B64- DOCUMENT ÉTUDE

[ACTIVE DIRECTORY : 2](#_Toc468724236)

[Définition : 2](#_Toc468724237)

[Forêts, arborescences et domaines 2](#_Toc468724238)

[Une arborescence Active Directory est donc composée de : 3](#_Toc468724239)

[Attributs des objets utilisateurs : 4](#_Toc468724240)

[Empêcher un utilisateur de joindre un ordinateur au domaine : 5](#_Toc468724241)

[Création d’objets -Notes : 5](#_Toc468724242)

[Critères pour la création d'un compte utilisateur : 6](#_Toc468724243)

[Mise en situation des deux erreurs possibles lors de la création d'un compte utilisateur 6](#_Toc468724244)

[Création UO par programmation PowerShell 7](#_Toc468724245)

[EXEMPLES : 7](#_Toc468724246)

[MODIFICATION TXT PAR PROGRAMMATION: 8](#_Toc468724247)

[Exemples: 8](#_Toc468724248)

[CREER UNITÉ ORGANISATION AVEC CSV PAR PROG 10](#_Toc468724249)

[Utilisation du GET 11](#_Toc468724250)

[Notes sur la prestation 11](#_Toc468724251)

[Pour trouver les propriétés du Domaine et de la Forêt 11](#_Toc468724252)

[Pour trouver les propriétés des Ordinateurs 11](#_Toc468724253)

[Pour trouver les propriétés des Utilisateurs 11](#_Toc468724254)

[Pour trouver les propriétés des Groupes 11](#_Toc468724255)

[Pour trouver les propriétés des "Unités d’organisation" 11](#_Toc468724256)

[Pour trouver les propriétés des différents "Objets" 12](#_Toc468724257)

[LDAP (Lightweight Directory Access Protocol) 13](#_Toc468724258)

[Les propriétés de bases d'un utilisateur 14](#_Toc468724259)

[Une liste de plusieurs cmdlets pour gérer un utilisateur : 16](#_Toc468724260)

[Exemples 16](#_Toc468724261)

[Objet de stratégie de groupe GPO : 17](#_Toc468724262)

[Définition 17](#_Toc468724263)

[Les trois phases de l'utilisation des stratégies de groupe 18](#_Toc468724264)

[Création et édition des stratégies de groupe 18](#_Toc468724265)

[Liaison des stratégies de groupe 18](#_Toc468724266)

[Application des stratégies de groupe 18](#_Toc468724267)

[Quelques commandes 19](#_Toc468724268)

[Exemples : 19](#_Toc468724269)

[Rapport GPO : 20](#_Toc468724270)

[Création d’un rapport par la console "Gestion de stratégie de groupe" 20](#_Toc468724271)

[Sauvegarde des GPO par progammation PowerShell 21](#_Toc468724272)

[Importation des GPO par la console 21](#_Toc468724273)

[Importation des GPO par programmation PowerShell 21](#_Toc468724274)

[La GPO "Default Domain Policy" : 22](#_Toc468724275)

[La GPO " Default Domain Controllers Policy " : 22](#_Toc468724276)

# ACTIVE DIRECTORY :

### Définition :

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés (en), les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l’accès aux ressources répertoriées.

### Forêts, arborescences et domaines

Active Directory introduit la notion de hiérarchie, inhérente aux annuaires objets dérivés de X.500, sous la forme d'une arborescence dans laquelle les utilisateurs et les ordinateurs sont organisés en groupes et sous groupes afin de faciliter l'administration des droits et restrictions utilisateur. C'est aussi Active Directory qui gère l'authentification des utilisateurs sur le réseau Windows. Active Directory exploite cette notion de hiérarchie intensivement, puisque l'entité de sécurité appelée « domaine » est également hiérarchisée dans un ensemble partageant un espace de nom commun, appelé « arborescence », enfin, l'entité de plus haut niveau regroupant les arborescences de domaines constitue la forêt Active Directory.

Active Directory permet une réplication multi-maître, c'est-à-dire que chaque contrôleur de domaine peut être le siège de modifications (ajout, modification, suppression) de l'annuaire, sous réserve de permission accordée par ACL, qui seront répliquées sur les autres contrôleurs de domaine. SAM ne disposait que d'une seule base en écriture, les autres répliquas étant en lecture seule.

Le mécanisme de réplication de ces modifications peut profiter de RPC (liaisons TCP/IP rapides et disponibles) ou SMTP dans les autres cas. La topologie de réplication est générée automatiquement mais elle peut être personnalisée par l'administrateur, tout comme sa planification.

À noter que les ensembles d'espaces de nom correspondant aux arborescences d'Active Directory formant la forêt Active Directory sont superposables à l'espace de nom formé par les zones DNS. DNS est un service indispensable pour le bon fonctionnement de toute l'architecture Active Directory, localisation des contrôleurs de domaine, réplication, etc.

### Une arborescence Active Directory est donc composée de :

La forêt : structure hiérarchique d'un ou plusieurs domaines indépendants (ensemble de tous les sous domaines Active Directory).

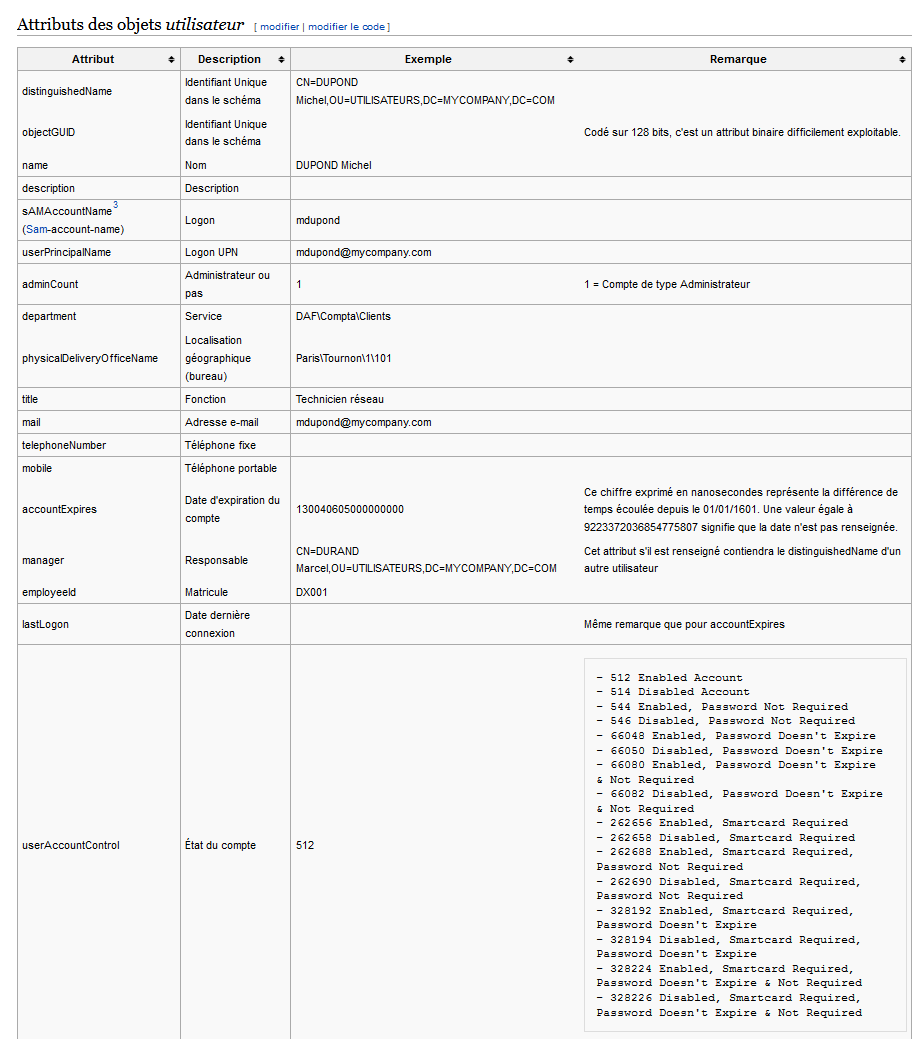
L'arbre ou l'arborescence : domaine de toutes les ramifications. Par exemple, dans l'arbre domaine.tld, sous1.domaine.tld, sous2.domaine.tld et photo.sous1.domaine.tld sont des sous-domaines de domaine.tld.

Le domaine : constitue les feuilles de l'arborescence. photo.sous1.domaine.tld peut-être un domaine au même titre que domaine.tld.

Le modèle de données Active Directory est dérivé du modèle de données de la norme X.500 : l'annuaire contient des objets représentant des éléments de différents types décrits par des attributs. Les stratégies de groupe (GPO) sont des paramètres de configuration appliqués aux ordinateurs ou aux utilisateurs lors de leur initialisation, ils sont également gérés dans Active Directory.

Le protocole principal d'accès aux annuaires est LDAP qui permet d'ajouter, de modifier et de supprimer des données enregistrées dans Active Directory, et qui permet en outre de rechercher et de récupérer ces données. N'importe quelle application cliente conforme à LDAP peut être utilisée pour parcourir et interroger Active Directory ou pour y ajouter, y modifier ou y supprimer des données.

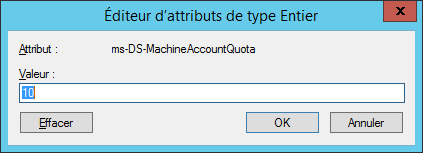
### Attributs des objets utilisateurs :



### Empêcher un utilisateur de joindre un ordinateur au domaine :

Par défaut, un utilisateur authentifié qui n'est pas membre du groupe Administrateurs peut joindre 10 ordinateurs au domaine.

Voici la valeur par défaut de l'attribut **ms-DS-MachineAccountQuota**



Pour empêcher un utilisateur authentifié de joindre des ordinateurs au domaine on doit modifier la valeur de l'attribut **ms-DS-MachineAccountQuota** pour **0**.

## Création d’objets -Notes :

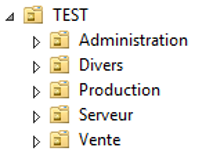
Dans la console "Utilisateurs et ordinateurs Active Directory" on peut

-créer des unités d’organisations

-modifier des unités d’organisations

-détruire des unités d’organisations

Exemple graphique :



\*\*\*ON DOIT ENLEVER PROTECTION SINON C’EST IMPOSSIBLE DE SUPPRIMER OU MODIFIER CORECTEMENT\*\*\*\*

### Critères pour la création d'un compte utilisateur :

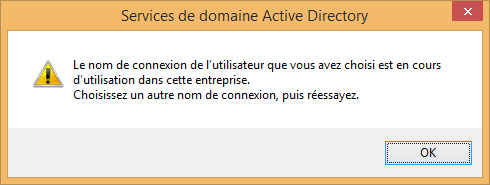
**note: lors de la création d'un utilisateur en utilisant l'environnement graphique, le système utilise le nom complet de l'utilisateur pour créer le nom de l'utilisateur**

### Mise en situation des deux erreurs possibles lors de la création d'un compte utilisateur

**Cas 1**

Si on veut créer un autre compte utilisateur dans l'unité d'organisation Production avec les propriétés suivantes:

* Prénom: **Jean**, Nom: **Coutu**
* Nom d'ouverture de session de l'utilisateur: **jeanC1**

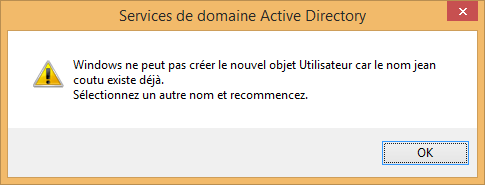


**IMPORTANT: Le nom de connexion d'un utilisateur doit être unique dans tout le domaine.**

**Cas 2**

Si on veut créer un autre compte utilisateur dans l'unité d'organisation Production avec les propriétés suivantes:

* Prénom: **Jean**, Nom: **Coutu**
* Nom d'ouverture de session de l'utilisateur: **jeanC2**



**IMPORTANT: Le nom de l'utilisateur doit être unique dans une OU**

Créer un compte d'utilisateur dans votre unité d'organisation Vente en indiquant les propriétés suivantes:

* Prénom: **Jean**, Nom: **Coutu**
* Nom d'ouverture de session de l'utilisateur: **jeanC3**

**note: la création de ce compte a fonctionné parce que le nom d'utilisateur "Jean Coutu" est unique dans la OU Vente et que le nom d'ouverture de connexion JeanC3 est unique dans le domaine**

### Création UO par programmation PowerShell

Il est recommandé de fermer votre console "Gestion des stratégies de groupe" quand vous faites de la programmation

Il existe 4 cmdlet spécifiques pour la gestion des unités d’organisation.

* Get-ADOrganizationalUnit
* New-ADOrganizationalUnit
* Remove-ADOrganizationalUnit
* Set-ADOrganizationalUnit

DC= Domain Controler

OU= Organizational Unit

#### EXEMPLES :

$nomDomaine = "DC=b64,DC=local"

Set-ADOrganizationalUnit -Identity "ou=PROG,$nomDomaine" -ProtectedFromAccidentalDeletion $false

Remove-ADOrganizationalUnit -Identity "ou=PROG,$nomDomaine" -Confirm $false -Recursive

New-ADOrganizationalUnit -Name "PROG" -Path "$nomDomaine" -Description "PROG est sous le domaine" ` -ProtectedFromAccidentalDeletion $false

New-ADOrganizationalUnit -Name "Niveau1" -Path "ou=PROG,$nomDomaine" -Description "Niveau1 est sous PROG" ` -ProtectedFromAccidentalDeletion $false

New-ADOrganizationalUnit -Name "Niveau2" -Path "ou=Niveau1,ou=PROG,$nomDomaine" -Description "Niveau2 est sous Niveau1" ` -ProtectedFromAccidentalDeletion $false

New-ADOrganizationalUnit -City:"Montréal" -Description:"Cegep" -Name:"CVM" -OtherAttributes:@{"c"="CA";"co"="Canada";"countryCode"="124"} -Path:"OU=TEST,DC=B64,DC=LOCAL" -PostalCode:"h2x1x6" -ProtectedFromAccidentalDeletion:$false -Server:"B64HV1.B64.LOCAL" -State:"QC" -Street:"255 rue Ontario Est"

### MODIFICATION TXT PAR PROGRAMMATION:

Vous avez besoin des cmdlets suivants:

* Add-Content
* Get-Content
* Set-Content

Vous avez besoin de la méthode "**.Replace**"

#### Exemples:

$content = get-content -Path "C:\UO.txt"

set-content -Path "C:\CANADA\_UO.CSV" -Value "Parent; nom; description"

foreach($line in $content)

{

$line = $line.replace("ville1", "Verdun")

$line = $line.replace("ville2", "Moncton")

$line = $line.replace("ville3", "Tofino")

$line = $line.replace("pays", "Canada")

add-content -Path "C:\CANADA\_UO.CSV" -value $line

}

(Get-Content -Path "Notice.txt") | ForEach-Object {$\_ -Replace "Warning", "Caution"} | Set-Content -Path "Notice.txt"

Get-Content -Path "C:\Chapters\Chapter1.txt"

Add-Content -Path "file1.log", "file2.log" -Value (Get-Date) -PassThru

#Permet de lire un fichier

Set-Content -Path c:\users\TECH\desktop\CANADA\_UO.csv -Value "UO\_Parent;UO\_ACreer;Description"

#Set-Content pourrait aussi fonctionner

$fichier = Get-Content "C:\Users\TECH\Desktop\UO.txt"

foreach ($ligne in $fichier)

{

$nouveau = $ligne

$nouveau = $nouveau.Replace("pays", "Canada")

$nouveau = $nouveau.Replace("ville1", "Verdun")

$nouveau = $nouveau.Replace("ville2", "Moncton")

$nouveau = $nouveau.Replace("ville3", "Tofino")

Add-Content -Path c:\users\TECH\desktop\CANADA\_UO.csv -Value $nouveau

}

### CREER UNITÉ ORGANISATION AVEC CSV PAR PROG

Ex :

$fichier = Import-Csv "C:\B64\_UO.csv" -Delimiter ";"

$domaine = ",DC=B64,DC=LOCAL"

$lepath = ""

$count = 0

$blah = " enregistrements créés"

New-ADOrganizationalUnit -Name B64 -otherAttributes @{c='CA';co='Canada';countryCode='124'} -ProtectedFromAccidentalDeletion:$false

foreach ($ligne in $fichier)

{

$lepath = $ligne.aParent + $domaine

$lepath

$ligne.aOu

$ligne.aDesc

$count = $count + 1

$count

$blah

Write-Host "------" -ForegroundColor Green

New-ADOrganizationalUnit -Name $ligne.aOu -Path $lepath -Description $ligne.aDesc -otherAttributes @{c='CA';co='Canada';countryCode='124'} -ProtectedFromAccidentalDeletion:$false

}

### Utilisation du GET

#### Notes sur la prestation

Cours axé sur les cmdlets GET du module ActiveDirectory

Pour obtenir de l'aide sur le paramètre **-Filter** dans les cmdlets GET de l'Active Directory

**# metre à jour l'aide du module ActiveDirectory**

**Update-Help -Module ActiveDirectory**

**# affiche l'aide du paramètre -Filter dans les cmdlets GET de l'Active Directory**

**Get-Help about\_ActiveDirectory\_Filter**

Get-Help about\_ActiveDirectory\_Filter | Out-File "c:\temp\About\_ActiveDirectory\_Filter.txt" -Encoding utf8

#### Pour trouver les propriétés du Domaine et de la Forêt

Get-ADDomain

Get-ADForest

#### Pour trouver les propriétés des Ordinateurs

Get-ADComputer

#### Pour trouver les propriétés des Utilisateurs

Get-ADUser

#### Pour trouver les propriétés des Groupes

Get-ADGroup

#### Pour trouver les propriétés des "Unités d’organisation"

Get-ADOrganizationalUnit

#### Pour trouver les propriétés des différents "Objets"

Get-ADObject

#### LDAP (Lightweight Directory Access Protocol)

Get-ADComputer

Get-ADGroup

Get-ADObject

Get-ADOrganizationalUnit

Get-ADUser

Ces cinq cmdlets peuvent utiliser le paramètre **-LDAPFilter**

Le code d'une requête LDAP utilise une syntaxe particulière.

**Pour nous aider à créer des requêtes LDAP**

La console "Utilisateurs et ordinateurs Active Directory" permet de créer des requêtes LDAP.

note: section "Requêtes enregistrées"

La console "Centre d'administration Active Directory" permet de créer des "Recherche globale" en utilisant l'interface graphique et de convertir cette requête en LDAP.

**Les opérateurs**

**Opérateur Signification**

= égal

>= plus grand ou égal

<= plus petit ou égal

& ET

| OU

! NÉGATION

ANR Ambiguous Name Resolution

**ANR (Ambiguous Name Resolution) est un opérateur qui effectue la recherche sur plusieurs attributs**

Cette commande PowerShell permet d'afficher la liste des attributs sur laquelle ANR effectue la recherche

Get-ADObject -SearchBase "cn=Schema,cn=Configuration,dc=dalton,dc=b64" `

-LDAPFilter "(searchFlags:**1.2.840.113556.1.4.803**:=4)" `

-Properties lDAPDisplayName | Select lDAPDisplayName

Get-ADObject -LDAPFilter "(anr=B64)"

### Les propriétés de bases d'un utilisateur

* + Prénom: **PRÉNOM**
  + Nom: **NOM**
  + Nom complet: **PRÉNOM NOM**
  + Nom d'ouverture de session de l'utilisateur: **test1@b64.local**
  + Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000): **B64\test1**
  + Mot de passe: AAAaaa111
  + Le mot de passe n'expire jamais

\*\*\*note: il y a trois attributs par pays

**LastLogon**

Cet attribut n'est jamais répliqué, ce qui veut dire que sa valeur est spécifique à chaque contrôleur de domaine.

Par défaut, LastLogon est un entier qui définit le nombre de 100 nano secondes depuis le 1601/01/01.

**LastLogonTimeStamp**

Cet attribut est répliqué sur chaque contrôleur de domaine mais seulement dans un intervalle de 9 à 14 jours.

Par défaut, LastLogonTimeStamp est un entier qui définit le nombre de 100 nano secondes depuis le 1601/01/01.

**UserAccountControl**

Ce tableau présente les différentes valeurs du paramètre **UserAccountControl**.

Les valeurs sont cumulatives.

|  |  |  |
| --- | --- | --- |
| Nom de la constante  pour la valeur | Valeur  hexadécimale | Explication de la valeur |
| **SCRIPT** | **0x1** | Exécution du script d'ouverture de session |
| **ACCOUNTDISABLE** | **0x2** | Désactivation du compte utilisateur |
| **HOMEDIR\_REQUIRED** | **0x8** | Dossier de base requis |
| **LOCKOUT** | **0x10** | Aucun mot de passe n'est requis. |
| **PASSWD\_NOTREQD** | **0x20** | Vous pouvez lire cette valeur, mais vous ne pouvez pas la définir directement. |
| **PASSWD\_CANT\_CHANGE** | **0x40** | Impossible de modifier le mot de passe. |
| **ENCRYPTED\_TEXT\_PWD\_ALLOWED** | **0x80** | L'utilisateur peut envoyer un message crypté. |
| **TEMP\_DUPLICATE\_ACCOUNT** | **0x100** | Compte pour les utilisateurs dont le compte principal se trouve dans un autre domaine. Ce compte fournit l'accès à ce domaine, mais pas à tous les domaines qui ont des relations d'approbation avec ce domaine. Il est parfois appelé compte utilisateur local. |
| **NORMAL\_ACCOUNT** | **0x200** | Type de compte par défaut représentant un utilisateur |
| **INTERDOMAIN\_TRUST\_ACCOUNT** | **0x800** | Autorisation d'approuver un compte pour un domaine du système qui a des relations d'approbation avec d'autres domaines. |
| **WORKSTATION\_TRUST\_ACCOUNT** | **0x1000** | Compte d'ordinateur |
| **SERVER\_TRUST\_ACCOUNT** | **0x2000** | Compte d'ordinateur d'un contrôleur de domaine membre de ce domaine. |
| **DONT\_EXPIRE\_PASSWORD** | **0x10000** | Représente le mot de passe, qui ne doit jamais expirer pour le compte. |
| **MNS\_LOGON\_ACCOUNT** | **0x20000** | Compte d'ouverture de session de jeu de nœuds majoritaire. |
| **SMARTCARD\_REQUIRED** | **0x40000** | Cette valeur force l'utilisateur à ouvrir une session avec une carte à puce. |
| **TRUSTED\_FOR\_DELEGATION** | **0x80000** | Le compte de service (compte d'utilisateur ou d'ordinateur) est approuvé pour la délégation Kerberos. N'importe lequel de ces services peut prendre l'identité d'un client demandant le service. |
| **NOT\_DELEGATED** | **0x100000** | Le contexte de sécurité de l'utilisateur n'est pas délégué à un service même si le compte de service est approuvé pour la délégation Kerberos. |
| **PASSWORD\_EXPIRED** | **0x800000** | Le mot de passe de l'utilisateur a expiré. |

### 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

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

Search-ADAccount -PasswordNeverExpires

# Trouve les comptes utilisateurs qui sont inactifs depuis 90 jours

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

# 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

# Objet de stratégie de groupe GPO :

Définition :

Les stratégies de groupe (ou GP pour group Policy) sont des fonctions de gestion centralisée de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory. Les stratégies de groupe font partie de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection des dossiers ainsi que la gestion des fichiers en mode déconnecté. Les stratégies de groupe sont gérées à travers des objets de stratégie de groupe communément appelés GPO (Group Policy Objects).

Les entreprises utilisent les stratégies de groupe pour restreindre les actions et les risques potentiels comme le verrouillage du panneau de configuration, la restriction de l’accès à certains dossiers, la désactivation de l’utilisation de certains exécutables, etc.

**Mise en garde**

**Sous aucun prétexte les stratégies suivantes ne peuvent être détruites ou modifiées:**

Default Domain Controllers Policy

Default Domain Policy

### Les trois phases de l'utilisation des stratégies de groupe

Les stratégies de groupe peuvent être considérées en trois phases distinctes - Création de la stratégie de groupe, Liaison des stratégies de groupe et Application des stratégies de groupe.

#### Création et édition des stratégies de groupe

Les stratégies de groupe peuvent être éditées au travers de deux outils – le Group Policy Object Editor (Gpedit.msc) et la Group Policy Management Console (gpmc.msc). GPEdit est utilisé pour créer et éditer une stratégie de groupe de façon unitaire. La GPMC simplifie grandement la gestion des stratégies de groupe en fournissant un outil permettant une gestion centralisée et collective des objets. La GPMC inclut de nombreuses fonctionnalités telles que la gestion des paramètres, un panneau pour la gestion du filtrage par groupe de sécurité, des outils de sauvegarde et de restauration et d’autres outils graphiques intégrés à la MMC. Le nom d’une stratégie de groupe peut être déterminé en utilisant l’outil GPOTool.exe.

#### Liaison des stratégies de groupe

Après avoir créé une stratégie de groupe, elle peut être liée à un site Active Directory, à un domaine ou à une unité d'organisation (UO).

#### Application des stratégies de groupe

Le client de stratégie de groupe du poste récupère la configuration (de base dans un intervalle aléatoire compris entre 60 et 120 minutes, mais cela est configurable via les stratégies de groupe) qui est applicable à l’ordinateur et à l’utilisateur connecté et l’applique en tenant compte des différents critères de filtre, de sécurité et d’héritage.

### Quelques commandes

Il est possible de vérifier l'application des GPO manuellement avec les commandes

GPResult

Il est possible de forcer l'application des GPO manuellement avec les commandes

GPUpdate /Force

Info: gpupdate ne déploie pas les GPO aux membres du domaine. Elle doit être exécutée sur chaque poste concerné.

### Exemples :

Créer un objet GPO "Gpo1" et "Gpo2"

**New-GPO –Name Gpo1**

**New-GPO –Name Gpo2**

Lier l’objet GPO "Gpo2" à l’unité "Niveau0"

**New-GPLink –Name GPO2 –Target "ou=Niveau0,dc=b64,dc=local"**

Créer un objet GPO "Gpo3"

**New-GPO –Name "GPO3"**

Lier l’objet GPO "Gpo3" à l’unité Niveau1

**New-GPLink –Name GPO3 –Target "ou=Niveau1,ou=Niveau0,dc=b64,dc=local"**

Créer un objet GPO "Gpo4"

**New-GPO –Name "GPO4"**

Lier l’objet GPO "Gpo4" à l’unité Niveau2

**New-GPLink –Name GPO4 –Target "ou=Niveau2,ou=Niveau1,ou=Niveau0,dc=b64,dc=local"**

### Rapport GPO :

#### Création d’un rapport par la console "Gestion de stratégie de groupe"

Dans la console "Gestion de stratégie de groupe"

* Le curseur sur l’objet "Default Domain Policy", faites afficher le contenu de l’onglet "Paramètres"
* Dans le menu contextuel de cette page choisir "Enregistrer le rapport…"
* En fichier HTML
* Dans C:\temp
* Donner un nom approprié au fichier

Avec un navigateur, visualiser votre rapport

#### Sauvegarde des GPO par progammation PowerShell

Dans "PowerShell ISE"

* Faire une sauvegarde de l’objet "Default Domain Controllers Policy"
* Emplacement: le dossier C:\GPObackup
* Description: "Default Domain Controllers Policy copie2"

note: le dossier utilisé pour les backups doit obligatoirement exister

"

réponse: **backupGPO – Name "default domain Controllers Policy" –Path C:\GPOBackup –Comment"ddcp copie2"**

#### Importation des GPO par la console

Dans la console "Gestion de stratégie de groupe"

* Le curseur sur "Objets de stratégie de groupe"
* Dans le menu contextuel choisir "Gérer les sauvegardes…"
* Choisir le dossier C:\GPObackup si nécessaire
* Choisir la stratégie "Gpo2"
* Faire "Restaurer"
* Lier l’objet à l’unité d'organisation "Niveau0"

#### Importation des GPO par programmation PowerShell

Attention nous avons deux choix de cmdlet: IMPORT ou RESTORE. De préférence nous utiliserons "IMPORT" car il permet de récupérer les sauvegardes faites dans un autre domaine.

Dans "PowerShell ISE"

* Faire une importation de l’objet "GpoC"
* Emplacement: le dossier C:\GPObackup
* Vers un objet portant le même nom
* Effectuer la création si le nouvel objet n’existe pas

réponse: **import-GPO –BackupGpoName "GpoC" –Path C:\GPOBackup –CreateIfNeeded –TargetName "GpoC"**

* Lier l’objet "GpoC" à l’unité d'organisation "Niveau0"

réponse: **New-GPLink –Name "GpoC" –Target "Niveau0,dc=b64,dc=local"**

### La GPO "Default Domain Policy" :

**Quelle est la durée maximale des mots de passe ?**

réponse: 42 jours

**Quelles valeurs sont recommandées comme durée maximale ?**

réponse: 30 a 90 jours

**Quelle est la durée minimale des mots de passe (antériorité) ?**

réponse: 1 jour

**Que signifie le paramètre "durée minimale du mot de passe" ?**

réponse: Durée minimale avant que l’utilisateur puisse le changer

**En fonction des réponses précédentes**

**Quand puis-je changer mon mot de passe si je viens tout juste de le modifier ?**

réponse: dans 24 heures

**Combien de mots de passe garde-t-on dans l'historique ?**

réponse:24 mots de passe

**Est-ce possible d’en conserver plus ?**

réponse: non

**Est-ce que les mots de passe doivent respecter des exigences de complexité ?**

réponse: oui

**Quelle est la longueur minimale des mots de passe ?**

réponse: 7 caracteres

**Est-il possible d’avoir une longueur minimale plus grande ?**

réponse: oui

**Dans la GPO de domaine, le seuil de verrouillage de comptes est à 0 tentative.**

**Qu’est-ce que cela signifie ?**

réponse: le compte ne sera jamais vérouillé

### La GPO " Default Domain Controllers Policy " :

Quel utilisateur ou quel groupe peut …

**Ajouter des stations de travail au domaine**

réponse: Utilisateurs authentifiés

**Arrêter le système**

réponse: Opérateur d’impression / Opérateurs de serveurs / Opérateurs de sauvegarde / Administrateurs

**Forcer l’arrêt à partir d’un système distant**

réponse: Opérateur de serveur / Administrateur

**Modifier l’heure système**

réponse: Opérateur de serveur / Administrateur / service local

**Permettre l'ouverture d’une session locale**

réponse: Enterprise domain controler / Opérateurs d’impression / Opérateurs de serveurs / Opérateurs de compte / Opérateurs de sauvegarde / Adminstrateurs

## Structure des dossiers

|  |
| --- |
| **Windows Serveur 2012 R2**  **Une liste de plusieurs dossiers du profil utilisateur C:\Users\*%username%*\...** |
| …\AppData\Local |
| …\AppData\Local\Microsoft\Windows\History |
| …\AppData\Local\Microsoft\Windows\Temporary Internet Files |
| …\AppData\Local\Temp |
| …\AppData\Roaming |
| …\AppData\Roaming\Microsoft\Windows\Cookies |
| …\AppData\Roaming\Microsoft\Windows\Network Shortcuts |
| …\AppData\Roaming\Microsoft\Windows\Printer Shortcuts |
| …\AppData\Roaming\Microsoft\Windows\Recent |
| …\AppData\Roaming\Microsoft\Windows\SendTo |
| …\AppData\Roaming\Microsoft\Windows\Start Menu |
| …\AppData\Roaming\Microsoft\Windows\Templates |
| …\Desktop |
| …\Documents |
| …\Downloads |
| …\Favorites |
| …\Links |
| …\Music |
| …\Pictures |
| …\Saved Games |
| …\Videos |

### Structure du profil par défaut

La structure du profil par défaut utilise le dossier "**C:\Users\Default**" et possède une structure similaire à un profil utilisateur.

|  |
| --- |
| **Windows Serveur 2012 R2** |
| C:\Users\Default |
| C:\Users\Default\AppData\Local\Microsoft\Windows\**appsFolder.itemdata-ms**  **note: ce fichier contient la configuration de l'écran d'accueil** |
| C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo |
| C:\Users\Default\Desktop |

### Structure du profil pour "Tous les utilisateurs"

La structure du profil pour "Tous les utilisateurs" utilise deux dossiers "**C:\ProgramData**" et "**C:\Users\Public**".

|  |
| --- |
| **Windows Serveur 2012 R2** |
| C:\ProgramData |
| C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp |
| C:\Users\Public |
| C:\Users\Public\Desktop |

## DFS :

La technologie Distributed File System (DFS), en français «Système de fichiers distribué » est un ensemble de services client et serveur permettant :

* de fournir une arborescence logique aux données partagées depuis des emplacements différents,
* de rassembler différents partages de fichiers à un endroit unique de façon transparente,
* d’assurer la redondance et la disponibilité des données grâce à la réplication.

Avec cette technologie, il est possible de monter un seul même lecteur sur le poste de tous les utilisateurs, les partages existant se présenteront sous forme de dossiers et fonctionneront comme des raccourcis. L’affichage ou non des dossiers se configure ensuite en fonction de l’appartenance aux groupes NTFS.

#### Espaces de noms

La première chose à réaliser est la création de la racine de l’espace de noms (également appelé racine DFS). C’est dans cette racine que seront placés les dossiers DFS avec cibles de dossier pointant vers des partages distants ainsi que les Dossiers DFS sans cibles de dossier.

Il existe deux types d’espace de noms : Les espaces de noms autonomes et les espaces de noms de domaine. Les espaces de noms de domaine permettent la redondance de l’accès au DFS grâce à la possibilité de définir plusieurs serveurs pour un même espace de noms DFS. Ce mode requiert d’être membre :

* d’un domaine Active directory de niveau fonctionnel 2008 minimum pour le mode server 2008,
* d’un domaine Active directory d’un niveau fonctionnel 2000 mixte pour le mode 2000 server.

#### Voici les différences :

Le mode server 2008 permet l’énumération basé sur l’accès mais demande que les serveurs DFS soient tous au minimum en version 2008.

Le mode server 2000 ne permet pas l’énumération basé sur l’accès, la taille de l’espace de noms est limité à environ 5000 dossiers avec cibles.

Les espaces de noms autonomes (standalone) ne permettent pas d’utiliser plusieurs serveurs d’espaces de nom. Il faut passer par un cluster de basculement pour assurer une tolérance de pannes. Ils ne demandent pas de faire partie d’un domaine.

#### Dossiers DFS

Il existe 2 types de dossiers DFS :

* Les Dossiers DFS sans cibles de dossiers servent uniquement à la structure et à la hiérarchie de l’espace de noms DFS. Ils ne peuvent pas contenir de fichiers ni de dossiers classiques.
* Les Dossiers DFS avec cibles de dossiers servent à pointer vers des partages existant, l’utilisateur est redirigé de façon transparente.

C’est en combinant ces deux types de dossiers qu’il est possible d’accéder a un endroit unique à des données placées a plusieurs endroits différents et cela de façon transparente.

#### Choix du serveur

Il existe plusieurs façons de choisir quel est le serveur qui sera choisi lors de la connexion par le client. Le choix est défini par ce paramètre. Voici les options :

* Moindre coût : Requiert que les coûts entre les sites Active Directory soient définis. Lorsque c’est le cas, la cible choisie lorsqu’il y a plusieurs sites est le moins coûteux
* Ordre aléatoire : La cible est celle du site où est l’utilisateur. Si ce n’est pas le cas celui-ci est choisi de façon aléatoire.
* Exclure les cibles en dehors du site du client : Si aucune cible ne fait partie du même site que le client, il ne peut pas accéder à l’espace de noms.

#### Énumération basée sur l'accès

L’énumération basée sur l’accès est un paramètre qui permet de définir si un dossier avec cible de dossiers est affiché ou non en fonction des groupes de sécurité définis. C’est cela qui permet par exemple de choisir ce que l’utilisateur voit lorsqu’il accède à un espace de noms DFS. Cela est comparable à des dossiers caché qui s’afficheraient en fonction de l’appartenance aux groupes de sécurité NTFS.

#### Compression

À partir de Windows2008, DFS utilise un algorithme de compression tenant compte uniquement des blocs modifiés, ce qui permet d'optimiser les flux de données en ne transférant pas les blocs inchangés1.