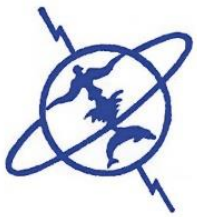


Rapport de TP :

Mise en place et gestion d'Active Directory et des stratégies de groupe (GPO)

Master CITEch

Administration et sécurité de l'Active Directory

Rédigé par : YAGOUT Yassir

Le 27-04-2025

---

1. Introduction

Le but de ce travail pratique (TP) est de mettre en place un contrôleur de domaine sur un serveur Windows Server 2012, puis de configurer un domaine, des stratégies de groupe (GPO) et d'assurer la gestion des utilisateurs et des ordinateurs dans un environnement Windows. Les compétences visées sont la création, la configuration et la gestion d'Active Directory, ainsi que l'application de stratégies de sécurité via des GPO.

2. Objectifs

- Créer et configurer un serveur Active Directory Domain Services (ADDS).
- Créer un domaine, configurer les clients pour qu'ils rejoignent le domaine.
- Créer et configurer une stratégie de groupe (GPO).
- Appliquer des politiques de sécurité à travers les GPO.

---

3. Déroulement du TP

3.1 Configuration de l'Infrastructure

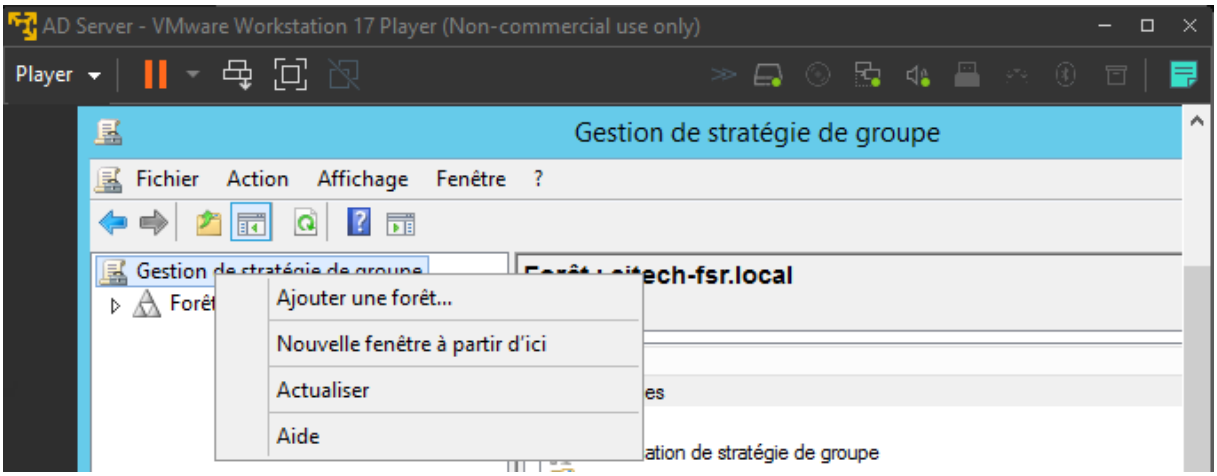
Nous avons mis en place une infrastructure avec trois machines virtuelles :

- **Serveur DC (Windows Server 2012)** : Contrôleur de domaine
- **PC-ETUD1 (Windows 7)** : Poste client 1
- **PC-ETUD2 (Windows 10)** : Poste client 2
- **PC-Externe (Windows 7)** : Poste externe pour tester la connectivité

3.2. Configuration du Contrôleur de Domaine et des Clients

3.2.1 Création du Domaine

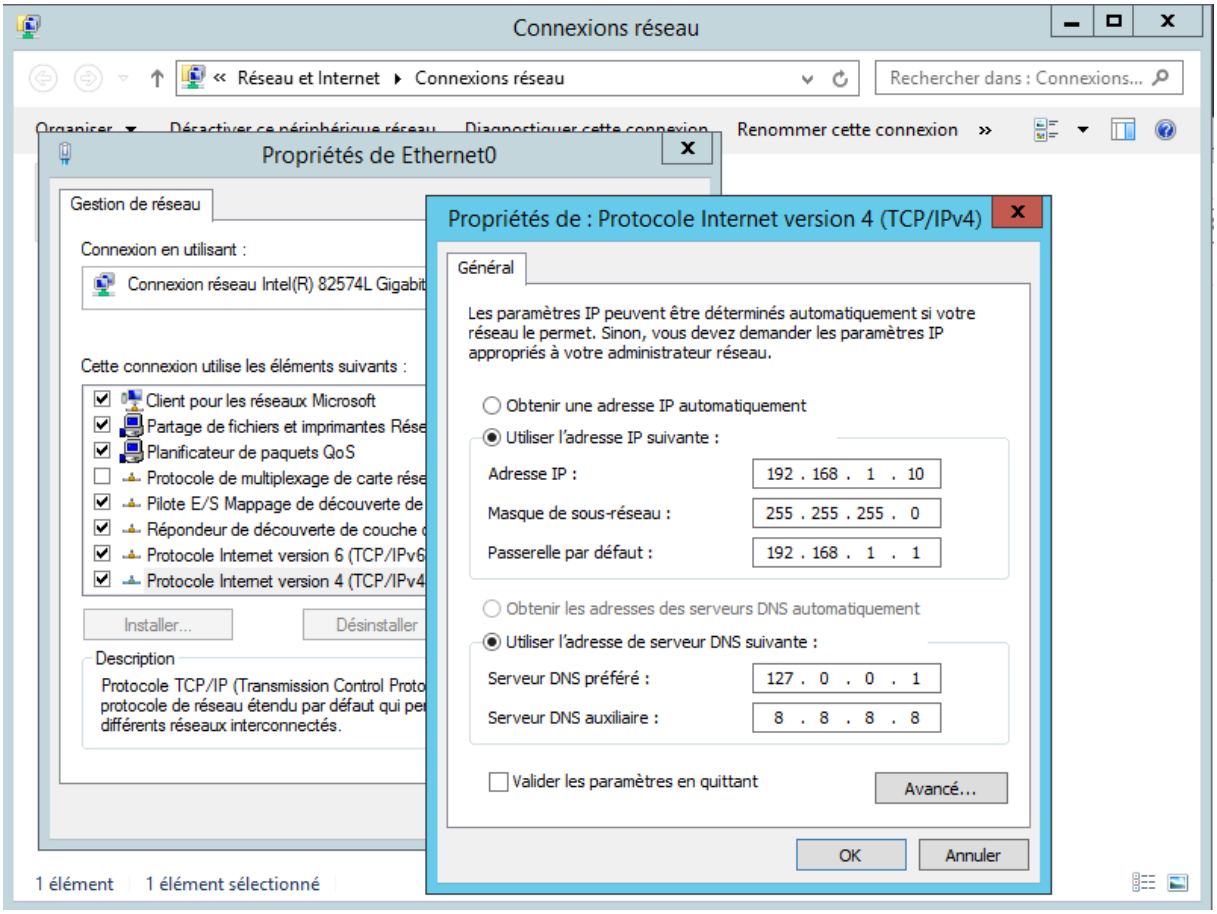
Le domaine **citech-fsr.local** a été créé à l'aide de l'assistant de gestion de serveur en choisissant l'option "Ajouter une nouvelle forêt". Une fois le domaine créé, le serveur a redémarré automatiquement.



3.2.2 Configuration de l'Adresse IP sur le Serveur et Clients

Serveur DC (Windows Server 2012)

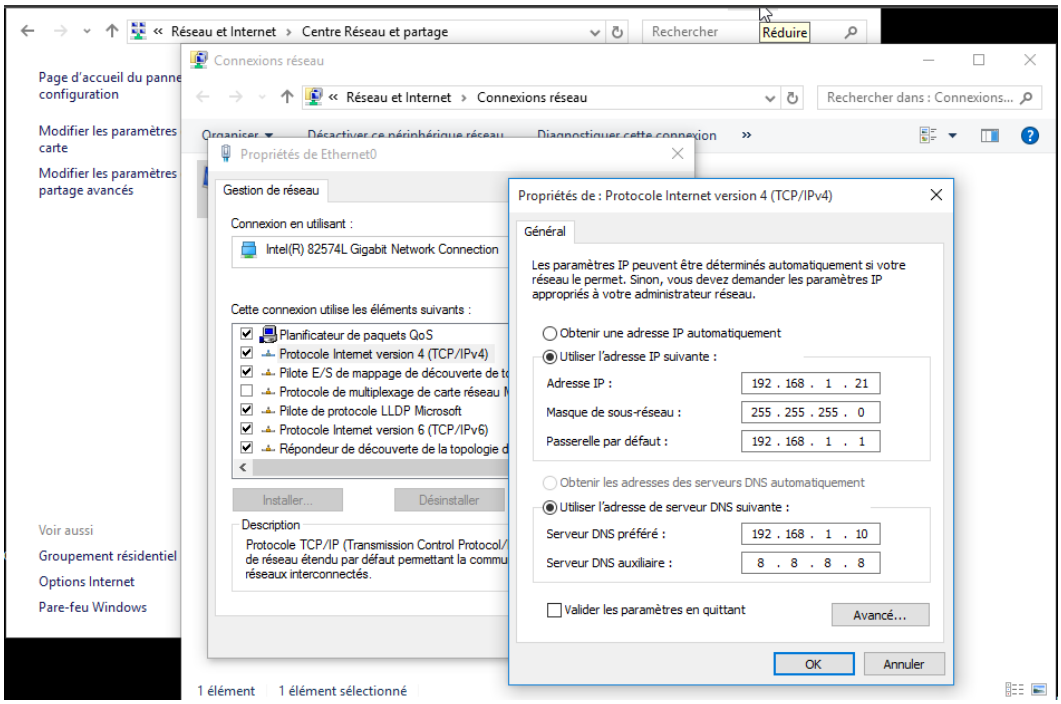
- Adresse IP : 192.168.1.10
- Serveur DNS : 192.168.1.10



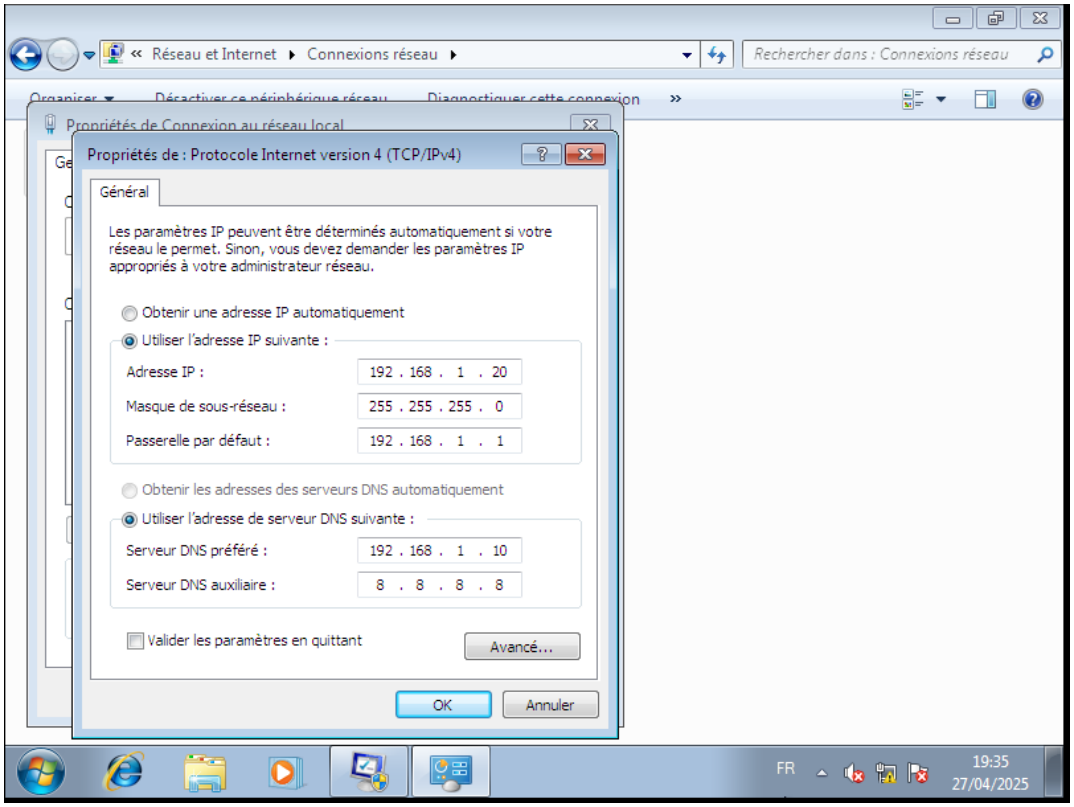
Clients (Windows 7 et Windows 10)

- Adresse IP : 192.168.1.20 (PC-ETUD1), 192.168.1.21 (PC-ETUD2)
- Serveur DNS : 192.168.1.10

Pour windows 10:



Pour windows 7:



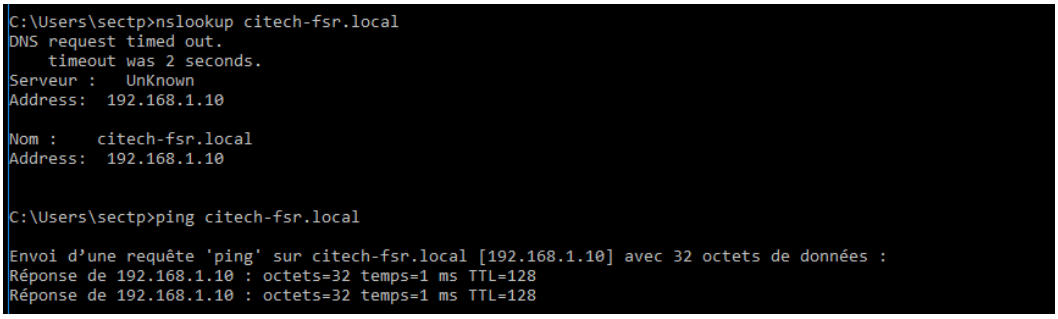
3.2.3 Vérification de la Connectivité

Les tests de connectivité ont été effectués à l'aide des commandes suivantes sur les clients :

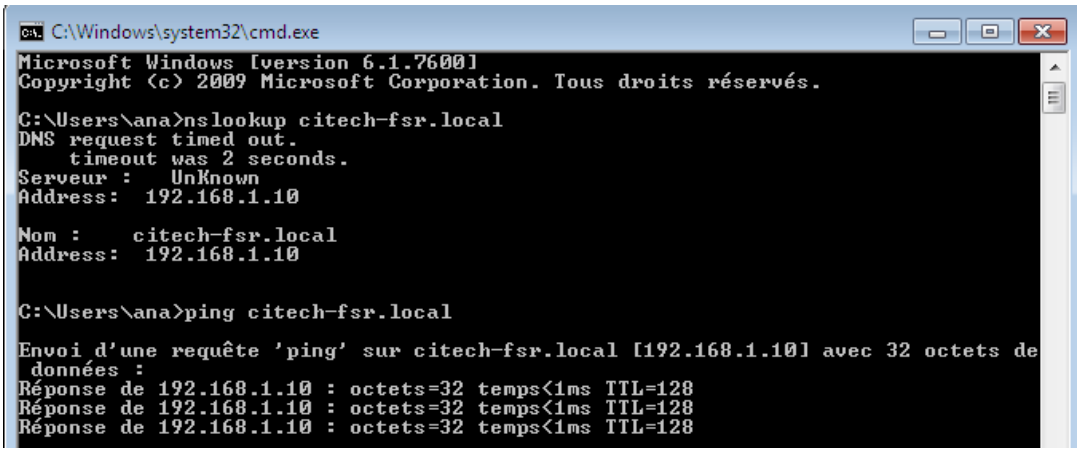
- **nslookup** pour vérifier la résolution DNS

- **ping 192.168.1.10** pour tester la connectivité avec le serveur AD

Pour windows 10 :

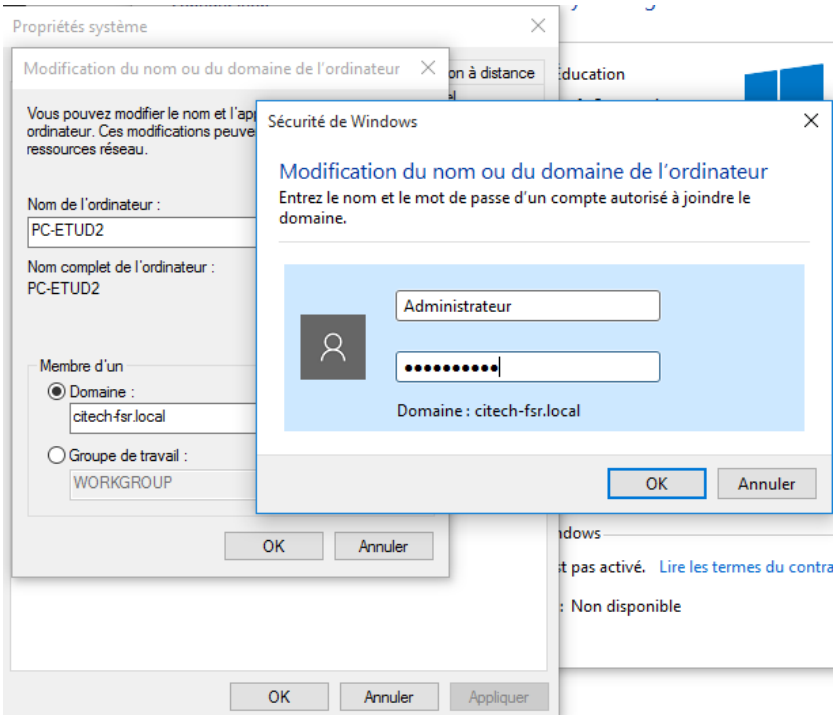


Pour Windows 7 :

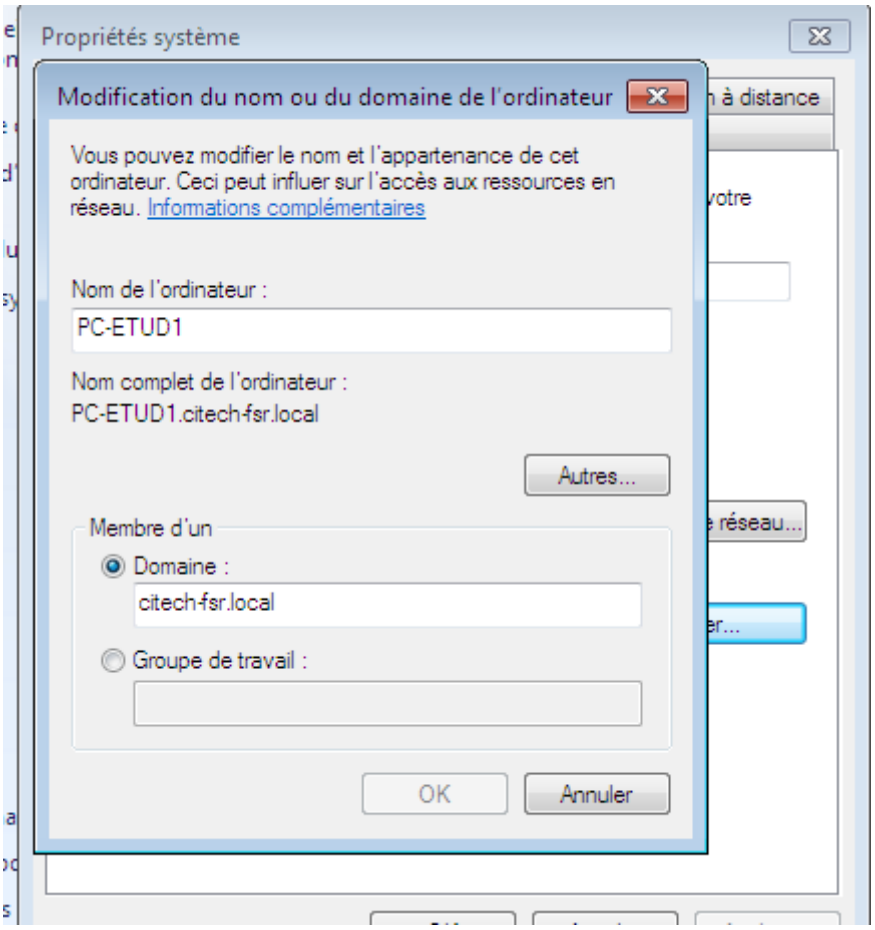


3.3. Ajout des Clients au Domaine

Pour Windows 10 (**PC-ETUD2**) : *utilisateur* : Administrateur, *mot de passe* : admin-2025



Pour Windows 7 (**PC-ETUD1**):



Les deux machines, **PC-ETUD1** et **PC-ETUD2**, ont été ajoutées au domaine **citech-fsr.local** via l'option « Modifier les paramètres système » et en renseignant les informations du domaine. Après redémarrage des clients, ceux-ci ont rejoint le domaine avec succès.

3.4 Création d'Unités Organisationnelles (OU) et Comptes Utilisateurs

3.4.1 Création des OUs

Deux unités organisationnelles ont été créées :

- **Utilisateurs_Etudiants**
- **Ordinateurs_Etudiants**

Commandes PowerShell :

```
New-ADOrganizationalUnit -Name "Utilisateurs_Etudiants" -Path "DC=citech-fsr,DC=local"

New-ADOrganizationalUnit -Name "Ordinateurs_Etudiants" -Path "DC=citech-fsr,DC=local"
```

```
PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name "Utilisateurs_Etudiants" -Path "DC=citech-fsr, DC=local"
New-ADOrganizationalUnit : Une tentative d'ajout d'un objet dans l'annuaire avec un nom déjà utilisé s'est produite
Au caractère Ligne:1 : 1
+ New-ADOrganizationalUnit -Name "Utilisateurs_Etudiants" -Path "DC=citech-fsr, DC ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (OU=Utilisateurs...h-fsr, DC=local:String) [New-ADOrganizationalUnit], ADE
   xception
    + FullyQualifiedErrorId : ActiveDirectoryServer:8305,Microsoft.ActiveDirectory.Management.Commands.NewADOrganizati
   onalUnit

PS C:\Users\Administrateur> New-ADOrganizationalUnit -Name "Ordinateurs_Etudiants" -Path "DC=citech-fsr, DC=local"
New-ADOrganizationalUnit : Une tentative d'ajout d'un objet dans l'annuaire avec un nom déjà utilisé s'est produite
Au caractère Ligne:1 : 1
+ New-ADOrganizationalUnit -Name "Ordinateurs_Etudiants" -Path "DC=citech-fsr, DC= ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (OU=Ordinateurs_...h-fsr, DC=local:String) [New-ADOrganizationalUnit], ADE
   xception
    + FullyQualifiedErrorId : ActiveDirectoryServer:8305,Microsoft.ActiveDirectory.Management.Commands.NewADOrganizati
   onalUnit
```

La création des OUs via PowerShell ou la console Active Directory.

Note : Le message d'erreur se produit en raison de l'existence préalable des deux unités d'organisation (OU).

Déplacemez les deux machines clientes dans l'OU :

```
$OUPath = "OU=Ordinateurs_Etudiants,DC=citech-fsr,DC=local"
```

```
Move-ADObject -Identity "CN=PC-ETUD1,CN=Computers,DC=citech-fsr,DC=local" -TargetPath $OUPath
```

```
Move-ADObject -Identity "CN=PC-ETUD2,CN=Computers,DC=citech-fsr,DC=local" -TargetPath $OUPath
```

Vérification de la création des OUs :

```
Get-ADComputer -Filter 'Name -like "PC-ETUD*"' | Select-Object Name, DistinguishedName
```

```
PS C:\Users\Administrateur> Get-ADOrganizationalUnit -Filter  * | Select-Object Name, DistinguishedName

Name                                                DistinguishedName
----                                                -----------------
Domain Controllers                                  OU=Domain Controllers,DC=citech-fsr,DC=local
Utilisateurs_Etudiants                              OU=Utilisateurs_Etudiants,DC=citech-fsr,DC=local
Ordinateurs_Etudiants                               OU=Ordinateurs_Etudiants,DC=citech-fsr,DC=local
```

Vérification de l'existence des deux machines clientes dans l'OU :

```
PS C:\Users\Administrateur> Get-ADComputer -Filter 'Name -like "PC-ETUD*"' | Select-Object Name, DistinguishedName

Name                                                DistinguishedName
----                                                -----------------
PC-ETUD1                                            CN=PC-ETUD1,CN=Computers,DC=citech-fsr,DC=local
PC-ETUD2                                            CN=PC-ETUD2,CN=Computers,DC=citech-fsr,DC=local
```

3.4.2 Création des Comptes Utilisateurs

Les comptes **Student1** et **Student2** ont été créés dans l'OU **Utilisateurs_Etudiants** à l'aide de PowerShell.

Commandes :

Pour Student1:

```
New-ADUser -Name "Student1" -SamAccountName "Student1" -UserPrincipalName "Student1@citech-fsr.local" -AccountPassword $Password -Enabled $true -Path "OU=Utilisateurs_Etudiants,DC=citech-fsr,DC=local"
```

```
PS C:\Users\Administrateur> $Username = "Student2"
PS C:\Users\Administrateur> $Password = ConvertTo-SecureString "Student@2025" -AsPlainText -Force
PS C:\Users\Administrateur> New-ADUser -Name $Username -SamAccountName $Username -UserPrincipalName "$Username@citech-fs
r.local" -AccountPassword $Password -Enabled $true -Path "OU=Utilisateurs_Etudiants,DC=citech-fsr,DC=local"
```

Pour Student 2 : Les mêmes commandes sont exécutées, avec un remplacement de '1' par '2'.

---

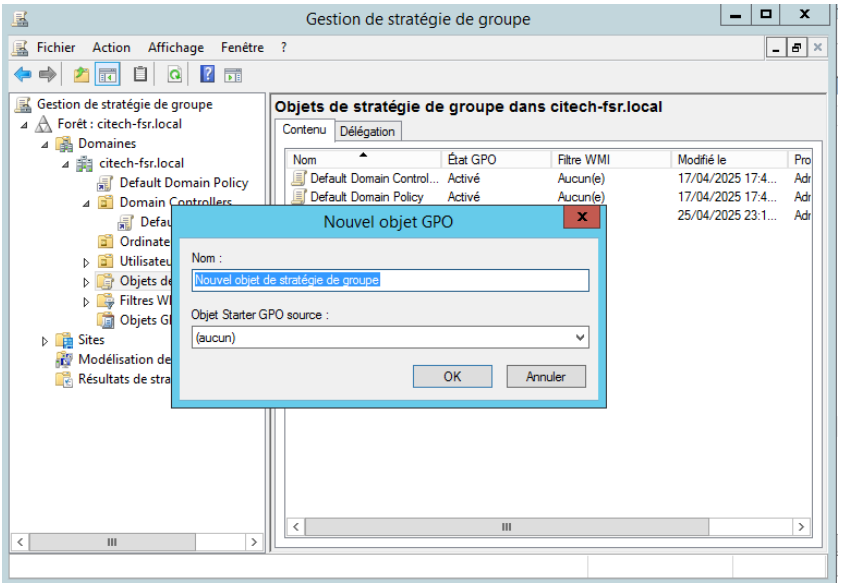
4. Création et Liaison des Stratégies de Groupe (GPO)

4.1 Création de la GPO "GPO_Securite_Etudiants"

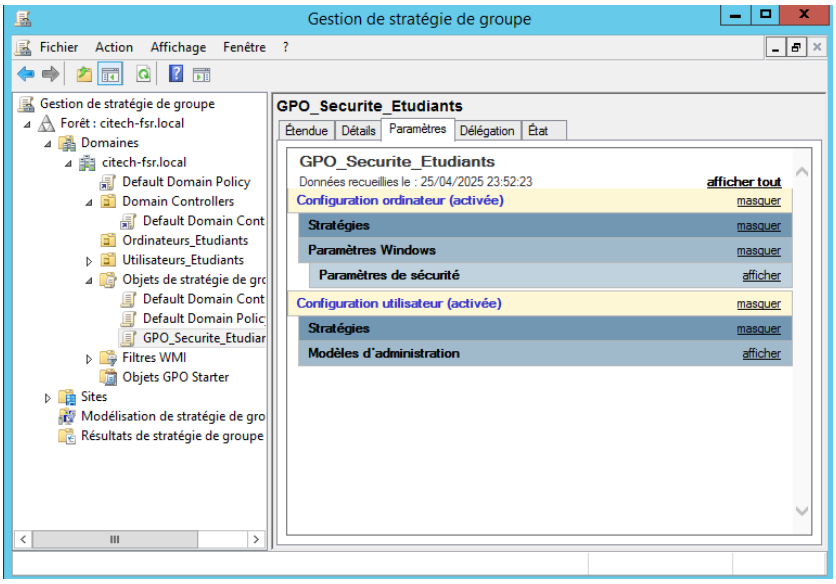
Pour ce faire, Ouvrez la Console de gestion des stratégies de groupe en exécutant la commande suivante :

```
PS C:\Users\Administrateur> gpmc.msc
```

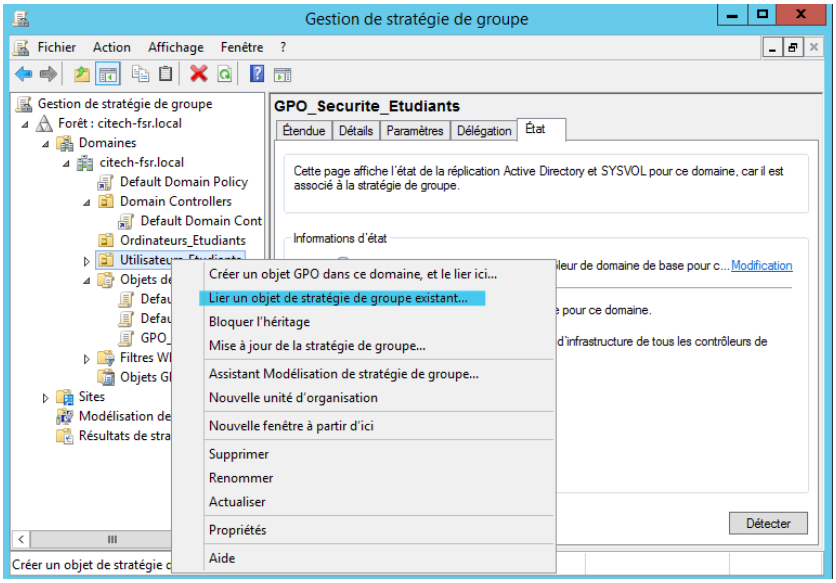
Effectuez un clic droit sur “Objets de stratégie de groupe” , puis sélectionnez “Nouveau”. Ensuite, donnez le nom "GPO_Securite_Etudiants" à la nouvelle GPO.



La GPO a été bien créée :



Un clic droit sur l'OU "Utilisateurs_Etudiants" puis sélectionnez "Lier un objet de Stratégie … ".

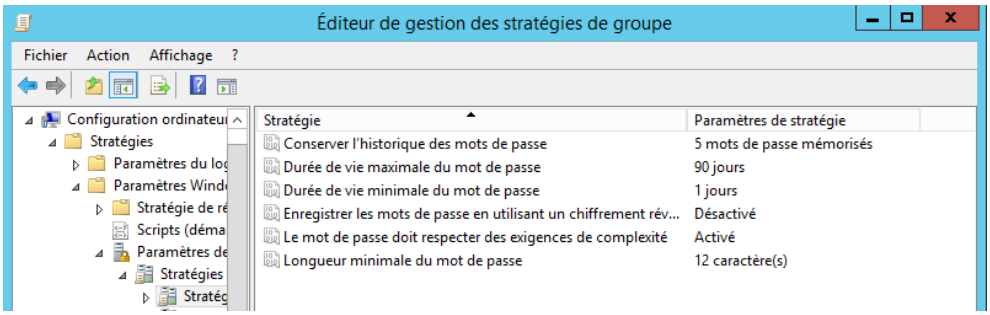


Puis sélectionnez GPO_Securite_Etudiants, puis clique sur OK.

4.2 Configuration des Politiques de Sécurité

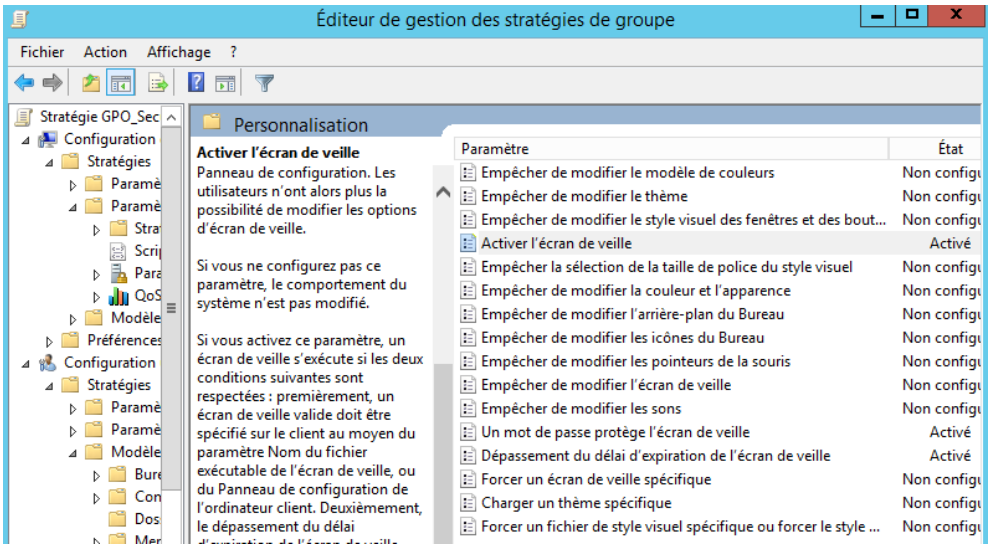
4.2.1 Politique de Mot de Passe

La politique de mot de passe a été configurée pour exiger un mot de passe complexe et sécurisé pour les utilisateurs.



4.2.2 Verrouillage Automatique de Session

La stratégie de verrouillage automatique après 10 minutes d'inactivité a été appliquée.



---

5. Vérification des Politiques et Test

Après l'application des GPO, les clients ont été redémarrés. La commande **gpupdate /force** a été utilisée pour appliquer les stratégies.

Les tests suivants ont été réalisés sur les utilisateurs **Student1** et **Student2** :

- **Test du mot de passe sécurisé** : Tentative de connexion avec un mot de passe faible (échoué).

Pour tester la stratégie de mot de passe en utilisant la commande **net user** sur un poste client avec un compte administrateur local, voici ce que tu devras faire :

```
PS C:\Users\Administrateur> net user Student1 123
Ce mot de passe ne correspond pas aux critères de stratégie de mot de passe. Vérifiez la longueur de mot de passe minima
le, la complexité du mot de passe et l'historique des critères de mots de passe.

Vous obtiendrez une aide supplémentaire en entrant NET HELPMSG 2245.

PS C:\Users\Administrateur>
```

- **Verrouillage de session** : La session s'est verrouillée après 10 minutes d'inactivité.

6. Conclusion

La mise en place de **Active Directory** et de **GPO** permet une gestion centralisée et sécurisée des utilisateurs et des ordinateurs dans un réseau. La configuration des politiques de sécurité, notamment la gestion des mots de passe et des verrouillages de session, renforce la sécurité des postes utilisateurs.

Les GPOs permettent de personnaliser les configurations pour différents groupes d'utilisateurs, offrant ainsi un contrôle administratif détaillé.

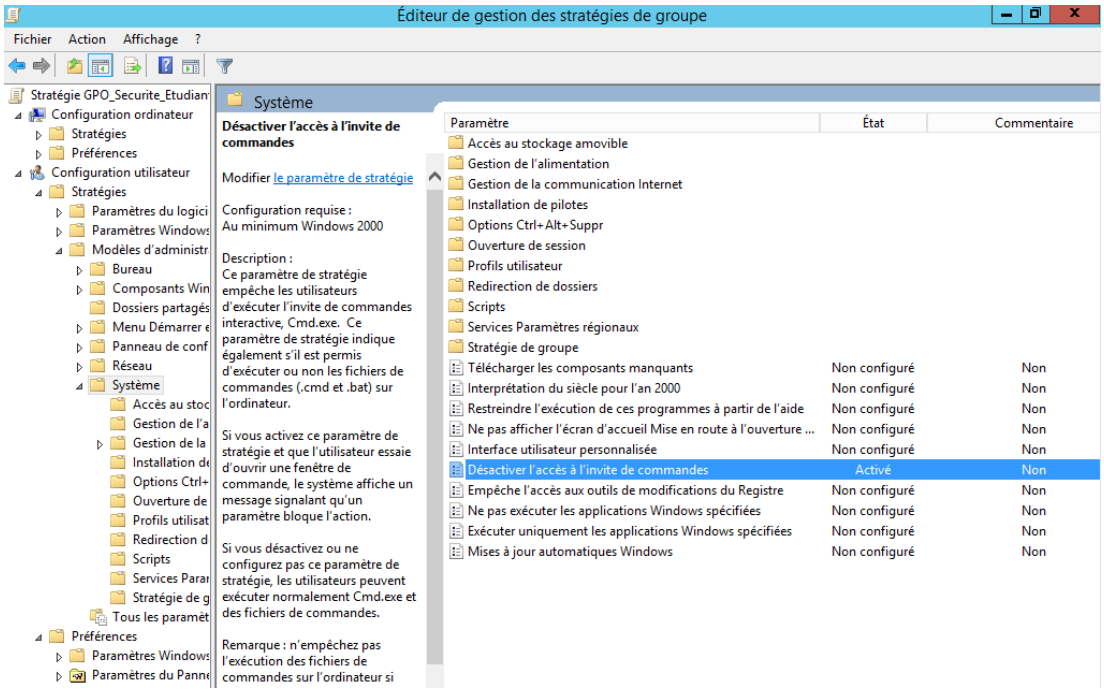
---

7. Devoirs

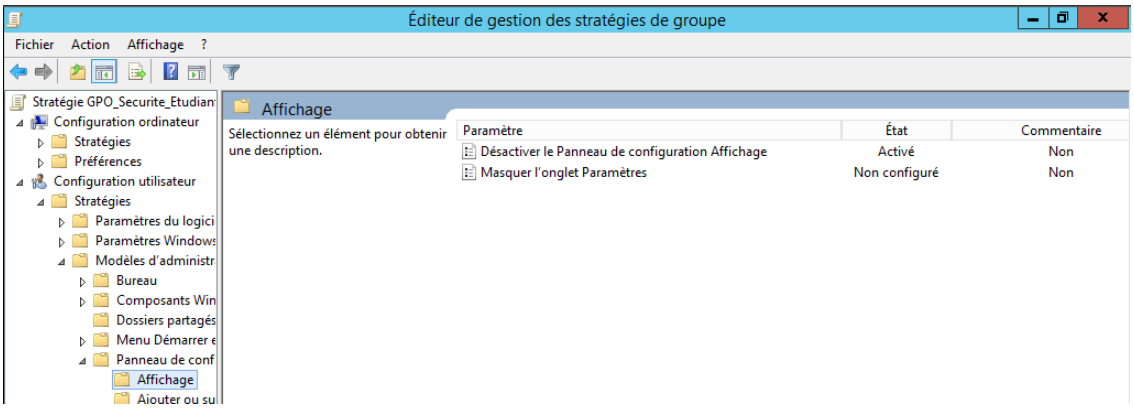
Devoir I : Sécurisation des Postes Étudiants

Les stratégies suivantes ont été configurées dans la GPO **GPO_Securite_Etudiants** :

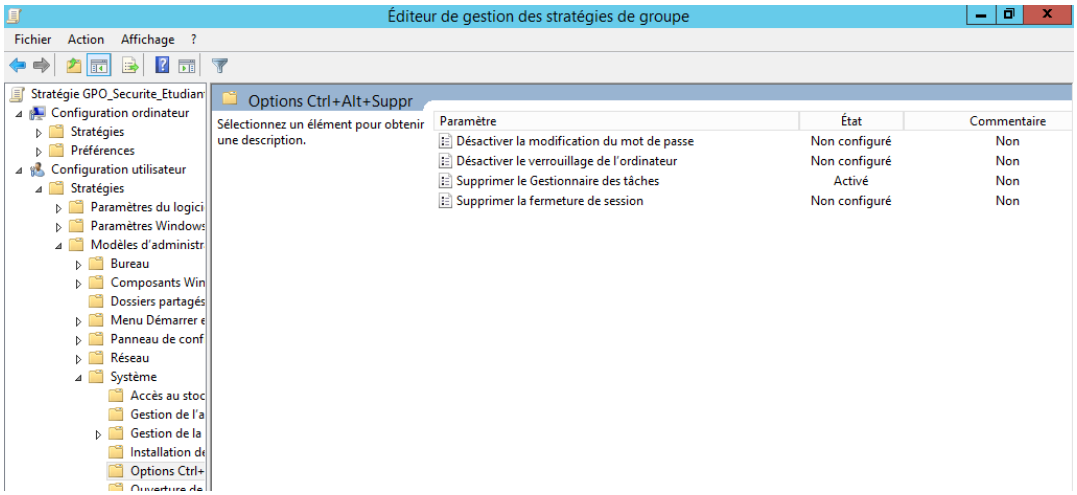
- Désactivation de l'accès à l'invite de commandes



- Désactivation du panneau de configuration d'affichage

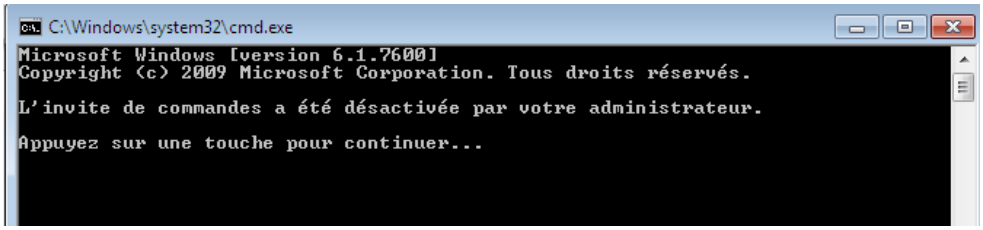


- Désactivation du gestionnaire de tâches

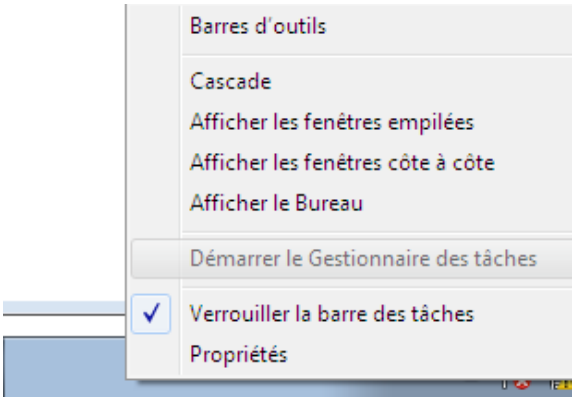


Test :

- L'accès à l'invite de commandes est désormais restreint.



- L'accès au gestionnaire de tâches a été désactivé.



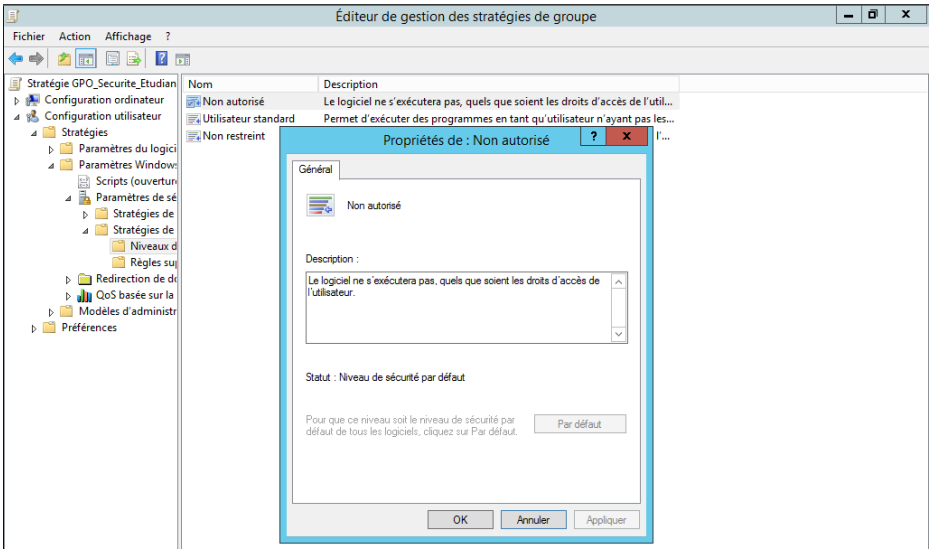
Devoir II : Empêcher l'Exécution de Logiciels Malveillants

Objectif :
Renforcer la sécurité des postes étudiants en empêchant l'exécution de logiciels non autorisés via les **Stratégies de Restriction Logicielle (SRP)** appliquées par la GPO GPO_Securite_Etudiants.

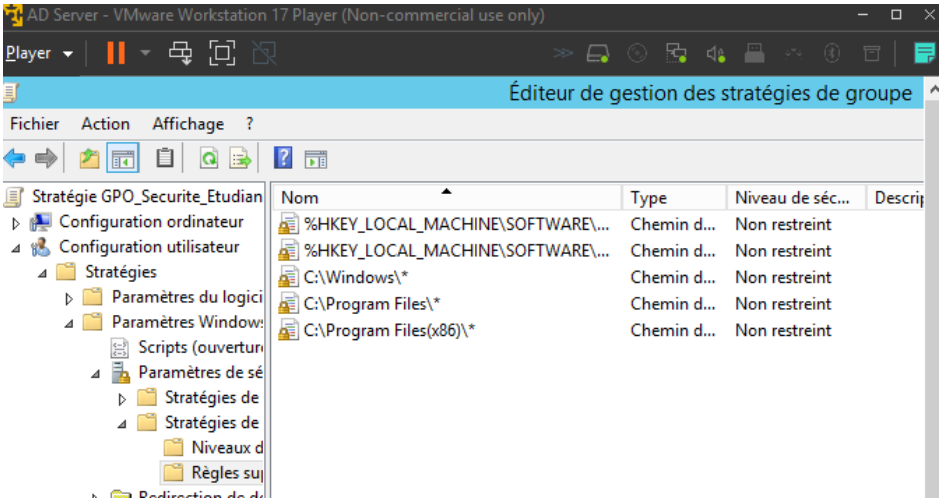
Procédure :

1. **Créer des SRP** dans :
   Configuration ordinateur → Paramètres Windows → Paramètres de sécurité → Stratégies de contrôle d'application

2. **Définir le niveau par défaut à Non autorisé** pour bloquer tous les exécutables.



3. **Créer des règles d'autorisation par chemin :**
   - C:\Windows* → Non restreint
   - C:\Program Files* → Non restreint
   - C:\Program Files (x86)* → Non restreint

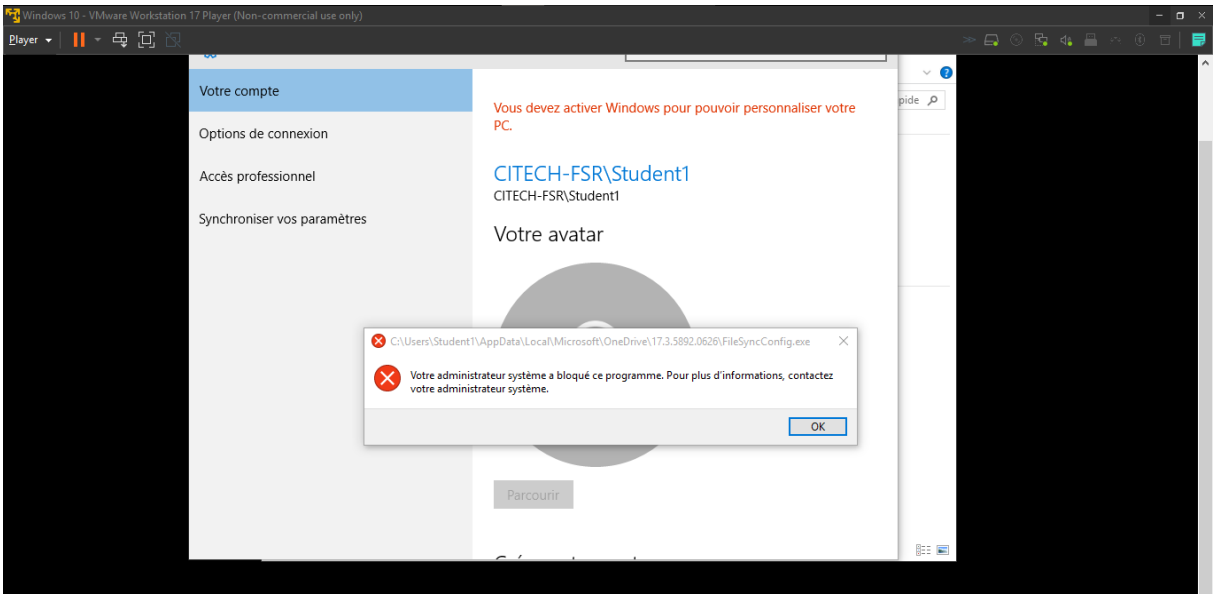


4. **Appliquer la GPO et forcer l'application avec : gpupdate /force**

```
PS C:\Users\Administrateur> gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

PS C:\Users\Administrateur> gpresult /r

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
© 2013 Microsoft Corporation. Tous droits réservés.

Créé le 27/04/2025 à 23:50:36
```

Vérifier :

Après avoir ouvert une session avec le compte Student1, un message s'est affiché confirmant le succès de la restriction : les fichiers .exe situés en dehors des chemins autorisés définis dans l'Active Directory ont bien été bloqués.



Bénéfices :

- Bloque les exécutables non validés.
- Protège contre les malwares et exécutions depuis clés USB ou téléchargements.
- Renforce le contrôle du parc informatique étudiant.