S3T5 - Powershell 3

PS et AD

Modif : 19/09/2021 exercice modifié afin de mieux préparer au devoir

Document à rendre sous le nom

S3T5 votre nom.docx

Tout fichier ne correspondant pas à cette demande sera ignoré !

1 Introduction

Au cours de ce TP, nous allons installer un gestionnaire de domaine et de comptes Microsoft : Active Directory.
Cet AD comportera aussi un DNS mais PAS DE DHCP (on verra plus tard)
Il permettra de tester des scripts Powershell d'administration de serveur Microsoft et on utilisera le bureau à distance pour le gérer

A l'issue de ce TP, vous saurez :

- Installer un AD
- Installer des modules pour l'AD,
- Installer le service de bureau à distance,
- Utiliser le bureau à distance
- Gérer l'AD (comptes utilisateur et groupes)
- Trouver des tutos pertinents sur Internet

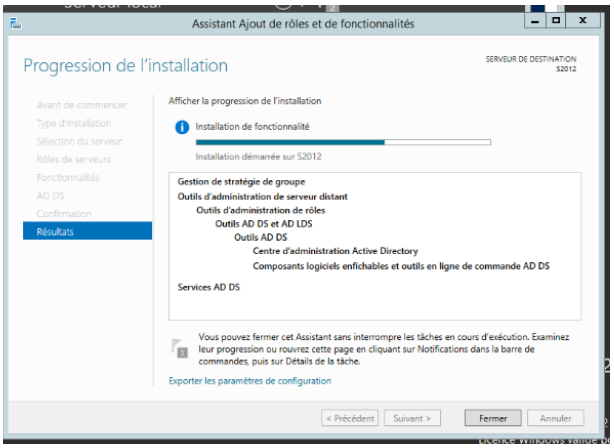
Ce TP contient des questions, vous écrirez vos réponses dans les cadres jaunes prévus à cet effet. Prêt ?

Oh OUI !

Alors c'est parti …

2 Installer le système et ses composants

Remarque :
Si vous avez un AD dans votre ferme de serveur, vous pourrez faire ces commandes sur une copie de celui-ci qui sera détruite en fin de TP.
Passez directement à la partie 3.



On va installer notre serveur S2016 (id=administrateur, mdp=Admin_S2016)

2.1 Installer l'AD et le DNS

Pour installer l'AD et le DNS, rien ne vaut mieux qu'un Tuto sur le net …Une bonne adresse (parmi d'autres) : Windows Server 2012 : Installer un contrôleur de domaine (ADDS) – Tech2Tech |

Note : l'install en W2012 est presque la même qu'avec les versions ultérieures, c'est beaucoup de design qui change mais les fondamentaux sont constants.

Attention au paramétrage de l'AD, au moment de la "promotion du serveur en contrôleur de domaine" :

1. Ecran : Configuration de déploiement
   - cocher "Ajouter une nouvelle forêt"
   - Notre domaine racine sera : **monDom.local**

2. Ecran : Option de contrôleur de domaine
   - Niveau fonctionnel de la forêt et du domaine : choisir Server 2008 pour les deux, ça nous permettra de gérer des machines sous W2008, si on en a.
   - Mot de passe : Admin_S2016 (attention, en entreprise il doit être plus robuste!)
   - Ecran d'erreur : Option DNS, normal car il n'est pas connecté à un domaine parent

3. Ecran : Options supplémentaires : RAS
4. Ecran : Chemin d'accès : RAS
5. Ecran : Examiner les options

   En fait, ici, l'assistant va générer un script powershell qui sera exécuté pour créer l'AD et le domaine.

   L'assistant ne sert qu'à faciliter le choix des arguments
   - Visualiser le script avec le bouton "Afficher le script".

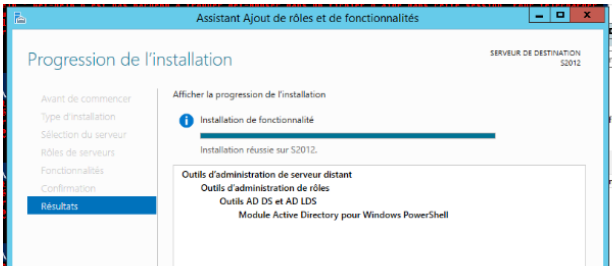
   Quelle commande (verbe-nom) va permettre de créer le domaine ?

6. Ecran : Vérification de la configuration requise
   - Il y plusieurs messages d'avertissement (/!\) mais on n'en tient pas compte pour l'instant (vous avez quand-même le droit de les lire …)

7. Ecran : Installation
   - Il rappelle les paramètres et les erreurs.
   - A l'issue de cet écran, le serveur demande à redémarrer (vous n'avez pas le choix)

8. Après redémarrage, c'est fini pour l'instant.

2.2 Installer le module AD, nécessaire à PS



Powershell ne sait pas gérer l'AD par défaut. Il faut

installer le module fonctionnel AD pour PS.

Pour cela, utilisez le tuto de ce site : How to install the PowerShell Active Directory module

Et rechercher le chapitre pour "Windows Server 2012 and Windows Server 2012 R2"

Il est en anglais (yes) facile à comprendre (ooh). Mais voici (ci-après) le résultat que vous devriez avoir

2.3 Installer le service de Bureau à distance

Trouver vous-même un tuto facile à utiliser. Ceci dit, les plus simples ne sont pas forcément en français … et même Microsoft fait de chouettes notices d'installation !

Notez ci-dessous l'adresse du tuto que vous avez utilisé.

3 Préparation du TP

ACHTUNG !!! AVANT DE COMMENCER

Fermez la session et essayez d'ouvrir la session administrateur avec un mauvais mot de passe.

(c'est pour créer un historique d'échec d'ouverture)

Ouvrez une session avec administrateur correctement

a) Modifiez la politique de mots de passe dans l'AD : autoriser les mdp simples, courts (minimum 1 caractère), enlever la nécessité de les renouveler tous les 42 jours (voir procédure W2008 en annexe à adapter à W2012.

TAF : indiquez ci-dessous la procédure de création d'utilisateur (menu, paramètres choisis, etc. …) ?

b) Créer ensuite le groupe utilisateur adherent (sans accent) puis les utilisateurs David/david Erik/erik et Farah/farah qui seront dans ce groupe avec les assistants de création dans l'AD.

ATTN : Le groupe sera local et de sécurité, les utilisateurs auront des identifiants en minuscule (comme les mdp) et leur mdp ne pourra pas être changé et n'expirera jamais.

TAF : indiquez ci-dessous la procédure de création d'utilisateur (menu, paramètres

choisis, etc. …) ?

c) Ouvrir le groupe adhérent puis y ajouter les utilisateurs erik et farah (pas les autres).

Ne pas oublier de cliquer sur le bouton "vérifier les noms" avant de valider (testez avec fara au lieu de farah …).

4 Premiers pas en PS pour AD

L'environnement du TP est maintenant prêt. On va pouvoir commencer le PS.

Connectez-vous sur la console avec administrateur et via le bureau à distance avec david

4.1 Consulter l'Active Directory

Tester les commandes suivantes :

Commande	Description (à remplir)
`Get-Domain`	
`Get-ADUser -Filter *`	
`Get-ADUser -Filter * | out-gridview`	
`Get-ADGroup adherent`	
`Get-ADPrincipalGroupMembership david`	
`Get-ADPrincipalGroupMembership "utilisateurs du domaine"`	

Tester les commandes suivantes :

Get-ADUser -Filter {Name -eq "Administrateur"} -Properties * | Select-Object Name, msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon

TAF : Que fait-elle ?

Get-ADUser -Filter * -Properties * | Select-Object Name, msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon | Sort-Object -Descending msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon

TAF : Que fait-elle ?

```
Get-ADUser -Filter * -Properties * | Where-Object msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon -gt 3 | Measure-Object | Select-Object Count
```

TAF : Que fait-elle ?

TAF : Combien avez-vous d'utilisateurs ?

TAF : insérez ci-dessous une copie d'écran (rognée) du résultat de la commande

[NE PAS FAIRE ci dessous en fond gris]

Tentez de faire la commande suivante (vous pouvez peut-être activer le presse-papier entre la VM et l'hôte … non? Ou tenter de passer par putty ou par le bureau à distance ?)

*Get-ADUser -Filter * -Properties * | Select-Object -Property Name, @{Name="Total failed logons"; Expression="msDS-FailedInteractiveLogonCount"}, @{Name="Recent failed logons"; Expression="msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon"}, @{"Name"="Last failed logon"; Zxpression={[datetime]::FromFileTime($_.'msDS-LastFailedInteractiveLogonTime')}}, @{"Name"="Last successful logon"; Expression={[datetime]::FromFileTime($_.'msDS-LastSuccessfulInteractiveLogonTime')}} | Sort-Object Name | Format-Table*

Remarquez les **;** qui permettent en fait d'exécuter plusieurs commandes sur une même ligne (c'est pas trop lisible, non?)

Remettez la commande en forme ci-dessous pour la rendre plus lisible :

*Get-ADUser -Filter * -Properties * | Select-Object -Property Name, @{Name="Total failed logons"; Expression="msDS-FailedInteractiveLogonCount"}, @{Name="Recent failed logons"; Expression="msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon"}, @{"Name"="Last failed logon"; Zxpression={[datetime]::FromFileTime($_.'msDS-LastFailedInteractiveLogonTime')}}, @{"Name"="Last successful logon"; Expression={[datetime]::FromFileTime($_.'msDS-LastSuccessfulInteractiveLogonTime')}} | Sort-Object Name | Format-Table*

C'est juste pour vous montrer qu'on peut faire du code illisible, compliqué. J'espère que cela vous incitera à être plus clair dans le devoir de … bientôt !!!

Exporter la liste des utilisateurs actifs

Afin d'avoir une liste d'utilisateurs actifs, nous allons exporter celle-ci dans un fichier CSV.

Dans un nouveau script obtenirListeUtilisateurs.ps1, copiez et complétez le code ci-dessous.

```
# initialiser le nom du fichier CSV
```

```
$fichierCSV = "c:\FTP\USERAD.csv"

# récupération des utilisateurs actifs
$users       = Get-ADUser -filter "enabled"

# Initialiser la liste vide (@() représente un tableau vide)
$liste =@()

# Pour chaque utilisateur, l'ajouter à $liste
...Ajouter le code nécessaire ici ...

# Exporter $liste vers un fichier CSV
$liste | select-object samAccountName | Export-Csv $fichierCSV -Encoding UTF8
```

Pour compléter ce code, vous aurez besoin :

- d'une boucle foreach qui permettra de remplir la liste
- l'export peut être simplifié à l'aide d'une syntaxe objet

```
$users | foreach {
  $liste = $liste + $_
}

Ou

foreach ($user in $users) {
  $liste = $liste + $user
}

ou encore :
$users | foreach {
  $liste = $liste + $_.samAccountName
}

$liste | export-csv $fichier ...
```

```
get-command help | foreach {
  $liste = $liste + $_
}

Ou

foreach ($ligne in $tableau) {
  $liste = $liste + $ligne
}
```

4.2 Modifier l'Active Directory

Juste un peu et on s'arrête. Ok ?

Tester les commandes suivantes, **attention**, vous devez vérifier que chaque commande ai fonctionné et que le résultat soit correct dans la gestion des utilisateurs de l'AD :

commande	Description (à remplir)
`Add-ADGroupMember adherent -member david`	
`Remove-ADGroupMember adherent -member erik`	
`Add-ADUser garfield`	

TAF : Quelle commande permet d'ajouter un utilisateur ?

TAF : Ajoutez "garfield" avec la commande trouvée puis vérifiez. Dans quel état est-il ?

Vérifiez que la session de david est bien ouverte puis, avec la console, supprimez l'utilisateur david.
TAF : Dans quel état est la connexion de david via le bureau à distance après la suppression de son compte ?

Bien, on arrête là les frais.

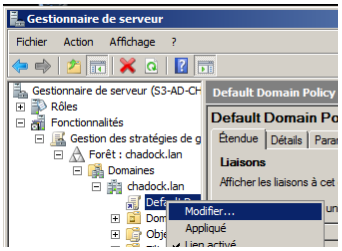
Question subsidiaire non notée : rechercher les sous-dossiers de C:\Users\ dans lesquels il existe des fichiers de plus de 2 Go afin de pouvoir savoir quel utilisateur consomme trop d'espace (VM, films, etc. …)

Faire la même chose avec des dossiers de plus de 2Go ...

Annexe 1 : si changer de mdp vous embête …

L'administrateur local du contrôleur du domaine est devenu celui de tout le domaine. Ils sont confondus. Donc … modifier la gestion de son mot de passe n'est peut-être pas une bonne idée!

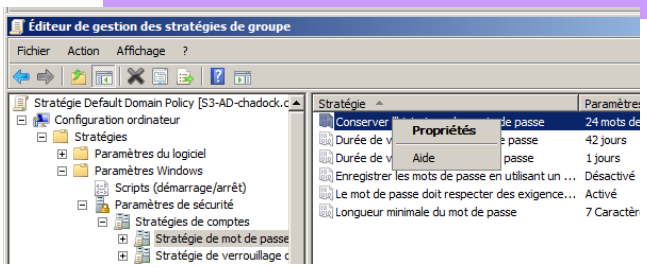
Cependant, on est en mode test et changer de mot trop souvent risque de vous le faire oublier, surtout s'il est compliqué. Donc … pour modifier la politique de mots de passes, suivre la procédure suivante :



- ouvrir le gestionnaire de serveur
- Développer l'arbre ci-contre,
- Modifier la politique par défaut (click droit, modifier)

Dans l'éditeur de stratégie de groupe,

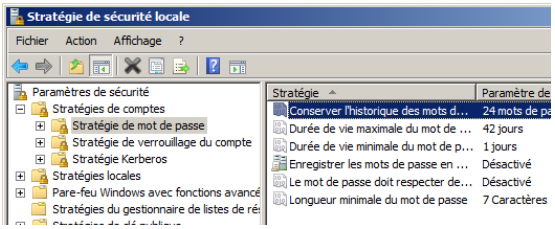
- Développer l'arborescence comme ci-dessous,
- Afficher les propriétés, elles sont (ici) en modif
- Modifier selon vos besoins : désactiver la restriction, modifier la restriction, etc…



Éviter de désactiver le respect des exigences de complexité des mdp

Ainsi que la longueur mini des mdp.

Il est maintenant possible de modifier le paramétrage local des restrictions désactivées dans l'AD :



- Démarrer >outils d'administration > stratégie de sécurité locale
- Développer l'arborescence comme suit et modifier les paramètres
- Historique : 0=aucun
- Durée maxi/mini : 0=sans limite