TP – Réplication Active Directory & gestion via WAC

Table des matières

Compétences mobilisées :

- Déployer un service
- Réaliser les tests d'intégration et d'acceptation d'un service
- Vérifier les conditions de continuité d'un service
- Mettre en place et vérifier les niveaux d'habilitation associés à un service
- Recenser et identifier les ressources numériques

I. Contexte

L'infrastructure actuelle du domaine tpsio.lab repose sur un unique contrôleur de domaine (SRVAD). Cette configuration présente un risque important de point de défaillance unique : en cas de panne, corruption du système ou attaque ciblant le contrôleur de domaine, l'authentification, la gestion des comptes et l'accès aux ressources du domaine seraient indisponibles.

Afin d'améliorer la_résilience du système d'information et de renforcer la sécurité liée aux services Active Directory, ce projet consiste à ajouter deux nouveaux contrôleurs de domaine complémentaires :

- Un contrôleur de domaine en lecture/écriture (RWDC – SRV2) afin d'assurer la réplication du service Active Directory et garantir la continuité de service.
- Un contrôleur de domaine en lecture seule (RODC – SRV3) permettant de disposer d'un DC sécurisé, adapté à un site distant ou à un environnement moins maîtrisé, limitant la surface d'attaque et l'exposition des informations sensibles.

Ce TP inclut également l'utilisation d'un poste d'administration pour centraliser la gestion via Windows Admin Center.

II. Objectifs

Les objectifs de ce TP sont les suivants :

- Mettre en place une architecture Active Directory plus résiliente grâce à la réplication entre plusieurs contrôleurs de domaine.
- Installer et configurer un contrôleur de domaine secondaire en lecture/écriture (RWDC) afin d'assurer la continuité d'activité.
- Installer et configurer un contrôleur de domaine en lecture seule (RODC) afin de réduire la surface d'attaque et sécuriser l'infrastructure.
- Administrer les contrôleurs de domaine et valider leur fonctionnement via un poste client d'administration avec Windows Admin Center.
- Vérifier la bonne réplication des objets Active Directory entre les contrôleurs et tester le comportement du RODC (limitations en écriture).
- Tester l'authentification d'un utilisateur du domaine à l'aide du nouveau contrôleur RODC.

III. Mise en place de l'infrastructure AD DS

Comme expliqué précédemment, deux nouveaux contrôleurs de domaine vont être déployés en complément de l'actuel SRVAD.

Ils auront la configuration suivante :

- SRVAD-02 : contrôleur de domaine RWDC, adresse IP 192.168.0.52
- SRVAD-03 : contrôleur de domaine RODC, adresse IP 192.168.0.53

1. Déploiement du RWDC (SRVAD-02) :

La mise en place de SRVAD-02 se fera via une machine virtuelle hébergée sur VM-Ware Workstation avec comme système d'exploitation Windows Server 2025 Core Version.

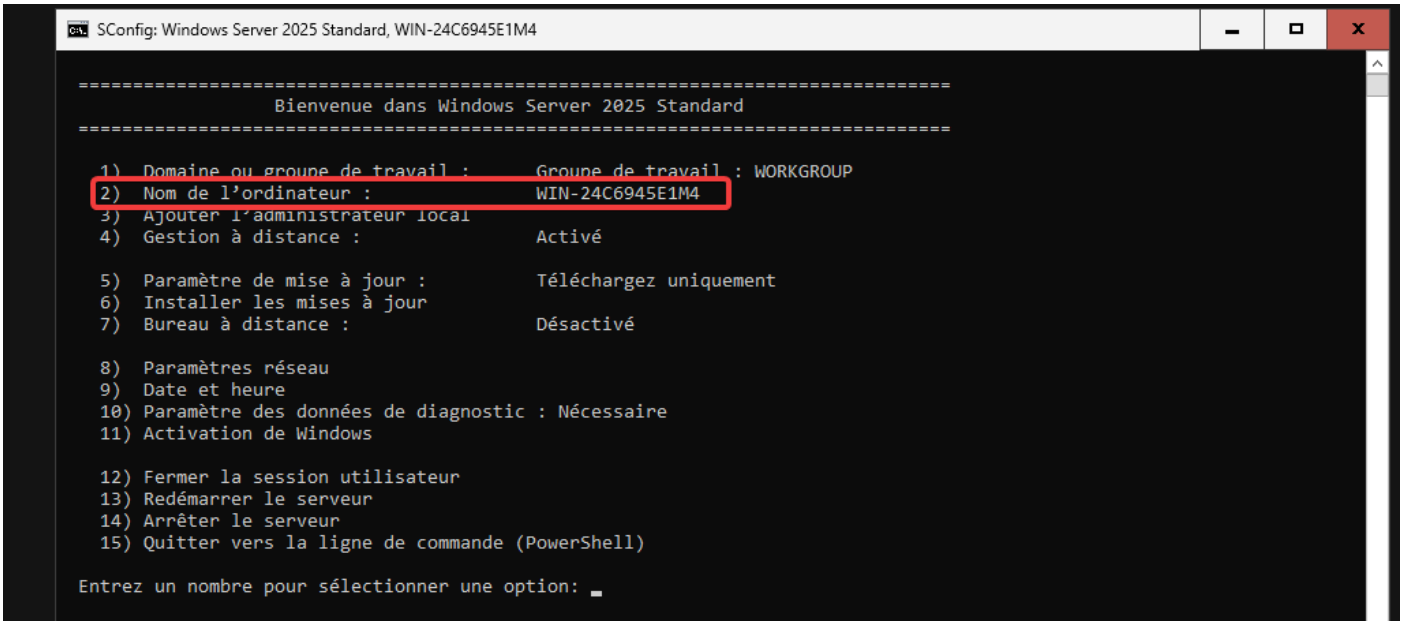
1. Configuration basique :

Une fois la machine créée et Windows Server installé, nous arrivons sur le menu de configuration.

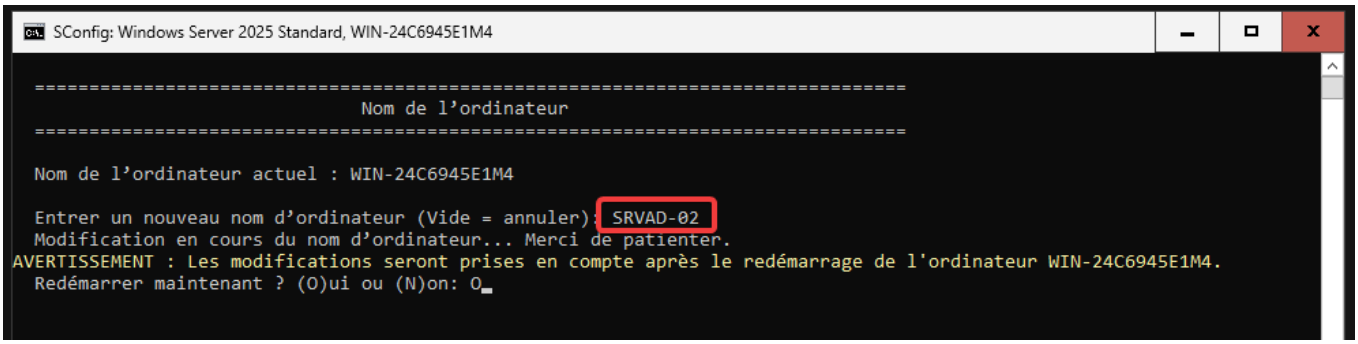
Nous allons effectuer les premières configurations avant de le promouvoir contrôleur de domaine, qui sont les suivantes :

- Changement du nom d'hôte
- Configuration du Réseau
- Activation du bureau à distance
- Ajout au domaine

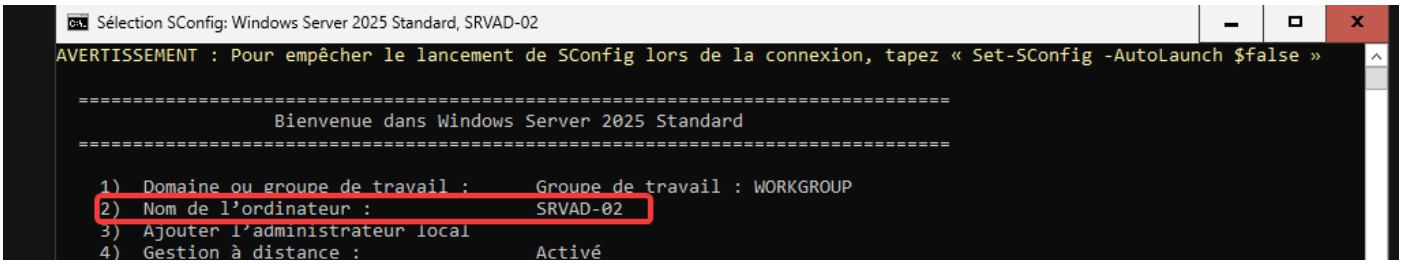
Commençons avec le changement de nom :



Le menu nous laisse, en choisissant l'option 2 et en indiquant le nouveau nom :

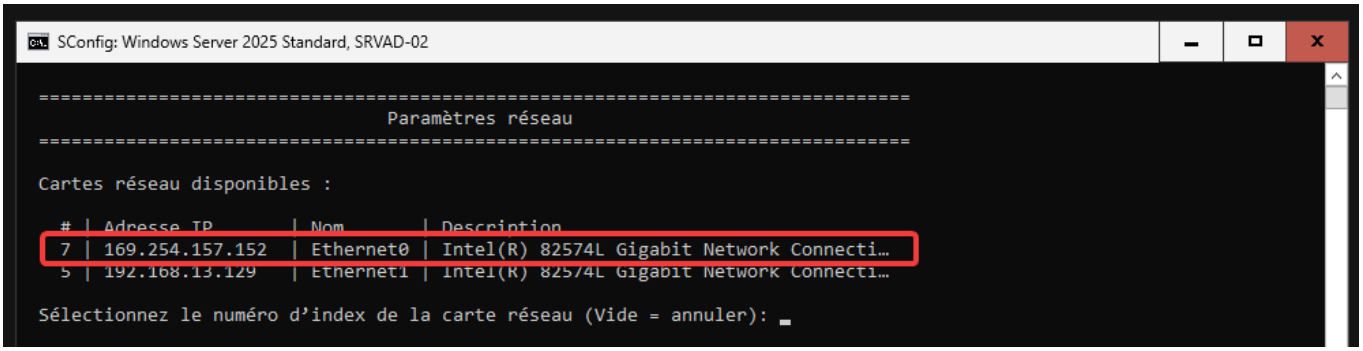


Un Redémarrage est nécessaire pour la prise en compte du nouveau nom.



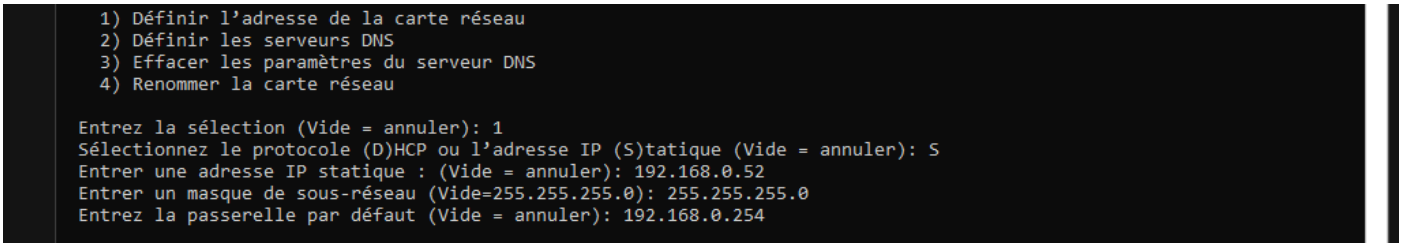
Le nom est maintenant bien changé !

Passons à la configuration du réseau, pour qu'il soit conforme à notre infrastructure. Elle va se faire aussi par le menu de configuration via l'option 8 « Paramètres réseau » :

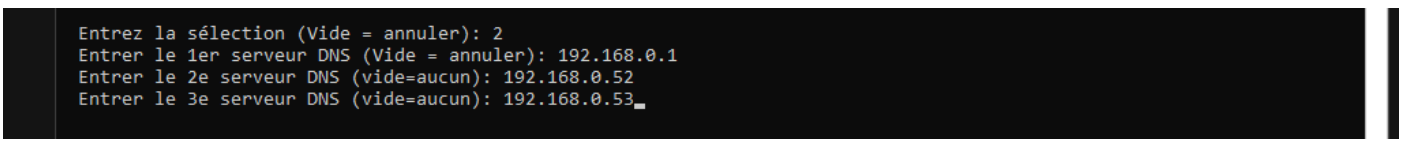


La carte qui va nous intéresser est la 1ère, la deuxième ne servant que pour l'accès à distance depuis notre machine hôte.

Nous allons premièrement changer l'adresse IP de la machine pour correspondre à celle que nous avons décidé (.52) et donner la passerelle de notre réseau afin de pouvoir accéder à internet :



Pour finir nous allons changer les DNS pour avoir la résolution de nom et nous permettre plus tard de s'ajouter au domaine :



Maintenant que la configuration est bien prise en compte, nous pouvons tester via des pings que tout

```
Index NIC :                   7
Nom :                         Ethernet0
Description :                 Intel(R) 82574L Gigabit Network Connection
Adresse IP :                  192.168.0.52,
                              fe80::5052:8130:fc2e:d3e
Masque de sous-réseau :       255.255.255.0
DHCP activé :                 False

Passerelle par défaut :       192.168.0.254
1er serveur DNS :             192.168.0.1
2e serveur DNS :              192.168.0.52
3e serveur DNS :              192.168.0.53
```

fonctionne :

```
Administrateur : C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrateur>
PS C:\Users\Administrateur> ping 192.168.0.1

Envoi d'une requête 'Ping'  192.168.0.1 avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.1:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
PS C:\Users\Administrateur> ping srvad.tpsio.lab

Envoi d'une requête 'ping' sur srvad.tpsio.lab [192.168.0.1] avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.1:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
PS C:\Users\Administrateur> ping google.fr

Envoi d'une requête 'ping' sur google.fr [142.250.201.163] avec 32 octets de données :
Réponse de 142.250.201.163 : octets=32 temps=19 ms TTL=127
Réponse de 142.250.201.163 : octets=32 temps=27 ms TTL=127
```

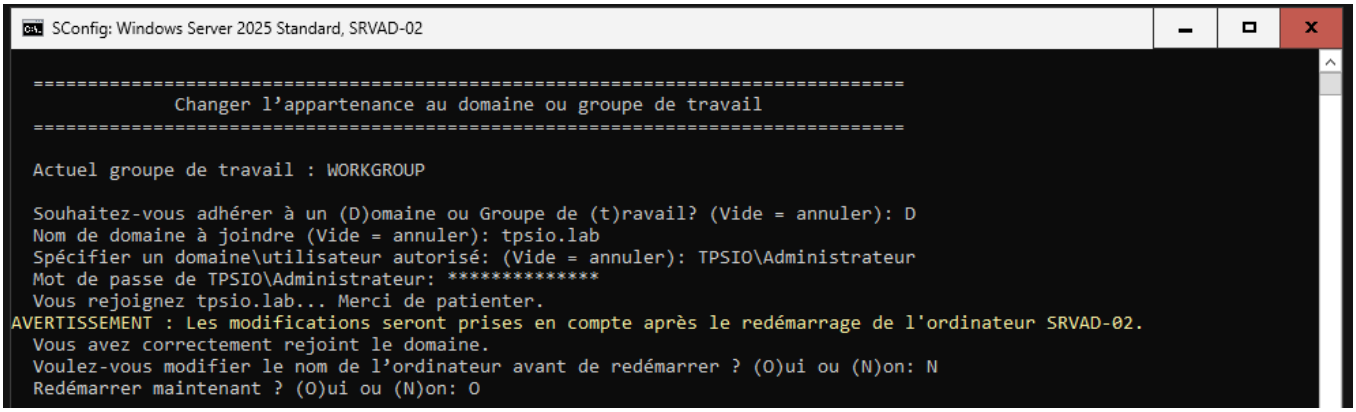
Tout fonctionne correctement, nous pouvons bien communiquer avec internet comme avec notre domaine tpsio.lab !

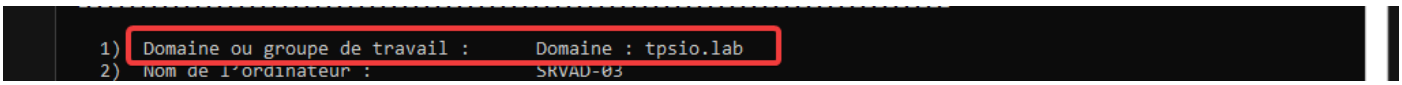
Tant que nous sommes encore dans la configuration, nous pouvons activer l'accès à distance, qui nous permettra d'accéder à l'écran de SRVAD-02 depuis notre pc hôte, sans passer par VM-Ware, cela passe par l'option 7 dans le menu :

```
SConfig: Windows Server 2025 Standard, SRVAD-02

===============================================================================
                            Bureau à distance
===============================================================================

Statut du bureau à distance : Désactivé

Souhaitez-vous (A)ctiver ou (D)ésactiver le Bureau à distance? (Vide = annuler): A

   1) Autoriser uniquement les clients exécutant le Bureau à distance l'authentification au niveau du réseau (NLA) qui
est plus sécurisée
   2) Autoriser les clients exécutant n'importe quelle version du Bureau à distance (moins sécurisé)

Entrez la sélection (Vide = annuler): 2
    6) Installer les mises à jour
    7) Bureau à distance :                Activé (tous les clients)
    8) Paramètres réseau
```

NB : Ici, comme nous somme dans un environnement de test, l'accès à distance est activé de façon non sécurisé, en production il ne faut pas faire ça.

Pour finir, nous allons ajouter SRVAD-02 en tant que membre du domaine, en prévision de sa promotion en RWDC, cela va se faire aussi par le menu, en changeant le WORKGROUP via l'option 1 :



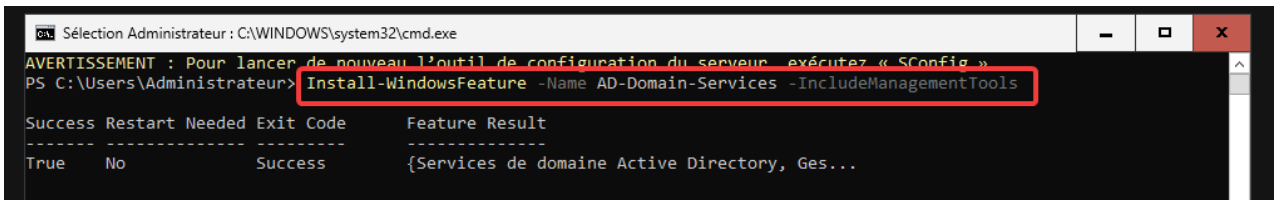


2. Installation & configuration d'ADDS :

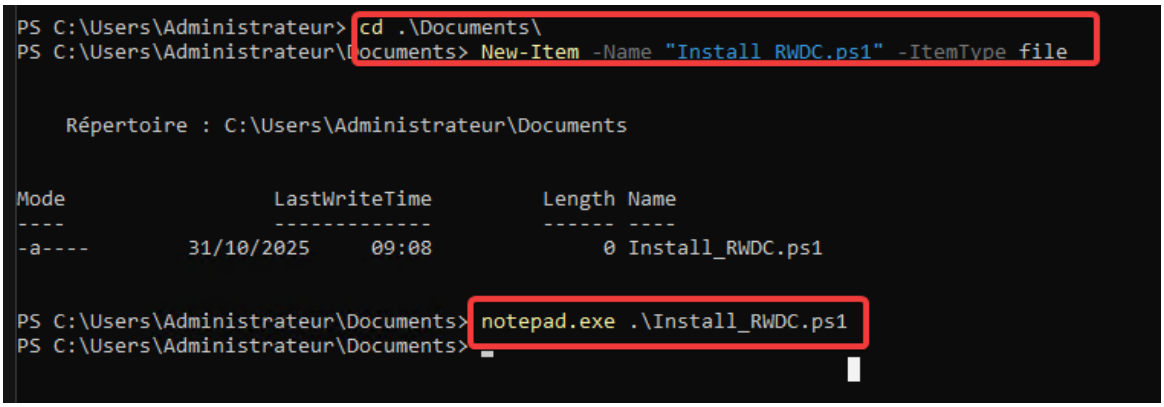
La configuration basique maintenant terminée, nous allons pouvoir nous tourner vers l'installation du rôle ADDS mais aussi son ajout en tant que second contrôleur de domaine à notre infrastructure.

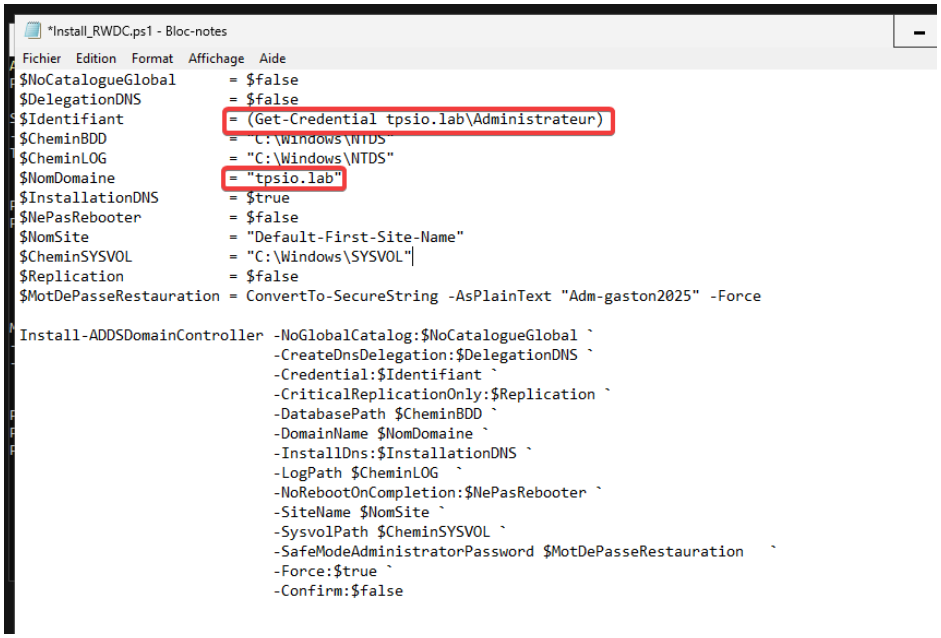
L'installation va se faire via le terminal powershell du serveur et via script fourni en annexe de ce TP.

Pour commencer nous allons installer le rôle ADDS (Active Directory Domain Services) via la commande **Install-Windows-Feature -Name AD-Domain-Services -IncludeManagementTools**



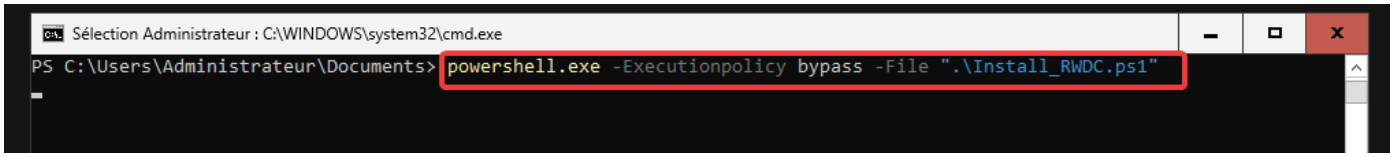
Maintenant que le rôle est installé nous allons mettre notre script dans un fichier powershell et l'exécuter :

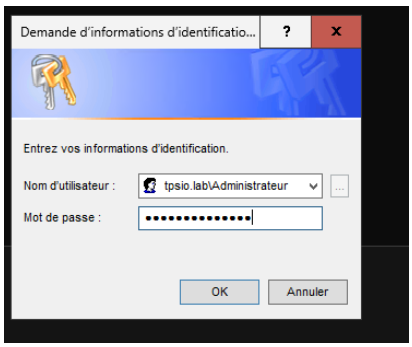


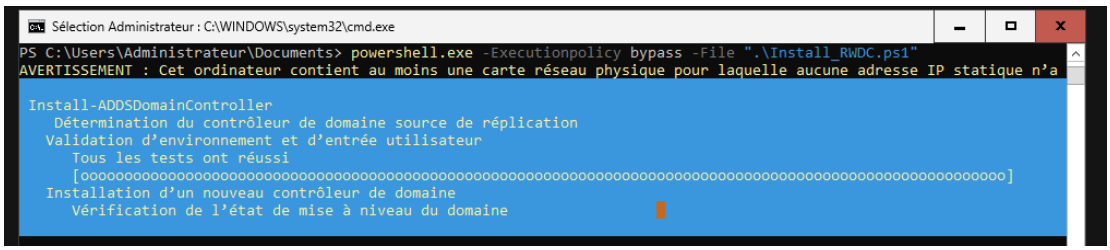


Les points à changer étaient l'identifiant du compte & le nom de domaine pour les faire correspondre à notre infrastructure.

Il suffit maintenant de l'exécuter et de rentrer les identifiants du compte Administrateur du domaine pour lancer la promotion en RWDC :



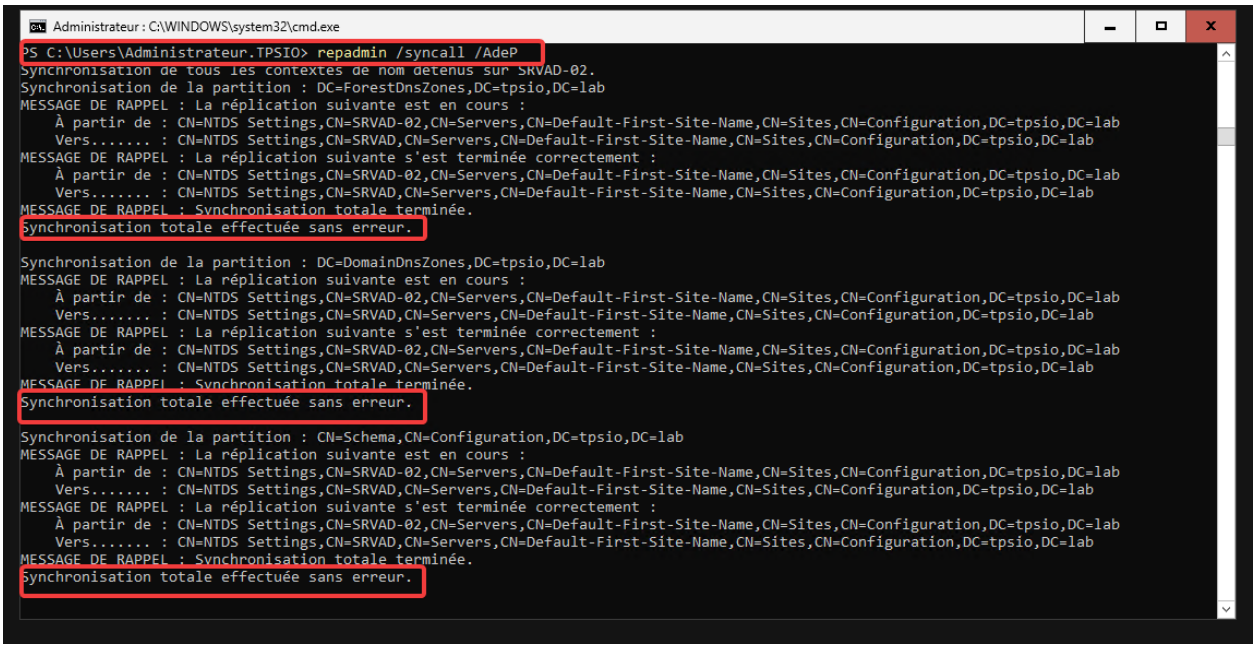




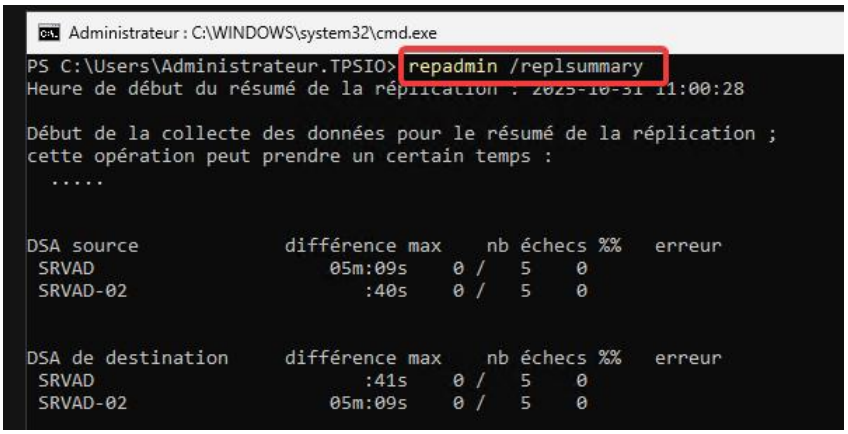
3. Test de la réplication :

L'installation étant maintenant terminé il nous suffit de tester la réplication via la commande repadmin pour voir si tout fonctionne correctement :

Nous allons déjà commencer par exécuter la commande **repadmin /syncall /AdeP** pour lancer une réplication complète :



Et pour finir lancer la commande **repadmin /replsummary** pour avoir un résumé de l'état de la réplication et nous assurer qu'il n'y a aucune erreur :



La réplication n'est passé sans soucis, le RWDC est maintenant pleinement fonctionnel dans notre infrastructure.

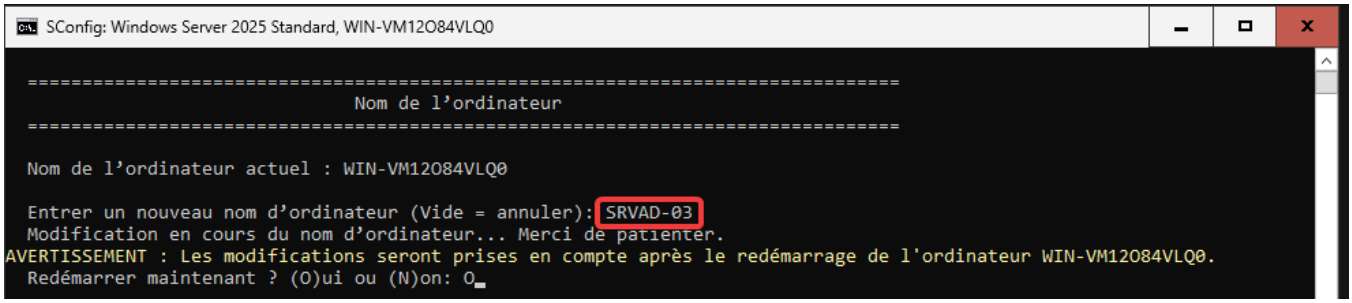
2. Déploiement du RODC (SRVAD-03) :

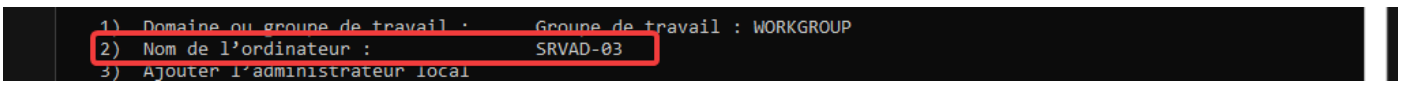
Comme pour SRVAD-02, la mise en place de SRVAD-03 se fera via une machine virtuelle hébergée sur VM-Ware Workstation avec comme système d'exploitation Windows Server 2025 Core Version.

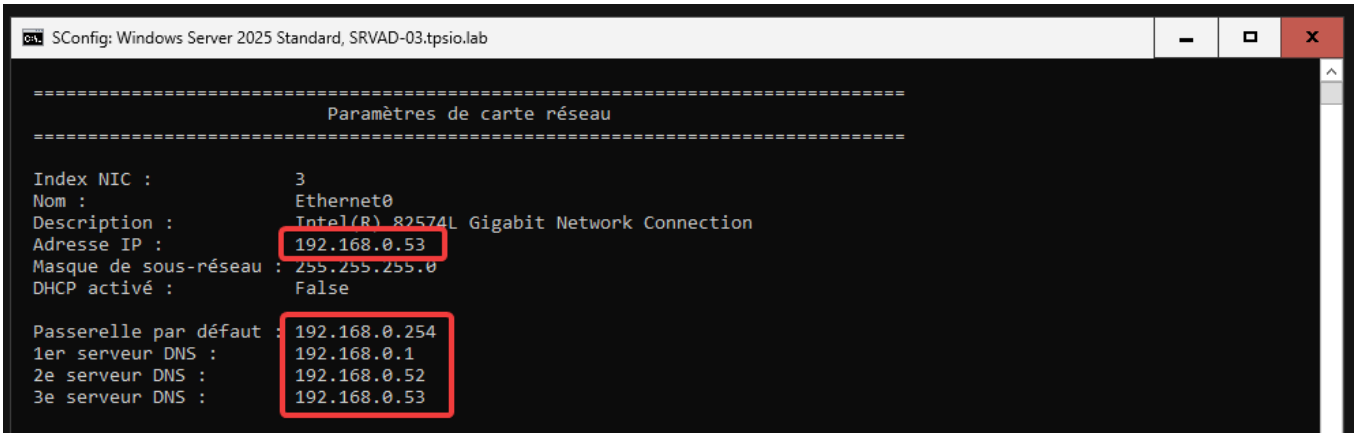
1. Configuration Basique :

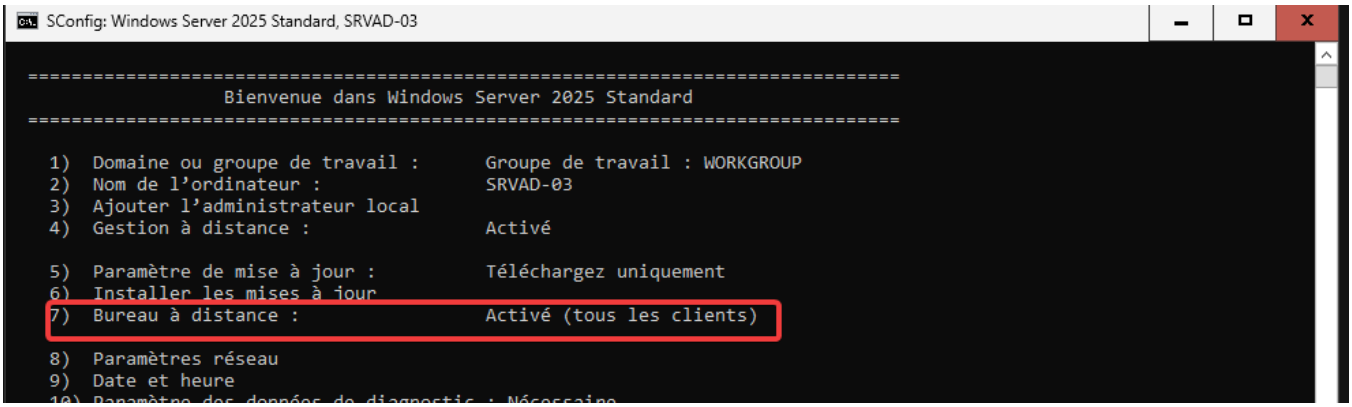
La configuration basique de SRVAD-03 sera la même que précédemment, c'est-à-dire :

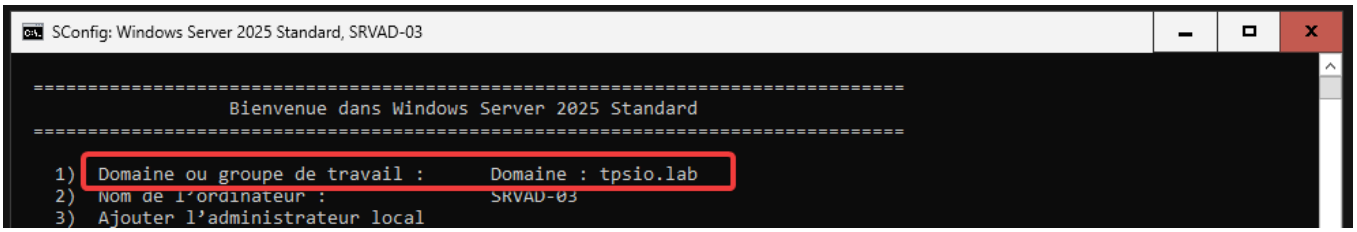
- Le changement du nom d'hôte
- Le changement de la configuration réseau
- L'activation du bureau à distance
- L'ajout au domaine





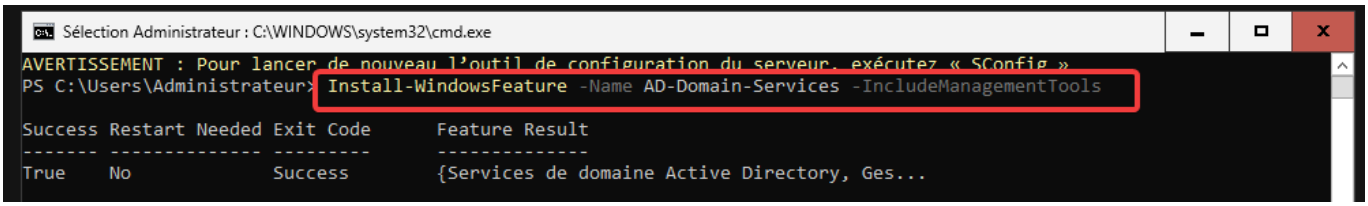




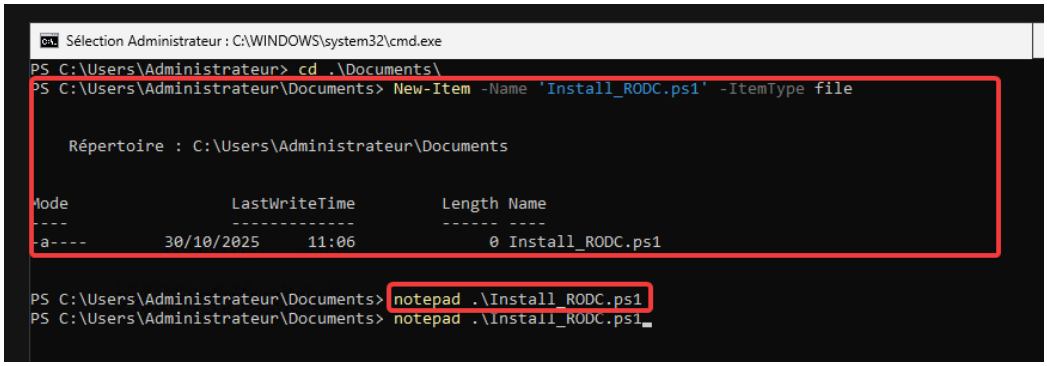


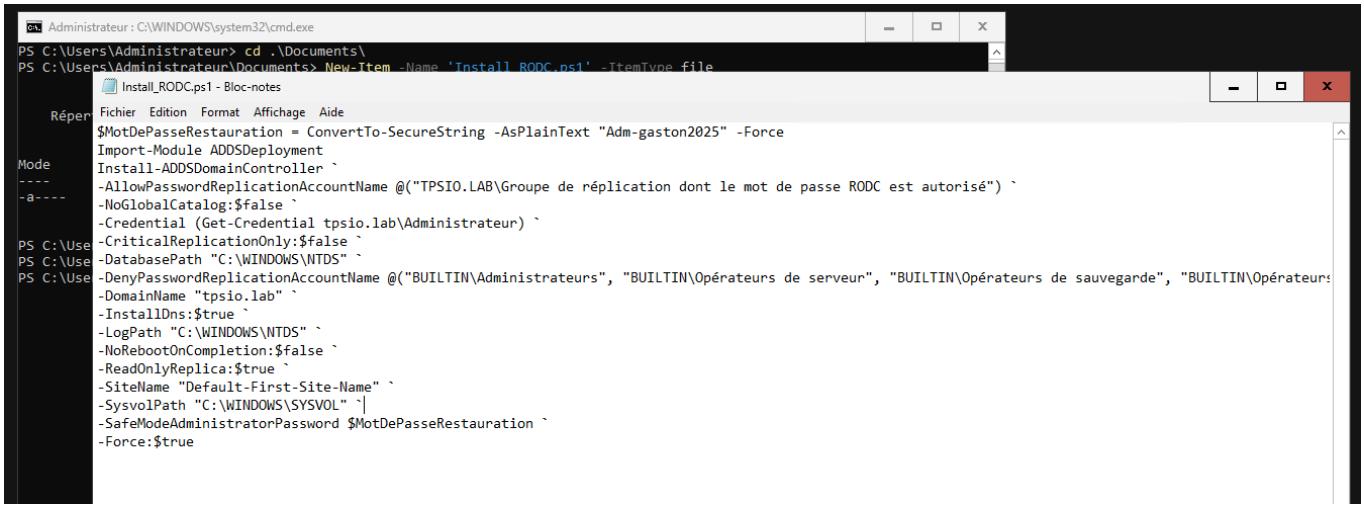
2. Installation & Configuration d'ADDS :

SRVAD-03 est maintenant bien configuré, comme pour SRVAD-02 nous allons passer par un script powershell afin de faire la promotion en RODC cette fois-ci. Nous allons déjà installer le rôle ADDS :



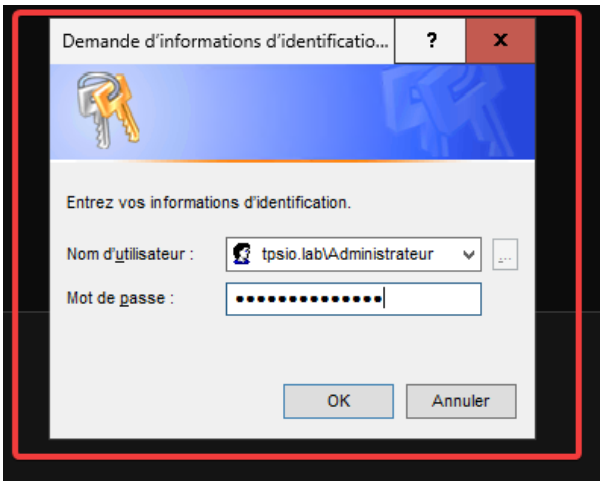
Et en suite créer notre script qui fera la promotion & la configuration du RODC :





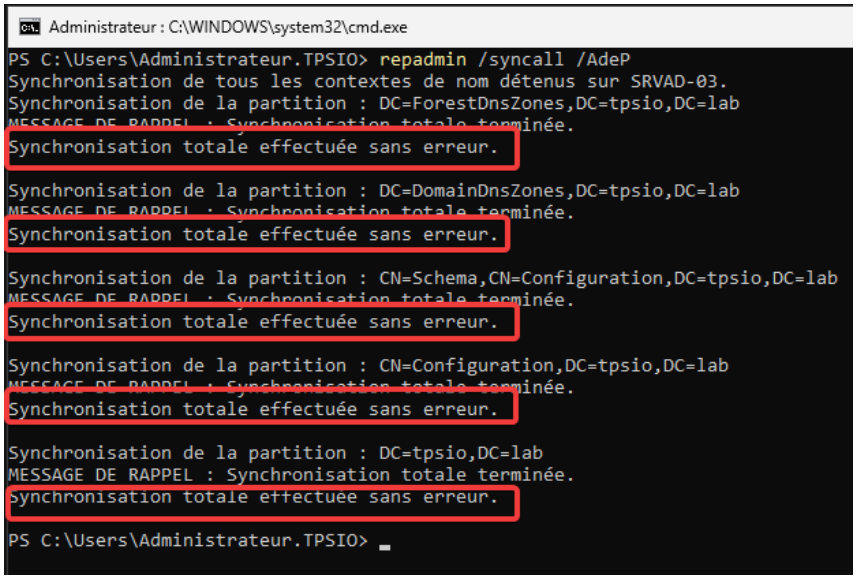
Il suffit maintenant de l'exécuter, et comme pour le RWDC, de rentrer les identifiants du compte Administrateur :

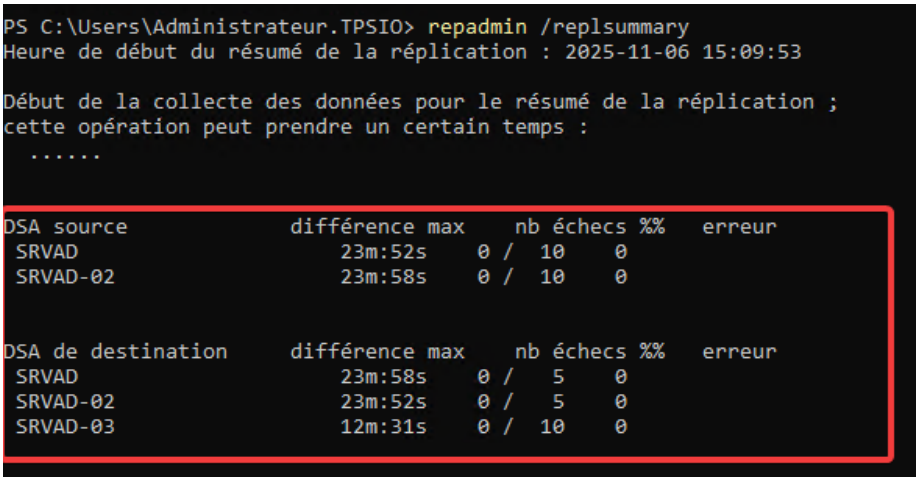
```
PS C:\Users\Administrateur\Documents> powershell.exe -ExecutionPolicy bypass -File ".\Install_RODC.ps1"
```



3. Test de la réplication :

Une fois l'installation via le script terminée, il suffit de venir tester la réplication via les commandes repadmin :





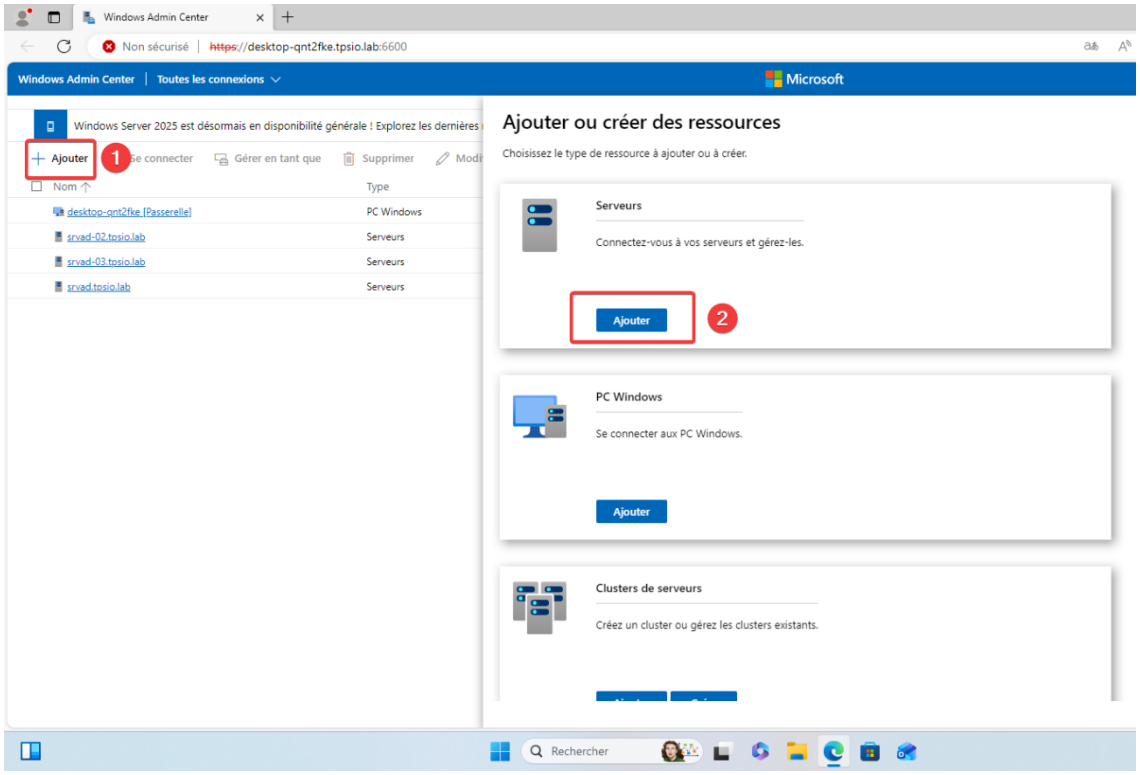
IV. Gestion à distance depuis un PC d'administration (PC-TECH)

À présent, nos serveurs sont bien répliqués ensemble dans notre infrastructure, avec SRVAD-02 en RWDC (lecture-écriture) et SRVAD-03 en RODC (lecture seule)

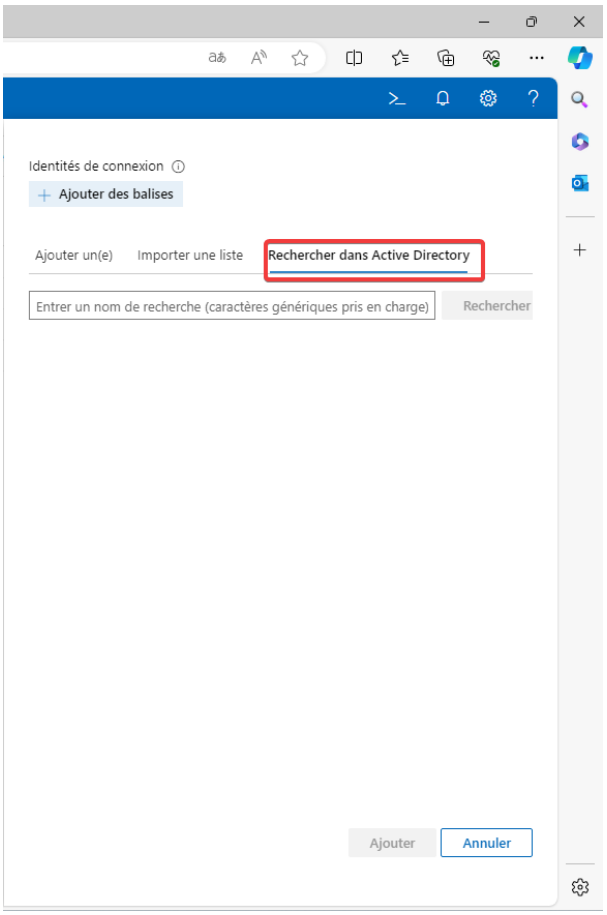
Avec la machine PC-TECH, qui est un client sous Windows 11 équipé de Windows Admin Center, nous allons pouvoir gérer ses machines à distance depuis l'interface.

1. Ajout des serveurs dans le WAC :

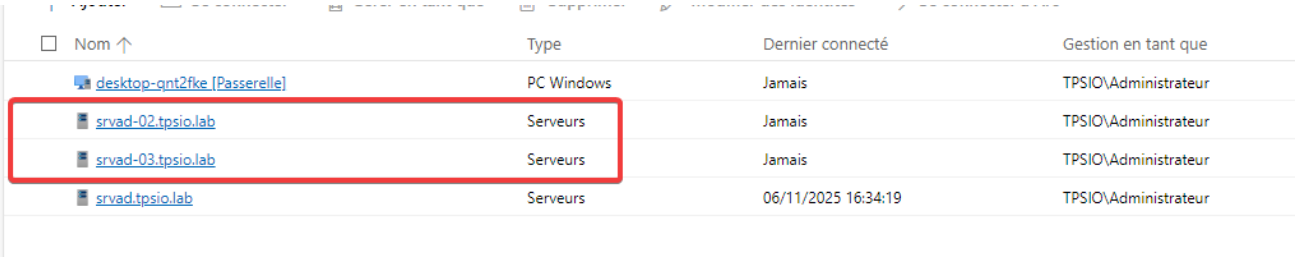
Une fois connecté sur l'interface d'administration, nous pouvons ajouter des serveurs en faisant la manipulation suivante :



Puis en recherchant dans l'active directory directement (et en tapant le nom du serveur en plus si nécessaire) :



Une fois les deux servers trouvés et ajoutés ils vont apparaître dans la liste avec notre serveur principal :

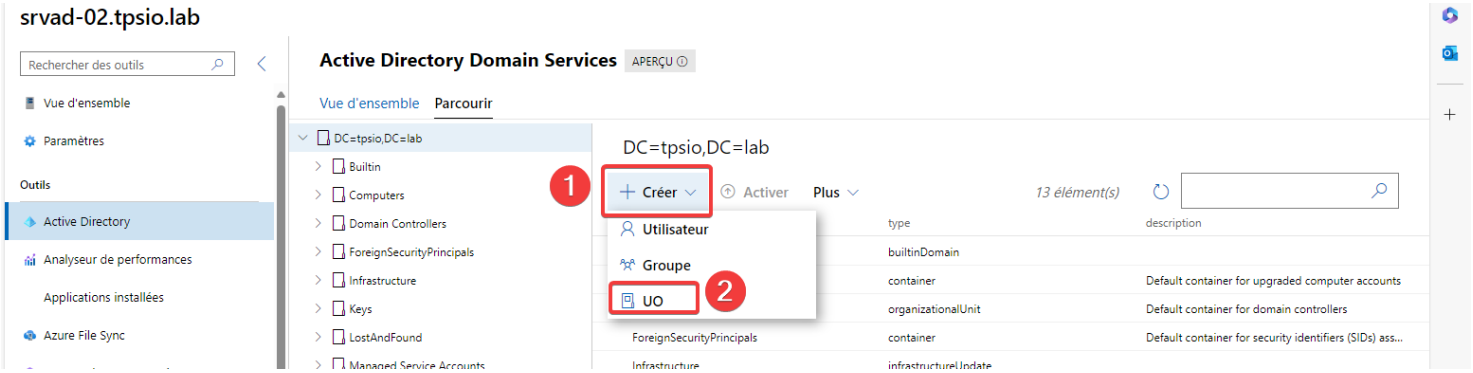


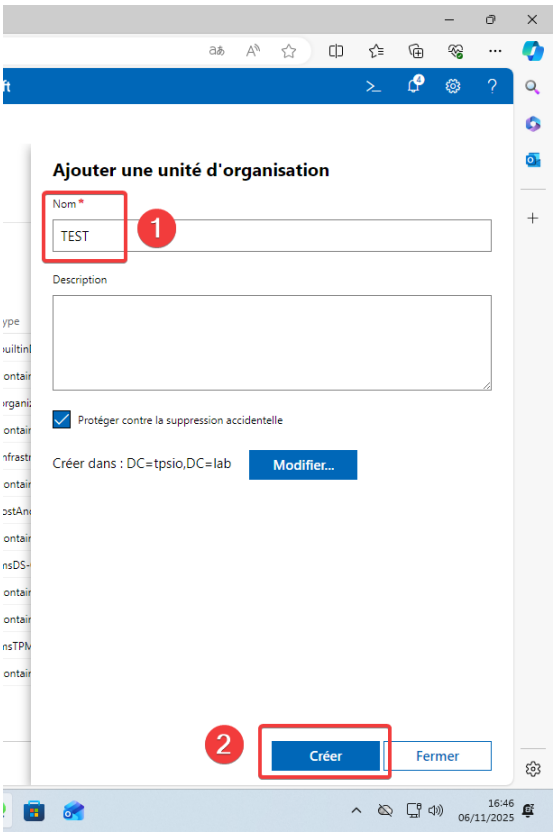
2. Gestion de l'AD dans le WAC :

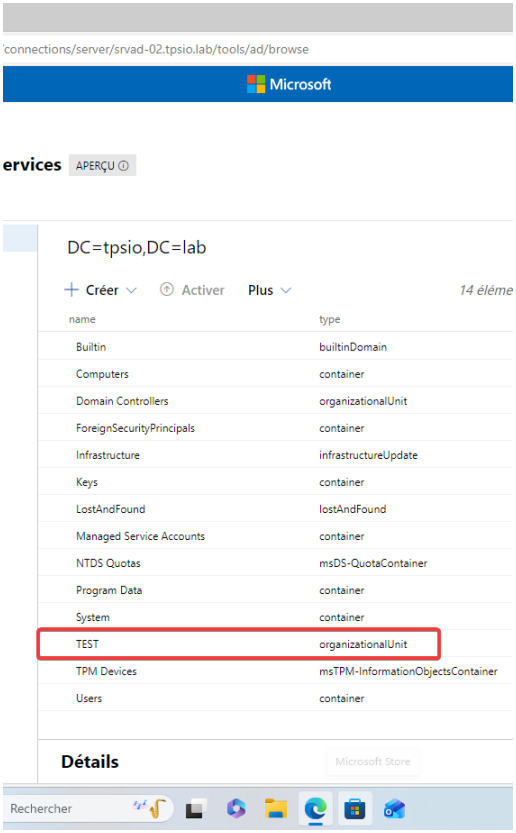
Une des fonctionnalités du Windows Admin Center qui va nous intéresser ici est la possibilité de gérer l'Active Directory et de pouvoir tester si la réplication fonctionne correctement.

Pour ce faire nous allons créer une OU Test et un utilisateur que nous appellerons toto pour les besoins de ce TP.

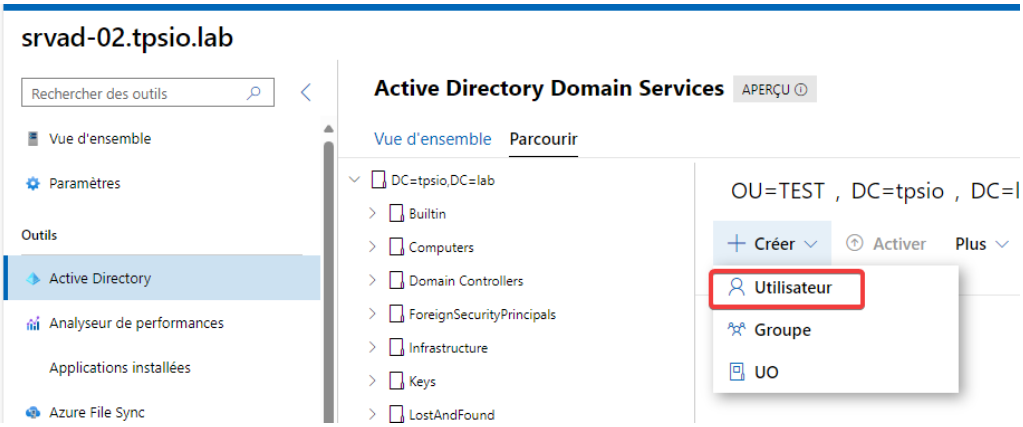
Pour ce faire il suffit de nous rendre sur un des serveurs et d'aller dans la rubrique Active Directory, puis parcourir et enfin d'appuyer sur le bouton « créer » :

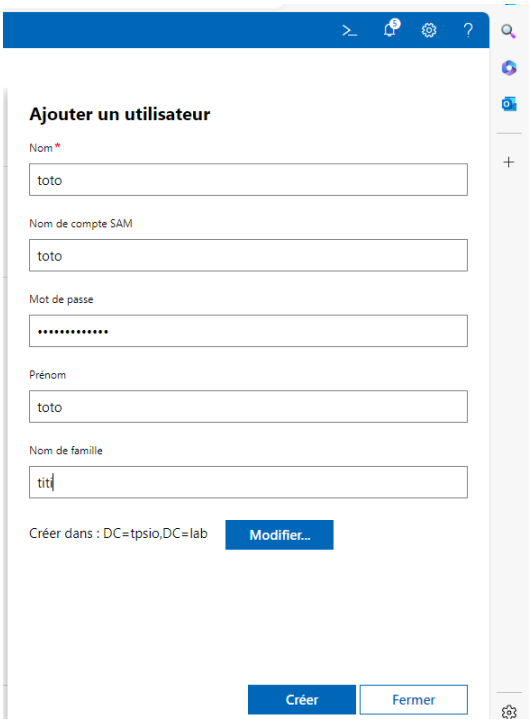


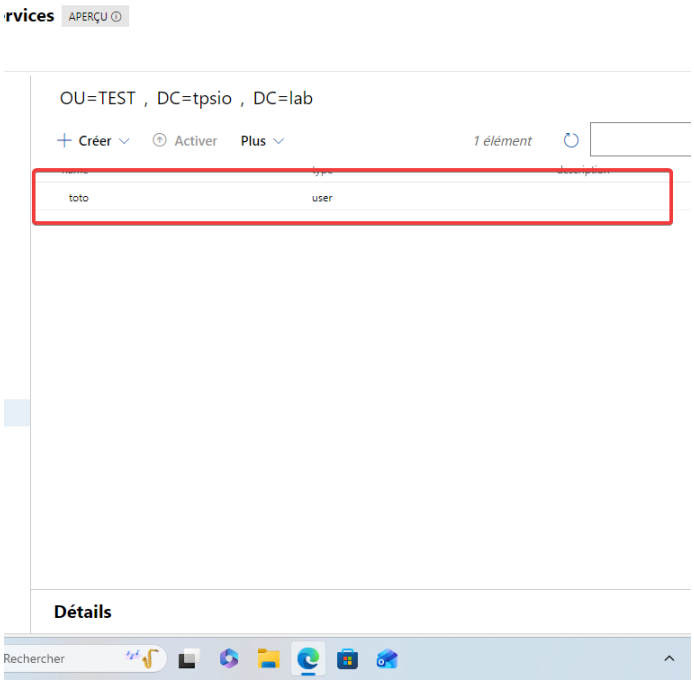




Maintenant que l'OU est bien créée, nous pouvons y ajouter un utilisateur toto :







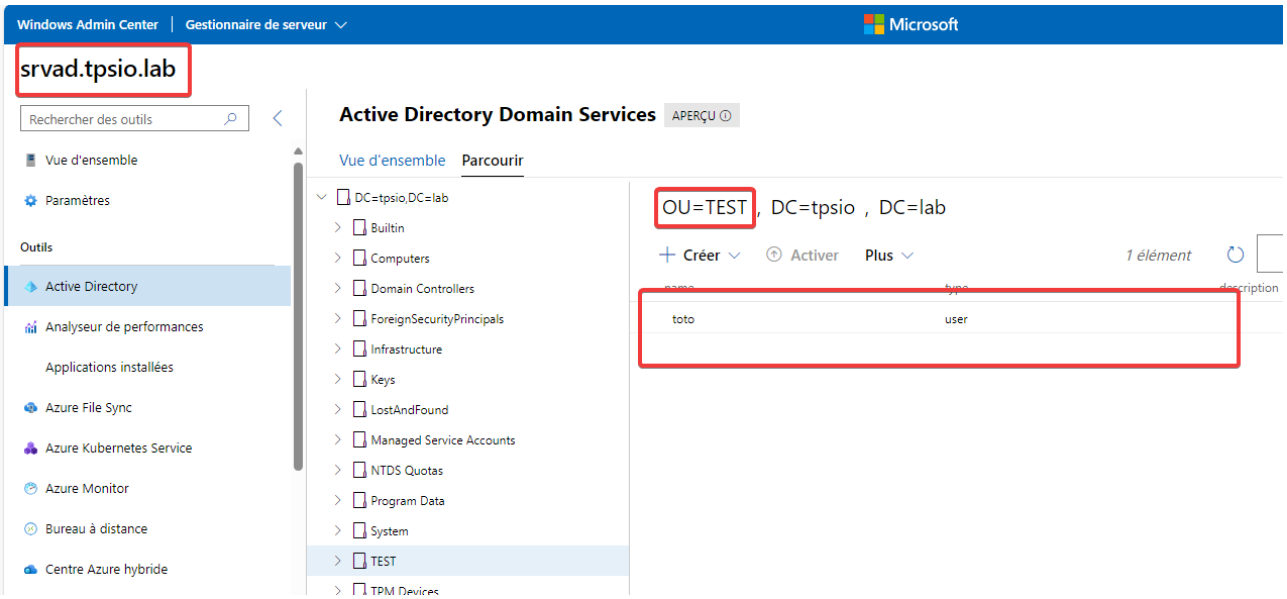
3. Test du bon fonctionnement de la réplication via le WAC :

Maintenant que notre OU et notre utilisateur est créé (depuis SRVAD-02) nous pouvons voir si la réplication que nous avons configurée précédemment fonctionne correctement. Normalement nous devrons trouver :

- L'OU et le compte sur les 3 DC
- L'impossibilité de modifier ou créer sur SRVAD-03 qui est en lecture seule.

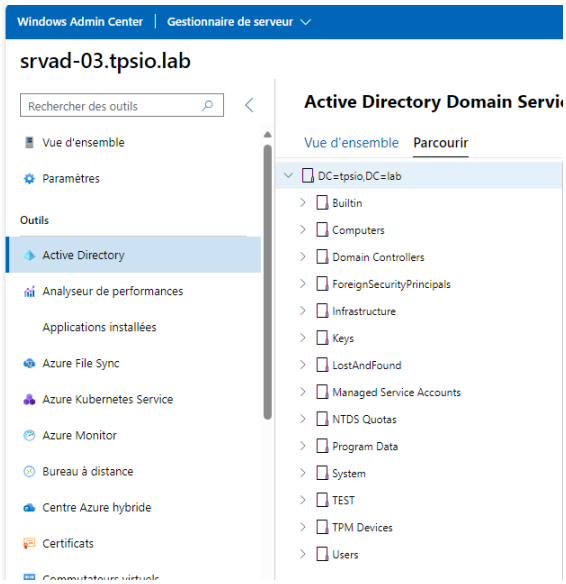
1. Sur SRVAD :

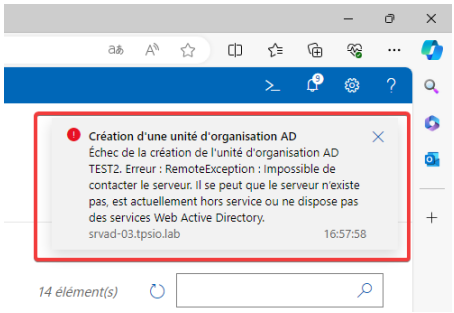
En nous rendant sur SRVAD, puis en parcourant son active directory, nous pouvons voir que l'OU et le compte sont bien présents :



2. Sur SRVAD-03 :

Sur SRVAD-03, l'OU & le compte sont bien présents, et en essayant de créer une nouvelle OU nous avons un message d'erreur qui nous l'empêche :

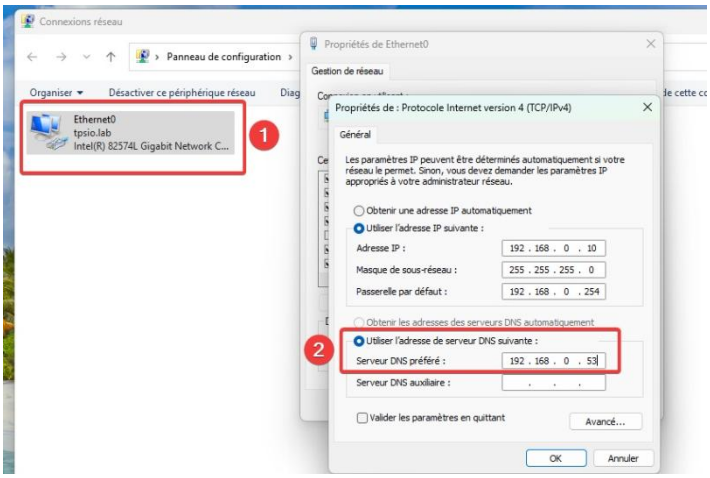




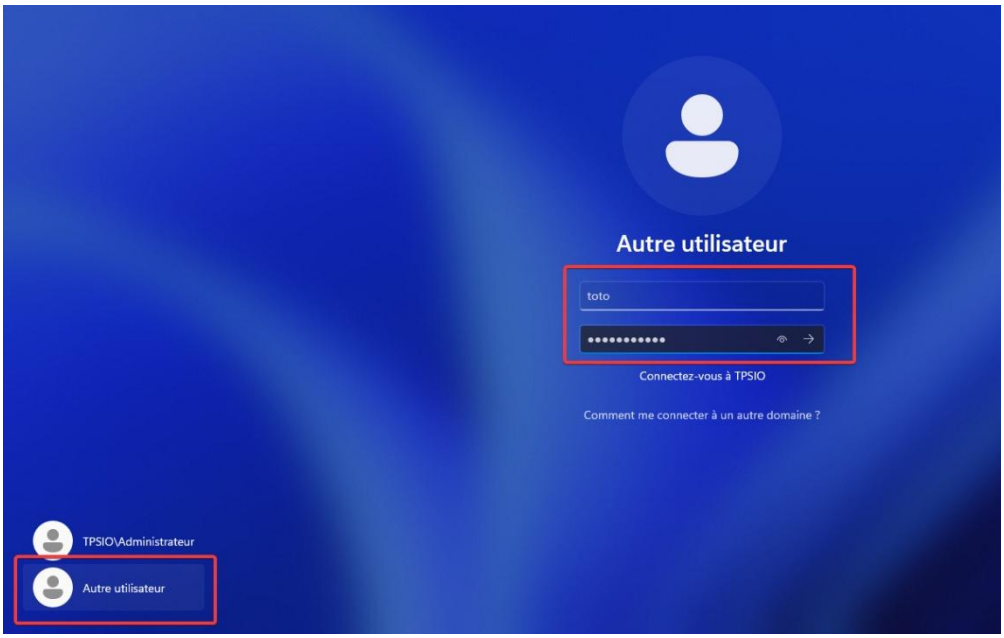
4. Test d'authentification depuis SRVAD-03 :

Notre dernier test consiste à essayer de s'authentifier avec notre utilisateur toto depuis notre PC-TECH en ne passant que par SRVAD-03 pour s'assurer que tout fonctionne correctement et que les DC sont officiellement bien déployés.

Pour ce faire, nous allons changer la configuration DNS afin de ne mettre que l'adresse de SRVAD-03 :



Pour finir il nous suffit de nous déconnecter ou de redémarrer le poste pour essayer de nous connecter avec l'utilisateur toto :



L'authentification sur SRVAD-03 à bien fonctionné, notre infrastructure de réplication Active Directory est fonctionnelle pour les utilisateurs !