**Programmation d’un utilisateur dans l'Active Directory**

Ce laboratoire doit être fait individuellement sur l'ordinateur virtuel 2

**Objectifs**

* Utiliser PowerShell dans le cadre de la création d’objets d’un domaine
* Créer un objet utilisateur dans votre domaine

**Étape 1 - Mise en place**

L’arborescence des unités d’organisation du domaine Formation.Local doit être déjà créée.

**Étape 2 - Introduction au cmdlet New-ADuser**

Le paramètre -Name est le seul paramètre obligatoire de New-ADUser.

Voici la commande la plus simple pour créer un utilisateur: **New-ADUser -Name TOTO**

* Le compte est créé mais il est désactivé.
* L'utilisateur doit changer le mot de passe à l'ouverture de session
* L'utilisateur TOTO est créé dans le conteneur "Users".

La valeur de l'attribut **samAccountName** est identique au paramètre **-Name** de **New-ADUser**.

**Je vous suggère de ne pas utiliser le paramètre -SamAccountName avec le cmdlet New-ADuser.**

**Étape 3 - Création d'un utilisateur avec le cmdlet New-ADuser**

Écrire un programme en PowerShell pour créer un utilisateur dans l'unité d'organisation TEST.

Votre code doit utiliser les cmdlets du module ActiveDirectory et des variables autant que possible.

Le mot de passe de l'utilisateur sera AAAaaa111

**$mdp = ConvertTo-SecureString -AsPlainText "AAAaaa111" -Force**

Voici les propriétés de l'onglet "**Général**" du nouvel utilisateur

* Prénom: JOHN
* Nom: DOE
* Nom complet: JOHN DOE
* Description: Utilisateur de la OU TEST
* Bureau: Informatique
* Numéros de téléphone du bureau: 514-999-6000
  + 514-999-7000, 514-999-8000
* Adresse de messagerie: JOHN.DOE@FORMATION.LOCAL
* Page WEB: www.formation.local

Voici les propriétés de l'onglet "**Adresse**" du nouvel utilisateur

* Pays: Canada

**note: un pays est constitué de trois attributs**

Voici les propriétés de l'onglet "**Compte**" du nouvel utilisateur

* Nom d'ouverture de session de l'utilisateur: JOHN.DOE@FORMATION.LOCAL
* Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000): FORMATION\JOHN.DOE
* Le mot de passe n’expire jamais: OUI
* Le compte est désactivé: NON

Voici les propriétés de l'onglet "**Téléphones**" du nouvel utilisateur

* Téléphone à domicile: 450-222-2222
* Téléphone mobile: 450-333-3333
* Télécopie: 450-444-4444

Au début de votre script de création de l’utilisateur ajouter une ligne de code qui va détruire votre utilisateur.

Votre code doit utiliser un "Try and Catch" pour ne pas afficher les messages d'erreurs de PowerShell.

Dans la section "Catch" vous devez utiliser le nom complet de l'erreur lorsqu'un objet de l'Active Directory n'existe pas.

**Étape 4 - Validation**

Après la création de l'utilisateur, vous devez vérifier les valeurs de chacune des propriétés dans l’onglet "Éditeur d’attribut" de ce nouvel utilisateur

Une fois toutes les propriétés exactes, vérifier la fonctionnalité de votre utilisateur en vous connectant.

**Pour "changer d’utilisateur" vous pouvez exécuter TSDISCON.EXE**

**Il est important de fermer la session d’un utilisateur si votre intention est de modifier son objet.**

**Par défaut, les utilisateurs qui ne sont pas membre du groupe "Administrateurs" ne peuvent pas se connecter au serveur membre si on utilise le mode de session étendu.**

Pour la solution à ce problème, voir la dernière page de ce document.

**ANNEXE - Une liste de plusieurs cmdlets pour gérer un utilisateur**

* Get-ADuser
* New-ADuser
* Remove-ADuser
* Set-ADuser
* Clear-ADAccountExpiration
* Disable-ADAccount
* Enable-ADAccount
* Search-ADAccount

**note: permet de chercher des comptes utilisateurs selon plusieurs critères**

* Set-ADAccountControl
* Set-ADAccountExpiration
* Set-ADAccountPassword

**note: permet de modifier le mot de passe d'un utilisateur**

* Unlock-ADAccount

**Exemples**

# Trouver les comptes utilisateurs dont le mot de passe n'expire jamais

Search-ADAccount -PasswordNeverExpires

# Trouver les comptes utilisateurs qui sont inactifs depuis 90 jours 0 heure 0 minute et 0 seconde

Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00 -UserOnly

# Trouver les comptes utilisateurs qui sont inactifs depuis 90 jours

Search-ADAccount -AccountInactive -TimeSpan "90" -UserOnly

# Trouver les comptes utilisateurs qui sont inactifs depuis 12 heures

Search-ADAccount -AccountInactive -TimeSpan "12:00" -UserOnly

# Trouver les comptes utilisateurs qui sont désactivés et affiche plusieurs propriétés

Search-ADAccount -AccountDisabled | Format-List -Property Name,LastLogonDate,UserPrinciplalName

# Remplacer le mot de passe d'un utilisateur

# et forcer l'utilisateur à modifier son mot de passe à la prochaine ouverture de session

$mdp = ConvertTo-SecureString -String "AAAaaa111" -AsPlainText -Force

Set-ADAccountPassword -Identity ETU -NewPassword $mdp -Reset

Set-ADUser -Identity ETU -ChangePasswordAtLogon $true

**PROBLÈME AVEC LE MODE DE SESSION ÉTENDU**

**Par défaut, les utilisateurs qui ne sont pas membre du groupe "Administrateurs" ne peuvent pas se connecter au serveur membre si on utilise le mode de session étendu.**



**SOLUTION SIMPLE À CE PROBLÈME**

**Modification à effectuer sur le serveur membre**

Dans "Propriétés système" cliquer sur le bouton "Sélectionnez des utilisateurs…" et ajouter le groupe "FORMATION\Utilisateurs du domaine".

 