

FACULTÉ DES SCIENCES DE RABAT

DÉPARTEMENT D'INFORMATIQUE

MASTER EN CYBERSÉCURITÉ INTELLIGENTE ET
TECHNOLOGIES ÉMERGENTES (CITECH)

Module : Administration et Sécurité de l'Active Directory

TP 1 : Mise en place et gestion d'Active Directory et des stratégies de groupe (GPO)

Réalisé par :
Maach Nada

Encadré par :
Mme Karima El Hachimi

Contents

1	Configuration	2
2	Exécution des commandes nslookup et ping	6
2.1	Windows 7	6
2.2	Windows 7 Externe	7
2.3	Windows 10	7
3	Ajout des machines PC-ETUD1 et PC-ETUD2 au domaine citech-fsr.local	8
4	Configuration via PowerShell	11
5	Création des OU et des comptes	12
6	Création et liaison d'une stratégie de groupe (GPO) de sécurité	14
7	Paramétrage des politiques de sécurité	15
8	Configuration du verrouillage automatique de session	16
9	Application des GPO et vérification	17
10	Devoir I	21
11	Devoir II	24

Chapter 1

Configuration

J'ai configuré les trois machines comme le montrent les captures suivantes :

Windows 7

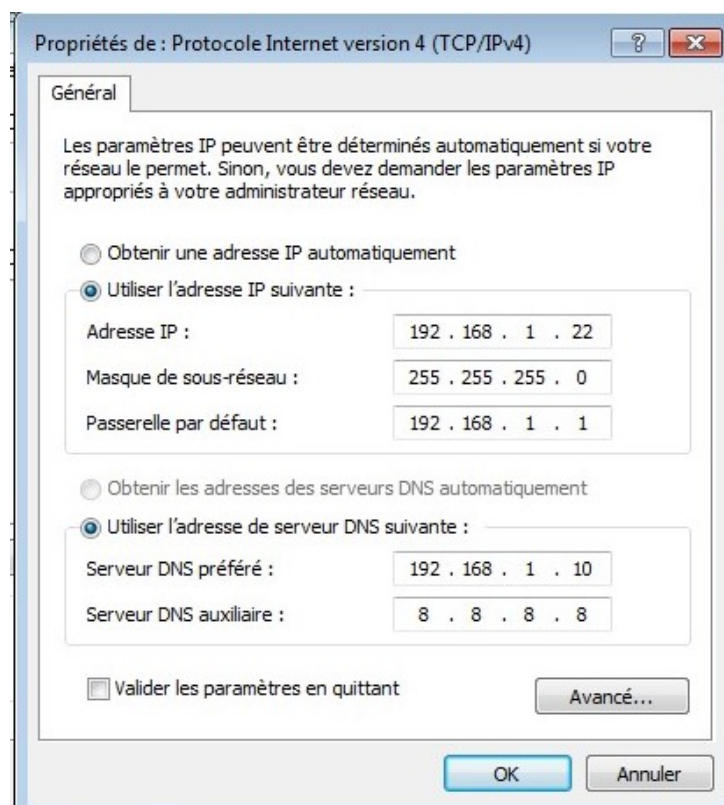


Figure 1.1: Configuration de Windows 7

Vérification de l'adresse IP :

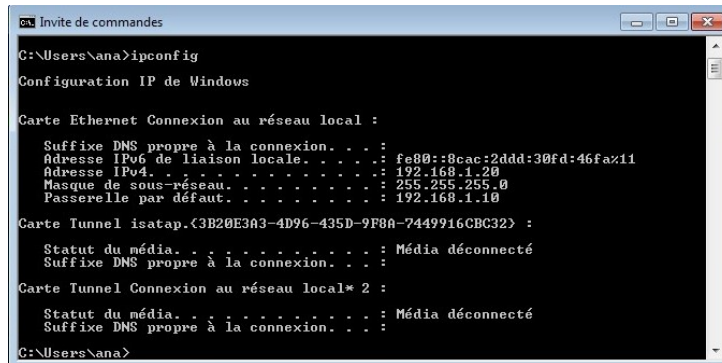


Figure 1.2: Vérification de l'adresse IP - Windows 7

Windows 7 (clone)

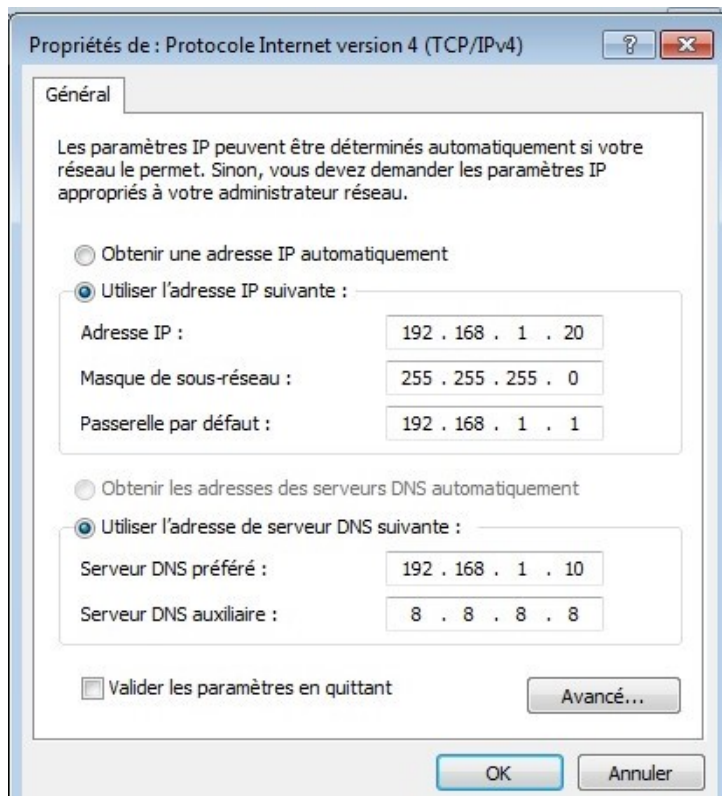


Figure 1.3: Configuration IP - Windows 7 clone

Windows 10

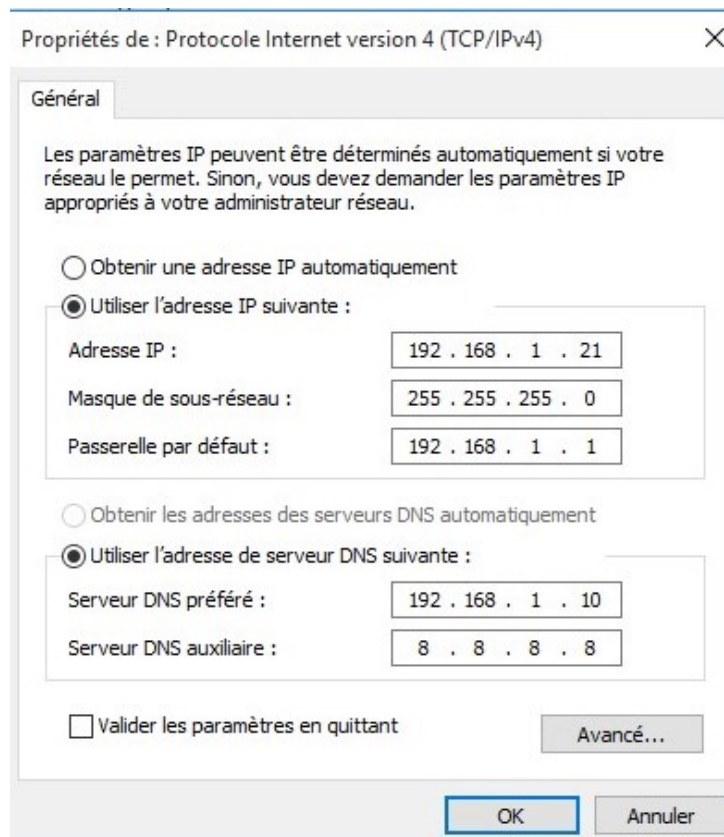


Figure 1.4: Configuration IP - Windows 10

Vérification de l'adresse IP :

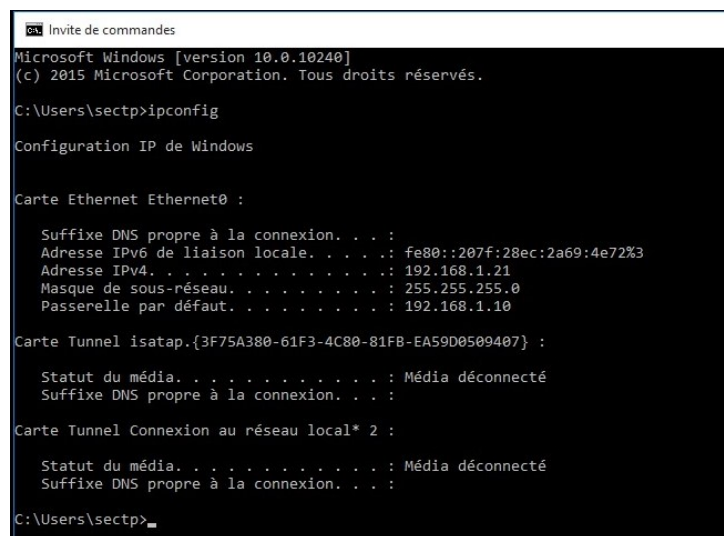
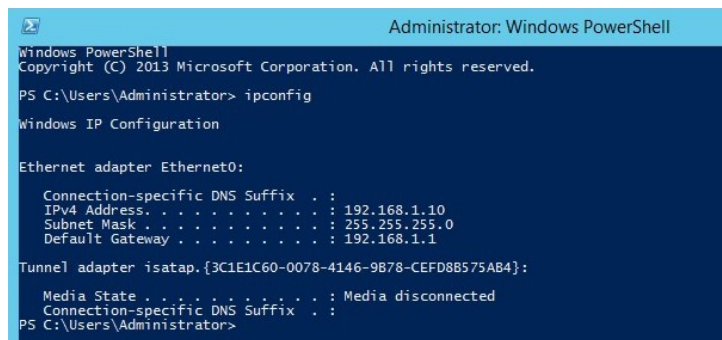


Figure 1.5: Vérification IP - Windows 10

Windows Server 2012



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{3C1E1C60-0078-4146-9B78-CEFD88575AB4}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
PS C:\Users\Administrator>
```

Figure 1.6: Capture du bureau de Windows Server 2012

Chapter 2

Exécution des commandes nslookup et ping

2.1 Windows 7

```
C:\Users\ana>nslookup citech-fsr.local
DNS request timed out.
    timeout was 2 seconds.
Serveur : UnKnown
Address: 192.168.1.10

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Le délai de la requête sur UnKnown est dépassé.
```

Figure 2.1: nslookup de Windows 7 vers le contrôleur de domaine

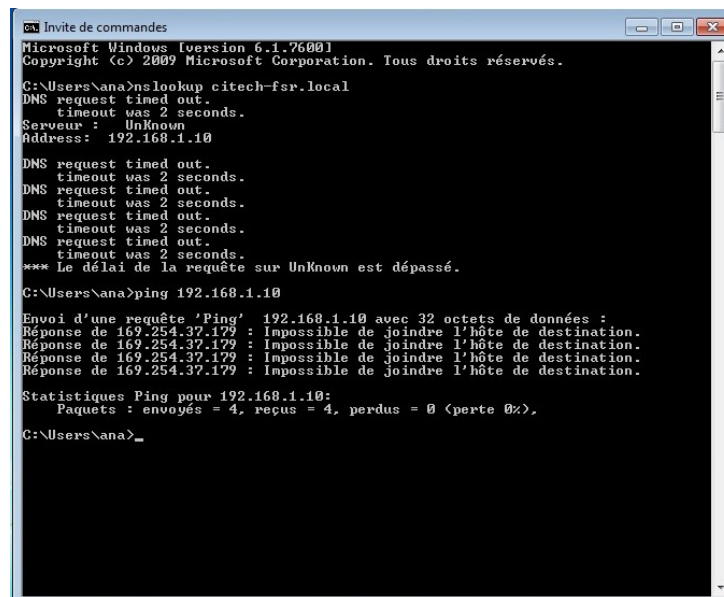
```
C:\Users\ana>ping 192.168.1.10

Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.22 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.22 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.22 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.22 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%).
```

Figure 2.2: ping de Windows 7 vers le contrôleur de domaine

2.2 Windows 7 Externe



```
Microsoft Windows [version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\ana>nslookup citech-fsr.local
DNS request timed out.
    timeout was 2 seconds.
Serveur : Unknown
Address: 192.168.1.10

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Le délai de la requête sur Unknown est dépassé.

C:\Users\ana>ping 192.168.1.10

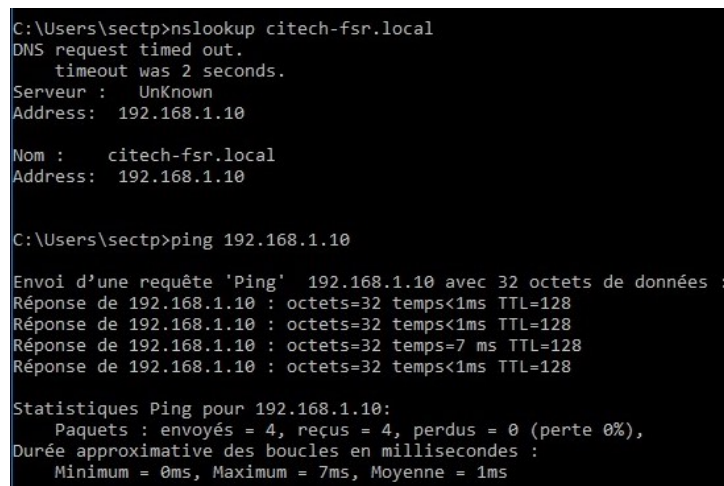
Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 169.254.37.179 : Impossible de joindre l'hôte de destination.
Réponse de 169.254.37.179 : Impossible de joindre l'hôte de destination.
Réponse de 169.254.37.179 : Impossible de joindre l'hôte de destination.
Réponse de 169.254.37.179 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

C:\Users\ana>
```

Figure 2.3: nslookup et ping du PC-Externe vers le contrôleur de domaine

2.3 Windows 10



```
C:\Users\sectp>nslookup citech-fsr.local
DNS request timed out.
    timeout was 2 seconds.
Serveur : Unknown
Address: 192.168.1.10

Nom : citech-fsr.local
Address: 192.168.1.10

C:\Users\sectp>ping 192.168.1.10

Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps=7 ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 7ms, Moyenne = 1ms
```

Figure 2.4: nslookup et ping de Windows 10 vers le contrôleur de domaine

Chapter 3

Ajout des machines PC-ETUD1 et PC-ETUD2 au domaine citech-fsr.local

PC-ETUD1 (Windows 10)

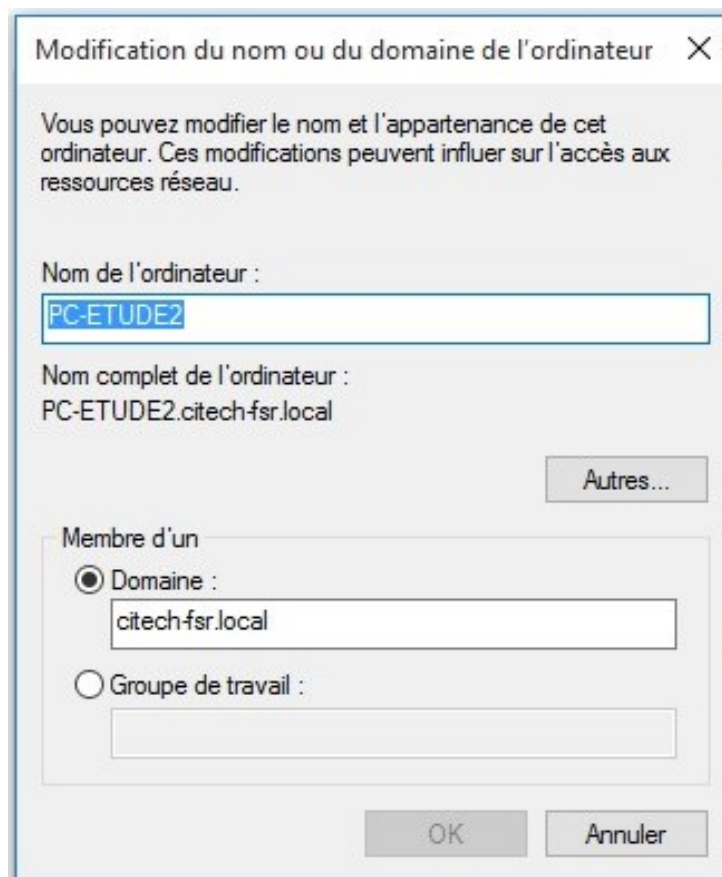


Figure 3.1: Ajout au domaine via Windows 10

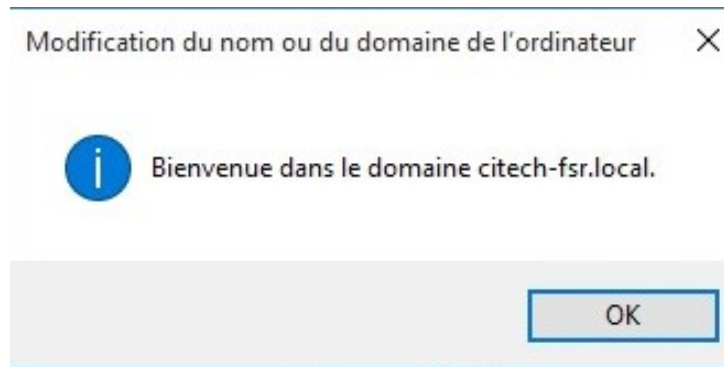


Figure 3.2: Ajout de Windows 10 au domaine citech-fsr.local

PC-ETUD2 (Windows 7)

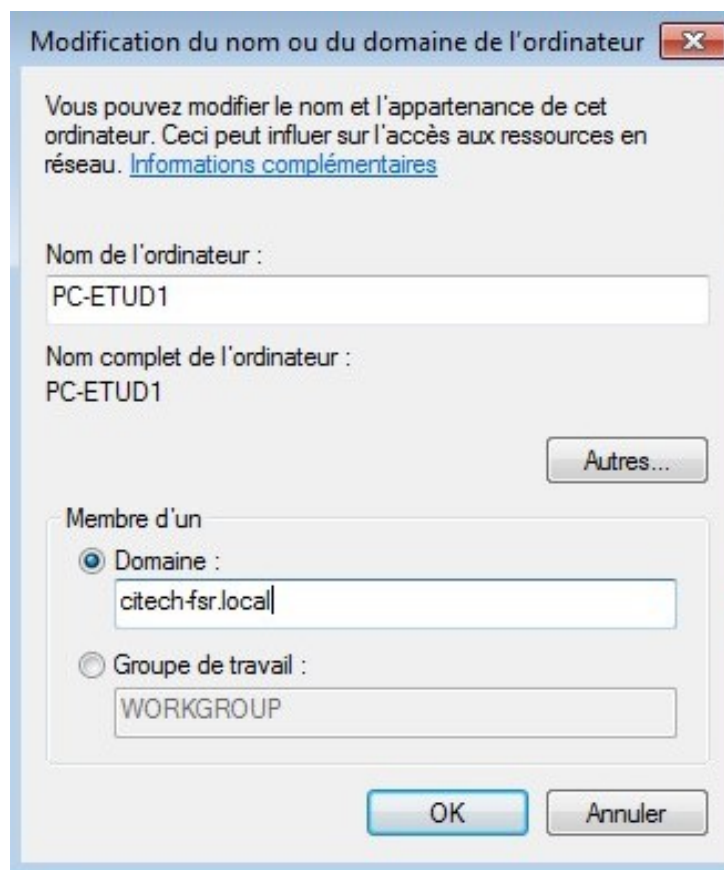


Figure 3.3: Ajout au domaine via Windows 7

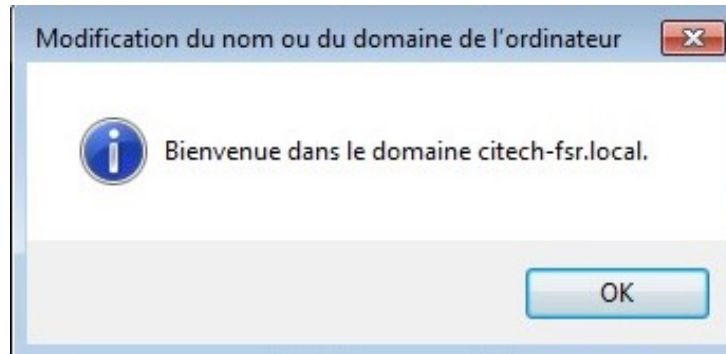


Figure 3.4: Ajout de Windows 7 au domaine citech-fsr.local

S'assurer que les domaines sont ajoute

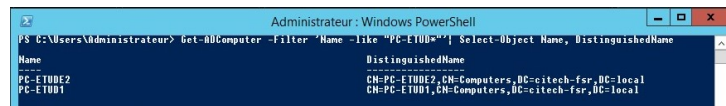


Figure 3.5:

Chapter 4

Configuration via PowerShell

PC-ETUD1 (Windows 10)

```
PS C:\Users\sectp> New-NetIPAddress -InterfaceAlias "Ethernet" `
>>> -IPAddress 192.168.1.21 -PrefixLength 24
>>> -DefaultGateway 192.168.1.1
>>>
PS C:\Users\sectp> Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses ("192.168.1.10")
```

Figure 4.1: Configuration IPv4 sur PC-ETUD1 (Windows 10)

Windows Server 2012

```
Administrateur: Windows PowerShell
PS C:\Users\Administrateur> New-NetIPAddress -InterfaceAlias "Ethernet" `
>>> -IPAddress 192.168.1.10 -PrefixLength 24
>>> -DefaultGateway 192.168.1.1
>>>
PS C:\Users\Administrateur> ipconfig
Configuration IP de Windows
```

Figure 4.2: Configuration IPv4 via PowerShell sur Windows Server 2012

```
PS C:\Users\Administrateur> Set-DnsClientServerAddress -InterfaceAlias "Ethernet" `
>>> ServerAddresses ("192.168.1.10", "8.8.8.8")
>>>
PS C:\Users\Administrateur>
```

Figure 4.3: Configuration DNS via PowerShell sur Windows Server 2012

Chapter 5

Création des OU et des comptes

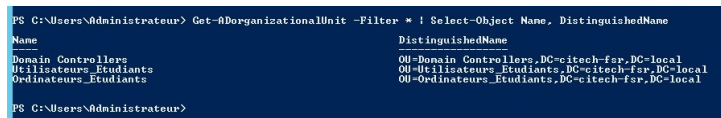
Création des OU

J'ai exécuté les deux commandes suivantes :

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

Pour m'assurer que les OU ont bien été créées, j'ai exécuté la commande suivante :

```
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

Figure 5.1: Vérification de la création des OU

Ensuite, j'ai initialisé la variable \$OUPath comme le montre la capture suivante :

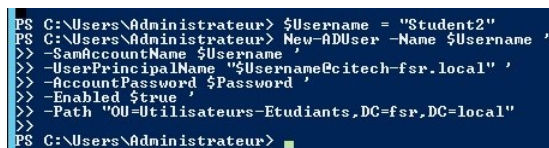


```
PS C:\Users\Administrateur> $OUPath = "OU=Ordinateurs_Etudiants,DC=citech-fsr,DC=local"
PS C:\Users\Administrateur>
```

Figure 5.2: Initialisation de la variable \$OUPath

Création des comptes utilisateurs

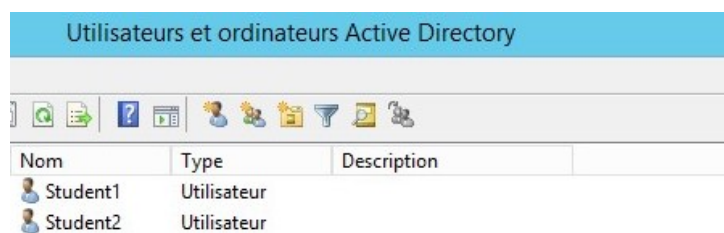
Comme le montre la capture d'écran suivante, j'ai créé deux comptes d'utilisateurs nommés Student1 et Student2 :



```
PS C:\Users\Administrateur> $Username = "Student2"
PS C:\Users\Administrateur> New-ADUser -Name $Username `
>> -SamAccountName $Username `
>> -UserPrincipalName "$Username@citech-fsr.local" `
>> -AccountPassword $Password `
>> -Enabled $true `
>> -Path "$OUPath"
PS C:\Users\Administrateur>
```

Figure 5.3: Création des utilisateurs via PowerShell

Pour m'assurer que les utilisateurs ont bien été créés, j'ai ouvert le Gestionnaire de serveur, puis cliqué sur *Outils* , *Utilisateurs et ordinateurs Active Directory*. Les nouveaux comptes sont bien présents, comme le montre la capture suivante :



The screenshot shows the 'Utilisateurs et ordinateurs Active Directory' (Active Directory Users and Computers) window. It features a toolbar with various icons for user management. Below the toolbar is a table listing the users in the directory.

Nom	Type	Description
Student1	Utilisateur	
Student2	Utilisateur	

Figure 5.4: Vérification de la création des utilisateurs

Chapter 6

Création et liaison d'une stratégie de groupe (GPO) de sécurité

La liaison d'une stratégie de groupe de sécurité a bien été réalisée, comme le montre la capture d'écran suivante :

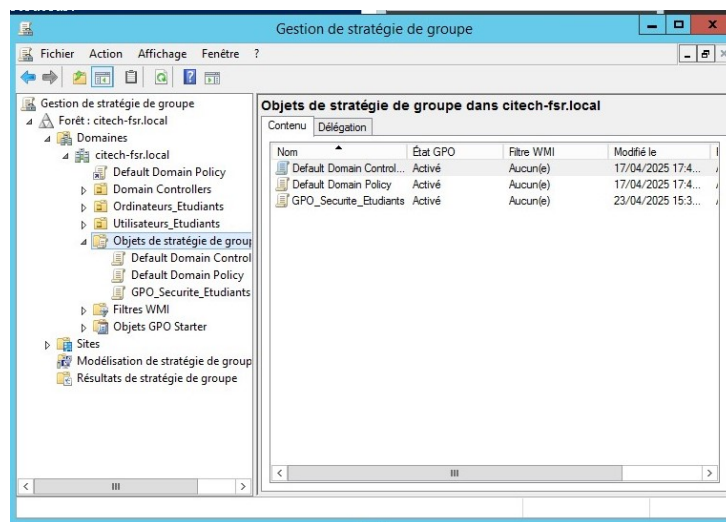


Figure 6.1: Création et liaison d'une GPO

Chapter 7

Paramétrage des politiques de sécurité

Le paramétrage de la GPO a été effectué comme illustré dans la capture suivante :

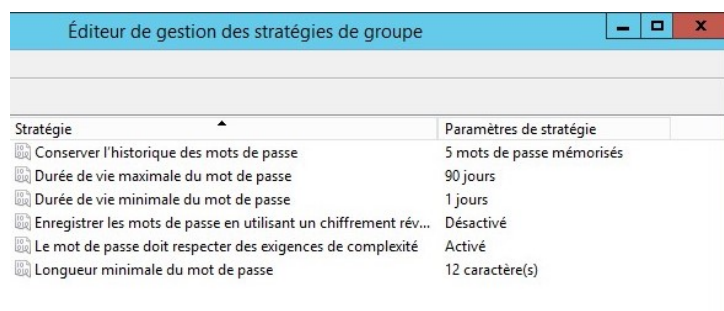


Figure 7.1: Configuration des paramètres de sécurité via GPO

Chapter 8

Configuration du verrouillage automatique de session

La configuration du verrouillage automatique de session a été appliquée.

Chapter 9

Application des GPO et vérification

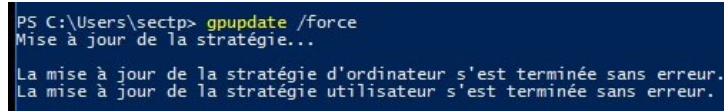
Nous avons vérifié l'application des GPO sur les deux utilisateurs :

ETUD1

Nous avons exécuté les commandes suivantes :

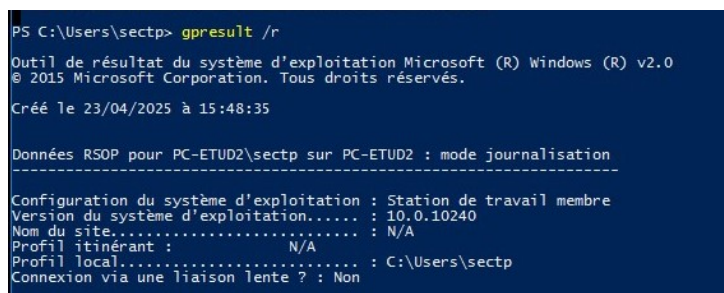
```
gpupdate /force  
gpresult /r
```

Comme le montre la capture suivante :



```
PS C:\Users\sectp> 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.
```

Figure 9.1: Exécution de gpupdate sur Windows 10



```
PS C:\Users\sectp> gpresult /r  
Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0  
© 2015 Microsoft Corporation. Tous droits réservés.  
Créé le 23/04/2025 à 15:48:35  
  
Données RSOP pour PC-ETUD2\sectp sur PC-ETUD2 : mode journalisation  
-----  
Configuration du système d'exploitation : Station de travail membre  
Version du système d'exploitation..... : 10.0.10240  
Nom du site..... : N/A  
Profil itinérant : N/A  
Profil local..... : C:\Users\sectp  
Connexion via une liaison lente ? : Non
```

Figure 9.2: Résultat de gpresult sur Windows 10

La nouvelle interface de connexion après application de la GPO :



Figure 9.3: Nouvelle interface de connexion (Windows 7)

ETUD2

Nous avons exécuté les mêmes commandes :

```
gpupdate /force  
gpresult /r
```

Comme le montre la capture suivante :

```
Windows PowerShell

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

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

PS C:\Users\ana> gpresult /r

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
Copyright (C) Microsoft Corp. 1981-2001
Jeu créé le 23/04/2025 à 13:47:00

Données RSOP pour PC-ETUDI\ana sur PC-ETUDI : mode journalisation

-----
Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 6.1.7600
Nom du site..... : N/A
Profil itinérant : N/A
Profil local..... : C:\Users\ana
Connexion via une liaison lente ? : Non

PARAMÈTRES UTILISATEURS
-----
Heure de la dernière application de la stratégie de groupe : 23/04/2025 à 13:46:09
Stratégie de groupe appliquée depuis : N/A
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : PC-ETUDI
Type de domaine : <Ordinateur local>

Objets Stratégie de groupe appliqués
-----
N/A
```

Figure 9.4: Exécution de gpupdate sur Windows 7

```
PS C:\Users\ana> gpresult /r

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
Copyright (C) Microsoft Corp. 1981-2001
Jeu créé le 23/04/2025 à 13:48:19

Données RSOP pour PC-ETUDI\ana sur PC-ETUDI : mode journalisation

-----
Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 6.1.7600
Nom du site..... : N/A
Profil itinérant : N/A
Profil local..... : C:\Users\ana
Connexion via une liaison lente ? : Non

PARAMÈTRES UTILISATEURS
-----
Heure de la dernière application de la stratégie de groupe : 23/04/2025 à 13:46:09
Stratégie de groupe appliquée depuis : N/A
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine : PC-ETUDI
Type de domaine : <Ordinateur local>

Objets Stratégie de groupe appliqués
-----
N/A
```

Figure 9.5: Résultat de gpresult sur Windows 7

Nouvelle interface de connexion (Windows 10) :

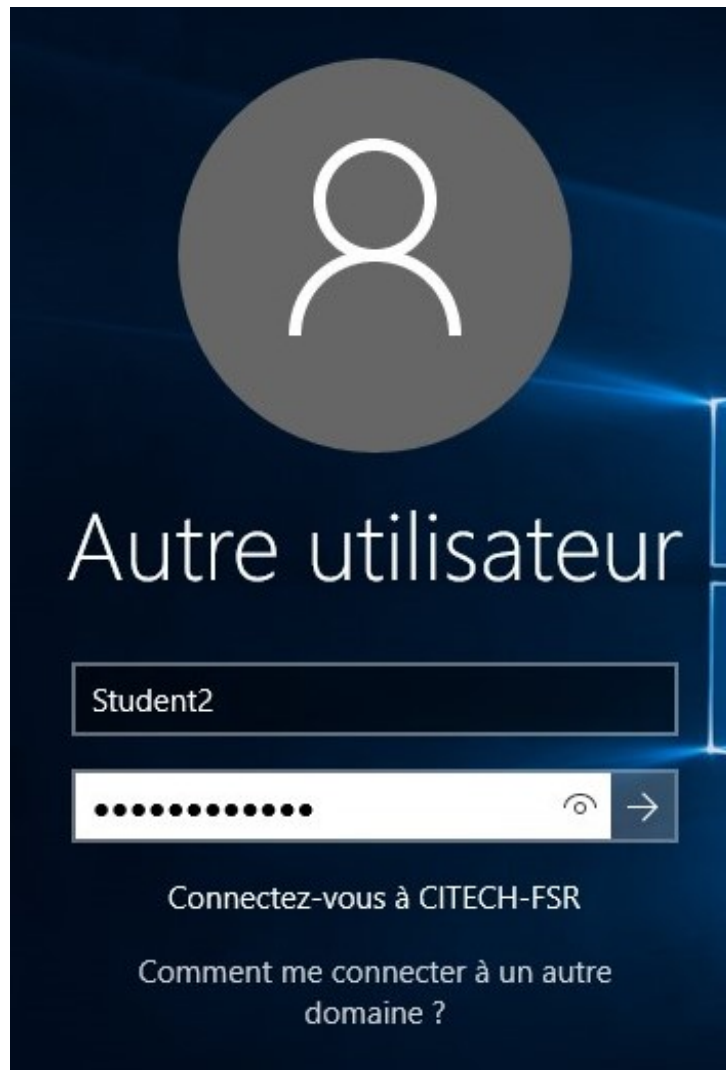


Figure 9.6: Interface de connexion après application de la GPO

Chapter 10

Devoir I

Désactivation du gestionnaire des tâches

Pour désactiver le gestionnaire des tâches pour Student1 et Student2, j'ai cliqué droit sur le GPO, puis sélectionné *Modifier > Configuration utilisateur > Stratégies > Modèles d'administration > Système > Options Ctrl+Alt+Suppr.*

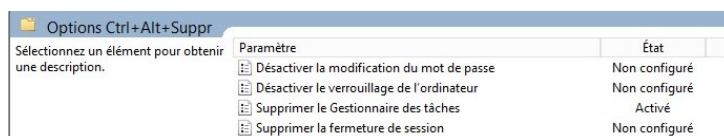


Figure 10.1: Désactivation du gestionnaire des tâches

Désactivation du panneau de configuration de l'affichage

Pour désactiver le panneau de configuration de l'affichage pour Student1 et Student2, j'ai cliqué droit sur le GPO, puis sélectionné *Modifier > Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration > Affichage.*

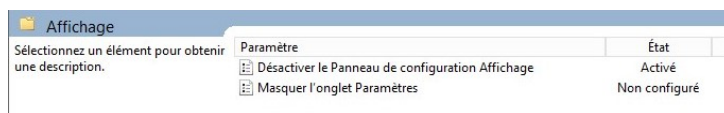


Figure 10.2: Désactivation du panneau d'affichage

Désactivation de l'accès à l'invite de commandes

Pour désactiver l'accès à l'invite de commandes pour Student1 et Student2, j'ai cliqué droit sur le GPO, puis sélectionné *Modifier > Configuration utilisateur > Stratégies > Modèles d'administration > Système.*

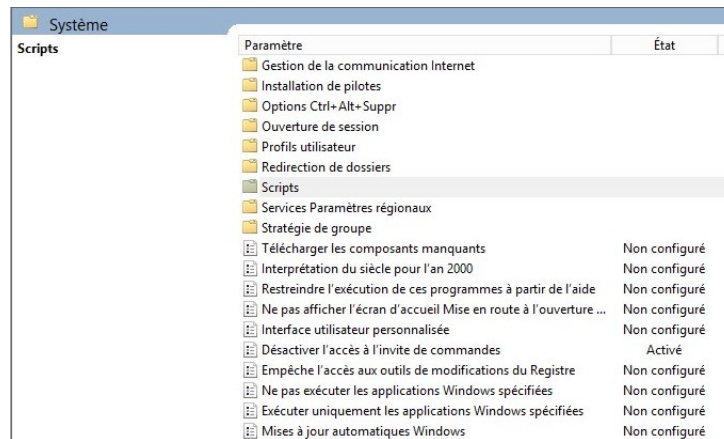


Figure 10.3: Désactivation de l'accès à l'invite de commandes

Vérification des résultats

- Vérifier que l'invite de commandes est bloquée : appuyer sur **Windows + R**, taper **cmd**, puis appuyer sur Entrée. L'invite de commande s'ouvre brièvement, puis se ferme immédiatement.

- Vérifier que le panneau d'affichage est inaccessible :

Essayer d'y accéder via : *Panneau de configuration > Apparence et personnalisation > Affichage*.

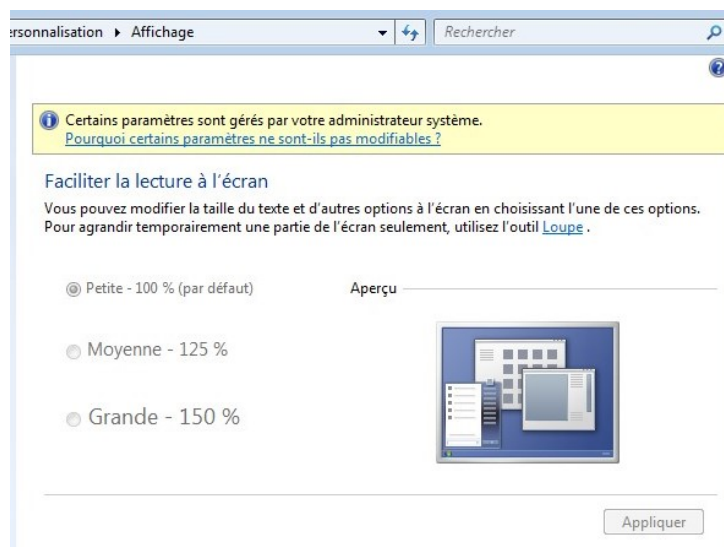


Figure 10.4: Affichage sous Windows 7

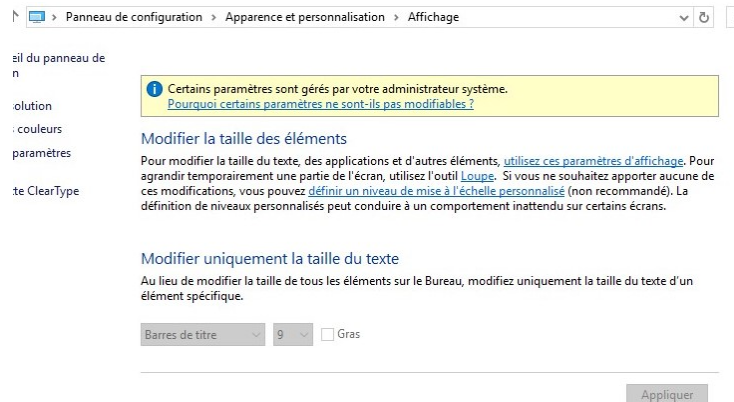


Figure 10.5: Affichage sous Windows 10

- En appuyant sur **Ctrl + Shift + Échap**, on vérifie que le gestionnaire des tâches ne s'ouvre pas.

Quelle est l'utilité de ces stratégies ?

Ces stratégies ont pour objectifs de :

- Sécuriser les postes utilisés par les étudiants.
- Limiter les abus, comme l'exécution de commandes système via l'invite de commande.
- Empêcher la modification de la configuration système (résolution, affichage, thèmes).
- Éviter l'arrêt de processus ou d'applications via le gestionnaire des tâches.
- Maintenir un environnement de travail stable et contrôlé, que ce soit dans un contexte éducatif ou professionnel.

Chapter 11

Devoir II

Configuration des restrictions logicielles

J'ai lié l'objet de stratégie de groupe **Ordinateur_Etudiant** avec le **GPO_Securite_Etudiants**, comme le montre la capture suivante :

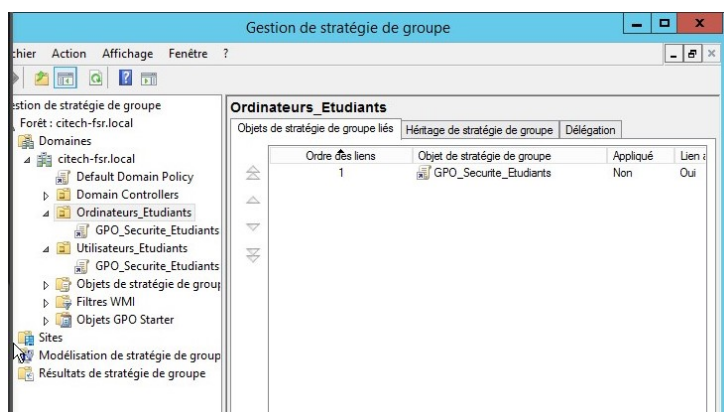


Figure 11.1: Création et liaison du GPO *GPO_Securite_Etudiants*

Un clic droit sur le GPO lié permet de le modifier.

Pour accéder aux stratégies de restriction logicielle, il faut suivre le chemin suivant :

Configuration de l'ordinateur → **Paramètres Windows** → **Paramètres de sécurité** → **Stratégies de contrôle des applications** → **AppLocker** → **Règles exécutables**

comme illustré ci-dessous :

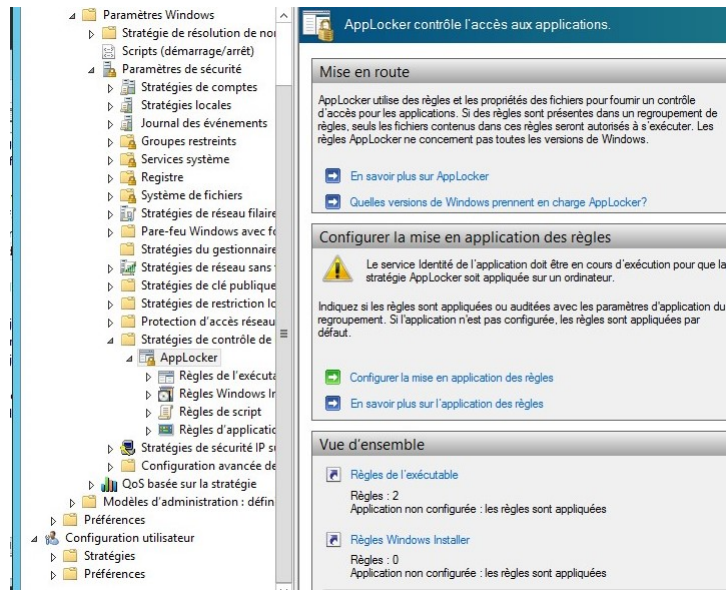


Figure 11.2: Accès aux règles exécutables dans AppLocker

Dans la section des règles exécutables, j'ai ajouté une règle qui interdit l'exécution de tout fichier **.exe** se trouvant dans le dossier **Téléchargements** de l'utilisateur. Cela permet de bloquer l'exécution de logiciels potentiellement malveillants téléchargés depuis Internet.

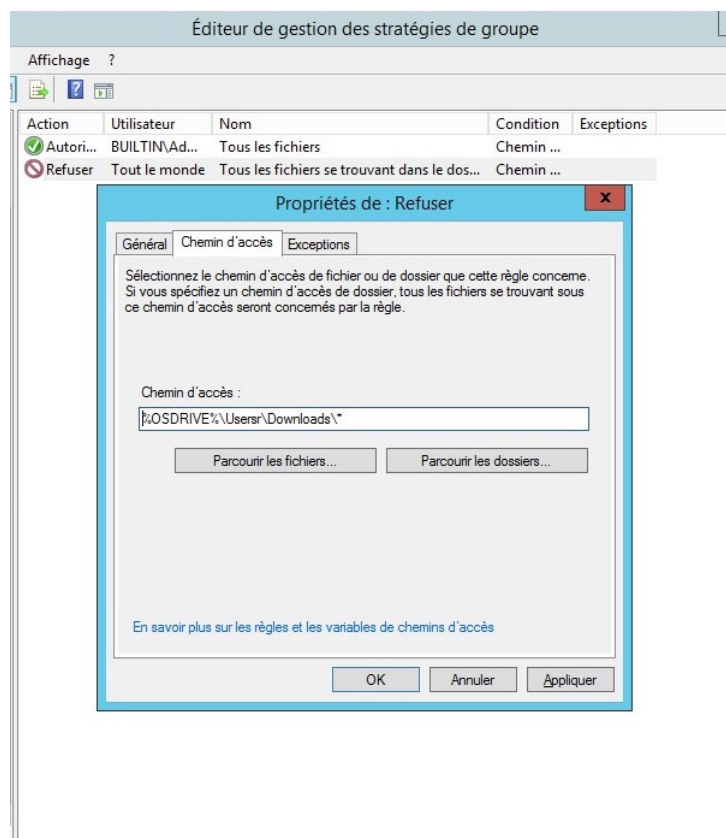


Figure 11.3: Blocage de l'exécution dans le dossier Downloads

Vérification

Étant donné que j'ai bloqué l'exécution des fichiers dans le chemin `Utilisateur\Downloads`, le fichier `notepad.exe`, copié dans ce dossier, ne peut pas être exécuté, même lorsque je double-clique dessus.

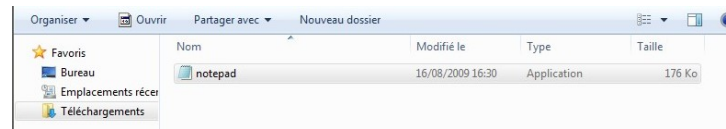


Figure 11.4: Blocage de l'exécution d'un fichier `.exe` placé dans Downloads