**GPO avec PowerShell**

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

**Objectifs**

* Utiliser plusieurs cmdlets relatifs aux stratégies de groupe.
* La gestion des filtres WMI ne fait pas parti du document.

**Le lien entre une stratégie et la base de registre**

La configuration d'un paramètre de stratégie de groupe modifie une clé de registre.

Les clés du registre pour la "Configuration utilisateur"

* HKEY\_CURRENT\_USER\Software\Policies
* HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Les clés du registre pour la "Configuration ordinateur"

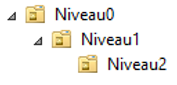
* HKEY\_LOCAL\_MACHINE\Software\Policies
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

**Étape 1 - Mise en place**

Connectez-vous sur votre serveur virtuel "SERVEURV2" avec l’utilisateur "TECH" du domaine

Créer des unités d’organisation

* Sous votre domaine créer la structure d’unités d’organisation suivante.



**Pour la création des unités d'organisation, vous pouvez utiliser la console "Utilisateurs et ordinateurs Active Directory" ou la programmation PowerShell.**

Créer les dossiers C:\\_RAPPORTS et C:\\_BACKUP.

L'annexe à la fin du document contient la liste complète des cmdlets du module GroupPolicy.

**Étape 2 - Gestion des objets de stratégie de groupe (GPO)**

Vous allez utiliser PowerShell pour gérer les objets de stratégie de groupe:

**Création par la console "Gestion de stratégie de groupe"**

Ouvrir la console "Gestion de stratégie de groupe"

Créer un objet

* Dans la section "Objets de stratégie de groupe" créer l’objet GPO "gpoA"

Créer un objet et le lier

* Dans la section "Objets de stratégie de groupe" créer l’objet GPO "gpoB"
* Dans l’unité Niveau2 lier l’objet GPO "gpoB"

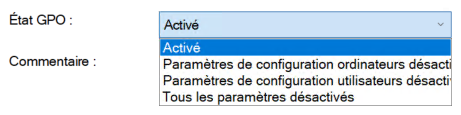
Créer deux objets et lier directement dans les unités

* Directement dans l’unité "Niveau0" créer l’objet GPO "gpoC"
* Directement dans l’unité Niveau1 créer l’objet GPO "gpoD"

La commande pour créer un objet GPO dont le nom est "gpo1"

**New-GPO -Name "gpo1"**

Il est possible de modifier l'état d'une GPO en modifiant la propriété "GpoStatus".



**(Get-GPO -Name "gpo1").GpoStatus = "AllSettingsEnabled"**

**(Get-GPO -Name "gpo1").GpoStatus = "ComputerSettingsDisabled"**

**(Get-GPO -Name "gpo1").GpoStatus = "UserSettingsDisabled"**

**(Get-GPO -Name "gpo1").GpoStatus = "AllSettingsDisabled"**

La commande pour afficher la valeur de "GpoStatus" de l’objet GPO "gpo1"

**(Get-GPO -Name gpo1).GpoStatus**

La commande pour modifier un commentaire à l’objet GPO "gpo1"

**(Get-GPO -Name "gpo1").Description = "La GPO gpo1 n'est pas liée à une OU."**

La commande pour afficher le commentaire de l’objet GPO "gpo1"

**(Get-GPO -Name gpo1).Description**

La commande pour créer un objet GPO et configurer un commentaire.

**New-GPO -Name "gpo2" `**

**-Comment "gpo2 est liée à la OU Niveau0"**

La commande pour lier l’objet GPO "gpo2" à l’unité d'organisation "Niveau0"

**New-GPLink -Name "gpo2" `**

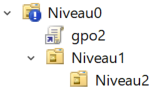
**-Target "ou=Niveau0,dc=formation,dc=local"**

**Étape 3 - Bloquer l'héritage sur une unité d'organisation**

La commande pour bloquer l'héritage sur une OU

**Set-GPinheritance -Target "ou=niveau0,dc=formation,dc=local" `**

**-IsBlocked Yes**



La commande pour ne pas bloquer l'héritage sur une OU

**Set-GPinheritance -Target "ou=niveau0,dc=formation,dc=local" `**

**-IsBlocked No**

**Étape 4 - "Appliqué" une GPO**

**IMPORTANT: Il ne faut pas confondre l'option "Appliqué" et "Lien activé".**

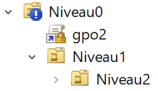


|  |  |
| --- | --- |
| **En français** | **En anglais** |
| Appliqué | Enforced |
| Lien activé | Link Enabled |

**Set-GPLink -Name gpo2 `**

**-Target "ou=niveau0,dc=formation,dc=local" `**

**-Enforced Yes**



Le paramètre **-Enforced** existe également dans **New-GPLink**.

**Étape 5 - Changer l'ordre d'application de la GPO**

La commande qui place une GPO en position 1 donc la plus haute priorité.

**Set-GPLink -Name "gpo2" `**

**-Target "OU=niveau0,DC=formation,DC=local" `**

**-Order 1**

Le paramètre **-Order** existe également dans **New-GPLink**.

**Étape 6 - Suppression d’objets de stratégie de groupe (GPO) et de liaison**

**Supprimer le lien d'une GPO sur une unité d'organisation**

La commande pour supprimer le lien "gpoB" qui est sur l'unité d'organisation "Niveau2" sans confirmation

**Remove-GPlink -Name "gpoB" `**

**-Target "ou=Niveau2,ou=Niveau1,ou=Niveau0,dc=formation,dc=local" `**

**-Confirm:$false**

**Supprimer une GPO**

La commande pour supprimer l’objet GPO "gpoB" sans confirmation

**Remove-GPO -Name gpoB `**

**-Confirm:$false**

**Étape 7 - Créer une GPO et configurer les paramètres avec les clés de registre**

Il est possible de désactiver le "Bureau à distance" à l'aide d'une clé de registre qui n'est pas une GPO.

**New-GPO -Name "PC\_DisableRDP"**

**Set-GPPrefRegistryValue -Name "PC\_DisableRDP" `**

**-Key "HKLM\System\CurrentControlSet\Control\Terminal Server" `**

**-ValueName fDenyTSConnections `**

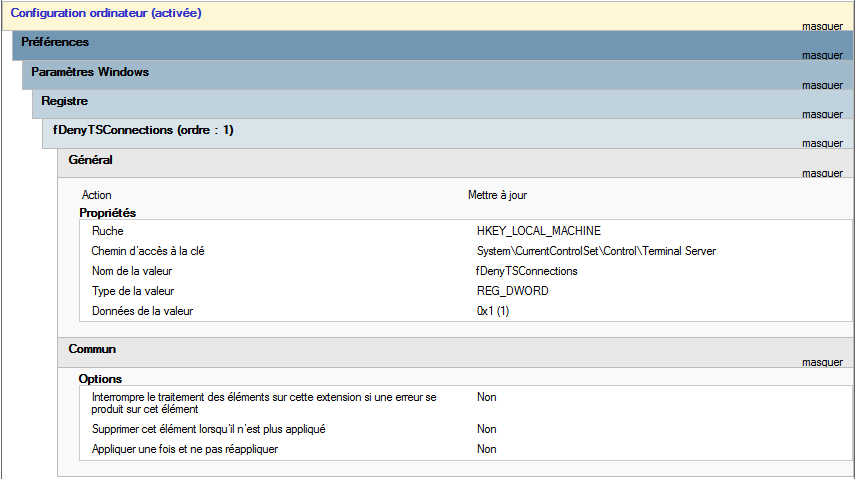
**-Type Dword `**

**-Value 1 `**

**-Context Computer `**

**-Action Update**

**Résultat de la commande**



**Remove-GPPrefRegistryValue -Name "PC\_DisableRDP" `**

**-Key "HKLM\System\CurrentControlSet\Control\Terminal Server" `**

**-Context Computer**

**Résultat de la commande**



Il est possible de désactiver le "Bureau à distance" à l'aide d'une clé de registre qui est une GPO.

Le fichier "Windows11andWindowsServer2019PolicySettings--21H2.xlsx" contient les informations.

**New-GPO -Name "C\_DisableRDP"**

**# Si la valeur est à 0 alors le paramètre de la GPO sera "Désactivé".**

**# Si la valeur est à 1 alors le paramètre de la GPO sera "Activé".**

**Set-GPRegistryValue -Name "C\_DisableRDP" `**

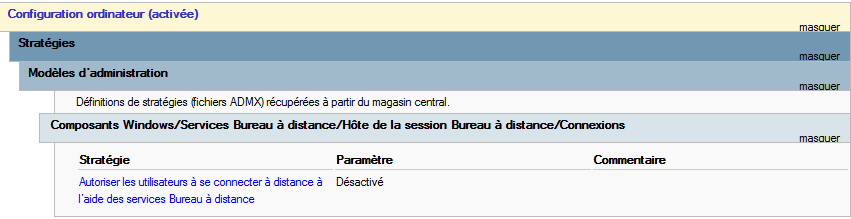
**-Key "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" `**

**-ValueName "fDenyTSConnections" `**

**-Type DWord `**

**-Value 1**

**Résultat de la commande**



**# Le paramètre de la GPO sera "Non configuré".**

**Set-GPRegistryValue -Name "C\_DisableRDP" `**

**-Disable `**

**-Key "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"**

**Résultat de la commande**



**Étape 8 - Mise à jour des GPO**

**Invoke-GPUpdate** est l'équivalent de "**gpupdate.exe**".

**Invoke-GPUpdate -Force**

**Invoke-GPUpdate -Computer "SERVEUR2" `**

**-Target "User" `**

**-Force**

**Étape 9 - Sauvegarder la résultante des stratégies**

**Get-GPResultantSetOfPolicy** est l'équivalent de "**gpresult.exe**".

**Get-GPResultantSetOfPolicy -ReportType Xml `**

**-Path "c:\\_rapports\UserAndComputer.xml"**

**Get-GPResultantSetOfPolicy -ReportType Xml `**

**-Path "c:\\_rapports\SERVEUR2\_UserAndComputer.xml" `**

**-Computer "SERVEUR2"**

**Étape 10 - Création d’un rapport HTML par programmation PowerShell**

La commande pour créer un rapport HTML pour l’objet "C\_DisableRDP"

**Get-GPOReport -Name "C\_DisableRDP" `**

**-ReportType HTML `**

**-Path c:\\_rapports\C\_DisableRDP.html**

**Étape 11 - Sauvegarde des GPO par programmation PowerShell**

La commande pour sauvegarder l’objet "PC\_DisableRDP"

* Emplacement: le dossier C:\\_BACKUP

note: le dossier utilisé pour les backups doit obligatoirement exister

* Description: "La GPO désactive le Bureau à distance"

**Backup-GPO -Name "PC\_DisableRDP" `**

**-Path C:\\_BACKUP `**

**-Comment "La GPO désactive le Bureau à distance"**

**ANNEXE**

Voici la liste des CMDLETS du module GroupPolicy.

**PS C:\\_OUTILS> (Get-Command -Module GroupPolicy).Name**

**Get-GPPermissions**

**Set-GPPermissions**

**Backup-GPO**

**Copy-GPO**

**Get-GPInheritance**

**Get-GPO**

**Get-GPOReport**

**Get-GPPermission**

**Get-GPPrefRegistryValue**

**Get-GPRegistryValue**

**Get-GPResultantSetOfPolicy**

**Get-GPStarterGPO**

**Import-GPO**

**Invoke-GPUpdate**

**New-GPLink**

**New-GPO**

**New-GPStarterGPO**

**Remove-GPLink**

**Remove-GPO**

**Remove-GPPrefRegistryValue**

**Remove-GPRegistryValue**

**Rename-GPO**

**Restore-GPO**

**Set-GPInheritance**

**Set-GPLink**

**Set-GPPermission**

**Set-GPPrefRegistryValue**

**Set-GPRegistryValue**