TP 12
Renforcement de la sécurité des serveurs

Objectif :

- configurer des stratégies AppLocker ;
- configurer le Pare-feu Windows.

Besoins :

Pour réaliser ce TP on aura besoin de trois machines :

- Une machine Windows 2012 server **DC1** qui va jouer le rôle du contrôleur de domaine et du serveur DNS
- Deux machines : **CL1 :** cliente Windows 7 et **SRV1** : serveur membre 2012.

Exercice 1: Configuration des stratégies AppLocker

Votre responsable vous a chargé de configurer de nouvelles stratégies AppLocker pour contrôler l'utilisation des applications sur les postes de travail des utilisateurs. La nouvelle configuration doit autoriser l'exécution des programmes uniquement à partir d'emplacements approuvés. Tous les utilisateurs doivent être en mesure d'exécuter les applications à partir des répertoires C:\Windows et C:\Program Files.

Tâche 1 : Créer une unité d'organisation pour les ordinateurs clients

1. Basculez vers **DC1**.
2. Ouvrez **Utilisateurs et ordinateurs Active Directory**.
3. Créez une nouvelle unité d'organisation appelée **Unité d'organisation Ordinateurs clients**.
4. Placez **CL1** dans **Unité d'organisation Ordinateurs clients**.

Tâche 2 : Créer un objet GPO de contrôle de logiciels et le lier à l'unité d'organisation Ordinateurs clients

1. Sur DC1, ouvrez la console **GPMC**.
2. Dans la console GPMC, dans le conteneur **Objets de stratégie de groupe**, créez un nouvel objet de stratégie de groupe nommé **Objet GPO Contrôle de logiciels**.

3. Modifiez l'objet GPO Contrôle de logiciels.

4. Dans la fenêtre de l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur/Stratégies/Paramètres Windows/Paramètres de sécurité/Stratégies de contrôle de l'application/AppLocker**.

5. Créez les règles par défaut pour les éléments suivants :

o **Règles de l'exécutable**

o **Règles Windows Installer**

o **Règles de script**

o **Règles d'applications empaquetées**

6. Configurez l'application des règles avec l'option **Auditer uniquement** pour les éléments suivants :

o **Règles de l'exécutable**

o **Règles Windows Installer**

o **Règles de script**

o **Règles d'applications empaquetées**

7. Dans l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\ Paramètres Windows\Paramètres de sécurité**, cliquez sur **Services système**, puis double-cliquez sur **Identité de l'application**.

8. Dans la boîte de dialogue **Propriétés de : Identité de l'application**, cliquez sur **Définir ce paramètre de stratégie** et, sous **Sélectionnez le mode de démarrage du service**, cliquez sur **Automatique**, puis cliquez sur **OK**.

9. Fermez l'Éditeur de gestion des stratégies de groupe.

10. Dans la console GPMC, liez **Objet GPO Contrôle de logiciels** à **Unité d'organisation Ordinateurs clients**.

Tâche 4 : Exécuter GPUpdate

1. Basculez vers **CL1**.

2. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante : **gpupdate /force**

3. Fermez la fenêtre d'invite de commandes et redémarrez **CL1**.

Tâche 5 : Exécuter iexplore.exe dans le dossier C:\CustomApp

1. Connectez-vous à **CL1** en tant que **OFPPT\Administrateur.**

2. À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée : **gpresult /R**

Examinez le résultat de la commande et vérifiez que **Objet GPO Contrôle de logiciels** est affiché sous Paramètres de l'ordinateur, Objets Stratégie de groupe appliqués. Si **Objet GPO Contrôle de logiciels** n'est pas affiché, redémarrez CL1 et répétez les étapes 1 et 2.

3. créez un dossier **C:\CustomApp** et copiez à l'intérieur le fichier **iexplore.exe** depuis **C:\programFiles\InternetExplorer.** À l'invite de commandes, tapez la commande suivante et appuyez sur Entrée : **C:\ CustomApp\iexplore**

Tâche 6 : Afficher les événements AppLocker dans un journal des événements

1. Sur CL1, démarrez l'**observateur d'événements**.

2. Dans la fenêtre de l'**observateur d'événements**, accédez à **Journaux des applications et des services/Microsoft/Windows/AppLocker**, puis passez en revue les événements.

3. Cliquez sur **Script** et examinez le journal des événements 8002 qui contient le texte suivant : **L'exécution de %OSDRIVE%\CUSTOMAPP\ IEXPLORE.EXE a été autorisée**.

Remarque : Si aucun événement ne s'affiche, assurez-vous que le service Identité de l'application a démarré et réessayez.

Tâche 7 : Modifier l'objet GPO Contrôle de logiciels pour appliquer des règles

1. Utilisez l'option **Appliquer les règles** pour configurer la mise en application des règles suivantes :

o **Règles de l'exécutable**

o **Règles Windows Installer**

o **Règles de script**

o **Règles d'applications empaquetées**

2. Fermez l'Éditeur de gestion des stratégies de groupe.
3. Connectez-vous à **CL1** en tant que **OFPPT\Karim**.

4. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante : **gpupdate /force**

5. Ouvrez une invite de commandes et vérifiez si vous pouvez exécuter l'application **iexplore.exe**, qui figure dans le dossier **C:\CustomApp**. Résultat est **NON** !! Car par défaut il va exécuter seulement les applications qui se trouvent dans **programFiles** ou sur **Windows** selon les règles de **Applocker.**

Tâche 8 : Créer une règle qui autorise l'exécution des logiciels figurant dans un emplacement spécifique

1. Sur DC1, modifiez l'objet GPO Contrôle de logiciels.

2. Accédez à l'emplacement de paramétrage suivant : **Configuration ordinateur/Stratégies/ Paramètres Windows/Paramètres de sécurité/Stratégies de contrôle de l'application/ AppLocker**.

3. Créez une nouvelle **règle de l'exécutable** avec la configuration suivante :

o Autorisations : **Autoriser**

o Conditions : **Chemin d'accès**

o Chemin d'accès : **%OSDRIVE%\CustomApp\iexplore.exe**

o Nom et description : **Règle d'application personnalisée**

Tâche 9 : Vérifier qu'une application peut encore être exécutée

1. Connectez-vous à **CL1** en tant que **OFPPT\Karim**.

2. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante : **gpupdate /force**

3. vérifiez que vous pouvez exécuter l'application **iexplore.exe**, qui figure dans le dossier **C:\CustomApp**.

Tâche 10 : Vérifier qu'une application ne peut pas être exécutée

1. Sur CL1, à partir du dossier **CustomApp**, copiez **iexplore.exe** dans le dossier **Documents**.

2. Vérifiez que l'application ne peut pas être exécutée à partir du dossier **Documents** et que le message suivant apparaît : « **Ce programme est bloqué par une stratégie de groupe. Pour plus d'informations, contactez votre administrateur système.** »

Exercice 2 : Configuration du Pare-feu Windows

Votre responsable vous a chargé de configurer les règles du Pare-feu Windows pour un ensemble de nouveaux serveurs d'applications. Ces serveurs d'applications ont une application Web à l'écoute sur un port non standard. Vous devez configurer le Pare-feu Windows pour autoriser la communication réseau via ce port. Vous utiliserez un filtrage de sécurité pour garantir que les nouvelles règles du Pare-feu Windows s'appliquent uniquement aux serveurs d'applications.

Tâche 1 : Créer un groupe nommé Serveurs d'applications

• Sur DC1, dans Utilisateurs et ordinateurs Active Directory, dans l'**unité d'organisation Serveurs membres**, créez un nouveau groupe de sécurité global nommé **Serveurs d'applications**.

Tâche 2 : Ajouter SVR1 en tant que membre du groupe

• Dans la console Utilisateurs et ordinateurs Active Directory, dans l'unité d'organisation Serveurs membres, ouvrez **Propriétés de : Serveurs d'applications**, puis ajoutez **SVR1** en tant que membre du groupe.

Tâche 3 : Créer un nouvel objet GPO Serveurs d'applications

1. Sur DC1, ouvrez la console **GPMC**.

2. Dans la console GPMC, dans le conteneur **Objets de stratégie de groupe**, créez un nouvel objet GPO nommé **Objet GPO Serveurs d'applications**.

3. Dans la fenêtre de l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur/Stratégies/Paramètres Windows/Paramètres de sécurité/ Pare-feu Windows avec fonctions avancées de sécurité/Pare-feu Windows avec fonctions avancées de sécurité - LDAP://CN={GUID}**.

4. Configurez une règle de trafic entrant avec les paramètres suivants :

o Type de règle : **Personnalisée**

o Type de protocole : **TCP**

o Ports spécifiques : **8080**

o Étendue : **Toute adresse IP**

o Action : **Autoriser la connexion**

o Profil **: Domaine** (désactivez les deux cases à cocher **Privé** et **Public**)

o Nom : **Règle de pare-feu de service de serveur d'applications**

5. Fermez l'Éditeur de gestion des stratégies de groupe.

Tâche 4 : Lier l'objet GPO Serveurs d'applications à l'unité d'organisation Serveurs membres

• Dans la console GPMC, liez l'**objet GPO Serveurs d'applications** à l'**unité d'organisation Serveurs membres**.

Tâche 5 : Utiliser le filtrage de sécurité pour limiter l'objet GPO Serveurs d'applications aux membres du groupe Serveurs d'applications

1. Sur DC1, ouvrez la console **GPMC**.

2. Développez **Unité d'organisation Serveurs membres**, puis cliquez sur **Objet GPO Serveurs d'applications**.

3. Dans le volet de droite, sous Filtrage de sécurité, supprimez **Utilisateurs authentifiés** et configurez l'**objet GPO Serveurs d'applications** pour qu'il s'applique uniquement au groupe de sécurité **Serveurs d'applications**.

Tâche 6 : Exécuter GPUpdate sur SVR1

1. Basculez vers **SVR1**.

2. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante : **gpupdate /force**
3. Fermez la fenêtre d'invite de commandes.

4. Redémarrez **SVR1**, puis connectez-vous à nouveau en tant que **OFPPT\Administrateur**.

Tâche 7 : Afficher les règles de pare-feu sur SVR1

1. Basculez vers **SVR1**.

2. Démarrez le **Pare-feu Windows avec fonctions avancées de sécurité**.

3. Dans la fenêtre du Pare-feu Windows avec fonctions avancées de sécurité, dans **Règles de trafic entrant**, vérifiez que la **règle de pare-feu de service de serveur d'applications** que vous avez créée auparavant à l'aide d'une stratégie de groupe est configurée.

4. Vérifiez que vous ne pouvez pas modifier la **règle de pare-feu de service de serveur d'applications**, car elle est configurée via une stratégie de groupe.

Résultats : À la fin de cet exercice, vous devrez avoir utilisé une stratégie de groupe pour configurer le Pare-feu Windows avec fonctions avancées de sécurité afin de créer des règles pour les serveurs d'applications.