Master Cybersécurité Intelligente et Technologies Emergentes CITEch

Cours : Administation et sécurité de l'Active Directory

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

Université Mohammed V de Rabat
Faculté des sciences de Rabat

Pr. Ghizlane ORHANOU
Mme Karima EL HACHIMI

2024/2025

Compétences visées

— Créer et configurer un serveur ADDS ;
— Créer un domaine ;
— Configurer les clients pour rejoindre le domaine ;
— Créer et configurer une stratégie de groupe ;
— Définir des stratégies de sécurité à travers les GPO.

Conditions de réalisation

— VMWare Player installé

Critères de réussite

— Réaliser le même environnement du travail décrit dans l'énoncé

Consignes

Le compte-rendu du TP doit être rendu une semaine après la séance du TP en format en format électronique dans la classroom.

Introduction

Ce TP propose une création d'un contrôleur de domaine (DC) qui va permettre de créer des stratégies de groupe. Une stratégie de groupe ou GPO (Group Policies Object) permet de configurer certains paramètres ou restrictions d'utilisation de windows, pour un groupe de postes, soit pour un utilisateur, soit pour l'ordinateur.

Pour ce faire, nous allons besoin :

— Trois utilisateurs : deux clients Windows 7 et un client Windows 10.
— Un serveur windows (Windows server 2012) avec le rôle ADDS(active directory domain server).

1 Déroulement du TP

Durant ce TP nous allons travailler avec des machines virtuelles. Chaque étudiant devra avoir au niveau de son ordinateur 3 machines virtuelles :

Machine	Version	Adresse IP	Nom de l'hôte
Controleur de domaine	Windows Server 2008/2012	192.168.1.10	DC-ETUD
PC-ETUD1	Windows 7	192.168.1.20	PC-ETUD1
PC-ETUD2	Windows 10	192.168.1.21	PC-ETUD2
PC-Externe	Windows 7	192.168.1.22	PC-Externe

TABLEAU 1 – Machines virtuelles de l'environnement

Le serveur doit avoir une adresse IP fixe afin d'être toujours accessible, car il sera configuré comme DNS primaire sur les clients.

2 Le Schéma

Durant ce TP, nous allons recréer la représentation du contrôleur de domaine et l'architecture de l'environnement suivant :

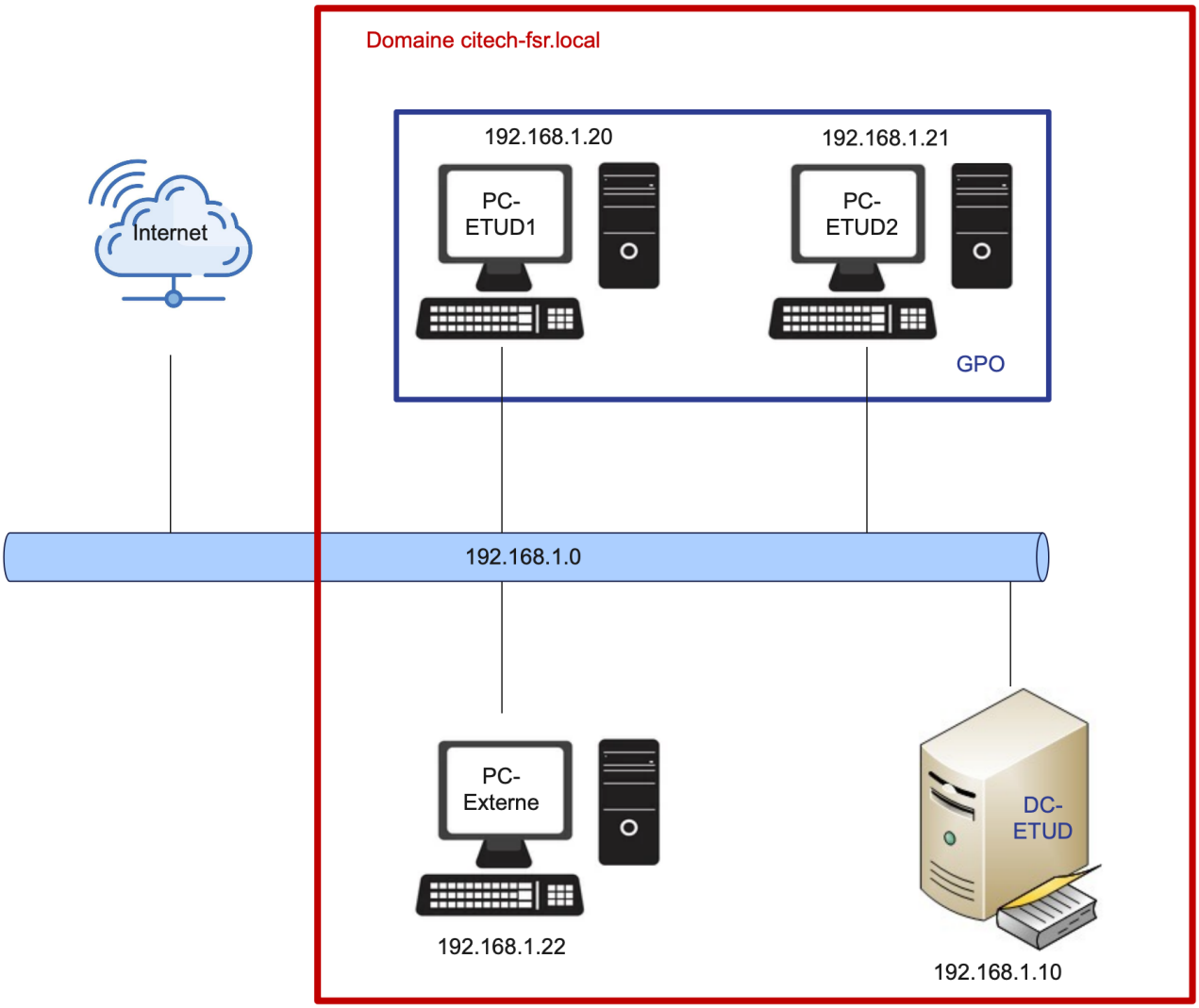

FIGURE 1 – Architecture de l'environnement Windows du TP

3 Création et configuration du contôleur de domaine et les clients

Dans le cadre de la mise en place de notre infrastructure, nous déployons deux postes clients sous Windows 7, un poste client sous Windows 10, ainsi qu'un serveur fonctionnant sous Windows Server 2012. Chaque machine, y compris le serveur, est renommée conformément à la convention de nommage définie, et se voit attribuer une adresse IP statique.

L'adressage IP constitue une étape cruciale, car l'ensemble des équipements doit appartenir au même sous-réseau afin de permettre au serveur d'assumer correctement son rôle de contrôleur de domaine.

3.1 Création de domaine

Pour créer le domaine racine "citech-fsr.local", il suffit d'ouvrir le Gestionnaire de serveur. Dans l'assistant de configuration, choisissez "Ajouter une nouvelle forêt". Dans le champ "Nom du domaine racine", saisissez "citech-fsr.local". Cliquez sur Suivant à chaque étape et à la fin, cliquez sur Installer.

Une fois le domaine "citech-fsr.local" créé, le serveur redémarrera automatiquement.

Le serveur est désormais le contrôleur de domaine du domaine citech-fsr.local.

3.2 Configuration de l'Active Directory

Après création du domaine "citech-fsr.local". L'illustration ci-dessous présente la configuration IP attribuée au serveur et aux différents clients Windows.

3.2.1 Via l'interface graphique (GUI)

a) Conrôleur de domaine :
Connectez-vous à votre machine virtuelle Windows Server. Puis, cliquez sur **Démarrer** > **Panneau de configuration** > **Réseau et Internet** > **Centre Réseau et partage**.

Ensuite, cliquez sur **"Modifier les paramètres de la carte"** dans le menu de gauche. Faites un clic droit sur la carte réseau **"Ethernet 0"**, puis sélectionnez **Propriétés**. Double-cliquez ensuite sur **Protocole Internet version 4 (TCP/IPv4)**.

Cochez **Utiliser l'adresse IP suivante**, puis renseignez les champs suivants :

- Adresse IP : 192.168.1.10
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 192.168.1.1
- Serveurs DNS : 192.168.1.10 (lui-même)
- Serveur DNS secondaire : 8.8.8.8

Cliquez sur **OK**, puis Fermer. Ensuite, vérifiez avec la commande `ipconfig` que l'adresse IP a bien été configurée.

b) Clients Windows De même, pour les clients Windows, nous utilisons la même méthode que pour le serveur, avec la configuration suivante :

i) PC-ETUD1 Windows 7 :

- Adresse IP : 192.168.1.20
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 192.168.1.1
- Serveurs DNS : 192.168.1.10 (l'adresse d'ADDS)
- Serveur DNS secondaire : 8.8.8.8

ii) PC-ETUD2 Windows 10 :

- Adresse IP : 192.168.1.21
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 192.168.1.1
- Serveurs DNS : 192.168.1.10 (l'adresse d'ADDS)

— Serveur DNS secondaire : 8.8.8.8

i) PC-Externe Windows 7 :

— Adresse IP : 192.168.1.22
— Masque de sous-réseau : 255.255.255.0
— Passerelle par défaut : 192.168.1.1
— Serveurs DNS : 192.168.1.10 (l'adresse d'ADDS)
— Serveur DNS secondaire : 8.8.8.8

Vérifiez la connectivité entre les trois clients et le contrôleur de domaine en utilisant les commandes suivantes :

— `nslookup citech-fsr.local` pour la résolution DNS ;
— `ping 192.168.1.10` pour tester la connectivité réseau avec l'AD

Il suffit maintenant d'ajouter les deux machines PC-ETUD1 et PC-ETUD2 au domaine "citech-fsr.local" de l'Active Directory. Pour se faire :

i) Effectuez un clic droit sur "Ordinateur" (ou "Ce PC" selon la version de Windows), puis clique sur "Propriétés".
ii) Dans la fenêtre ouverte, cliquez sur "Modifier les paramètres" situés à droite du nom de l'ordinateur.
iii) Dans l'onglet "Nom de l'ordinateur", cliquez sur le bouton "Modifier les paramètres".
iv) Dans la section "Membre de", sélectionnez "Domaine".
v) Saisissez le nom du domaine "citech-fsr.local", puis clique sur "OK".
vi) Un écran s'affiche pour l'authentification : entrez les identifiants du compte administrateur (utilisateur : Administrateur, mot de passe : admin-2025).
vii) Si les informations sont correctes, un message de bienvenue dans le domaine "citech-fsr.local" s'affichera.
viii) Cliquez sur "OK" pour fermer les fenêtres.
ix) Redémarrez la machine pour appliquer les changements.

Il est à noter qu'il faut modifier les noms des machines avec PC-ETUD1 et PC-ETUD2 à cette étape.
Au niveau du contrôleur de domaine localiser les deux machines avec la commande suivante sur Powershell :

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

Les postes client sont désormais membre du domaine Active Directory citech-fsr.local.

3.2.2 Via PowerShell

a) Conrôleur de domaine :
Configuration de l'adresse IPv4 :

```
New-NetIPAddress -InterfaceAlias "Ethernet" ‘
          -IPAddress 192.168.1.10 -PrefixLength 24 ‘
          -DefaultGateway 192.168.1.1
```

Configuration du DNS :

```
NSet-DnsClientServerAddress -InterfaceAlias "Ethernet" ‘
         -ServerAddresses ("192.168.1.10", "8.8.8.8")
```

b) Clients Windows :

i) PC-ETUD1 Windows 7 :

```
New-NetIPAddress -InterfaceAlias "Ethernet" ‘
          -IPAddress 192.168.1.20 -PrefixLength 24 ‘
          -DefaultGateway 192.168.1.1

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses ("192.168.1.10")
```

ii) PC-ETUD2 Windows 10 :

```
New-NetIPAddress -InterfaceAlias "Ethernet" ‘
          -IPAddress 192.168.1.21 -PrefixLength 24 ‘
          -DefaultGateway 192.168.1.1

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses ("192.168.1.10")
```

iii) PC-Externe Windows 7 :

```
New-NetIPAddress -InterfaceAlias "Ethernet" ‘
          -IPAddress 192.168.1.22 -PrefixLength 24 ‘
          -DefaultGateway 192.168.1.1

Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses ("192.168.1.10")
```

4 Création des OU et des comptes

4.1 Creation des OU

Dans un premier temps créer une OU "Utilisateurs_Etudiants" et "Ordinateurs_Etudiants". Pour se faire, il suffit d'ouvrir PowerShell en tant qu'administrateur et d'executer les commandes suivantes :

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

Vérifiez les OUs crées avec la commande Powershell suivante :

```
Get-ADOrganizationalUnit -Filter * | Select-Object Name, DistinguishedName
```

Finalement, déplacemez les deux machines clientes dans l'OU "Ordinateurs_Etudiants".

```
$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
```

4.2 Creation des utilisateurs

Ensuite, ajoutez deux comptes de test "Student1" et "Student2" dans l'OU Utilisateurs_Etudiants via PowerShell, en utilisant les commandes suivantes :

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

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

Il suffit de remplacer "username" avec "Student1" et après "Student2" pour créer les deux comptes.

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

Dans cette étape, nous allons créer une stratégie de groupe GPO_Securité_Etudiants dédiée à la sécurité des comptes étudiants, puis la lier à l’OU Utilisateurs_Etudiants. Pour ce faire, Ouvrez la Console de gestion des stratégies de groupe en exécutant la commande suivante :

```
gpmc.msc
```

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

Une fois la GPO créée, effectuez un clic droit sur l’OU “Utilisateurs_Etudiants”, puis sélectionnez “Lier un GPO existant”. Dans la liste des GPO, sélectionnez GPO_Securite_Etudiants, puis clique sur **OK**. La stratégie de groupe GPO_Securite_Etudiants est désormais liée à l’OU Utilisateurs_Etudiants, prête à être configurée pour appliquer des règles de sécurité.

6 Paramétrage des politiques de sécurité

À cette étape, nous allons configurer les stratégies de sécurité à l’aide de la GPO précédemment créée.

6.1 Politique de mot de passe sécurisé

Pour configurer la politique de sécurité des mots de passe, il suffit de suivre le chemin : **Configuration ordinateur** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies de compte** > **Stratégie de mot de passe**. Ensuite, modifier les paramètres avec la configuration ci-dessous :

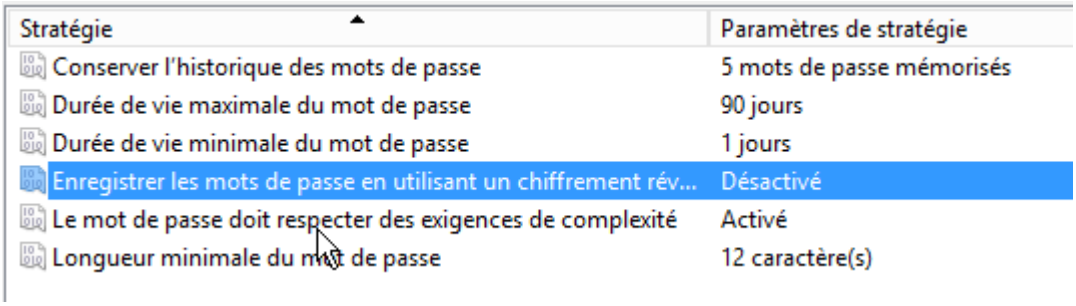

Figure 2 – Politique de sécurité des mots de passe

6.2 Verrouillage automatique de session

Durant cette étape, nous allons configurer le Verrouillage automatique de la session utilisateur après 10 minutes d’inactivité.

Dans **Configuration utilisateur > Modèles d'administration > Panneau de configuration > Personnalisation**, configurez l'écran de veille avec mot de passe comme ci-dessous :

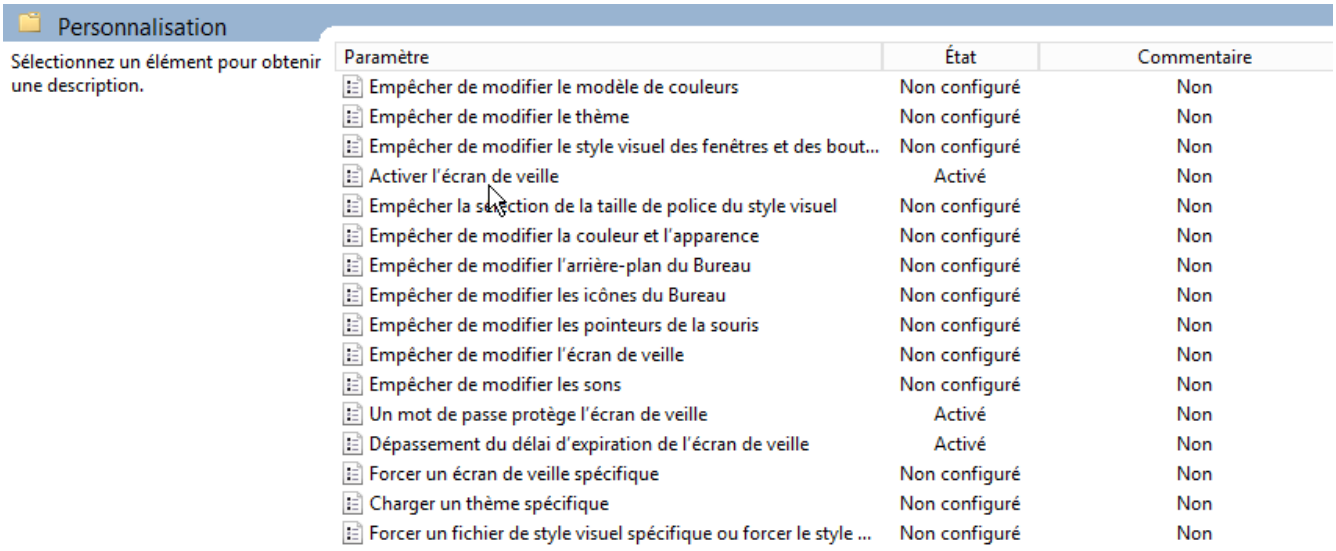

FIGURE 3 – Verrouillage de session

Il est à noter qu'il faut définir un délai de 600 secondes avant l'activation de l'écran de veille.

6.3 Application des GPO et vérification

Pour appliquer et vérifier les GPOs mises en place, il suffit d'utiliser la commande suivante sur le client :

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

Après l'application de la GPO, redémarrez le client. Ensuite, connectez-vous depuis l'utilisateur affecté par la GPO (Student1 et Student2).

- Essayez de saisir un mot de passe erroné, qu'est-ce que vous remarquez ?
- Après application de la GPO, essayer de modifier le mots de passe avec un moins sécurisé. Qu'est-ce que vous remarquez ?

Conclusion

En conclusion, le déploiement du rôle Active Directory Domain Services (AD DS) nous a permis de mettre en place un domaine centralisé, au sein duquel tout utilisateur inscrit dans l'annuaire peut se connecter depuis n'importe quel poste appartenant au domaine.

Grâce à la gestion des stratégies de groupe (GPO), il est possible d'appliquer des configurations spécifiques à des groupes ou à des utilisateurs, afin de restreindre ou d'optimiser leur environnement de travail. Ces stratégies permettent également, entre autres, de déployer automatiquement des logiciels à l'ouverture de session.

L'un des principaux avantages d'Active Directory, notamment en entreprise, réside dans la capacité à authentifier les utilisateurs de manière centralisée : un utilisateur peut ainsi accéder à sa session depuis n'importe quelle machine du domaine, en utilisant ses identifiants enregistrés dans l'annuaire.

Devoir I

L'administrateur souhaite sécuriser les postes utilisés par les étudiants en limitant l'accès à certains outils du système. Configurez les stratégies suivantes dans la GPO GPO_Securite_Etudiants :

- Désactiver l'accès à l'invite de commandes
- Désactiver le panneau de configuration de l'affichage
- Désactiver le gestionnaire de tâches

Après l'application de la GPO, redémarrez le client. Ensuite, connectez-vous depuis l'utilisateur affecté par la GPO Student2 et vérifiez si :

- L'invite de commandes est bloquée
- Le panneau d'affichage est inaccessible
- Le gestionnaire de tâches est désactivé

Quelle est l'utilité de ces stratégies ?

Devoir II

Dans le but de renforcer la sécurité des postes utilisés par les étudiants, l'administrateur souhaite empêcher l'exécution de logiciels potentiellement malveillants. Pour ce faire, configurez les stratégies adéquates au sein de la GPO nommée GPO_Securite_Etudiants, en vous appuyant sur les mécanismes de restriction logicielle ou de contrôle d'application. Enfin, procédez à la vérification de l'application effective de cette stratégie sur les postes ciblés.