

# PowerShell

# Active Directory



# Création du Domaine et de la Forêt

# Création du Domaine Racine de la Forêt : Install-ADDSForest

- Il faut donner des paramètres identiques à ceux qui sont provisionnés en mode graphique

```
Install-ADDSForest `‐
    -DomainName "formation.lab"      -DomainNetbiosName "FORMATION" `‐
    -CreateDnsDelegation:$false     -DomainMode "7"      -ForestMode "7" `‐
    -InstallDns:$true              -DatabasePath "C:\Windows\NTDS" `‐
    -SysvolPath "C:\Windows\Sysvol"   -Logpath "C:\Windows\NTDS" `‐
    -NoRebootOnCompletion:$false     -Force:$true
```

# Création du Domaine Racine

- Il manque le mot de passe **DSRM** de Récupération des Services d'Annuaire
- Ce mot de passe est demandé lors de l'exécution du cmdlet **Install-ADDSForest**
- L'administrateur du Server sur lequel s'exécute cette commande devient l'administrateur de la Forêt

# Ajout d'un Contrôleur de Domaine supplémentaire

# Sur le premier Contrôleur de Domaine

- Il est fortement conseillé de passer la zone DNS qui supporte Active Directory en **Zone Intégrée à Active Directory** si ce n'est pas le cas avec le cmdlet : **Set-DnsServerPrimaryZone**

```
Set-DnsServerPrimaryZone -Name "formation.lab" -ReplicationScope "Forest"
```

# Sur le futur Contrôleur de Domaine

- Avant de lancer l'installation d'Active Directory il faut configurer le Client\_DNS avec comme DNS Préféré celui du Contrôleur Principal et lui même en DNS Auxiliaire

```
Set-DnsClientServerAddress -InterfaceIndex 5 -ServerAddresses 192.168.108.11,192.168.108.12
```

- Et inverser ces DNS après l'installation d'Active Directory

```
Set-DnsClientServerAddress -InterfaceIndex 5 -ServerAddresses 192.168.108.12,192.168.108.11
```

# Installation du Contrôleur de Domaine : **Install-ADDSDomainController**

- Les paramètres à fournir sont très semblables à ceux utilisés pour l'installation du Principal

```
Install-ADSDomainController `n`n    -InstallDns:$true `n    -Credential (Get-Credential "FORMATION\administrateur") `n    -DomainName "formation.lab"      -SiteName 'Default-First-Site-Name' `n    -DatabasePath "C:\Windows\NTDS"     -SysvolPath "C:\Windows\Sysvol" `n    -Logpath "C:\Windows\NTDS"        -NoGlobalCatalog:$false `n    -NoRebootOnCompletion:$false     -Force:$true
```

# Installation du Contrôleur de Domaine :

## Install-ADDSDomainController

- Les paramètres qui ne sont pas demandés pendant l'installation de la Forêt sont :
  - **Credential** : le compte administrateur du domaine
  - **SiteName** : site Active Directory - ici valeur par défaut
  - **NoGlobalCatalog** : le Contrôleur Principal est obligatoirement Catalogue Global - le choix est possible pour les autres contrôleurs de le configurer ou non

# Gestion des Objets Active Directory

# Unités d'Organisation

- Permettent d'organiser l'Annuaire Active Directory
- Crédation d'une OU : **New-ADOrganizationalUnit**

```
New-ADOrganizationalUnit `‐  
‐Name "Corp" `‐  
‐Path "DC=formation,DC=lab" `‐  
‐ProtectedFromAccidentalDeletion $true
```

Les seuls Attributs obligatoires sont **Name et Path**

# Unités d'Organisation

- Modification d'une OU : **Set-ADOrganizationalUnit**

```
Set-ADOrganizationalUnit ` 
    -Identity "OU=corp,DC=formation,DC=lab" ` 
    -Description "OU Corporate de l'entreprise Formation."
```

L'Attribut **ProtectedFromAccidentalDeletion** lors de la création permet d'éviter la suppression accidentelle de l'OU

# Utilisateurs

- Crédation d'un Utilisateur : **New-ADUser**

```
New-ADUser `n
  -GivenName "Neymar"    -Surname "Jean" `n
  -Name "Jean Neymar"    -DisplayName "Jean Neymar" `n
  -SamAccountName "jNeymar" `n
  -UserPrincipalName "mEnfaillitte@formation.lab" `n
```

Les seuls attributs obligatoires sont le **Nom** avec **Name** et le **Login NTLM** avec **SamAccountName**

# Utilisateurs

- L'utilisateur est créé par défaut dans le Conteneur **Users**
- Sans mot de passe, il n'est pas activé !
- Crédit d'un mot de passe : **Set-ADAccountPassword**

```
Set-ADAccountPassword  
    -Identity "CN=Jean Neymar,CN=Users,DC=formation,DC=lab"  
    -NewPassword (ConvertTo-SecureString -AsPlainText "Azerty00" -Force)
```

Les chemins sont au format **LDAP**

# Utilisateurs

- Modification d'utilisateur : **Set-ADUser**
- Activation et configuration pour changement du mot de passe au prochain login

```
Set-ADUser ` 
-Identity "CN=Jean Neymar,CN=Users,DC=formation,DC=lab" ` 
-ChangePasswordAtLogon $true ` 
-Enabled $true
```

# Utilisateurs

- Déplacement d'un utilisateur dans une OU particulière avec **Move-ADObject**

```
Move-ADObject  
-Identity "CN=Jean Neymar,CN=Users,DC=formation,DC=lab" `  
-TargetPath "OU=Support,OU=Corp,DC=formation,DC=lab"
```

- Variante

```
Get-ADObject "Jean Neymar" | `  
Move-ADObject -TargetPath "OU=Support,OU=Corp,DC=formation,DC=lab"
```

# Utilisateurs

- Annexe à la création d'un Utilisateur : **New-ADUser**
  - Il est possible de configurer le mot de passe de l'utilisateur pendant sa création avec l'attribut **AccountPassword**
  - Et de forcer son changement de mot de passe au prochain login avec l'attribut **ChangePasswordAtLogon**
  - De même l'attribut **Path** permet de positionner l'utilisateur créé directement dans une OU particulière

# Groupes

- Crédation d'un groupe : **NewADGroup**

```
New-ADGroup ` 
    -GroupScope "Global"    -GroupCategory "Security" ` 
    -Name "Groupe Direction"    -SamAccountName "G_Direction"
```

Les attributs obligatoires sont **Name** et **SamAccountName** comme pour un utilisateur, mais en plus il faut préciser le **Type** avec **GroupCategory** et la **Portée** avec **GroupScope**

# Groupes

- Ajouter un utilisateur à un groupe : **Add-ADGroupMember**

```
Add-ADGroupMember ` 
    -Identity "CN=Groupe Direction,OU=Groupes,OU=Corp,DC=formation,DC=lab" ` 
    -Members "jNeymar"
```

- Visualisation des membres du groupe : **Get-ADGroupMember**

```
Get-ADGroupMember -Identity "Groupe Direction"
```

# Recherches dans Active Directory

- Recherches d'objets : **Search-ADAccount**
- Exemple : Recherche d'utilisateurs verrouillés dans tout l'Annuaire

```
Search-ADAccount ` 
    -LockedOut ` 
    -SearchBase "DC=formation,DC=lab" -SearchScope Subtree ` 
    -UsersOnly | Select Name, SID
```

L'étendue des recherches est paramétrable avec **SearchBase** et **SearchScope**

# Recherches dans Active Directory

- Les résultats de la recherche peuvent être filtrés avec **-Filter**

```
Get-ADUser -filter { Title -eq "manager" } `  
| ForEach-Object { Write-Host "$_ est un Responsable de Formation" }
```

De nombreux attributs peuvent être utilisés dans le filtre associés à des RegEx (expressions régulières)

# Ajouter un Ordinateur dans Active Directory

# Sur la station qui va joindre le domaine

- Il faut d'abord disposer d'un compte ayant le droit d'ajouter un ordinateur au domaine

```
$Username = "FORMATION\TechIT"  
$PlainPwd = "Respons11"  
$SecurePwd = $PlainPassword | ConvertTo-SecureString -AsPlainText -Force  
$mycreds = `'  
New-Object System.Management.Automation.PSCredential ($Username, $SecurePwd)
```

# Sur la station qui va joindre le domaine

- Et utiliser ce compte pour joindre la station au domaine

```
add-computer -Credential $mycreds -DomainName formation.lab -force  
Start-Sleep -Seconds 1000  
Restart-Computer
```

Le cmdlet **Start-Sleep** permet d'attendre une minute pour être sur que le contrôleur de domaine a eu le temps de valider la demande

# Gestion des GPO dans Active Directory

# Gestion des GPO

- La gestion utilise 4 cmdlet de base
  - Lister les GPO existantes : **Get-GPO**
  - Créer une GPO : **New-GPO** et **Set-GPPrefRegistryValue**
  - Lier une GPO à une OU : **New-GPLink**
- Il faut d'abord importer un module spécial

```
Import-Module -Name "Group-Policy" -Verbose  
Get-GPO -All -Domain "formation.lab"
```

# Création et application d'une GPO

- D'abord créer une GPO vide : **New-GPO**

```
$NewGPO = New-GPO ` 
    -Name "USER_PREF_Desactiver Menu Exécuter" ` 
    -Domain "formation.lab"
```

# Création et application d'une GPO

- Ensuite configurer la GPO : **Set-GPPrefRegistryValue**

```
$NewGPO | Set-GPPrefRegistryValue  
    -Context "User" `  
    -Key "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" `  
    -ValueName "NoRun"  
    -Type "DWORD" `  
    -Value "1" `  
    -Action "Create"
```

# Création et application d'une GPO

- Lier cette GPO avec une OU : **New-GPLink**

```
New-GPLink `‐  
‐Name "USER_PREF_Desactiver Menu Exécuter" `‐  
‐Target "OU=Accueil,OU=Corp,DC=formation,DC=lab"
```