OFPPT مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle
et de la Promotion du Travail

Module : Administration d'un Réseau sous Windows

Gestion d'objets ADDS

Unité d'organisation, Utilisateurs, Groupe et Ordinateur

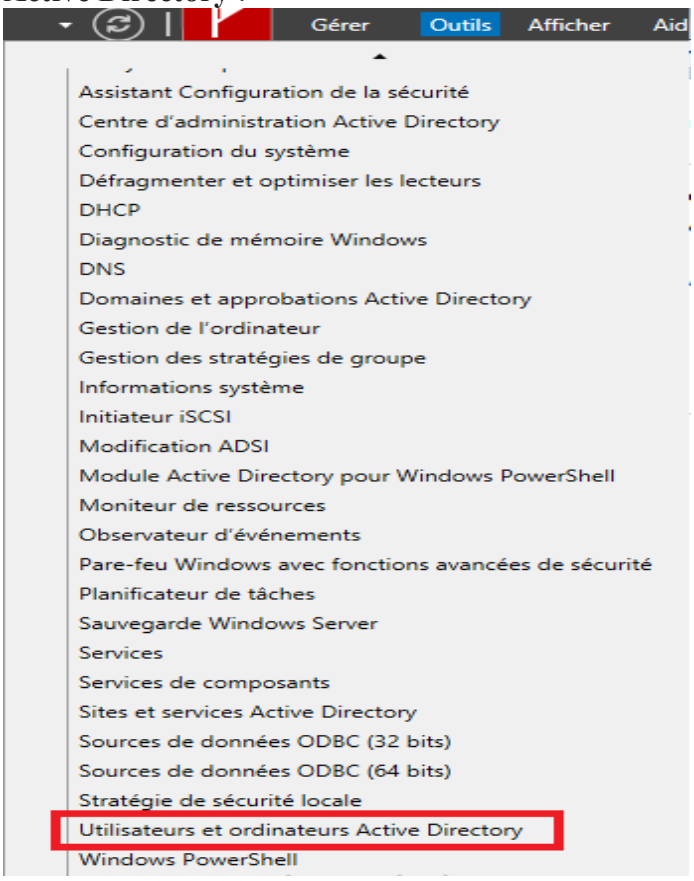
Sommaire

1. Introduction 4
2. Gestion des Unités organisationnelles 4
   2.1 Graphiquement 4
   2.2 PowerShell 5
      a. Ajouter une Ou 5
      b. Modifier une OU 5
      c. Supprimer une OU 6
      d. Afficher la liste des OU 6
   2.3 Commande DS 7
      a. Ajouter une OU 7
      b. Supprimer une OU 8
      c. Afficher la liste des OU 8
3. Gestion des utilisateurs 8
   3.1 Graphiquement 8
   3.2 PowerShell 12
      a. Ajoute un utilisateur 13
      b. Activer et désactiver un compte utilisateur 14
      c. Déverrouiller un compte d'utilisateur 14
      d. Supprimer un utilisateur 14
      e. Recherche d'un utilisateur 14
   3.3 Commande DS 15
      a. Ajouter un utilisateur 15
      b. Modifier un compte d'utilisateur 16
      c. Activer ou désactiver un compte utilisateur 16
      d. Rechercher un utilisateur 16
      e. Supprimer un utilisateur 16
4. Test : Joindre un domaine Active Directory 16
5. Profils itinérants graphiquement 17
   5.1 Configuration 17

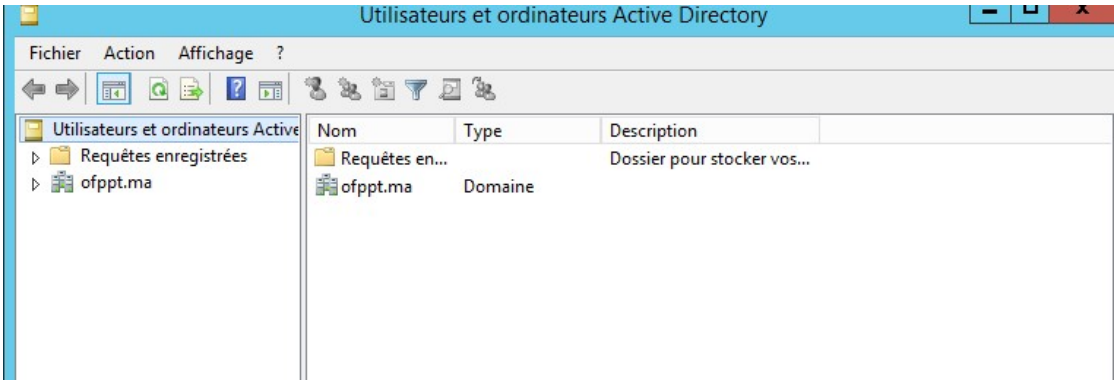
5.2 Test 20
6. Profils itinérants en ligne de commande 24
6.1 Partager un répertoire 24
6.2 Créer un utilisateur profile 25
a. Commande DS 25
b. Commande PowerShell 25
7. Gestion groupe 25
7.1 Présentation 25
a. Etendu du groupe 26
b. Type de groupe 26
7.2 Graphiquement 26
7.3 Commande DS 27
a. Ajouter un groupe 27
b. Modifier un groupe 28
c. Chercher un groupe 28
d. Voir les groupes qu'un user appartient 28
e. Supprimer un groupe 29
7.4 Commande Powershell 29
a. Ajouter un groupe 29
b. Modifier Groupe 29
c. Supprimer un groupe 29
8. Gestion ordinateur 29
8.1 Commande DS 29
a. Ajouter un ordinateur 29
b. Chercher un ordinateur 30
c. Supprimer un ordinateur 30
8.2 Commande PowerShell 30
a. Ajouter un ordinateur 30
b. Chercher des ordinateurs du domaine 30
c. Supprimer un ordinateur 31
9. Reference 31

1. Introduction

Pour peupler notre Active Directory il faut lancer la console **Utilisateurs et ordinateurs Active Directory** .



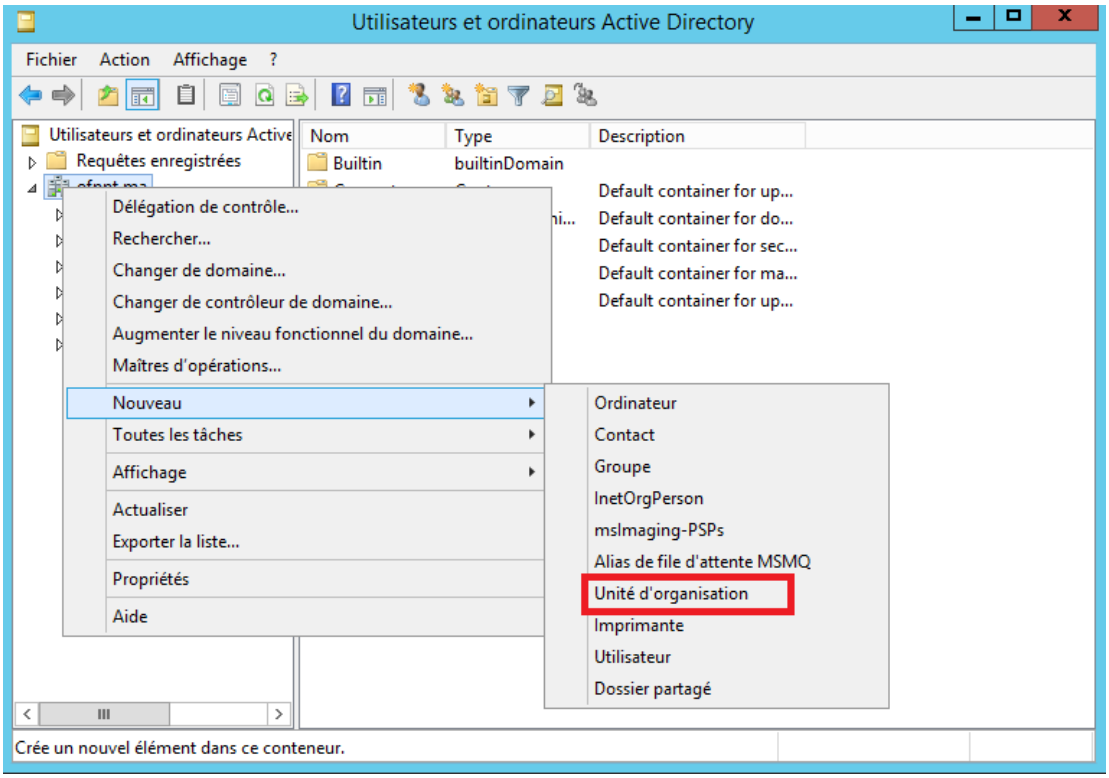
On arrive sur la console



2. Gestion des Unités organisationnelles

2.1 Graphiquement

Pour créer une unité organisationnelle afin d'y mettre l'ensemble des utilisateurs et groupes dans le cadre de notre entreprise.
Dans l'arbre à la hauteur de notre domaine. Faite un clic droite dans la fenêtre de droite, puis **Nouveau** et on choisit **Unité d'organisation**



Choisir le nom de l'unité

NB : L'option supplémentaire **Protéger le conteneur contre une suppression accidentelle** est apparu avec Windows serveur 2012. Cette option n'est pas présente dans Windows serveur 2008.

2.2 PowerShell

a. Ajouter une Ou

Le nom du module est « ADOrganizationalUnit ».Pour créer une nouvelle unité d'organisation nommée « TRI » utilisé la commande :

```
New-ADOrganizationalUnit  -Name  TRI
```

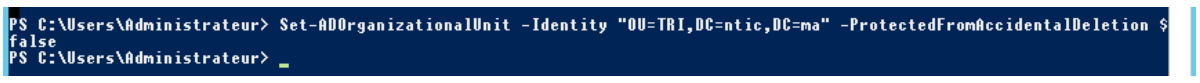
Pour ajouter l'unité « TP » à l'unité « TRI », utiliser l'option « Path »

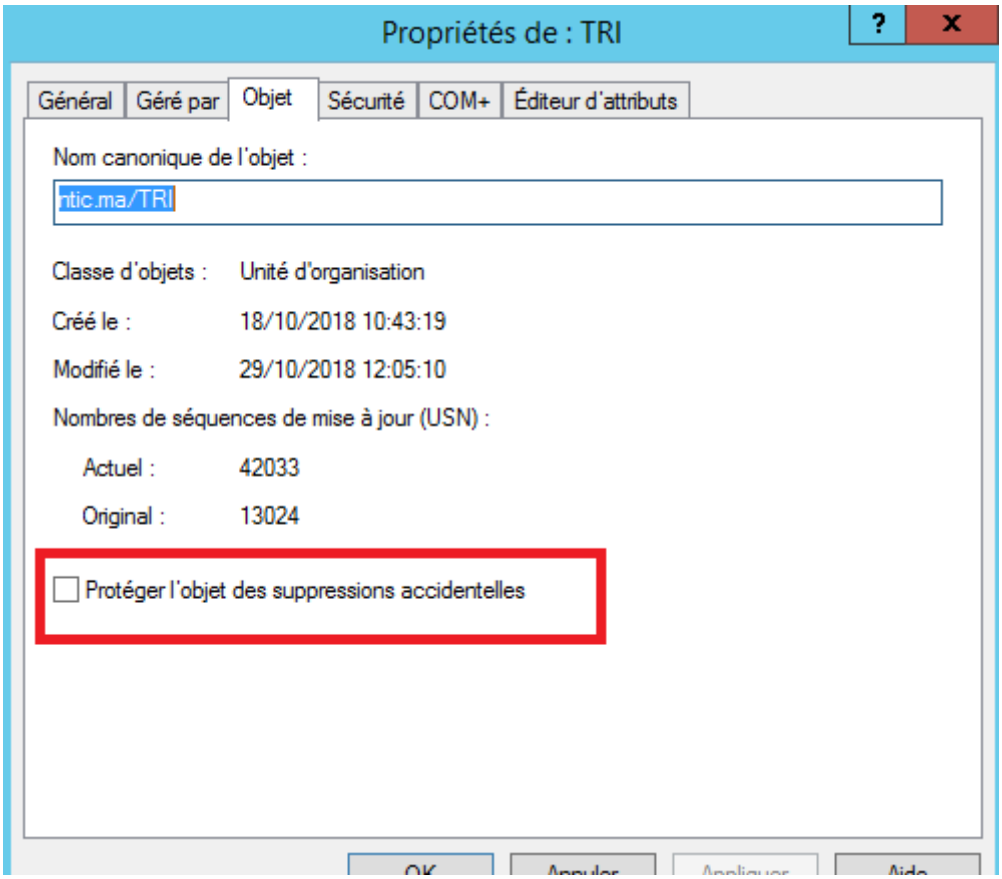
```
New-ADOrganizationalUnit  -Path "ou=TRI,dc=ntic,dc=ma"  -Name TP
```

b. Modifier une OU

Pour modifier par exemple la sécurité contre la suppression de l'unité TRI

```
Set-ADOrganizationalUnit  -Identity  "ou=TRI,dc=ntic,dc=ma" -
ProtectedFromAccidentalDeletion $false
```





c. Supprimer une OU

Pour supprimer une unité d'organisation il faut commencer par enlever la sécurité contre la suppression.

Puis lancer la suppression en utilisant la commande suivante :

```
Remove-ADOrganizationalUnit "ou=TRI,dc=ntic,dc=ma"  -recursive
```

L'option « **-recursive** » est utiliser pour supprimer toutes les sous OU

d. Afficher la liste des OU

Pour afficher la liste des unités d'organisation du domaine :

```
Get-ADOrganizationalUnit –filter *
```

```
PS C:\Users\Administrateur> Get-ADOrganizationalUnit  -filter *


City                        :
Country                     :
DistinguishedName           : OU=Domain Controllers,DC=ntic,DC=ma
LinkedGroupPolicyObjects    : {CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=ntic,DC=ma}
ManagedBy                   :
Name                        : Domain Controllers
ObjectClass                 : organizationalUnit
ObjectGUID                  : 7bfcb4ec-f060-4d61-a530-d35ae4b03a9a
PostalCode                  :
State                       :
StreetAddress               :

City                        :
Country                     :
DistinguishedName           : OU=TRI,DC=ntic,DC=ma
LinkedGroupPolicyObjects    : {}
ManagedBy                   :
Name                        : TRI
ObjectClass                 : organizationalUnit
ObjectGUID                  : 84f73183-9a22-4351-aad0-dc537fe0c4f9
PostalCode                  :
State                       :
StreetAddress               :

City                        :
Country                     :
DistinguishedName           : OU=tel,DC=ntic,DC=ma
LinkedGroupPolicyObjects    : {}
ManagedBy                   :
Name                        : tel
ObjectClass                 : organizationalUnit
ObjectGUID                  : 2c60f2da-a54a-48d9-bf65-c75f2c27be45
PostalCode                  :
State                       :
StreetAddress               :

City                        :
Country                     :
DistinguishedName           : OU=cour,OU=tel,DC=ntic,DC=ma
LinkedGroupPolicyObjects    : {}
ManagedBy                   :
Name                        : cour
ObjectClass                 : organizationalUnit
```

2.3 Commande DS

a. Ajouter une OU

Pour ajouter dans le domaine l'unité organisationnelle suivante :

- Nom de l'unité organisationnelle : tel
- Nom du domaine : ntic.ma

```
dsadd ou "ou=tel,dc=ntic,dc=ma"
```

```
C:\Users\Administrateur>dsadd ou "ou=tel,dc=ntic,dc=ma"
dsadd réussite:ou=tel,dc=ntic,dc=ma
```

Pour ajouter une unité nommée **cour** dans l'unité **tel**

```
dsadd ou "ou=cour,ou=tel,dc=ntic,dc=ma"
```

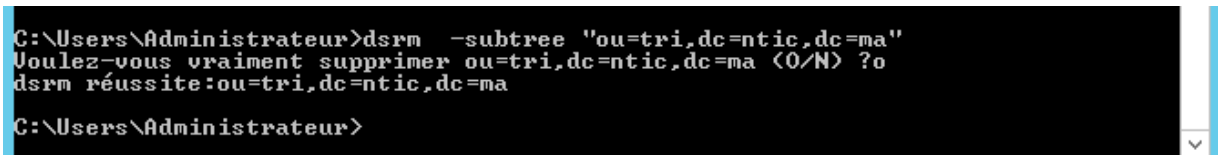
```
C:\Users\Administrateur>dsadd ou "ou=cour,ou=tel,dc=ntic,dc=ma"
dsadd réussite:ou=cour,ou=tel,dc=ntic,dc=ma

C:\Users\Administrateur>_
```

b. Supprimer une OU

Pour supprimer l'unité **cour** utiliser la commande

```
Dsrm –subtree  ou=cour,ou=tel,dc=ntic,dc=ma
```



c. Afficher la liste des OU

```
dsquery ou domainroot
```



Renommer une Ou :

```
dsmove "ou=yassine,dc=maroc,dc=ma" -newname yassinet
```

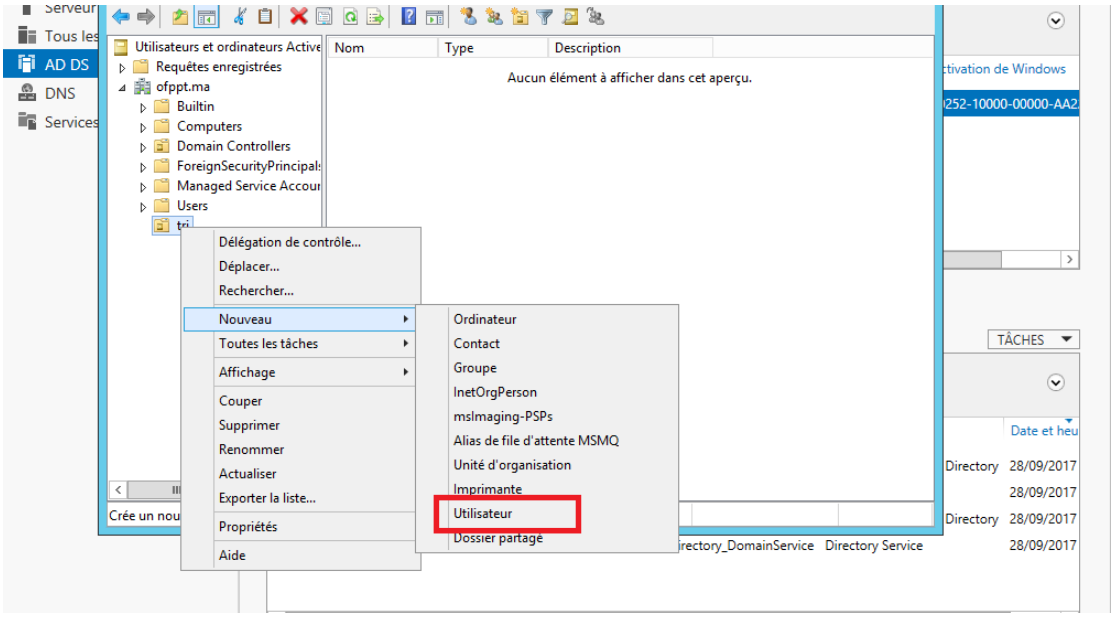
Déplacer une OU :

```
dsmove "ou=yassine,dc=maroc,dc=ma" -newparent ou=casa,dc=maroc,dc=ma
```

3. Gestion des utilisateurs

3.1 Graphiquement

Pour créer un nouvel utilisateur dans l'unité **TRI**. Clic droit sur **TRI** ensuite Nouveau puis **Utilisateur.**



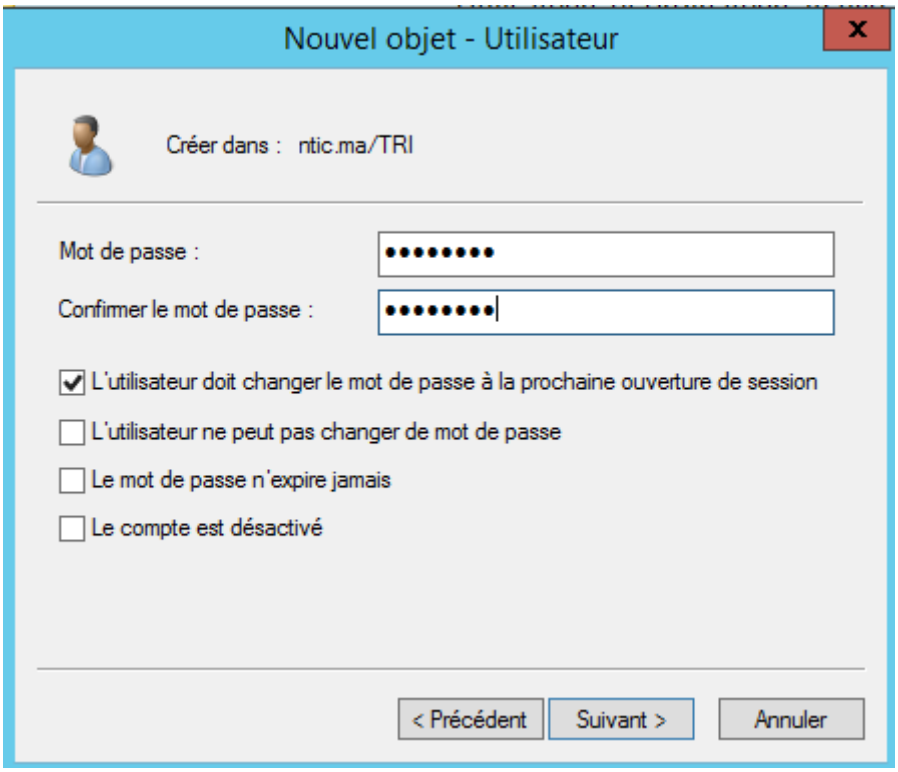
Dans notre exemple, nous allons créer un utilisateur qui s'appelle **Ilham ZITI** avec le nom d'ouverture de session **iziti**



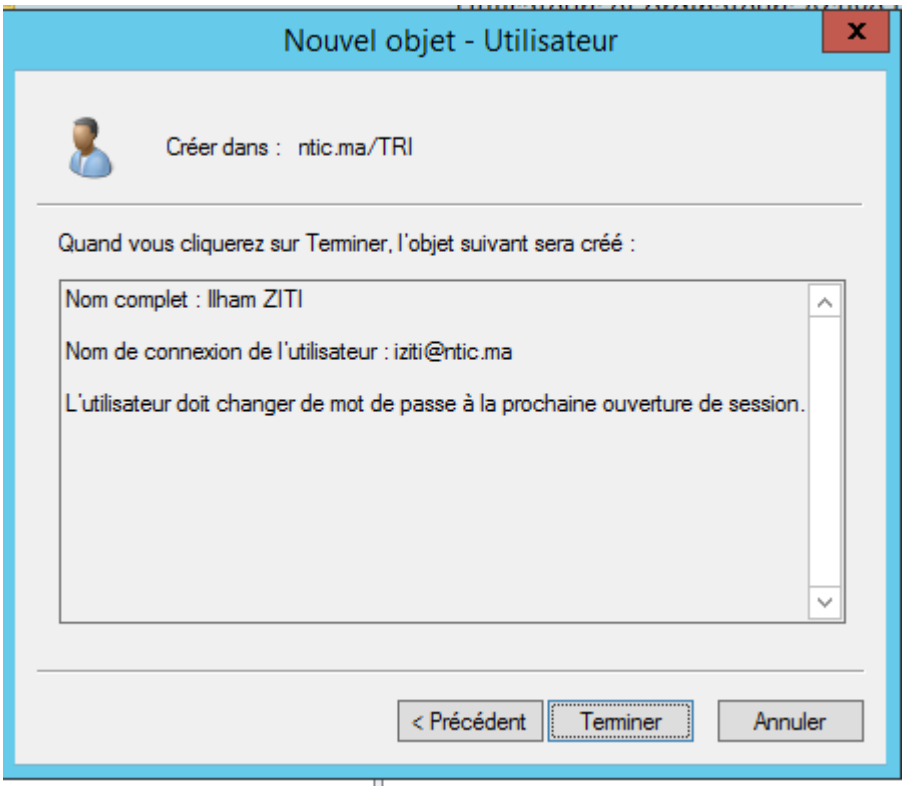
L'utilisateur a deux moyens pour ouvrir une session. :

- UPN, c'est-à-dire la forme d'adresse email, iziti@ntic.ma
- Authentification Windows NT ou 2000 avec le nom du domaine Netbios suivi de l'utilisateur, NTIC\iziti.

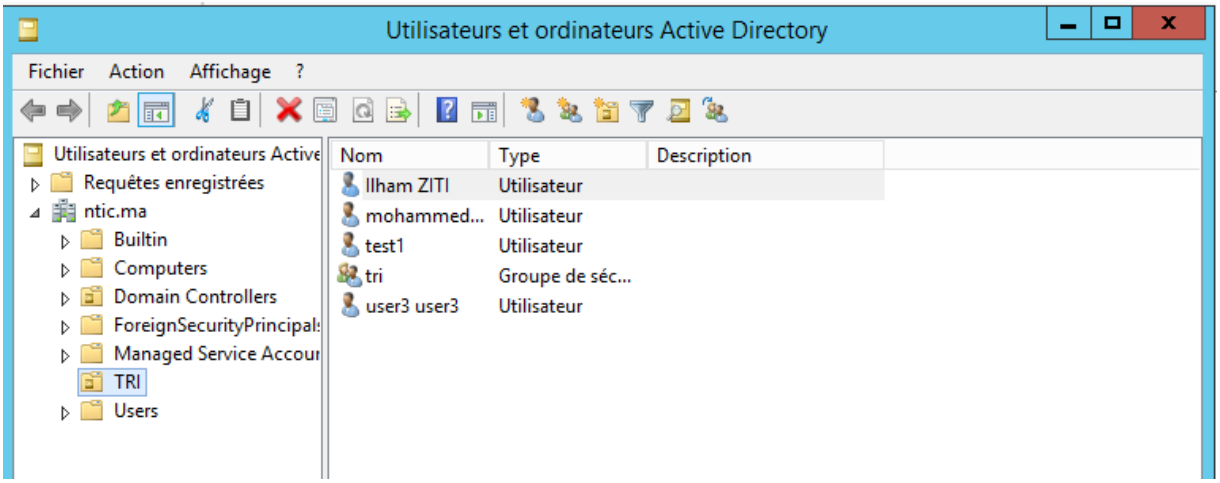
Saisir un mot de passe complexe, le mot de passe doit contenir au moins 7 caractères avec au moins 3 des éléments suivants : une majuscule, une minuscule, un nombre et un symbole



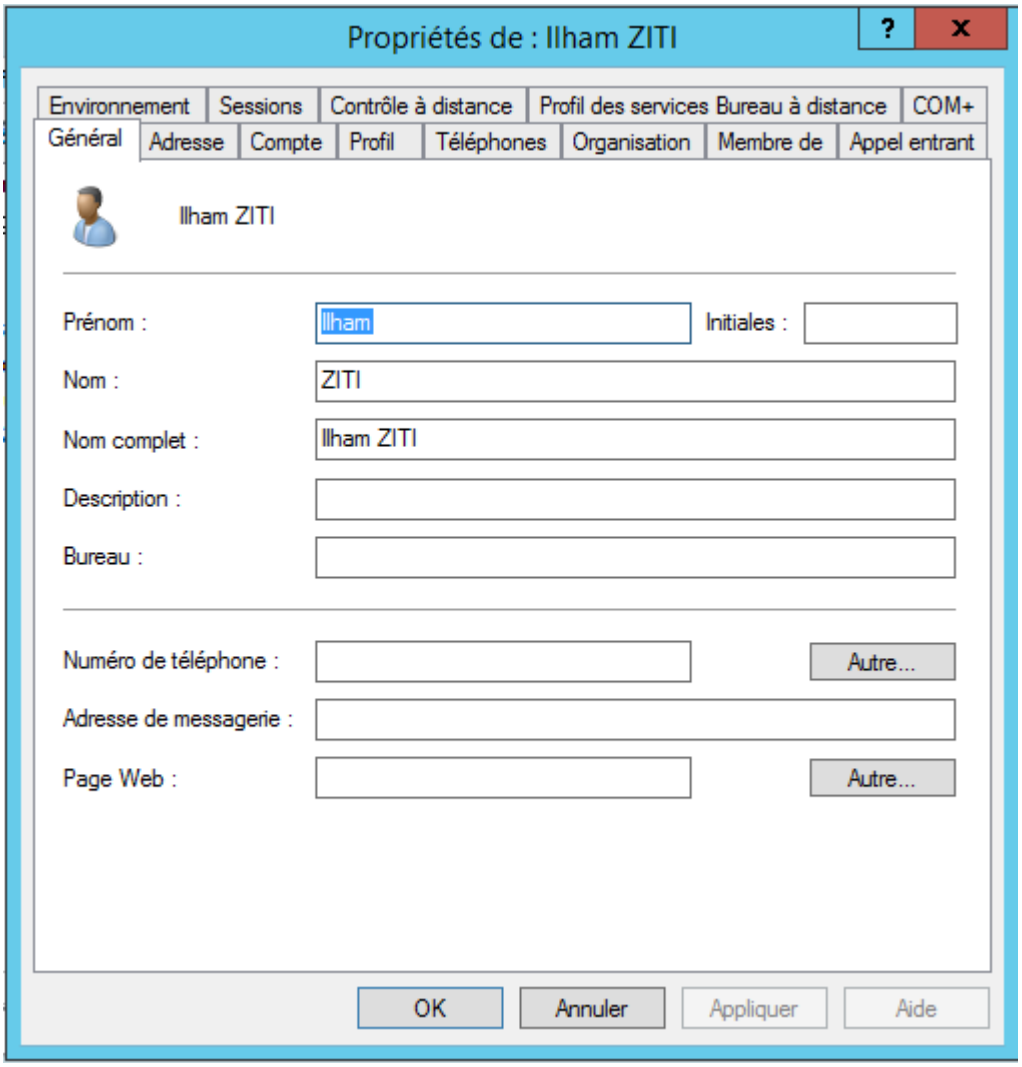
L'option L'utilisateur doit changer le mot de passe à la prochaine ouverture de session forcera l'utilisateur à changer le mot de passe transmis et entré ci-dessus à la première connexion sur le domaine. Après avoir entré le mot de passe, nous obtenons un résumé des informations de l'utilisateur.



Cliquer sur Terminer et l'utilisateur est créé.



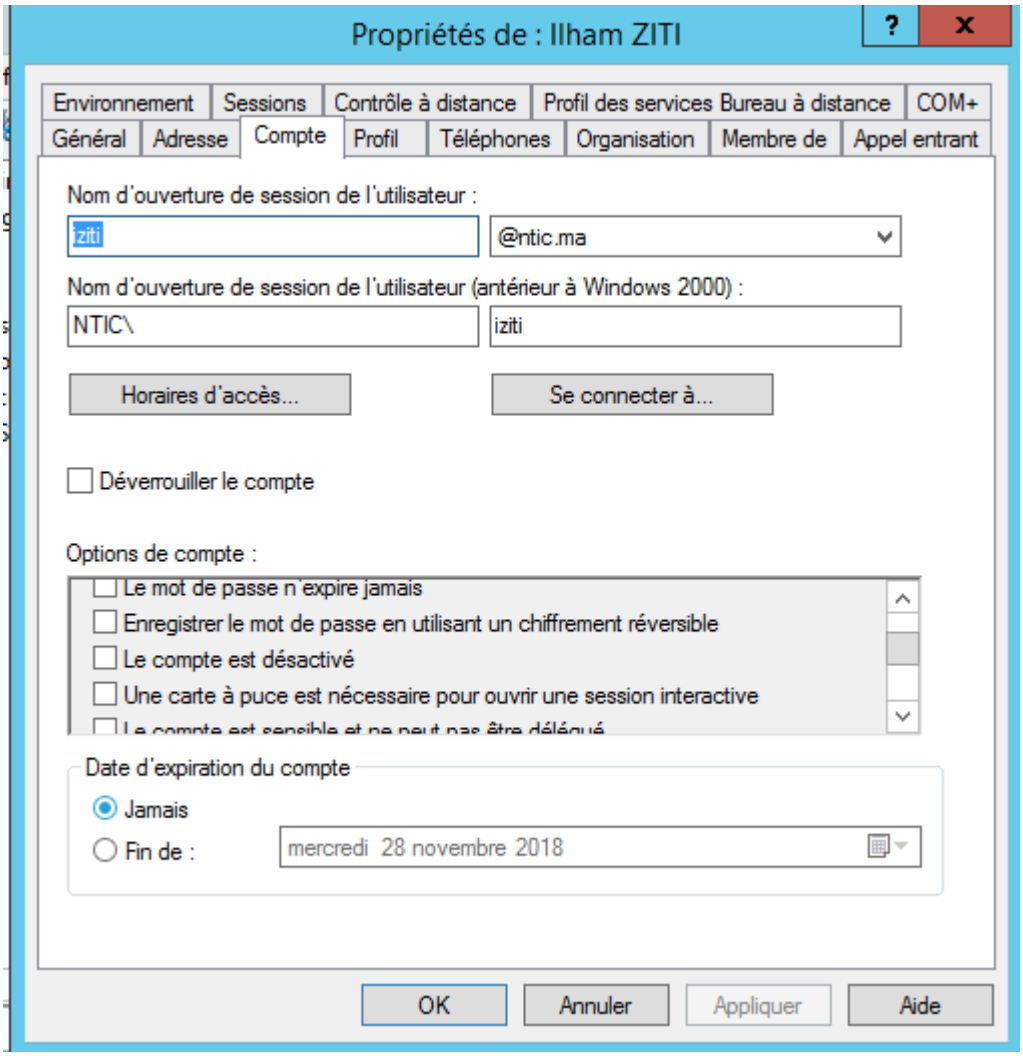
S'il on affiche les propriétés de l'utilisateur avec un clique droite puis **Propriétés** ou en double cliquant dessus, on voit que l'on a beaucoup plus d'informations que dans l'assistant. On peut alors remplir le bureau, le numéro de téléphone, etc. de l'utilisateur.



Dans l'anglet Compte on trouve :

- La partie liée à l'ouverture de la session

- Horaire d'accès : restriction des horaires d'accès
- Se connecter à : Restriction des ordinateur
- Verrouillage du compte
- Option de compte : Gestion de mot de passe, activation ou nom du compte, chiffrement,….
- Date d'expiration



3.2 PowerShell

Le nom du module est « **ADuser** ». Pour obtenir ces commandes vous pouvez utiliser la commande suivante :

```
get-command –noun ADUser
```

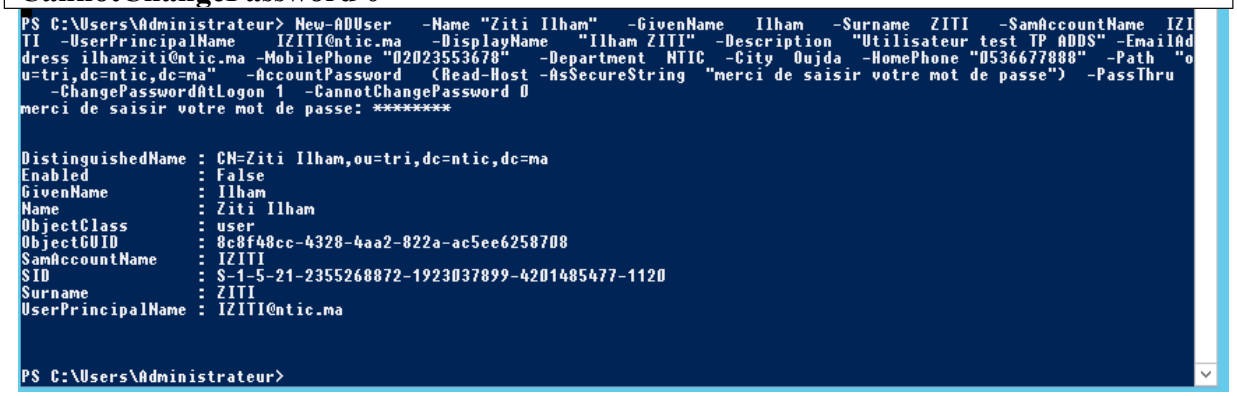
Pour afficher les options de chaque commande, par exemple « new-aduser »

```
Get-Help "new-aduser"
```

a. Ajoute un utilisateur

La commande qui permet d'ajouter un utilisateur « ZITI Ilham » avec plusieurs options :

New-ADUser -Name "Ziti Ilham" **-GivenName** Ilham **-Surname** ZITI **-SamAccountName** IZITI **-UserPrincipalName** IZITI@ntic.ma **-DisplayName** "Ilham ZITI" **-Description** "Utilisateur test TP ADDS" **–EmailAddress** ilhamziti@ntic.ma **-MobilePhone** "02023553678" **-Department** NTIC **-City** Oujda **-HomePhone** "0536677888" **-Path** "ou=tri,dc=ntic,dc=ma" **-AccountPassword** (Read-Host -AsSecureString "merci de saisir votre mot de passe") **-PassThru -PasswordNeverExpires** $true **-ChangePasswordAtLogon 1 -CannotChangePassword 0**



L'explication des options est présentée dans le tableau suivant

Options	Explication
Name	Spécifie le nom de l'objet.
GivenName	Spécifie le prénom de l'utilisateur
Surname	Spécifie le nom de famille
SamAccountName	Spécifie le nom du compte Security Account Manager (SAM)
UserPrincipalName	Spécifie le nom d'utilisateur, il a un nom d'utilisateur principal (UPN) au format <utilisateur> @ <nom-domaine-DNS>.
Description	Spécifie la description de l'objet
DisplayName	Spécifie le nom d'affichage de l'objet.
EmailAddres	Spécifie l'adresse mail de l'utilisateur
MobilePhone	Spécifie le numéro de téléphone mobile de l'utilisateur
HomePhone	Spécifie le numéro de téléphone fixe de l'utilisateur
Department	Spécifie le département de l'utilisateur
City	Spécifie la ville de l'utilisateur
AccountPassword	Spécifie une nouvelle valeur de mot de passe pour un compte. Cette valeur est stockée sous forme de chaîne cryptée.
PassThru	Retourne le nouvel objet ou l'objet modifié. Par défaut (c'est-à-dire si -PassThru n'est pas spécifié), cette applet de commande ne génère aucune sortie.
CannotChangePassword	Spécifie si le mot de passe du compte peut être modifié. Les valeurs possibles pour ce paramètre : $false or 0 ou $true or 1 L'exemple suivant montre comment définir ce paramètre pour que le mot de passe du compte puisse être modifié : -CannotChangePassword $false

ChangePasswordAtLogon	Spécifie si un mot de passe doit être modifié lors de la prochaine tentative d'ouverture de session Ce paramètre ne peut pas être défini sur $ true ou 1 pour un compte ayant également la propriété PasswordNeverExpires sur true
PasswordNeverExpires	Spécifie si le mot de passe d'un compte peut expirer ou non
Path	Spécifie le chemin de l'unité d'organisation ou du conteneur dans lequel le nouvel objet est créé.
ProfilePath	Spécifie un chemin d'accès au profil de l'utilisateur.
HomeDirectory	Spécifie le répertoire de base d'un utilisateur.Exemple : - HomeDirectory "\\ user\HomeDir"
HomeDrive	Spécifie un lecteur associé au chemin UNC défini par la propriété HomeDirectory.Exemple : -HomeDirectory "$Home" -HomeDrive "E"
AccountExpirationDate	L'heure par défaut est 12h00 (heure locale). La date par défaut est la date actuelle.Exemple : AccountExpirationDate " 05/01/2019 5:00:00 PM "

b. Activer et désactiver un compte utilisateur

Pour activer le compte iziti

```
Enable-ADAccount -Identity iziti
```

Pour désactiver le compte iziti

```
Disable-ADAccount -Identity iziti
```

c. Déverrouiller un compte d'utilisateur

Pour Déverrouiller le compte iziti

```
Unlock-ADAccount iziti
```

d. Supprimer un utilisateur

Pour supprimer le compte iziti

```
Remove-ADUser iziti
```

e. Recherche d'un utilisateur

Pour chercher tous les utilisateurs présents dans l'OU « utilisateurs »

```
get-ADUser -filter * -SearchBase " ou=tri,dc=ntic,dc=ntic"
```

```
PS C:\Users\Administrateur> Get-ADUser -filter * -SearchBase "ou=tri,dc=ntic,dc=ma"


DistinguishedName : CN=Ilham ZITI,OU=tri,DC=ntic,DC=ma
Enabled           : True
GivenName         : Ilham
Name              : Ilham ZITI
ObjectClass       : user
ObjectGUID        : c1859031-56c1-410f-a8b8-8bbd99a8c29e
SamAccountName    : iziti
SID               : S-1-5-21-2355268872-1923037899-4201485477-1157
Surname           : ZITI
UserPrincipalName : iziti@ntic.ma

DistinguishedName : CN=khadija Filali,OU=tri,DC=ntic,DC=ma
Enabled           : True
GivenName         : khadija
Name              : khadija Filali
ObjectClass       : user
ObjectGUID        : 20aba4a5-52cf-489f-a6f0-7d63779d3c94
SamAccountName    : khadija.filali
SID               : S-1-5-21-2355268872-1923037899-4201485477-1158
Surname           : Filali
UserPrincipalName : khadija.filali@ntic.ma


PS C:\Users\Administrateur>
```

Pour d'afficher les propriétés de l'utilisateur Ilham ZITI

get-ADUser iziti **-Properties** *

```
PS C:\Users\Administrateur> Get-ADUser  iziti -Properties *


AccountExpirationDate                :
accountExpires                       : 9223372036854775807
AccountLockoutTime                   :
AccountNotDelegated                  : False
AllowReversiblePasswordEncryption    : False
AuthenticationPolicy                 : {}
AuthenticationPolicySilo             : {}
BadLogonCount                        : 0
badPasswordTime                      : 0
badPwdCount                          : 0
CannotChangePassword                 : False
CanonicalName                        : ntic.ma/tri/Ilham ZITI
Certificates                         : {}
City                                 :
CN                                   : Ilham ZITI
codePage                             : 0
Company                              :
CompoundIdentitySupported            : {}
Country                              :
countryCode                          : 0
Created                              : 07/11/2018 12:34:10
createTimeStamp                      : 07/11/2018 12:34:10
Deleted                              :
Department                           :
Description                          :
DisplayName                          : Ilham ZITI
DistinguishedName                    : CN=Ilham ZITI,OU=tri,DC=ntic,DC=ma
Division                             :
DoesNotRequirePreAuth                : False
dSCorePropagationData                : {01/01/1601 01:00:00}
EmailAddress                         : iziti@gmail.com
EmployeeID                           :
EmployeeNumber                       :
Enabled                              : True
Fax                                  :
GivenName                            : Ilham
HomeDirectory                        :
HomedirRequired                      : False
HomeDrive                            :
HomePage                             :
HomePhone                            :
Initials                             :
```

3.3 Commande DS

a. Ajouter un utilisateur

La commande **DSADD user** permet de créer un utilisateur avec tous les paramètres qui s'y rattache.

dsadd user "cn=IZITI,ou=tri,dc=ntic,dc=ma" **-fn** "Ilham" **-ln** "ZITI" **–samid** iziti **-pwd** * -**mustchpwd** yes **-memberof** "cn=groupe,ou=tri,dc=ntic,dc=ma" **-disabled** no

Paramètres	Signification
samid	Sam account name
upn	User principal name
fn	First name (Prénom)
Ln	Last name (Nom)
pwd Mot de Passe ou *	Mot de passe, * vous invite à saisir un mot de passe
memberof	Faisant partie du groupe
hmdir	Répértoir de base
hmdrv	Lettre du lecteur, fonctionne avec l'option hmdir
Profile	Chemin du profile
Mustchpwd yes ou non	Doit changer le mot de passe
Pwdneverexpires yes ou non	Mot de passe n'expire jamais
Disabled yes ou non	Le compte doit être activé ou non

Pour plus de détails, sous l'invite de commande taper :DSADD USER / ?

b. Modifier un compte d'utilisateur

Pour ajouter ou modifier la valeur du numéro de téléphone de l'utilisateur iziti

```
dsmod user "cn=IZITI,ou=tri,dc=ntic,dc=ma" -tel 061234567
```

c. Activer ou désactiver un compte utilisateur

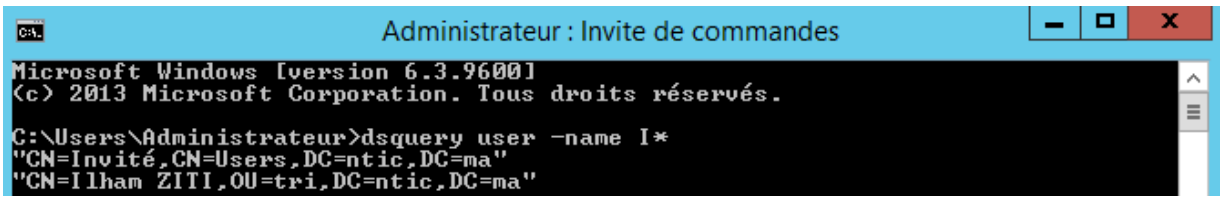
Pour activer ou désactive le compte

```
dsmod user " cn=IZITI,ou=tri,dc=ntic,dc=ma " -desabled  yes/no
```

d. Rechercher un utilisateur

Pour afficher tous les utilisateur dont le nom commence par I

```
dsquery user -name I*
```



e. Supprimer un utilisateur

```
dsrm  "cn=IZITI,ou=tri,dc=ntic,dc=ma"
```



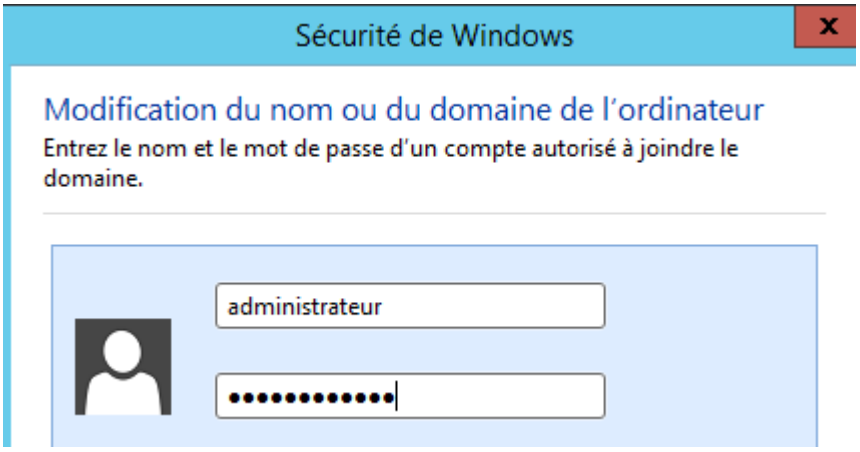
4. Test : Joindre un domaine Active Directory

Au début assurez-vous que le poste client reçoit en serveur DNS celui de votre domaine Active Directory.

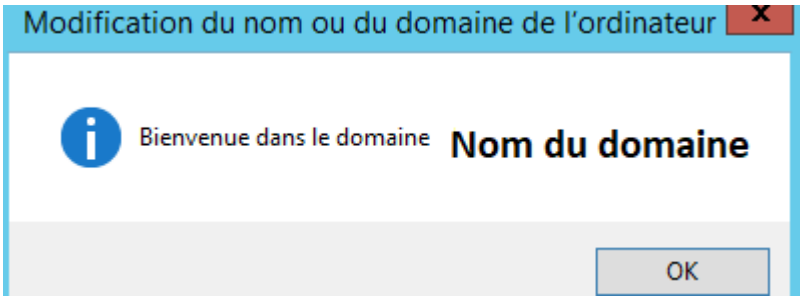
Pour ajouter un poste client dans le domaine Active Directory suivre les étapes :

Panneau de configuration - Système - Paramètres système avancés
- Nom de l'ordinateur - Modifier
- Sélectionner Domaine
- Saisir le nom de domaine

Saisir vos informations d'identification sur le domaine (le compte doit disposer des privilèges nécessaires pour joindre le domaine)



Après quelques instants, vous obtenez le message suivant :



Redémarrer le poste pour finir la configuration

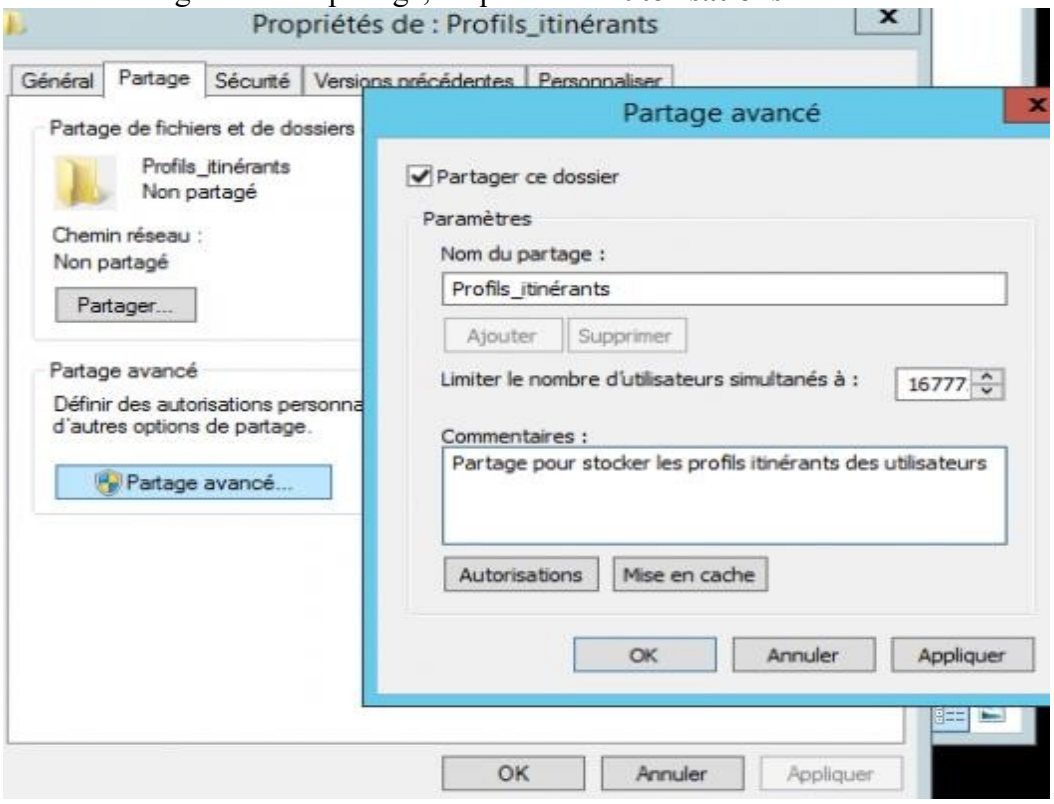
5. Profils itinérants graphiquement

Le **profils** itinérant permet de synchroniser le profil d'un utilisateur sur un serveur pour rendre ces données accessible depuis l'ensemble du réseau local.

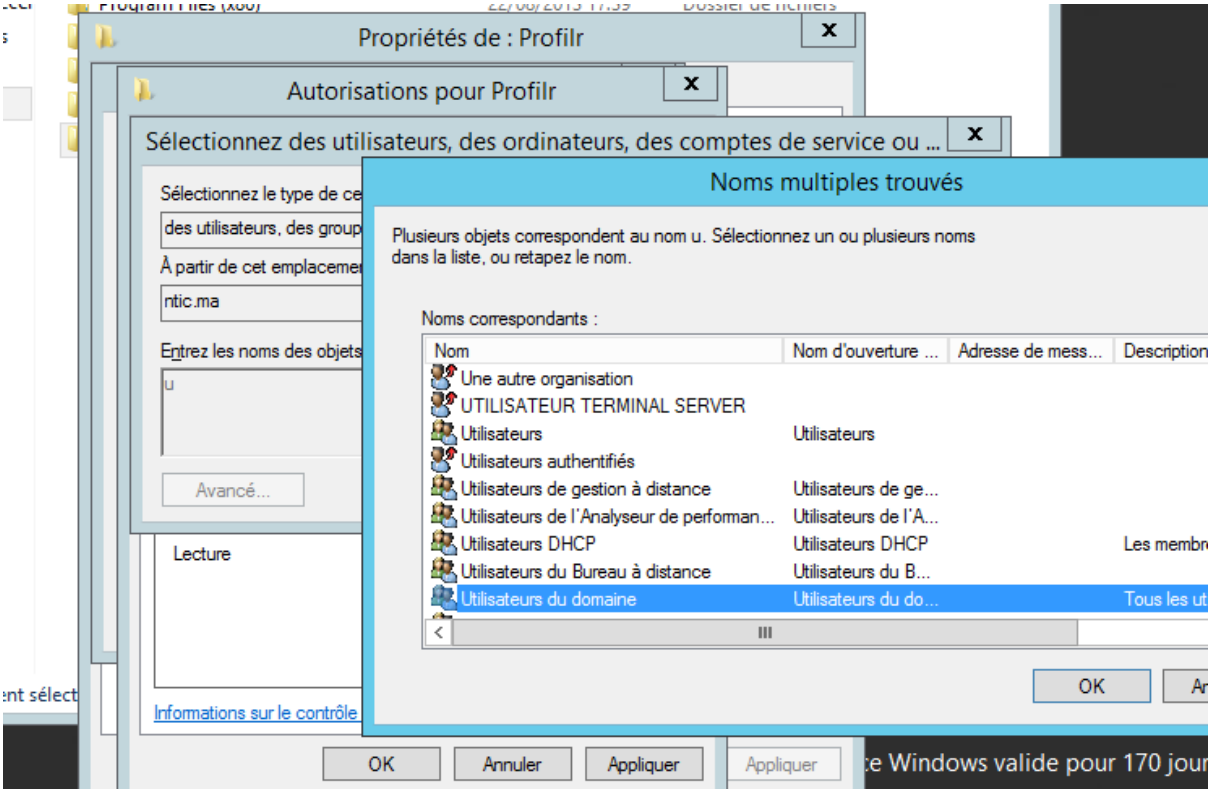
5.1 Configuration

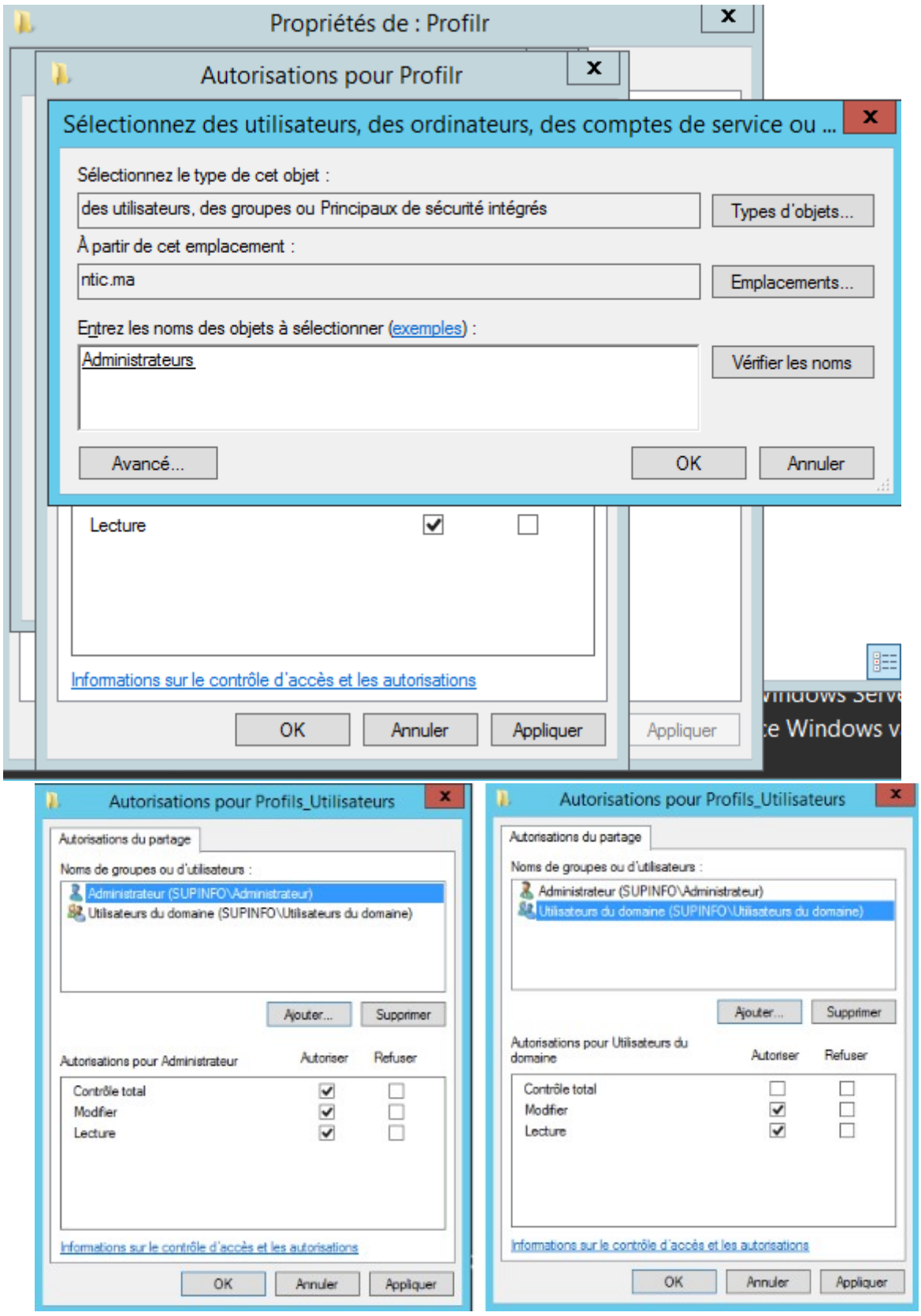
La première étape consiste à créer un répertoire que nous allons partager et qui servira à stocker les données des profils. Par exemple, pour ma part je crée répertoire nommé "**Profils_itinérants**" que je partage sous le même nom.

Dans la configuration du partage, cliquez sur "**Autorisations**"



Attribuer le contrôle tôtal à l'administrateur et les droits de lecture/ecriture aux utilisateurs du domaine



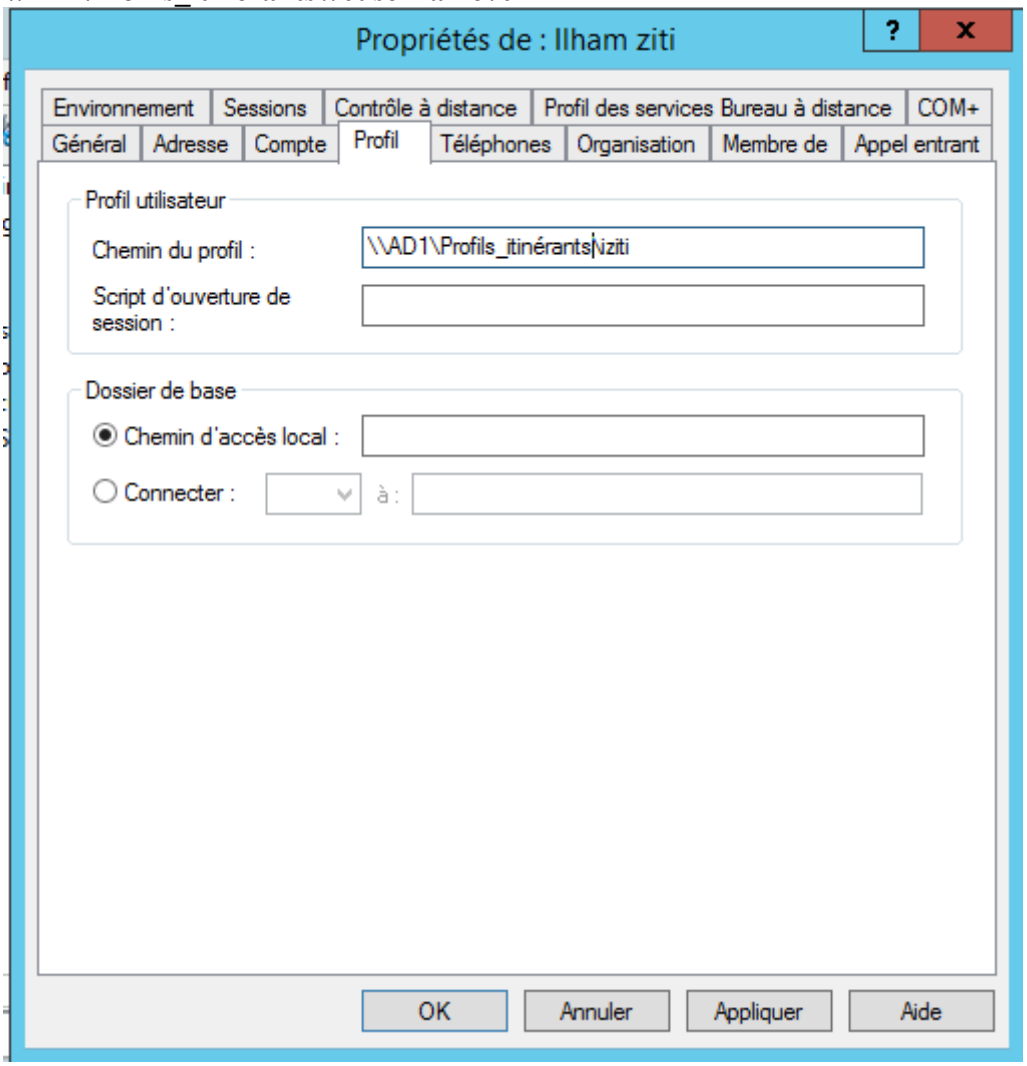


Effectuer un clic droit sur un utilisateur qui doit disposer d'un profil itinérant, cliquer sur "**Propriétés**". Accédez à l'onglet "**Profil**" et au niveau du champ "**Chemin du profil**", indiquer :

\\Nom du serveur AD\Nom du repertoire\%username%

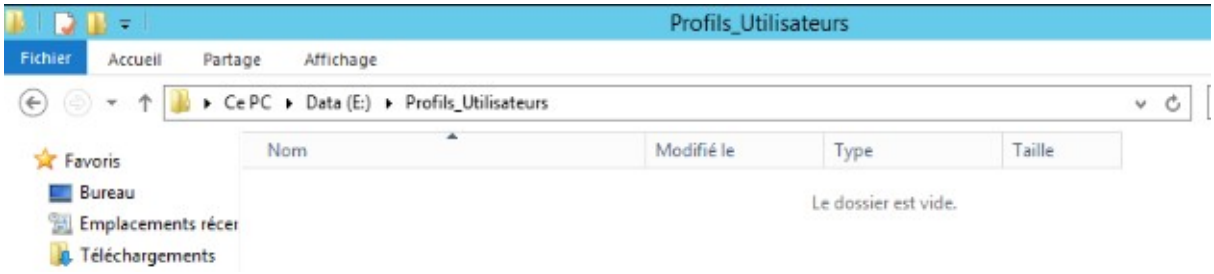
Dans notre exemple la ligne ressemble à cela :

\\AD1\Profils_itinérants\%username%



5.2 Test

A ce moment notre dossier partagé est vide.



Sur la machine n°1:

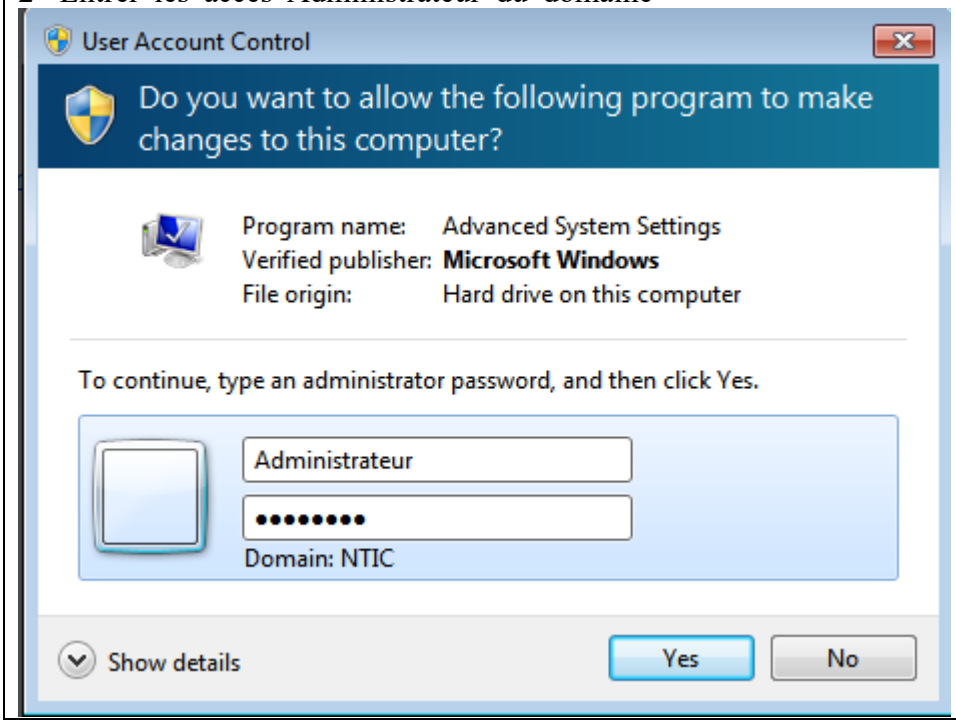
- ouvrir la session iziti

- Vérifier que l'utilisateur est en état Profils (Roaming) :

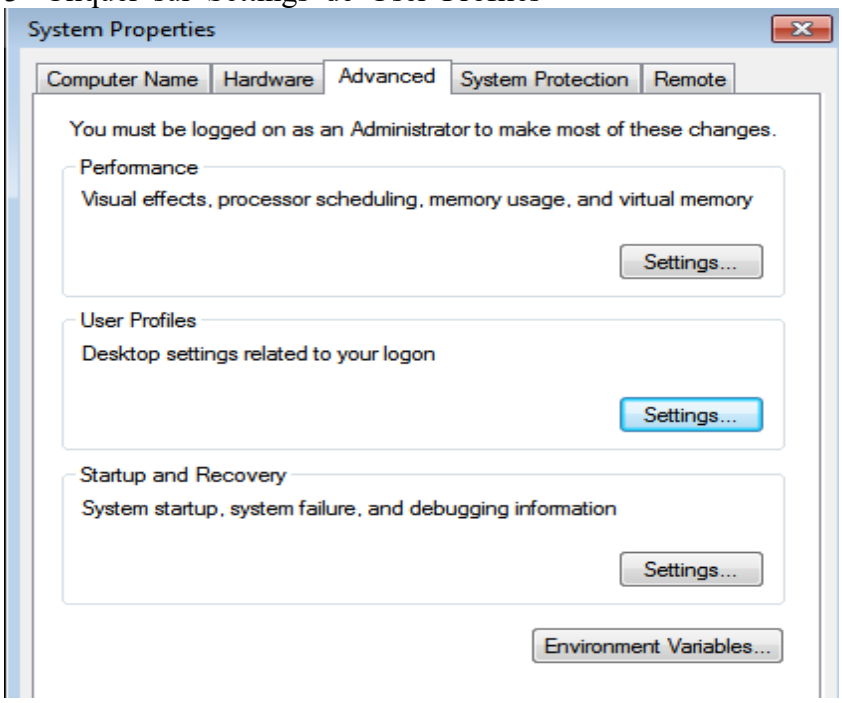
1-Cliquer sur Advanced system settings du Propriété du PC



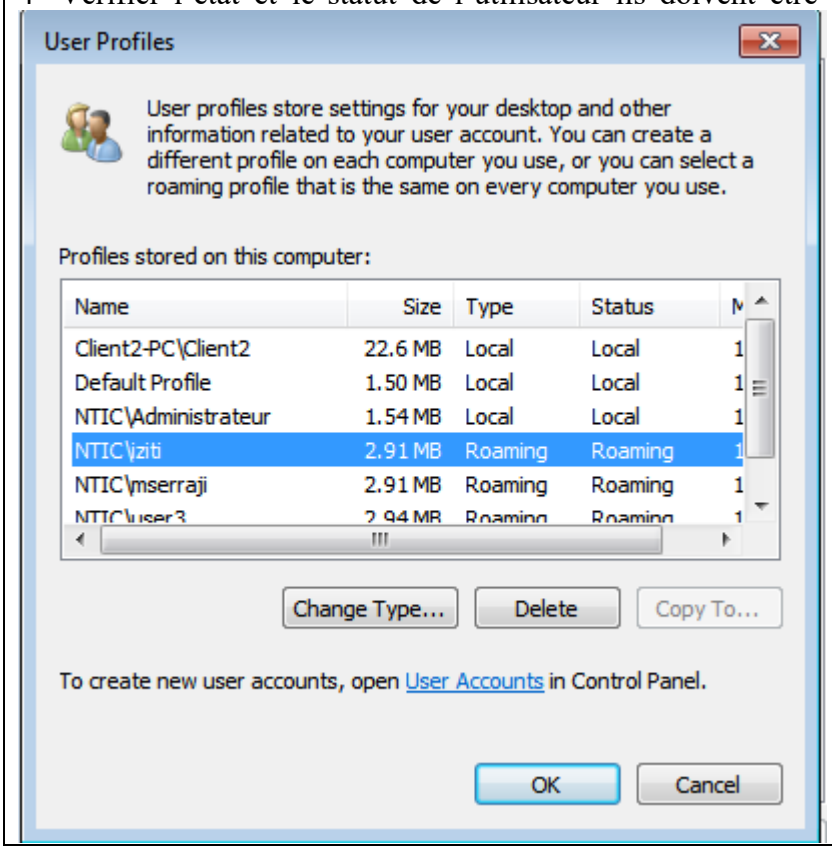
2- Entrer les accès Administrateur du domaine



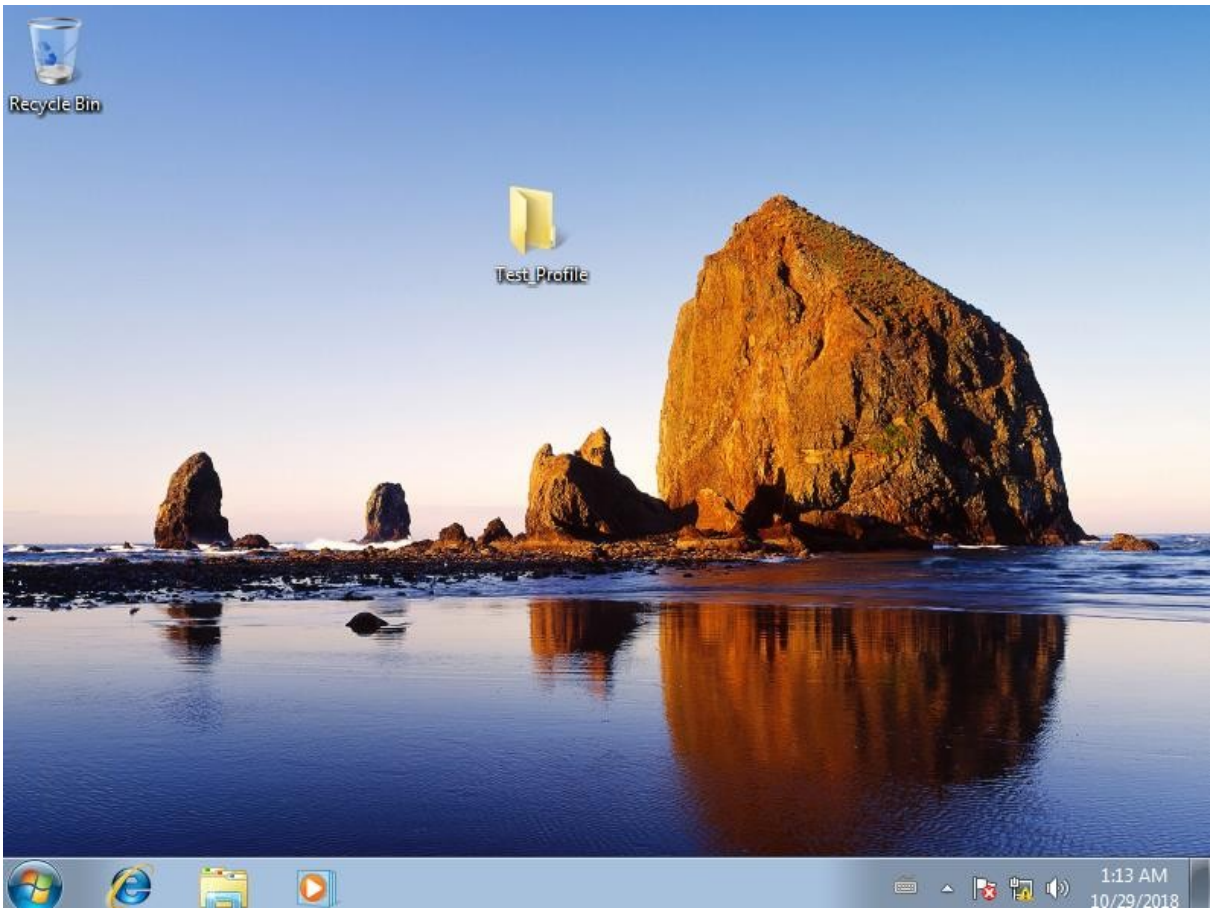
3- Cliquer sur Settings de User Profiles



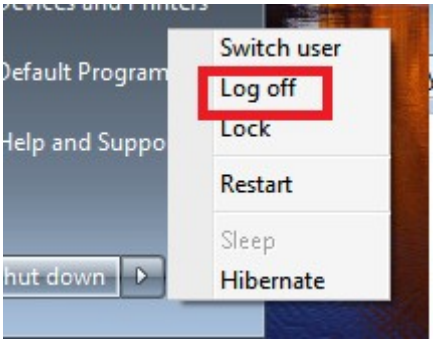
4- Vérifier l'état et le statut de l'utilisateur ils doivent être égale à **Roaming**



Effectuer des modifications : Exemple changement arrière-plan un fichier test1.txt sur le bureau, création d'un nouveau dossier , ….

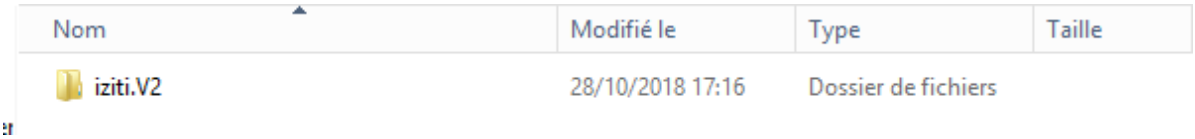


- Fermer la session



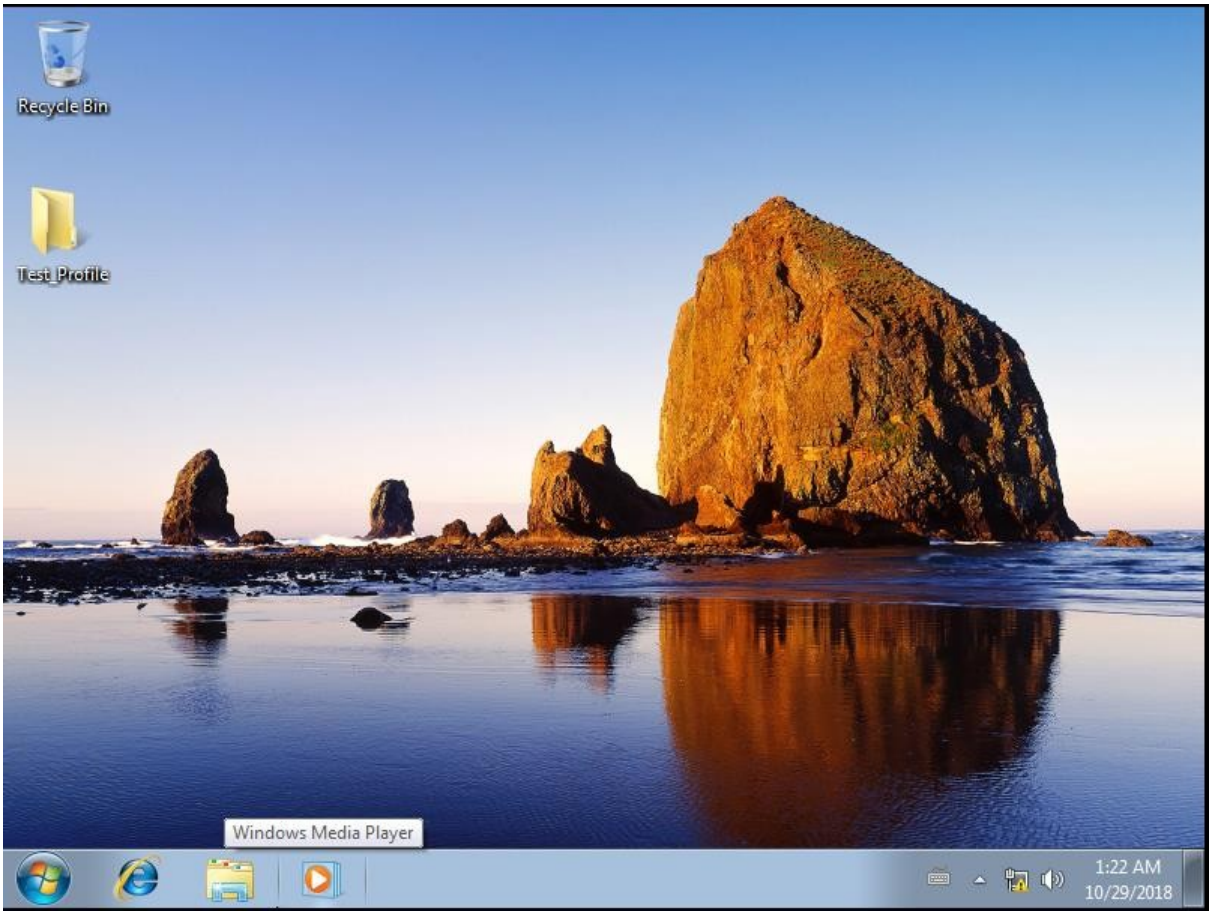
Sur le serveur Active Directory:

Observer le contenu du dossier "Profils_Utilisateurs" *(***un dossier contenant le profil iziti a été crée)**



Sur la machine n°2:

- Ouvrir la session iziti
- Observer les modifications présente sur le bureau



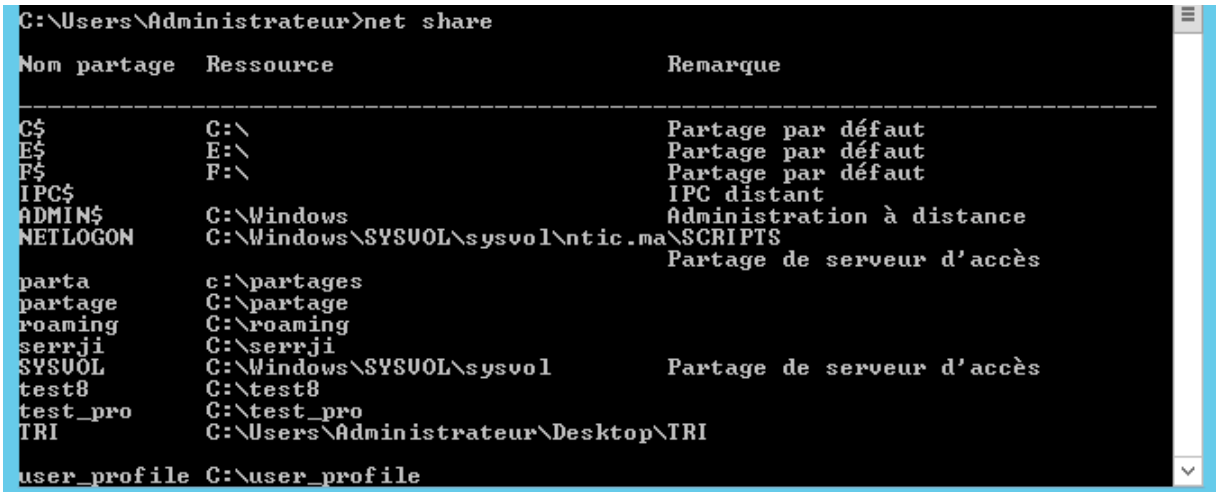
6. Profils itinérants en ligne de commande

6.1 Partager un répertoire

La commande **net share** permet de gérer les ressources partagée

Pour afficher des informations concernant toutes les ressources partagées sur l'ordinateur, tapez :

```
net share
```



Pour partager le répertoire C:\Données d'un ordinateur avec le nom de partage **ressources** et donner tous les droit à tout le monde

net share Ressources =**C:** Donnees **/GRANT:** "tout le monde,FULL"

Pour mettre fin au partage du dossier **ressources** créé par l'exemple précédent, tapez :

net share ressources /delete

6.2 Créer un utilisateur profile

a. Commande DS

dsadd user "cn=IZITI,ou=tri,dc=ntic,dc=ma" -fn "Ilham" -ln "ZITI" –samid iziti -pwd * -mustchpwd yes **-hmdir** C:\ **Donnees -profil \\AD1\Ressource** -disabled no

b. Commande PowerShell

New-ADUser -Name "Ziti Ilham" -GivenName Ilham -Surname ZITI -SamAccountName IZITI -UserPrincipalName IZITI@ntic.ma -Path "ou=tri,dc=ntic,dc=ma" **–ProfilePath \\AD1\Ressource - HomeDirectory** C:\ **Donnees** -AccountPassword (Read-Host -AsSecureString "merci de saisir votre mot de passe") -PassThru -ChangePasswordAtLogon 1

7. Gestion groupe

7.1 Présentation

Les es groupes sont créés pour donner des droits sur des fichiers, imprimantes, base de données, etc ..

Les groupes sont caractérisé par leurs étendue et leur type

a. Etendu du groupe

- **Domaine local** : Les membres de ces groupes ne peuvent recevoir des autorisations qu'au sein d'un domaine. Les groupes avec une étendue de domaine local vous permettent de définir et de gérer l'accès aux ressources dans un seul domaine.

- **Globale** :Les membres des groupes globaux peuvent inclure d'autres groupes et comptes provenant uniquement du domaine où le groupe est défini. Les membres de ces groupes peuvent recevoir des autorisations dans n'importe quel domaine de la forêt. Les groupes à étendue globale ne sont pas répliqués à l'extérieur de leur propre domaine, vous pouvez modifier fréquemment les comptes

- **Universelle** :Les membres des groupes universels peuvent inclure d'autres groupes et comptes provenant des domaines de la forêt ou de l'arborescence de domaine. Les membres de ces groupes peuvent recevoir des autorisations dans n'importe quel domaine de la forêt ou de l'arborescence de domaine.

b. Type de groupe

Il existe deux types de groupes : distribution et sécurité.

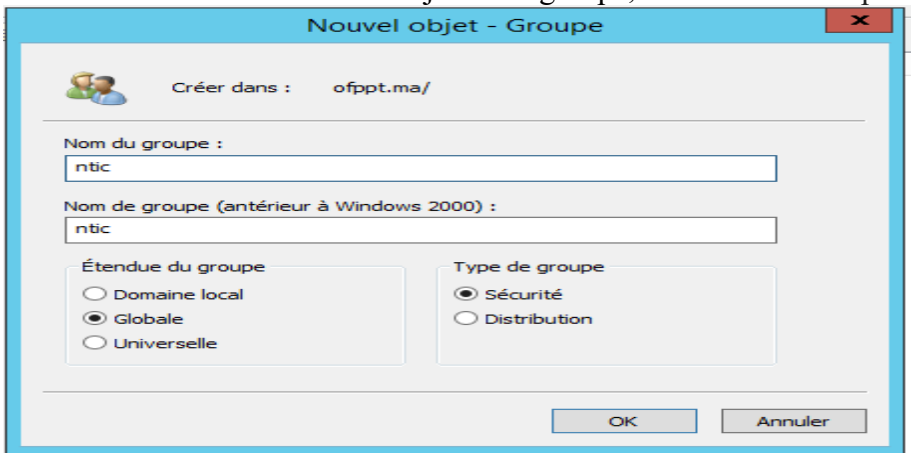
Les groupes de **distribution** sont utilisés pour créer des listes de distribution électronique Les groupes de **sécurité** sont utilisés pour affecter des autorisations à des ressources partagées. Les groupes de distribution ne sont pas sécurisés, ce qui signifie qu'ils ne peuvent pas être répertoriés dans les listes de contrôle d'accès discrétionnaire (DACL).

Les groupes de sécurité permettent :

- Assigner des droits d'utilisateurs à des groupes de sécurité dans AD DS.
- Affecter des autorisations aux groupes de sécurité sur des ressources.

7.2 Graphiquement

Sélectionner l'unité dont il faut ajouter le groupe, bouton de droite puis *Nouveau* et *Groupe*.

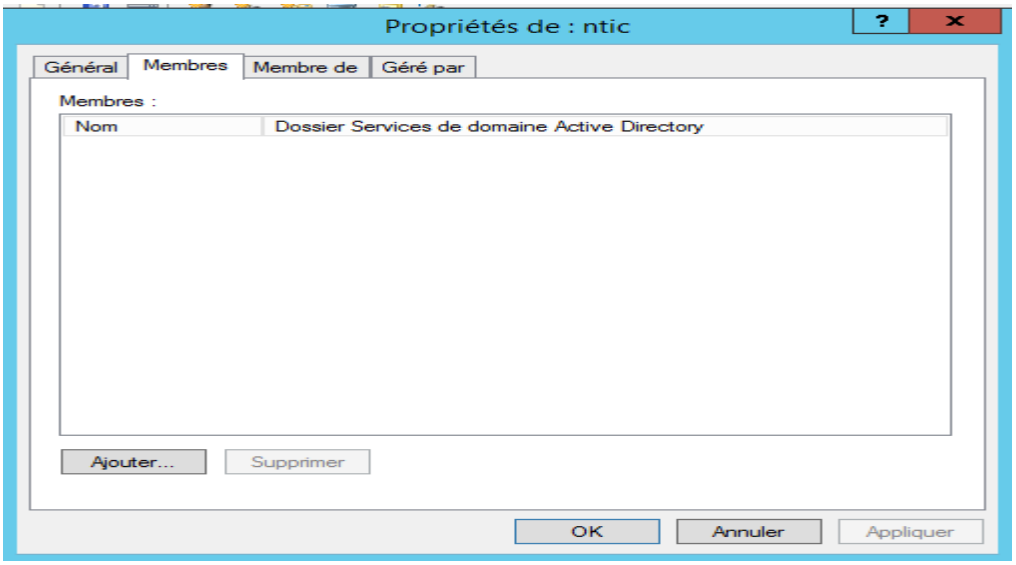


On rappelle brièvement les choix possible dans l'encadré *Étendue du groupe* et *Type de groupe*.

Dans notre cas, nous avons un groupe d'utilisateur. Nous allons choisir l'étendu du groupe Globale car nous avons un assez fréquent aux informations et le type de groupe Sécurité afin d'accéder à des partages.

Dans ce groupe ntic, nous allons ajouter des utilisateurs. Dans les propriétés ou en double cliquant sur le groupe voulu, nous pouvons nous rendre l'onglet *Membres* et ajouter les membres que l'on souhaite. On clique sur *Ajouter…* puis sur *Avancé…* et on recherche nos utilisateurs.

On peut également taper directement le nom dans *les noms des objets à sélectionner* puis *Vérifier les noms*



7.3 Commande DS

a. Ajouter un groupe

Pour créer un groupe nommée group1 dans l'unité TRI, Etendue : domaine locale , Type :Sécurisé

dsadd group "cn=group2,ou=TRI,dc=ntic,dc=ma" **-secgrp** yes **–scope** L

```
C:\Users\Administrateur>dsadd group "cn=group2,ou=TRI,dc=ntic,dc=ma" -secgrp yes
 -scope L
dsadd réussite:cn=group2,ou=TRI,dc=ntic,dc=ma

C:\Users\Administrateur>_
```

Pour créer un groupe nommée group2 dans l'unité TRI, Etendue : domaine Globale et dont member l'utilisateur iziti

dsadd group "cn=group2,ou=TRI,dc=ntic,dc=ma" **-secgrp** yes **–scope** G **–members** "cn=iziti,ou=TRI,dc=ntic,dc=ma"

```
C:\Users\Administrateur>dsadd group "cn=g1,ou=TRI,dc=ntic,dc=ma" -secgrp yes -sc
ope G -members  "cn=iziti,ou=TRI,dc=ntic,dc=ma"
dsadd réussite:cn=g1,ou=TRI,dc=ntic,dc=ma

C:\Users\Administrateur>
```

Pour créer un groupe membre d'un autre groupe utiliser l'option memberof

Il faut faire attention à l'étendue du groupe en effet un groupe local ne peux pas etre memebre du groupe global (voir la partie introduction des groupe)

dsadd group "cn=group1,ou=TRI,dc=ntic,dc=ma" **-secgrp** yes **–scope** G **–memberof** "cn=groupe1,ou=TRI,dc=ntic,dc=ma"

```
C:\Users\Administrateur>dsadd group "cn=groupe3,ou=TRI,dc=ntic,dc=ma" -secgrp ye
s -scope G -memberof  "cn=group1,ou=TRI,dc=ntic,dc=ma"
dsadd réussite:cn=groupe3,ou=TRI,dc=ntic,dc=ma
```

Option	Description
secgrp	Un groupe de sécurité (yes) ou un groupe de distribution (no) par défaut = yes
scope	Domain local = L, global = g, universal =u. Par default=g.
memberof	Ajouter le nouveau groupe à d'autres groupes
members	Membres à ajouter à ce nouveau groupe

b. Modifier un groupe

Pour modifier par exemple l'étendue du groupe « groupe2 » en domaine local

Dsmod group "cn=group2,ou=TRI,dc=ntic,dc=ma" **-scope** L

On peut modier le type « secgrp », la discription « desc »,…. (pour plus d'information utiliser dsmod group / ?)

c. Chercher un groupe

Chercher les groupes dont le nom commence par G

Dsquery group –name g*

```
C:\Users\Administrateur>Dsquery   group   -name g*
"CN=g1,OU=tri,DC=ntic,DC=ma"
"CN=Générateurs d'approbations de forêt entrante,CN=Builtin,DC=ntic,DC=ma"
"CN=group1,OU=tri,DC=ntic,DC=ma"
"CN=Groupe d'accès d'autorisation Windows,CN=Builtin,DC=ntic,DC=ma"
"CN=Groupe de réplication dont le mot de passe RODC est autorisé,CN=Users,DC=nti
c,DC=ma"
"CN=Groupe de réplication dont le mot de passe RODC est refusé,CN=Users,DC=ntic,
DC=ma"
"CN=groupe2,OU=tri,DC=ntic,DC=ma"
"CN=groupe3,OU=tri,DC=ntic,DC=ma"

C:\Users\Administrateur>
```

d. Voir les groupes qu'un user appartient

dsget user "cn=iziti,ou=TRI,dc=ntic,dc=ma" **– memberof**

```
C:\Users\Administrateur>dsget user "cn=iziti,ou=tri,dc=ntic,dc=ma"  -memberof
"CN=groupe2,OU=tri,DC=ntic,DC=ma"
"CN=g1,OU=tri,DC=ntic,DC=ma"
"CN=Utilisateurs du domaine,CN=Users,DC=ntic,DC=ma"
```

e. Supprimer un groupe

dsrm "cn=group1,ou=tri,dc=ntic,dc=ma"

7.4 Commande Powershell

a. Ajouter un groupe

Pour créer un nouveau groupe global de type sécurité dans l'unité « tri »utiliser la commande suivante

New-ADGroup **-name** "Stagiaire" **-Path** "ou=tri,dc=ntic,dc=ma" **-GroupCategory** Security **-groupscope** Global

```
PS C:\Users\Administrateur> New-ADGroup     -name   "Stagiaire"      -Path  "ou=tri,dc=ntic,dc=ma"     -GroupCategory Se
curity   -groupscope   Global
PS C:\Users\Administrateur> _
```

Option	Explications
name	Nom du groupe
Path	Emplacement du groupe
GroupCategory	Type de groupe Distribution ou Security
Groupscope	L'étendue du groupe : DomainLocal, Global, Universal

Pour ajouter l'utilisateur « iziti» au groupe « stagiaire »

Add-ADGroupMember **-Identity** "Stagiaire" **-Member** "iziti"

```
$ C:\Users\Administrateur> Add-ADGroupMember -Identity stagiaire -Members iziti
$ C:\Users\Administrateur>
```

La même commande si on veut ajouter un autre groupe au groupe « stagaire »

Add-ADGroupMember **-Identity** "Stagiaire" **-Members** StageOujda,StageRabat

b. Modifier Groupe

Pour modifier par exemple le type du groupe « Stagiaire »

Set-ADGroup -Identity "cn=stagiaire,ou=tri,dc=ntic,dc=ma" **-GroupCategory** Distribution

c. Supprimer un groupe

Remove-ADGroup stagiaire

8. Gestion ordinateur

8.1 Commande DS

a. Ajouter un ordinateur

Pour ajouter un ordinateur PC1 dans l'unité « tri » et emplacement « direction »

dsadd computer “cn=PC1,ou=TRI,dc=ntic,dc=ma” **–loc** Direction

```
PS C:\Users\Administrateur> dsadd computer  "cn=PC1,ou=tri,dc=ntic,dc=ma" -loc  Direction
dsadd réussite:cn=PC1,ou=tri,dc=ntic,dc=ma
PS C:\Users\Administrateur>
```

b. Chercher un ordinateur

Chercher les groupes de l’unité TRI

dsquery computer “ou=TRI,dc=ntic,dc=ma”

c. Supprimer un ordinateur

dsrm “cn=PC1,ou=TRI,dc=ntic,dc=ma”

8.2 Commande PowerShell

a. Ajouter un ordinateur

Pour ajouter un ordinateur PC1 dans l’unité « tri » et emplacement « direction »

New-ADComputer **-Name** "PC1" -SamAccountName "PC1" **-Path** "OU=tri,DC=ntic,DC=ma" **-Enabled** $true **-Location** "Direction"

```
PS C:\Users\Administrateur> New-ADComputer     -Name "PC2"    -SamAccountName "PC2"   -Path "OU=tri,DC=ntic,DC=ma"   -En
abled   $true    -Location    "Direction"
PS C:\Users\Administrateur>
```

b. Chercher des ordinateurs du domaine

De la même façon que les groupes et utilisateurs

```
PS C:\Users\Administrateur> Get-ADComputer -Filter *


DistinguishedName : CN=AD1,OU=Domain Controllers,DC=ntic,DC=ma
DNSHostName       : AD1.ntic.ma
Enabled           : True
Name              : AD1
ObjectClass       : computer
ObjectGUID        : 8511de8c-3c7b-48a6-b95a-f0a7332b0e05
SamAccountName    : AD1$
SID               : S-1-5-21-2355268872-1923037899-4201485477-1001
UserPrincipalName :

DistinguishedName : CN=AD2,OU=Domain Controllers,DC=ntic,DC=ma
DNSHostName       : AD2.ntic.ma
Enabled           : True
Name              : AD2
ObjectClass       : computer
ObjectGUID        : bbd7968c-ec01-4d8a-a4e8-8ae62b2dcba2
SamAccountName    : AD2$
SID               : S-1-5-21-2355268872-1923037899-4201485477-1105
UserPrincipalName :

DistinguishedName : CN=AD5,OU=Domain Controllers,DC=ntic,DC=ma
DNSHostName       : AD5.ntic.ma
Enabled           : True
Name              : AD5
ObjectClass       : computer
ObjectGUID        : c8e82932-2264-40c8-95c0-ad441cea80df
SamAccountName    : AD5$
SID               : S-1-5-21-2355268872-1923037899-4201485477-1110
UserPrincipalName :

DistinguishedName : CN=CLIENT-PC,CN=Computers,DC=ntic,DC=ma
DNSHostName       : CLIENT-PC.ntic.ma
Enabled           : True
Name              : CLIENT-PC
ObjectClass       : computer
ObjectGUID        : a04d0eb4-262d-4689-ab47-633253805e9a
SamAccountName    : CLIENT-PC$
SID               : S-1-5-21-2355268872-1923037899-4201485477-1603
```

c. Supprimer un ordinateur

```
Remove-ADComputer  -Identity  "cn=PC1,ou=tri,dc=ntic,dc=ma"
```

9. Reference

https://www.it-connect.fr/active-directory-creer-des-profils-itinerants-pour-ses-utilisateurs/

https://www.supinfo.com/articles/single/1922-creer-profils-itinerants