**PowerShell - WMI - CIM**

Ce laboratoire doit être fait individuellement sur votre serveur réel

Voici trois raisons de ne plus utiliser les cmdlets WMI

Raison 1: Les cmdlets CIM utilisent WS-MAN pour les accès distants.

Raison 2: Les cmdlets WMI utilisent DCOM qui est bloqué par défaut dans le "Pare-feu Windows".

Raison 3: Les cmdlets CIM effectuent du travail à notre place, voir l'exemple 1

**Exemple 1 - Avantage de CimInstance versus WmiObject**

1. **Utilisation de Win32\_OperatingSystem pour afficher la date d'installation du système d'exploitation**

**# Retourne la date d'installation du système d'exploitation**

**$rep1 = (Get-WmiObject Win32\_OperatingSystem).InstallDate**

* $rep1 contient "20160910092428.000000-240"

1. **# Utilisation de Win32\_OperatingSystem pour afficher la date d'installation du système d'exploitation**

**# Retourne la date d'installation du système d'exploitation**

**$rep2 = (Get-CimInstance Win32\_OperatingSystem).InstallDate**

* $rep2 contient "10 septembre 2016 09:24:28"

**Conclusion: La date est plus facile à lire avec Get-CimInstance.**

**Exemple 2 - Utilisation de Get-CimInstance**

**Exemple de l'utilisation de Get-CimInstance avec la classe Win32\_OperatingSystem pour afficher la description d'un ordinateur.**

**Get-CimInstance -ClassName Win32\_OperatingSystem | Select-Object Description**

**# Voici trois façons de vérifier la description d'un ordinateur**

**Get-CimInstance -Query "Select \* from Win32\_OperatingSystem where Description ='ORDI1'"**

**Get-CimInstance -ClassName Win32\_OperatingSystem -Filter "Description ='ORDI1'"**

**Get-CimInstance -ClassName Win32\_OperatingSystem | Where-Object Description -eq "ORDI1"**

**Exemple 3 - Utilisation de Set-CimInstance**

**Exemple de l'utilisation de Set-CimInstance avec la classe Win32\_OperatingSystem pour modifier la description d'un ordinateur.**

**# EXEMPLE 1**

**$nom = Get-CimInstance -ClassName Win32\_OperatingSystem**

**$nom.Description = "ORDI1"**

**Set-CimInstance -CimInstance $nom**

**# EXEMPLE 2**

**$nom = Get-CimInstance -ClassName Win32\_OperatingSystem**

**Set-CimInstance -CimInstance $nom -Property @{Description="ORDI2"}**

**# EXEMPLE 3**

**Set-CimInstance -Query 'Select \* from Win32\_OperatingSystem' `**

**-Property @{Description="ORDI3"}**

**# EXEMPLE 4**

**Get-CimInstance -ClassName Win32\_OperatingSystem | `**

**Set-CimInstance -Property @{Description = "ORDI4"}**

**Exemple 4 - Utilisation de Get-CimInstance et Set-CimInstance**

**# VERSION 1**

**# IMPORTANT: ce code est valide si l'ordinateur est dans un "Groupe de travail"**

NOTE: il n'y a pas de cmdlet pour **déverrouiller** le compte d'un utilisateur local

**Voici le code pour déverrouiller un compte d'un utilisateur local**

**$liste = "ETU","PROF","TECH"**

**$users = Get-CimInstance -ClassName Win32\_UserAccount `**

**-Filter "LocalAccount=True and Lockout=True" | `**

**Where-Object Name -in $liste**

**foreach ($user in $users)**

**{**

**# Affiche le nom de l'utilisateur**

**$nom = $User.name**

**Write-Warning "Nom de l'utilisateur: $nom"**

**# Affiche le contenu de la propriété Lockout avant la modification**

**$user.Lockout**

**# Modification de la propriété Lockout**

**$user.Lockout = "False"**

**# Affiche le contenu de la propriété Lockout après la modification**

**$user.Lockout**

**# Mise à jour de l'utilisateur**

**Set-CimInstance -CimInstance $user**

**}**

**# VERSION 2**

**# IMPORTANT: ce code est valide si l'ordinateur est dans un "Groupe de travail"**

NOTE: il n'y a pas de cmdlet pour **déverrouiller** le compte d'un utilisateur local

**Voici le code pour déverrouiller un compte d'un utilisateur local**

**$liste = "PROF","TECH"**

**$users = Get-CimInstance -ClassName Win32\_UserAccount `**

**-Filter "LocalAccount=True and Lockout=True" | `**

**Where-Object Name -in $liste**

**foreach ($user in $users)**

**{**

**# Mise à jour de l'utilisateur pour déverrouiller son compte**

**Set-CimInstance -CimInstance $user `**

**-Property @{LockOut=$false}**

**$nom = $user.name**

**Write-Warning "Le compte de l'utilisateur est déverrouillé: $nom"**

**}**

**Étape 1 - Utilisation de plusieurs fonctions du namespace ROOT\CIMV2**

Dans PowerShell ISE, écrire les commandes permettant d’obtenir les informations demandées.

**Vous devez utiliser le cmdlet Get-CimInstance du module CimCmdlets.**

**Win32\_ComputerSystem**

Écrire la commande pour afficher toutes les propriétés de win32\_ComputerSystem

get-ciminstance Win32\_ComputerSystem | select-object \*

Écrire la commande qui affiche

* Le nom de votre ordinateur
* Le nom du domaine ou du groupe de travail
* Le nom de l’utilisateur qui est connecté pour exécuter le test
* Pour l'affichage utiliser Format-Table avec le paramètre -AutoSize

get-ciminstance Win32\_ComputerSystem | format-table -autosize Caption,Domain,UserName

**Win32\_Group**

Écrire la commande pour afficher le nom et le SID de tous les groupes de votre ordinateur

* Pour l'affichage utiliser Format-Table avec le paramètre -AutoSize

get-ciminstance Win32\_Group | format-table -autosize Name,SID

**Win32\_UserAccount**

Écrire la commande pour afficher le nom et le SID de tous les usagers de votre ordinateur

* Pour l'affichage utiliser Format-Table avec le paramètre -AutoSize

get-ciminstance Win32\_UserAccount | format-table -autosize Name,SID

**Win32\_Environment**

Écrire la commande pour afficher la valeur de toutes les variables d’environnement de votre ordinateur

* Pour l'affichage utiliser Format-Table avec les paramètres -AutoSize et -Wrap

get-ciminstance Win32\_Environment | Select-Object \* | format-table -autoSize -wrap

**Win32\_VideoController**

Écrire la commande pour afficher des informations sur la carte vidéo de votre ordinateur

* Le nom de votre ordinateur
* Le nom du modèle de la carte vidéo
* Le nom du processeur vidéo
* La résolution de l'écran utilisée et le nombre de couleurs
* La quantié de mémoire sur la carte vidéo
* La version du pilote de la carte vidéo

**Get-CimInstance -ClassName Win32\_VideoController | `**

**Select-Object -Property SystemName,**

**Name,**

**VideoProcessor,**

**AdapterRAM,**

**VideoModeDescription,**

**CurrentRefreshRate,**

**MaxRefreshRate,**

**DriverDate,**

**DriverVersion | Format-List**

**SystemName : VM70035316**

**Name : NVIDIA Quadro M2000**

**VideoProcessor : Quadro M2000**

**AdapterRAM : 4293918720**

**VideoModeDescription : 1680 x 1050 x 4294967296 couleurs**

**CurrentRefreshRate : 59**

**MaxRefreshRate : 75**

**DriverDate : 2021-02-22 19:00:00**

**DriverVersion : 27.21.14.6172**

**Win32\_LogicalDisk**

Afficher la liste des disques locaux présents avec les informations suivantes:

* Leur nom (lettre)
* Leur type
* Leur système de fichier
* Les lecteurs de disque qui ne contiennent pas de média n’ont pas de système de fichier.
* Consulter le fichier "C:\\_Outils\documentation - WMI\wmisdk\_book.chm" pour connaître les valeurs de l’attribut DriveType.
* La taille
* Espace libre
* Pour l'affichage utiliser Format-Table avec les paramètres -AutoSize et -Wrap

Écrire trois réponses en utilisant trois façons différentes de faire cette requête (-filter, -query, where-object)

get-ciminstance Win32\_LogicalDisk -Filter "DriveType = 3" | `

format-table -autosize –wrap DeviceID,Description,FileSystem,Size,FreeSpace

get-ciminstance -Query "Select \* from Win32\_LogicalDisk Where DriveType = 3" | `

format-table -autosize –wrap DeviceID,Description,FileSystem,Size,FreeSpace

get-ciminstance Win32\_LogicalDisk | where-object drivetype -eq 3 | `

format-table -autosize –wrap DeviceID,Description,FileSystem,Size,FreeSpace

**Win32\_Service**

Faire afficher la liste des services dont l’état est à "démarrer" avec les informations suivantes:

* le nom du service
* le nom complet du service
* le chemin
* le mode de démarrage
* Pour l'affichage utiliser Format-List

Écrire trois réponses en utilisant trois façons différentes de faire cette requête (-filter, -query, where-object)

get-ciminstance Win32\_Service -Filter 'state = "running"' | `

format-list name,displayname,pathname,startmode

get-ciminstance -Query 'select \* from Win32\_Service where state = "running"' | `

format-list name,displayname,pathname,startmode

get-ciminstance Win32\_Service | where-object state -eq "Running" | `

format-list name,displayname,pathname,startmode

**Win32\_NetWorkConnection**

Faire afficher le nom et le chemin des disques réseaux présentement connectés

* Pour l'affichage utiliser Format-Table avec le paramètre -AutoSize

get-ciminstance win32\_NetworkConnection | format-table -autosize LocalName,RemoteName

get-ciminstance win32\_NetworkConnection | select-object LocalName,RemoteName | Out-GridView

**Win32\_NetworkAdapter**

Afficher l’index, l’adresse MAC et le nom des cartes réseaux (NetConnectionID).

note 1: le paramètre MACAddress ne doit pas être nul

note 2: le paramètre NetConnectionID ne doit pas être nul

note 3: Pour l'affichage utiliser Format-Table avec les paramètres -AutoSize et -Wrap

Écrire trois réponses en utilisant trois façons différentes de faire cette requête (-filter, -query, where-object)

get-ciminstance Win32\_NetworkAdapter `

-Filter "MACAddress is not null and NetConnectionID is not null" | `

format-table -autosize –wrap Index,MACAddress,NetConnectionID

get-ciminstance -Query "select \* from Win32\_NetworkAdapter where `

MACAddress is not null and NetConnectionID is not null" | `

format-table -autosize –wrap Index,MACAddress,NetConnectionID

get-ciminstance Win32\_NetworkAdapter | `

where-object { $PSItem.MACAddress -ne $null -and $PSItem.NetConnectionID -ne $null } | `

format-table -autosize –wrap Index,MACAddress,NetConnectionID

**Win32\_NetworkAdapterConfiguration**

Afficher l’index, la description des cartes réseaux, l'adresse MAC, l’adresse IP, le masque de sous-réseau, la passerelle, les adresses des serveurs DNS

note 1: le paramètre MACAddress ne doit pas être nul

note 2: le paramètre Description net doit pas être nul

note 3: Pour l'affichage utiliser Format-List

Écrire trois réponses en utilisant trois façons différentes de faire cette requête (-filter, -query, where-object)

get-ciminstance Win32\_NetworkAdapterConfiguration `

-Filter "MACAddress is not null and Description is not null" | `

FL Index,Description,MACAddress,IPAddress,IPSubnet,DefaultIPGateway,DNSServerSearchOrder

get-ciminstance -Query "select \* from Win32\_NetworkAdapterConfiguration where `

MACAddress is not null and Description is not null" | `

FL Index,Description,MACAddress,IPAddress,IPSubnet,DefaultIPGateway,DNSServerSearchOrder

get-ciminstance Win32\_NetworkAdapterConfiguration | `

where-object { $PSItem.MACAddress -ne $null -and $PSItem.Description -ne $null } | `

FL Index,Description,MACAddress,IPAddress,IPSubnet,DefaultIPGateway,DNSServerSearchOrder

**Win32\_BIOS**

Les propriétés de Win32\_BIOS sont en lecture seulement.

**Clear-Host**

**$computer = $env:COMPUTERNAME**

**$namespace = "ROOT\CIMV2"**

**$classname = "Win32\_BIOS"**

**Write-Output "====================================="**

**Write-Output "Computer : $computer"**

**Write-Outpui "NameSpace : $namespace"**

**Write-Output "ClassName : $classname"**

**Write-Output "====================================="**

**Get-CimInstance -Namespace $namespace -ClassName $classname**

**La compagnie "Hewlett Packard Enterprise" offre un module PowerShell pour administrer le BIOS des serveurs. Le module "HPEBIOSCmdlets" permet de modifier les propriétés du BIOS.**

Le module "**HPEBIOSCmdlets**" est offert avec des scripts pour faciliter la gestion du BIOS.

* ConfigureAdminInfo.ps1
* ConfigureAMDCorePerformanceBoosting.ps1
* ConfigureBIOSAdminPassword.ps1
* ConfigureBootMode.ps1
* ConfigureBootOrder.ps1
* ConfigureEMSConsoleAndSerialPort.ps1
* ConfigureIntelCoreBoosting.ps1
* ConfigureIntelTurboBoost.ps1
* ConfigureNetworkBootsettings.ps1
* ConfigureNVDIMMConfiguration.ps1
* ConfigurePCIDeviceWithPCIeLinkSpeedForGen10.ps1
* ConfigurePowerOnPassword.ps1
* ConfigureProcessorJitterControl.ps1
* ConfigureProcessorPower.ps1
* ConfigureServerAvailability.ps1
* ConfigureServerSecurity.ps1
* ConfigureThermalAndFanOption.ps1
* ConfigureTPM.ps1
* ConfigureUEFIOptimizedBoot.ps1
* ConfigureVirtualInstallDisk.ps1
* ConfigureWorkloadProfileForGen10servers.ps1
* ResetBIOSAdminPassword.ps1
* ResetBIOSDefaultManufacturingSettings.ps1
* ResetPowerOnPassword.ps1

**Étape 2 - Exemple avec une fonction dans le namespace ROOT\virtualization\V2**

Programme pour afficher le GUID du BIOS de chaque ordinateur virtuel.

**Clear-Host**

**$VMNames = (Get-VM).Name**

**ForEach ($VMName in $VMNames)**

**{**

**Get-CimInstance -Namespace Root\Virtualization\V2 `**

**-ClassName Msvm\_VirtualSystemSettingData `**

**-Filter "ElementName = '$VMName'" `**

**| Select-Object ElementName,BiosGUID**

**}**

## Stratégie de groupe locale avec Windows

Le service "Client de stratégie de groupe" (gpsvc) est responsable de l’application des paramètres configurés par les administrateurs pour l’ordinateur et pour les utilisateurs.

Les fichiers ADMX et ADML

* les fichiers ADMX sont dans le dossier c:\windows\PolicyDefinitions
* les fichiers ADML sont dans le dossier c:\windows\PolicyDefinitions\fr-FR

les fichiers ADML sont des fichiers spécifiques à la langue

On peut ajouter des fichiers ADMX et ADML supplémentaires.

Microsoft distribue des fichiers ADMX et ADML pour "**Office 365 - Office 219 - Office 216**".

**Administrative Template files (ADMX/ADML) and Office Customization Tool for Microsoft 365 Apps for enterprise, Office 2019, and Office 2016**

* admintemplates\_x64\_5191-1000\_en-us.exe
* office2016grouppolicyandoctsettings.xlsx

Microsoft distribue des fichiers ADMX et ADML pour "Edge Chromium".

* MicrosoftEdgePolicyTemplates.zip

Google distribue des fichiers ADMX et ADML pour "Chrome".

* policy\_templates.zip

**Lien entre stratégie de groupe locale et le registe**

La "Stratégie de groupe locale" permet de configurer des restrictions pour l'utilisation de Windows en spécifiant des paramètres à appliquer à l'ordinateur ou à l'utilisateur.

Lorsqu'on configure un paramètre de la stratégie de groupe locale on 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

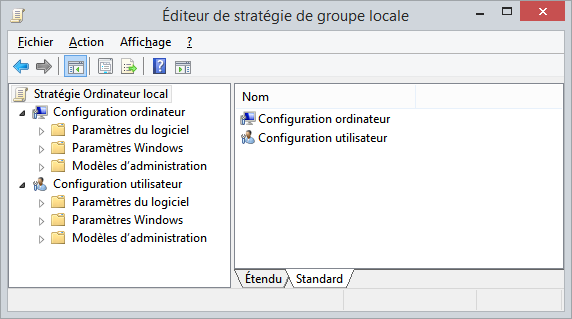
Les clés du registre pour la "Configuration ordinateur":

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

"Windows Serveur 2019" et "Windows 10" permettent de configurer environ 4500 stratégies.

**Les paramètres qui sont dans les Stratégies ne peuvent pas être modifiés par l'utilisateur.**

On démarre l'éditeur de stratégie de groupe locale avec gpedit.msc.



**GPEDIT.MSC et la "Configuration ordinateur**"

* Lorsque l’on configure la partie "**Configuration ordinateur**", elle s’applique que si la GPO est liée à une OU contenant des ordinateurs.
* Les paramètres de la stratégie de l'ordinateur sont appliqués lors du démarrage du poste et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.

Les fichiers POL pour la configuration ordinateur

* %ALLUSERSPROFILE%\ntuser.pol
* %windir%\system32\GroupPolicy\Machine\Registry.pol

**GPEDIT.MSC et la "Configuration utilisateur"**

* Lorsque l’on configure la partie "**Configuration utilisateur**", elle s’applique que si la GPO est liée à une OU contenant des utilisateurs.
* Les paramètres de la stratégie utilisateur sont appliqués à l'ouverture d'une session et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.

Les fichiers POL de la configuration utilisateur

* %USERPROFILE%\ntuser.pol
* %windir%\system32\GroupPolicy\User\Registry.pol

Les outils avec une interface graphique

* **gpedit.msc** est l’éditeur de stratégie de groupe locale
* **rsop.msc**

Cet outil affiche le jeu de stratégies résultant (RSoP).

Cet outil ne permet pas de sauvegarder le résultat.

RSOP (Resultant Set of Policy)

Les programmes sans interface graphique

* **gpresult.exe**

Cet outil de ligne de commande affiche le jeu de stratégies résultant (RSoP).

Cet outil permet de sauvegarder le résultat de la commande dans un fichier HTML.

* **gpupdate.exe**

Cet outil met à jour les paramètres de stratégie de groupe.

**exemples**

* Il est possible de gérer l'accès aux périphériques amovibles (USB, CD-RW, DVD-RW, ...)

si on modifie un des nombreux paramètres dans

Configuration ordinateur / Modèles d'administration / Système / Accès au stockage amovible

* Il est possible de modifier la liste des utilisateurs qui peuvent changer le fuseau horaire

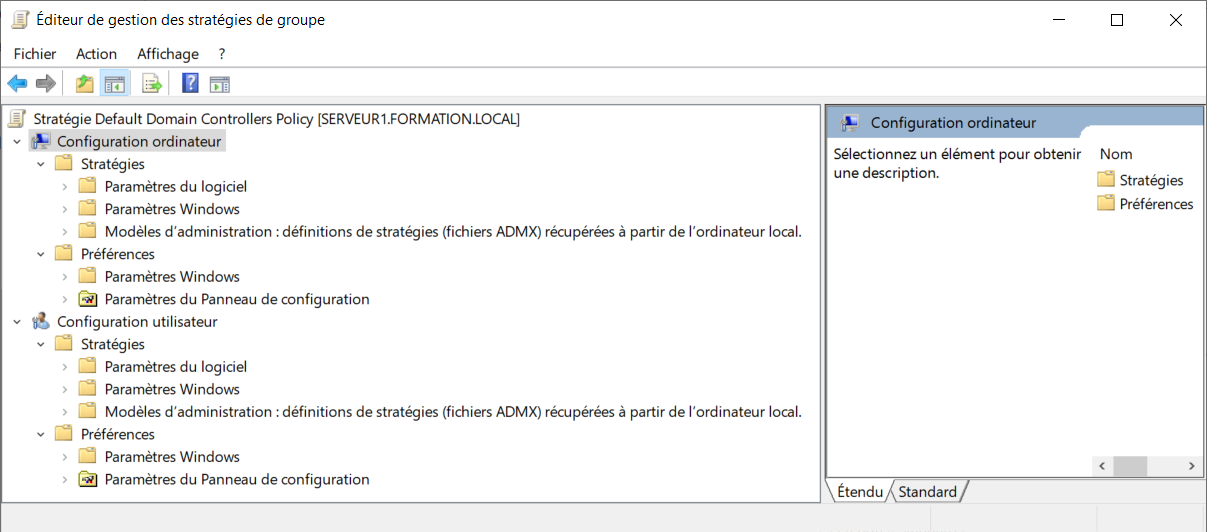
si on modifie le paramètre "Changer le fuseau horaire" dans

Configuration ordinateur / Paramètres Windows / Paramètres de sécurité /

Stratégies locales / Attribution des droits utilisateur

**Les GPO dans un domaine**

Les stratégies de groupe permettent une gestion centralisée des ordinateurs et des utilisateurs dans un environnement Active Directory.



Dans un domaine, un administrateur peut configurer des Stratégies et des Préférences.

Les paramètres qui sont dans les Préférence peuvent être modifiés par l'utilisateur.

Une GPO peut être liée

* à une OU 🡺 on la voit sous la OU
* à plusieurs OU 🡺 on la voit sous chaque OU
* à aucune OU 🡺 on la voit seulement dans la section OSG (Objets de stratégie de groupe)

Les GPO sont emmagasinées dans SYSVOL.

Dans un domaine, il existe deux GPO par défaut:

* Default Domain Policy
* Default Domain Controllers Policy

**Documentation sur l'ordre d'exécution des GPO**

L'ordre d'exécution des GPO respecte la formule LSDOU.

L pour Locale

S pour Site

D pour Domaine

OU pour "Unité d'organisation"

**Les bonnes pratiques pour la gestion des GPO**

1. Ne modifiez pas les stratégies "**Default Domain Policy**" et "**Default Domain Controller Policy**".

Si vous devez modifier des paramètres dans ces stratégies, vous devez créer d'autres stratégies.

1. Votre structure Active Directory doit faciliter l'application des stratégies.

La conception d’UO a une incidence sur le déploiement des stratégies de groupe.

Il est important de ne pas mélanger les comptes utilisateurs et ordinateurs dans une même UO.

Ne gardez pas les utilisateurs et les ordinateurs dans les conteneurs "**Users**" et "**Computers**".

1. Vous devez donner des noms significatifs à vos stratégies.

Les stratégies qui s'appliquent à des utilisateurs **U\_nom\_de\_la\_GPO**

Les stratégies qui s'appliquent à des ordinateurs **C\_nom\_de\_la\_GPO**

Les préférences qui s'appliquent à des utilisateurs **PU\_nom\_de\_la\_GPO**

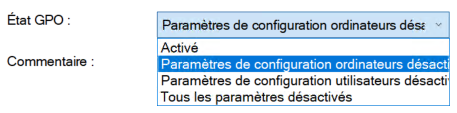
Les préférences qui s'appliquent à des ordinateurs **PC\_nom\_de\_la\_GPO**

1. Il est recommandé d'ajouter des commentaires à vos stratégies.
2. Vous ne devez pas créer des stratégies au niveau du domaine.

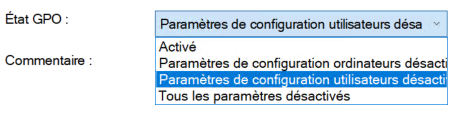
Parce que les stratégies s'appliquent à tous les utilisateurs et à tous les ordinateurs du domaine.

1. Il est préférable de créer plusieurs petites stratégies.
2. Pour augmenter la vitesse d'application des stratégies

Il faut désactiver les paramètres de configuration ordinateurs si la stratégie n'a aucun paramètre dans la section "**Configuration ordinateur**".



Il faut désactiver les paramètres de configuration utilisateurs si la stratégie n'a aucun paramètre dans la section "**Configuration utilisateur**".



## Stratégies de domaine

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

**Objectifs**

* Utiliser l’éditeur des objets de stratégies de groupe
* Se familiariser avec les objets de stratégie "Default Domain Policy" et "Default Domain Controllers Policy"
* Créer des objets de stratégie de groupe au niveau du domaine

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

* Default Domain Controllers Policy
* Default Domain Policy

**Par défaut, les paramètres de la stratégie de l'ordinateur sont appliqués lors du démarrage du poste et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.**

**Par défaut, les paramètres de la stratégie utilisateur sont appliqués à l'ouverture d'une session et mis à jour aux 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes sur les postes clients mais aux 5 minutes sur le contrôleur de domaine.**

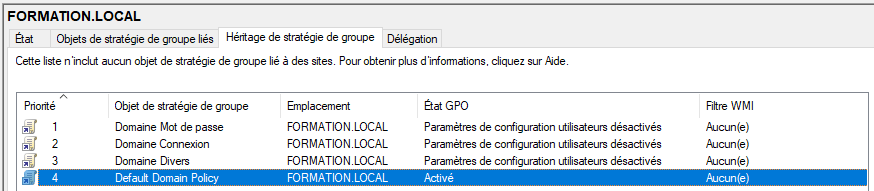
**Documentation sur les GPO qui sont liées au domaine**

Les paramètres qui sont dans la section "**Configuration utilisateur**" d'une stratégie de groupe qui est liée au niveau du domaine s'appliquent à tous les utilisateurs du domaine même si les utilisateurs sont dans le conteneur "**Users**".

Les paramètres qui sont dans la section "**Configuration ordinateur**" d'une stratégie de groupe qui est liée au niveau du domaine s'appliquent à tous les ordinateurs du domaine même si les ordinateurs sont dans le conteneur "**Computers**".

**Documentation sur la priorité d'exécution des GPO**

L’exécution commence par la dernière, celle qui a le chiffre le plus gros et termine par celle qui a le numéro 1, donc la plus haute priorité.



La GPO qui s'exécute en premier est "Default Domain Policy".

Si un administrateur veut modifier des paramètres qui sont dans "Default Domain Policy".

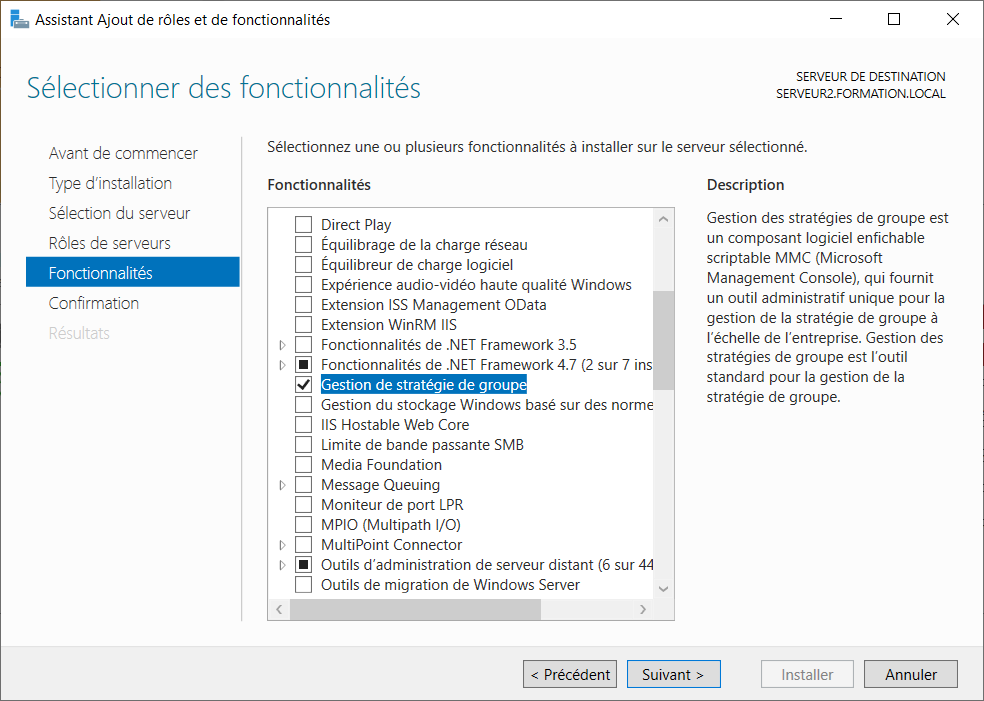
1. Il va créer des GPO qui vont modifier les paramètres.
2. Il va s'assurer que ses GPO vont s'exécuter après la GPO "Default Domain Policy".

**Si un même paramètre existe dans une autre GPO alors le paramètre est remplacé par l'exécution d'une GPO qui a une plus grande priorité d'exécution.**

**La console "Gestion des stratégies de groupe"**

La console "**Gestion des stratégies de groupe**" est présente sur le serveur virtuel SERVEUR1 parce que c'est le contrôleur de domaine.

Sur votre serveur virtuel SERVEUR2, vous devez installer la console "**Gestion des stratégies de groupe**"



**Étape 1 - La GPO "Default Domain Policy"**

Vous devez créer un rapport HTM de la GPO "Default Domain Policy" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "Default Domain Policy" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

Voici la section du rapport "HTM" que vous devez consulter pour répondre aux prochaines questions.

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes /**

**Stratégie de mot de passe**

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

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**42 jours**

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

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**1 jour**

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

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**24**

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

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Oui, le paramètre est activé**

* Quelle est la longueur minimale des mots de passe ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**7 caractères**

En utilisant la console "Gestion des stratégies de groupe" sélectionner la GPO "Default Domain Policy"

* Vous devez choisir "**Modifier…**" dans le menu contextuel.
* Vous devez sélectionner le paramètre.
* Vous devez afficher les propriétés du paramètre et cliquer sur l’onglet "**Expliquer**".

Voici la section que vous devez consulter pour répondre aux prochaines questions.

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes /**

**Stratégie de mot de passe**

* Quelles valeurs sont recommandées comme durée maximale ?

réponse: **De 30 à 90 jours**

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

réponse: **Le nombre de jours avant que l’usager puisse changer son mot de passe.**

* Quel est le nombre maximal de mots de passe qu’on peut conserver dans l’historique ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**24**

* Quelle est la plus grande longueur minimale pour les mots de passe ?

réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**14 caractères**

Voici la section que vous devez consulter pour répondre à la prochaine question.

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes /**

**Stratégie de verrouillage du compte**

* 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 verrouillé si l'utilisateur entre un mauvais mot de passe.**

**Étape 2 - La GPO "Default Domain Controllers Policy"**

Vous devez créer un rapport HTM de la GPO "Default Domain Controllers Policy" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "Default Domain Controllers Policy" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

Voici la section du rapport "HTM" que vous devez consulter pour répondre aux prochaines questions.

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales /**

**Attribution des droits utilisateur**

Vous devez vérifier si les groupes mentionnés sont présents dans les paramètres suivants.

Vous devez répondre par **absent** ou **présent**.

* **Accéder à cet ordinateur à partir du réseau**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **présent**

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **présent**

Tout le monde réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **présent**

* **Ajouter des stations de travail au domaine**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **présent**

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **absent**

* **Arrêter le système**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **absent**

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **présent**

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

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **absent**

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **présent**

* **Modifier l’heure système**

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **absent**

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **présent**

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

AUTORITE NT\Utilisateurs authentifiés réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **absent**

BUILTIN\Administrateurs réponse: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **présent**

**Ce qui veut dire que les utilisateurs qui ne sont pas membres du groupe Administrateurs ne peuvent pas se connecter sur le "Contrôleur de domaine".**

**Étape 3 - Création de stratégies au niveau du domaine**

Dans la console "Gestion des stratégies de groupe"

* Créer les GPO suivants dans la section "Objets de stratégies de groupe"

La GPO "C\_Domaine Mot de passe" qui définit des paramètres sur les mots de passe

La GPO "C\_Domaine Connexion" qui définit des paramètres pour l'ouverture de session

La GPO "C\_Domaine Divers" qui définit divers paramètres

**note: au début chaque GPO est vide**

* Fixer les paramètres mentionnés pour chaque GPO.

**note: présentement, les GPO ne sont liés à aucune unité d’organisation**

**La GPO "C\_Domaine Mot de passe"**

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO"

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies de comptes /**

**Stratégie de mot de passe**

* Durée de vie maximale du mot de passe

**note: configurer la valeur de ce paramètre à 365 jours**

* Durée de vie minimale du mot de passe

**note: configurer la valeur de ce paramètre à 0 jours**

* Longueur minimale du mot de passe

**note: configurer la valeur de ce paramètre à 9 caractères**

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales /**

**Options de sécurité**

* Ouverture de session interactive: prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il n'expire

**note: configurer la valeur de ce paramètre à 7 jours**

Vous devez créer un rapport HTM de de la GPO "C\_Domaine Mot de passe" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "C\_Domaine Mot de passe" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

**La GPO "C\_Domaine Divers"**

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO"

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales /**

**Options de sécurité**

* Arrêt: permet au système d’être arrêté sans avoir à se connecter

**note: configurer la valeur de ce paramètre à Activé**

**Configuration ordinateur / Stratégies / Modèles d'administration / Composants Windows / Windows PowerShell**

* Activer l’exécution des scripts

**note: configurer la valeur de ce paramètre à "Autoriser tous les scripts"**

Vous devez créer un rapport HTM de de la GPO "C\_Domaine Divers" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "C\_Domaine Divers" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

**La GPO "C\_Domaine Connexion"**

La section utilisateur doit être désactivée sur la GPO, onglet "Détails", paramètre "État GPO"

**Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales /**

**Options de sécurité**

* Ouverture de session interactive: ne pas afficher le nom du dernier utilisateur connecté

**note: configurer la valeur de ce paramètre à Activé**

* Ouvertures de sessions interactives: nombre d’ouverture de sessions précédentes réalisées en utilisant la cache (lorsqu'aucun contrôleur de domaine n'est disponible)

**note: configurer la valeur de ce paramètre à 0**

**Configuration ordinateur / Stratégies / Modèles d'administration / Composants Windows /**

**Options d'ouverture de session Windows**

* Afficher les informations sur les ouvertures de session précédentes au cours d'une ouverture de session utilisateur

**note: configurer la valeur de ce paramètre à Activé**

**Configuration ordinateur / Stratégies/ Modèles d'administration / Système**

* Afficher le moniteur d’évènements de mise hors tension

**note: configurer la valeur de ce paramètre à Désactivé**

**Configuration ordinateur / Stratégies / Modèles d'administration / Système / Ouverture de session**

* Toujours attendre le réseau lors du démarrage de l’ordinateur et de l’ouverture de session

**note: configurer la valeur de ce paramètre à Activé**

Vous devez créer un rapport HTM de de la GPO "C\_Domaine Connexion" dans le dossier C:\\_GPO\_RAPPORTS.

* Vous devez sélectionner la GPO "C\_Domaine Connexion" et dans le menu contextuel sélectionner "**Enregistrer le rapport…**".

**Étape 4 - Vérification**

Dans la console de gestion des GPO

* Lier les GPO au niveau du domaine
* Dans *Ordre des liens*, faire correspondre le plus petit chiffre (le chiffre 1) à la GPO "Domaine Mot de passe"

Rectifier l’ordre des GPO au besoin

Inscrire l’ordre final des liens dans le tableau suivant:

|  |  |
| --- | --- |
| **Stratégie** | **Ordre** |
| **C\_Domaine Mot de passe** | **1** |
| **C\_Domaine Connexion** | **2 ou 3** |
| **C\_Domaine Divers** | **2 ou 3** |
| **Default Domain Policy** | **4 - Cette stratégie doit être complètement en bas de la liste.** |

Ouvrir une "Invite de commandes" en tant qu'administrateur et exécuter la commande "**gpupdate.exe /force**".

Fermer la session de FORMATION\TECH sur le SERVEUR2.

Avant d’entrer le nom de l'utilisateur et le mot de passe, remarquez le bouton en bas à droite de l’écran.

C’est à cause de la GPO "C\_Domaine Divers" (permet au système d’être arrêté sans avoir à se connecter).

Ouvrir une session en tant que FORMATION\TECH.

Remarquez les informations qui sont affichées tout de suite après l'ouverture de session (écran bleu).

C’est à cause de la GPO "C\_Domaine Connexion" (afficher les informations lors de l'ouverture de session).

Le changement de mot de passe de l'utilisateur TECH pour **Secret1** sera refusé.

Comparer les rubriques "Longueur minimale du mot de passe" des GPO "C\_Domaine Mot de passe" et "Default Domain Policy".

Que concluez-vous ? **La GPO "C\_Domaine Mot de passe" a priorité sur "Default Domain Policy" à cause de l'ordre d'application des GPO.**

**Étape 5 - Créer une sauvegarde des GPO**

Vous devez créer une copie de sécurité de toutes les GPO dans le dossier C:\\_GPO\_BACKUP.

* Dans le menu contextuel de "**Objets de stratégie de groupe**"
* Vous devez sélectionner l'option "**Sauvegarder tout…**"

**Étape 6 - Supprimer des GPO et les récupérer dans la sauvegarde**

Vous devez supprimer les GPO "C\_Domaine Mot de passe", "C\_Domaine Divers" et "C\_Domaine Connexion".

* Dans le menu contextuel de "**Objets de stratégie de groupe**"
* Vous devez sélectionner l'option "**Gérer les sauvegarde…**"

Vous devez restaurer une GPO à la fois.

Vous devez lier chaque GPO au domaine.

**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**

## Stratégies "Utilisateur"

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

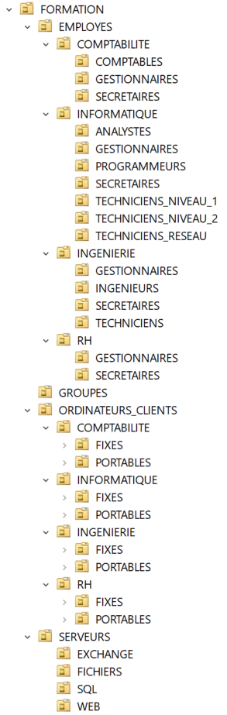
**Objectifs**

* Maîtriser la création d’un objet GPO, section Utilisateur contenant des stratégies et des préférences
* Maîtriser la modélisation et les rapports résultants

**Étape 1 - Mise en place**

Les unités d’organisations et les utilisateurs de l'unité d'organisation FORMATION doivent exister.

**Voici la structure des 41 unités d'organisation**



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

* Default Domain Controllers Policy
* Default Domain Policy

**Étape 2 - Création d’un objet de stratégie de groupe**

Créer la stratégie "**U\_EMPLOYES**" et la lier à votre unité d'organisation "**EMPLOYES**"

Désactiver la section "Ordinateur" de votre stratégie

Modifier votre stratégie "U\_EMPLOYES" en paramétrant ce qui suit:

**Paramètres pour l'utilisateur**

**Configuration utilisateur / Stratégies / Modèles d'administration / Bureau / Bureau**

Vous devez trouver un fichier JPG qui servira de fond d’écran et qui sera déposé dans le partage NETLOGON. Vous devez donner un nom significatif au fichier, par exemple "Logo\_Corpo.jpg".

"Papier peint du Bureau"

* Activé

Nom du papier peint = \\formation.local\netlogon\Logo\_Corpo.jpg

Style du papier peint = Remplir

**Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration**

"Toujours afficher tous les éléments du Panneau de configuration à son ouverture"

* Activé

**Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration / Personnalisation**

"Forcer un écran de veille spécifique"

* Activé

Nom du fichier exécutable de l'écran de veille: bubbles.scr

**Configuration utilisateur / Stratégies / Modèles d'administration / Composants Windows / Explorateur de fichiers**

"Démarrer l'Explorateur de fichiers avec le ruban réduit"

* Activé

Sélectionner: "Ne jamais ouvrir de nouvelles fenêtres de l'Explorateur de fichiers avec le ruban réduit"

**Étape 3 - Validation**

**Sur votre serveur virtuel 2**

Ouvrir une session avec un des utilisateurs de l'unité d'organisation FORMATION

note: le nom des utilisateurs varie de **EMP01** à **EMP32**

* Vérifier l’application de chaque paramètre de votre stratégie "EMPLOYES\_GPO"
* Fermer la session

**Tableau résumé**

|  |  |
| --- | --- |
| **Paramètres** | **EMP01 à EMP32**  **Répondre par Oui ou NON** |
| Papier peint (Logo\_Corpo.jpg) | **OUI** |
| Affichage du panneau de configuration (pas en catégorie) | **OUI** |
| Écran de veille est "Bulles" | **OUI** |
| Explorateur de fichiers ouvre sans le ruban réduit | **OUI** |

**Étape 4 - Modélisation**

Dans la console "Gestion de stratégie de groupe"

* Section "Modélisation de stratégie de groupe"
* Menu contextuel
* Sélectionner "Assistant Modélisation de stratégie de groupe..."

Les configurations générales à effectuer dans l'Assistant de modélisation

* Sélection du contrôleur de domaine
* Sélectionner l'option "Tout contrôleur de domaine exécutant …"
* Sélection d'ordinateurs et d'utilisateurs
* Sélectionner "Utilisateur"

Parcourir pour sélectionner l’utilisateur visé par la modélisation

* Sélectionner "Ordinateur"

Parcourir pour sélectionner le serveur virtuel 2

* Cocher l'option "Se rendre à la dernière page de cet Assistant …"

Lorsque le rapport s'affiche, il est possible de l'enregistrer dans un fichier HTML.

**Étape 5 - Jeu de stratégies résultant**

**Sur votre serveur virtuel 2**

Ouvrir une session avec un des utilisateurs de l'unité d'organisation FORMATION

note: le nom des utilisateurs varie de **EMP01** à **EMP32**

Exécuter la commande suivante: RSOP.MSC

**Le refus sur la section Ordinateur est normal étant donné que les utilisateurs de l'unité d'organisation FORMATION ne sont pas membres du groupe "Administrateurs".**

RSOP.MSC affiche le jeu de stratégies résultant dans une fenêtre.

RSOP.MSC ne permet pas de sauvegarder le résultat dans un fichier.

Exécuter la commande suivante dans une invite de commandes (ne pas exécuter en tant qu'administrateur)

* **gpresult.exe /SCOPE USER /H C:\\_outils\rapport\_EMPxx.html /F**

Consulter le fichier C:\\_GPO\rapport\_EMP20.html

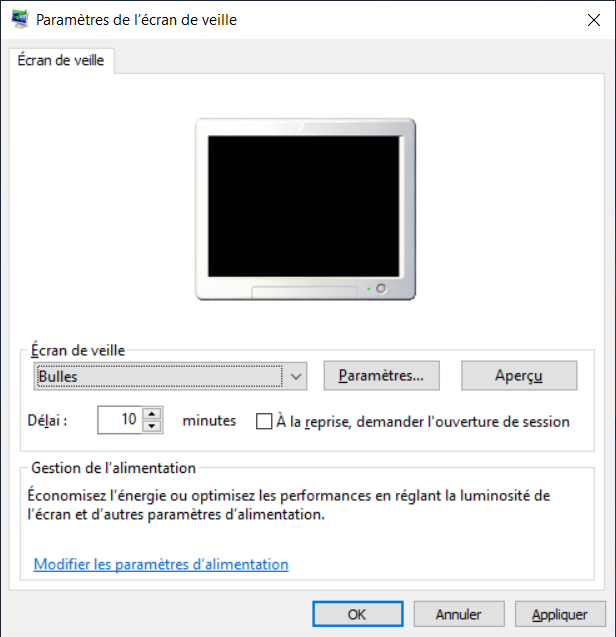
Fermer cette session

**La commande gpresult.exe permet de sauvegarder le résultat dans un fichier HTML.**

**ANNEXE**

Comment ouvrir la console "**Paramètres de l'écran de veille**" avec une commande.

**control.exe desk.cpl,screensaver,@screensaver**



## Préférences UTILISATEUR

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

**Objectif**

* Introduction aux préférences

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

* Default Domain Controllers Policy
* Default Domain Policy

Les préférences sont des paramètres que les utilisateurs peuvent modifier.

Lors de la création d'une préférence, nous devons choisir entre Créer, Remplacer, Mette à jour, Supprimer

Exemples avec la préférence "**Mappages de lecteurs**" pour les utilisateurs

**Créer**

Permet de créer un nouveau lecteur réseau mappé pour les utilisateurs.

**Remplacer**

Permet de supprimer et de recréer les lecteurs mappés pour les utilisateurs.

Le résultat de l’action Remplacer est d’écraser tous les paramètres existants associés au lecteur mappé.

Si le mappage du lecteur n’existe pas, l’action Remplacer crée un nouveau mappage du lecteur.

**Mettre à jour**

Permet de modifier les paramètres d’un lecteur mappé existant pour les utilisateurs.

Le résultat de l'action "Mettre à jour" est de mettre à jour que les paramètres définis dans la "Préférences".

Tous les autres paramètres restent configurés sur le lecteur mappé.

Si le mappage du lecteur n’existe pas, l’action "Mettre à jour" crée un nouveau mappage du lecteur.

**Supprimer**

Permet de supprimer un lecteur réseau mappé pour les utilisateurs.

|  |  |  |
| --- | --- | --- |
| Créer | Un triangle vert est présent. |  |
| Remplacer | Un triangle rouge est présent. |  |
| Mettre à jour | Un triangle jaune est présent. |  |
| Supprimer | Un X rouge est présent. |  |

**Création d’une GPO de préférences au niveau de la UO EMPLOYES**

Créer la GPO "**PU\_EMPLOYES**" et la lier à votre unité d'organisation "**EMPLOYES**"

Désactiver la section "Configuration ordinateur".

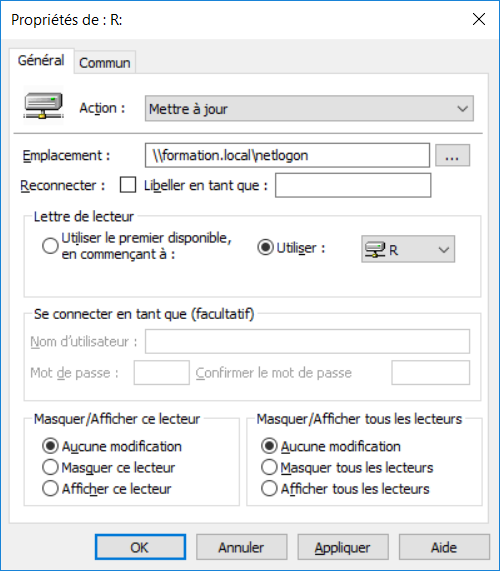
Toutes les options se trouvent dans la section "Configuration utilisateur / Préférences"

**Configuration utilisateur / Préférences / Paramètres Windows / Mappages de lecteurs**

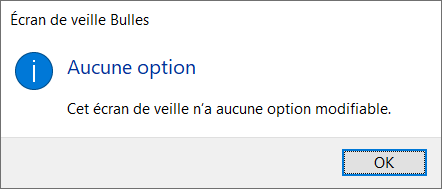
Lier la lettre R: au partage "netlogon" de votre domaine.

* **Mappages de lecteurs**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Lecteur mappé"



* Action: Mette à jour
* Emplacement: [\\formation.local\netlogon](file:///\\formation.local\netlogon)
* Utiliser: R
* Cliquer sur le bouton Appliquer
* Cliquer sur le bouton OK

**Configuration utilisateur / Préférences / Paramètres Windows / Registre**

Par défaut, l'écran de veille "Bulles" ne permet pas de modifier le comportement des bulles.

En modifiant le registre Windows, il est possible de modifier l'aspect des bulles pour l'écran de veille "Bulles".

* **Registre**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Élément Registre"

* Action: Mettre à jour
* Ruche: HKEY\_CURRENT\_USER
* Chemin d'accès de la clé: Software\Microsoft\Windows\CurrentVersion\Screensavers\Bubbles
* Nom de valeur: MaterialGlass
* Type de valeur: REG\_DWORD
* Données de valeur: 0
* Cliquer sur le bouton Appliquer
* Cliquer sur le bouton OK

MaterialGlass

* 0 pour afficher des bulles métalliques
* 1 pour afficher des bulles transparentes

**Configuration utilisateur / Préférences / Paramètres Windows / Raccourcis**

Créer un raccourci sur le Bureau vers NCPA.CPL

* **Raccourcis**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Raccourci"

* Action: Mettre à jour
* Nom: Connexions réseau
* Type de cible: Objet du système de fichiers
* Emplacement: Bureau
* Chemin d’accès cible: c:\windows\system32\ncpa.cpl
* Chemin d'accès du fichier d’icône: c:\windows\system32\netshell.dll
* Index de l’icône: 0
* Cliquer sur le bouton Appliquer
* Cliquer sur le bouton OK

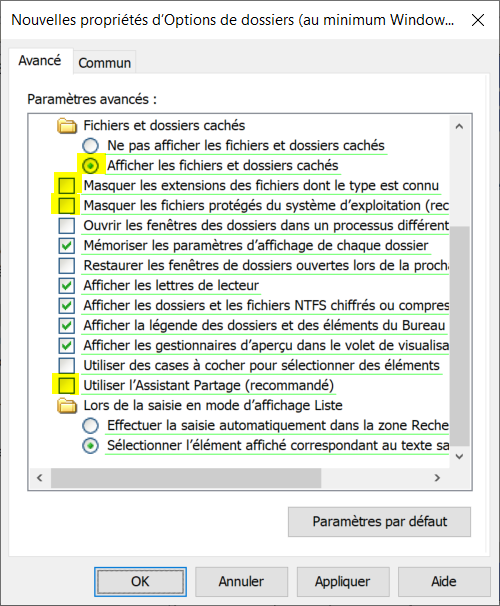
**Configuration utilisateur / Préférences / Paramètres du Panneau de configuration / Options des dossiers**

Configurer les options de dossiers qui permettront

* **Options des dossiers**

dans le menu contextuel de la fenêtre blanche,

sélectionner "Nouveau / Options des dossiers (au minimum Windows Vista)"



* ACTIVÉ Afficher les fichiers et dossiers cachés
* DÉSACTIVÉ Masquer les extensions des fichiers dont le type est connu
* DÉSACTIVÉ Masques les fichiers protégés du système d'exploitation (recommandé)
* DÉSACTIVÉ Utiliser l'assistant de Partage (recommandé)
* Cliquer sur le bouton Appliquer
* Cliquer sur le bouton OK

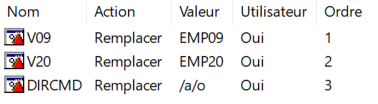
**Création d’une GPO de préférences au niveau de la UO INFORMATIQUE**

Créer une GPO "**PU\_INFORMATIQUE\_CIBLAGE\_EMP09\_EMP20**" et la lier à votre unité d'organisation "**INFORMATIQUE**"

Désactiver la section "Configuration ordinateur".

Toutes les options se trouvent dans la section "Configuration utilisateur / Préférences"

**Configuration utilisateur / Préférences / Paramètres Windows / Environnement**

Créer une variable d'environnement pour l'utilisateur EMP09.

Créer une variable d'environnement pour l'utilisateur EMP20.

Créer une variable d'environnement pour les utilisateurs.

* **Environnement**

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

* Action: Remplacer
* Onglet Général
* Variable utilisateur
* Nom: V09
* Valeur: EMP09
* Onglet Commun
* Cocher "Supprimer l’élément lorsqu’il n’est plus appliqué"
* Ciblage au niveau de l'élément: **EMP09**
* Cliquer sur le bouton Appliquer
* Cliquer sur le bouton OK

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

* Action: Remplacer
* Onglet Général
* Variable utilisateur
* Nom: V20
* Valeur: EMP20
* Onglet Commun
* Cocher "Supprimer l’élément lorsqu’il n’est plus appliqué"
* Ciblage au niveau de l'élément: **EMP20**
* Cliquer sur le bouton Appliquer
* Cliquer sur le bouton OK

dans le menu contextuel de la fenêtre blanche, sélectionner "Nouveau / Variable d'environnement"

* Action: Remplacer
* Variable utilisateur
* Nom: DIRCMD
* Valeur: /a/o
* Onglet Commun
* Cocher "Supprimer l’élément lorsqu’il n’est plus appliqué"
* Cliquer sur le bouton Appliquer
* Cliquer sur le bouton OK

**Validation**

**Sur votre serveur virtuel 2**

Ouvrir une session avec l'utilisateur **EMP01**

* Vérifier l’application des paramètres des préférences qui sont dans les deux GPO

**"PU\_EMPLOYES"**

**"PU\_INFORMATIQUE\_CIBLAGE\_EMP09\_EMP20"**

* Fermer la session

Ouvrir une session avec l'utilisateur **EMP09**

* Vérifier l’application des paramètres des préférences qui sont dans les deux GPO

**"PU\_EMPLOYES"**

**"PU\_INFORMATIQUE\_CIBLAGE\_EMP09\_EMP20"**

* Fermer la session

Ouvrir une session avec l'utilisateur **EMP20**

* Vérifier l’application des paramètres des préférences qui sont dans les deux GPO

**"PU\_EMPLOYES"**

**"PU\_INFORMATIQUE\_CIBLAGE\_EMP09\_EMP20"**

* Fermer la session

**Tableau résumé**

|  |  |  |  |
| --- | --- | --- | --- |
| **Paramètres des préférences de la GPO**  **"PU\_EMPLOYES"** | **EMP07** | **EMP09** | **EMP20** |
| Le lecteur R: est mappé vers \\formation.local\netlogon | **OUI** | **OUI** | **OUI** |
| Écran de veille "Bulles" et les bulles sont opaques | **OUI** | **OUI** | **OUI** |
| Présence du raccourci vers NCPA.CPL sur le Bureau | **OUI** | **OUI** | **OUI** |
| Les quatre options des dossiers sont présentes | **OUI** | **OUI** | **OUI** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Paramètres des préférences de la GPO**  **"PU\_INFORMATIQUE\_CIBLAGE\_EMP09\_EMP20"** | **EMP07** | **EMP09** | **EMP20** |
| Présence des variables d’environnement:  V09  V20  DIRCMD | **NON**  **NON**  **OUI** | **OUI**  **NON**  **OUI** | **NON**  **OUI**  **OUI** |

L'utilisateur EMP01 est dans l'unité d'organisation suivante:

**OU=COMPTABLES,OU=COMPTABILITE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL**

L'utilisateur EMP09 est dans l'unité d'organisation suivante:

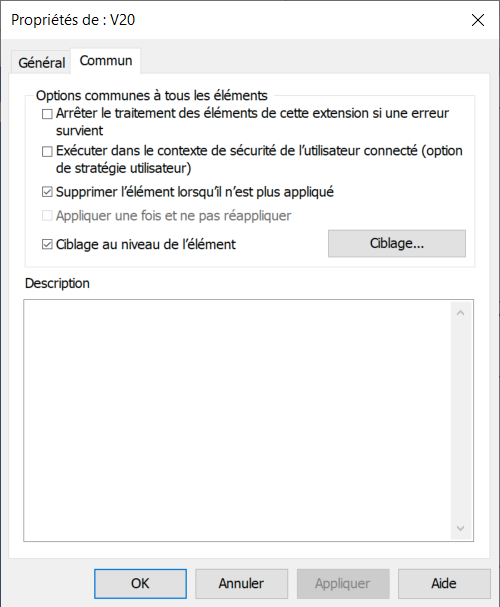
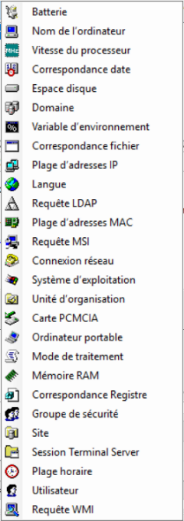
**OU=GESTIONNAIRES,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL**

L'utilisateur EMP20 est dans l'unité d'organisation suivante:

**OU=TECHNICIENS\_RESEAU,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL**

**ANNEXE**

Voici les différents critères qui sont disponibles pour le ciblage.

**ANNEXE**

Commande qui permet de démarrer l'écran de veille "**Bulles**" avec une commande.

**C:\Windows\System32\Bubbles.scr /s**

## Stratégies ORDINATEUR

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

**Objectif**

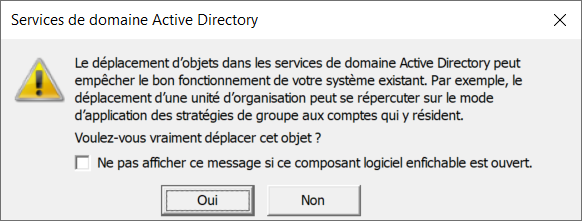
* Maîtrise des stratégies Ordinateurs

**Étape 1 - Mise en place**

Déplacer l'ordinateur SERVEUR2 dans l'unité d’organisation

**OU=FICHIERS,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL**

**Lors du déplacement de l'ordinateur SERVEUR2 un message va s'afficher à l'écran si vous effectuer le déplacement avec un "drag and drop".**



**Étape 2 - Création d'une stratégie ordinateur**

Créer la stratégie "C\_Serveurs\_Fichiers" liée à votre unité d'organisation "FICHIERS".

Désactiver la section "Utilisateur" de votre stratégie

Modifier votre stratégie "C\_Serveurs\_Fichiers" en paramétrant ce qui suit:

**Paramètres pour l'ordinateur**

Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité

"Accès réseau: ne pas autoriser le stockage de mots de passe et d’informations d’identification pour l’authentification du réseau"

* Activé

"Ouverture de session interactive: titre du message pour les utilisateurs essayant de se connecter"

* Le titre sera: "Message important"

"Ouverture de session interactive: contenu du message pour les utilisateurs essayant de se connecter"

* Le contenu du message sera: "Le serveur ne sera pas accessible à partir de 23:00."

Configuration ordinateur / Stratégies / Modèles d’administration / Système / Ouverture de session

"Afficher l’animation à la première connexion"

* Désactivé

**Étape 3 - Création d'une stratégie ordinateur**

Créer la stratégie "C\_Serveurs\_Fichiers\_Administrateurs" liée à votre unité d'organisation "FICHIERS".

Désactiver la section "Utilisateur" de votre stratégie

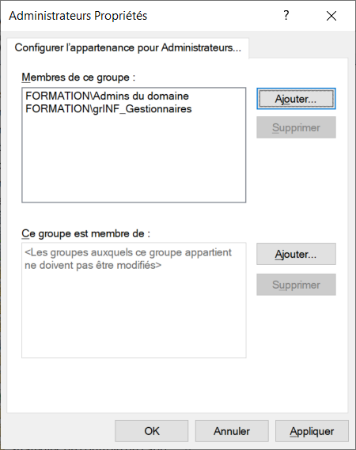
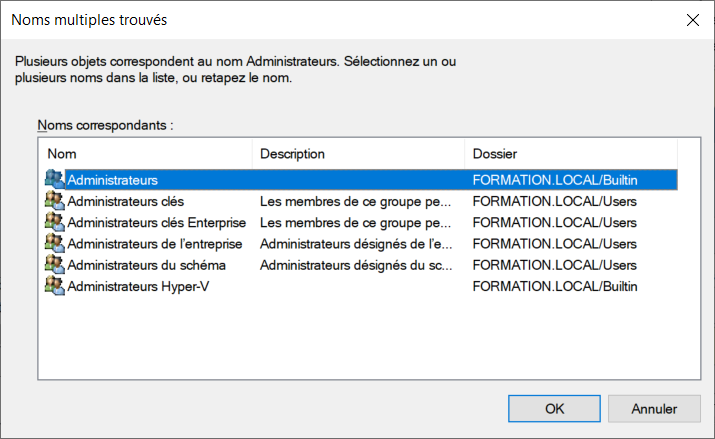
Modifier votre stratégie "C\_Serveurs\_Fichiers\_Administrateurs" en paramétrant ce qui suit:

**Paramètres pour l'ordinateur**

Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Groupes restreints

Dans le menu contextuel de "Groupes restreints" choisir l'option "Ajouter un groupe…"

* Ajouter le groupe "Administrateurs"



Ajouter le groupe "**FORMATION\Admins du domaine**" dans la section "**Membres de ce groupe**".

Ajouter le groupe "**FORMATION\grINF\_Gestionnaires**" dans la section "**Membres de ce groupe**"

**Étape 4 - Test**

Ouvrir une "Invite de commandes" en tant qu'administrateur et exécuter la commande "**gpupdate.exe /force**".

Fermer la session de FORMATION\TECH sur le SERVEUR2.

Vous devez ouvrir une session avec **EMP09** ou **EMP10**.

* Vérifier l'application de la stratégie "**C\_Serveurs\_Fichiers**"

Un message s'affiche avant de s'authentifier au serveur.

* Vérifier l'application de la stratégie "**C\_Serveurs\_Fichiers Administrateurs**"

Ouvrir une fenêtre cmd.exe et exécuter la commande suivante "**whoami /groups**"

Dans la liste des groupes, vous allez voir que **EMP09** ou **EMP10** est membre du groupe **BUILTIN\Administrateurs**

Vous devez vous déconnecter de la session **EMP09** ou **EMP10**.

IMPORTANT: il n'y a que les membres des groupes **grINF\_Gestionnaires** et "**FORMATION\Admins du domaine**" qui auront des autorisations **Administrateurs** sur le serveur SERVEUR2.

**Étape 5 - TRAITEMENT PAR BOUCLAGE**

Le traitement par bouclage permet d’appliquer des paramètres utilisateurs dans une unité d’organisation qui contient des ordinateurs.

Il existe deux modes pour le traitement par bouclage.

* "**Remplacer**" indique que les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" remplacent les paramètres utilisateur normalement appliqués à l’utilisateur.
* "**Fusionner**" indique que les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" et les paramètres utilisateur normalement appliqués à l’utilisateur se combinent.

Si les paramètres entrent en conflit, les paramètres utilisateur dans la stratégie de groupe de "traitement par bouclage" prévalent sur les paramètres normalement appliqués à l’utilisateur.

Cette solution est souvent appliquée pour des lecteurs réseaux et des imprimantes.

Créer la GPO "**Bouclage\_Fichiers**" liée à votre unité d'organisation "FICHIERS".

**Paramètres pour l'ordinateur**

Configuration ordinateur / Stratégies / Modèles d’administration / Système / Stratégie de groupe

"Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur"

* Activé le paramètre et choisir le mode **Remplacer**.

**Paramètres pour l'utilisateur**

**Configuration utilisateur / Stratégies / Modèles d'administration / Bureau / Bureau**

Vous devez trouver un fichier JPG qui servira de fond d’écran et qui sera déposé dans le partage NETLOGON. Vous devez donner un nom significatif au fichier, par exemple "serveur2.jpg".

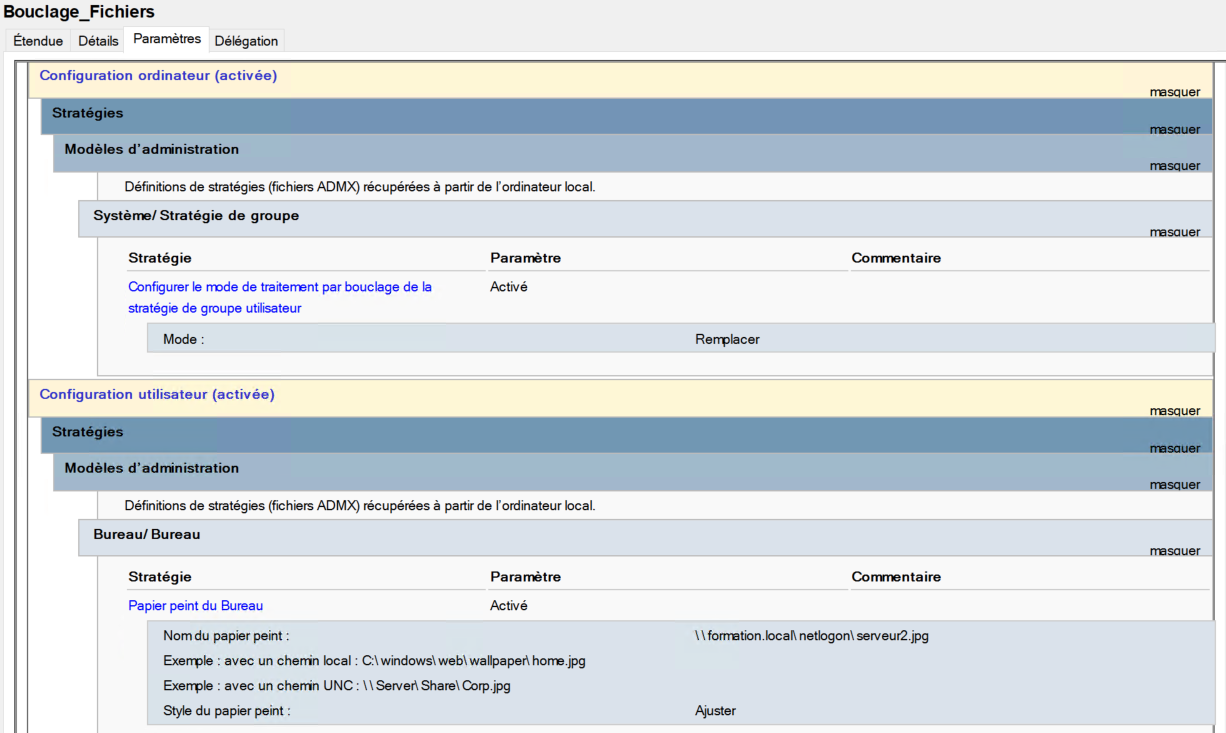
"Papier peint du Bureau"

* Activé

Nom du papier peint = \\formation.local\netlogon\serveur2.jpg

Style du papier peint = Remplir

**La section "Configuration ordinateur" et la section "Configuration utilisateur" sont activées.**



Tester l'application de la GPO "**Bouclage\_Fichiers**" avec le mode "**Remplacer**".

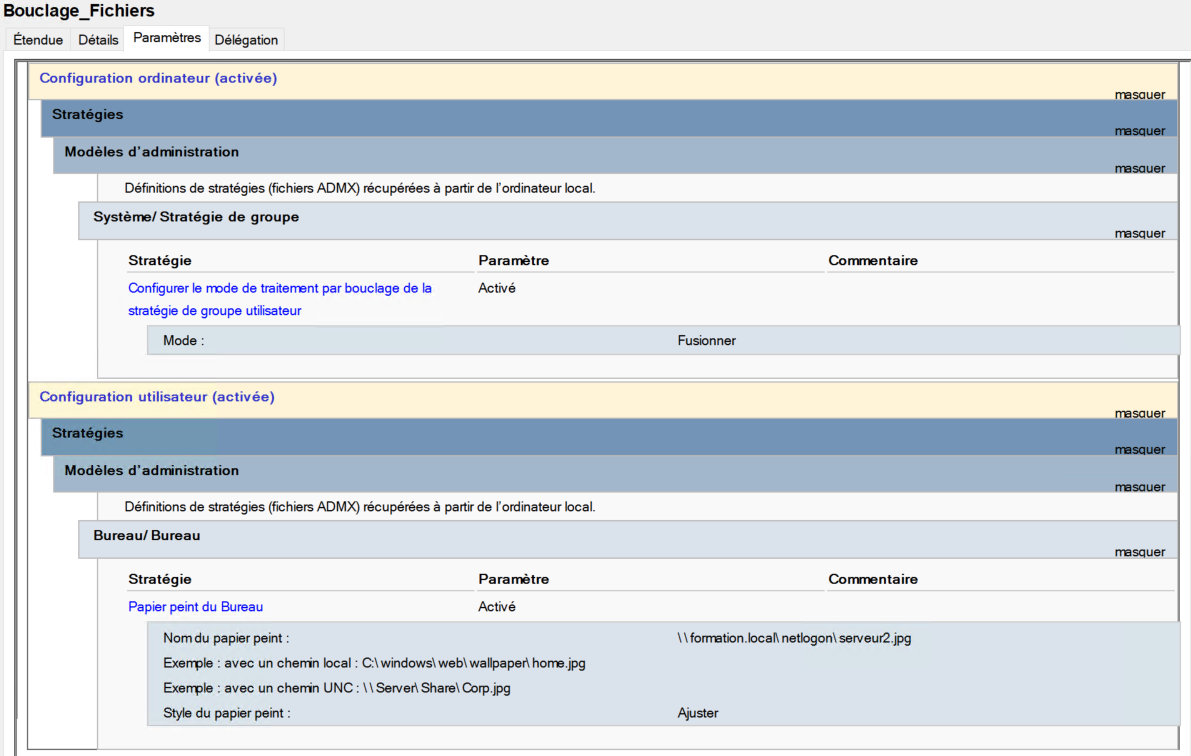
Les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" remplacent les paramètres utilisateur normalement appliqués à l’utilisateur.

**Après l'ouverture d'une session:**

Le papier peint du Bureau s'affiche avec l'image serveur2.jpg. "Bouclage\_Fichiers"

Dans la GPO "**Bouclage\_Fichiers**" changé le mode pour "**Fusionner**".

**La section "Configuration ordinateur" et la section "Configuration utilisateur" sont activées.**



Tester l'application de la GPO "**Bouclage\_Fichiers**" avec le mode "**Fusionner**".

Les paramètres utilisateur définis dans la stratégie de groupe de "traitement par bouclage" et les paramètres utilisateur normalement appliqués à l’utilisateur se combinent.

Si les paramètres entrent en conflit, les paramètres utilisateur dans la stratégie de groupe de "traitement par bouclage" prévalent sur les paramètres normalement appliqués à l’utilisateur.

**Après l'ouverture d'une session:**

Le papier peint du Bureau s'affiche avec l'image serveur2.jpg. "Bouclage\_Fichiers"

L'écran de veille spécifique est "bubbles.scr". "U\_EMPLOYES"

…

Les bulles de l'écran de veille sont métalliques "PU\_EMPLOYES

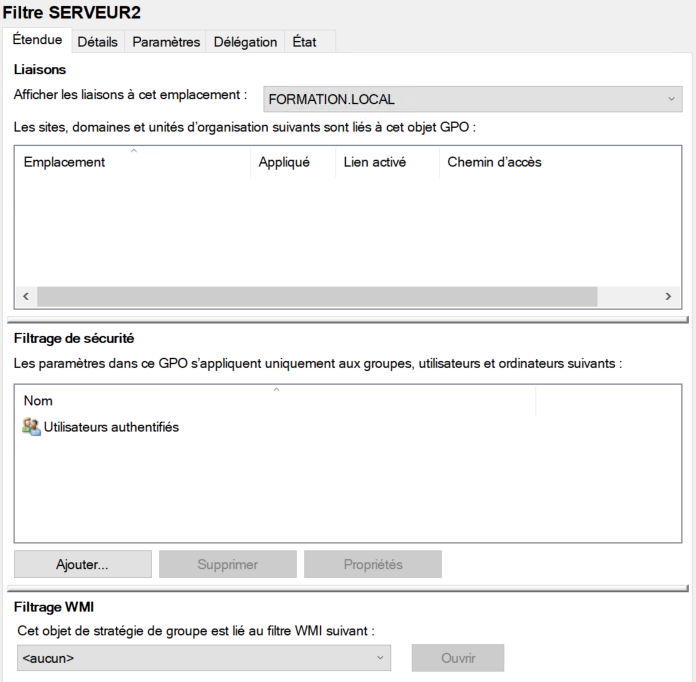
…

## Filtres WMI

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

**Objectif**

* Maîtrise des stratégies avec filtres WMI
* Avec un filtre WMI il est possible d'appliquer des "GPO Utilisateurs" sur des ordinateurs en spécifiant une requête WMI afin de sélectionner un ou plusieurs ordinateurs

**Il est possible de filtrer l'application d'une stratégie. Le plus simple est de créer un filtre WMI.**

C'est possible de supprimer "Utilisateurs authentifiés" dans la section "Filtrage de sécurité" et d'ajouter seulement les utilisateurs, les ordinateurs ou les groupes visés par la stratégie. Mais ce n'est pas si simple, voir l'annexe.



**Étape 1 - Mise en place**

Les unités d’organisations et les utilisateurs de l'unité d'organisation FORMATION doivent exister.

Vous devez supprimer le lien de la GPO "**Bouclage\_Fichiers**" qui est sur l'unité d'organisation "**FICHIERS**".

**# Code PowerShell pour ajouter un ordinateur**

**New-ADComputer -Name SERVEUR3 `**

**-Path "OU=WEB,OU=SERVEURS,OU=FORMATION,DC=FORMATION,DC=LOCAL"**

**Étape 2 - Création des filtres WMI**

1. Créer une requête WMI pour sélectionner le serveur SERVEUR2

Nom de la requête WMI: SERVEUR2

**Select Name from Win32\_ComputerSystem where Name = "SERVEUR2"**

1. Créer une requête WMI pour sélectionner le serveur SERVEUR3

Nom de la requête WMI: SERVEUR3

**Select Name from Win32\_ComputerSystem where Name = "SERVEUR3"**

1. Créer une requête WMI pour sélectionner les deux serveurs: SERVEUR2 et SERVEUR3

Nom de la requête WMI: SERVEUR2 et SERVEUR3

note: cette requête vérifie exactement les deux noms

**Select Name from Win32\_ComputerSystem where ((Name = "SERVEUR2") OR (Name = "SERVEUR3"))**

1. Pour sélectionner l'ensemble des ordinateurs dont le nom débute par SERVEUR

**Select Name from Win32\_ComputerSystem where Name LIKE "SERVEUR%"**

Voici comment vérifier votre requête WMI dans PowerShell

Get-CimInstance -Query **'votre requête WMI**'

**Exemple**

$req = '**Select Name from Win32\_ComputerSystem where Name = "SERVEUR2"**'

Get-CimInstance -Query $req | Format-Table -AutoSize

**Étape 3 - Création d’un objet de stratégie de groupe**

Vous devez trouver un fichier JPG qui servira de fond d’écran et qui sera déposé dans le partage Netlogon.

Le nom du fichier sera "Fond\_UO\_Programmeurs.jpg".

Créer la stratégie "U\_Programmeurs\_filtre" qui sera liée à l'unité d'organisation

**OU=PROGRAMMEURS,OU=INFORMATIQUE,OU=EMPLOYES,OU=FORMATION,DC=FORMATION,DC=LOCAL**

Désactiver la section "Ordinateur" de votre stratégie

Modifier votre stratégie "Filtre SERVEUR2" en paramétrant ce qui suit:

**Paramètres pour l'utilisateur**

Configuration utilisateur / Stratégies / Modèles d'administration / Bureau / Bureau

"Papier peint du Bureau"

* Activé

Nom du papier peint = \\formation.local\netlogon\Fond\_UO\_Programmeurs.jpg

Style du papier peint = Remplir

**Filtrage WMI**

Vous devez lier la requête WMI "SERVEUR2" à la GPO "U\_Programmeurs\_Filtre"

**Étape 4 - Test**

**Sur votre serveur virtuel 2**

Ouvrir une session avec l'utilisateur **EMP11** ou **EMP12**

* Vérifier que le fond d'écran qui est spécifié dans le paramètre de votre stratégie "U\_Programmeurs\_filtre" s'applique
* Fermer la session

**Étape 5 - Modification du filtrage WMI sur la GPO "Filtre SERVEUR2"**

Sélectionner votre GPO "U\_Programmeurs\_filtre" et modifier le filtrage WMI pour la requête "SERVEUR3".

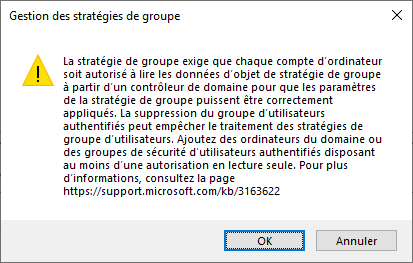
**Étape 6 - Test**

**Sur votre serveur virtuel 2**

Ouvrir une session avec l'utilisateur **EMP11** ou **EMP12**

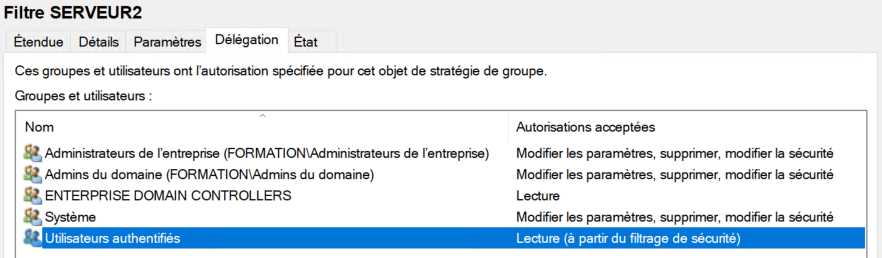
* Vérifier que le fond d'écran qui est spécifié dans le paramètre de votre stratégie "U\_Programmeurs\_filtre" ne s'applique pas
* Fermer la session

**ANNEXE**

C'est possible de supprimer "Utilisateurs authentifiés" dans la section "Filtrage de sécurité" et d'ajouter seulement les utilisateurs, les ordinateurs ou les groupes visés par la stratégie. **C'est une solution trop compliquée.**

En supprimant "Utilisateurs authentifiés" dans la section "Filtrage de sécurité", il y a un message qui s'affiche.

L'onglet "Délégation" affiche les autorisations.



Dans l’onglet "Délégation", cliquer sur le bouton "Avancé..." et sélectionner "**Utilisateurs authentifiés**".



Par exemple, si vous voulez que la stratégie s'applique seulement à l'utilisateur EMP11.

Il faut ajouter l'utilisateur "**EMP11**".

Les autorisations pour "**EMP11**" seront:

* **Lire**
* **Appliquer la stratégie de groupe**

Il faut **obligatoirement** ajouter le groupe "**Ordinateurs du domaine**".

Les autorisations minimales pour "**Ordinateurs du domaine**" seront

* **Lire**

Pour revenir au comportement normal de la stratégie, vous devez défaire vos modifications

* Ajouter "**Utilisateurs authentifiés**"

note: vérifier que les autorisations "**Lire**" et "**Appliquer la stratégie de groupe**" sont cochées

* Supprimer l'utilisateur **EMP11**
* Supprimer le groupe "**Ordinateurs du domaine**"

**Cette méthode de filtrage est à éviter.**

## Stratégies pour le navigateur "Google Chrome"

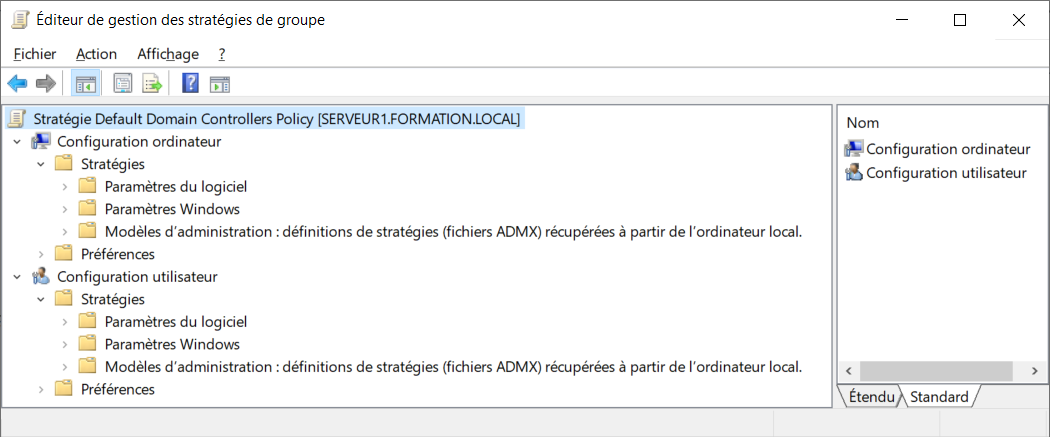
Ce laboratoire doit être fait individuellement sur l'ordinateur virtuel 2

**Objectif**

* Création du "Magasin central"
* Ajout des fichiers ADMX et ADML pour le navigateur "Google Chrome"

L’utilisation d’un magasin central permet d’utiliser les mêmes fichiers ADMX et ADML sur l’ensemble des contrôleurs de domaine quelle que soit la version de Windows Server.

Avant la création du "Magasin central", les stratégies dans "Modèles d'administration" sont récupérées à partir de l'ordinateur local.



**Étape 1 - Création du "Magasin central"**

Copier le dossier "**\\SERVEUR1\C$\Windows\PolicyDefinitions**" dans le dossier

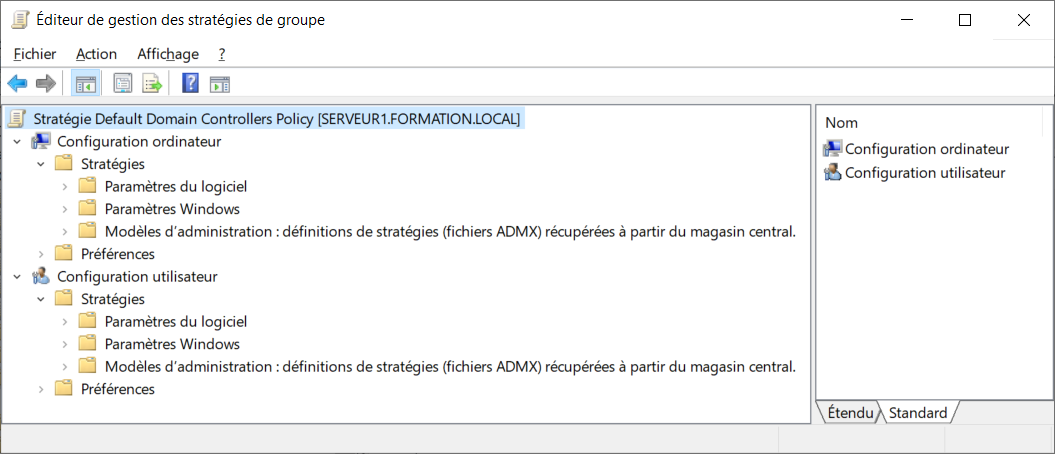
"**\\formation.local\SYSVOL\formation.local\Policies**"

**Pour éviter les erreurs, vous pouvez utiliser la commande suivante:**

**xcopy \\SERVEUR1\C$\Windows\PolicyDefinitions**

**\\formation.local\SYSVOL\formation.local\Policies\PolicyDefinitions\ /S**

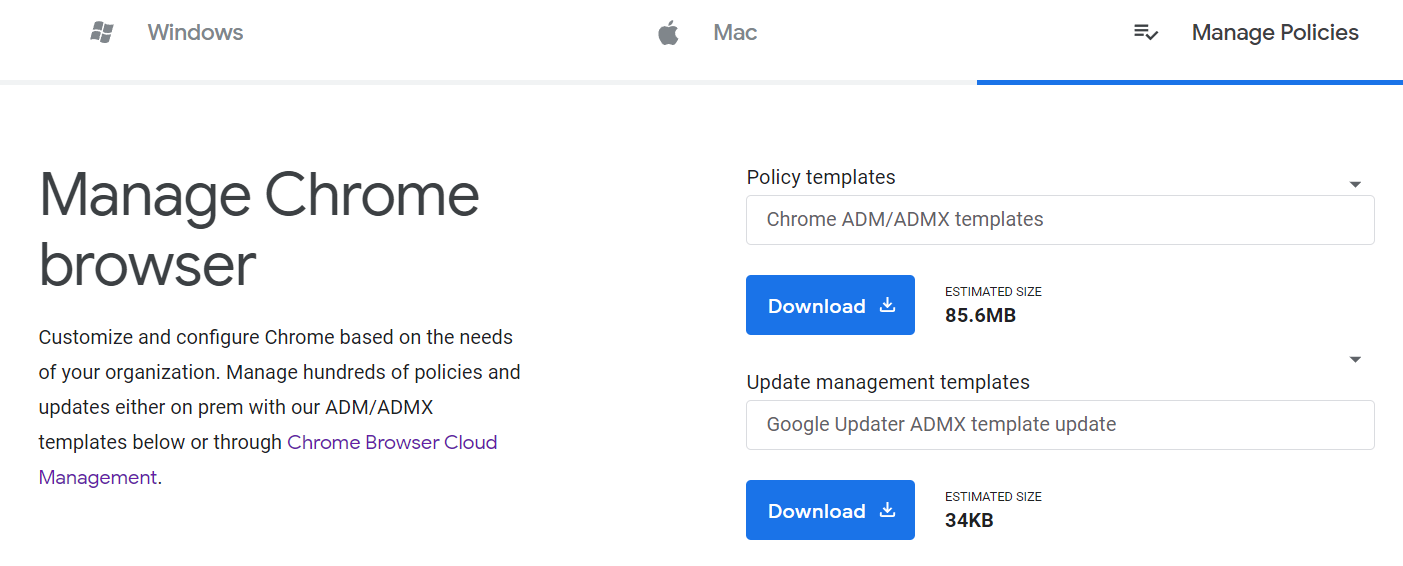
Après la création du "Magasin central", les stratégies dans "Modèles d'administration" sont récupérées à partir du magasin central.



**Étape 2 - Copier les fichiers ADMX et ADML de "Chrome" dans le magasin central**

Le fichier **policy\_templates.zip** est disponible sur le site "**Download Chrome browser for your enterprise**"

**https://chromeenterprise.google/browser/download/#manage-policies-tab**



Extraire le contenu du fichier **policy\_templates.zip** dans un dossier.

Vous devez récupérer les fichiers suivants

..\windows\admx\chrome.admx

..\windows\admx\google.admx

..\windows\admx\fr-FR\chrome.adml

..\windows\admx\fr-FR\google.adml

Copier les fichiers "..\windows\admx\chrome.admx" et "..\windows\admx\google.admx"

dans le dossier

\\formation.local\SYSVOL\formation.local\Policies\PolicyDefinitions\

Copier les fichiers "..\windows\admx\fr-FR\chrome.adml" et "..\windows\admx\fr-FR\google.adml"

dans le dossier

\\formation.local\SYSVOL\formation.local\Policies\PolicyDefinitions\fr-FR\

**Étape 3 - Création d'une GPO pour "Chrome"**

Créer la stratégie "**U\_EMPLOYES\_Google\_Chrome**" et la lier à votre unité d'organisation "**EMPLOYES**"

Désactiver la section "Ordinateur" de votre stratégie

Les paramètres de la GPO serviront à configurer les pages d'accueil du navigateur "Google Chrome".

On doit activer le paramètre de stratégie "**Action au démarrage**" qui est sous:

**Configuration utilisateur / Modèles d'administration / Google / Google Chrome / Démarrage, page d'accueil et page Nouvel onglet**

On doit sélectionner l'action au démarrage "**Ouvrir une liste d'URL**".

On doit activer le paramètre de stratégie "**URL à ouvrir au démarrage**" qui est sous:

**Configuration utilisateur / Modèles d'administration / Google / Google Chrome / Démarrage, page d'accueil et page Nouvel onglet**

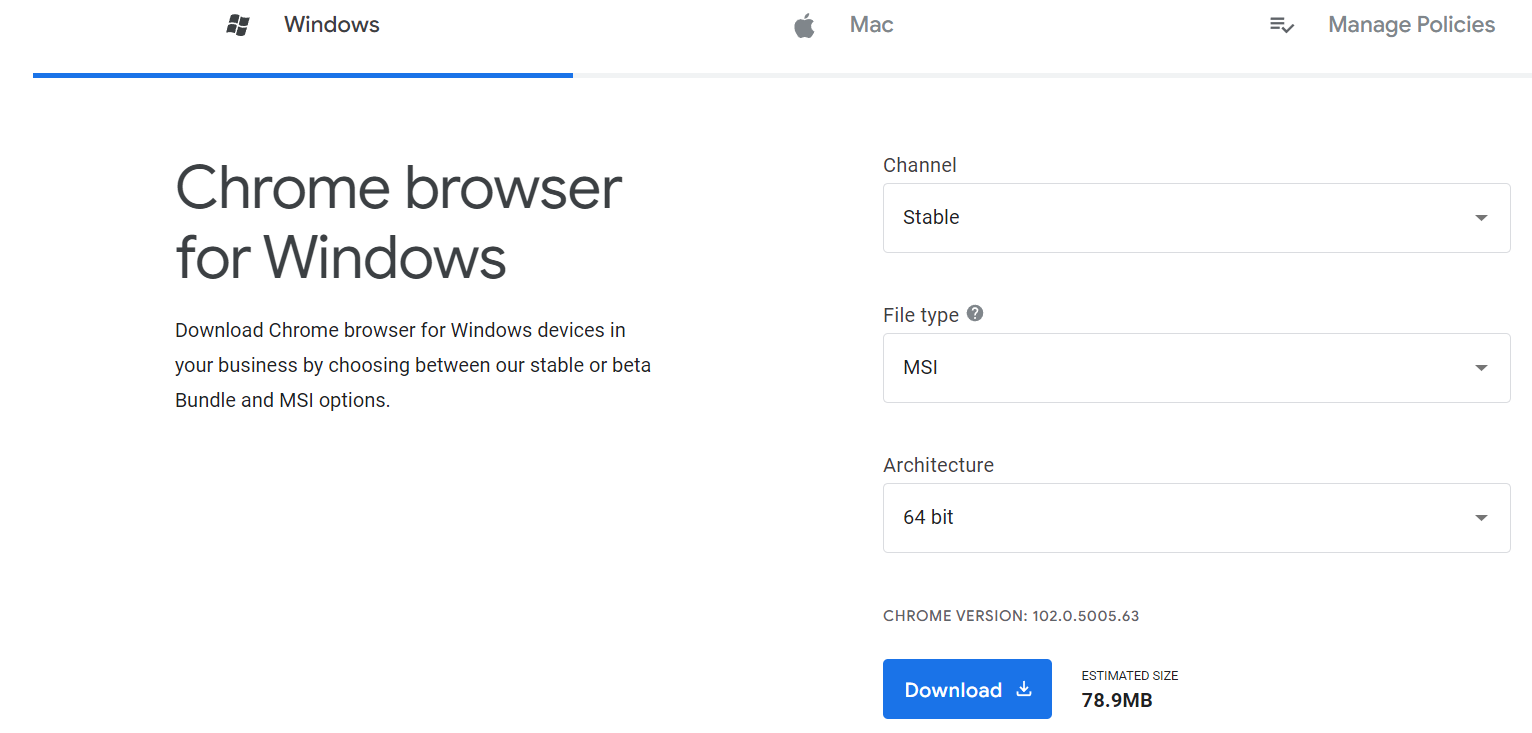
On doit inscrire une liste de site web que l'on désire ouvrir au démarrage de Chrome.

**Étape 4 - Vérifier l'application de la GPO pour le navigateur "Google Chrome"**

Vous devez installer le navigateur "Google Chrome" sur le SERVEUR2.

Le fichier googlechromestandaloneenterprise64.msi est disponible sur le site suivant dans la section "Windows"

**https://chromeenterprise.google/browser/download**

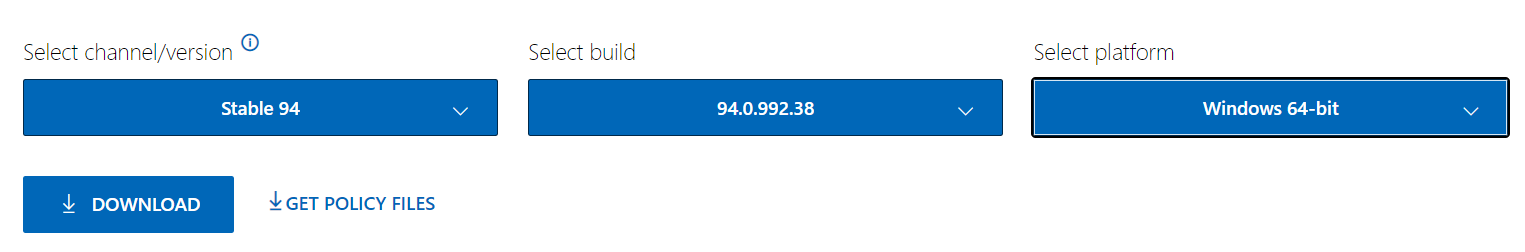


1. Fermer la session de l'utilisateur "FORMATION\TECH"
2. Ouvrir une session avec un des utilisateurs EMP01 à EMP32
3. Vérifier l'application des GPO pour le navigateur "Google Chrome".

**ANNEXE**

Voici le lien pour récupérer les fichiers ADMX et ADML pour "**Edge Chromium**".

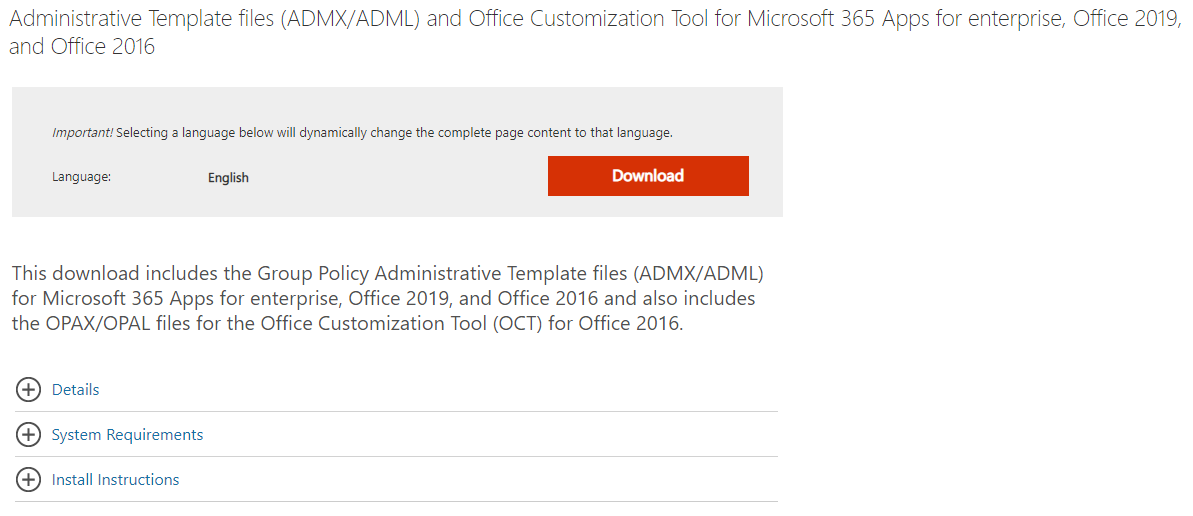
**https://www.microsoft.com/en-us/edge/business/download**



Voici le lien pour récupérer les fichiers ADMX et ADML pour "**Office 365** - **Office 219 - Office 216**".

**https://www.microsoft.com/en-us/download/office.aspx**

note: vous devez rechercher "**Administrative Template files**"



## 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"

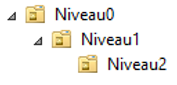
* HKEY\_LOCAL\_MACHINE\Software\Policies
* HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies

**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"

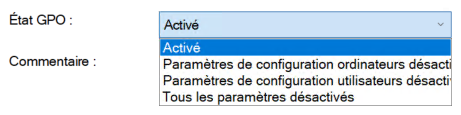
Créer deux objets et lier directement dans les unités

* 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" `**

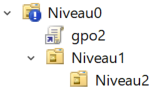
**-Target "ou=Niveau0,dc=formation,dc=local"**

**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".**

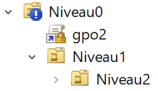
|  |  |
| --- | --- |
| **En français** | **En anglais** |
| Appliqué | Enforced |
| Lien activé | Link Enabled |



**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 `**

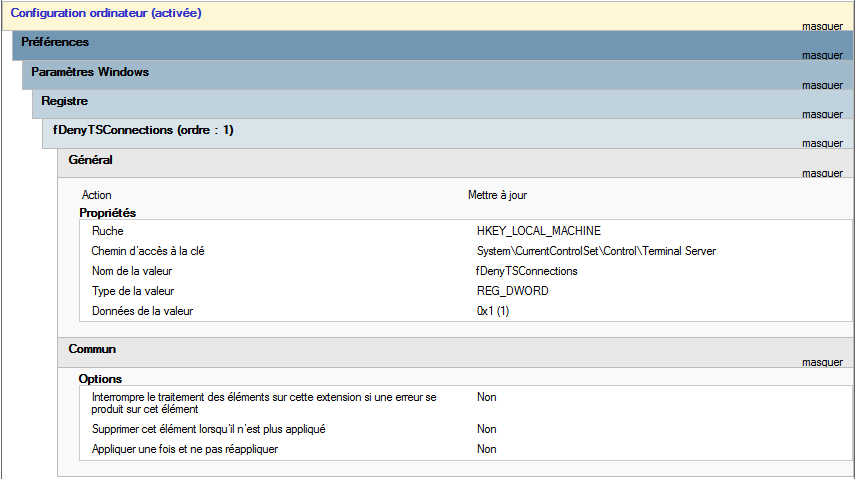
**-Type Dword `**

**-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".**

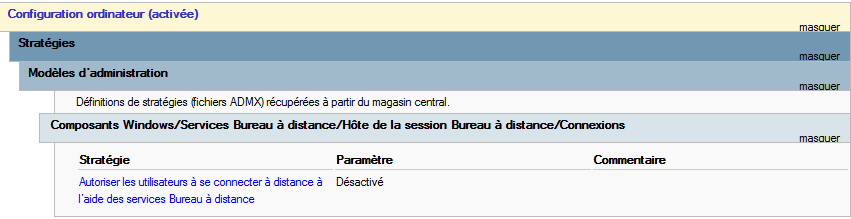
**Set-GPRegistryValue -Name "C\_DisableRDP" `**

**-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**

## Informations supplémentaires sur les GPO

**Objectifs**

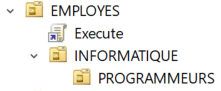
* Comprendre l'implication du blocage de l'héritage
* Comprendre la différence entre "Appliqué" et "Lien activé"

**Étape 1 - Création et test d’un objet de stratégie de groupe**

Si l'unité d'organisation "EMPLOYES" est directement sous le domaine "FORMATION.LOCAL".

Si l'utilisateur EMP100 est dans l'unité d'organisation "EMPLOYES".

Si l'utilisateur PROG100 est dans l'unité d'organisation "PROGRAMMEURS".



Si la stratégie "Execute" est liée à l'unité d'organisation "EMPLOYES" et la section "Ordinateur" est désactivée.

**En supposant que les paramètres de la stratégie "Execute" sont les suivants:**

Configuration utilisateur / Stratégies / Modèles d'administration / Panneau de configuration

"Interdire l’accès au Panneau de configuration et à l’application Paramètres du PC"

* Activé

Configuration utilisateur / Stratégies / Modèles d'administration / Système

"Ne pas exécuter les applications Windows spécifiées"

* calc.exe
* win32calc.exe

Si l’utilisateur **EMP100** ouvre une session

* **EMP100 n'a pas d'accès au panneau de configuration**
* **EMP100 n'a pas d'accès à la calculatrice**

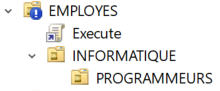
Si l’utilisateur **PROG100** ouvre une session

* **PROG100 n'a pas d'accès au panneau de configuration**
* **PROG100 n'a pas d'accès à la calculatrice**

**C'est le comportement normal de l'application des GPO.**

**Étape 2 - L'option "Bloquer l’héritage"**

L'option "**Bloquer l’héritage**" est dans le menu contextuel d'une unité d'organisation.



Un point d'exclamation blanc dans un rond bleu nous indique que l'option "**Bloquer l'héritage**" est activée.

Si l’utilisateur **EMP100** ouvre une session

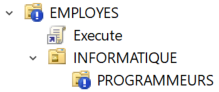
* **EMP100 n'a pas d'accès au panneau de configuration**
* **EMP100 n'a pas d'accès à la calculatrice**

Si l’utilisateur **PROG100** ouvre une session

* **PROG100 n'a pas d'accès au panneau de configuration**
* **PROG100 n'a pas d'accès à la calculatrice**

**Le blocage de l'héritage n'a aucun effet sur la GPO qui est liée directement à "EMPLOYES".**

L'héritage est bloqué à deux niveaux.



Si l’utilisateur **EMP100** ouvre une session

* **EMP100 n'a pas d'accès au panneau de configuration**
* **EMP100 n'a pas d'accès à la calculatrice**

Si l’utilisateur **PROG100** ouvre une session

* **PROG100 a accès au panneau de configuration**
* **PROG100 a accès à la calculatrice**

**La GPO "Execute" ne s'applique pas sur les utilisateurs de l'unité d'organisation "PROGRAMMEURS".**

**Le blocage empêche l’application des GPO qui sont au-dessus d'une UO mais pas à celles qui sont liées directement à une UO.**

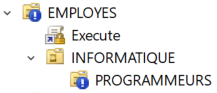
**Avant de continuer**

**Laisser** le blocage d’héritage sur la UO "EMPLOYES"

**Laisser** le blocage d’héritage sur la UO "PROGRAMMEURS"

**Étape 3 - L'option "Appliqué"**

L'option "**Appliqué**" est dans le menu contextuel du lien d'une GPO.



Un cadenas nous indique que l'option "**Appliqué**" est activée.

L'option "**Bloquer l'héritage**" doit être active pour voir l’effet de l’option "**Appliqué**".

Si l’utilisateur **EMP100** ouvre une session

* **EMP100 n'a pas d'accès au panneau de configuration**
* **EMP100 n'a pas d'accès à la calculatrice**

Si l’utilisateur **PROG100** ouvre une session

* **PROG100 n'a pas d'accès au panneau de configuration**
* **PROG100 n'a pas d'accès à la calculatrice**

**L'option "Appliqué" a priorité sur l'option "Bloquer l'héritage".**

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

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



## Gestion de la sauvegarde des GPO

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

**Objectif**

* Apprendre à lire le contenu du fichier manifest.xml
* Sauvegarder et restaurer des GPO dans un domaine

**Informations sur la structure du fichier manifest.xml**

Quand on effectue une sauvegarde de nos stratégies de groupe, à la racine de notre dossier un fichier "**manifest.xml**" est créé.

Ce fichier a la structure suivante:

* Backups
* BackupInst
  + GPOGuid
  + GPODomain
  + GPODomainGuid
  + GPODomainController
  + BackupTime
  + ID
  + Comment
  + GPODisplayName

Pour exécuter le cmdlet Import-GPO nous avons besoin du contenu de la balise "**GPODisplayName**" ou de la balise "**ID**".

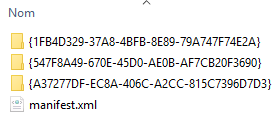
Avant de commencer, vous devez sauvegarder les GPO suivantes dans le dossier "**C:\\_GPO\_BACKUP\UTILISATEURS**".

* PU\_EMPLOYES
* PU\_INFORMATIQUE\_CIBLAGE\_EMP09\_EMP20
* U\_EMPLOYES

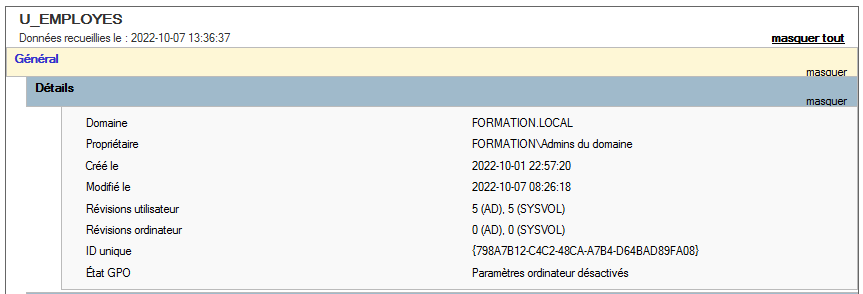
**Informations**

La sauvegarde des GPO génère un fichier manifest.xml et des dossiers dont le nom ne correspond pas au nom des stratégies.

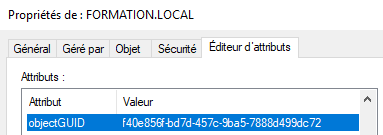
Par exemple, voici le contenu du dossier "**C:\\_GPO\_BACKUP\UTILISATEURS**".



Le nom de chaque dossier correspond à la balise "**GPOID**".



La valeur de "**ID unique**" correspond à la balise "**GPOGuid**".



La valeur de l'attribut "**objectGUID**" du domaine correspond à la balise "**GPODomainGuid**".

Voici un script PowerShell qui va lire le contenu d'un fichier "manifest.xml" et afficher toutes les informations des stratégies qui sont dans le dossier de la sauvegarde.

**# Le chemin complet du fichier MANIFEST.XML**

**$xmlPath = 'C:\\_GPO\_BACKUP\UTILISATEURS\manifest.xml'**

**$xml = [xml](Get-Content -Path $xmlPath -Encoding UTF8)**

**$xmlExpanded = $xml.DocumentElement.BackupInst**

**Write-Host $("-" \* 80) -ForegroundColor Cyan**

**foreach ($item in $xmlExpanded)**

**{**

**"GPOGuid = " + $item.GPOGuid.InnerText**

**"GPODomain = " + $item.GPODomain.InnerText**

**"GPODomainGuid = " + $item.GPODomainGuid.InnerText**

**"GPODomainController = " + $item.GPODomainController.InnerText**

**"GPOBackupTime = " + $item.BackupTime.InnerText**

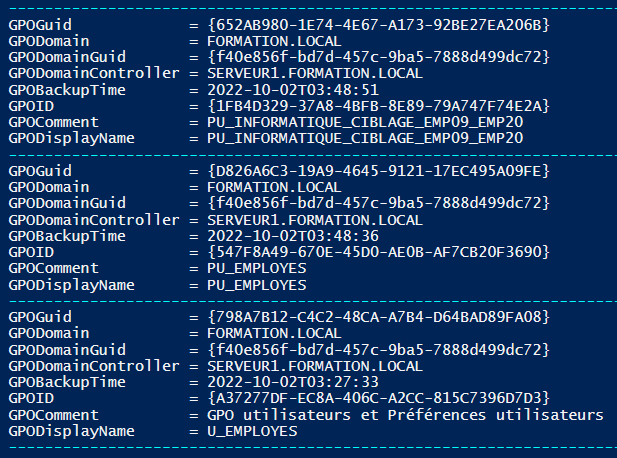
**"GPOID = " + $item.ID.InnerText**

**"GPOComment = " + $item.Comment.InnerText**

**"GPODisplayName = " + $item.GPODisplayName.InnerText**

**Write-Host $("-" \* 80) -ForegroundColor Cyan**

**}**



Il existe deux cmdlets pour importer des GPO: Import-GPO ou Restore-GPO.

**Import-GPO**

* Import-GPO permet de restaurer une GPO en utilisant un nom différent de l'original.
* La restauration d'une GPO peut se faire dans un domaine ou une forêt différente de la sauvegarde qui a été faite et n’a pas besoin d'exister.

**Restore-GPO**

* Restore-GPO permet de restaurer une ou plusieurs GPO dans un domaine à condition que les GPO proviennent du même domaine.
* Si le domaine original n'est pas disponible ou si la GPO n'existe plus dans le domaine alors le cmdlet génère une erreur.

Exemples en utilisant le nom de la GPO qui est dans la balise "**GPODisplayName**".

# Importation de la GPO si elle n'existe plus.

# Dans ce cas, le paramètre **-CreateIfNeeded** est obligatoire.

**Import-GPO -BackupGpoName "U\_EMPLOYES" `**

**-Path "C:\\_GPO\_BACKUP\UTILISATEURS" `**

**-TargetName "U\_EMPLOYES" `**

**-CreateIfNeeded**

# Importation de la GPO si elle existe.

# Dans ce cas, le paramètre **-CreateIfNeeded** n'est pas obligatoire.

**Import-GPO -BackupGpoName "U\_EMPLOYES" `**

**-Path "C:\\_GPO\_BACKUP\UTILISATEURS" `**

**-TargetName "U\_EMPLOYES"**

Exemples en utilisant la valeur qui est dans la balise "**ID**".

# Importation de la GPO si elle n'existe plus.

# Dans ce cas, le paramètre **-CreateIfNeeded** est obligatoire.

**Import-GPO -BackupId A37277DF-EC8A-406C-A2CC-815C7396D7D3 `**

**-Path "C:\\_GPO\_BACKUP\UTILISATEURS" `**

**-TargetName "U\_EMPLOYES" `**

**-CreateIfNeeded**

# Importation de la GPO si elle existe.

# Dans ce cas, le paramètre **-CreateIfNeeded** n'est pas obligatoire.

**Import-GPO -BackupId A37277DF-EC8A-406C-A2CC-815C7396D7D3 `**

**-Path "C:\\_GPO\_BACKUP\UTILISATEURS" `**

**-TargetName "U\_EMPLOYES"**

## **Introduction aux "Espaces de noms"**

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

**Objectifs**

* Maîtriser les concepts reliés aux DFS (espace de nom, racine, cible et dossier, réplication)
* Maîtriser la gestion des DFS (création, modification, réplication)
* Maîtriser l’utilisation des DFS

**Étape 1 - Création de la racine d’un espace de noms**

Sur le SERVEUR2, dans la console "Gestion du système de fichiers distribués DFS"

* Sur l’item "Espace de noms", dans le menu contextuel, choisir l’option "Nouvel espace de noms…"

Répondre aux questions de l’assistant "**Nouvel Espace de noms**"

* Écran "**Serveur d’espaces de noms**"
* inscrire le nom de votre serveur virtuel 2 = **SERVEUR2**
* Écran "**Nom et paramètres de l’espace de noms**"

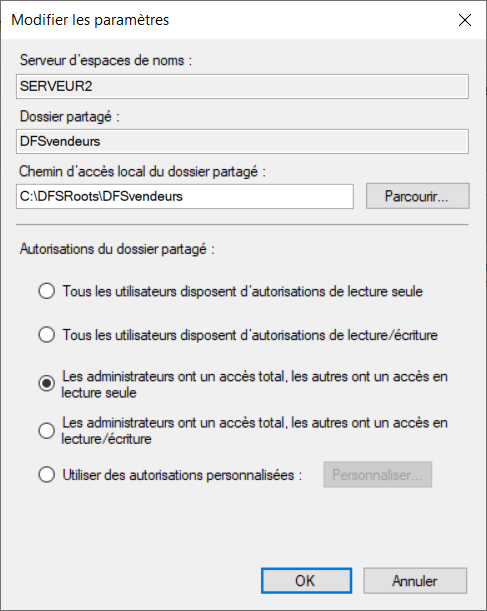
Vous devez inscrire le nom de l’espace de noms pour que le bouton "Modifier les paramètres…" soit actif.

* + Nom: **DFSvendeurs**
  + Bouton "Modifier les paramètres…"
* Serveur d'espaces de noms = SERVEUR2
* Dossier partagé = DFSvendeurs
* Chemin d’accès local du dossier partagé = C:\DFSRoots\DFSvendeurs

Le dossier "**C:\DFSRoots**" est créé lors de la création du premier espace de noms.

* Autorisations du dossier partagé

"Les administrateurs ont un accès total, les autres ont un accès en lecture seule"



* Écran "**Type d’espace de noms**"
* Sélectionner "Espace de noms de domaine"
* Cocher "Activer le mode Windows Server 2008"
* Aperçu de l'espace de noms de domaine

Le nom de référence de votre espace de nom est **\\FORMATION.LOCAL\DFSvendeurs**

* Écran "**Revoir les paramètres et créer l'espace de noms**"
* Cliquer sur le bouton "Créer" pour déclencher la création de votre espace de noms

Lors de la création de votre Espace de Noms via la console, voici les étapes qui sont faites automatiquement:

* Création du dossier C:\DFSRoots\DFSVendeurs
* Création du partage DFSvendeurs sur le dossier C:\DFSRoots\DFSVendeurs
* Création de l'espace de noms \\FORMATION.LOCAL\DFSVendeurs

Il est important de connaître ces étapes, car elles ne sont pas faites automatiquement lors de la création d’un espace de nom en PowerShell. Il faut utiliser des cmdlets pour faire les différentes étapes.

**Étape 2 - Insertion de dossiers et de cibles**

Dans votre console, dans l’écran de gauche, sélectionner votre nouvel espace de noms \\FORMATION.LOCAL\DFSvendeurs et ajouter des dossiers.

Vous pouvez utiliser les fonctionnalités Ajouter, Parcourir, Rechercher et Afficher les partages

pour trouver les "cibles du dossier"

Premier dossier

* Sur votre espace de nom, dans le menu contextuel, choisir l’option "**Nouveau dossier…**"
* Nom: Commandes
* Cible du dossier (chemin d’accès): **\\SERVEUR2\C53\_Cmd**

**La console va créer le dossier "C:\DFSRoots\DFSvendeurs\Commandes" qui sera utilisé pour la gestion de cet espace de noms.**

Deuxième dossier

* Sur votre espace de nom, dans le menu contextuel, choisir l’option "**Nouveau dossier…**"
* Nom: Clients
* Cible du dossier (chemin d’accès): **\\SERVEUR1\C53\_Cli**

**La console va créer le dossier "C:\DFSRoots\DFSvendeurs\Clients" qui sera utilisé pour la gestion de cet espace de noms.**

**Étape 3 - Utilisation de votre espace de noms**

Tester votre espace de noms en l'associant à une lettre dans votre explorateur de fichiers.

Ouvrir l'Explorateur de fichiers

* Effectuer l’opération "Connecter un lecteur réseau"
* Lier cet espace de noms à la lettre V:
* Le nom de référence de l’espace de noms: **\\FORMATION.LOCAL\DFSvendeurs**
* Ne pas cocher "Se reconnecter lors de la connexion"

**Test 1**

Ouvrir l’explorateur de fichiers et accéder à votre espace de noms en utilisant la lettre V.

Vous devez vérifier si les deux dossiers "Commandes" et "Clients" sont présents sous la DFS.

**Test 2**

Vous devez vérifier que vous pouvez écrire dans les dossiers "Commandes" et "Clients".

**Test 3**

Vous devez vérifier que le contenu des partages **\\SERVEUR2\C53\_Cmd** et **\\SERVEUR1\C53\_Cli** correspond au contenu des dossiers "**Commandes**" et "**Clients**" qui sont sous la DFS.

**Étape 4 - Création d’un espace de noms avec réplication**

Sur le SERVEUR2, dans la console "Gestion du système de fichiers distribués DFS" créer un nouvel espace de noms ayant les caractéristiques suivantes

* Écran "**Serveur d’espaces de noms**"
* inscrire le nom du contrôleur de domaine (SERVEUR1)
* Écran "**Nom et paramètres de l’espace de noms**"

Vous devez inscrire le nom de l’espace de noms, mais faites attention un bouton "Modifier les paramètres…" sera disponible dès que votre nom sera inscrit et vous devrez l’utiliser.

* + Nom: **DFSproduction**
  + Bouton "Modifier les paramètres…"
* Chemin d’accès local du dossier partagé: C:\DFSRoots\DFSproduction
* Autorisations du dossier partagé

"Les administrateurs ont un accès total, les autres ont un accès en lecture seule"

* Écran "**Type d’espace de noms**"
* Sélectionner "Espace de noms de domaine"
* Cocher "Activer le mode Windows Server 2008"
* Aperçu de l'espace de noms de domaine

Le nom de référence de votre espace de nom est **\\FORMATION.LOCAL\DFSproduction**

* Écran "**Revoir les paramètres et créer l'espace de noms**"
* Cliquer sur le bouton "Créer" pour déclencher la création de votre espace de noms

Dans votre console, dans l’écran de gauche, sélectionner votre nouvel espace de noms "\\FORMATION.LOCAL\DFSproduction"

Premier dossier

* Nom: Commandes
* Cible du dossier (chemin d’accès): **\\SERVEUR2\C53\_Cmd**

Deuxième dossier

* Nom: Inventaire
* Cible du dossier (chemin d’accès): **\\SERVEUR1\C53\_InvB**

Troisième dossier

* Nom: Production
* Cible du dossier (chemin d’accès): **\\SERVEUR2\C53\_Prod**

Comme l’inventaire est un dossier d’une importance primordiale pour la compagnie, il est emmagasiné à deux endroits. En créant une "réplique" dans un espace de noms pour un dossier, on crée un processus de synchronisation automatique. Nous aurons donc par la même occasion un mécanisme de tolérance de panne.

Le curseur sur "**Inventaire**", dans le menu contextuel vous allez créer une réplique.

Choisir l’option "Ajouter une cible de dossier…"

* Chemin d’accès à la cible du dossier: **\\SERVEUR2\C53\_InvA**
* Au message de réplication qui demande de créer un groupe, vous devez répondre OUI
* Écran "Nom du groupe de réplication et du dossier répliqué"
* Ne rien changer dans le premier écran
* Écran "Éligibilité de réplication"
* Les deux partages d’inventaire devraient être listés
* Écran "Membre principal"
* Choisir le contrôleur de domaine (SERVEUR1)
* Écran "Sélection de topologie"
* Sélectionner "Maille pleine"
* Écran "Planification du groupe de réplication et bande passante"
* Choisir l’option "Répliquer aux jours et heures spécifiés"
* Horaire de réplication: **Tous les jours de 08:00 à 18:00, avec une utilisation complète de la bande passante**

Lier cet espace de noms à la lettre T:

Tester votre espace de nom

* Ajouter des dossiers ou des fichiers dans les dossiers physiques et vérifier via la lettre T dans l’explorateur

**Étape 5 - Création d’un espace de noms avec une DFS**

Créer un "nouvel espace de nom"

* Écran "Serveur d'espaces de noms"
* inscrire le nom de votre serveur virtuel 2
* Écran "Nom et paramètres de l’espace de noms"
  + Nom: **DFSmarketing**
  + Bouton "Modifier les paramètres…"
* Chemin d’accès local du dossier partagé: C:\DFSRoots\DFSmarketing
* Autorisations du dossier partagé

"Les administrateurs ont un accès total, les autres ont un accès en lecture seule"

* Écran "Type d’espace de noms"
* Sélectionner "Espace de noms de domaine"
* Cocher "Activer le mode Windows Server 2008"
* Aperçu de l'espace de noms de domaine

Le nom de référence de votre espace de nom est **\\FORMATION.LOCAL\DFSmarketing**

* Écran "**Revoir les paramètres et créer l'espace de noms**"
* Cliquer sur le bouton "Créer" pour déclencher la création de votre espace de noms

Dans votre nouvel espace de noms créer trois dossiers

Premier dossier

* Nom : Publicité
* Cible du dossier (chemin d’accès): **\\SERVEUR1\C53\_Pub**

Deuxième dossier

* Nom : WEB
* Cible du dossier (chemin d’accès): **\\SERVEUR2\C53\_Web**

Troisième dossier (attention: ce sera une DFS et non un partage simple)

* Nom : Vendeurs
* Cible du dossier (chemin d’accès): **\\SERVEUR2\DFSvendeurs**

Afficher la feuille de propriétés de l’espace de noms

Comme cet espace de noms contient le partage "Publicité" pour lequel il y a des droits différents selon les utilisateurs, vous allez activer "l’énumération basée sur l’accès"

* Dans l’onglet "Avancée" des "Propriétés" de votre espace de noms, cocher "Activer l’énumération basée sur l’accès pour cet espace de noms"

Dans la console "Gestionnaire de serveur \ Services de fichiers et de stockage \ Partages", dans les propriétés du partage C53\_Pub, vous devez cochez "Activer l'énumération basée sur l'accès".

Lier cet espace de noms à la lettre W:

* Observer ce qui est visible

**Étape 6 - Affichage des DFS**

Dans la console de gestion des DFS faites afficher toutes les DFS de votre réseau.

**Étape 7 - Tester l'accès aux DFS**

Tester vos DFS avec les utilisateurs du groupe grINF\_Gestionnaires à partir du SERVEUR2.

Vérifier vos droits de lecture et d’écriture

Vérifier ce qui est visible dans le cas du dossier "Publicité"

## DFS Mise en place

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

**Objectifs**

* Révision de PowerShell pour
* la création des dossiers et l'attribution des autorisations NTFS
* la création des partages et l'attribution des autorisations de partage
* Création d'une structure de dossiers sur plusieurs serveurs
* Installation des services de rôle pour les DFS

**Documentation sur les DFS**

Les espaces de noms DFS et la réplication DFS dans "Windows Server" sont des services de rôle au sein du rôle "Services de fichiers et de stockage".

**Espaces de noms DFS**

Ils permettent de grouper des dossiers partagés qui se trouvent sur des serveurs différents en un ou plusieurs espaces de noms logiquement structurés. Pour les utilisateurs, chaque espace de noms apparaît sous la forme d’un dossier partagé unique avec une série de sous-dossiers.

**Réplication DFS**

Elle permet de répliquer des dossiers de manière efficace (y compris les dossiers désignés par un chemin d’accès à un espace de noms DFS) sur une multitude de serveurs et de sites. La réplication DFS utilise un algorithme de compression appelé "compression différentielle à distance" (RDC). L’algorithme RDC détecte les changements de données dans un fichier et permet à la réplication DFS de répliquer uniquement les blocs de fichiers modifiés à la place du fichier entier.

L'accès à un dossier partagé se fait avec **\\NomDuServeur\NomPartage**

L'accès à une DFS se fait avec **\\NomDuDomaine\NomDFS**

**Étape 1 - Identification des serveurs**

Pour ce laboratoire nous utiliserons vos deux ordinateurs pour simuler un "datacenter" comportant plusieurs serveurs de fichiers.

|  |  |
| --- | --- |
| Nom du serveur | Informations supplémentaires |
| SERVEUR1 | Le contrôleur de domaine |
| SERVEUR2 | Le serveur membre du domaine |

**Étape 2 - Les utilisateurs**

Nous utiliserons les 2 utilisateurs EMP09 et EMP10 qui sont membres du groupe grINF\_Gestionnaires.

**Étape 3a - Les dossiers et les autorisations NTFS**

La création de tous les dossiers et les attributions des autorisations NTFS se fera dans un seul script à partir du serveur SERVEUR2.

Pour attribuer les autorisations NTFS, vous devez utiliser la commande "icacls.exe".

**Liste des autorisations communes**

Sauf avis contraire, les autorisations sur les dossiers utilisent l'héritage standard (OI)(CI).

**Pour chaque dossier qui débute par C:\\_C53**

* Désactiver l'héritage et choisir l'option "Supprimer toutes les autorisations héritées de cet objet".
* Ajouter les autorisations
* "Administrateurs" "Contrôle total" "Ce dossier, les sous-dossiers et les fichiers"
* "Système" "Contrôle total" "Ce dossier, les sous-dossiers et les fichiers"
* TECH "Contrôle total" "Ce dossier, les sous-dossiers et les fichiers"

**Liste des autres autorisations particulières:**

|  |  |  |
| --- | --- | --- |
| Nom  du serveur | Dossiers | Ajouter les autorisations suivantes |
| SERVEUR1 | C:\\_C53\_Clients | **grINF\_Gestionnaires**  "Modification" "Ce dossier, les sous-dossiers et les fichiers" |
| SERVEUR1 | C:\\_C53\_Inventaire | **grINF\_Gestionnaires**  "Modification" "Ce dossier, les sous-dossiers et les fichiers" |
| SERVEUR1 | C:\\_C53\_Publicite | **grINF\_Gestionnaires**  "Lecture et exécution" "Ce dossier seulement" |
| SERVEUR1 | C:\\_C53\_Publicite\**EMP09** | **Le dossier EMP09 hérite des autorisations de son parent.**  **EMP09** "Modification" "Ce dossier, les sous-dossiers et les fichiers" |
| SERVEUR1 | C:\\_C53\_Publicite\**EMP10** | **Le dossier EMP10 hérite des autorisations de son parent.**  **EMP10** "Modification" "Ce dossier, les sous-dossiers et les fichiers" |
| SERVEUR2 | C:\\_C53\_Commande | **grINF\_Gestionnaires**  "Modification" "Ce dossier, les sous-dossiers et les fichiers" |
| SERVEUR2 | C:\\_C53\_Inventaire | **grINF\_Gestionnaires**  "Modification" "Ce dossier, les sous-dossiers et les fichiers" |
| SERVEUR2 | C:\\_C53\_Production | **grINF\_Gestionnaires**  "Lecture et exécution" "Ce dossier, les sous-dossiers et les fichiers"  **EMP10** "Modification" "Ce dossier, les sous-dossiers et les fichiers" |
| SERVEUR2 | C:\\_C53\_Web | **grINF\_Gestionnaires**  "Modification" "Ce dossier, les sous-dossiers et les fichiers" |

**Étape 3b - Les partages sur les dossiers et les autorisations de partage**

La création de tous les partages se fera dans un seul script à partir du serveur SERVEUR2.

Pour chaque partage, les autorisations de partage seront "Tout le monde", "Contrôle total".

Pour chaque partage, vous devez désactiver la mise en cache du partage.

Pour chaque partage, vous devez activer l’énumération basée sur l'accès

|  |  |  |
| --- | --- | --- |
| Nom du serveur | Dossiers | Partages |
| **SERVEUR1** | C:\\_C53\_Clients | C53\_Cli |
| C:\\_C53\_Inventaire | C53\_InvB |
| C:\\_C53\_Publicite | C53\_Pub |
| C:\\_C53\_Publicite\EMP09 | aucun partage sur ce dossier |
| C:\\_C53\_Publicite\EMP10 | aucun partage sur ce dossier |
| **SERVEUR2** | C:\\_C53\_Commande | C53\_Cmd |
| C:\\_C53\_Inventaire | C53\_InvA |
| C:\\_C53\_Production | C53\_Prod |
| C:\\_C53\_Web | C53\_Web |

**Vérification des partages**

Pour vérifier la liste de vos partages, vous pouvez utiliser les commandes

* **Get-SmbShare -CimSession SERVEUR1**
* **Get-SmbShare -CimSession SERVEUR2**

Pour vérifier la liste de vos partages, vous pouvez utiliser

* la console "Gestionnaire de serveur \ Services de fichiers et de stockage \ Partages"

**Étape 4 - Exemples pour la programmation des dossiers et des partages**

L’objectif est d’écrire un script PowerShell qui permet de créer des dossiers et des partages sur votre serveur et sur des serveurs à distance. Le script PowerShell doit s'exécuter à partir du SERVEUR2.

Je vous conseille d’inclure des instructions de "suppression" des partages et des dossiers, avant les énoncés de création afin d’éviter les problèmes si vous devez exécuter votre script à plusieurs reprises.

**IMPORTANT: vous devez supprimer les partages avant de supprimer les dossiers**

**#-------------------------------------------------------------------**

**# Le serveur SERVEUR1 est le contrôleur de domaine**

**#-------------------------------------------------------------------**

**# Supprime les anciens partages sur le SERVEUR1**

**Get-SmbShare -Name C53\_\* -CimSession $ordi | `**

**Remove-SmbShare -Force -ErrorAction SilentlyContinue**

**# Supprime les anciens dossiers sur le SERVEUR1**

**$chemin = "\\SERVEUR1\C$\\_C53\_"**

**Remove-Item -Path $chemin"\*" -Recurse -Force -ErrorAction SilentlyContinue**

**New-Item** permet de créer des fichiers et des dossiers.

Pour créer un dossier sur un ordinateur distant, vous devez utiliser l’accès au partage administratif C$ de l'ordinateur distant.

Pour créer le dossier C:\\_C53\_TEST sur le SERVEUR1 à partir de l'ordinateur SERVEUR2

**$dossierTEST = "\\SERVEUR1\c$\\_C53\_TEST"**

**New-Item -ItemType Directory -Path $dossierTEST**

#"Désactiver l’héritage" et "Supprimer toutes les autorisations héritées de cet objet"

**icacls.exe $dossierTEST /inheritance:r**

# Ajout des autorisations NTFS

**icacls.exe $dossierTEST /grant "administrateurs:(CI)(OI)(F)"**

**icacls.exe $dossierTEST /grant "system:(CI)(OI)(F)"**

**icacls.exe $dossierTEST /grant "FORMATION\TECH:(CI)(OI)(F)"**

**icacls.exe $dossierTEST /grant "grINF\_Gestionnaires:(CI)(OI)(M)"**

**New-SMBShare** permet de créer un partage sur un dossier.

Pour créer un partage sur un dossier qui est sur un ordinateur distant, vous devez utiliser le chemin local et utiliser le paramètre -CimSession pour spécifier le nom de l'ordinateur distant.

Pour créer le partage C53\_TEST sur le dossier C:\\_C53\_TEST qui est sur l'ordinateur SERVEUR1 à partir de l'ordinateur SERVEUR2

**New-SMBShare -Name C53\_TEST `**

**-Path C:\\_C53\_TEST `**

**-FullAccess "Tout le monde" `**

**-CachingMode none `**

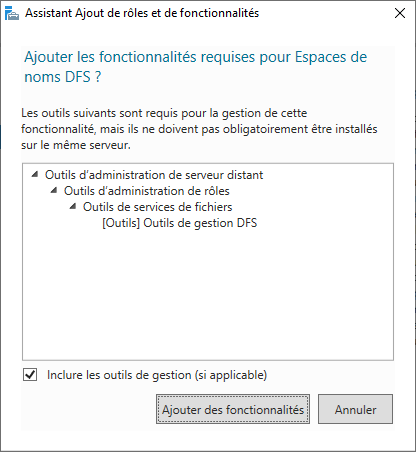
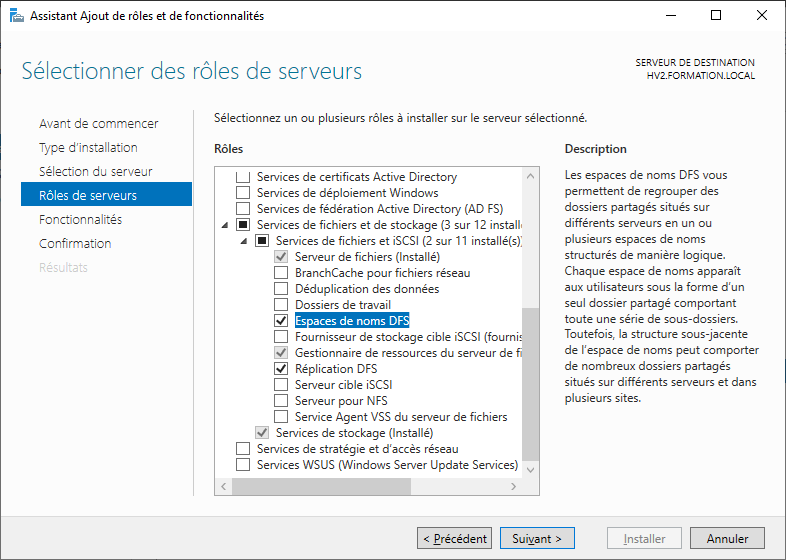
**-FolderEnumerationMode AccessBased `**

**-CimSession SERVEUR1**

**Étape 5 - Installation du rôle DFS**

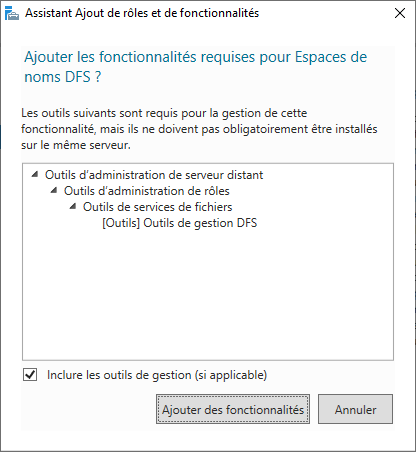
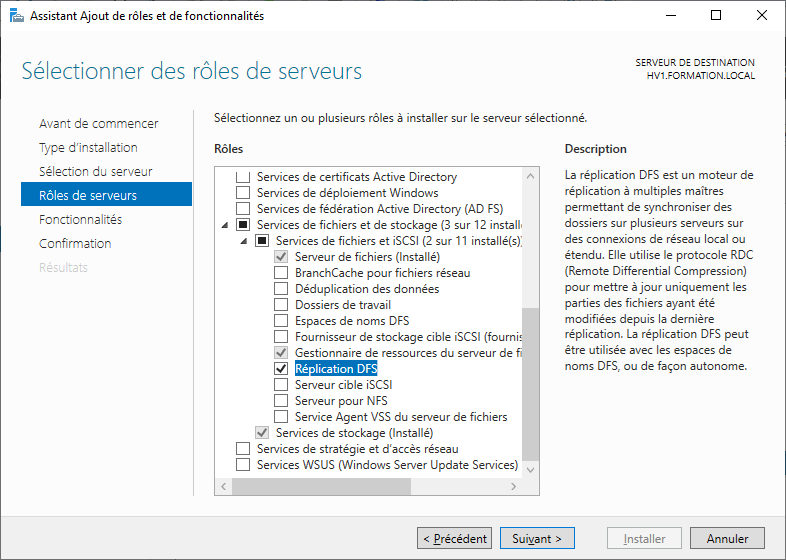
Dans le gestionnaire du serveur SERVEUR2

* Sélectionner le rôle "Services de fichiers et de stockage"
* Sélectionner "Services de fichiers et iSCSI"
* Cocher "Espaces de noms DFS" et accepter les fonctionnalités
* Cocher "Réplication DFS"



Dans le gestionnaire du serveur SERVEUR1

* Sélectionner le rôle "Services de fichiers et de stockage"
* Sélectionner "Services de fichiers et iSCSI
* Cocher "Réplication DFS"" et accepter les fonctionnalités



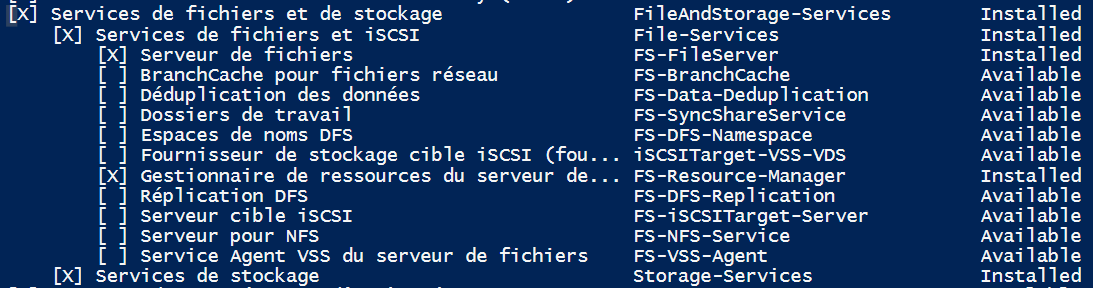
Le rôle de réplication DFS est obligatoire sur un serveur qui héberge une copie des espaces de noms DFS.

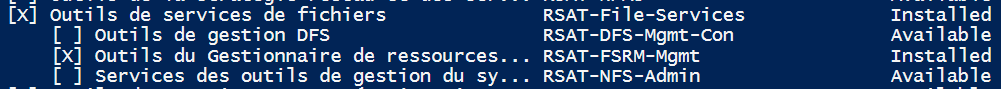
**ANNEXE**

**Installation du rôle DFS par programmation PowerShell**

Get-WindowsFeature permet d'afficher l'état des rôles et des fonctionnalités.







# Pour afficher les rôles et fonctionnalités qui sont installés

**Get-WindowsFeature | Where-Object InstallState -eq "Installed"**

FS-DFS-Namespace correspond à "Espaces de noms DFS"

FS-DFS-Replication correspond à "Réplication DFS"

RSAT-DFS-Mgmt-Con correspond à "Outils de gestion DFS"

**Get-WindowsFeature -Name FS-DFS-Namespace,FS-DFS-Replication,RSAT-DFS-Mgmt-Con**



Install-WindowsFeature permet d'installer des rôles et des fonctionnalités.

Sur le serveur SERVEUR2

**Install-WindowsFeature -Name FS-DFS-Namespace -Verbose**

**Install-WindowsFeature -Name FS-DFS-Replication -Verbose**

**Install-WindowsFeature -Name RSAT-DFS-Mgmt-Con -Verbose**

Sur le serveur SERVEUR1

**Install-WindowsFeature -Name FS-DFS-Replication -Verbose**

**Install-WindowsFeature -Name RSAT-DFS-Mgmt-Con -Verbose**