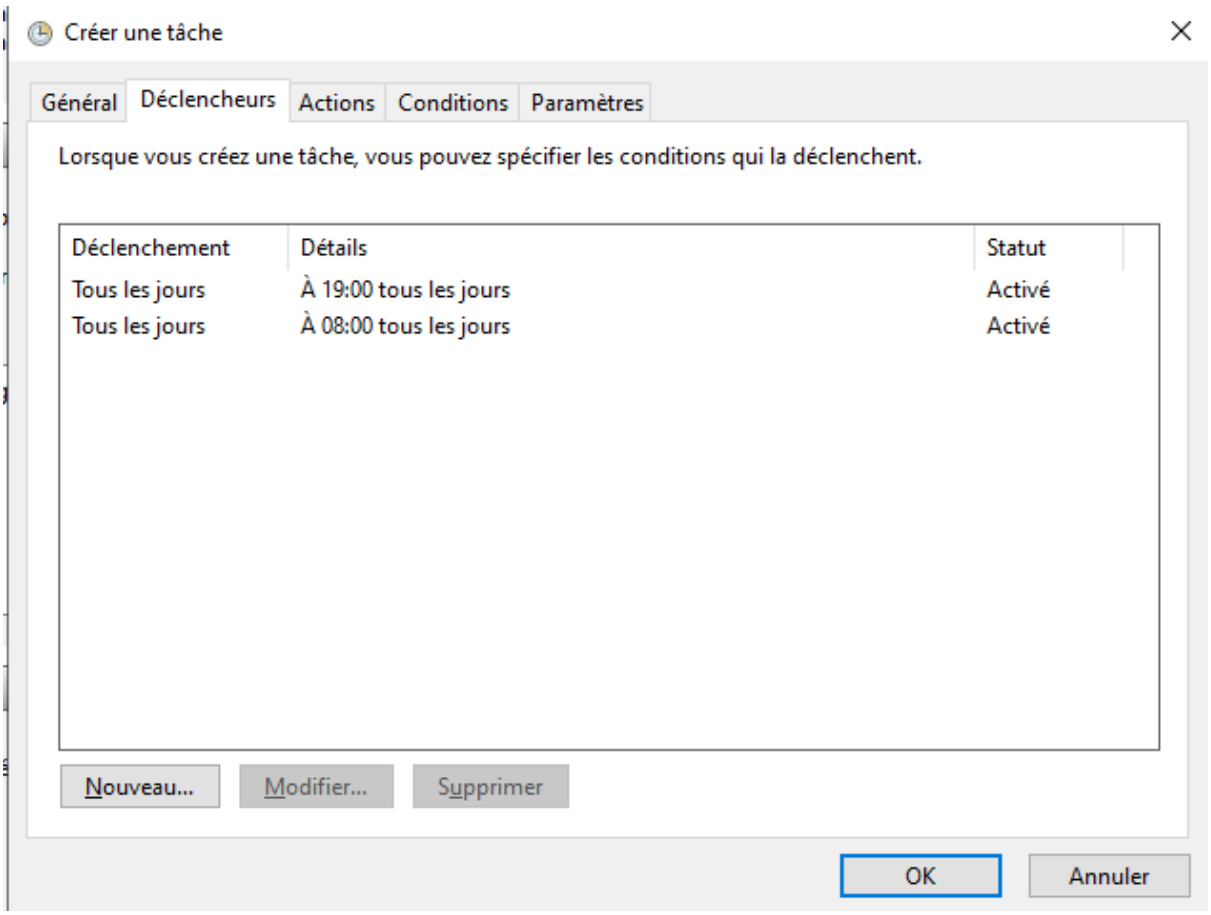
Il faut ensuite créer une deuxième imprimante avec la même IP/port pour la direction et ensuite supprimer “Tout le monde” et rajouter “Direction” dans la Sécurité de l’imprimante. Bien sûr, il faut penser à activer le partage pour l’imprimante.

Contrainte n°15 :

“Une deuxième imprimante de marque RICOH sera connectée au serveur de fichier du siège. Cette imprimante sera accessible par tous de 08H00 à 19h00 et disponible uniquement par la comptabilité sur le créneau 19h00-08h00 afin de pouvoir sortir les états des commandes et ventes durant la nuit.”

Pour l’imprimante RICOH, il faut définir une plage de disponibilité via l’onglet Avancé de ses Propriétés. On va la mettre de 8 à 19h pour tout le monde. La seconde étape va être de gérer le changement de droit grâce à un script powershell.

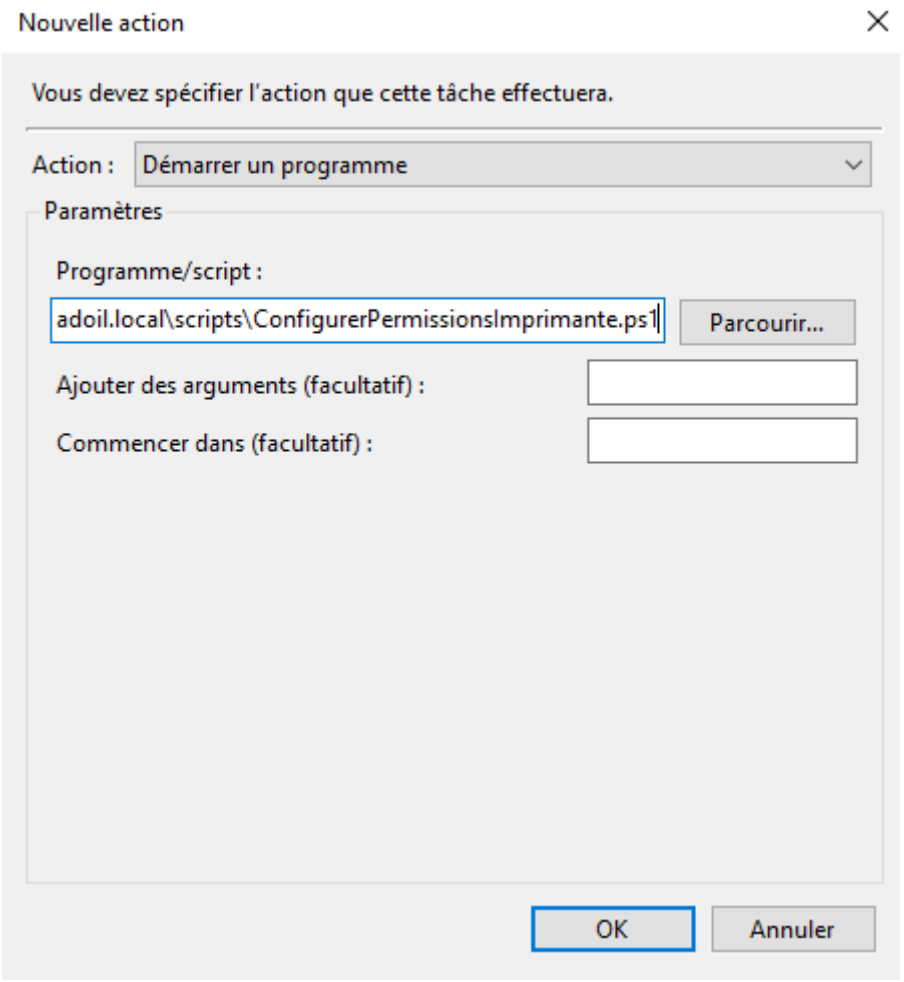
Je vais créer une nouvelle tâche via le Planificateur.
Le déclenchement se fera tous les jours à 19h00 pour échanger les droits puis une deuxième tâche viendra le remettre à 8h00.



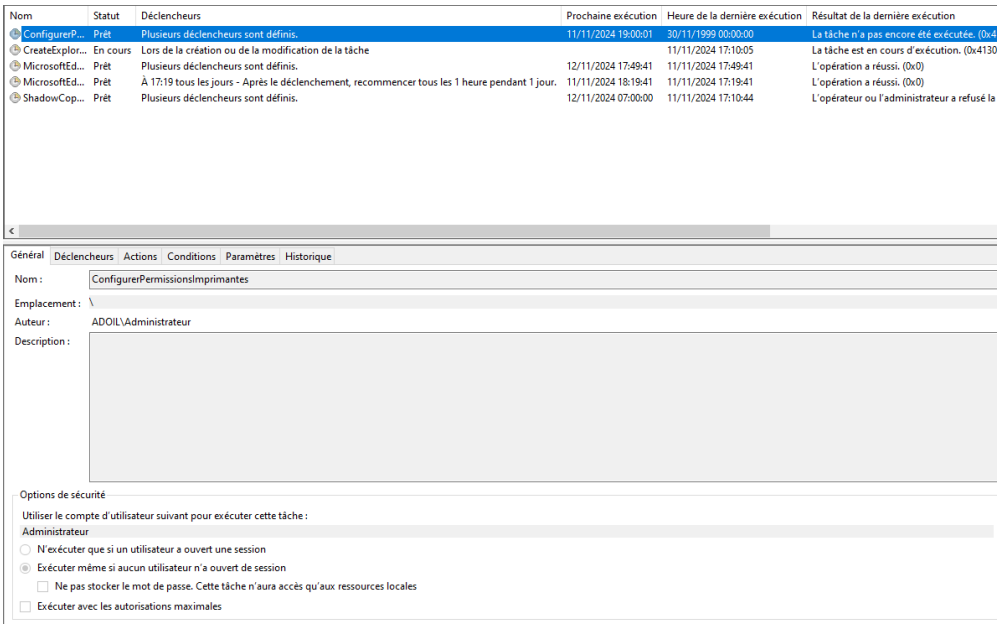
Puis on ajoute une action qui sera de “Démarrer un programme” qui exécutera notre script PowerShell.

Voici le script :

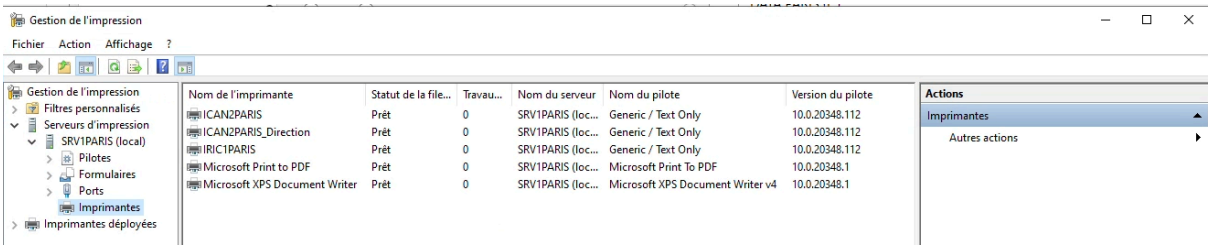
```
# Variables
$PrinterName = "IRIC1PARIS"
$GroupAll = "Tous les utilisateurs"
$GroupComptabilite = "Comptabilité"

# Permettre l'accès uniquemnt à la comptabilité de 19h00 à 08h00
$hour = (Get-Date).Hour

if ($hour -ge 19 -or $hour -lt 8) {
    # Enlève l'accès aux autres groupe
    Remove-PrinterPermission -Name $PrinterName -UserName $GroupAll
    Add-PrinterPermission -Name $PrinterName -UserName $GroupComptabilite
-AccessRights Print
} else {
    # Permet l'accès général en journée
    Add-PrinterPermission -Name $PrinterName -UserName $GroupAll -AccessRights Print
    Remove-PrinterPermission -Name $PrinterName -UserName $GroupComptabilite
}
```



On valide et on a mis en place le changement de permissions sur l'imprimante RICOH a partir de 19h pour la comptabilité et à partir de 8h pour remettre les droits initiaux.



A la fin, on obtient la gestion d'impression suivante :

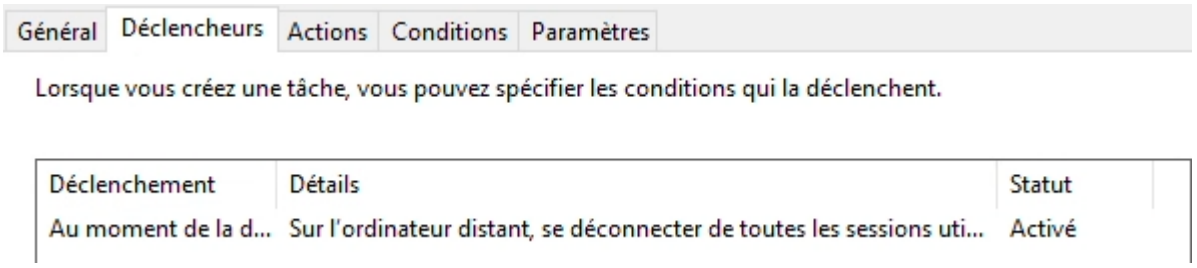


PS : Les imprimantes de Toulouse et autres sites ne sont pas définis mais la procédure est la même.

Contrainte n°16 :

"Un script permettra de vider le dossier « temp » de chaque utilisateur à la fermeture de session."

Pour vider le temp à chaque fin de session, il faut mettre en place une nouvelle tâche et mettre comme déclencheur : Au verrouillage de session.



Puis on lui assigne le script suivant pour le vider (démarrer un programme).
Voici le script :

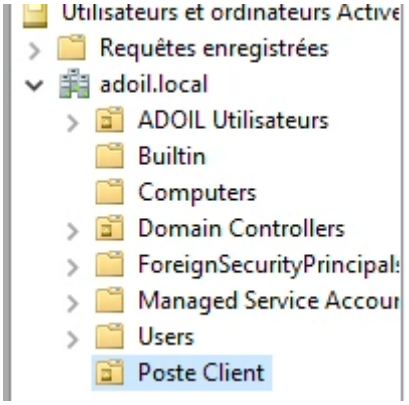
```
# Chemin du dossier Temp de l'utilisateur actuel
$tempFolder = [System.IO.Path]::GetTempPath()

# Récupérer tous les fichiers et dossiers dans le dossier Temp
$files = Get-ChildItem -Path $tempFolder -Recurse -ErrorAction SilentlyContinue

# Supprimer chaque fichier et dossier
foreach ($file in $files) {
    # Vérifier si c'est un fichier
    if ($file.PSIsContainer -eq $false) {
        Remove-Item -Path $file.FullName -Force -ErrorAction SilentlyContinue
    }
    # Vérifier si c'est un dossier
    elseif ($file.PSIsContainer -eq $true) {
        Remove-Item -Path $file.FullName -Recurse -Force -ErrorAction SilentlyContinue
    }
```

}

Contrainte n°17 :

“Les clients seront sous Windows 10, les comptes ordinateurs des postes clients seront stockés dans Active directory dans une OU nommé « Postes clients ». Le compte d’ordinateur de tout nouveau poste intégré dans le domaine sera automatiquement stocké dans l’OU « Postes clients ».”

Pour mettre tous les comptes ordinateurs des postes clients, il faut déjà créer l’OU “Postes Client”. Une fois fait, on va devoir exécuter une commande PowerShell pour pouvoir rediriger automatiquement (pensez à passer en admin)



La commande PS va être :

redircmp "OU=Poste client,DC=adoil,DC=local"

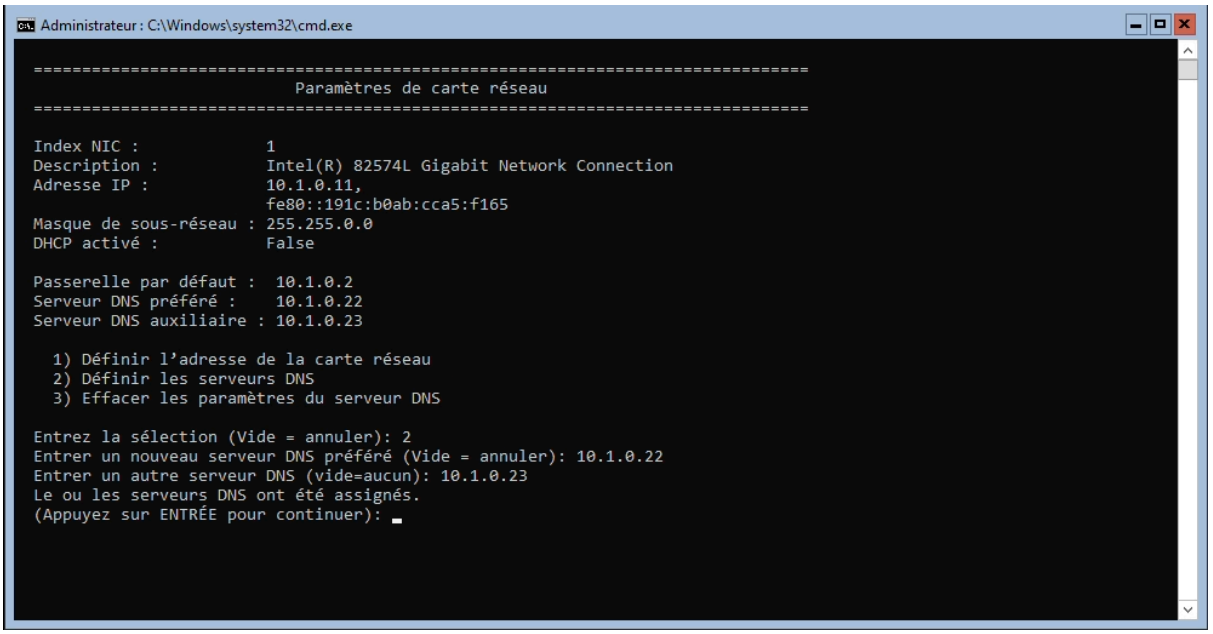
```
PS C:\Users\Administrateur> redircmp "OU=Poste client,DC=adoil,DC=local"
La redirection a réussi.
PS C:\Users\Administrateur>
```

La redirection est maintenant active.

III - Nouveau RODC sur Toulouse

Pour finir, on ajoute une nouveau contrôleur de domaine sur Toulouse mais en version Core de Windows Server.

Même principe que pour les autres. On change l'adresse IP en statique et on lui définit son nom.



Ensuite on lui ajoute le serveur DNS de Paris et celui de Toulouse en secondaire.

Puis ensuite le faire rejoindre le domaine ADOIL.

On lui ajoute le rôle AD DS via la commande suivante :

```
Install-WindowsFeature AD-Domain-Services
```

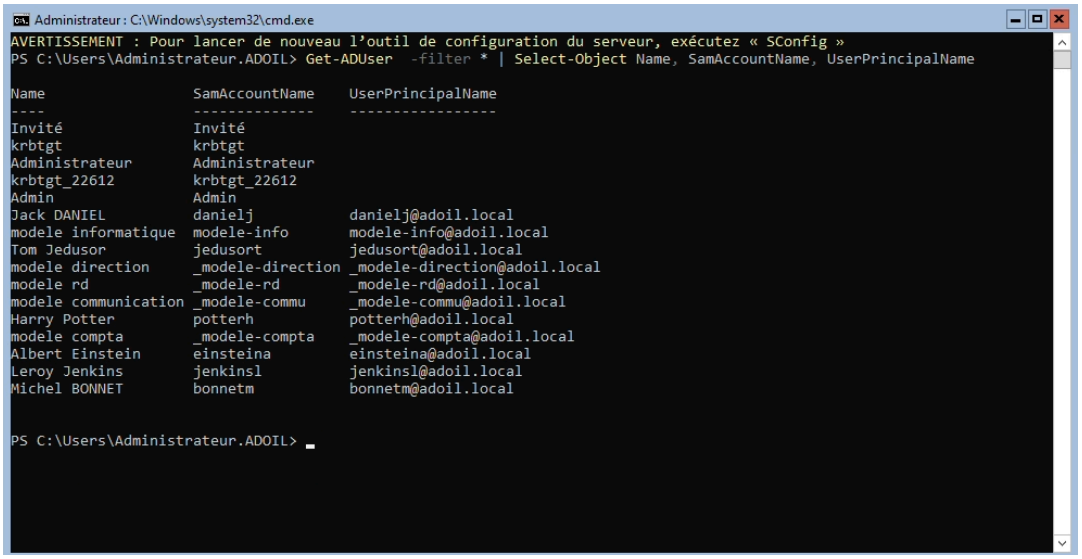
Pour finir, il faut le promouvoir en RODC via une seconde commande PS :

```
Install-ADDSDomainController -Credential (Get-Credential) -DomainName ADOIL
-InstallDNS:$false -ReadOnlyReplica:$true -SiteName "SiteAdoil" -Force:$true
```

PS : Au préalable, j'ai changé le nom du site par défaut sur le SRV1PARIS pour éviter le nom générique de "Default-First-Site-Name". J'ai mis "SiteAdoil"

Pour voir si le contrôle est bien initialisé, on peut sortir une commande PS sur l'AD tel que :

```
Get-ADUser -Filter * | Select-Object Name, SamAccountName, UserPrincipalName
```


Administrateur : C:\Windows\system32\cmd.exe
AVERTISSEMENT : Pour lancer de nouveau l'outil de configuration du serveur, exécutez « SConfig »
PS C:\Users\Administrateur.ADOIL> Get-ADUser -filter * | Select-Object Name, SamAccountName, UserPrincipalName
Name SamAccountName UserPrincipalName
---- -------------- -----------------
Invité Invité
krbtgt krbtgt
Administrateur Administrateur
krbtgt_22612 krbtgt_22612
Admin Admin
Jack DANIEL danielj danielj@adoil.local
modele informatique modele-info modele-info@adoil.local
Tom Jedusor jedusort jedusort@adoil.local
modele direction _modele-direction _modele-direction@adoil.local
modele rd _modele-rd _modele-rd@adoil.local
modele communication _modele-commu _modele-commu@adoil.local
Harry Potter potterh potterh@adoil.local
modele compta _modele-compta _modele-compta@adoil.local
Albert Einstein einsteina einsteina@adoil.local
Leroy Jenkins jenkinsl jenkinsl@adoil.local
Michel BONNET bonnetm bonnetm@adoil.local
PS C:\Users\Administrateur.ADOIL>