TP : Introduction aux domaines Windows

1 Mise en place d'un domaine

Nous allons créer un domaine avec deux machines :
— un contrôleur de domaine sous Windows Server 2012 R2 ;
— une station membre du domaine sous Windows 7.

1.1 Installation du *domain controller*

Attention
Pour l'installation de votre DC, vous aurez besoin d'environ 8Go d'espace disque sur votre machine hôte.

Pour créer notre DC, nous allons utiliser un Windows Server 2012 R2.

— Commencez par installer Windows Server 2012 R2 sur une VM :
  — Les VM seront interconnectées via un réseau interne (il faut donc ajouter un *network adapter* à votre VM).
  — Pour installer le serveur, utilisez l'ISO que vous pouvez télécharger sur : `https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-server-2012-r2`.
  — Pendant l'installation choisissez l'installation de : "Windows Server 2012 R2 Standard Evaluation (Server with a GUI)".
— Une fois l'installation réalisée, activez la license temporaire d'évaluation à l'aide de la commande suivante :

```
slmgr /rearm
```

— À l'aide de l'utilitaire *sconfig* changez le nom de votre machine ainsi que la configuration réseau :
  — Pour changer le nom de la machine choisissez l'option 2 de *sconfig*.
  — Pour changer la configuration réseau choisissez l'option 8 :
    — choisissez une IP statique ;
    — vous pouvez choisir l'IP 192.168.1.2 et le masque 255.255.255.0 par exemple.

— Nous allons maintenant transformer notre serveur en DC à l'aide de *powershell* :
  — Commencez par visualiser toutes les *features* Windows disponibles avec la commande suivante :

```
Get-WindowsFeature
```

  — La *feature* qui nous intéresse est *AD-Domain-Services*, on va donc l'installer avec la commande suivante :

```
Install-WindowsFeature AD-Domain-Services
```

  — Les composants nécessaires à notre *domain controller* sont maintenant présents, il suffit donc d'indiquer à notre serveur de les utiliser pour prendre le rôle d'un DC :

```
Import-Module ADDSDeployment
Install-ADDSForest
```

  — Votre DC est maintenant installé, il ne reste plus qu'à ajouter des machines au domaine.

1.2 Ajout d'une machine au domaine

Attention
Pour l'installation de cette station, vous aurez besoin d'environ 7Go d'espace disque sur votre machine hôte.

Nous allons ajouter une station Windows 7 à notre domaine.

— Commencez par installer Windows 7 sur une VM :
  — Ajoutez un adaptateur dans le même réseau interne que votre DC.
  — Pour installer la station, utilisez l'ISO que vous pouvez télécharger sur : `http://care.dlservice.microsoft.com/dl/download/evalx/win7/x64/EN/7600.16385.090713-1255_x64fre_enterprise_en-us_EVAL_Eval_Enterprise-GRMCENXEVAL_EN_DVD.iso`.
— Une fois l'installation réalisée, activez la license temporaire d'évaluation à l'aide de la commande suivante (vous aurez besoin de lancer un invité de commande en tant qu'administrateur) :

```
slmgr /rearm
```

— Pour la configuration de notre DC nous avons utilisé des outils en ligne de commande (*sconfig*, *powershell*). Pour configurer notre station nous allons utiliser l'approche plus classique pour manipuler une machine Windows : l'interface graphique ("le cliquodrome").
— Pour changer le nom de la machine, allez dans le panneau de configuration (*control panel*) puis allez dans *System and Security/System/-See the name of this computer/Change Settings/Change....*
— Pour changer la configuration réseau, depuis le panneau de configuration allez dans *Network and Internet/Network and Sharing Center/Changing adapter settings*. À l'aide d'un clique droit allez dans le propriétés de l'adaptateur puis allez dans les propriétés de *Internet Protocol Version 4 (TCP/IPv4)*.
  — Choisissez une IP (par exemple 192.168.1.3 avec le masque 255.255.255.0).
  — Pour le *prefered DNS server* mettez l'IP de votre DC.
— Pour ajouter la machine au domaine, comme pour changer le nom de la machine, allez dans le panneau de configuration puis allez dans *System and Security/System/See the name of this computer/Change Settings/Change...* et modifiez le paramètre *Member of* pour y mettre votre domaine. Il vous sera alors demandé le nom et le mot de passe d'un utilisateur de ce domaine qui a le droit d'ajouter une machine au domaine.
— Pour tester que votre machine appartient bien à votre domaine, vous pouvez vous *logger* avec le compte *Administrator* du domaine.

2 Manipulation du domaine

2.1 Installation des outils

Pour cette partie nous allons utiliser les outils graphiques d'administration du domaine. Nous pourrions les installer avec *powershell* (en utilisant *Install-WindowsFeature*) mais nous allons les installer avec l'interface graphique : *Server Manager*.

— Sur votre DC, lancez *Server Manager*.
— Allez dans *Manage/Add Roles and Features*.
— Quand vous arriverez à la partie *Features*, choisissez *Remote Server Administration Tools/Role Administration Tools/AD DS and AD LDS Tools/AD DS Tools*.
— Dans l'onglet *Tools* de *Server Manager* vous avez maintenant de nouveaux outils (noms commençant par *Active Directory*).

2.2 Votre première OU

— À l'aide de l'outil *Active Directory Users and Computers*, créez une OU (par exemple appelée "Comptabilité").
— Dans cette OU, créez deux OU, une pour mettre les utilisateurs (par exemple appelée "Comptables") et une pour mettre les postes de travail (par exemple appelée "Postes").
— Placez la machine que vous avez ajouté au domaine dans l'OU des postes de travail.
— Créez deux utilisateurs dans l'autre OU.

2.3 Votre première GPO

— Dans un premier temps, nous allons voir les GPO appliquées sur la machine Windows 7. Lancez les commandes suivantes (en tant qu'administrateur) :

```
gpresult /V > gpresult-1.txt
notepad gpresult-1.txt
```

— Ensuite sur le DC, avec l'outil *Group Policy Management* augmentez la taille minimale de mot de passe autorisée sur **l'ensemble du domaine**.
  — Il faut aller dans *Computer Configuration/Policies/Windows Settings/Security Settings/Account Policy*.
— Sur la machine Windows 7, inspectez à nouveau les GPO :

```
gpresult /V > gpresult-2.txt
notepad gpresult-2.txt
```

— Quelles différences voyez-vous par rapport au premier resultat de *gpresult* ?
— Forcez la mise à jour des GPO sur la machine :

```
gpupdate
```

— Visualisez à nouveau les GPO de la machine :

```
gpresult /V > gpresult-3.txt
notepad gpresult-3.txt
```

— Mettez une valeur différente de taille minimale de mot de passe au niveau de l'OU contenant la station (vous aurez besoin de créer une nouvelle GPO).
— Visualisez les GPO appliquées à la machine Windows 7. Quelle est la valeur de la taille minimale de mot de passe ? Expliquez ce résultat.
— Mettez l'attibut *enforced* à la GPO s'appliquant à l'ensemble du domaine (clique droit puis *Enforce*).
— À nouveau, visualisez les GPO appliquées à la machine Windows 7. Quelle est la valeur de la taille minimale de mot de passe ? Expliquez ce résultat.

— Créez une nouvelle GPO au niveau de l'OU contenant vos utilisateurs. Avec cette GPO, empêchez les utilisateurs d'utiliser le panneau de configuration.
— Vérifiez le bon fonctionnement de votre GPO.

— Ajoutez le droit de modifier le propriétaire de la GPO s'appliquant à l'ensemble du domaine à un de vos utilisateurs :
  — Voyez-vous à quoi peut servir ce réglage ? Dans quel contexte peut-il être utilisé ?

2.4 Délégation de privilèges

— Créez un nouveau groupe depuis *Active Directory Users and Computers* (par exemple "Comptabilité-Administrateurs").
— Ajoutez un de vos utilisateurs à ce groupe (clique droit sur l'utilisateur et *Add to a group...*).
— Nous allons déléguer le droit de gérer les utilisateurs de notre OU à ce groupe.
  — Effectuez un clique droit sur votre OU et sélectionnez *Delegate Control....*
  — Dans la partie *Tasks to Delegate* choisissez les 5 premières options.
— Pour tester le bon fonctionnement de cette délégation nous allons nous *logger* sur le DC avec le compte ajouté dans le groupe.
  — Dans un premier temps nous allons autoriser l'utilisateur à se connecter sur le DC (configuration évidemment non souhaitable dans un environnement de production).
    — Depuis l'outil *Group Policy Management*, ajoutez à la GPO des DC l'utilisateur en question dans *Computer Configuration/Policies/Windows Settings/Local Policies/User Rights Assignment/Allow log on locally.*

— Connectez vous avec le compte sur le DC, lancez *Active Directory Users and Computers*. Que pouvez-vous modifier dans le domaine ?

2.5 Ajout d'administrateurs locaux

— Nous allons commencer par créer un groupe qui sera administrateur local sur les machines de notre OU.
  — On pourrait utiliser l'utilitaire *Active Directory Users and Groups* pour faire ça. Ici nous allons utiliser *powershell*. Avec la *cmdlet New-ADGroup*, créez un groupe global (appelé "Administrateurs-Locaux" par exemple).
  — Avec la *cmdlet Add-ADGroupMember* ajoutez un de vos deux utilisateurs à ce groupe.
— Pour rendre ce groupe administrateur local sur les machines de notre OU, il faut créer une nouvelle GPO au niveau de l'OU regroupant les postes. Dans cette OU, il faut ajouter aux *Restricted Groups* notre nouveau groupe et paramètrer ce groupe comme appartenant **localement** au groupe *Administrators*.
— Testez que votre GPO fonctionne bien en lançant un invité de commande en tant qu'administrateur avec le compte que vous avez ajouté au nouveau groupe.

3 Chemins de contrôle

Dans cette partie vous allez utiliser l'outil *Bloodhound*[1].

1. Utilisez *SharpHound*[2] [3] pour collecter les données de votre AD ;
   — vous pouvez le lancer depuis votre station Windows avec l'utilisateur standard.
2. Installez *neo4j* sur la machine où vous souhaitez faire l'analyse (peut être votre machine hôte) ;
3. Importez les données dans la base *neo4j* de *Bloodhound* (via l'interface graphique de *Bloodhound*) ;
   — également faisable sans l'interface graphique avec *bloodhound-import*[4].

1. `https://github.com/BloodHoundAD/Bloodhound`
2. `https://github.com/BloodHoundAD/SharpHound`
3. `https://github.com/BloodHoundAD/BloodHound/blob/master/Ingestors/SharpHound.exe`
4. `https://github.com/fox-it/bloodhound-import`

4. Analysez les chemins de contrôle (par exemple regardez quels sont les chemins de contrôle vers le groupe *Domain Admins*).