FACULTÉ DES SCIENCES DE RABAT

Rapport de TP N°1 : Mise en place et gestion d'Active Directory et des GPO

Master CyberSécurité Intelligente et Technologies Émergentes

Année : 2024-2025

Réalisé par : Youness AZZAKANI

Encadré par : Pr. Karima EL HACHIMI

Table des matières

1 Objectifs du TP

— Installer et configurer un serveur Active Directory Domain Services (ADDS).
— Créer un domaine Active Directory.
— Ajouter des clients Windows au domaine.
— Déployer et configurer des GPOs.
— Appliquer des politiques de sécurité sur les comptes utilisateurs.

2 Environnement de travail

Machine	Systéme	Adresse IP	Nom d'hôte
Serveur DC	Windows Server 2012	192.168.1.10	DC-ETUD
Client 1	Windows 7	192.168.1.20	PC-ETUD1
Client 2	Windows 10	192.168.1.21	PC-ETUD2
Client externe	Windows 7	192.168.1.22	PC-Externe

TABLE 1 – Configuration des machines virtuelles

3 Déroulement du TP

3.1 Installation et Configuration du Contrôleur de Domaine

Installation du rôle ADDS sur DC-ETUD et création du domaine citech-fsr.local.

3.2 Installation et Configuration du Contrôleur de Domaine

— On installe le rôle ADDS sur DC-ETUD.
— On crée une nouvelle forêt avec le domaine **citech-fsr.local**.
— On redémarre le serveur.

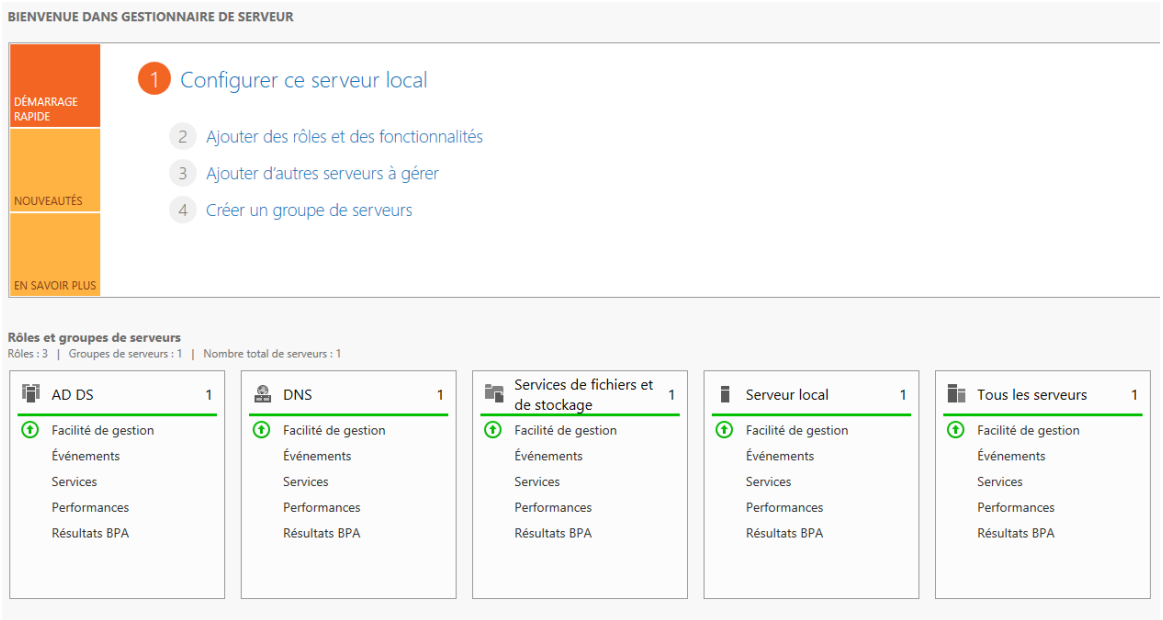


FIGURE 1 – Création du serveur ADDS

3.3 Configuration IP

Afin d'assurer une communication réseau stable entre le serveur et les clients, chaque machine virtuelle reçoit une adresse IP statique dans le même sous-réseau. Cela est essentiel pour permettre l'intégration dans le domaine Active Directory et assurer la résolution DNS.

— On configure une IP fixe sur chaque machine.
— On met le DNS primaire sur **192.168.1.10**.
— On teste avec `ping` et `nslookup`.

3.3.1 Étapes pour configurer une adresse IP statique

1. **Accéder aux paramètres réseau** : Naviguer vers Panneau de configuration → Réseau et Internet → Centre Réseau et partage.
2. **Modifier les paramètres de la carte** : Cliquer sur Modifier les paramètres de la carte (à gauche).
3. **Accéder aux propriétés d'Ethernet** : Clic droit sur Ethernet → Propriétés.
4. **Configurer TCP/IPv4** : Sélectionner Protocole Internet Version 4 (TCP/IPv4) → Propriétés.
5. **Renseigner les informations IP** : Entrer les informations suivantes dans les champs correspondants :

Machine	Adresse IP	Masque	Passerelle	DNS primaire
DC-ETUD	192.168.1.10	255.255.255.0	192.168.1.1	192.168.1.10
PC-ETUD1	192.168.1.20	255.255.255.0	192.168.1.1	192.168.1.10
PC-ETUD2	192.168.1.21	255.255.255.0	192.168.1.1	192.168.1.10
PC-Externe	192.168.1.22	255.255.255.0	192.168.1.1	192.168.1.10

Le serveur DNS secondaire peut être défini à **8.8.8.8** pour permettre une résolution externe, mais le DNS principal doit impérativement pointer vers le contrôleur de domaine (**192.168.1.10**).

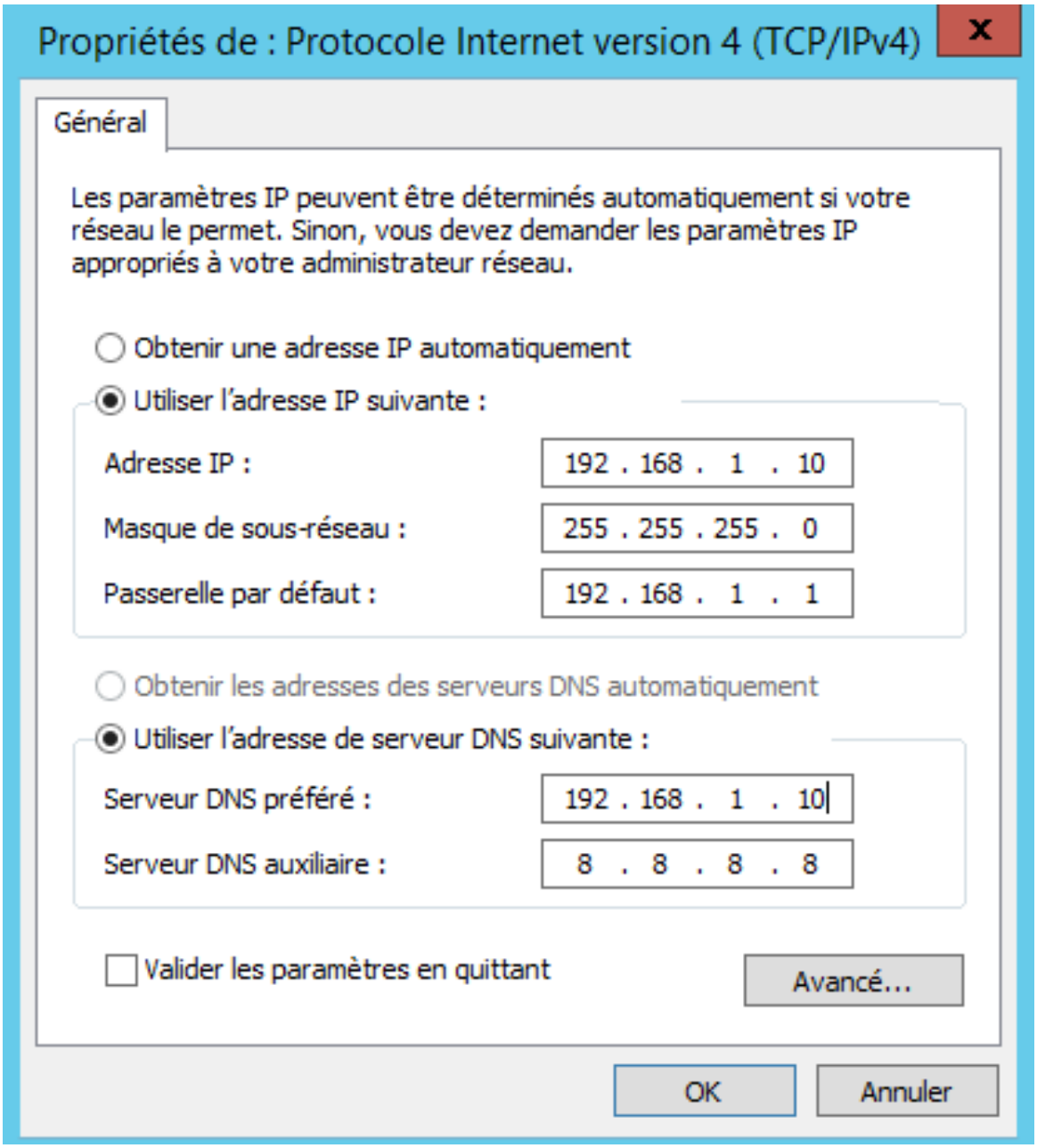


FIGURE 2 – Configuration statique de l'adresse IP de la machine DC-ETUD

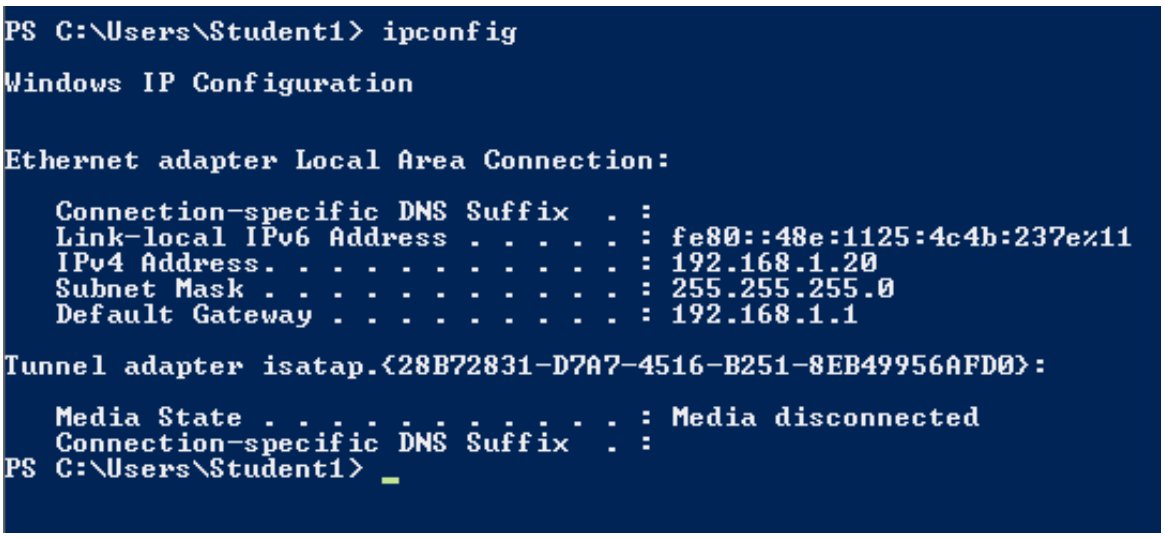


FIGURE 3 – Adresse IP de la machine PC-ETUD1

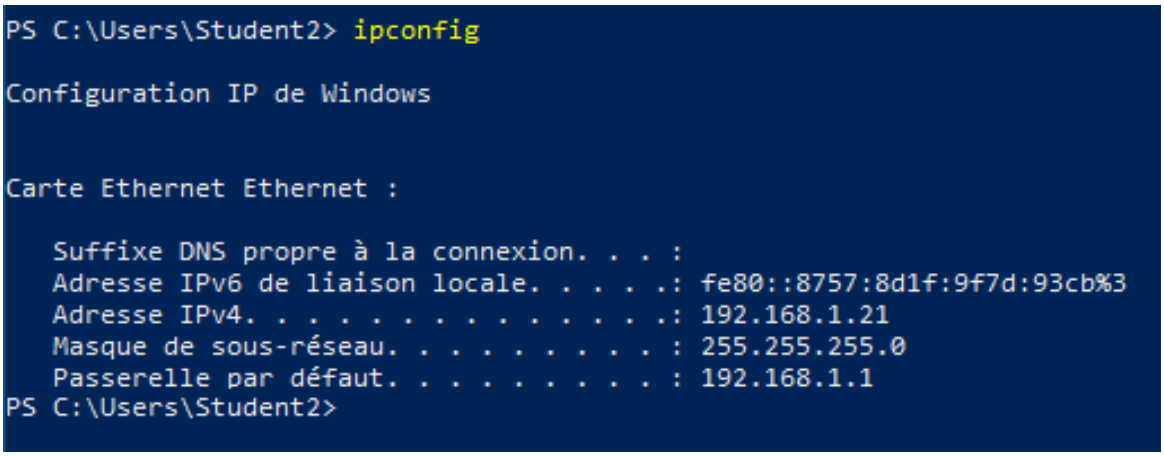


FIGURE 4 – Adresse IP de la machine PC-ETUD2

3.3.2 Vérification de la configuration réseau

1. **Ouvrir l'invite de commandes** : Lancer **cmd.exe**.
2. **Vérifier l'adresse IP** : Utiliser la commande `ipconfig` pour vérifier la configuration IP.
3. **Tester la connectivité** : Exécuter les commandes suivantes :

```
ping 192.168.1.10
nslookup citech-fsr.local
```

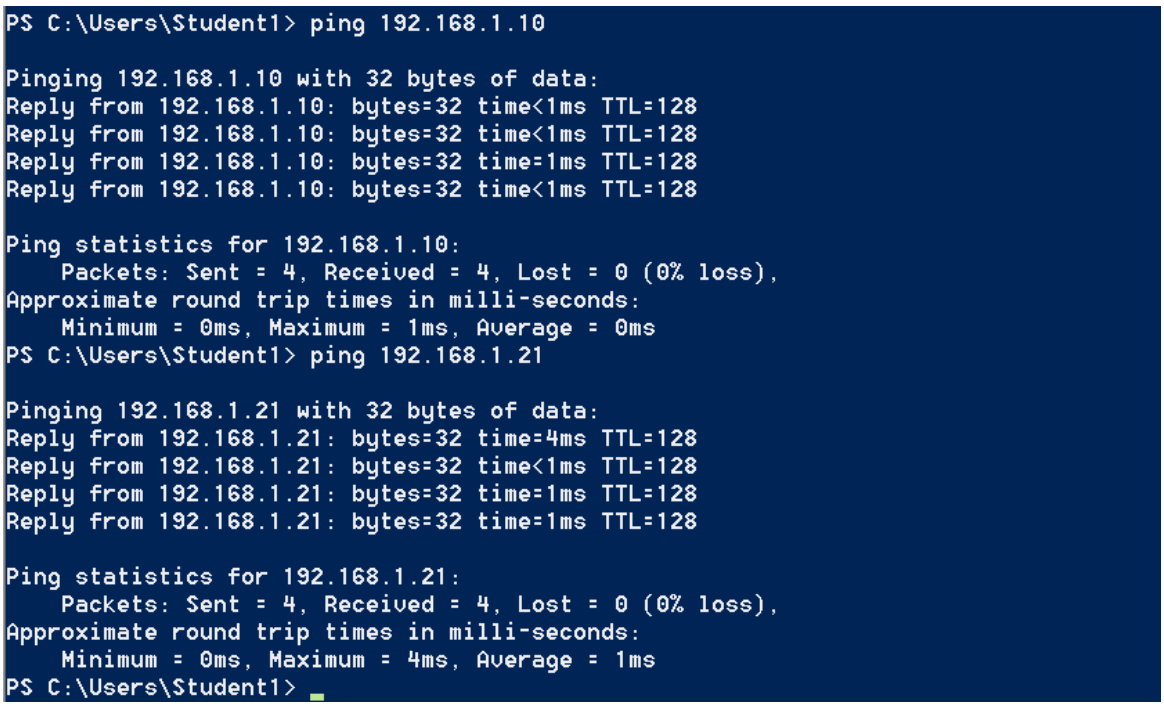


FIGURE 5 – Test de connectivité à partir de la machine PC-ETUD1

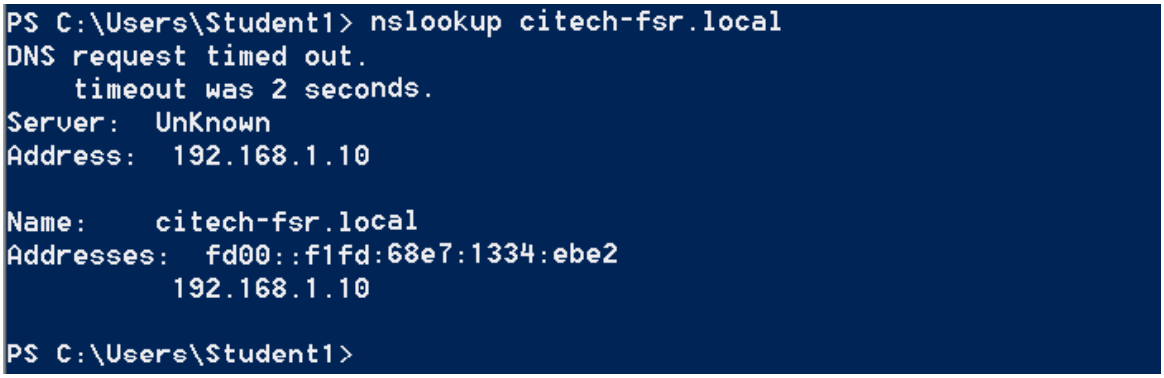


FIGURE 6 – Test de la commande nslookup

3.4 Intégration des Clients au Domaine

L'objectif de cette étape est de faire rejoindre les clients Windows (PC-ETUD1 et PC-ETUD2) au domaine Active Directory citech-fsr.local, afin qu'ils puissent être gérés centralement par le serveur DC-ETUD.

1. Changer le nom du PC :
   — On clique droit sur Ce PC → Propriétés
   — Puis on clique sur Modifier les paramètres → onglet Nom de l'ordinateur → Modifier
   — On saisie PC-ETUD1 ou PC-ETUD2 selon la machine → Redémarrer
2. Rejoindre le domaine :
   — Retourner dans Modifier les paramètres système
   — Dans "Membre de", choisir Domaine
   — On entre : citech-fsr.local
   — Puis, on saisie les identifiants administrateur :
   — Nom d'utilisateur : Administrateur
   — Mot de passe : admin-2025
3. Confirmation :
   — Un message "Bienvenue dans le domaine citech-fsr.local" doit s'afficher
   — On redémarre la machine pour finaliser l'intégration

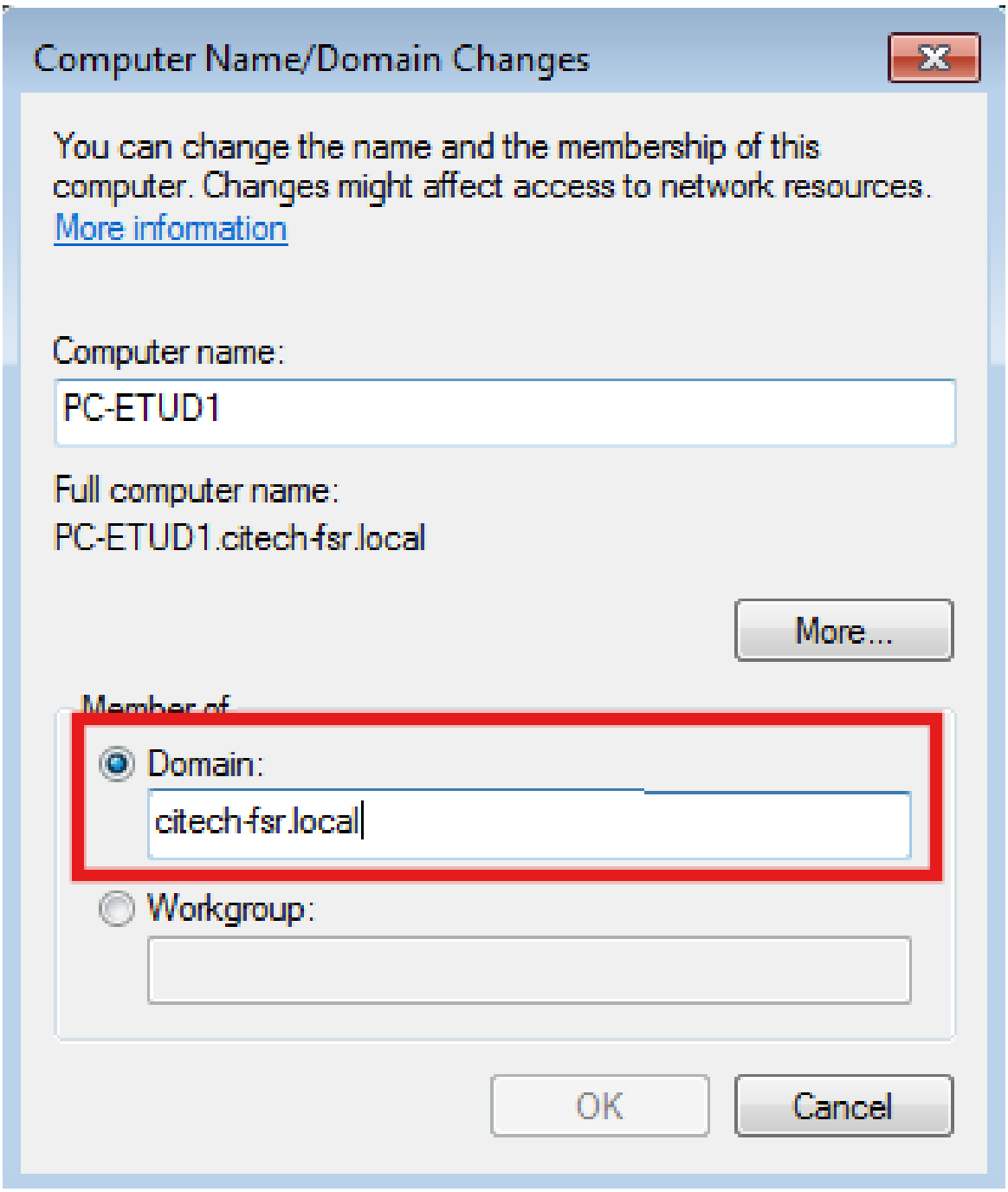


FIGURE 7 – Ajout du domaine

FIGURE 8 – Authentification au compte Administrateur

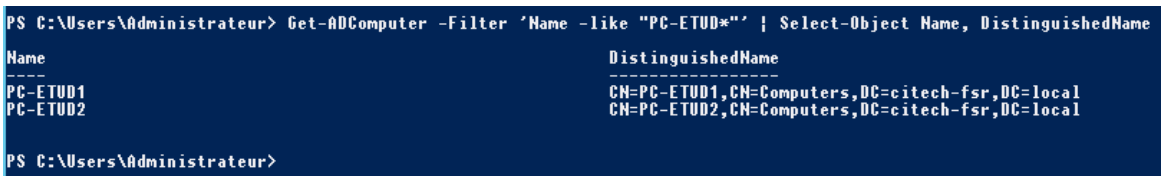


FIGURE 9 – Vérification de l'intégration des postes clients dans Active Directory

La commande permet de rechercher et d'afficher les objets ordinateur dont le nom commence par "PC-ETUD". Le résultat confirme que les postes clients PC-ETUD1 et PC-ETUD2 ont bien été ajoutés au domaine citech-fsr.local et se trouvent initialement dans le conteneur 'Computers' par défaut, comme l'indique leur DistinguishedName. Donc les deux machines sont intégrées avec succés dans l'AD.

3.5 Création des OU et des Utilisateurs

L'objectif est de structurer l'annuaire Active Directory en créant des Unités d'Organisation (OU) permettant de séparer :

— les ordinateurs clients ;
— les utilisateurs étudiants.

Puis, de créer deux comptes utilisateurs (**Student1** et **Student2**) qui seront affectés à l'OU correspondante. Cette séparation permet une gestion ciblée et efficace des stratégies de groupe (GPO).

3.5.1 Étapes réalisées

1. **Création des OU**
   Nous avons utilisé PowerShell depuis le contrôleur de domaine `DC-ETUD` pour créer deux OU :

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

   Ces OU sont désormais visibles dans la console `Active Directory Users and Computers`.

2. **Déplacement des ordinateurs dans l'OU appropriée**
   Par défaut, les ordinateurs intégrés au domaine sont placés dans le conteneur `Computers`. Nous avons déplacé les deux machines `PC-ETUD1` et `PC-ETUD2` vers l'OU `Ordinateurs_Etudiants` :

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

Move-ADObject -Identity "CN=PC-ETUD1,OU=Computers,DC=citech-fsr,DC=local" -TargetPath $OUPath
Move-ADObject -Identity "CN=PC-ETUD2,OU=Computers,DC=citech-fsr,DC=local" -TargetPath $OUPath
```

   Ce déplacement permet de leur appliquer des GPO spécifiques à l'OU.

3. **Création des comptes utilisateurs**
   Nous avons ensuite créé deux comptes : **Student1** et **Student2**, avec un mot de passe sécurisé. Toujours via PowerShell :

```
$Password = ConvertTo-SecureString "Student@2025" -AsPlainText -Force

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

New-ADUser -Name "Student2" `
    -SamAccountName "Student2" `
    -UserPrincipalName "Student2@citech-fsr.local" `
    -AccountPassword $Password `
    -Enabled $true `
    -Path "OU=Utilisateurs_Etudiants,DC=citech-fsr,DC=local"
```

   Les deux comptes sont ainsi actifs et prêts à être utilisés sur n'importe quel poste membre du domaine.

3.5.2 Résultat

— Deux OU bien séparées : une pour les utilisateurs, une pour les ordinateurs ;
— Deux utilisateurs étudiants créés, avec mots de passe conformes à la politique de sécurité ;
— Les ordinateurs sont prêts à recevoir les GPO ciblées via leur OU.

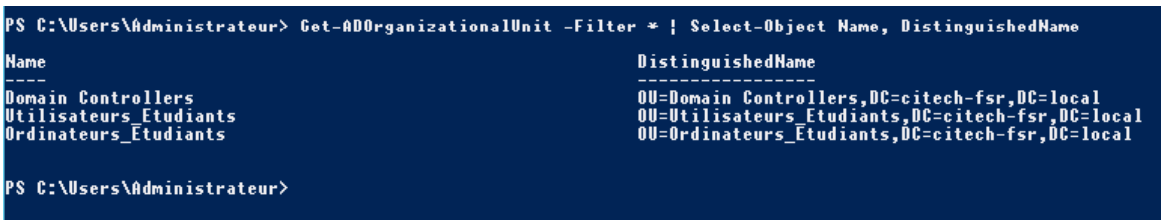


FIGURE 10 – Vérification des OUs crées avec la commande Powershell

3.5.3 Intérêt de cette organisation

Organiser l'Active Directory en OU distinctes permet de :
— Appliquer des politiques spécifiques à chaque groupe d'objets (utilisateurs ou ordinateurs) ;
— Gagner en lisibilité et en maintenabilité pour l'administrateur ;
— Limiter les erreurs en ciblant précisément les éléments concernés par une GPO.
— On crée deux OUs : Utilisateurs_Etudiants et Ordinateurs_Etudiants.
— On déplace les ordinateurs dans Ordinateurs_Etudiants.
— On crée deux utilisateurs Student1 et Student2 avec mot de passe Student@2025.

3.6 Création et Liaison d'une GPO

L'objectif de cette étape est de créer une stratégie de groupe (GPO) nommée **GPO_Securite_Etudiants**, et de la lier à l'OU **Utilisateurs_Etudiants**, afin que toutes les règles de sécurité définies dans cette GPO s'appliquent uniquement aux utilisateurs étudiants du domaine **citech-fsr.local**.

Étapes de création et de liaison

1. **Ouvrir la console de gestion des stratégies de groupe**
   Sur le serveur **DC-ETUD** :
   — Ouvrir la console GPMC :

   ```
   gpmc.msc
   ```

   — Dans l'arborescence : **Forêt : citech-fsr.local** > **Domaines** > **citech-fsr.local**.
2. **Créer la GPO**
   Clic droit sur **Objets de stratégie de groupe** → **Nouveau**.
   Nommer la stratégie :

   ```
   GPO_Securite_Etudiants
   ```

   Valider.
   Cette GPO sera utilisée pour configurer les politiques de sécurité ciblées sur les étudiants.
3. **Lier la GPO à l'OU Utilisateurs_Etudiants**
   Cliquer droit sur l'OU **Utilisateurs_Etudiants**.
   Sélectionner **Lier un GPO existant**.
   Choisir **GPO_Securite_Etudiants** dans la liste, puis valider.

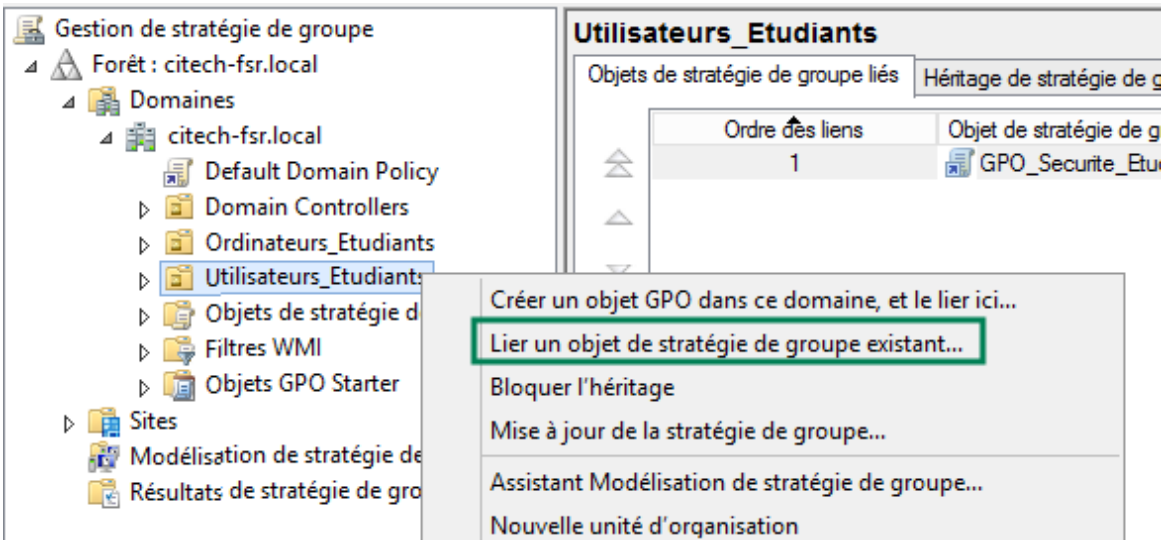


FIGURE 11 – Lier la stratégie de groupe GPO_Securite_Etudiants à l'OU Utilisateurs_Etudiants

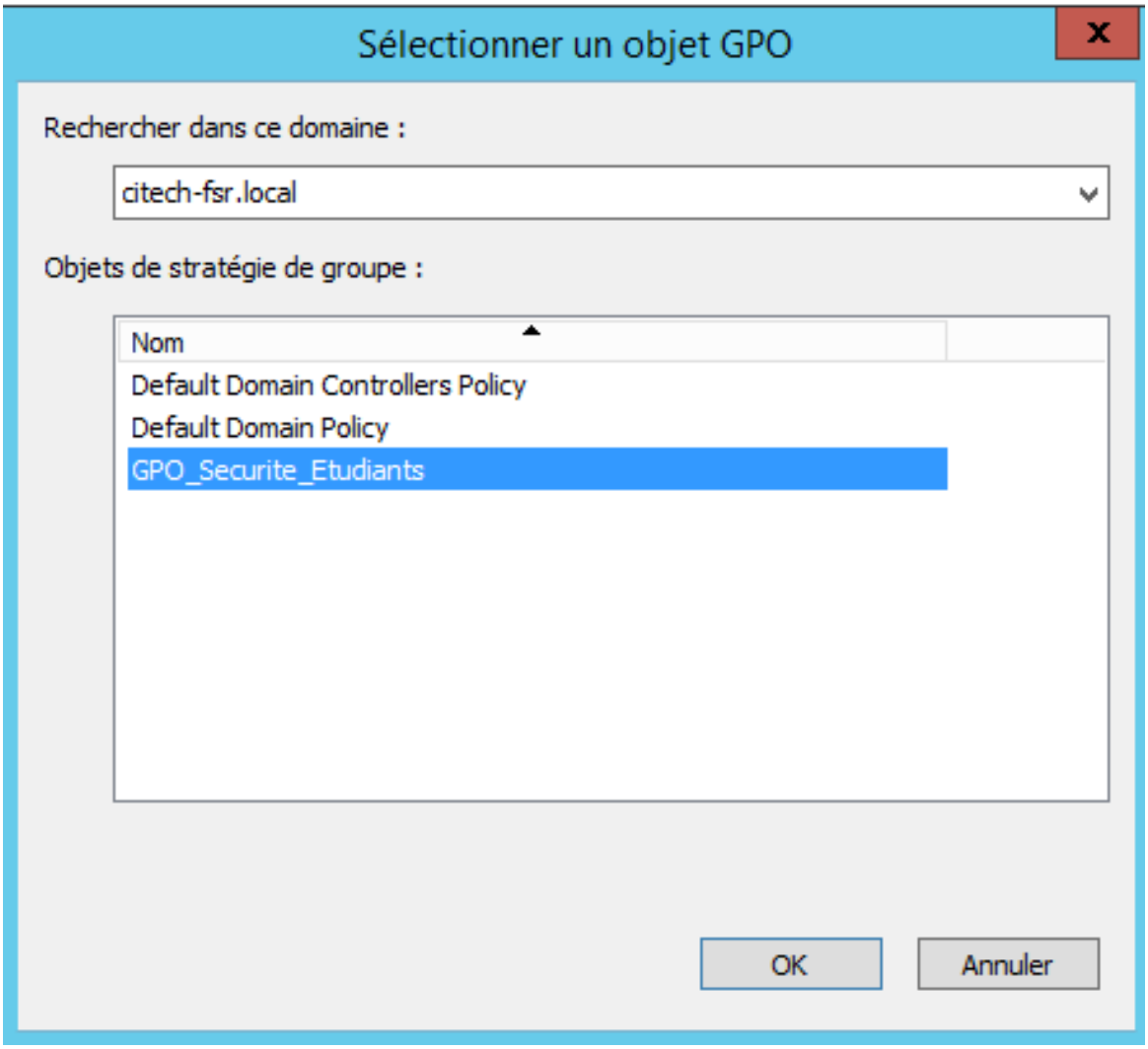


FIGURE 12 – Sélectionner GPO_Securite_Etudiants

Résultat

La GPO **GPO_Securite_Etudiants** est maintenant liée à l'OU contenant les comptes **Student1** et **Student2**. Toutes les règles définies dans cette GPO ne s'appliqueront qu'aux utilisateurs appartenant à cette

unité d'organisation, ce qui garantit un ciblage précis et sécurisé.

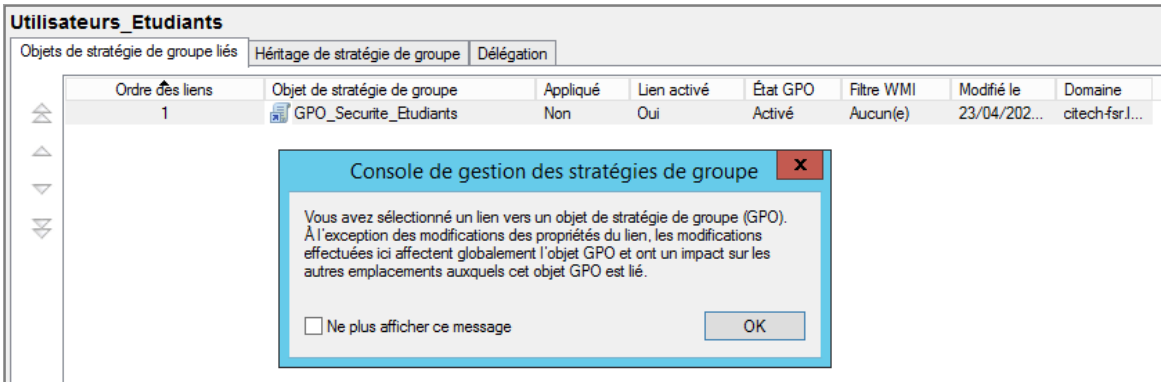


FIGURE 13 – Liaison de stratégie de groupe GPO_Securite_Etudiants à l'OU Utilisateurs_Etudiants effectuée

Intérêt de cette liaison

Lier une GPO à une OU spécifique permet :
— De segmenter les politiques de sécurité par groupe d'utilisateurs ;
— D'éviter l'application globale à tous les objets du domaine ;
— D'organiser la gestion des règles de façon claire et efficace.

3.7 Configuration des Stratégies de Sécurité

Cette étape consiste à configurer des stratégies de sécurité essentielles pour les utilisateurs du domaine, via la GPO **GPO_Securite_Etudiants**. Les paramètres choisis permettent de renforcer la sécurité des comptes utilisateurs et de limiter les abus en cas d'inactivité des sessions.

3.7.1 Étapes de configuration

1. **Accès à la GPO**
   Ouvrir la console et entrer :

```
gpmc.msc
```

   Modifier la stratégie **GPO_Securite_Etudiants** :

2. **Configuration de la politique de mot de passe**
   Chemin : **Configuration ordinateur** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies de compte** > **Stratégie de mot de passe**.
   Nous avons configuré les options suivantes :

Paramètre	Valeur définie
Longueur minimale du mot de passe	8 caractères
Complexité des mots de passe	Activée (majuscules, chiffres, symboles...)
Durée de vie maximale du mot de passe	42 jours (valeur par défaut)
Historique des mots de passe	5 anciens mots mémorisés

   → Ces paramètres garantissent que les mots de passe sont complexes, régulièrement renouvelés et non réutilisables immédiatement.

3. **Configuration du verrouillage automatique de session**
   Chemin : **Configuration utilisateur** > **Modèles d'administration** > **Panneau de configuration** > **Personnalisation**.
   Les paramètres appliqués sont :

Paramètre	Valeur
Activer l'écran de veille	Activé
Mot de passe à la reprise	Activé
Délai avant activation	600 secondes (10 minutes)

   → Cela permet de verrouiller la session automatiquement après 10 minutes d'inactivité, réduisant les risques d'accès non autorisé sur une machine laissée sans surveillance.

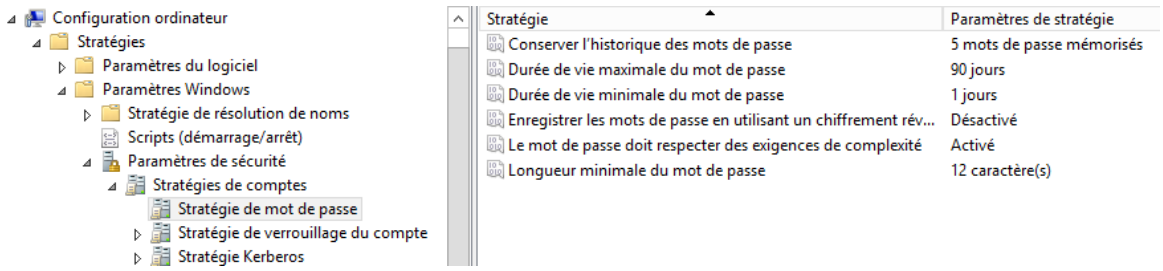


FIGURE 14 – Configuration de la stratégie de mot de passe

Paramètre	État	Commentaire
Empêcher de modifier le modèle de couleurs	Non configuré	Non
Empêcher de modifier le thème	Non configuré	Non
Empêcher de modifier le style visuel des fenêtres et des bout...	Non configuré	Non
Activer l'écran de veille	Activé	Non
Empêcher la sélection de la taille de police du style visuel	Non configuré	Non
Empêcher de modifier la couleur et l'apparence	Non configuré	Non
Empêcher de modifier l'arrière-plan du Bureau	Non configuré	Non
Empêcher de modifier les icônes du Bureau	Non configuré	Non
Empêcher de modifier les pointeurs de la souris	Non configuré	Non
Empêcher de modifier l'écran de veille	Non configuré	Non
Empêcher de modifier les sons	Non configuré	Non
Un mot de passe protège l'écran de veille	Activé	Non
Dépassement du délai d'expiration de l'écran de veille	Activé	Non
Forcer un écran de veille spécifique	Non configuré	Non
Charger un thème spécifique	Non configuré	Non
Forcer un fichier de style visuel spécifique ou forcer le style ...	Non configuré	Non

FIGURE 15 – Configuration du verrouillage de session par écran de veille

3.7.2 Résultat attendu

Les utilisateurs **Student1** et **Student2** doivent désormais :
— Choisir un mot de passe fort à la connexion ;
— Se reconnecter après inactivité prolongée ;
— Les postes clients se conforment aux exigences minimales de sécurité.

3.7.3 Intérêt de ces stratégies

L'application de ces politiques permet :
— D'empêcher les mots de passe faibles ou évidents ;
— De renforcer la sécurité physique des postes ;
— D'éduquer les utilisateurs à de bonnes pratiques de sécurité.
Ces stratégies constituent la base d'une politique de sécurité sérieuse dans un environnement d'entreprise ou d'école.

3.8 Application des GPO et vérification

Après avoir créé et configuré la GPO **GPO_Securite_Etudiants**, il est indispensable de forcer son application sur les postes clients du domaine, puis de vérifier que les paramètres de sécurité sont bien pris en compte.

3.8.1 Étapes d'application des GPO

1. **Mise à jour des stratégies de groupe sur les clients**
   Sur chaque poste client (ex. : **PC-ETUD1** ou **PC-ETUD2**), on ouvre l'invite de commandes (ou PowerShell), et on exécute :

```
gpupdate /force
```

Cette commande permet de forcer l'application immédiate des stratégies de groupe, sans attendre la prochaine actualisation automatique.

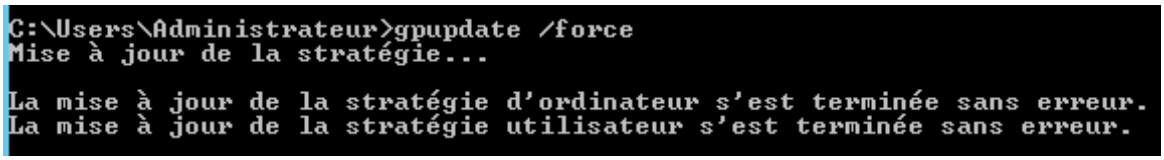


FIGURE 16 – Mise à jour forcée des stratégies de groupe (gpupdate /force)

2. **Vérification des stratégies appliquées**
   Toujours depuis la session du client (par exemple connecté avec **Student1**), exécuter :

```
gpresult /r
```

Cette commande affiche les stratégies appliquées à l'utilisateur et à la machine.
Dans le résultat affiché, on doit voir la GPO **GPO_Securite_Etudiants** listée dans les objets de stratégie appliqués.
On peut aussi vérifier si elle est appliquée au niveau utilisateur et/ou ordinateur.

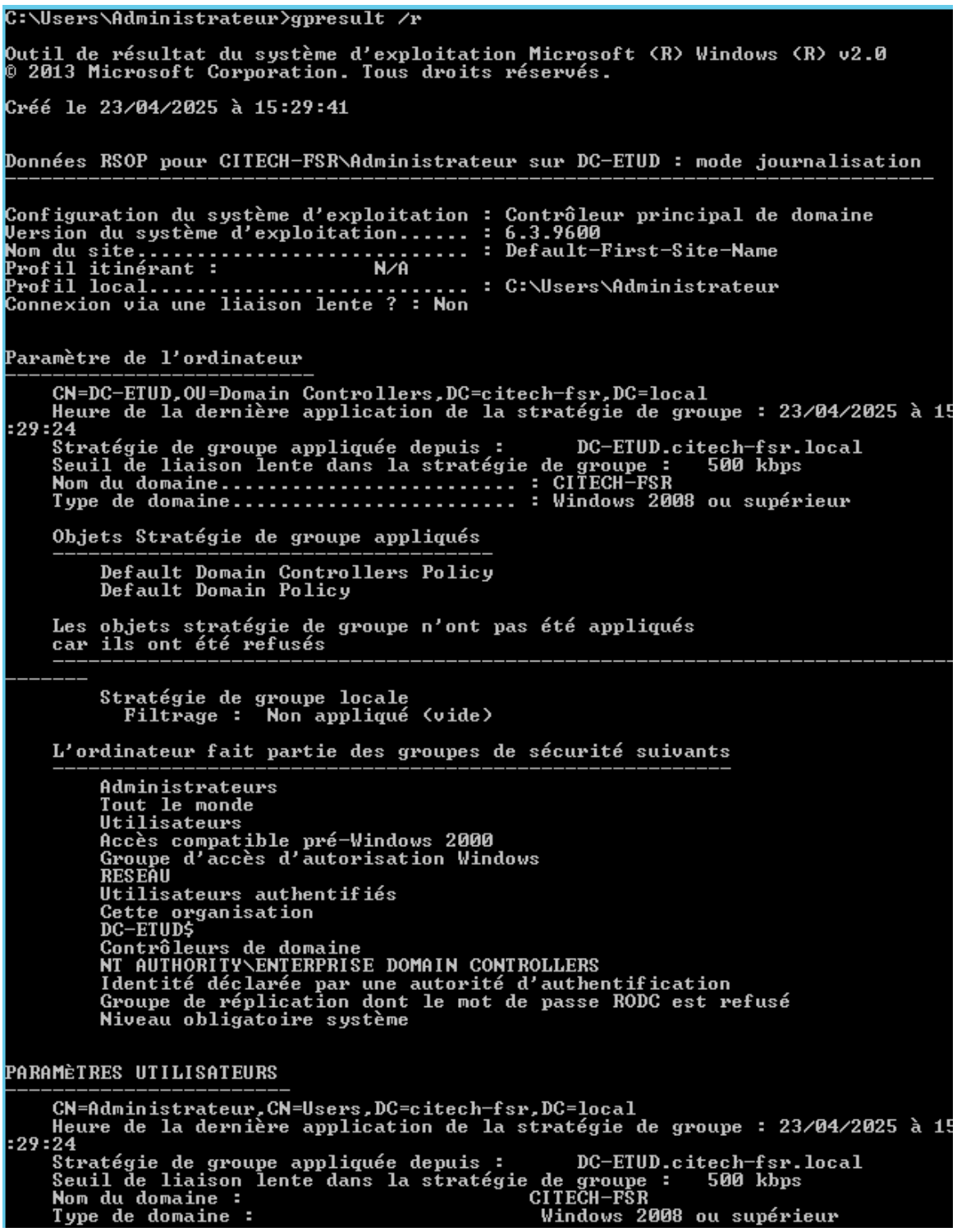


FIGURE 17 – Résultat de l'application des stratégies de groupe (gpresult /r)

3.8.2 Tests de vérification

Une fois les GPO appliquées, nous avons effectué des tests concrets :

— Connexion avec **Student1** et **Student2** ;
— Saisie de mots de passe faibles → Refusé (politique de complexité) ;
— Inactivité prolongée (>10 min) → Verrouillage automatique de la session.

Ces tests valident que la stratégie :

— Renforce la sécurité dès la connexion ;
— S'applique de manière ciblée grâce à l'OU ;
— Fonctionne de façon fiable sur les clients intégrés au domaine.

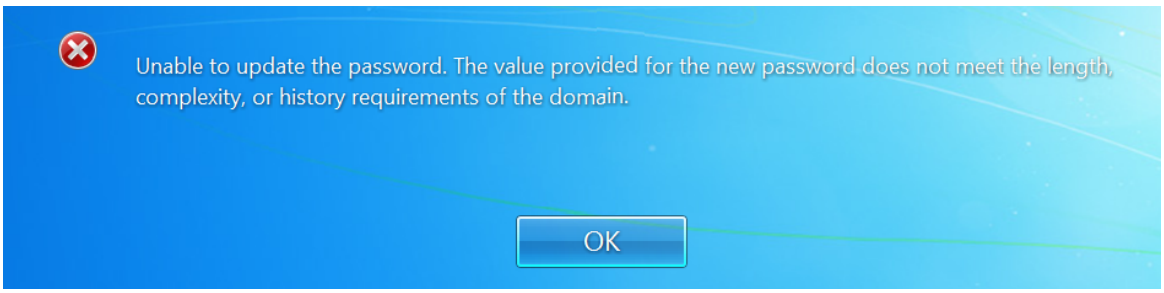


FIGURE 18 – Essayer de modifier le mots de passe avec un autre moins sécurisé

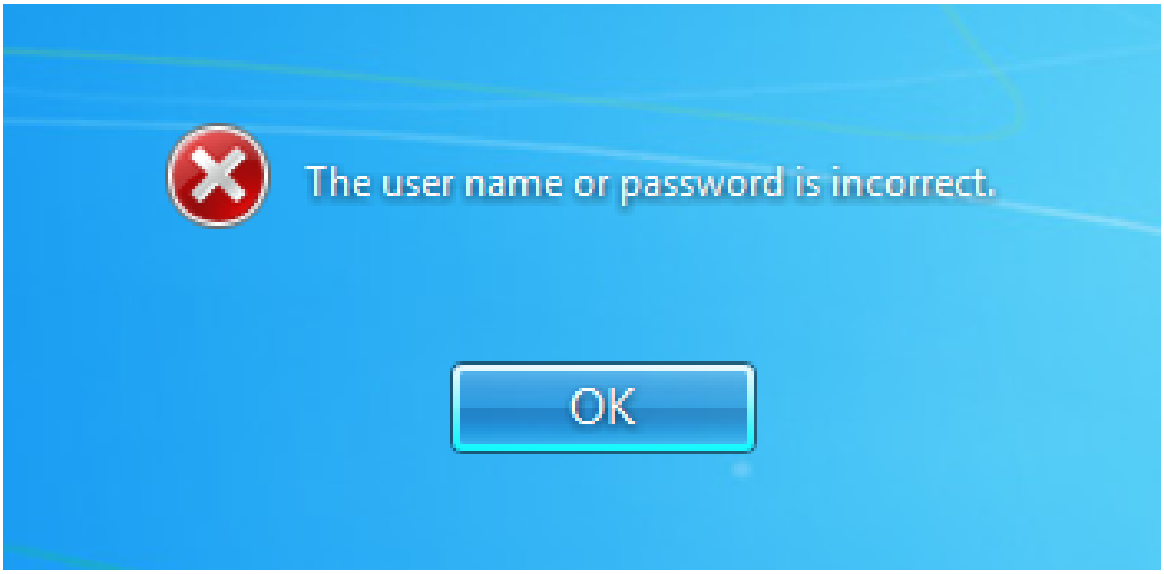


FIGURE 19 – Essayez un mot de passe erroné

— Après une tentative erronée, le système a affiché un message d'erreur du type : « Le nom d'utilisateur ou le mot de passe est incorrect ».

4 Devoir I – Sécurisation des Postes Ètudiants

L'objectif de ce devoir est de renforcer la sécurité des postes étudiants en désactivant l'accès à certains outils système, à savoir :

— L'invite de commandes (cmd)
— Le panneau d'affichage
— Le gestionnaire des tâches

Ces restrictions sont appliquées via la GPO existante GPO_Securite_Etudiants, déjà liée à l'OU Utilisateurs_Etudiants.

4.1 Étapes de mise en œuvre

4.1.1 Ouverture de la stratégie GPO :

On ouvre la GPO avec la console **gpmc.msc**, puis on clique droit sur `GPO_Securite_Etudiants` → Modifier.

4.1.2 Blocage de l'invite de commandes :

— Chemin :
Configuration utilisateur > Modèles d'administration > Système
— Stratégie activée :
Désactiver l'accès à l'invite de commandes → Activé

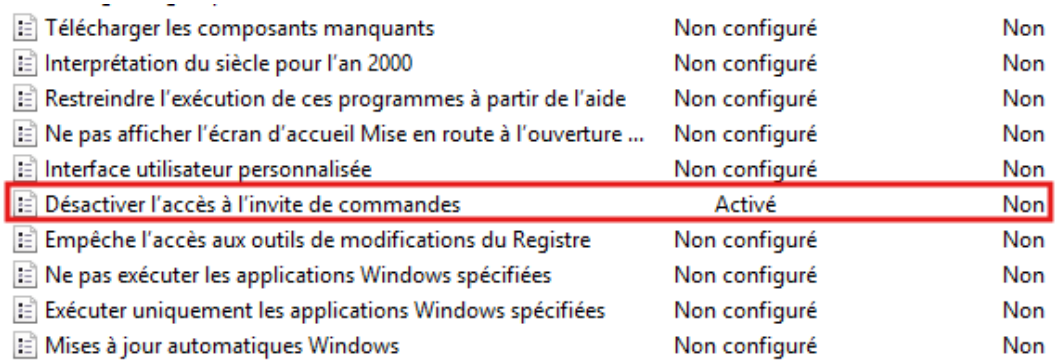


FIGURE 20 – Désactiver l'accès à l'invite de commandes

4.1.3 Blocage du panneau d'affichage :

— Chemin :
Configuration utilisateur > Modèles d'administration > Panneau de configuration > Affichage
— Stratégie activée :
Empêcher l'accès au panneau de configuration d'affichage → Activé

FIGURE 21 – Désactiver le panneau de configuration de l'affichage

4.1.4 Blocage du gestionnaire de tâches :

— Chemin :
Configuration utilisateur > Modèles d'administration > Système > Options Ctrl+Alt+Suppr
— Stratégie activée :
Supprimer le Gestionnaire des tâches → Activé

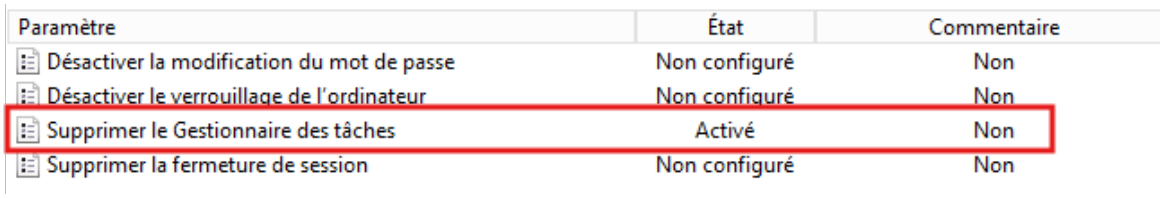


FIGURE 22 – Désactiver le gestionnaire de tâches

4.2 Application et vérification :

— Une mise à jour des stratégies est effectuée avec la commande :

```
sudo tail -f /var/log/auth.log
```

— Puis, un redémarrage des machines PC-ETUD1 et PC-ETUD2 est réalisé pour appliquer les restrictions.

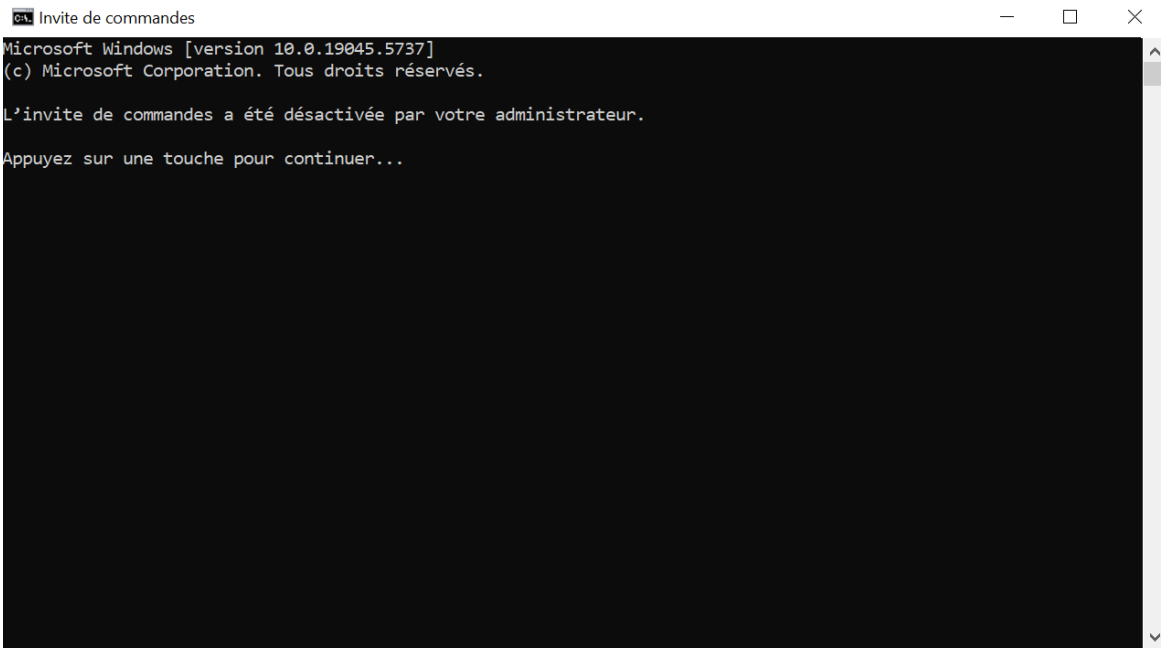


FIGURE 23 – Vérification du blocage de l'invite de commandes

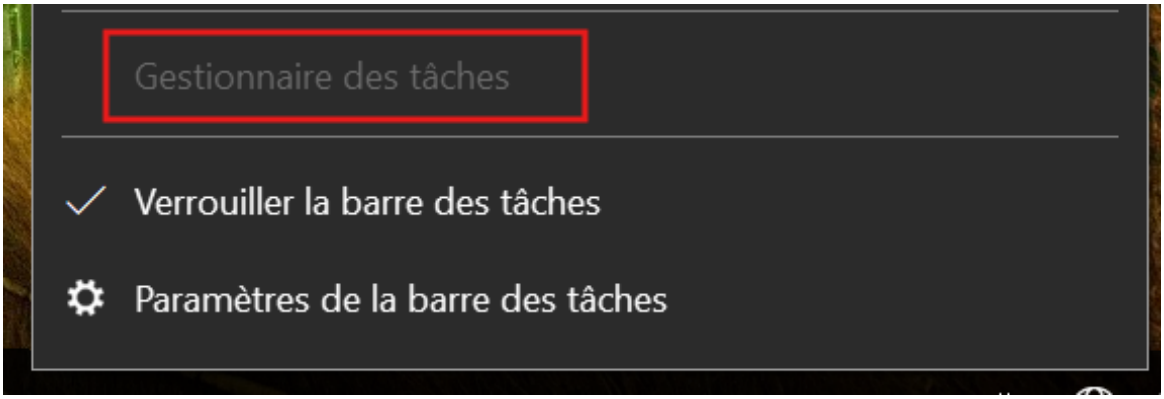


FIGURE 24 – Vérification du blocage du panneau d'affichage

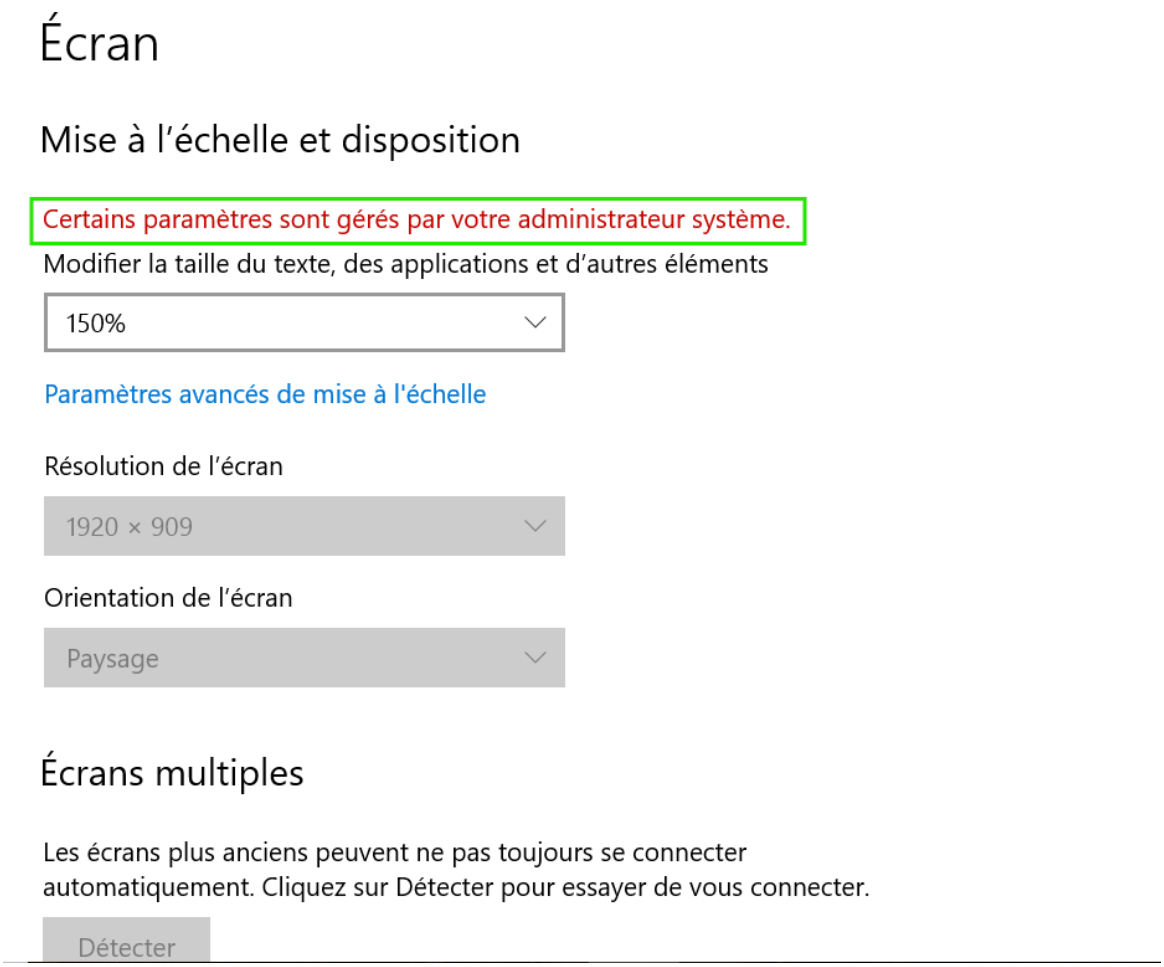


FIGURE 25 – Vérification du blocage du gestionnaire des tâches

5 Devoir II – Restriction Logicielle

— On crée une stratégie pour interdire l'exécution de programmes non autorisés.
— On teste l'application de cette stratégie.

Pour empêcher les étudiants d'exécuter des logiciels non autorisés, nous avons utilisé les stratégies de restriction logicielle (SRP) dans la GPO GPO_Securite_Etudiants :

5.1 Étapes de mise en œuvre

1. **Ouverture de la GPO :**
   Nous avons ouvert la stratégie via la console gpmc.msc, puis modifié GPO_Securite_Etudiants.
2. **Création de la stratégie SRP :**
   Dans le chemin suivant :
   Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de contrôle des applications > Stratégies de restriction logicielle
   Nous avons fait un clic droit sur **"Stratégies de restriction logicielle"** puis sélectionné **"Créer une nouvelle stratégie de restriction logicielle"** .
3. **Définir le comportement par défaut :**
   Dans les propriétés, nous avons choisi : **Niveau de sécurité par défaut : Interdire**
   Cela signifie que tout programme non autorisé sera bloqué.
4. **Ajout des règles d'autorisation :**
   Pour ne pas bloquer les programmes légitimes, nous avons ajouté deux règles d'autorisation par chemin :
   — `C:\Windows\*`
   — `C:\Program Files\*`

5.2 Application et vérification :

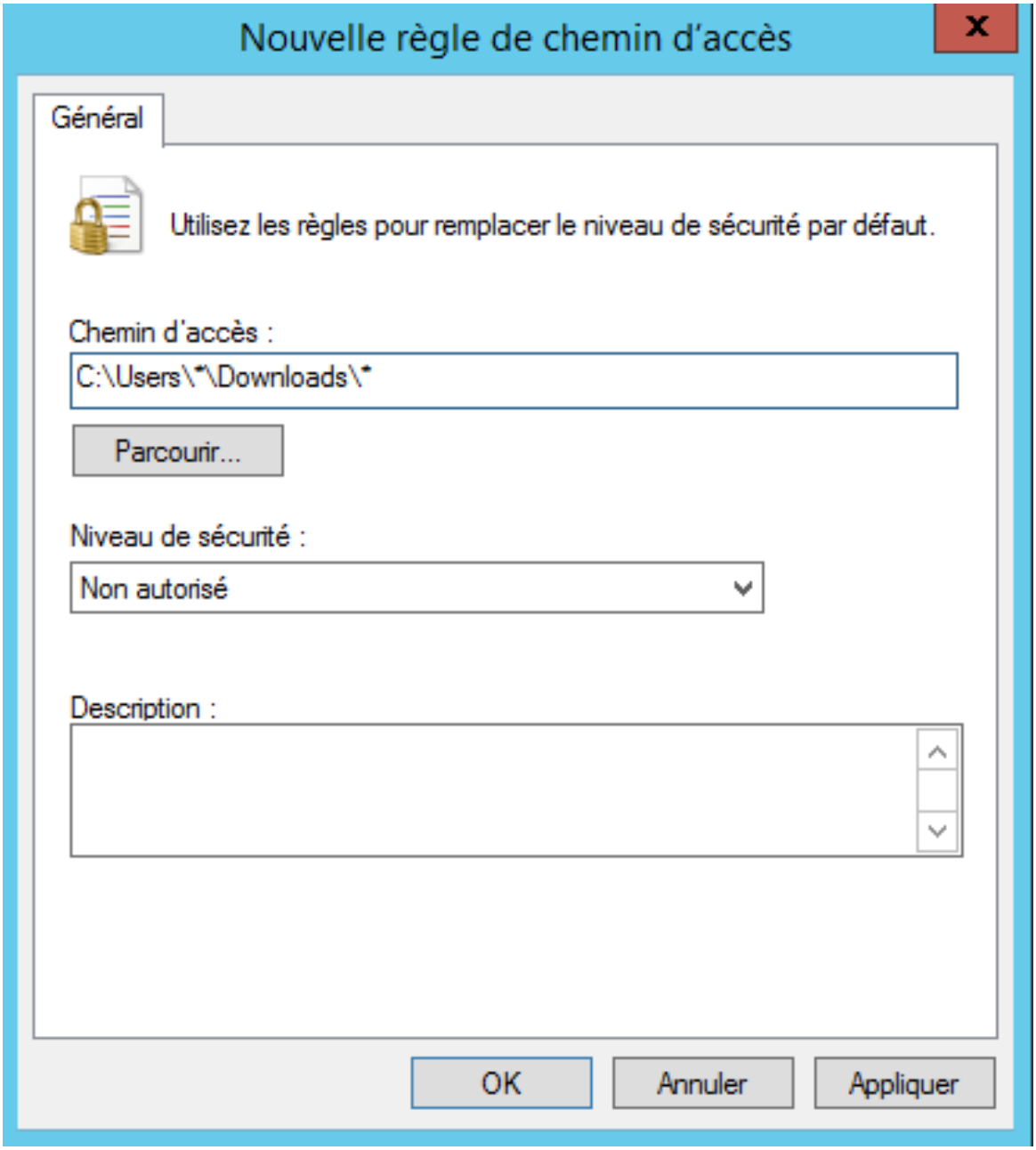


FIGURE 26 – Définir la règle de restriction 1

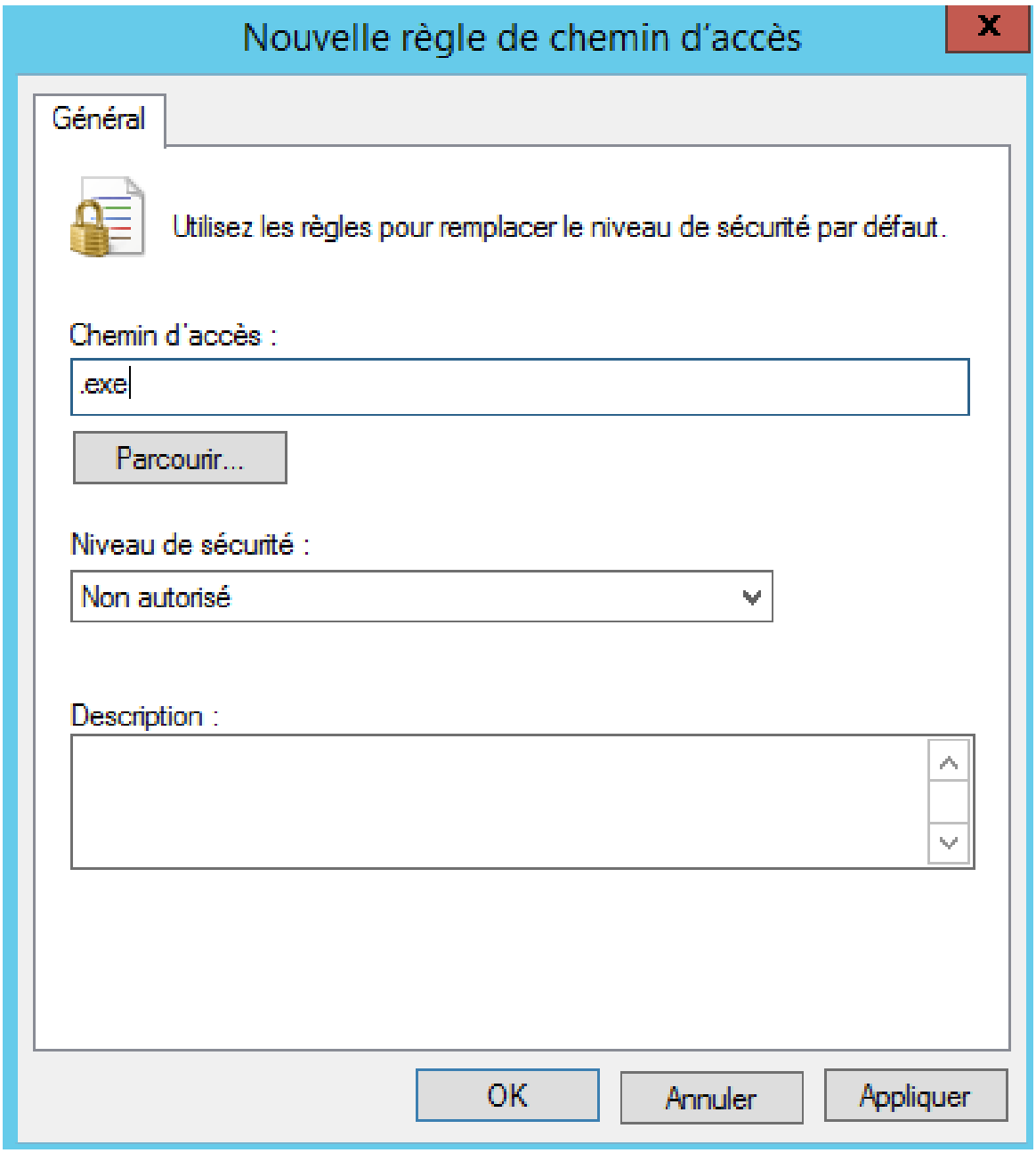


FIGURE 27 – Définir la règle de restriction 2

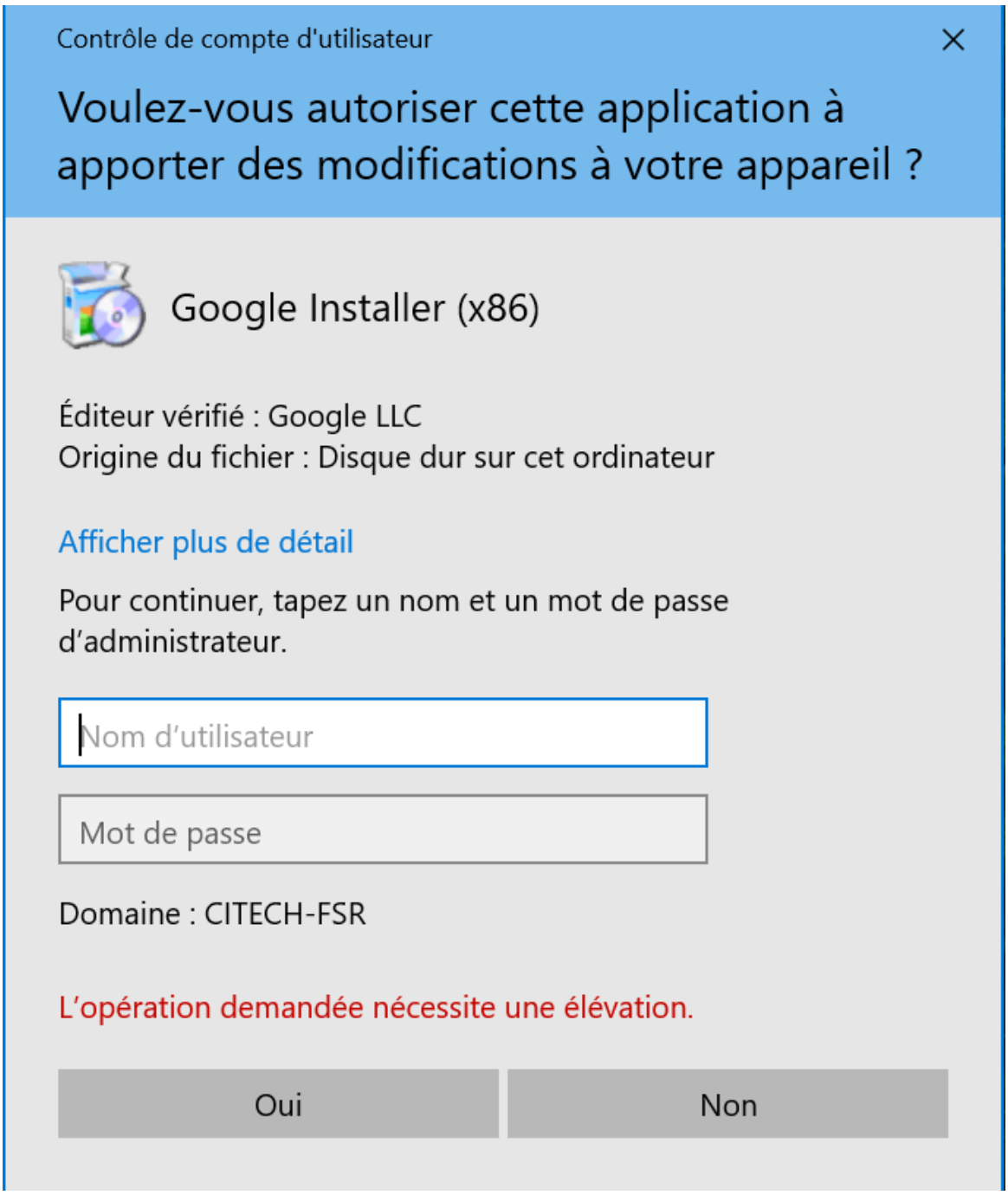
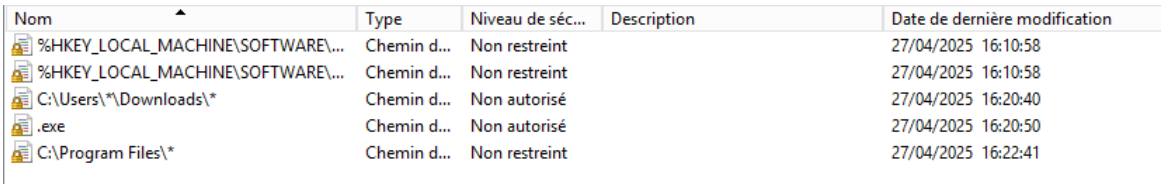


FIGURE 28 – Vérification des règles de restriction appliquées

Après application de la stratégie (gpupdate /force), nous avons tenté d'exécuter des .exe depuis des emplacements non autorisés comme Bureau ou Téléchargements. Le système a bloqué l'exécution, ce qui confirme l'efficacité de la politique.



Nom	Type	Niveau de séc...	Description	Date de dernière modification
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Chemin d...	Non restreint		27/04/2025 16:10:58
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Chemin d...	Non restreint		27/04/2025 16:10:58
C:\Users*\Downloads*	Chemin d...	Non autorisé		27/04/2025 16:20:40
.exe	Chemin d...	Non autorisé		27/04/2025 16:20:50
C:\Program Files*	Chemin d...	Non restreint		27/04/2025 16:22:41

FIGURE 29 – L'ensembles des règles appliquées

6 Conclusion

On a réussi à mettre en place un contrôleur de domaine, à intégrer des clients, à créer des utilisateurs et à appliquer des stratégies de groupe pour renforcer la sécurité du réseau.