

MISE EN PLACE D'UN ACTIVE  
DIRECTORY  
INSTALLATION ET CONFIGURATION



Réalisé par : **SOULAIMAN Rayane**  
Administrateur système, réseau et sécurité

## Table des matières

<b>1. PRÉSENTATION DU GUIDE .....</b>	2
1.1. À propos de Windows Server 2025 .....	2
1.2. L'Active Directory et son rôle .....	2
1.3. Objectif du guide .....	2
1.4. Prérequis matériels et logiciels .....	2
1.5. Schéma réseau .....	3
1.6. Méthodologie.....	3
<b>2. INSTALLATION ET PROMOTION D'UN CONTRÔLEUR DE DOMAINE ACTIVE DIRECTORY.....</b>	3
2.1. Configuration de l'environnement réseau.....	3
2.2. Installer le rôle Active Directory .....	5
2.3. Promouvoir le serveur en contrôleur de domaine .....	7
<b>3. GESTION DES UNITÉS D'ORGANISATION (OU) .....</b>	9
3.1. Comprendre le rôle des Unités d'Organisation.....	9
3.2. Création d'une Unité d'Organisation (OU) .....	9
3.3. Organisation hiérarchique recommandée .....	12
<b>4. CRÉATION D'UTILISATEURS ET INTÉGRATION D'UN POSTE WINDOWS 11 .....</b>	13
4.1. Création d'un utilisateur .....	13
4.2. Ajout d'une machine Windows 11 au domaine .....	15
<b>5. MISE EN ŒUVRE DES STRATÉGIES DE GROUPE (GPO).....</b>	18
5.1. Type de groupes et bonnes pratiques .....	18
5.2. Création d'un groupe .....	18
5.3. Ajouter un utilisateur dans le groupe .....	19
<b>6. CRÉATION ET GESTION DES STRATÉGIES DE GROUPES (GPO).....</b>	21
6.1. Qu'est-ce qu'une GPO ?.....	22
6.2. Comment créer une GPO et la lier au domaine ?.....	22
6.3. Comment forcer le fond d'écran sur tous les postes des utilisateurs ?.....	22
<b>CONCLUSION .....</b>	28

## 1. PRÉSENTATION DU GUIDE

### 1.1. À propos de Windows Server 2025

Windows Server 2025 est la dernière version du système serveur de Microsoft, conçue pour répondre aux besoins modernes des infrastructures informatiques. Elle offre de meilleures performances, une sécurité renforcée et une intégration fluide avec les environnements hybrides (cloud + local).

Cette version met particulièrement l'accent sur :

- La sécurité des identités et des accès,
- La gestion simplifiée des rôles et fonctionnalités,
- La compatibilité accrue avec les environnements Windows 11 et Azure,
- Et le renforcement de la stabilité du noyau serveur.

Dans les entreprises, Windows Server 2025 constitue une **plateforme solide** pour déployer des services réseau essentiels, dont l'**Active Directory Domain Services (AD DS)**.

### 1.2. L'Active Directory et son rôle

L'Active Directory (AD DS) est un service annuaire intégré à Windows Server qui permet de :

- Centraliser la gestion des utilisateurs, ordinateurs et ressources d'un réseau ;
- Authentifier et autoriser les utilisateurs lors de leur connexion au domaine ;
- Appliquer des stratégies de sécurité (GPO) de manière uniforme sur tous les postes ;
- Faciliter l'administration grâce à une organisation hiérarchique et logique du réseau.

En résumé, l'AD est le **cœur de l'infrastructure réseau Windows**, gérant identités, sécurité et communication entre tous les éléments du domaine.

### 1.3. Objectif du guide

Ce guide pratique a pour objectif de **décrire pas à pas la mise en place d'un Active Directory sous Windows Server 2025** dans un **environnement virtualisé avec VirtualBox**.

A la fin, vous serez capable de :

- Installer et promouvoir un serveur en contrôleur de domaine ;
- Créer des unités d'organisation (OU) adaptées à la structure de votre entreprise ;
- Gérer des utilisateurs et groupes de manière centralisée ;
- Intégrer des postes Windows 11 au domaine ;
- Appliquer des stratégies de groupe (GPO) pour sécuriser et uniformiser les postes

### 1.4. Prérequis matériels et logiciels

Avant de commencer, assurez-vous de disposer de l'environnement suivant :

- **Matériel (pour la VM) :** 2 GHz processeur minimum, 4-8 Go RAM, 60 Go disque, réseau interne VirtualBox
- **Logiciels :** Windows Server 2025, Windows 11 Pro, outils d'administration

### 1.5. Schéma réseau

Toutes les manipulations seront faites dans VirtualBox avec deux machines virtuelles :

Equipement	Nom de la machine	Adresse IP	Rôle
Serveur	SRV-AD	192.168.90.20	Contrôleur de domaine + DNS
Poste client	PC-W11	192.168.90.24	Machine cliente à intégrer au domaine

Domaine utilisé : **TECH.LAN**

### 1.6. Méthodologie

Chaque chapitre présente :

- Une **courte explication théorique** pour comprendre le concept,
- Des **étapes détaillées** pour la mise en œuvre,

## 2. INSTALLATION ET PROMOTION D'UN CONTRÔLEUR DE DOMAINE ACTIVE DIRECTORY

L'installation et la promotion d'un contrôleur de domaine constituent la première étape de la mise en place d'une infrastructure réseau centralisée sous Windows Server 2025.

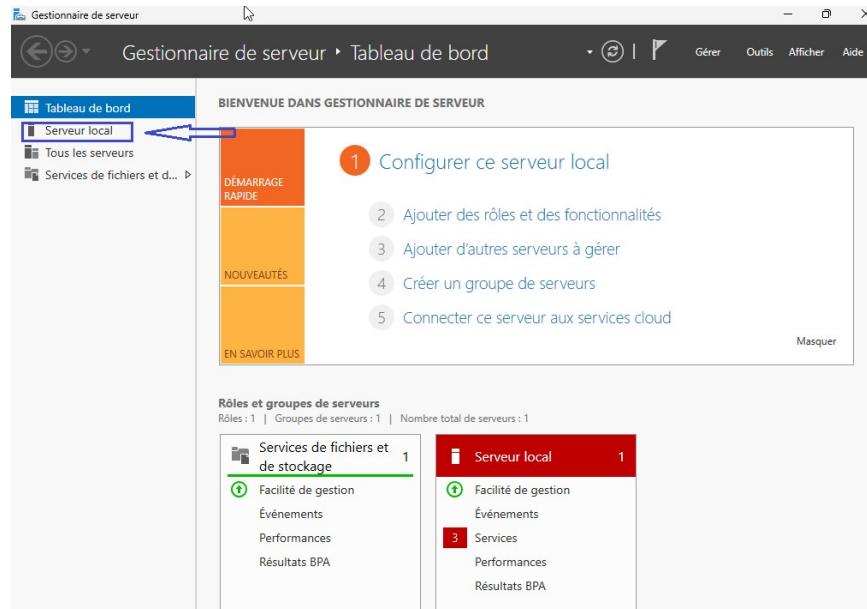
Le rôle Active Directory Domain Services (AD DS) permet d'administrer les utilisateurs, les ordinateurs et les ressources du réseau à partir d'un point unique.

### 2.1. Configuration de l'environnement réseau

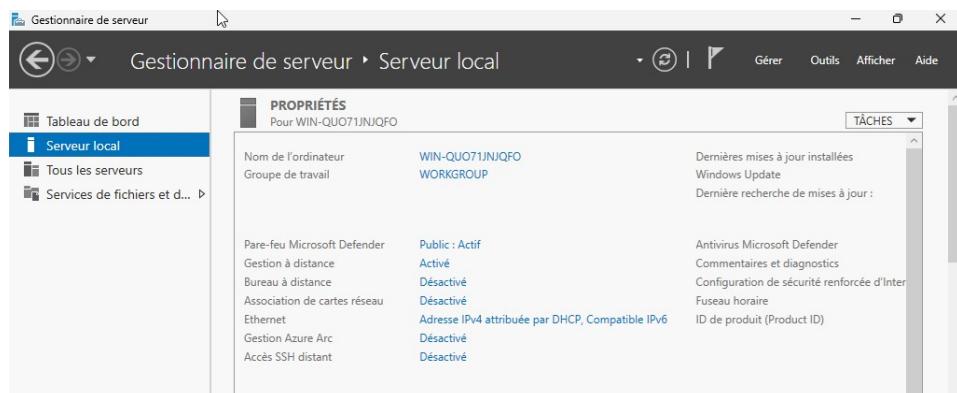
Avant d'installer Active Directory, il est important de préparer l'environnement virtuel.

- **Créer une machine virtuelle sous VirtualBox :**
  - Nom : Serveur AD ○ Système : Windows Server 2025 ○ Processeur : 2 cœurs minimum ○ RAM : 4 Go (8 Go recommandé) ○ Disque dur : 60 Go minimum
  
- **Configurer le réseau VirtualBox :**
  - Mode : Réseau interne (Internal Network) ou Réseau privé hôte selon ton besoin.
  - Cette configuration permettra la communication entre le serveur et le futur poste client Windows 11.

- Une fois cette première configuration et que l'installation proprement de votre serveur est faite, vous accédez au tableau de bord de votre gestionnaire de serveur.



- Ensuite, cliquer sur Serveur local



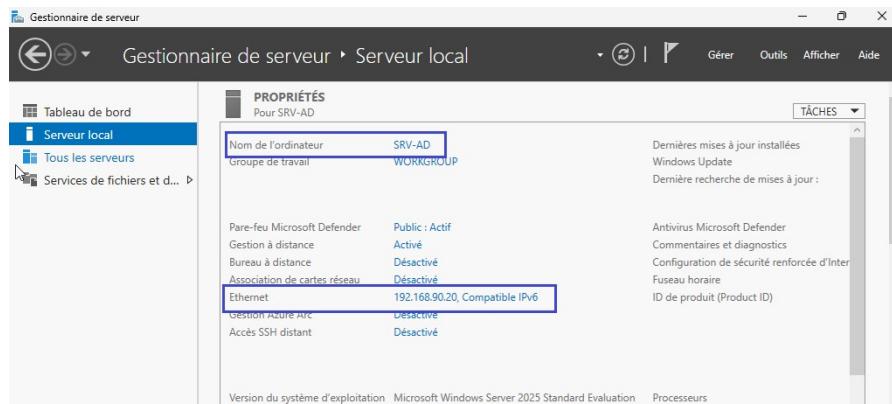
➤ Attribuer ensuite une adresse IP statique sur Windows Server :

- IP : 192.168.90.20 ○ Masque : 255.255.255.0 ○ Passerelle : 192.168.90.1 ○ DNS : 127.0.0.1

➤ Renommer le serveur :

- Nouveau nom : SRV-AD01 ○ Redémarrer après la modification.

Ainsi, après redémarrage du serveur on a :

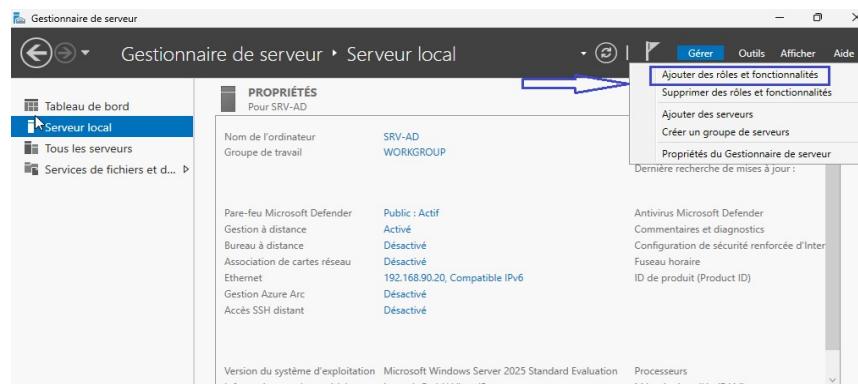


Notre serveur étant totalement prêt, on peut passer à l'installation du rôle Active Directory.

## 2.2. Installer le rôle Active Directory

L'installation du rôle AD DS ajoute au système les composants nécessaires pour transformer le serveur en contrôleur de domaine.

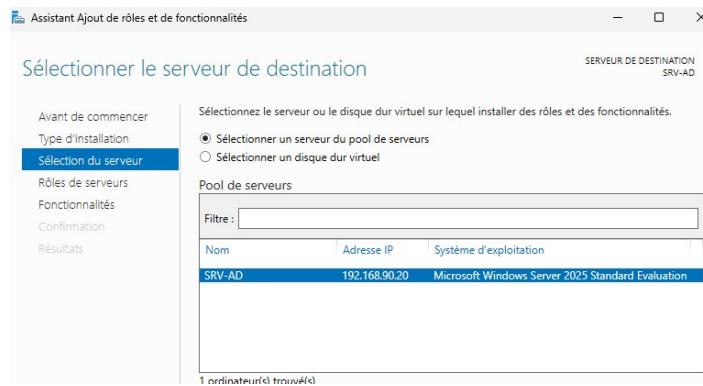
- Cliquer sur gérer puis sur ajouter rôle et fonctionnalités



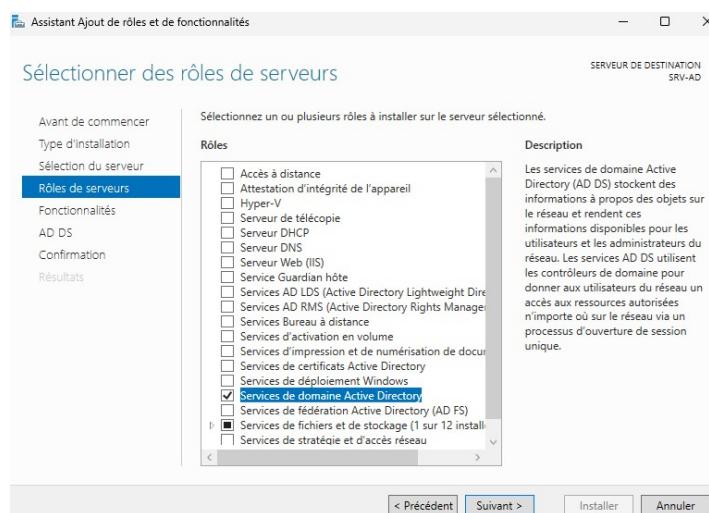
- Sélectionner installation basée sur un rôle ou une fonctionnalité



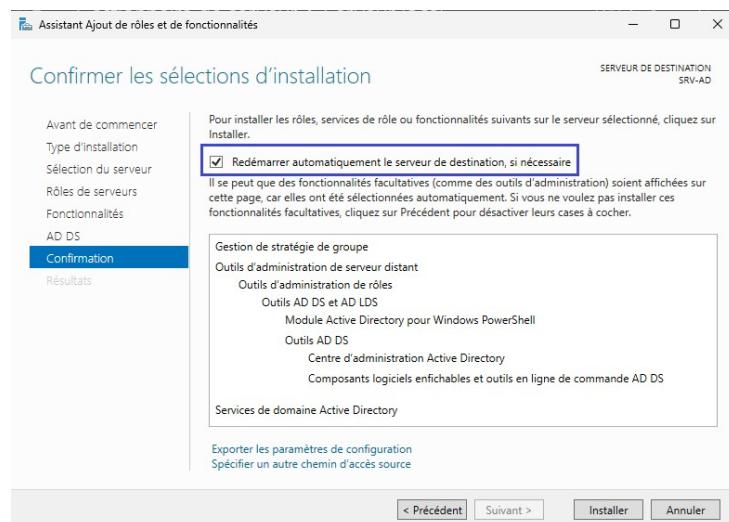
- Choisir le serveur sur lequel on veut installer un rôle ou fonctionnalité



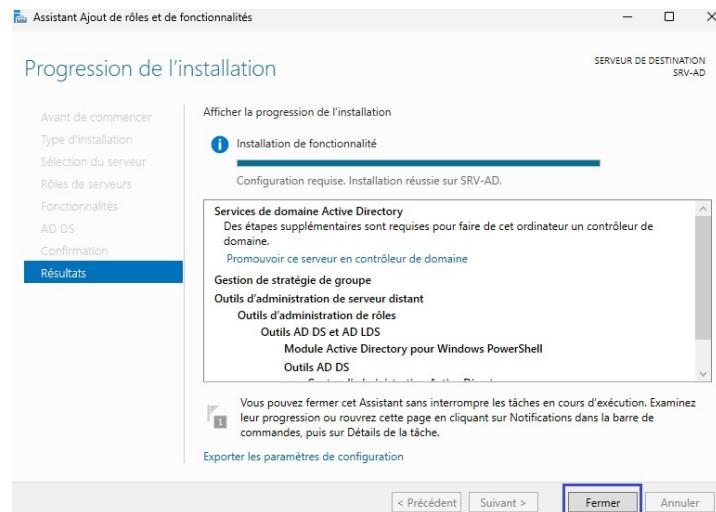
➤ Selectionner les services de domaine Active Directory



➤ Cocher la case redémarrer puis appuyer sur installer



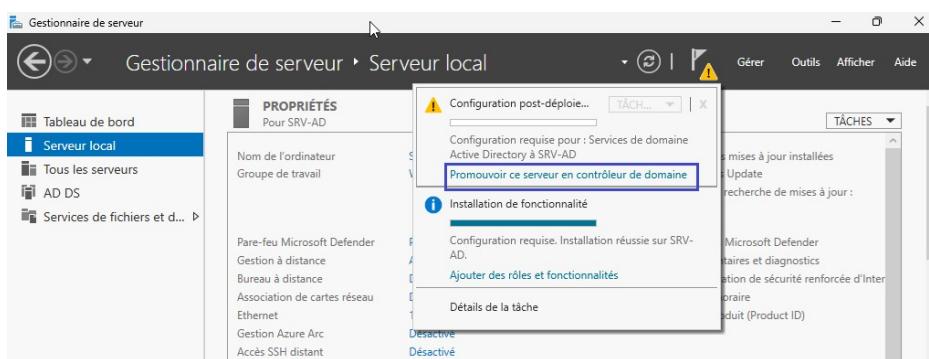
➤ Une fois l'installation terminer appuyer sur fermer



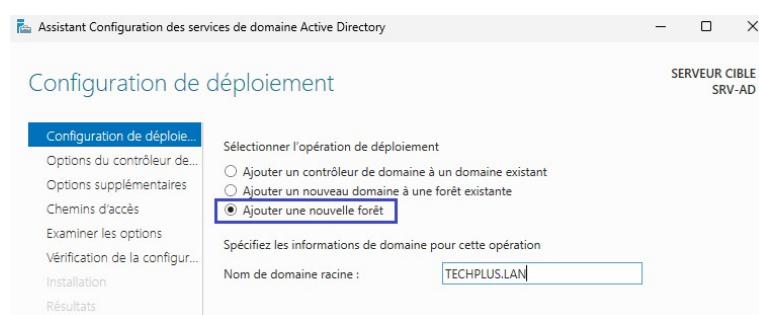
## 2.3. Promouvoir le serveur en contrôleur de domaine

Cette étape transforme le serveur en **contrôleur de domaine** et crée la **première forêt Active Directory**.

- Appuyer sur promouvoir ce serveur en contrôleur de domaine



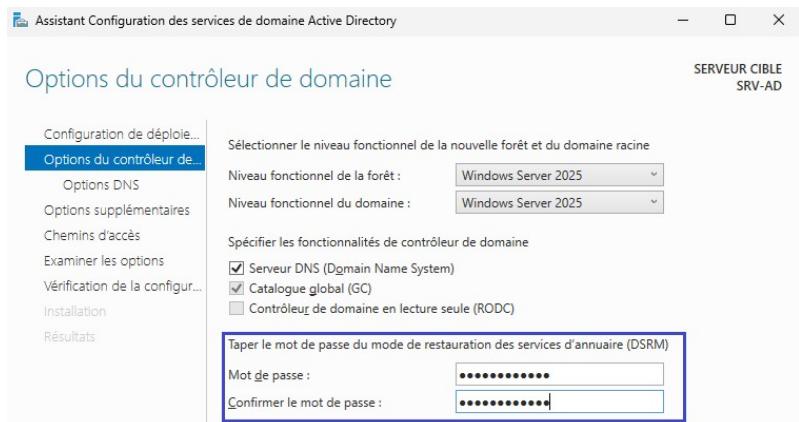
- Ajouter une nouvelle forêt



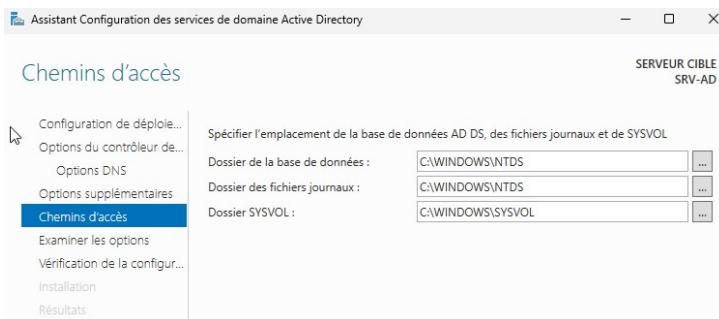
Ici, j'ai créé ma forêt qui est : TECHPLUS.LAN

- Ajouter le mot de passe de mode de restauration des services d'annuaire

Très important pour démonter le contrôleur de domaine

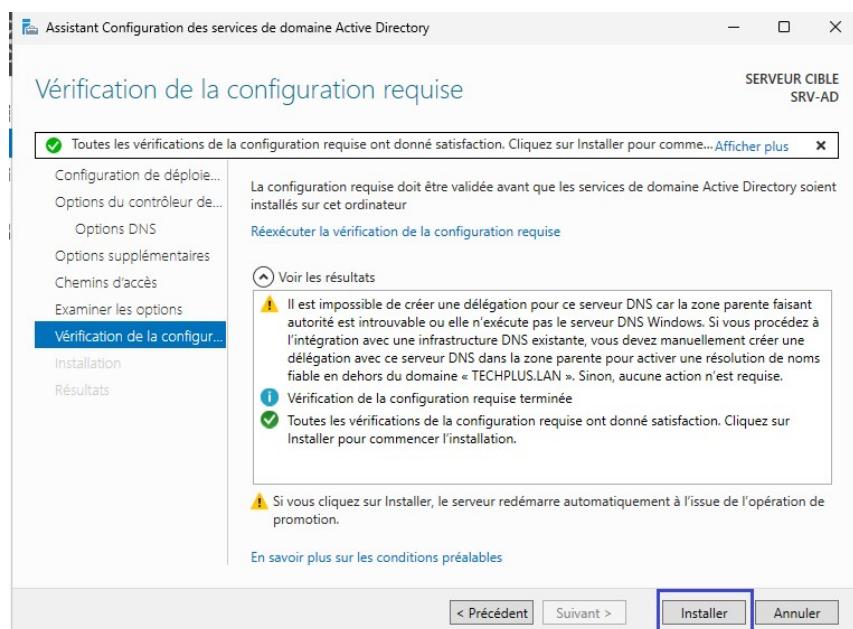


- Chemin de base de données AD DS, des fichiers journaux et dossier SYSVOL (ensembles des stratégies de groupes et des chemins d'accès).



- Vérification de la configuration requise.

Après que le système a vérifié que tout est Ok, appuyer sur installer.



### **3. GESTION DES UNITÉS D'ORGANISATION (OU)**

Les Unités d'**Organisation (OU)** sont des conteneurs logiques dans l'Active Directory. Elles permettent de structurer le domaine de manière hiérarchique et de **faciliter l'administration** des comptes, ordinateurs et groupes.

Grâce aux OU, il est possible d'appliquer des **stratégies de groupe (GPO)** ciblées sur des ensembles précis d'utilisateurs ou de machines.

#### **3.1. Comprendre le rôle des Unités d'Organisation**

Une **OU** sert à :

- Classer les objets de l'annuaire selon la structure réelle de l'entreprise (par service, site, ou fonction).
- Déléguer des droits d'administration à des responsables locaux.
- Appliquer des stratégies de sécurité différentes selon les services.

**Exemple** : Dans une société comme TechPlus., on peut créer les OU suivantes :

- Direction
- Comptabilité
- Ressources Humaines
- Informatique

Chaque OU contiendra ses propres utilisateurs, ordinateurs et politiques de sécurité.

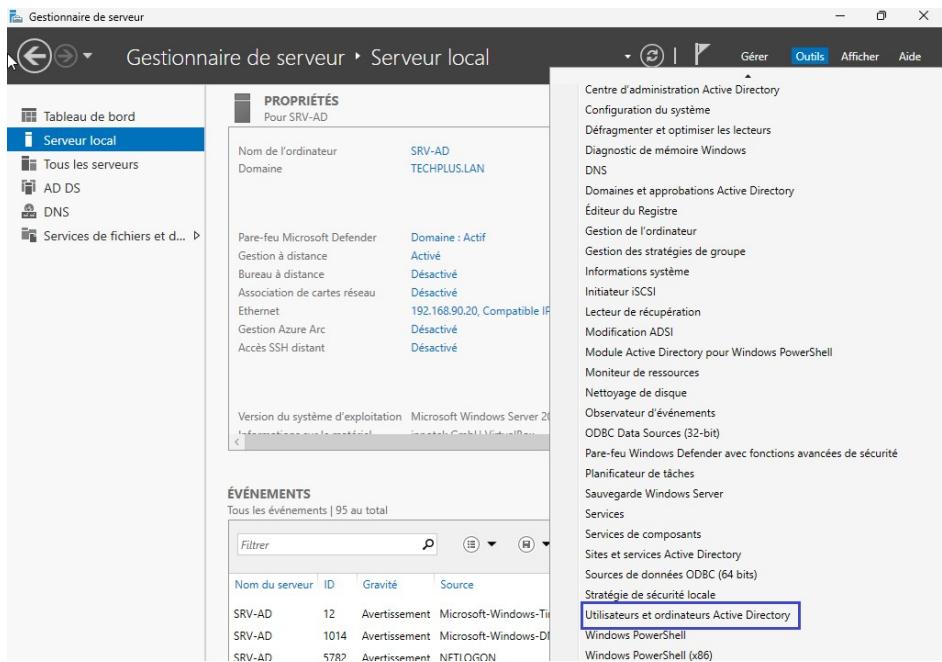
#### **3.2. Crédation d'une Unité d'Organisation (OU)**

La création des OU peut se faire de deux manières :

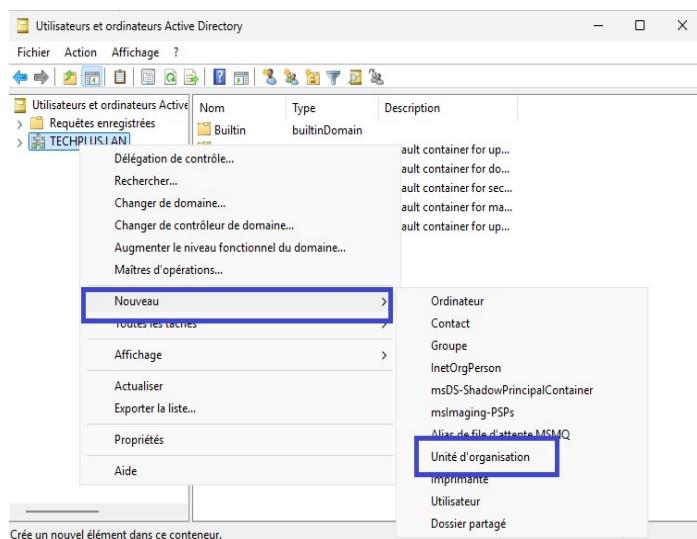
- **Graphiquement**, via la console Utilisateurs et Ordinateurs Active Directory
- **En PowerShell**, plus rapide et adaptée aux environnements professionnels

##### **❖ Méthode 1 : Crédation d'un OU via l'interface graphique (dsa.msc)**

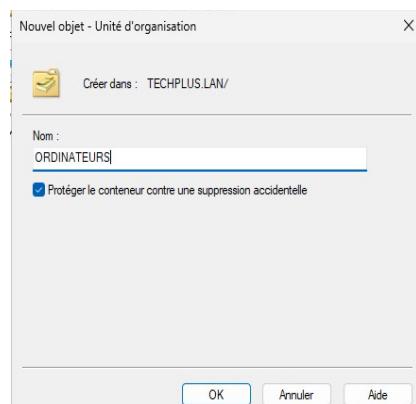
➤ Appuyer sur Outils puis sélectionner utilisateurs et ordinateurs Active Directory



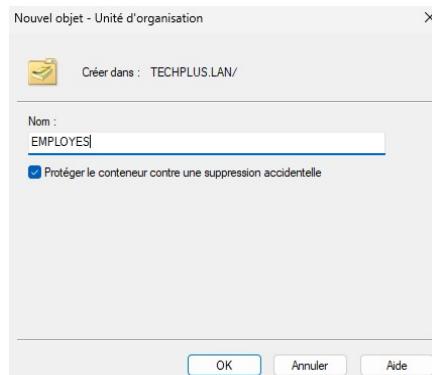
➤ Faire un clic droit sur le domaine, appuyer sur nouveau puis sélectionner unité d'organisation



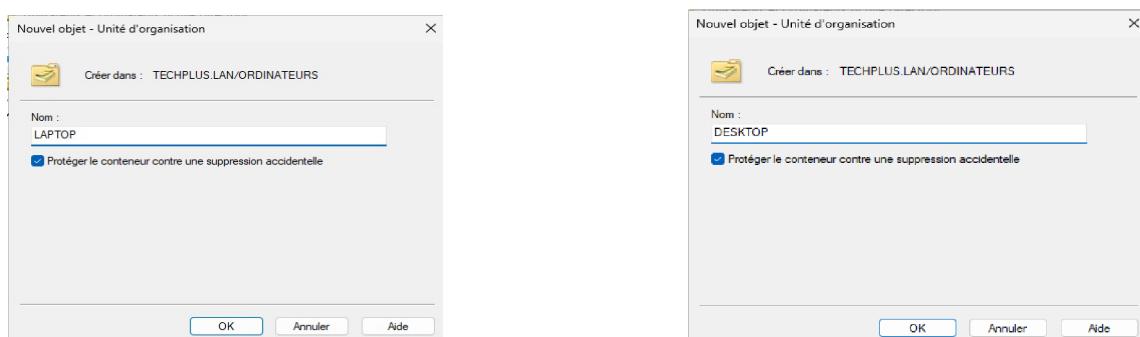
➤ Créer l'OU : ORDINATEURS



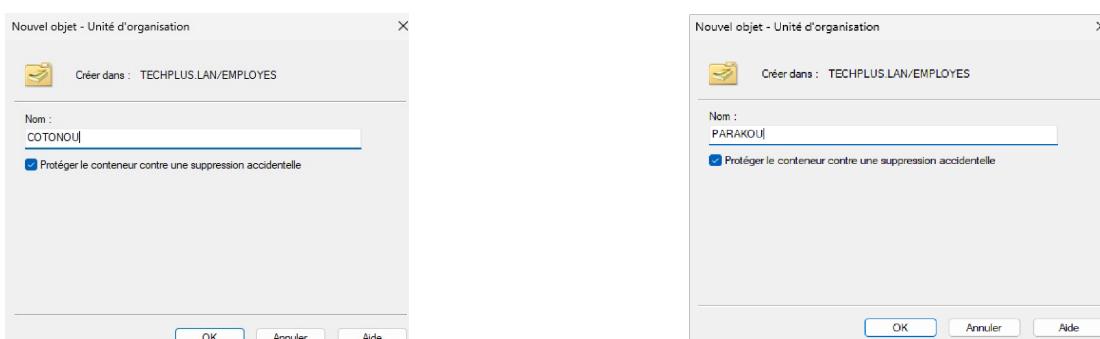
➤ Créer l'OU : EMPLOYES



➤ Crée des sous OU : DESKTOP & LAPTOP dans ORDINATEURS



➤ Crée des sous OU : COTONOU & PARAKOU dans EMPLOYES



❖ Méthode 2 : Création d'une OU via PowerShell (recommandé)

PowerShell est la méthode la plus efficace, particulièrement utile en entreprise ou pour automatiser la structure du domaine.

- Ouvrez PowerShell en tant qu'administrateur.
- Exécutez la commande suivante pour créer une OU :

```
Administrator: Windows PowerShell + 
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name:"DIRECTION" -Path:"DC=TECHPLUS, DC=LAN" -ProtectedFromAccidentalDeletion:$true -Server:"SRV-AD.TECHPLUS.LAN"
PS C:\Users\Administrateur>
```

- `-Name "Direction"` → Nom de l'OU
- `-Path "DC=sonama,DC=local"` → Emplacement dans l'arborescence du domaine
- `-ProtectedFromAccidentalDeletion:$true` → Empêche la suppression accidentelle

(bonne pratique AD) ○ `Server:"SRV-AD.TECHPLUS.LAN"` → Force la commande à s'exécuter sur un contrôleur de domaine spécifique

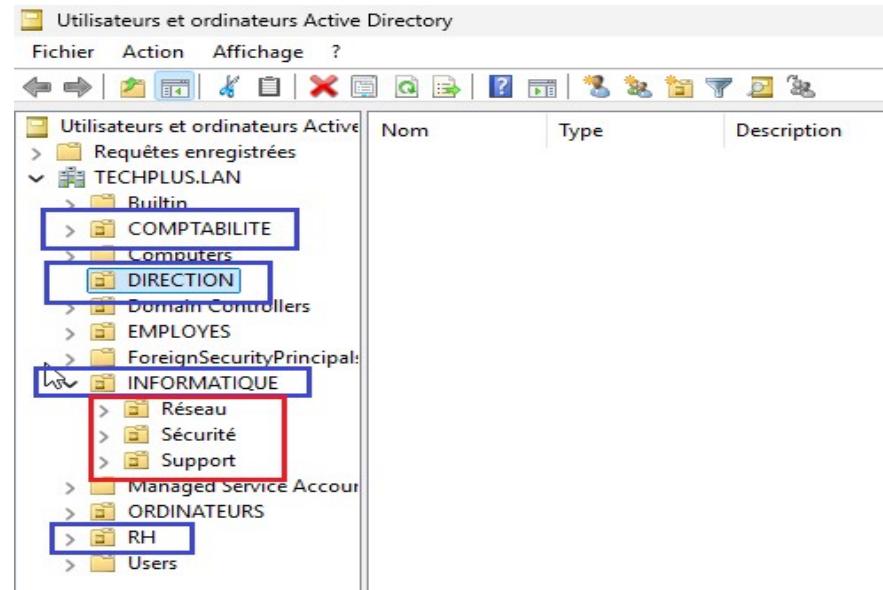
C'est exactement ce que recommandent les administrateurs professionnels.

- Pour créer plusieurs OU successivement :

```
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name:"COMPTABILITE" -Path:"DC=TECHPLUS, DC=LAN" -Protect
edFromAccidentalDeletion:$true -Server:"SRV-AD.TECHPLUS.LAN"
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name:"INFORMATIQUE" -Path:"DC=TECHPLUS, DC=LAN" -Protect
edFromAccidentalDeletion:$true -Server:"SRV-AD.TECHPLUS.LAN"
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name:"RH" -Path:"DC=TECHPLUS, DC=LAN" -ProtectedFromAcci
dentalDeletion:$true -Server:"SRV-AD.TECHPLUS.LAN"
PS C:\Users\Administrateur>
```

- Pour créer des sous-OU :

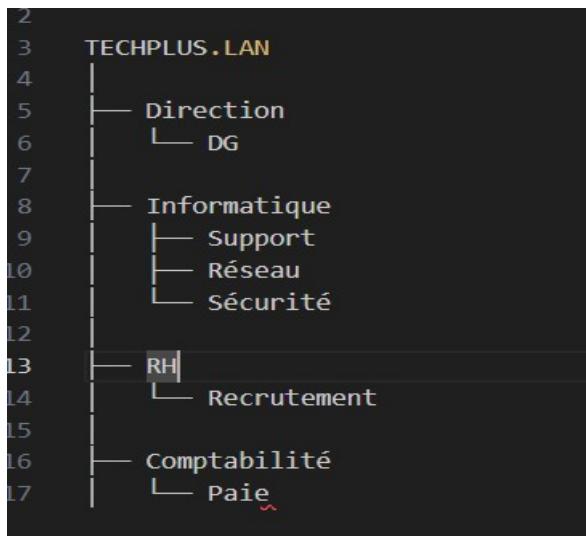
```
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name "Support" -Path:"OU=INFORMATIQUE,DC=TECHPLUS, DC=LA
N" -ProtectedFromAccidentalDeletion:$true -Server:"SRV-AD.TECHPLUS.LAN"
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name "Sécurité" -Path:"OU=INFORMATIQUE,DC=TECHPLUS, DC=L
AN" -ProtectedFromAccidentalDeletion:$true -Server:"SRV-AD.TECHPLUS.LAN"
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name "Réseau" -Path:"OU=INFORMATIQUE,DC=TECHPLUS, DC=LAN
" -ProtectedFromAccidentalDeletion:$true -Server:"SRV-AD.TECHPLUS.LAN"
PS C:\Users\Administrateur> |
```



Méthode professionnelle, rapide et idéale pour déployer un domaine complet

### 3.3. Organisation hiérarchique recommandée

Voici un exemple d'arborescence logique adaptée à une PME :



Cette structure permet une gestion claire, avec possibilité d'appliquer des GPO différentes sur chaque service.

## 4. CRÉATION D'UTILISATEURS ET INTÉGRATION D'UN POSTE WINDOWS 11

La gestion des utilisateurs est l'élément central d'un Active Directory.

Un utilisateur représente une identité (personne ou service) capable de se connecter au domaine pour accéder aux ressources du réseau. Une fois les utilisateurs créés, il est essentiel d'intégrer les postes Windows 11 dans le domaine afin que les comptes puissent s'y connecter et appliquer les stratégies de sécurité (GPO).

### 4.1. Création d'un utilisateur

Avant toute opération de création de compte, il est essentiel de respecter les règles internes de gestion des identités. Celles-ci garantissent la sécurité, la traçabilité et la cohérence de l'annuaire Active Directory.

#### Règles préalables obligatoires :

- Aucune création de compte ne doit être effectuée sans une demande formelle provenant de la hiérarchie ou du responsable concerné.
  - Cela permet d'éviter les comptes non autorisés et d'assurer une validation claire avant l'attribution des accès.
- Chaque création d'utilisateur doit être soigneusement documentée dans un fichier Excel dédié, incluant les informations essentielles (identité, OU, date, demandeur, etc.).
  - Cette méthode assure un suivi précis et facilite les audits internes.

	A	B	C	D	E	F	G
1	GROUPE/USER	Karl Zola	Jacques Figo	Deen Quen	Eunice Wash	Jules Debge	Cyntia Ballo
2	Direction					X	
3	Comptabilité		X				
4	RH				X		
5	Informatique	X		X			X
6							
7							
8							
9							

Utilisateur AD



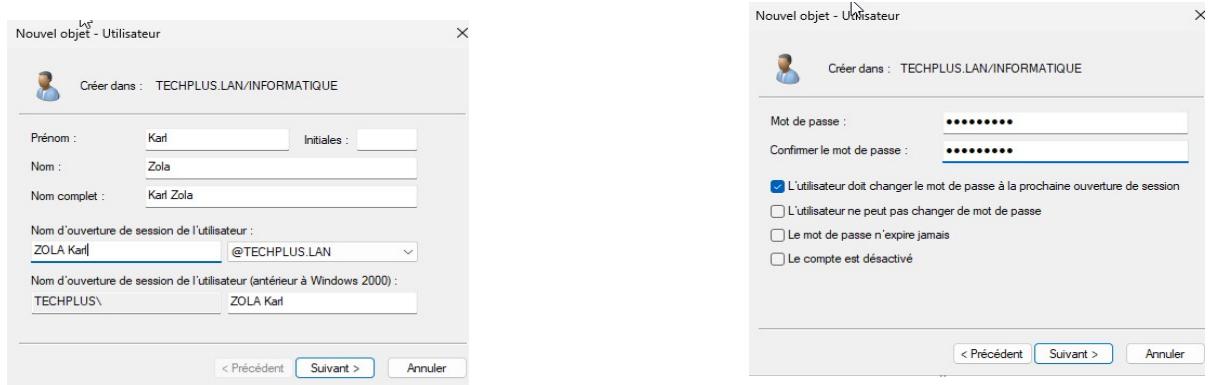
- Appuyer sur Outils puis sélectionner utilisateurs et ordinateurs Active Directory.

The screenshot shows the Windows Server Management Console. The left pane displays a navigation tree with 'Tableau de bord', 'Serveur local' (selected), and various services like AD DS, DNS, and File Services. The right pane shows the 'PROPRIÉTÉS Pour SRV-AD' for the local computer, including system configuration and event logs. A context menu is open over the 'Outils' tab, listing various administrative tools. The 'Utilisateurs et ordinateurs Active Directory' option is highlighted with a blue box and a yellow arrow pointing to it.

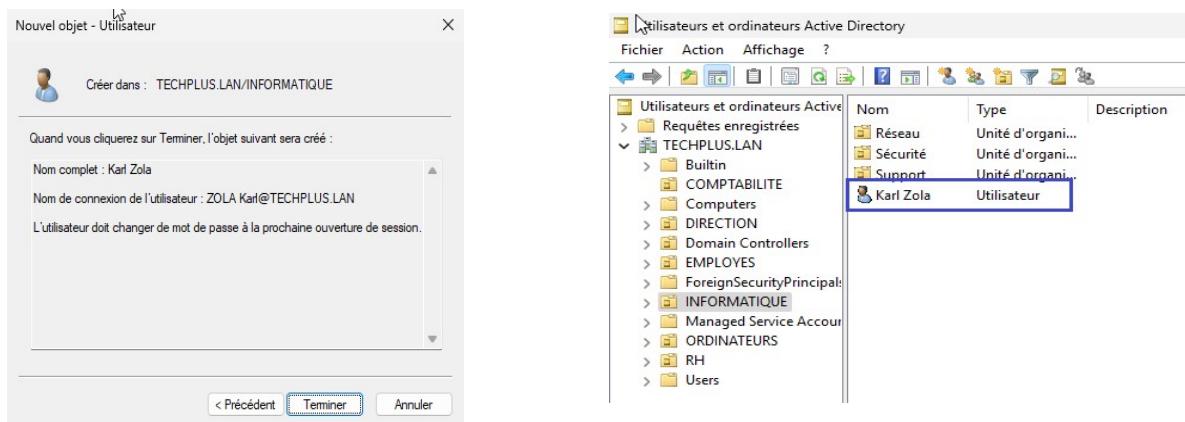
- Sélectionner l'unité d'organisation INFORMATIQUE et puis l'icône utilisateur

The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' snap-in. The left pane shows the organizational structure of the domain 'TECHPLUS.LAN', with several OUs listed: 'Requêtes enregistrées', 'TECHPLUS.LAN', 'Builtin', 'COMPTABILITE', 'Computers', 'DIRECTION', 'Domain Controllers', 'EMPLOYES', 'ForeignSecurityPrincipal', and 'INFORMATIQUE'. The 'INFORMATIQUE' OU is selected and highlighted with a blue box. The right pane shows a list of users categorized by their type: 'Réseau', 'Sécurité', and 'Support'. Each user entry includes a small user icon and a description indicating they are part of the 'Unité d'organisation...'.

- Ensuite ajouter le prénom, nom et identifiant. Ajouter aussi un mot de passe et exiger son changement à la première connexion.

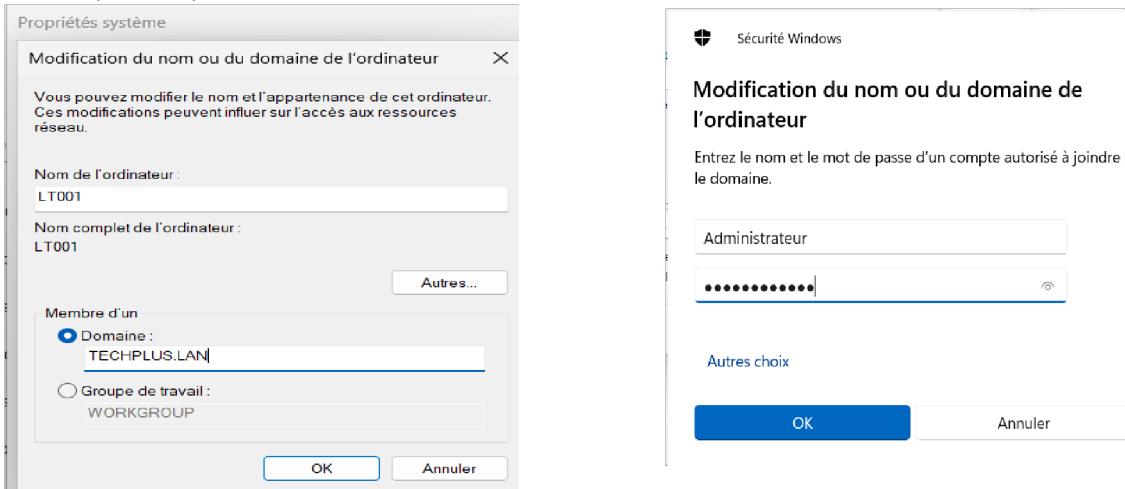


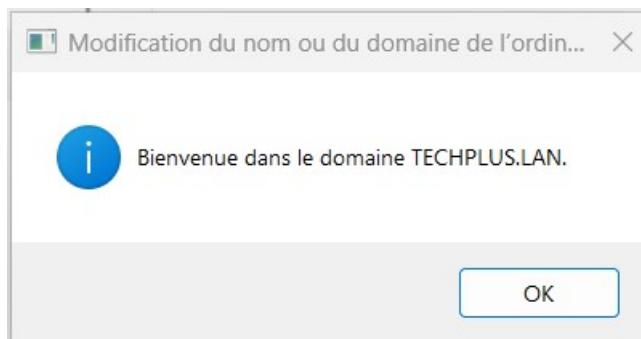
- Enfin passer à la validation de la création de l'utilisateur en cliquant sur terminer.



## 4.2. Ajout d'une machine Windows 11 au domaine

- Procéder au changement du nom de la machine et ajouter le nom de domaine sur la machine client (Win 11).

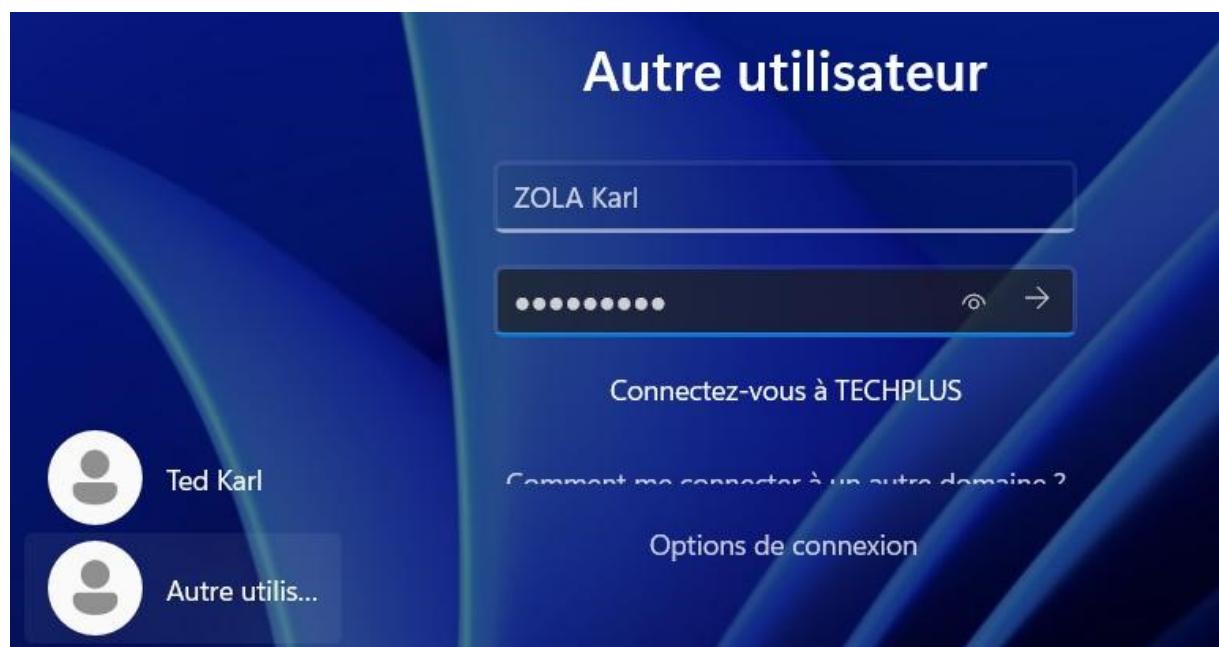




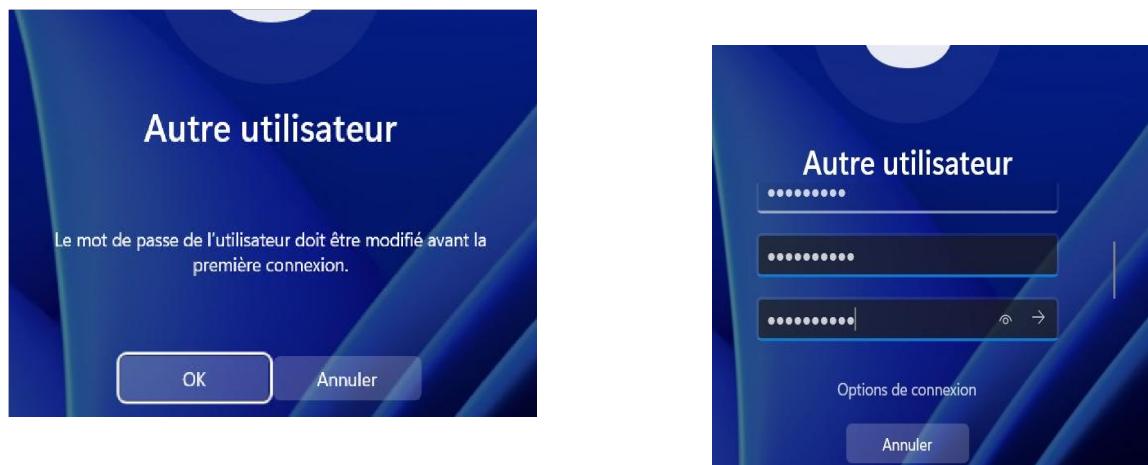
- Ensuite passer à la vérification de la machine dans l'AD

Norm	Type	Description
LT001	Ordinateur	

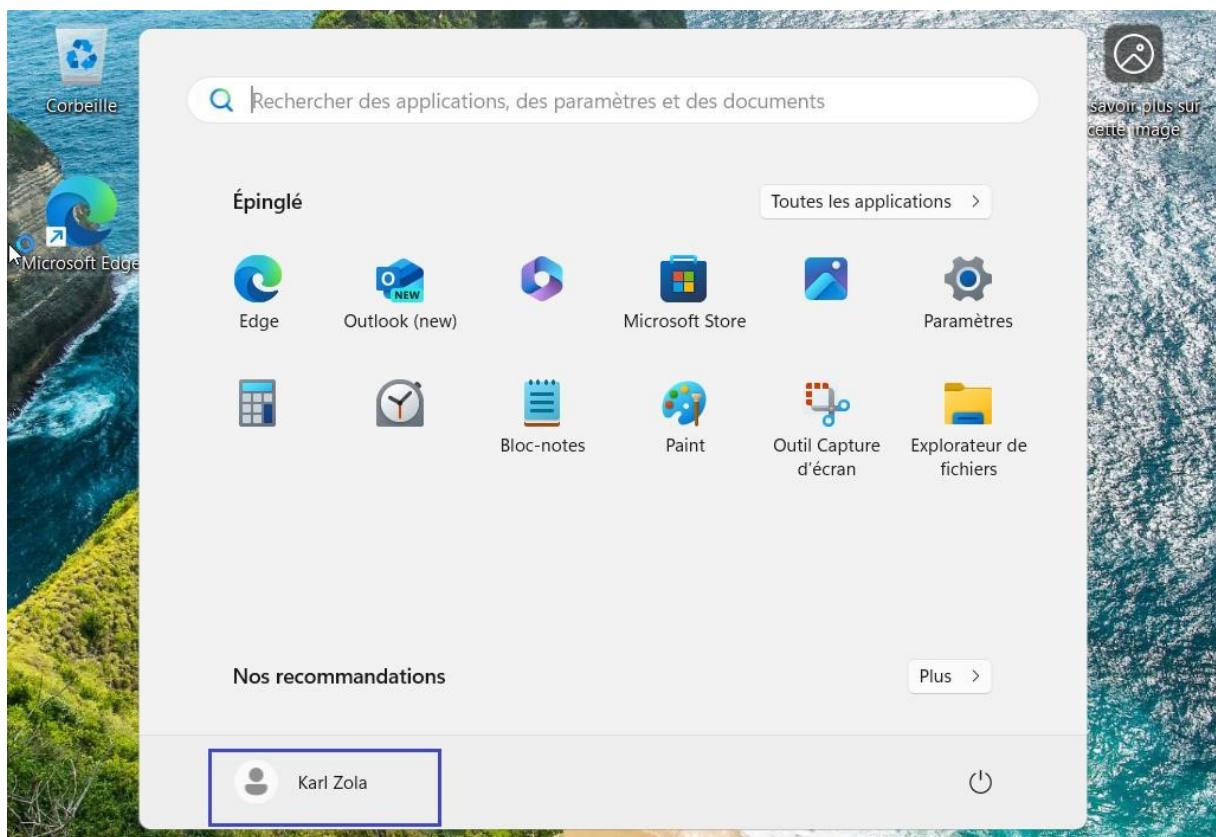
- Connecter vous au domaine avec l'utilisateur Karl ZOLA sur le poste client Windows 11.



- Passer à la modification obligatoire du mot de passe exiger à la première connexion.



- Enfin, accéder à l'interface Utilisateur.



## 5. MISE EN ŒUVRE DES STRATÉGIES DE GROUPE (GPO)

Les groupes Active Directory permettent de gérer plus facilement les droits, les accès et les permissions. Ils évitent d'attribuer des priviléges individuellement à chaque utilisateur, ce qui améliore la sécurité et simplifie l'administration.

### 5.1. Type de groupes et bonnes pratiques

Avant de créer un groupe, il est important de bien choisir son type :

- **Groupe de sécurité** : pour gérer les accès (partages, GPO, ressources).
- **Groupe de distribution** : utilisé pour les listes de diffusion (messagerie).

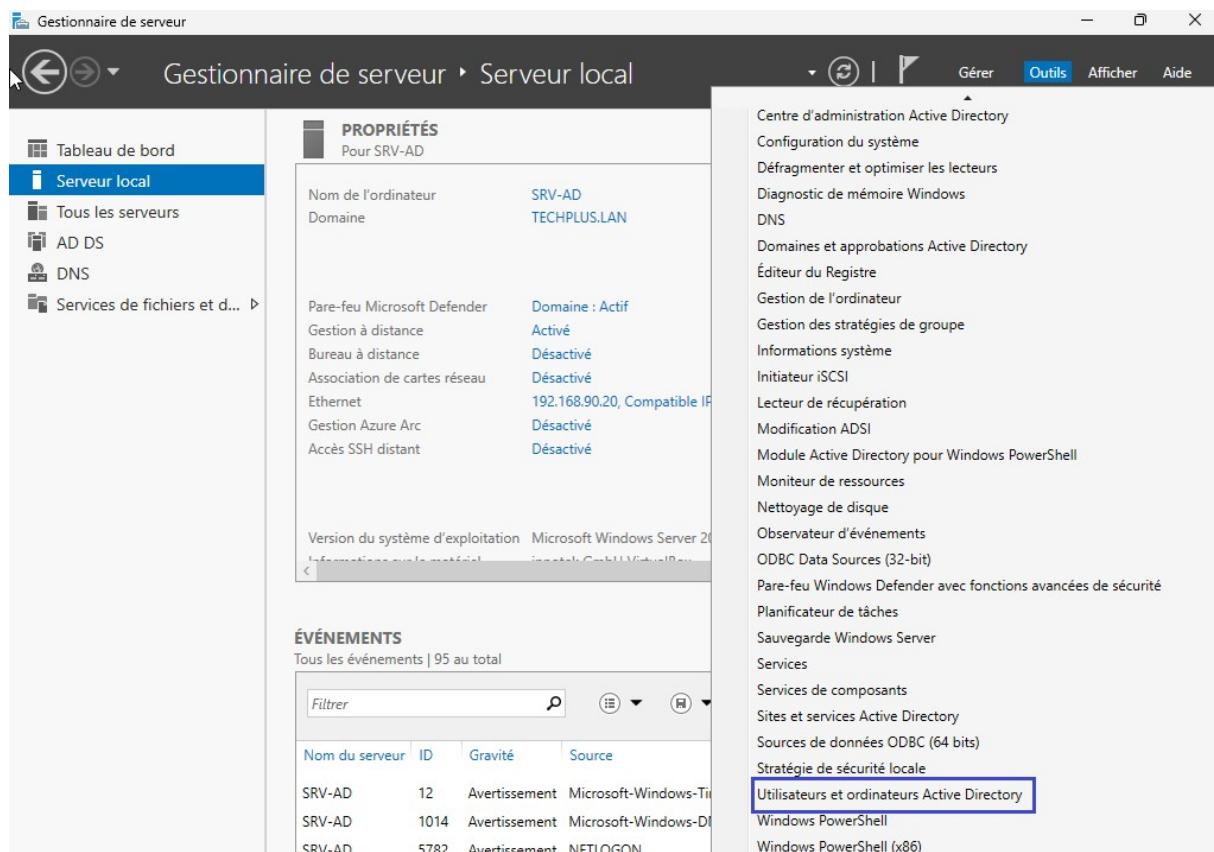
Dans le cadre de l'administration AD, **on utilise principalement des groupes de sécurité**.

**Bonnes pratiques :**

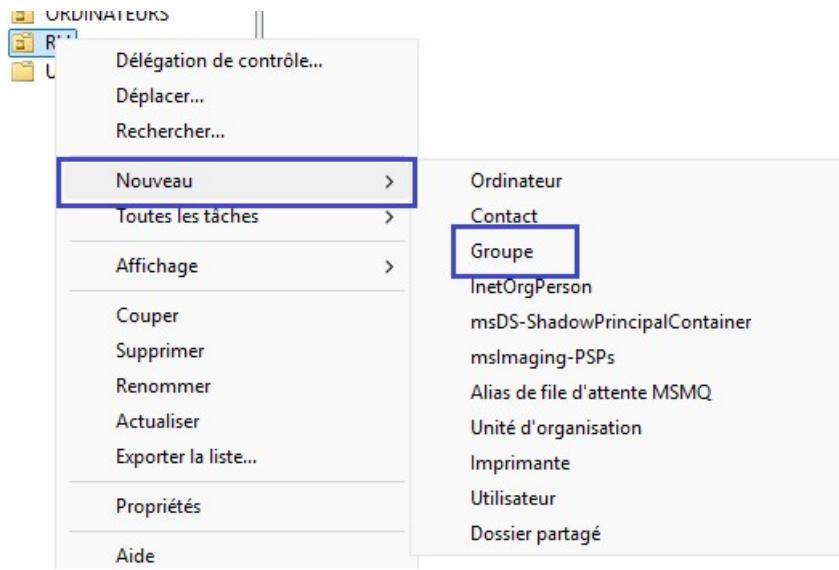
- Utiliser un nom explicite (ex. : G\_Informaticiens, G\_Compta\_Paie).
- Les groupes doivent être créés dans l'OU correspondant au service.
- Ne jamais ajouter des utilisateurs directement dans des GPO : toujours passer par un groupe.
- Documenter chaque création dans le fichier Excel de suivi (comme pour les utilisateurs).

### 5.2. Création d'un groupe

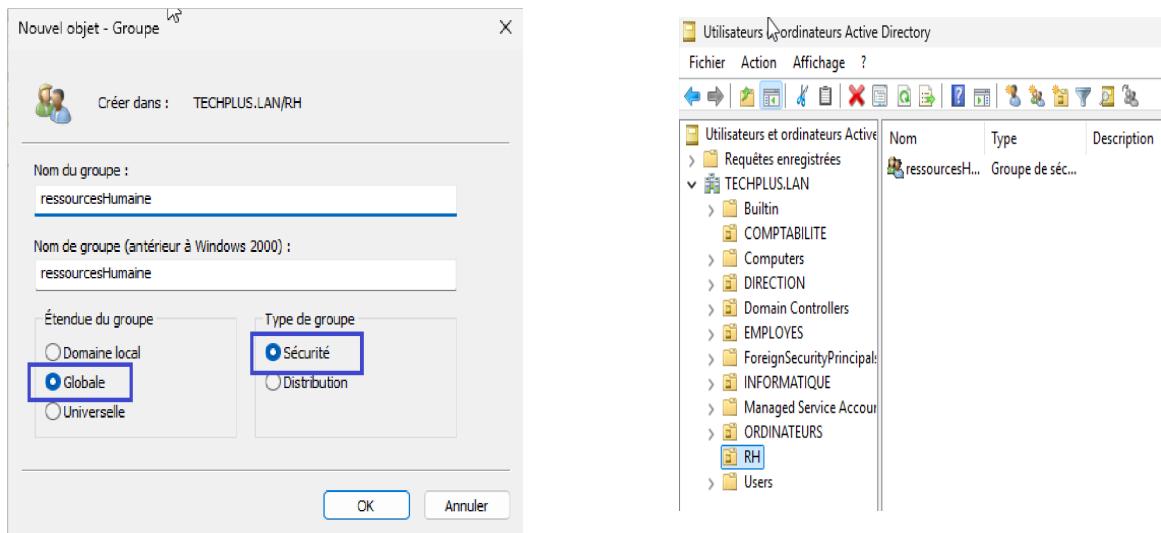
- Appuyer sur Outils puis sélectionner utilisateurs et ordinateurs Active Directory.



- Faire un click droit sur l'OU RH et appuyer sur nouveau groupe



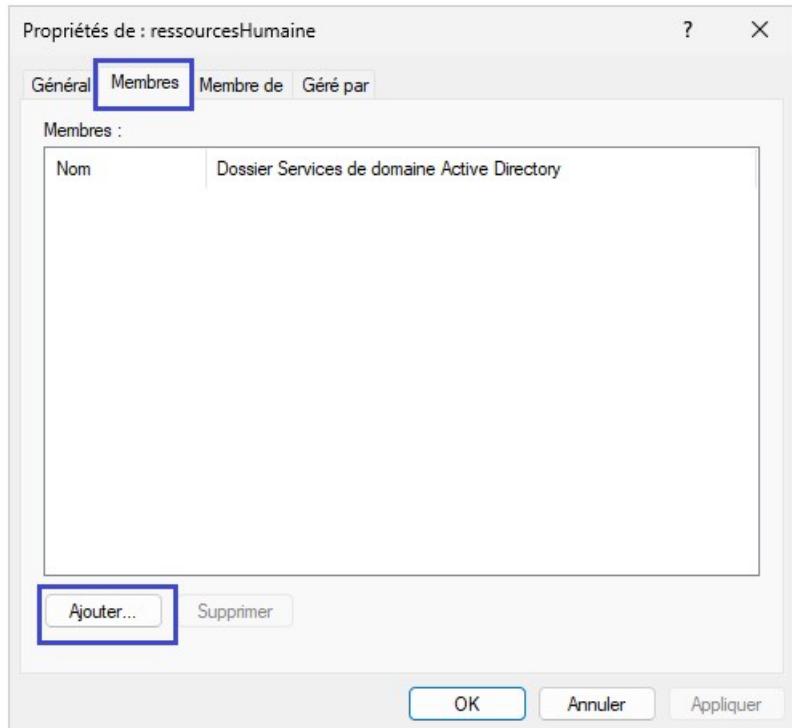
- Créer ensuite le groupe ressourcesHumaine dans TECHPLUS.LAN/RH



### 5.3. Ajouter un utilisateur dans le groupe

#### Méthode 1 : ajout depuis le groupe

- Ouvrir le groupe créer et appuyer sur membre et sur ajouter.

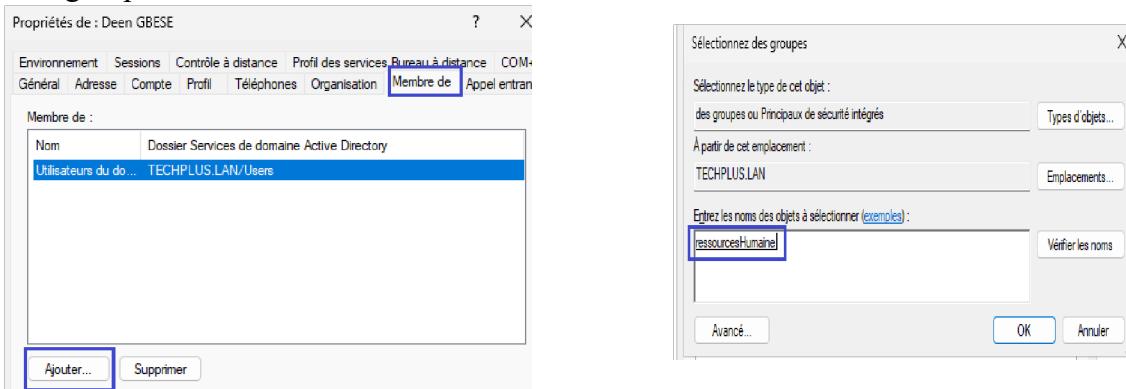


➤ Ensuite, rechercher l'utilisateur à ajouter au groupe et valider.

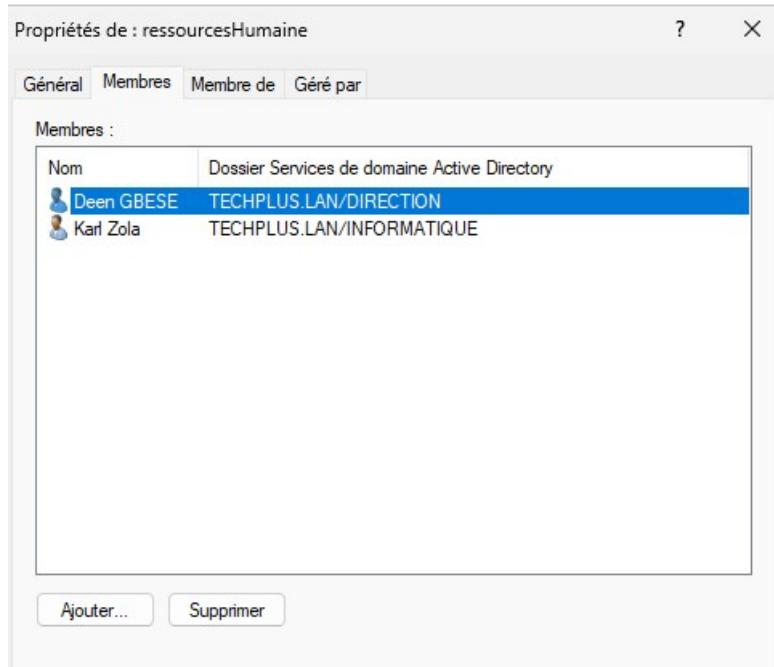
## Méthode 2 : depuis l'utilisateur

➤ Utiliser un utilisateur existant comme Deen GBESE qui se trouve dans l'Ou DIRECTION

- Ensuite faites un double clic, puis allez dans membre de et cliquer sur ajouter. Puis rechercher le groupe et valider



- Enfin, procéder à la vérification.



## 6. CRÉATION ET GESTION DES STRATÉGIES DE GROUPES (GPO)

Les GPO (Group Policy Objects) permettent de contrôler la configuration des utilisateurs et ordinateurs du domaine : restrictions, paramètres système, sécurité, interface, fond d'écran, scripts, etc.

Elles sont l'un des outils les plus puissants d'Active Directory.

## 6.1. Qu'est-ce qu'une GPO ?

Une GPO (Group Policy Object) est un ensemble de paramètres permettant de contrôler et de configurer automatiquement les postes et utilisateurs d'un domaine Active Directory. Elle sert notamment à :

- appliquer des règles de sécurité,
- configurer l'environnement Windows,
- déployer des restrictions,
- imposer des paramètres système (fond d'écran, mot de passe, scripts, etc.).

Les GPO s'appliquent soit à un domaine, soit à une OU, et se répliquent automatiquement sur tous les contrôleurs de domaine.

## 6.2. Comment créer une GPO et la lier au domaine ?

Pour créer un GPO nous avons la possibilité de le créer à plusieurs niveaux soit à partir du domaine ou on applique la stratégie sur une OU (Unité d'organisation).

OU = Organisation et gestion administrative + application de GPO.

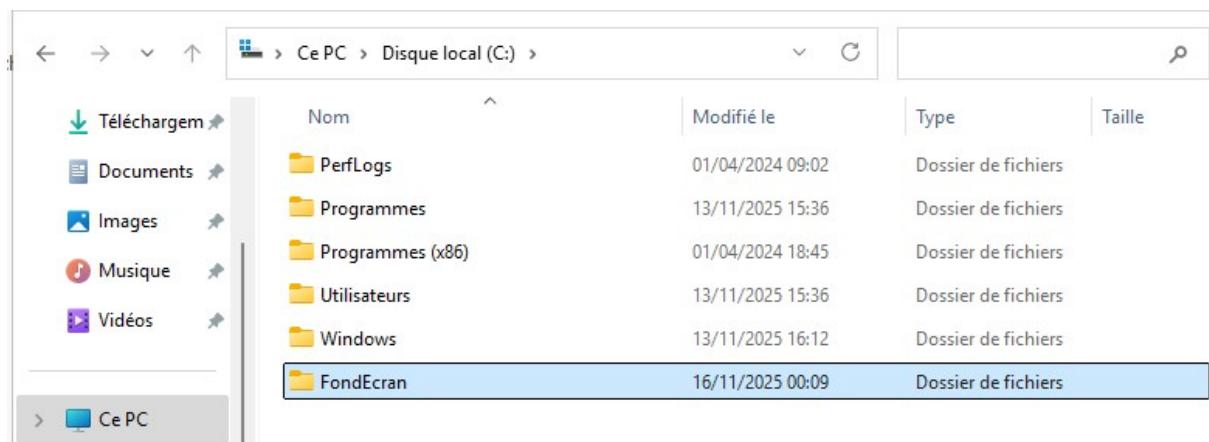
Groupe = Attribution de droits et autorisations (sécurité, accès, mails).

On peut mettre un utilisateur dans une OU et dans plusieurs groupes à la fois.

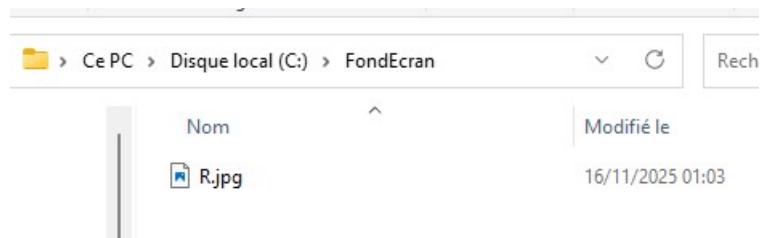
Une GPO ne s'applique pas à un groupe directement, mais à une Unité d'organisation.

## 6.3. Comment forcer le fond d'écran sur tous les postes des utilisateurs ?

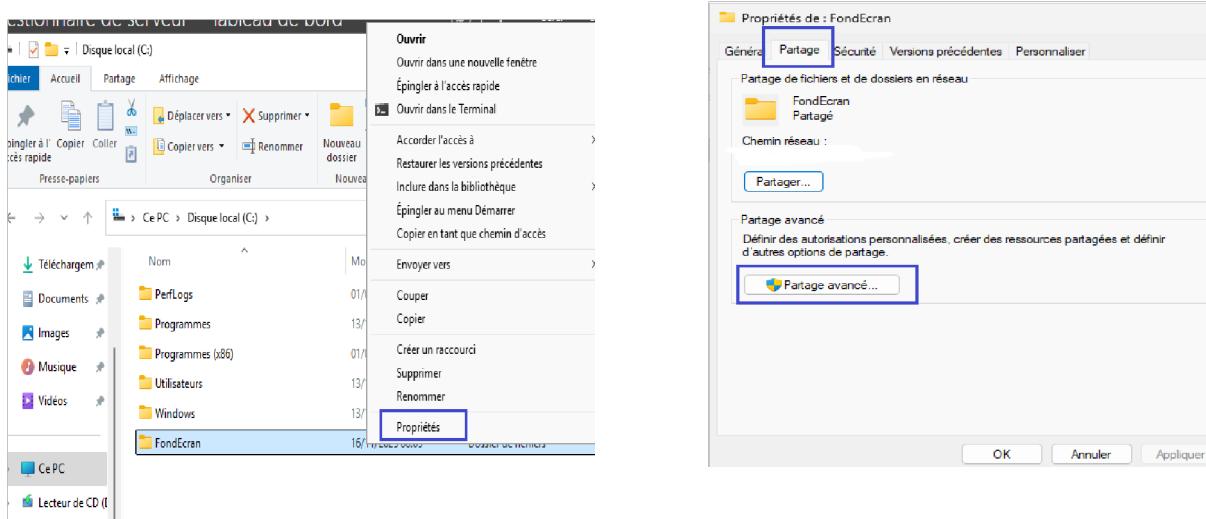
- Aller dans gestionnaire de fichier et cliquer sur le lecteur C puis créer le dossier FondEcran.



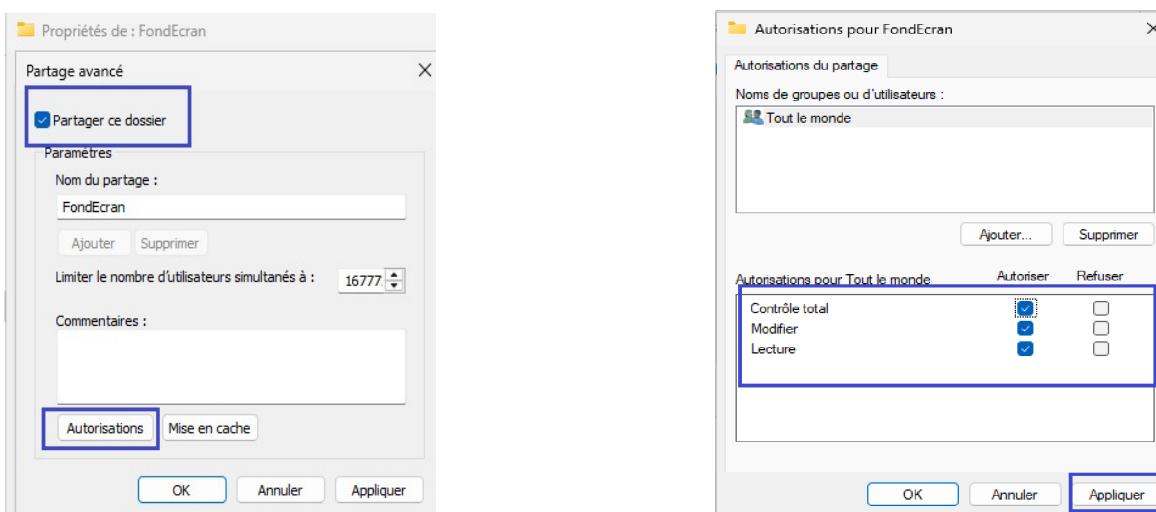
- Ajouter ensuite l'image dans le dossier FondEcran.



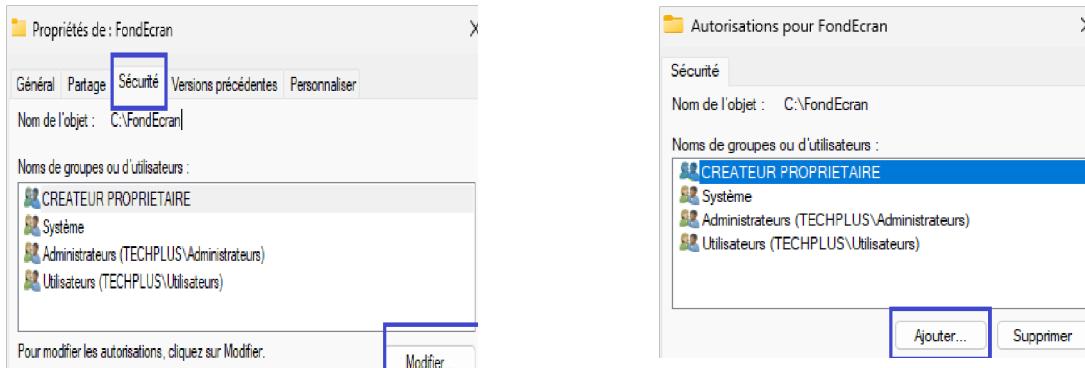
- Faire un clic droit sur FondEcran et appuyer sur propriétés. Appuyer ensuite sur partage et sélectionner partage avancée



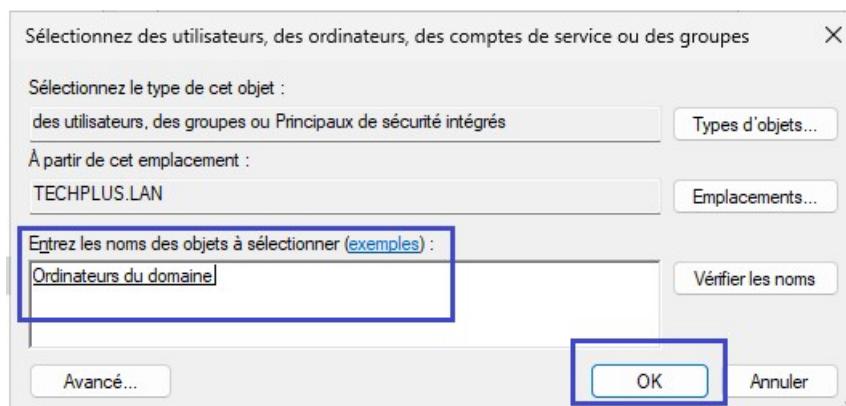
- Sélectionner partager ce dossier et cliquer sur autorisations. Par la suite, sélectionner contrôle total puis cliquer sur appliquer pour valider les modifications.



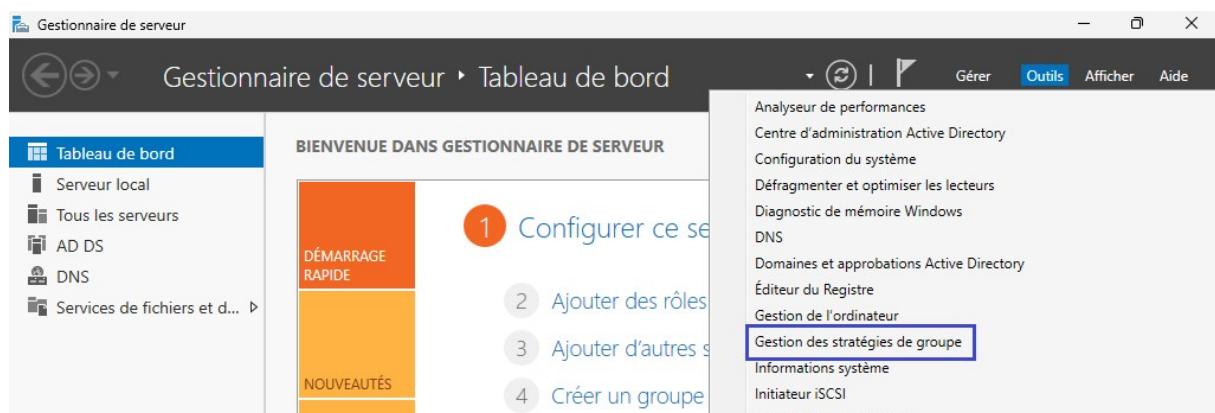
- Sélectionner sécurité puis modifier. Ensuite cliquer sur ajouter.



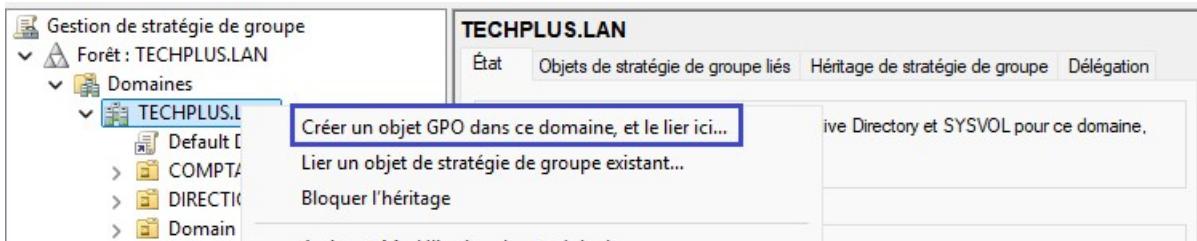
- Rechercher ordinateurs du domaine puis valider



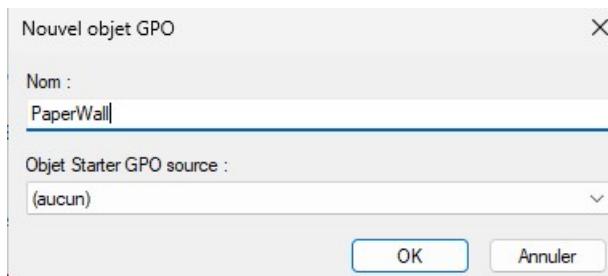
- Sélectionner le domaine sur lequel on veut appliquer les stratégies de groupes. Ici c'est TECHPLUS.LAN



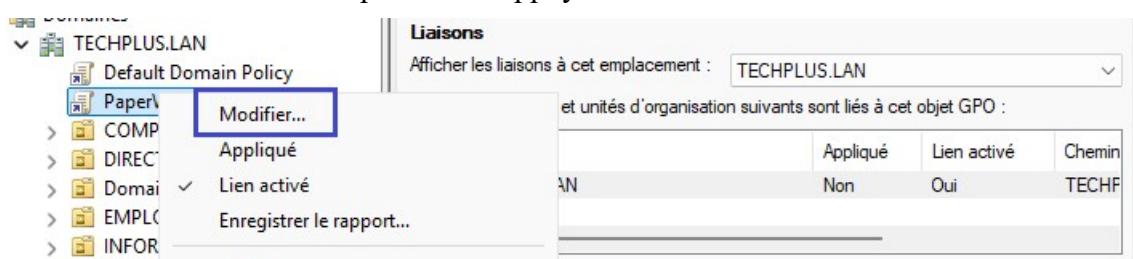
- Faire un clic droit sur TECHPLUS.LAN puis appuyer sur créer.



➤ Créer l'objet GPO PaperWall



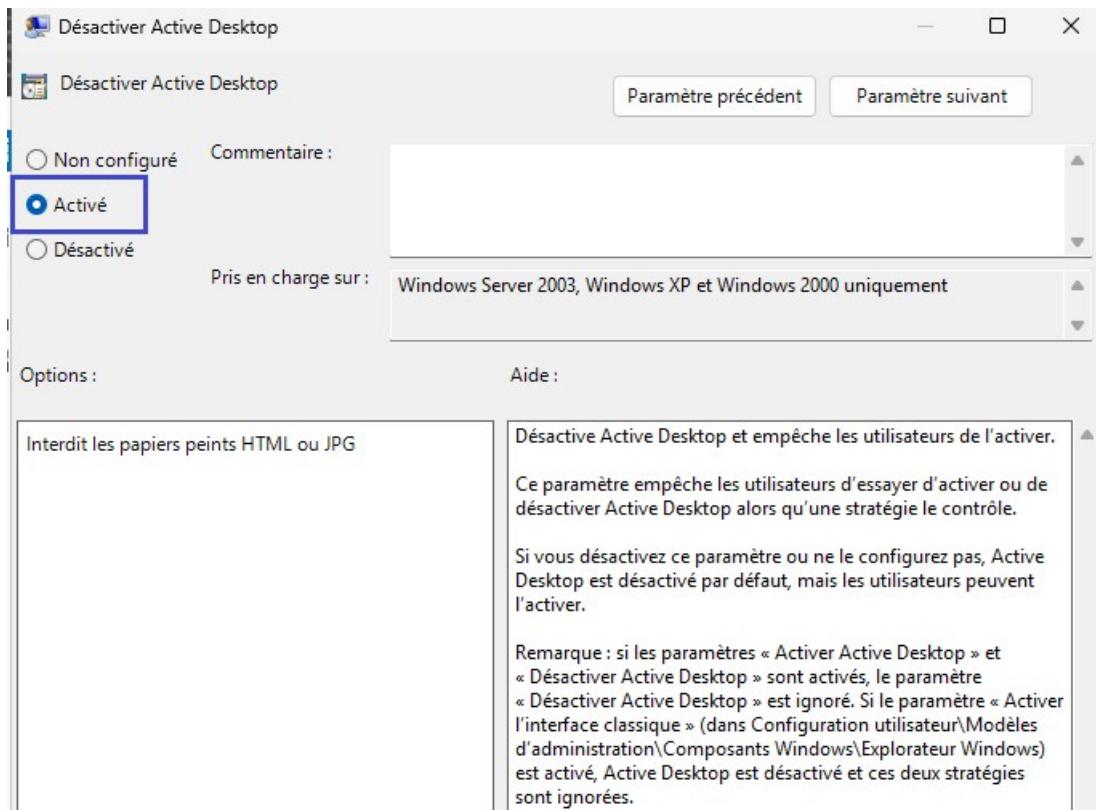
➤ Faire un clic droit sur PaperWall et appuyer sur modifier



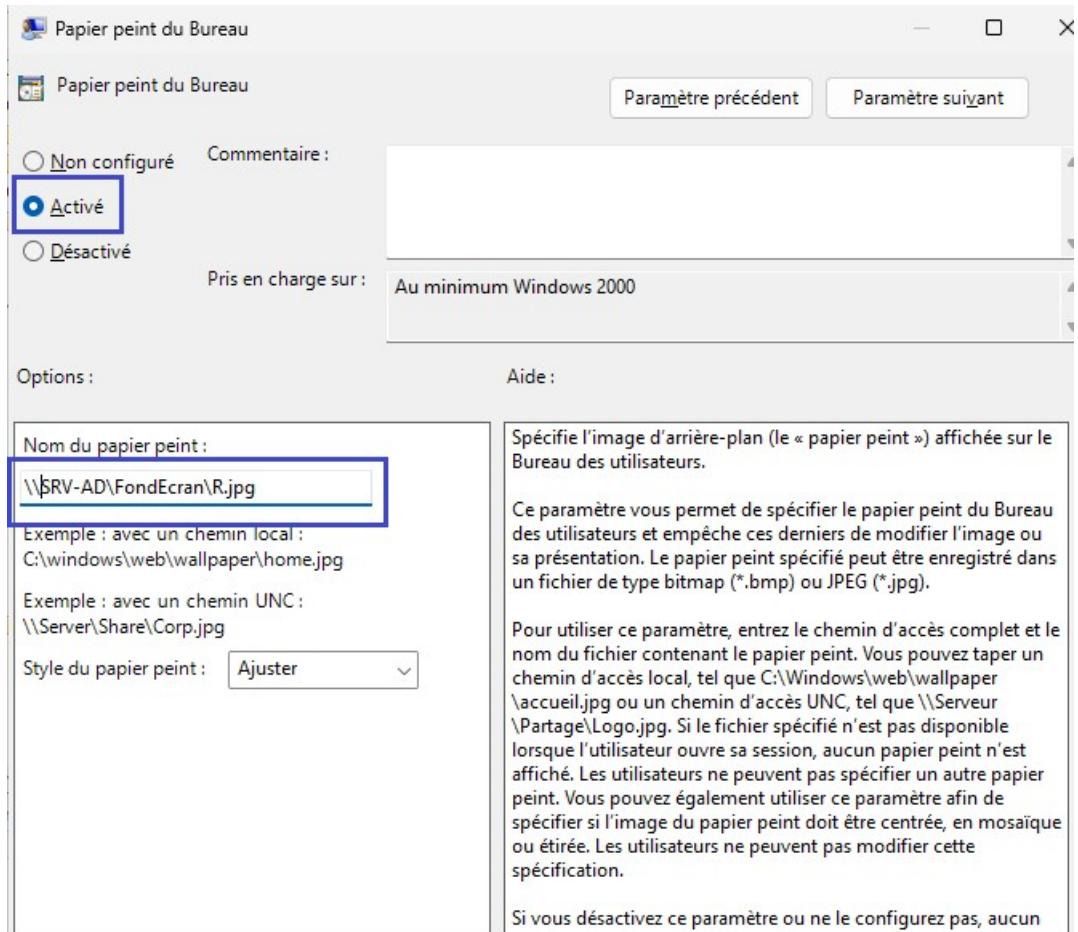
➤ Sélectionner configuration utilisateur, ensuite Stratégies. Cliquer sur Modèles d'administration, sur Bureau et sur Bureau

Paramètre
Activer Active Desktop
<b>Désactiver Active Desktop</b>
Interdire les modifications
Papier peint du Bureau
Empêcher l'ajout d'éléments
Empêcher la fermeture d'élément
Empêcher la suppression d'élément
Empêcher la modification d'élément
Désactiver tous les éléments
Ajouter/supprimer des éléments
N'autoriser que les papiers peints

➤ Désactiver Active Desktop



## ➤ Activer papier peint du Bureau



➤ Appliquer le GPO

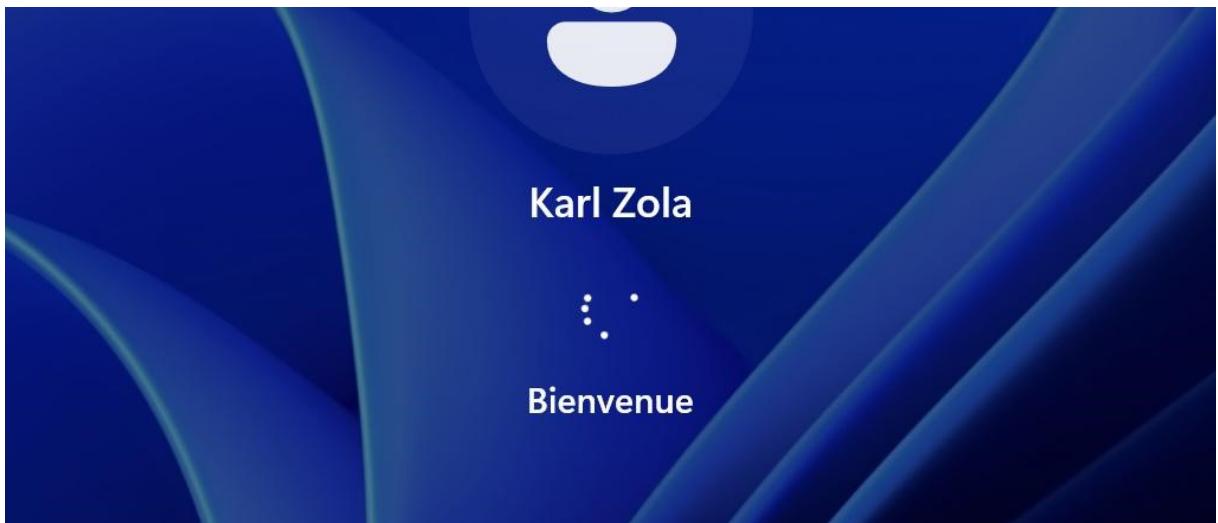
The screenshot shows the 'Gestion de stratégie de groupe' (Group Policy Management) console. On the left, under 'Forêt : TECHPLUS.LAN / Domaines / TECHPLUS.LAN', the 'PaperWall' GPO is selected. A context menu is open over it, with 'Appliqué' (Applied) highlighted. On the right, the 'PaperWall' GPO properties window is displayed. The 'Liaisons' tab is selected, showing a table of links:

	Appliqué	Lien activé	Chemin
TECHPLUS.LAN	Non	Oui	TECHPLUS.LAN

A note at the bottom states: 'Les GPO s'appliquent uniquement aux groupes, utilisateurs et ordinateurs de ce domaine.'

➤ Se connecter avec la machine Windows 11 pour tester le GPO

➤ Connexion avec l'utilisateur Karl Zola



➤ On constate que le fond d'écran est appliqué avec succès. Ce qui montre que la stratégie de groupe marche.

## **CONCLUSION**

Ce document a présenté l'essentiel de la mise en place et de l'administration d'un environnement Active Directory, depuis l'installation du contrôleur de domaine jusqu'à l'application de stratégies de groupe. Nous avons appris à structurer l'annuaire avec des unités d'organisation, créer et gérer des utilisateurs, intégrer des postes Windows 11 au domaine et appliquer des configurations centralisées via les GPO.

L'ensemble des étapes abordées constitue une base solide pour administrer efficacement et en toute sécurité une infrastructure Windows Server. Ce guide pourra servir de référence pour toute future évolution ou maintenance de l'environnement Active Directory.