

TP – Réplication Active Directory & gestion via WAC

Table des matières

I.	Contexte	2
II.	Objectifs	2
III.	Mise en place de l'infrastructure AD DS	2
1.	Déploiement du RWDC (SRVAD-02) :	3
1.	Configuration basique :	3
2.	Installation & configuration d'ADDS :	6
3.	Test de la réplication :	8
2.	Déploiement du RODC (SRVAD-03) :	9
1.	Configuration Basique :	9
2.	Installation & Configuration d'ADDS :	10
3.	Test de la réplication :	12
IV.	Gestion à distance depuis un PC d'administration (PC-TECH)	12
1.	Ajout des serveurs dans le WAC :	12
2.	Gestion de l'AD dans le WAC :	14
3.	Test du bon fonctionnement de la réplication via le WAC :	15
1.	Sur SRVAD :	15
2.	Sur SRVAD-03 :	16
4.	Test d'authentification depuis SRVAD-03 :	16

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.

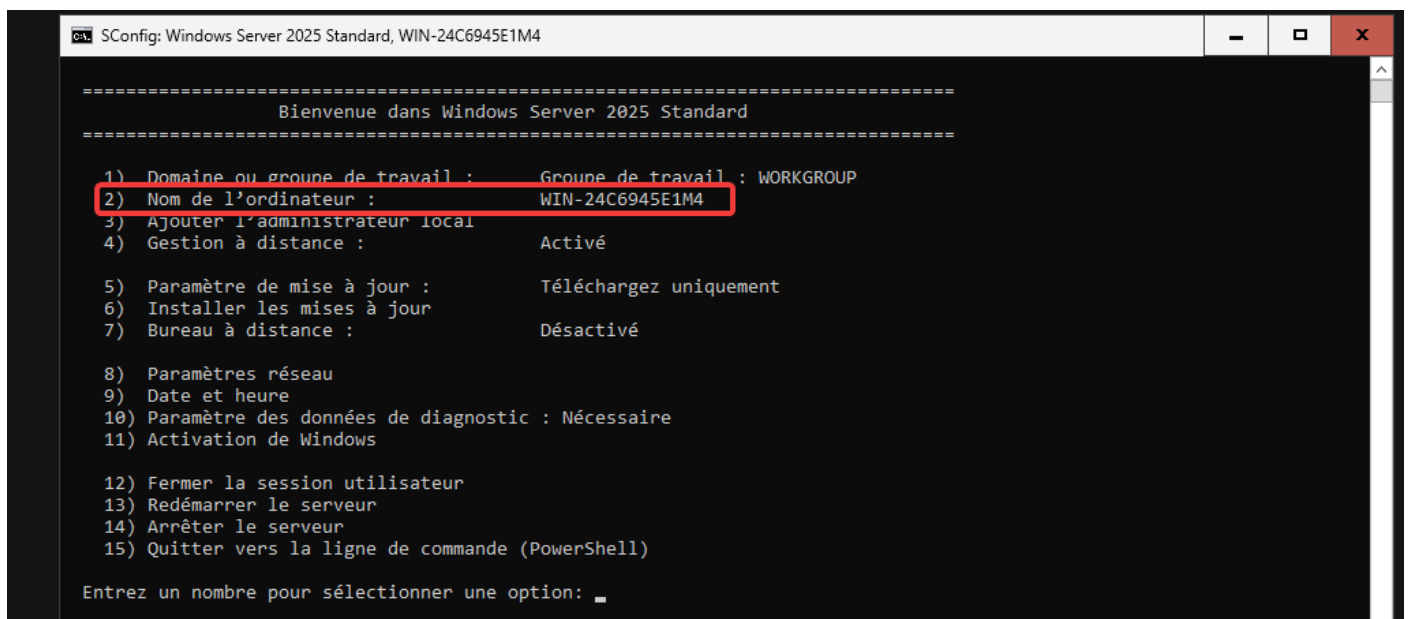
1. Configuration basique :

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

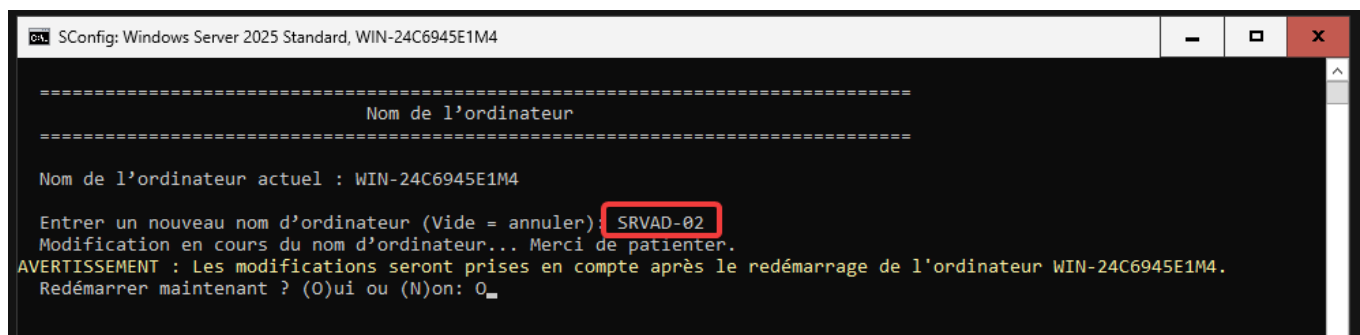
Nous allons effectuer les premières configurations avant de le promouvoir contrôleur de domaine, qui sont les suivantes :

- 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.

```
Sélection SConfig: Windows Server 2025 Standard, SRVAD-02
AVERTISSEMENT : Pour empêcher le lancement de SConfig lors de la connexion, tapez « Set-SConfig -AutoLaunch $false »

=====
Bienvenue dans Windows Server 2025 Standard
=====

1) Domaine ou groupe de travail : Groupe de travail : WORKGROUP
2) Nom de l'ordinateur : SRVAD-02
3) Ajouter l'administrateur local
4) Gestion à distance : Activé
```

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 » :

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

=====
Paramètres réseau
=====

Cartes réseau disponibles :

# | Adresse IP | Nom | Description
7 | 169.254.157.152 | Ethernet0 | Intel(R) 82574L Gigabit Network Connecti...
5 | 192.168.13.129 | Ethernet1 | Intel(R) 825/4L Gigabit Network Connecti...

Sélectionnez le numéro d'index de la carte réseau (Vide = annuler):
```

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 :

```
1) Définir l'adresse de la carte réseau
2) Définir les serveurs DNS
3) Effacer les paramètres du serveur DNS
4) Renommer la carte réseau

Entrez la sélection (Vide = annuler): 1
Sélectionnez le protocole (D)HCP ou l'adresse IP (S)tatique (Vide = annuler): S
Entrez une adresse IP statique : (Vide = annuler): 192.168.0.52
Entrez un masque de sous-réseau (Vide=255.255.255.0): 255.255.255.0
Entrez la passerelle par défaut (Vide = annuler): 192.168.0.254
```

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

```
Entrez la sélection (Vide = annuler): 2
Entrez le 1er serveur DNS (Vide = annuler): 192.168.0.1
Entrez le 2e serveur DNS (vide=aucun): 192.168.0.52
Entrez le 3e serveur DNS (vide=aucun): 192.168.0.53
```

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 sommes 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 :

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

=====
      Changer l'appartenance au domaine ou groupe de travail
=====

Actuel groupe de travail : WORKGROUP

Souhaitez-vous adhérer à un (D)omaine ou Groupe de (t)ravail? (Vide = annuler): D
Nom de domaine à joindre (Vide = annuler): tpsio.lab
Spécifier un domaine/utilisateur autorisé: (Vide = annuler): TPSIO\Administrateur
Mot de passe de TPSIO\Administrateur: *****
Vous rejoignez tpsio.lab... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur SRVAD-02.
Vous avez correctement rejoint le domaine.
Voulez-vous modifier le nom de l'ordinateur avant de redémarrer ? (O)ui ou (N)on: N
Redémarrer maintenant ? (O)ui ou (N)on: O
```

```
1) Domaine ou groupe de travail :   Domaine : tpsio.lab
2) Nom de l'ordinateur :           SRVAD-03
```

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**

```
Sélection Administrateur : C:\WINDOWS\system32\cmd.exe

AVERTISSEMENT : Pour lancer de nouveau l'outil de configuration du serveur exécutez « SConfig »
PS C:\Users\Administrateur> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
-----
True      No          Success          {Services de domaine Active Directory, Ges...
```

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

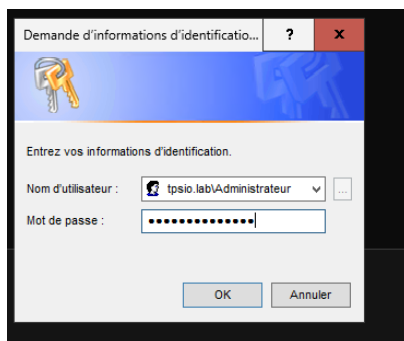
```
PS C:\Users\Administrateur> cd .\Documents\  
PS C:\Users\Administrateur\Documents> New-Item -Name "Install_RWDC.ps1" -ItemType file  
  
Répertoire : C:\Users\Administrateur\Documents  
  
Mode                LastWriteTime         Length Name  
----                -  
-a-----          31/10/2025    09:08             0 Install_RWDC.ps1  
  
PS C:\Users\Administrateur\Documents> notepad.exe .\Install_RWDC.ps1  
PS C:\Users\Administrateur\Documents>
```

```
*Install_RWDC.ps1 - Bloc-notes  
Fichier Edition Format Affichage Aide  
$NoCatalogueGlobal = $false  
$DelegationDNS = $false  
$Identifiant = (Get-Credential tpsio.lab\Administrateur)  
$CheminBDD = "C:\Windows\NTDS"  
$CheminLOG = "C:\Windows\NTDS"  
$NomDomaine = "tpsio.lab"  
$InstallationDNS = $true  
$NePasRebooter = $false  
$NomSite = "Default-First-Site-Name"  
$CheminSYSVOL = "C:\Windows\SYSVOL\  
$Replication = $false  
$MotDePasseRestauration = ConvertTo-SecureString -AsPlainText "Adm-gaston2025" -Force  
  
Install-ADDSDomainController -NoGlobalCatalog:$NoCatalogueGlobal `  
-CreateDnsDelegation:$DelegationDNS `  
-Credential:$Identifiant `  
-CriticalReplicationOnly:$Replication `  
-DatabasePath $CheminBDD `  
-DomainName $NomDomaine `  
-InstallDns:$InstallationDNS `  
-LogPath $CheminLOG `  
-NoRebootOnCompletion:$NePasRebooter `  
-SiteName $NomSite `  
-SysvolPath $CheminSYSVOL `  
-SafeModeAdministratorPassword $MotDePasseRestauration `  
-Force:$true `  
-Confirm:$false
```

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 :

```
C:\Sélection Administrateur : C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrateur\Documents> powershell.exe -Executionpolicy bypass -File ".\Install_RWDC.ps1"
```



```
C:\Sélection Administrateur : C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrateur\Documents> powershell.exe -Executionpolicy bypass -File ".\Install_RWDC.ps1"
AVERTISSEMENT : Cet ordinateur contient au moins une carte réseau physique pour laquelle aucune adresse IP statique n'a
Install-ADDSDomainController
Détermination du contrôleur de domaine source de réplication
Validation d'environnement et d'entrée utilisateur
Tous les tests ont réussi
[oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]
Installation d'un nouveau contrôleur de domaine
Vérification de l'état de mise à niveau du domaine
```

3. Test de la réplication :

L'installation étant maintenant terminée 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 :

```
C:\Administrateur : C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrateur\TPSIO> repadmin /syncall /AdeP
Synchronisation de tous les contextes de nom détenus sur SRVAD-02.
Synchronisation de la partition : DC=ForestDnsZones,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : La réplication suivante est en cours :
À partir de : CN=NTDS Settings,CN=SRVAD-02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
Vers..... : CN=NTDS Settings,CN=SRVAD,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : La réplication suivante s'est terminée correctement :
À partir de : CN=NTDS Settings,CN=SRVAD-02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
Vers..... : CN=NTDS Settings,CN=SRVAD,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : Synchronisation totale terminée.
Synchronisation totale effectuée sans erreur.
Synchronisation de la partition : DC=DomainDnsZones,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : La réplication suivante est en cours :
À partir de : CN=NTDS Settings,CN=SRVAD-02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
Vers..... : CN=NTDS Settings,CN=SRVAD,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : La réplication suivante s'est terminée correctement :
À partir de : CN=NTDS Settings,CN=SRVAD-02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
Vers..... : CN=NTDS Settings,CN=SRVAD,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : Synchronisation totale terminée.
Synchronisation totale effectuée sans erreur.
Synchronisation de la partition : CN=Schema,CN=Configuration,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : La réplication suivante est en cours :
À partir de : CN=NTDS Settings,CN=SRVAD-02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
Vers..... : CN=NTDS Settings,CN=SRVAD,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : La réplication suivante s'est terminée correctement :
À partir de : CN=NTDS Settings,CN=SRVAD-02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
Vers..... : CN=NTDS Settings,CN=SRVAD,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=tpcio,DC=lab
MESSAGE DE RAPPEL : Synchronisation totale terminée.
Synchronisation totale effectuée sans erreur.
```

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 :


```
Administrateur : C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrateur.TPSIO> repadmin /replsummary
Heure de début du résumé de la réplication : 2025-10-31 11:00:28

Début de la collecte des données pour le résumé de la réplication ;
cette opération peut prendre un certain temps :
.....

DSA source                différence max    nb échecs %%   erreur
SRVAD                     05m:09s        0 / 5    0
SRVAD-02                  :40s          0 / 5    0

DSA de destination        différence max    nb échecs %%   erreur
SRVAD                     :41s          0 / 5    0
SRVAD-02                  05m:09s        0 / 5    0
```

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

```
SConfig: Windows Server 2025 Standard, WIN-VM12084VLQ0

=====
Nom de l'ordinateur
=====

Nom de l'ordinateur actuel : WIN-VM12084VLQ0

Entrer un nouveau nom d'ordinateur (Vide = annuler): SRVAD-03
Modification en cours du nom d'ordinateur... Merci de patienter.
AVERTISSEMENT : Les modifications seront prises en compte après le redémarrage de l'ordinateur WIN-VM12084VLQ0.
Redémarrer maintenant ? (O)ui ou (N)on: 0_
```

```
1) Domaine ou groupe de travail : Groupe de travail : WORKGROUP
2) Nom de l'ordinateur : SRVAD-03
3) Ajouter l'administrateur local
```

```
SConfig: Windows Server 2025 Standard, SRVAD-03.tpsio.lab

=====
Paramètres de carte réseau
=====

Index NIC : 3
Nom : Ethernet0
Description : Intel(R) 82574L Gigabit Network Connection
Adresse IP : 192.168.0.53
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
```

```
SConfig: Windows Server 2025 Standard, SRVAD-03

=====
Bienvenue dans Windows Server 2025 Standard
=====

1) Domaine ou groupe de travail :   Groupe de travail : WORKGROUP
2) Nom de l'ordinateur :           SRVAD-03
3) Ajouter l'administrateur local
4) Gestion à distance :             Activé

5) Paramètre de mise à jour :       Téléchargez uniquement
6) Installer les mises à jour
7) Bureau à distance :              Activé (tous les clients)
8) Paramètres réseau
9) Date et heure
10) Paramètres des données de diagnostic : Nécessaire
```

```
SConfig: Windows Server 2025 Standard, SRVAD-03

=====
Bienvenue dans Windows Server 2025 Standard
=====

1) Domaine ou groupe de travail :   Domaine : tpsio.lab
2) Nom de l'ordinateur :             SRVAD-03
3) Ajouter l'administrateur local
```

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 :

```
Sélection Administrateur : C:\WINDOWS\system32\cmd.exe

AVERTISSEMENT : Pour lancer de nouveau l'outil de configuration du serveur, exécutez « SConfig »
PS C:\Users\Administrateur> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
-----
True      No          Success      {Services de domaine Active Directory, Ges...
```

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

```
Sélection Administrateur : C:\WINDOWS\system32\cmd.exe

PS C:\Users\Administrateur> cd .\Documents\
PS C:\Users\Administrateur\Documents> New-Item -Name 'Install_RODC.ps1' -ItemType file

Répertoire : C:\Users\Administrateur\Documents

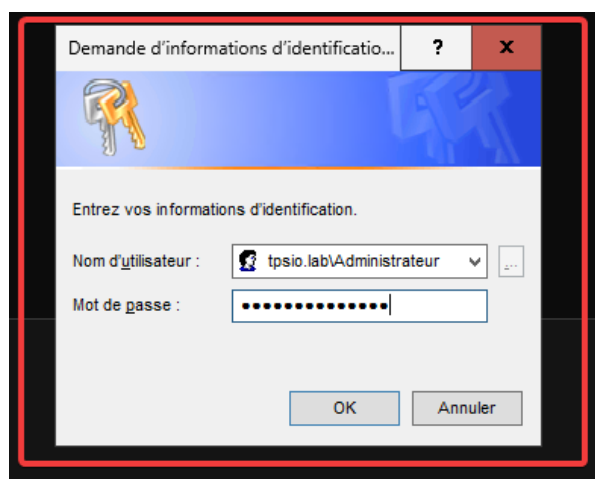
Mode                LastWriteTime         Length Name
----                -
-a----           30/10/2025    11:06             0 Install_RODC.ps1

PS C:\Users\Administrateur\Documents> notepad .\Install_RODC.ps1
PS C:\Users\Administrateur\Documents> notepad .\Install_RODC.ps1
```

```
Administrateur : C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrateur> cd .\Documents\
PS C:\Users\Administrateur\Documents> New-Item -Name 'Install_RODC.ps1' -ItemType file
Install_RODC.ps1 - Bloc-notes
Fichier Edition Format Affichage Aide
$MotDePasseRestauration = ConvertTo-SecureString "Adm-gaston2025" -Force
Import-Module ADDSDeployment
Install-ADDSDomainController `
-AllowPasswordReplicationAccountName @("TPSIO.LAB\Groupe de réplcation dont le mot de passe RODC est autorisé") `
-NoGlobalCatalog:$false `
-Credential (Get-Credential tpsio.lab\Administrateur) `
-CriticalReplicationOnly:$false `
-DatabasePath "C:\WINDOWS\NTDS" `
-DenyPasswordReplicationAccountName @("BUILTIN\Administrateurs", "BUILTIN\Opérateurs de serveur", "BUILTIN\Opérateurs de sauvegarde", "BUILTIN\Opérateurs de sauvegarde") `
-DomainName "tpsio.lab" `
-InstallDns:$true `
-LogPath "C:\WINDOWS\NTDS" `
-NoRebootOnCompletion:$false `
-ReadOnlyReplica:$true `
-SiteName "Default-First-Site-Name" `
-SysvolPath "C:\WINDOWS\SYSVOL" `
-SafeModeAdministratorPassword $MotDePasseRestauration `
-Force:$true
```

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 :

```
Administrateur : C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrateur.TPSIO> repadmin /syncall /AdeP
Synchronisation de tous les contextes de nom détenus sur SRVAD-03.
Synchronisation de la partition : DC=ForestDnsZones,DC=tpsio,DC=lab
MESSAGE DE RAPPEL : Synchronisation totale terminée.
Synchronisation totale effectuée sans erreur.

Synchronisation de la partition : DC=DomainDnsZones,DC=tpsio,DC=lab
MESSAGE DE RAPPEL : Synchronisation totale terminée.
Synchronisation totale effectuée sans erreur.

Synchronisation de la partition : CN=Schema,CN=Configuration,DC=tpsio,DC=lab
MESSAGE DE RAPPEL : Synchronisation totale terminée.
Synchronisation totale effectuée sans erreur.

Synchronisation de la partition : CN=Configuration,DC=tpsio,DC=lab
MESSAGE DE RAPPEL : Synchronisation totale terminée.
Synchronisation totale effectuée sans erreur.

Synchronisation de la partition : DC=tpsio,DC=lab
MESSAGE DE RAPPEL : Synchronisation totale terminée.
Synchronisation totale effectuée sans erreur.

PS C:\Users\Administrateur.TPSIO>
```

```
PS C:\Users\Administrateur.TPSIO> repadmin /replsummary
Heure de début du résumé de la réplication : 2025-11-06 15:09:53

Début de la collecte des données pour le résumé de la réplication ;
cette opération peut prendre un certain temps :
.....

DSA source      différence max  nb échecs %  erreur
SRVAD           23m:52s      0 / 10  0
SRVAD-02        23m:58s      0 / 10  0

DSA de destination  différence max  nb échecs %  erreur
SRVAD             23m:58s      0 / 5  0
SRVAD-02          23m:52s      0 / 5  0
SRVAD-03         12m:31s      0 / 10  0
```

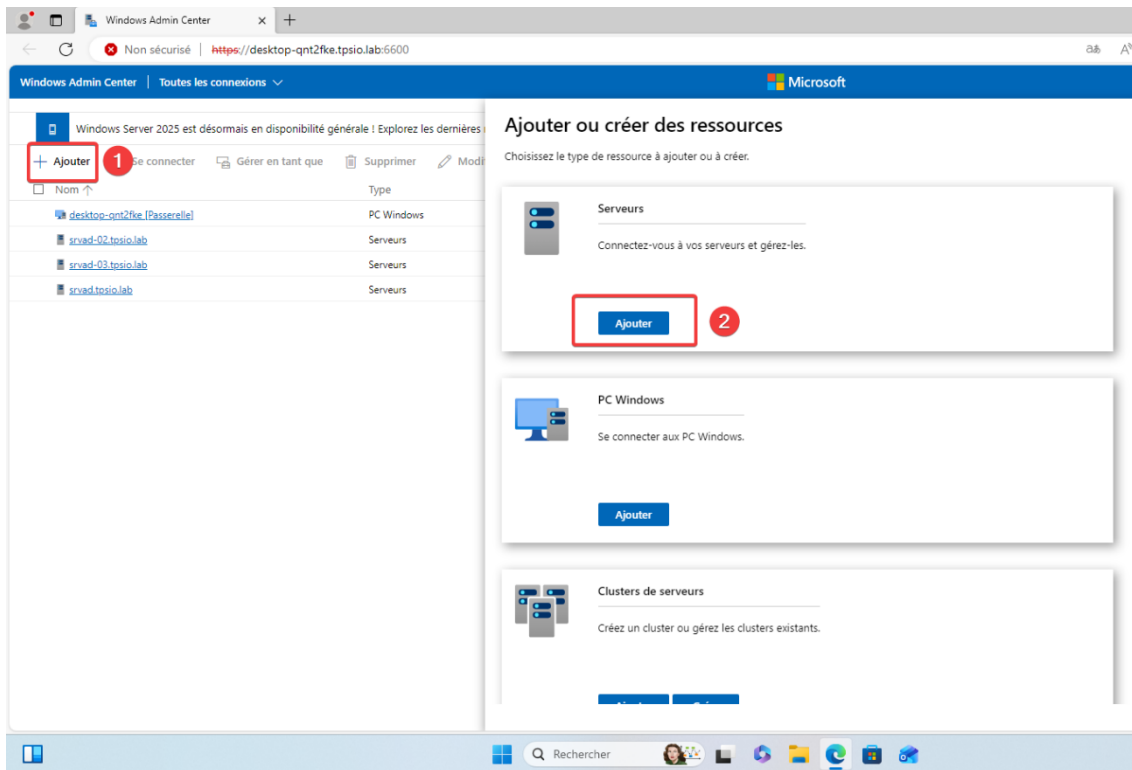
IV. Gestion à distance depuis un PC d'administration (PC-TECH)

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)

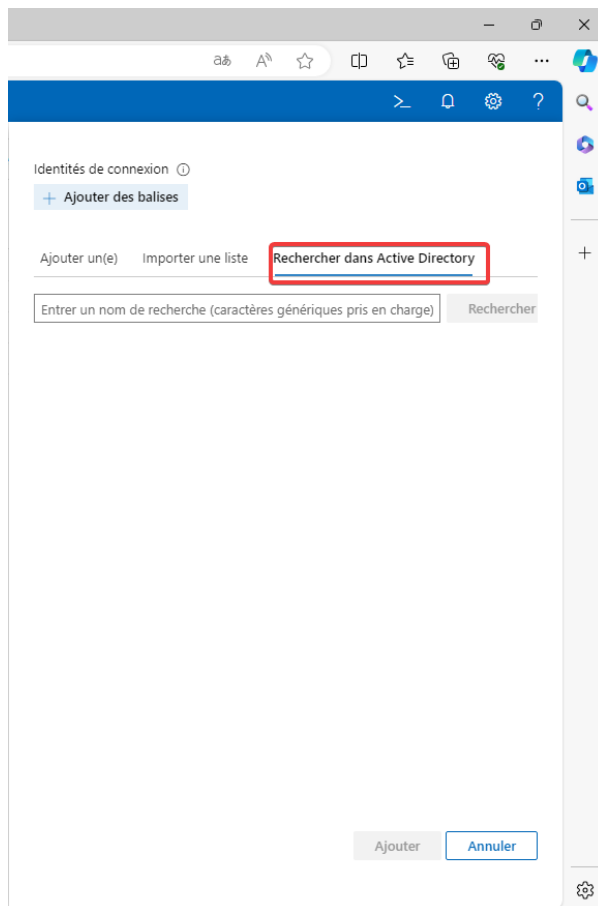
Avec la machine PC-TECH, qui est un client sous Windows 11 équipé de Windows Admin Center, nous allons pouvoir gérer ses machines à distance depuis l'interface.

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 :

☐ Nom ↑	Type	Dernier connecté	Gestion en tant que
desktop-gnt2fke [Passerelle]	PC Windows	Jamais	TPSIO\Administrateur
srvad-02.tpsio.lab	Serveurs	Jamais	TPSIO\Administrateur
srvad-03.tpsio.lab	Serveurs	Jamais	TPSIO\Administrateur
srvad.tpsio.lab	Serveurs	06/11/2025 16:34:19	TPSIO\Administrateur

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 » :

srvad-02.tpsio.lab

Rechercher des outils

Vue d'ensemble Paramètres Outils

Active Directory

Analyseur de performances Applications installées Azure File Sync

Active Directory Domain Services APERÇU

Vue d'ensemble Parcourir

DC=tpsio,DC=lab

1 + Créer 2 Utilisateur Groupe UO

13 élément(s)

type	description
builtinDomain	
container	Default container for upgraded computer accounts
organizationalUnit	Default container for domain controllers
container	Default container for security identifiers (SIDs) ass...
ForeignSecurityPrincipals	
Infrastructure	infrastructureUpdate

Ajouter une unité d'organisation

Nom * 1 TEST

Description

☒ Protéger contre la suppression accidentelle

Créer dans : DC=tpsio,DC=lab

2 Créer Fermer

connections/server/srvad-02.tpsio.lab/tools/ad/browse

Microsoft

services APERÇU

DC=tpsio,DC=lab

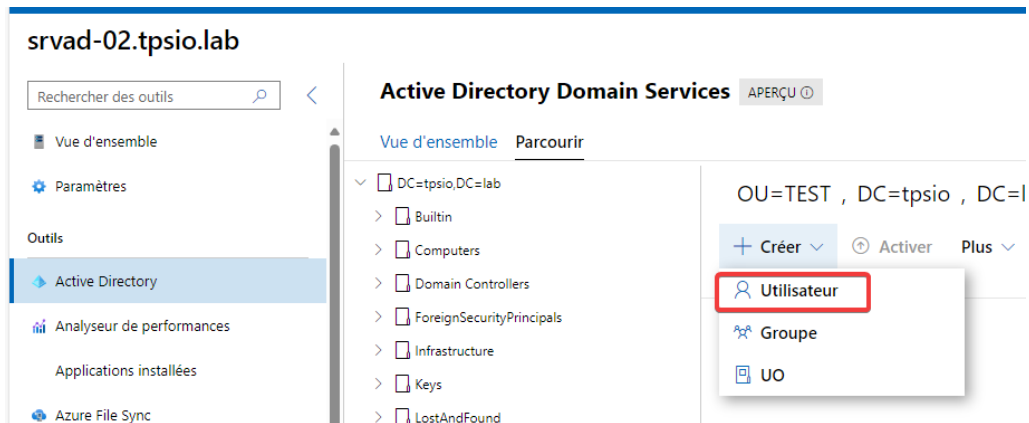
+ Créer Activer Plus 14 élém

name	type
Builtin	builtinDomain
Computers	container
Domain Controllers	organizationalUnit
ForeignSecurityPrincipals	container
Infrastructure	infrastructureUpdate
Keys	container
LostAndFound	lostAndFound
Managed Service Accounts	container
NTDS Quotas	msDS-QuotaContainer
Program Data	container
System	container
TEST	organizationalUnit
TPM Devices	msTPM-InformationObjectsContainer
Users	container

Détails

Rechercher

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



Ajouter un utilisateur

Nom *
toto

Nom de compte SAM
toto

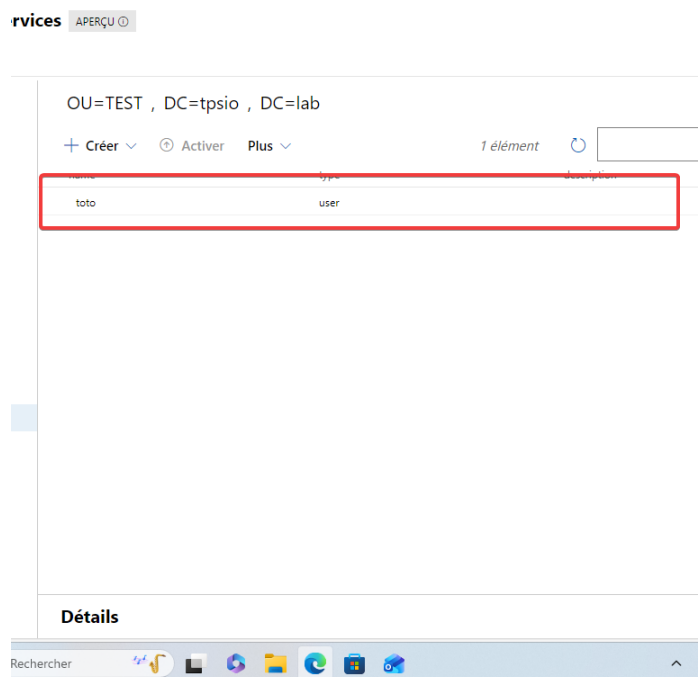
Mot de passe

Prénom
toto

Nom de famille
titit

Créer dans : DC=tpsio,DC=lab [Modifier...](#)

[Créer](#) [Fermer](#)



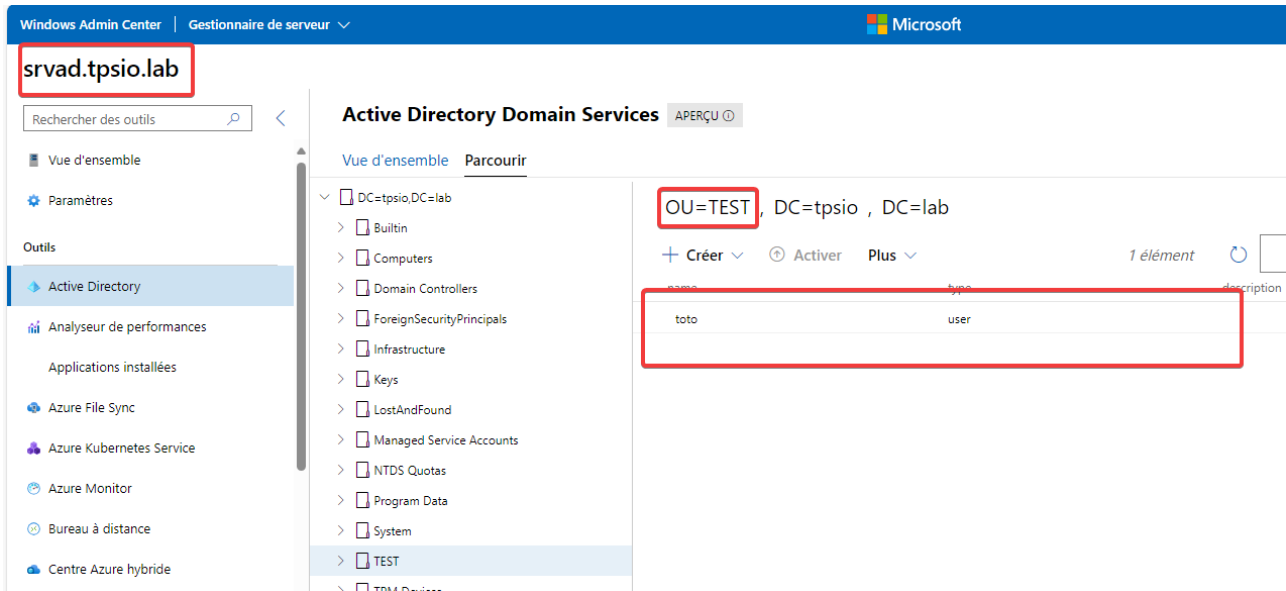
3. Test du bon fonctionnement de la réplication via le WAC :

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 devons trouver :

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

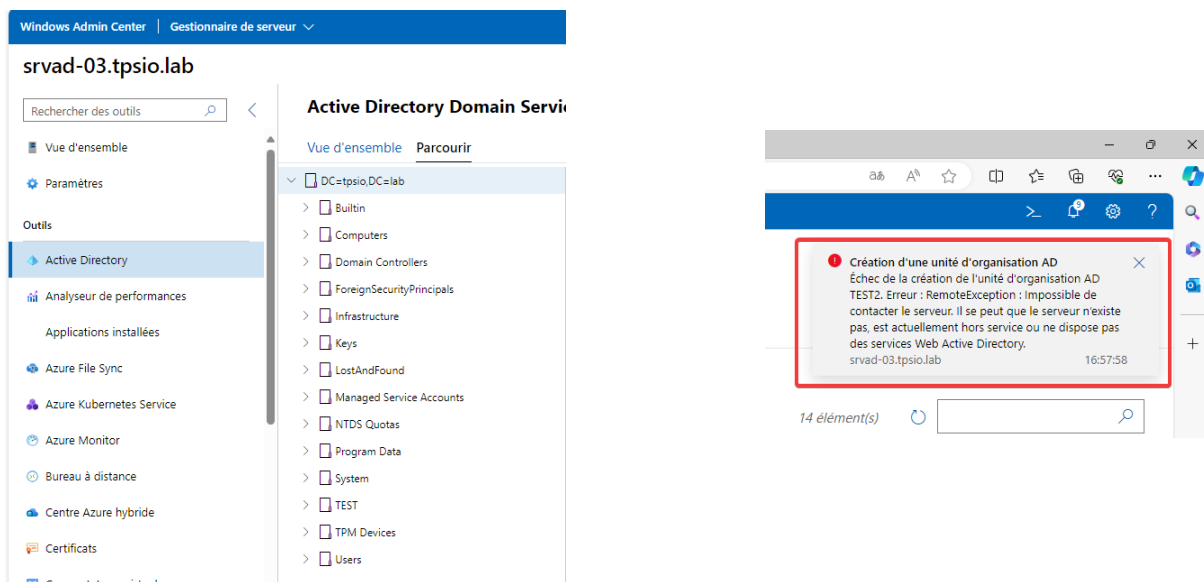
1. Sur SRVAD :

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 :

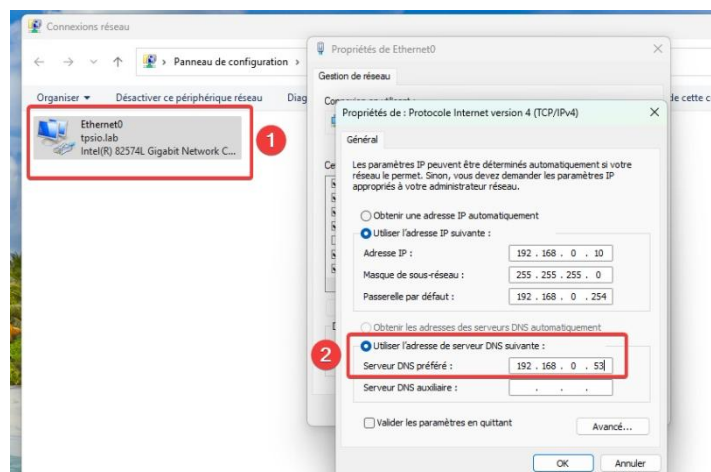
Sur SRVAD-03, l'OU & le compte sont bien présents, et en essayant de créer une nouvelle OU nous avons un message d'erreur qui nous l'empêche :



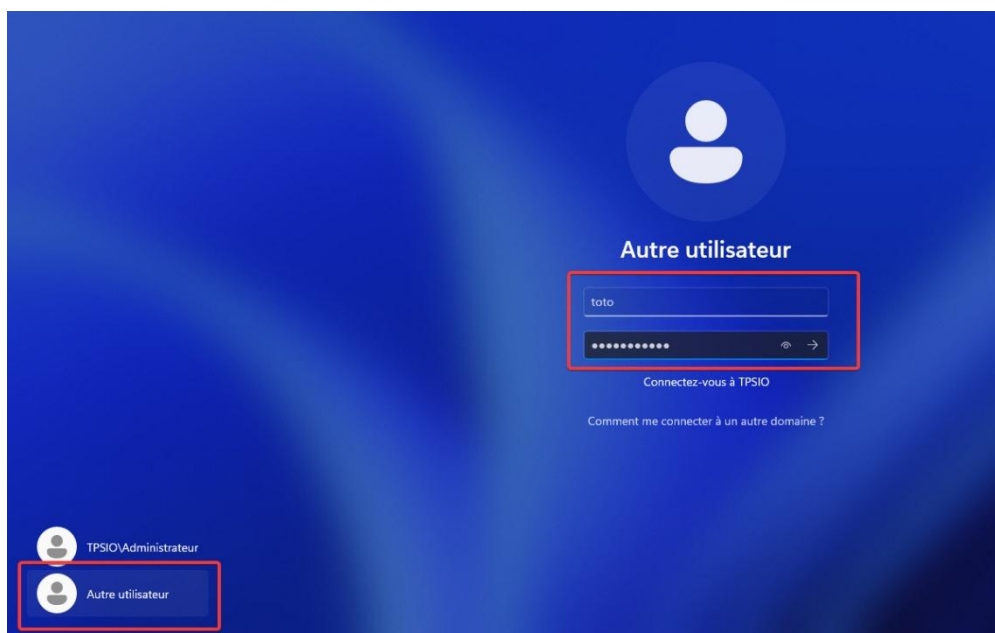
4. Test d'authentification depuis SRVAD-03 :

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 !

