http://WWW.CABARE.NET ©

Stratégies GPO & AD sous Windows 2026 - 2012R2
– sys 26 – cours -

Stratégies Windows & GPO de Domaine 2016

Michel Cabaré – Ver 2.5 – Juin 2017-

Stratégies GPO & AD sous Windows 2016 – 2012R2
Cours

Michel Cabaré – Ver 2.5 – Juin 2017

www.cabare.net ©

La formation que vous suivez, à pour but de vous initier avec les logiciels Microsoft Windows 2016-2012R2 Serveur et clients Windows 10- 7.

Ce Support à pour but de vous fournir un certain nombre d'éléments concernant soit des manipulations, soit des notions théoriques concernant la gestion de réseaux locaux

Il ne peut en aucun cas se substituer à la participation à la formation, ni à tout ou partie de la documentation fournie avec le logiciel.

En effet, **et c'est là sa vocation première**, ce document doit **"servir de support à la prise de notes en formation, et sera donc avantageusement complété par vos soins"**. Son but est de permettre une présentation de vos notes plus structurée et donc plus facilement utilisable ensuite.

Bon Travail

Michel Cabaré

TABLE DES MATIÈRES

STRATEGIES LOCALES WINDOWS 10-7

Types de stratégie :

Les stratégies permettent de modifier la configuration d'un ordinateur.

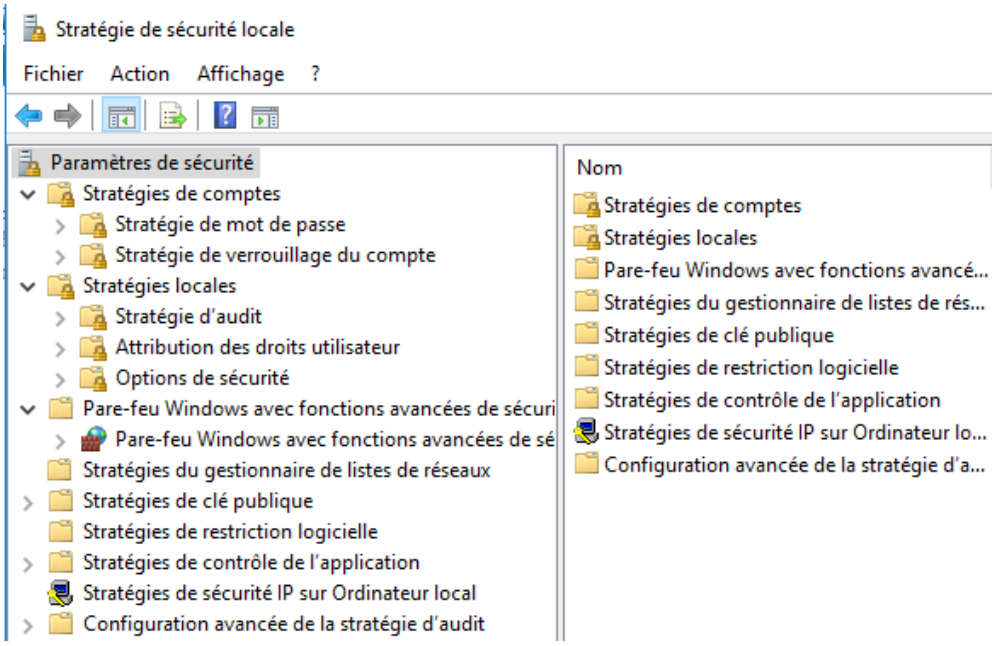
il existe essentiellement 2 méthodes pour implémenter des stratégies sur des postes Windows depuis 7, les **stratégie système locale** appliquée sur un ordinateur unique, ou les **stratégies de groupe** appliquée dans un domaine et déployée sur plusieurs ordinateurs…

Stratégies locales (cf microsoft GPO hors AD):

Lorsque un ordinateur n'appartient à aucun domaine, pour configurer une stratégie il faut obligatoirement passer par une **stratégie locale**…. Ces stratégies locales sont disponibles

- Depuis **Windows 7** (et Windows -XP 2000)
  (qu'il soit membre d'un domaine ou non)
- Sur les **Serveurs 2016 2012R2** même **Contrôleur de Domaine** et sur les **Serveur 2008R2-2003** (s'ils ne sont pas **Contrôleur de Domaine**).

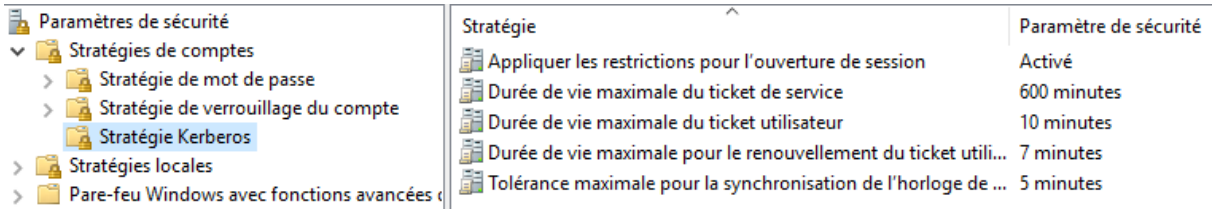
On demande **Outils d'administration / Stratégies de sécurités locales**,



avec

Nom	Description
Stratégies de comptes	Stratégies de mot de passe et de verrouillage de compte
Stratégies locales	Stratégies des options d'audit, de droits d'utilisateurs et de sécurité
Pare-feu Windows avec fonctions avancé...	Pare-feu Windows avec fonctions avancées de sécurité
Stratégies du gestionnaire de listes de rés...	Stratégies de groupes relatives au nom, à l'icône et à l'emplacement du réseau.
Stratégies de clé publique	
Stratégies de restriction logicielle	
Stratégies de contrôle de l'application	Stratégies de contrôle de l'application
Stratégies de sécurité IP sur Ordinateur lo...	Administration de la sécurité du protocole Internet (IPSec). Gère les stratégies IPSec...
Configuration avancée de la stratégie d'a...	Configuration avancée de la stratégie d'audit

Par exemple sur un Serveur 2016 2012 on aura en plus par rapport à un client Windows 10 dans les stratégies locales une entrée dans les **Stratégies de comptes - Stratégie Kerberos**



Stratégies de Groupe GPO (cf microsoft GPO dans AD):

Lorsque un ordinateur appartient à un domaine, on peut alors aussi utiliser les stratégies de groupes dites **GPO**. On étudiera ces **GPO** ultérieurement, mais il faut savoir que l'on peut poser des stratégies de groupes à différents niveaux, Lorsque l'on est dans un domaine, les **stratégies locales** peuvent être écrasées par des stratégies de plus haut niveau.

Configurer des stratégies localement – paramètres GPO stratégies locales:

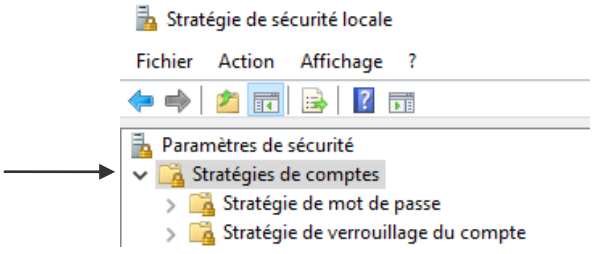
Il ne faut pas confondre "*configurer des stratégies localement*", qui suppose que l'action soit faite localement sur chaque machine, via le **Panneau de Configuration**, avec la notion de "*paramètres de stratégie locale*".

En effet on l'a vu, Les **paramètres de stratégie locale** sont configurables en partie localement depuis la console mmc "**Stratégie de sécurité locale**" mais aussi dans une **stratégie de groupe GPO**, définie au niveau du domaine ou d'une UO… dans ce cas ces paramètres se superposent voire écrasent les valeurs définies via la console de stratégie de sécurité locale…

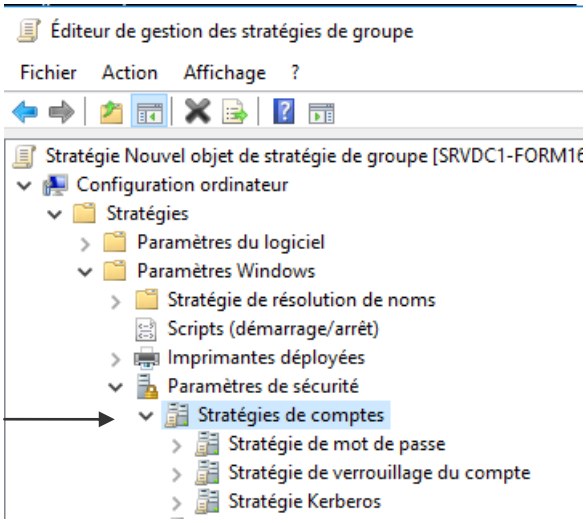
Les paramètres communs aux **Stratégie de sécurité locale** et aux **Stratégie de groupe GPO** sont donc principalement les suivants:

- **Stratégies de compte** (~gestion compte utilisateur)

Passées via le **Panneau de configuration**

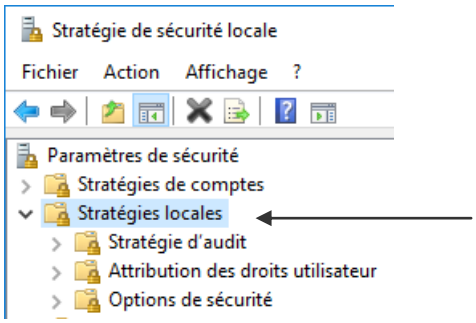


Passées via domaine par **GPO**

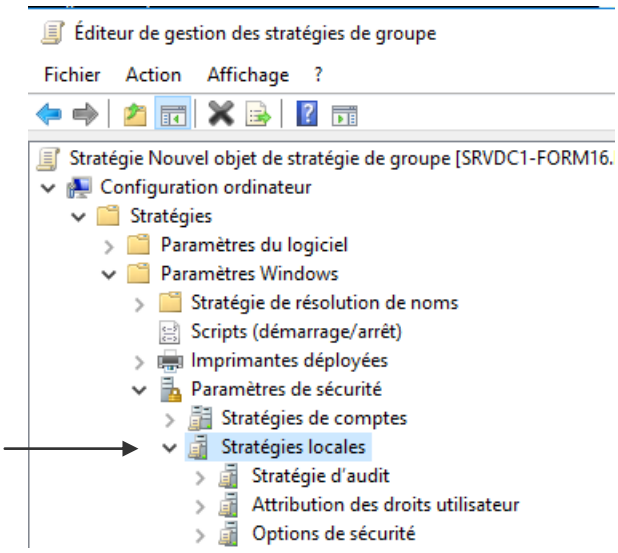


- **Stratégies locales** (~ouverture session locale et prérogatives associées)

Passées via le **Panneau de configuration**

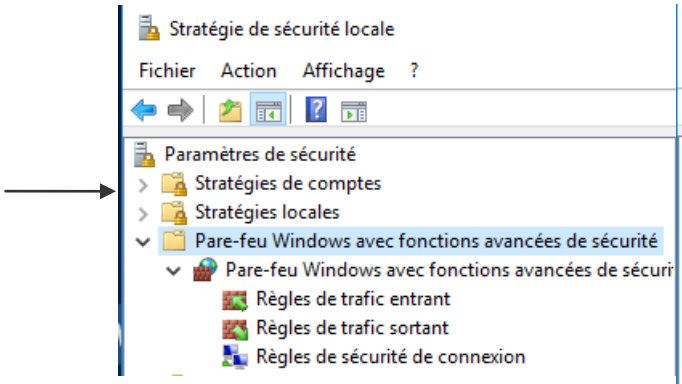


Passées via domaine par **GPO**

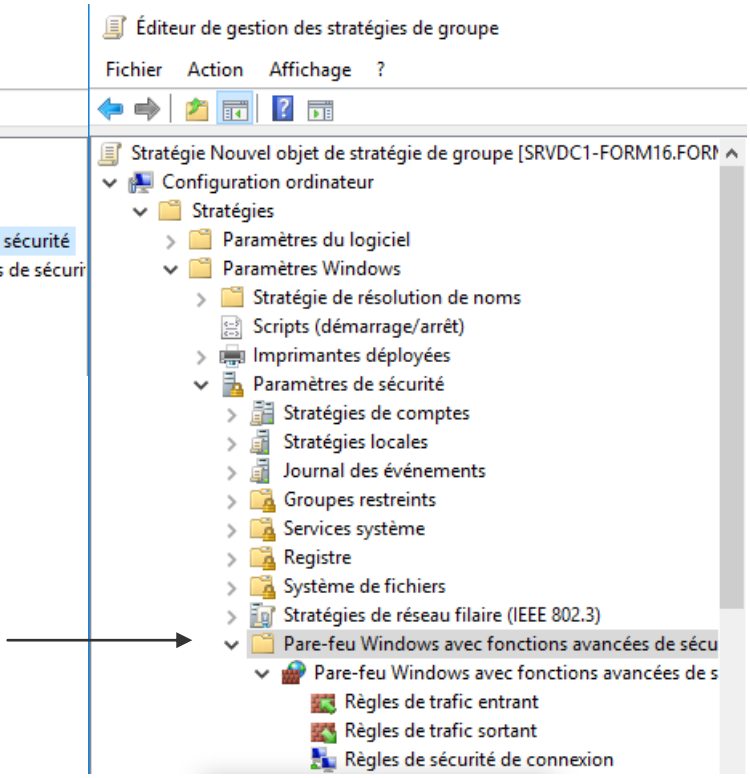


- **Pare-feu Windows** (~gestion du pare-feu)

Passées via **Panneau de configuration**

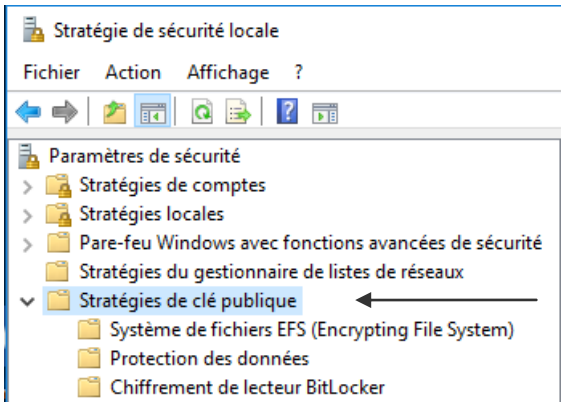


Passées via domaine par **GPO**

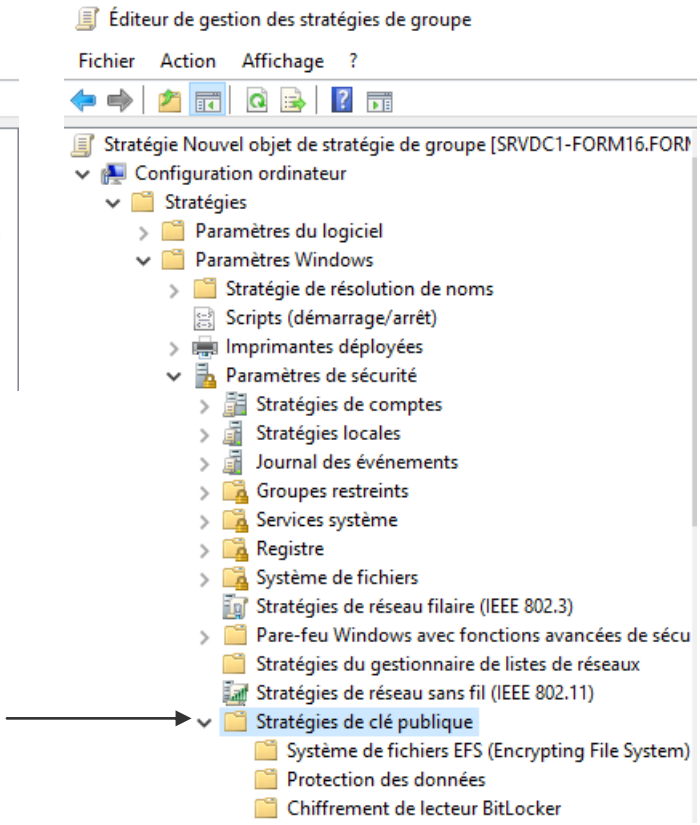


- **Stratégies de clé publique** (agent de récupération EFS)

Passées via **Panneau de configuration**



Passées via domaine par **GPO**

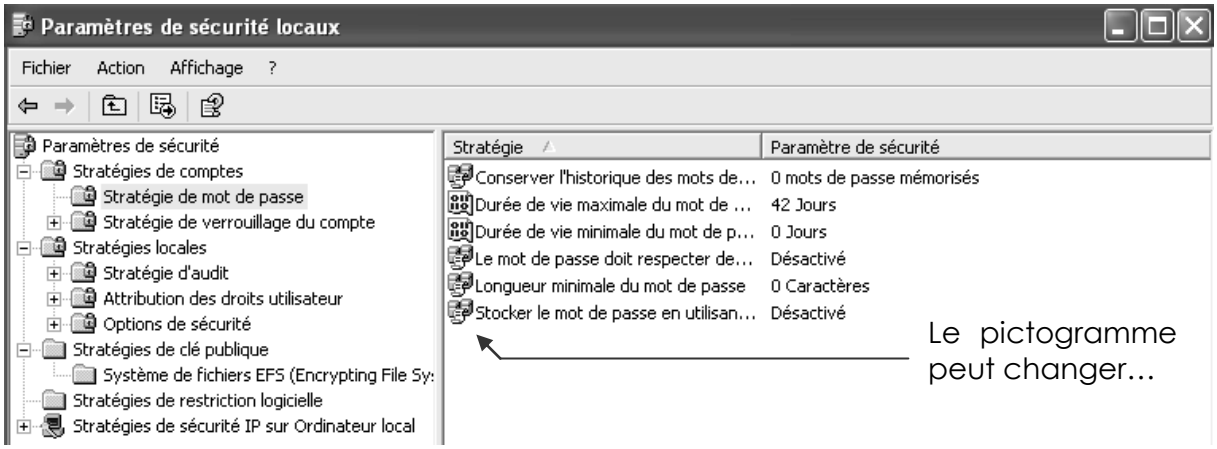


Et aussi

- **Stratégies IPSEC** (cryptage IP)
- **Stratégies de restriction logicielle** (sécurisation lancement applications)

Configurer une stratégie localement – Pictogramme:

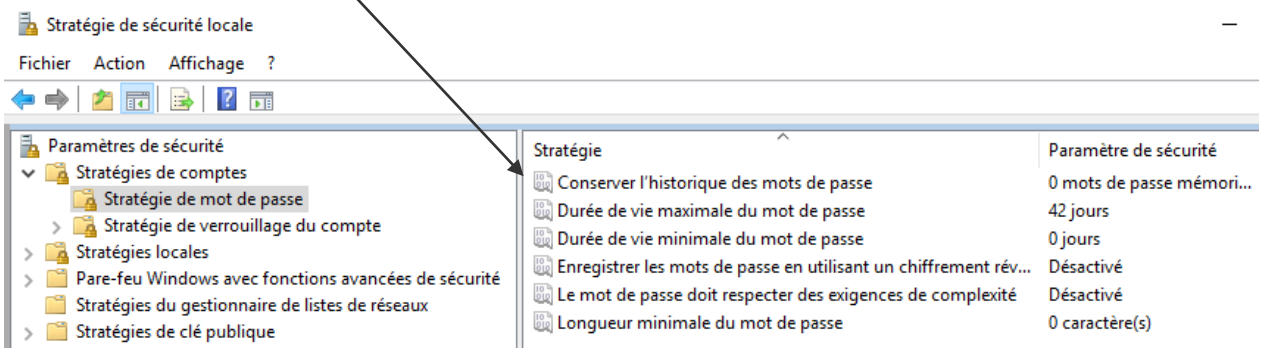
Dans l'arborescence, on visualise à droite les différentes composantes…



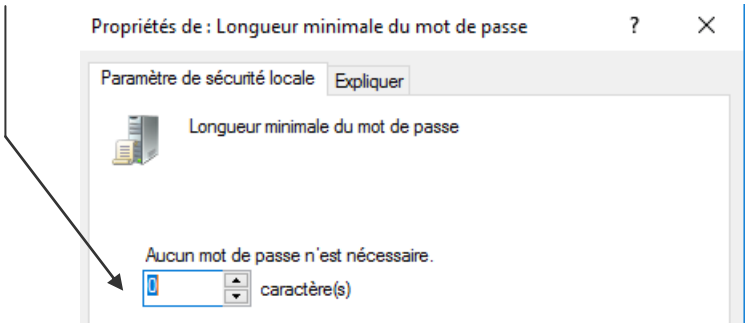
Si une stratégie de domaine s'est propagée, la visualisation de la **stratégie locale** sera marquée d'une icône indiquant qu'elle vient du Domaine,  sinon elle indiquera qu'elle est gérée localement. 

Par exemple, dans **Stratégies de compte/ Stratégies de mot de passe / longueur minimale du mot de passe**

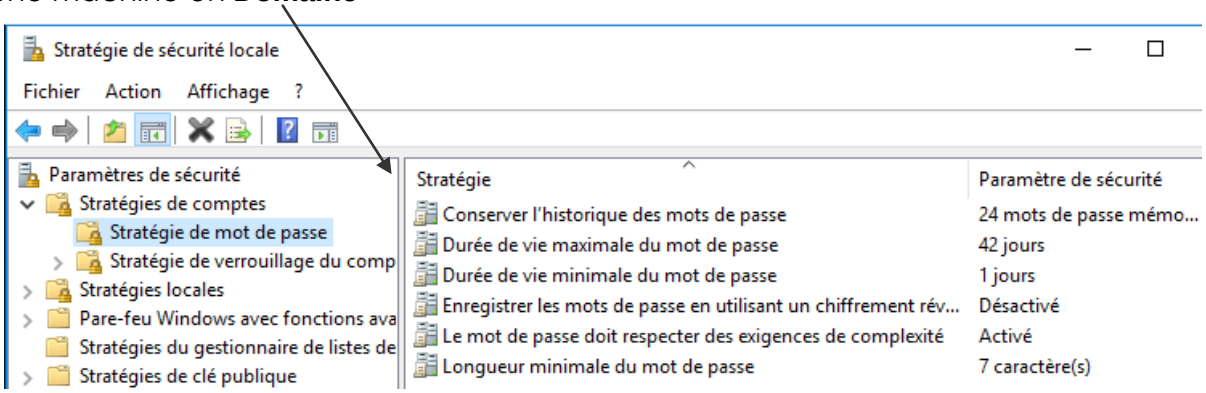
Sur une machine en **Workgroup**



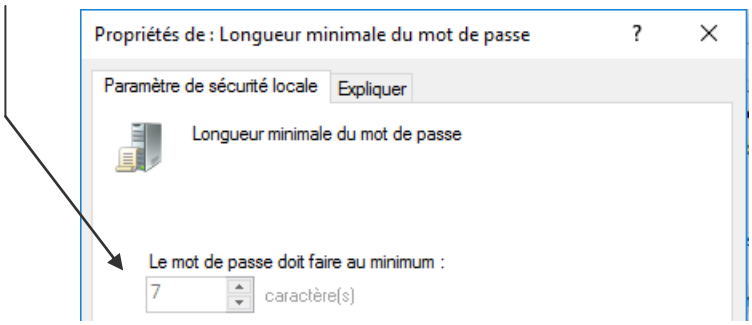
On la « main »



Sur une machine en **Domaine**



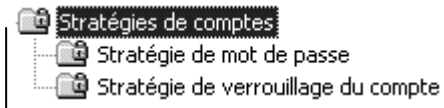
On n'a pas la « main »



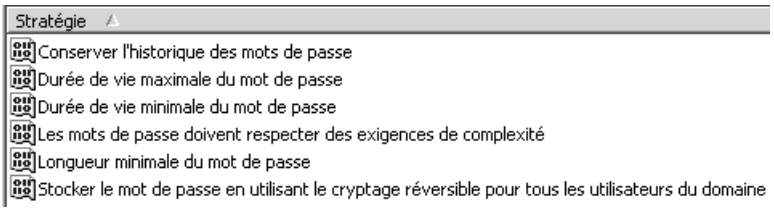
Contenu des Paramètres locaux de sécurité :

N.B : il faut bien évidemment faire attention à ce que toutes les stratégies ne sont pas disponibles à l'identiques sur toutes les machines, en fonctions des systèmes Windows 10, Seven, voire Xp et des services packs installés, voir des modules complémentaires spécifiques, les noms des stratégies peuvent varier, parfois considérablement.

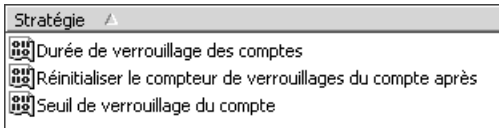
Stratégies de comptes



Stratégies de mot de passe

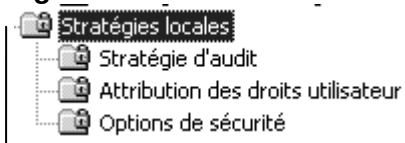


Stratégies de verrouillage du compte

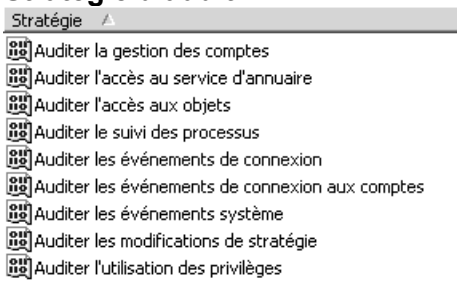


N.B : concernant la gestion des mots de passe, si un domaine existe, alors il serait bon de gérer ces stratégies essentiellement au niveau du Domaine, et jamais à un niveau inférieur, sous peine d'avoir des incohérences et des problèmes d'accès !

Stratégies locales

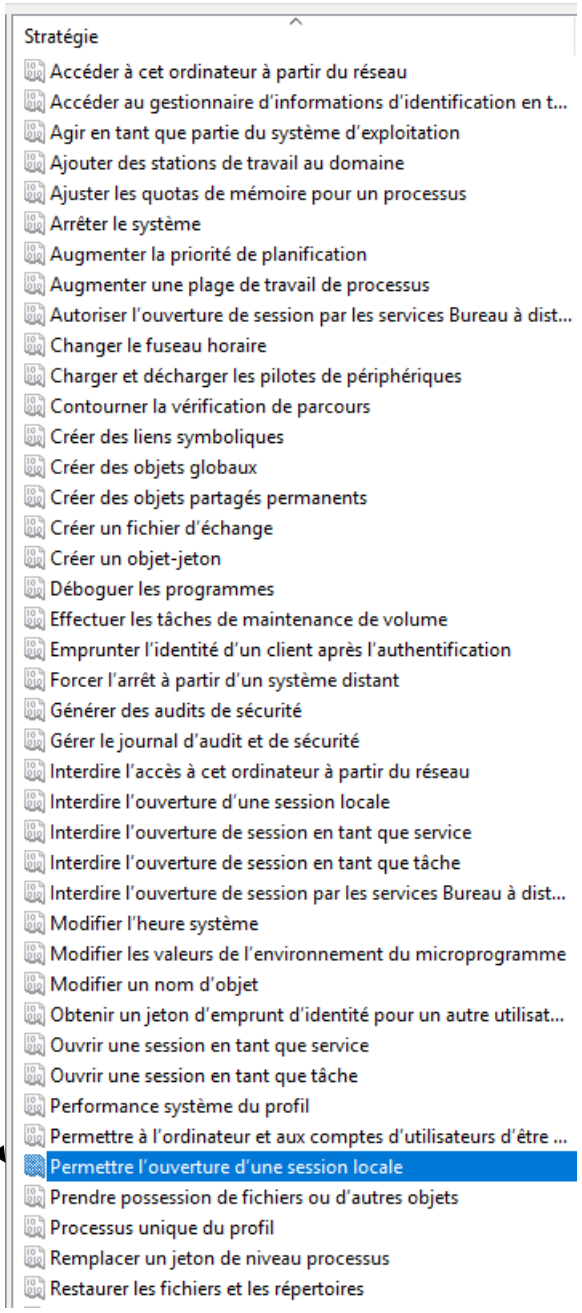


Stratégie d'audit



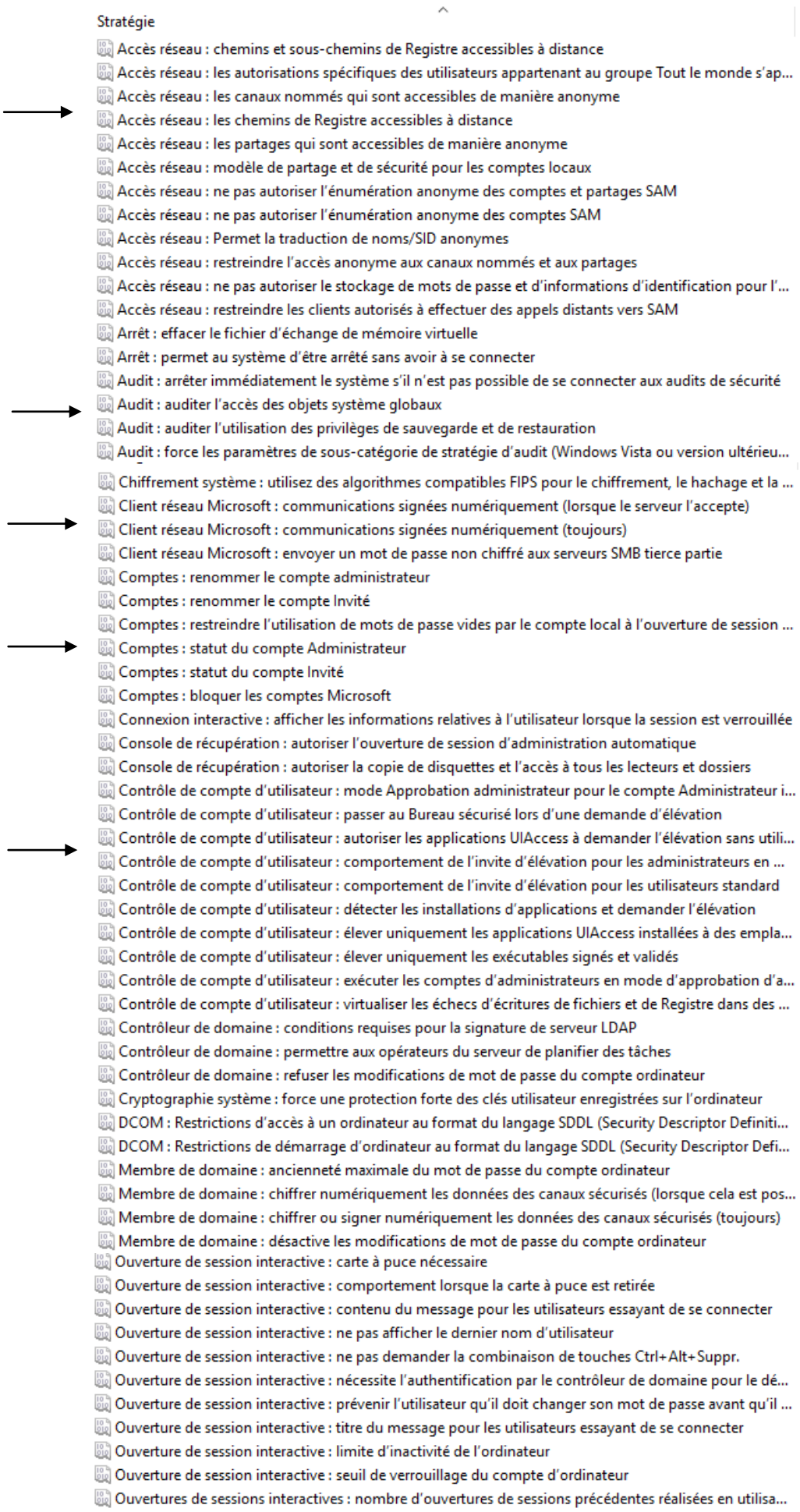
Attribution des droits utilisateurs

Exemple de différence de libellé



Options de sécurité

Depuis il y a un effort de regroupement des stratégies par « famille » : **Accès réseau : - Arrêt – Audit – Comptes – contrôle de compte Utilisateur (UAC)…Ouverture de session interactive** …

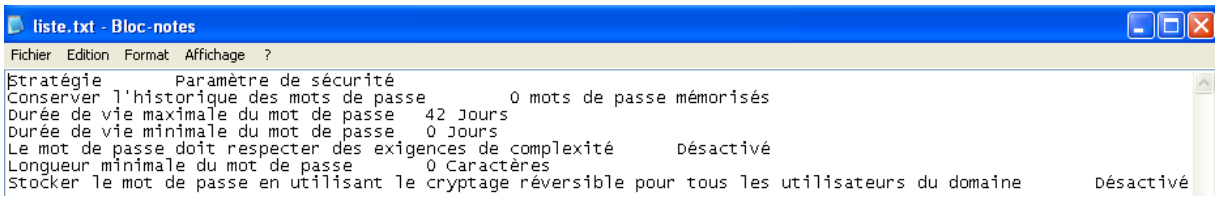

Stratégie
Accès réseau : chemins et sous-chemins de Registre accessibles à distance
Accès réseau : les autorisations spécifiques des utilisateurs appartenant au groupe Tout le monde s'ap...
Accès réseau : les canaux nommés qui sont accessibles de manière anonyme
Accès réseau : les chemins de Registre accessibles à distance
Accès réseau : les partages qui sont accessibles de manière anonyme
Accès réseau : modèle de partage et de sécurité pour les comptes locaux
Accès réseau : ne pas autoriser l'énumération anonyme des comptes et partages SAM
Accès réseau : ne pas autoriser l'énumération anonyme des comptes SAM
Accès réseau : Permet la traduction de noms/SID anonymes
Accès réseau : restreindre l'accès anonyme aux canaux nommés et aux partages
Accès réseau : ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'...
Accès réseau : restreindre les clients autorisés à effectuer des appels distants vers SAM
Arrêt : effacer le fichier d'échange de mémoire virtuelle
Arrêt : permet au système d'être arrêté sans avoir à se connecter
Audit : arrêter immédiatement le système s'il n'est pas possible de se connecter aux audits de sécurité
Audit : auditer l'accès des objets système globaux
Audit : auditer l'utilisation des privilèges de sauvegarde et de restauration
Audit : force les paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieu...
Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la ...
Client réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)
Client réseau Microsoft : communications signées numériquement (toujours)
Client réseau Microsoft : envoyer un mot de passe non chiffré aux serveurs SMB tierce partie
Comptes : renommer le compte administrateur
Comptes : renommer le compte Invité
Comptes : restreindre l'utilisation de mots de passe vides par le compte local à l'ouverture de session ...
Comptes : statut du compte Administrateur
Comptes : statut du compte Invité
Comptes : bloquer les comptes Microsoft
Connexion interactive : afficher les informations relatives à l'utilisateur lorsque la session est verrouillée
Console de récupération : autoriser l'ouverture de session d'administration automatique
Console de récupération : autoriser la copie de disquettes et l'accès à tous les lecteurs et dossiers
Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur i...
Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation
Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans utili...
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en ...
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard
Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation
Contrôle de compte d'utilisateur : élever uniquement les applications UIAccess installées à des empla...
Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés
Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'a...
Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre dans des ...
Contrôleur de domaine : conditions requises pour la signature de serveur LDAP
Contrôleur de domaine : permettre aux opérateurs du serveur de planifier des tâches
Contrôleur de domaine : refuser les modifications de mot de passe du compte ordinateur
Cryptographie système : force une protection forte des clés utilisateur enregistrées sur l'ordinateur
DCOM : Restrictions d'accès à un ordinateur au format du langage SDDL (Security Descriptor Definiti...
DCOM : Restrictions de démarrage d'ordinateur au format du langage SDDL (Security Descriptor Defi...
Membre de domaine : ancienneté maximale du mot de passe du compte ordinateur
Membre de domaine : chiffrer numériquement les données des canaux sécurisés (lorsque cela est pos...
Membre de domaine : chiffrer ou signer numériquement les données des canaux sécurisés (toujours)
Membre de domaine : désactive les modifications de mot de passe du compte ordinateur
Ouverture de session interactive : carte à puce nécessaire
Ouverture de session interactive : comportement lorsque la carte à puce est retirée
Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter
Ouverture de session interactive : ne pas afficher le dernier nom d'utilisateur
Ouverture de session interactive : ne pas demander la combinaison de touches Ctrl+Alt+Suppr.
Ouverture de session interactive : nécessite l'authentification par le contrôleur de domaine pour le dé...
Ouverture de session interactive : prévenir l'utilisateur qu'il doit changer son mot de passe avant qu'il ...
Ouverture de session interactive : titre du message pour les utilisateurs essayant de se connecter
Ouverture de session interactive : limite d'inactivité de l'ordinateur
Ouverture de session interactive : seuil de verrouillage du compte d'ordinateur
Ouvertures de sessions interactives : nombre d'ouvertures de sessions précédentes réalisées en utilisa...

Imprimer lister les stratégies :

Il est possible lorsque l'on se trouve sur une entrée précise de la stratégie, de demander via le bouton droit de la souris

Exporter la liste…

Un fois le fichier texte crée, on peut l'imprimer…



Ou le travailler (fichier texte délimité par des tabulations)

	A	B
1	Conserver l'historique des mots de passe	0 mots de passe mémorisés
2	Durée de vie maximale du mot de passe	42 Jours
3	Durée de vie minimale du mot de passe	0 Jours
4	Le mot de passe doit respecter des exigences de complexité	Désactivé
5	Longueur minimale du mot de passe	0 Caractères
6	Stocker le mot de passe en utilisant le cryptage réversible pour tous les utilisateurs du domaine	Désactivé
7	Stratégie	Paramètre de sécurité

STRATEGIES LOCALES MULTIPLES MLGPO

Stratégies locales multiples dites MLGPO

Sous **Windows Xp**, il ne pouvait y avoir qu'une seule stratégie locale, contenant un lot de commandes, valable pour :

- tous les utilisateurs….

On pouvait manipuler cela depuis l'interface du panneau de configuration, **stratégies de sécurité locales**…

On pouvait augmenter la quantité les réglages par la commande **gpedit.msc**… valable globalement pour :

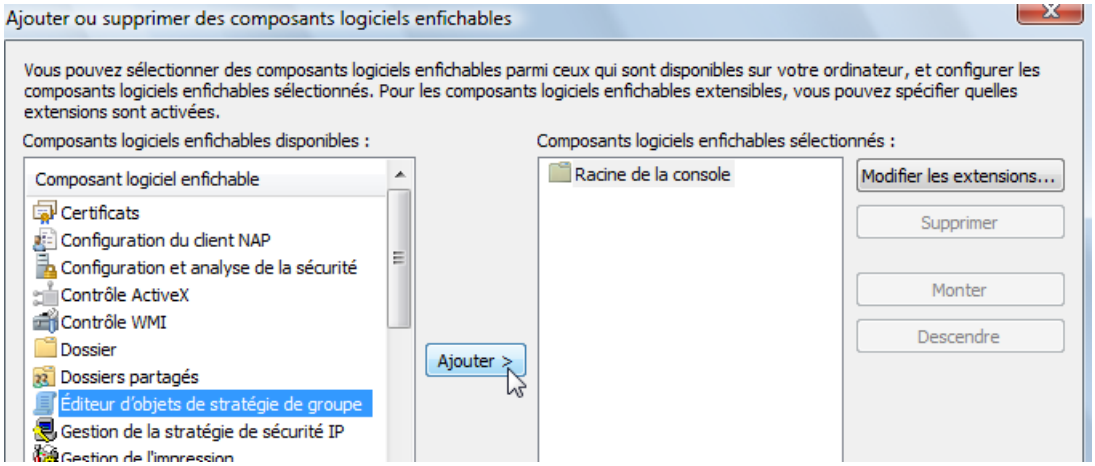
- l'ordinateur, et/ ou
- tous les utilisateurs.

Depuis **Windows Seven** il est possible maintenant de définir des stratégies multiples locales **MLGPO Multiples Local Group Policies Objects** dont la portée peut être plus fine…

- l'ordinateur, et/ ou (idem stratégie locale)
- tous les utilisateurs. (idem stratégie locale)
- Tous les administrateurs (locaux)
- Touts les non-administrateurs (locaux)
- Un utilisateur local du poste

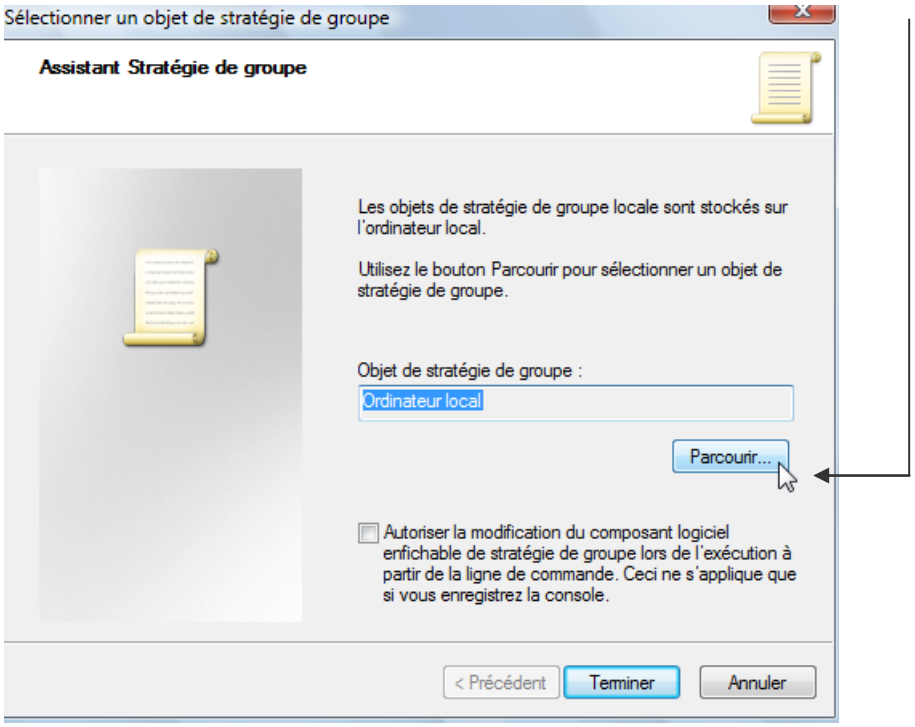
Définir une MLGPO

On construit une nouvelle **mmc**, avec **l'Editeur d'objets de stratégie de groupe**

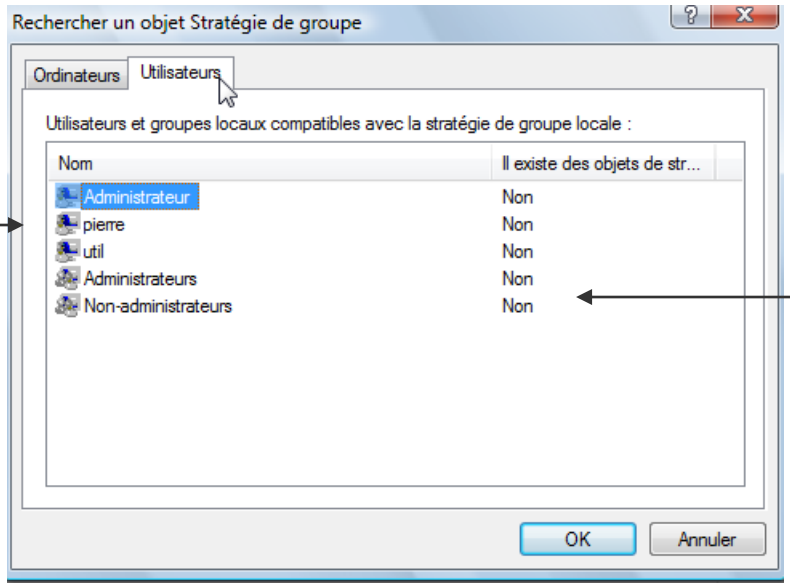


Lorsque on ajoute **l'Editeur d'objets de stratégie de groupe**, On ne demande surtout pas **Terminer**(*),

mais plutôt **Parcourir**



Et on choisit l'onglet **Utilisateur**



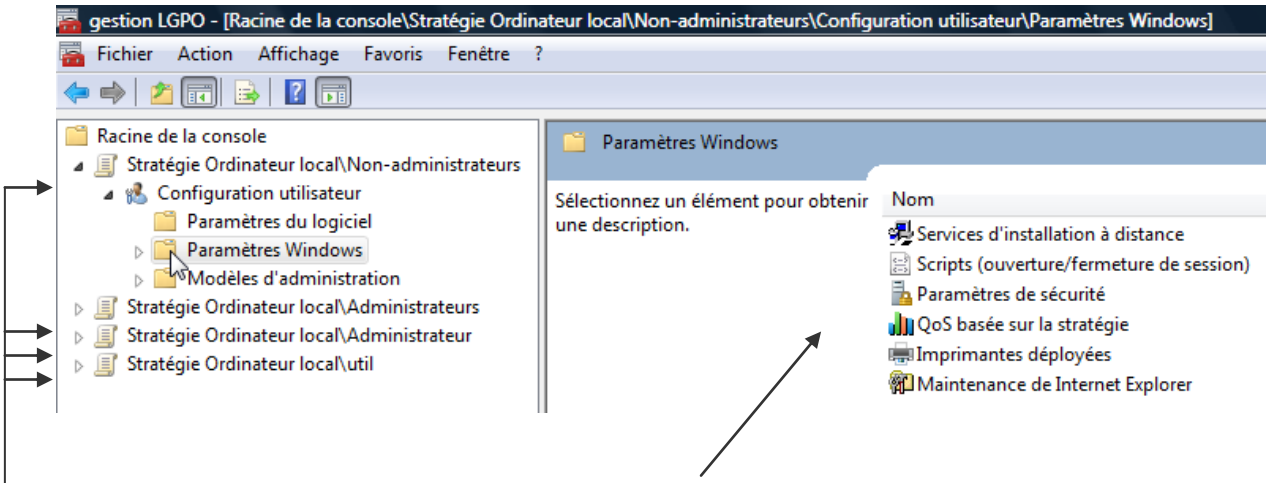
On retrouve ici les choix annoncés

- l'ordinateur, -il aurait fallut faire terminer (*)
- tous les utilisateurs. - il aurait fallut faire terminer(*)
- Tous les administrateurs (locaux)
- Tous les non-administrateurs (locaux)
- Un utilisateur local du poste

N.B: si on veut des stratégies locales multiples, il faut donc refaire autant de fois que nécessaire la manip **Ajouter / Editeur de stratégies de Groupes** en précisant à chaque fois la portée de cette stratégie locale…

*: Si on fait terminer, on obtient la même console que celle des stratégies locales ... ce n'était pas la peine de faire ce détour...

On obtient



Pour chaque Stratégie locale, on effectue les réglages…

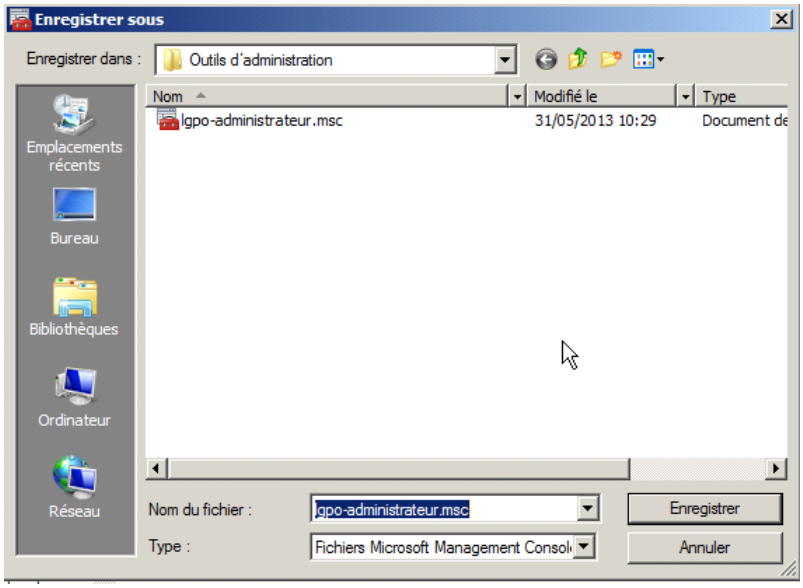
N.B: Attention, à ne pas cumuler plusieurs stratégies locales pour un même utilisateur, autrement dit si on utilise une LGPO de groupe, ne pas utiliser une LGPO pour un utilisateur particulier de ce groupe ! L'ordre théorique d'application est le suivant :

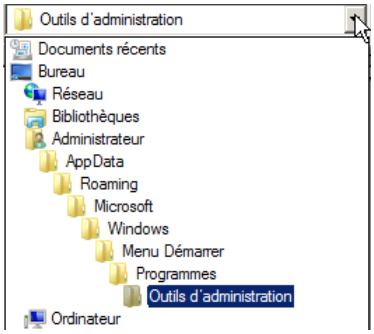
1. **MLGPO** d'ordinateur
2. **MLGPO** groupe Administrateurs
3. **MLGPO** groupe NON Administrateur
4. **MLGPO** utilisateur

N.B: le conseil c'est de ne pas utiliser ces **MLGPO** dans un domaine:

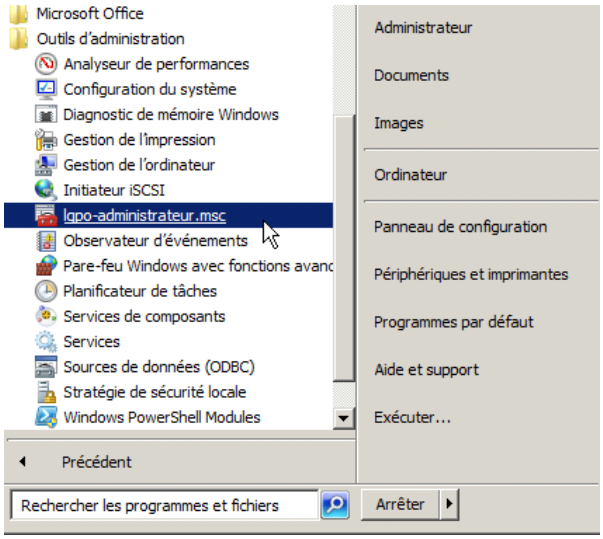
Enregistrer la MMC editeur de strategie MLGPO

Si on veut enregistrer une mmc editeur **MLGPO** pour la retrouver on peut...



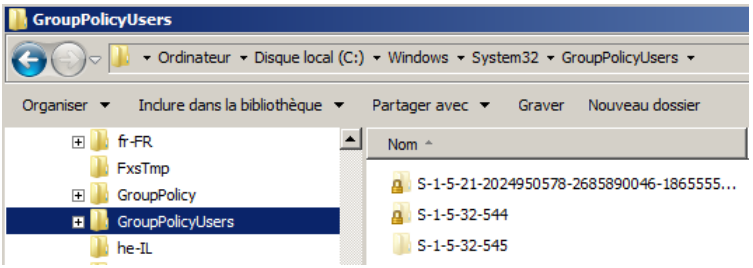


Ce qui permettrais ensuite de la retrouver via

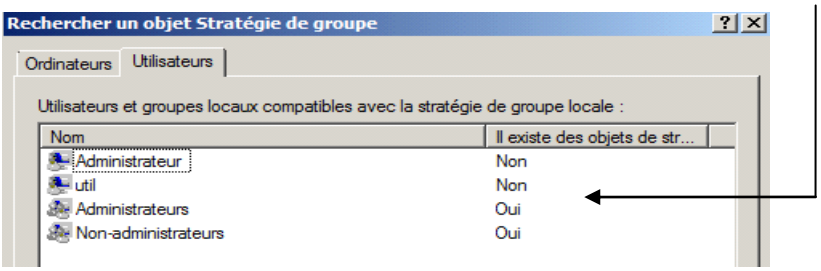


Supprimer les MLGPO

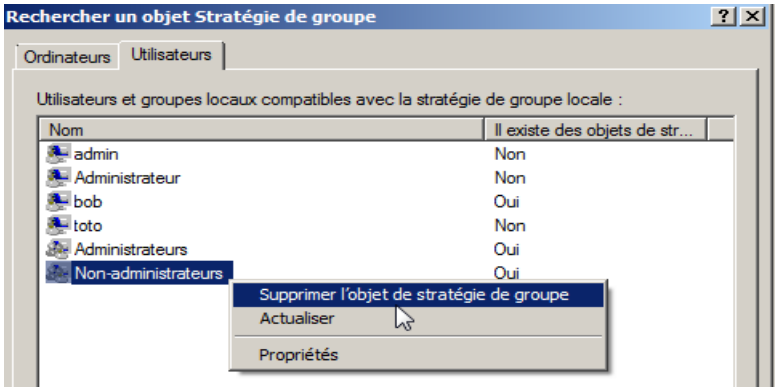
Les MLGPO sont stockées dans **System32\GroupPolicy** et **\GroupPolicyUsers**



on peut aussi plus facilement dans la mmc editeur de strategies vérifier



le clic droit souris permet de les Supprimer

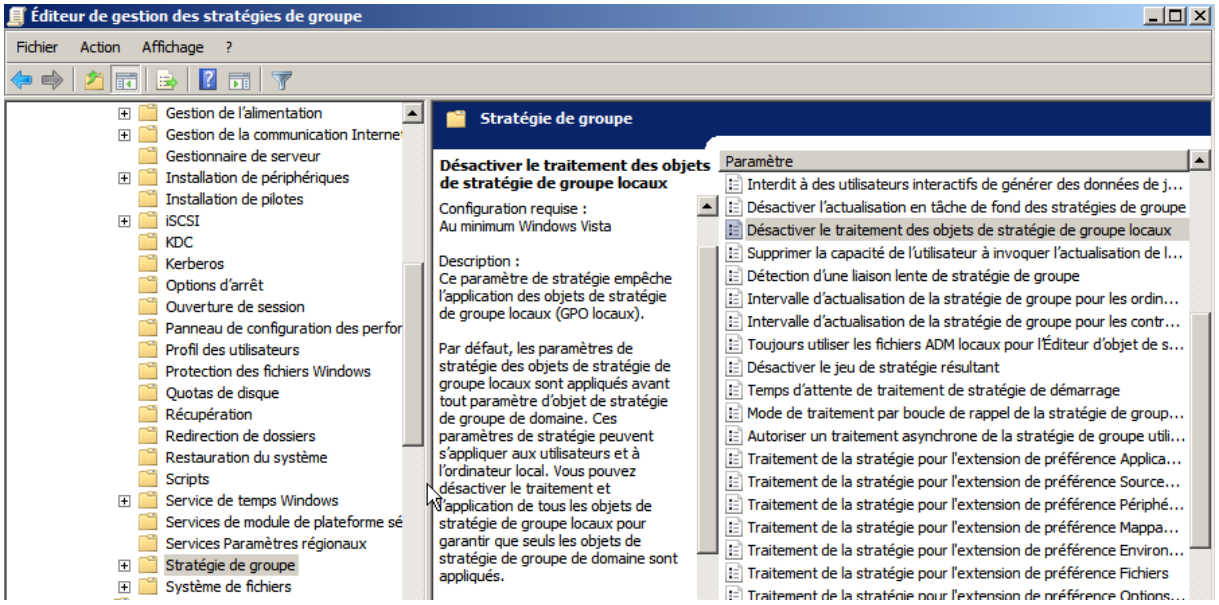


Désactivation des MLGPO

Dans le cas d'un domaine, on peut désactiver les stratégies locales… qu'elles soient locales simples ou LGPO…

Dans **Ordinateur \ modèles d'administration \ système \stratégies de groupe**\

Desactiver le traitement des objets de stratégie de groupe locaux



NB: évidemment cela n'a de sens que pour les machines en Domaine…

WINDOWS 10 - SCT SECURITY COMPLIANCE TOOLKIT LGPO

Windows 10 SCT Security Compliance Toolkit - utilitaire LGPO.exe :

Microsoft a publié pour Windows 10 un **Security Compliance Toolkit** (**SCT**) remplaçant le **Security Compliance Manager** (**SCM**) de windows 7.

L'outil en ligne de commande appelé **LGPO** vient donc remplacer le script **LocalGPO.swf** fourni auparavant pour **Seven** dans **Security Compliance Manager** (**SCM**). Ce nouvel utilitaire permet simplement pour nous de pouvoir réaliser un :

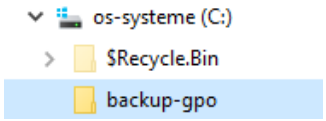
- Import de paramètres dans les stratégies locales à partir de GPOs sauvegardées ou de fichiers individuels (Registry.pol, modèle de sécurité, fichiers CSV, etc.)
- Export de stratégies locales vers des sauvegardes GPO

Cette version supporte les **Multiple Local Group Policy Objects** (**MLGPO**) .

On peut copier l'utilitaire **LGPO.exe** dans le dossier **c:\windows\system32** pour plus de confort

Export – import avec LGPO.exe :

Supposons que l'on souhaite exporter notre stratégie locale dans un dossier spécifique, par exemple ***c:\backup-gpo***



On peut exporter notre GPO locale avec la commande suivante :

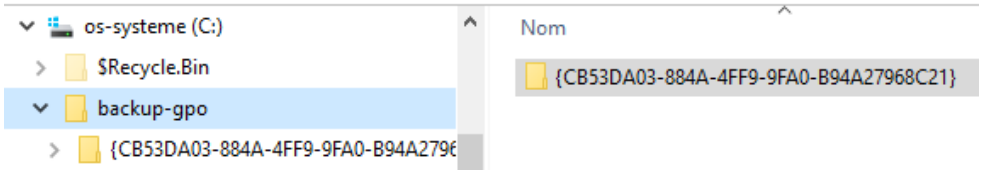
LGPO.exe /b C:\GPO

Donc dans l'exemple

```
C:\backup-gpo>lgpo /b c:\backup-gpo
LGPO.exe v2.2 - Local Group Policy Object utility

Creating LGPO backup in "c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}"
```

Ce qui crée une GPO dans le dossier de destination



On peut importer les paramètres GPO avec la commande suivante :

LGPO.exe /g c:\GPO\{GPO GUID}

LGPO.exe /g: c:\GPO sans spécifier, prend tous le dossier

Toutes les stratégies seront restaurées,

```
Audit policy directory exists
Copied c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.cs
v
to C:\Windows\system32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv
Clearing existing audit policy
Apply Audit policy from c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GPO\Machine\microsoft\windows
nt\Audit\audit.csv
Apply security template: c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GPO\Machine\microsoft\windows
 nt\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GPO\Machine
\registry.pol
Import User settings from registry.pol: c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GPO\User\regis
try.pol
```

Il ne faut pas oublier de redémarrer le poste !

WINDOWS 7 – SCM SECURITY COMPLIANCE MANAGER - LPT

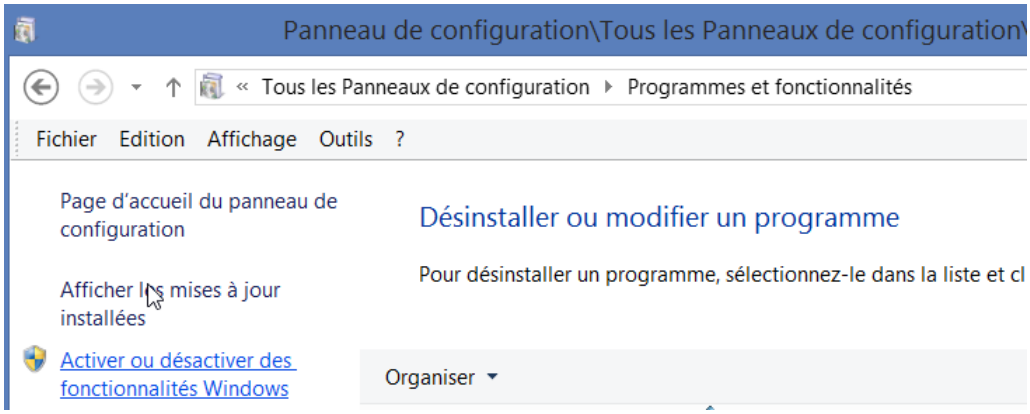
Windows 7 - SCM Security Compliance Manager - LPT:

Il faut télécharger les **LPT** au sein d'un package technet plus complet nommé **Security_Compliance_Manager_Setup**

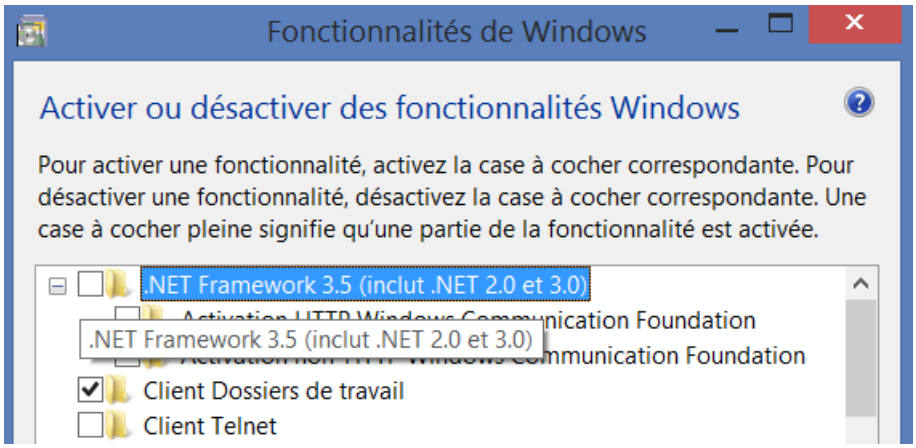
Pour installer ce package, Microsoft .net framewort 3.5 est requis

N.B : le .NET Framework 3.5 n'est pas automatiquement installé avec Windows 8 ou Windows 8.1. Vous pouvez procéder de plusieurs façons mais toutes requièrent une connexion Internet et désactivation pare-feu

- Installer.NET Framework 3.5 en stand alone
- Installer - exécuter une application qui requiert le .NET Framework 3.5 (c'est-à-dire, en installant le .NET Framework 3.5 à la demande)
- Activer le .NET Framework 3.5 dans le **Panneau de configuration**.



puis



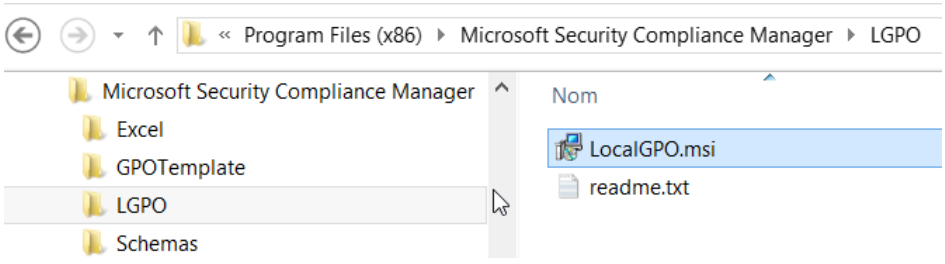
Extraire Local Policy Tool depuis SCM:

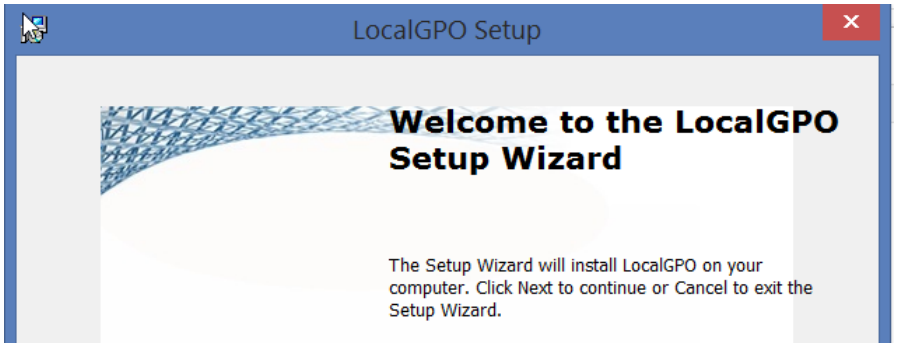
Après avoir installer **SCM Security_Compliance_Manager_Setup**

Qui se stockeront dans

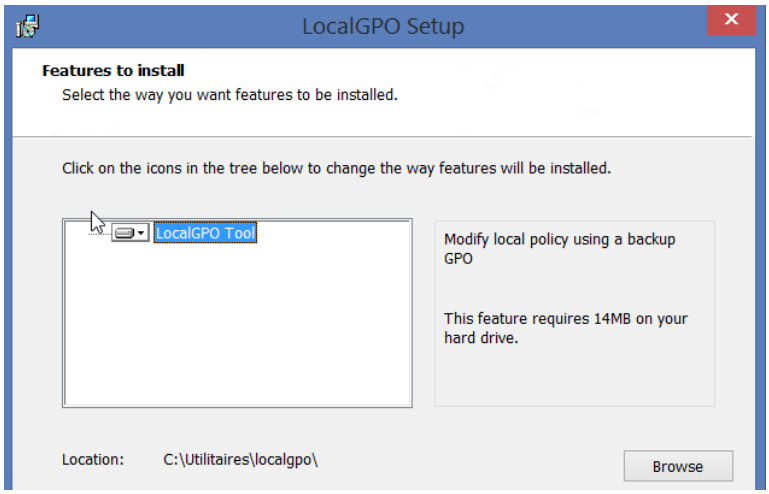
Les fichiers nécessaires à LGPO sont stockés dans **C:\Program Files (x86)\Microsoft Security Compliance Manager\LGPO**.

Pour installer l'outil **LGPO** il suffit d'installer le fichier **LocalGPO.msi**



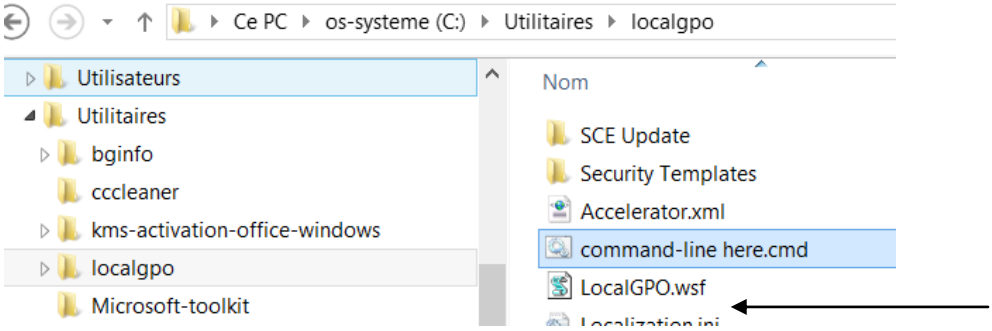


Onchoisit un dossier d'installation



Lancer le script en ligne de commande LocalGPO.wsf:

Pour executer l'outil il faut lancer une invite de commande en Administrateur depuis le dossier ou l'outil est installé



N.B: pour lancer cet outils sur des machines Windows 8 il fait modifier dans le fichier **LocalGPO.wsf** la detection d'OS, et ajouter (ou remplacer) la version 6.1 par respectivement 6.2 (windows 8) et 6.3 (windows 8.1)

Exporter une LGPO Seven avec LPT:

La syntaxe pourrait être

cscript LocalGPO.wsf /path:c:\gpbackups /export

avec

- **/path** l'option pour indiquer un chemin
- **c:\gpbackups** un chemin d'accès au dossier de stockage des GPO
- **/export** l'option disant que l'on veut effectuer une sauvegarde

Par exemple

```
C:\Utilitaires\localgpo>cscript LocalGPO.wsf /Path:C:\utilitaires\stock-gpo /export
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. Tous droits réservés.

Exporting Local Policy... this process can take a few moments.

Local Policy Exported to C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}
```

Importer une LGPO Seven avec LPT:

La syntaxe pourrait être

cscript LocalGPO.wsf /path:C:\gpbackups\{42ADD8FE-EDF6-479B-92C6-557343D8D091}

avec

- **/path** l'option pour indiquer un chemin
- **c:\gpbackups** un chemin d'accès au dossier de stockage des GPO
- **\{ GUUID }** le gguid de la GPO que l'on veut récupérer

Par exemple

```
C:\Utilitaires\localgpo>cscript LocalGPO.wsf /Path:C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. Tous droits réservés.


Modifying Local Policy... this process can take a few moments.

Applied valid INF from C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}
Applied valid Machine POL from C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}
Applied valid User POL from C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}
Applied valid Audit Policy CSV from C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}

Local Policy Modified!


Please restart the computer to refresh the Local Policy
```

Restaurer une LGPO par défaut avec LPT:

La syntaxe pourrait être

cscript LocalGPO.wsf /restore

```
C:\Utilitaires\localgpo>cscript LocalGPO.wsf /restore
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. Tous droits réservés.


Modifying Local Policy... this process can take a few moments.

Restoring Security Settings...
```

STRATEGIES DE DOMAINE

Stratégies de Domaine :

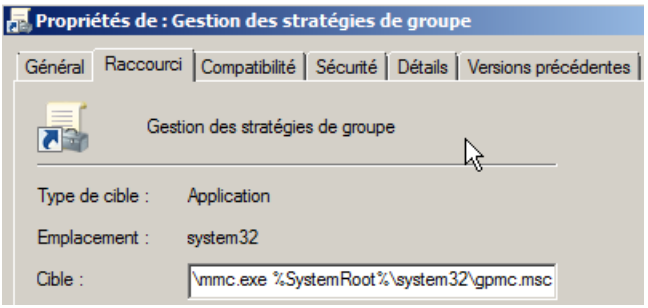
Lorsque l'on configure une stratégie de domaine, cela signifie que l'on souhaite que cette stratégie s'applique potentiellement à toutes les machines de notre domaine.

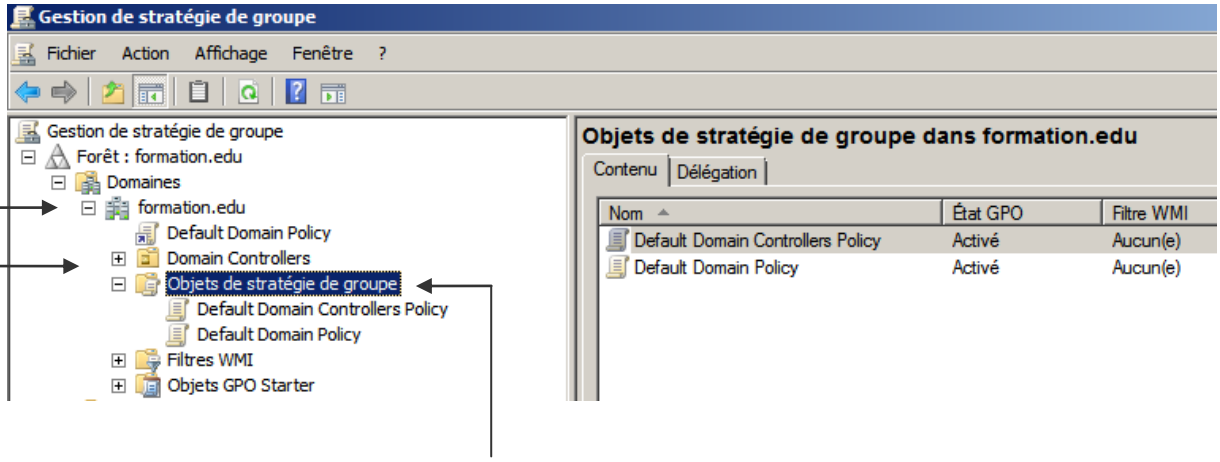
- les **contrôleurs de domaine** en font partie

Encore faut-il que cette stratégie soit définie au bon endroit, et soit transmise sur le domaine….

Gestion des stratégies de groupe - gpmc.msc:

Pour donner une stratégie de domaine, il faut lancer la **Gestion des stratégies de groupe** dans les **Outils d'Administration**

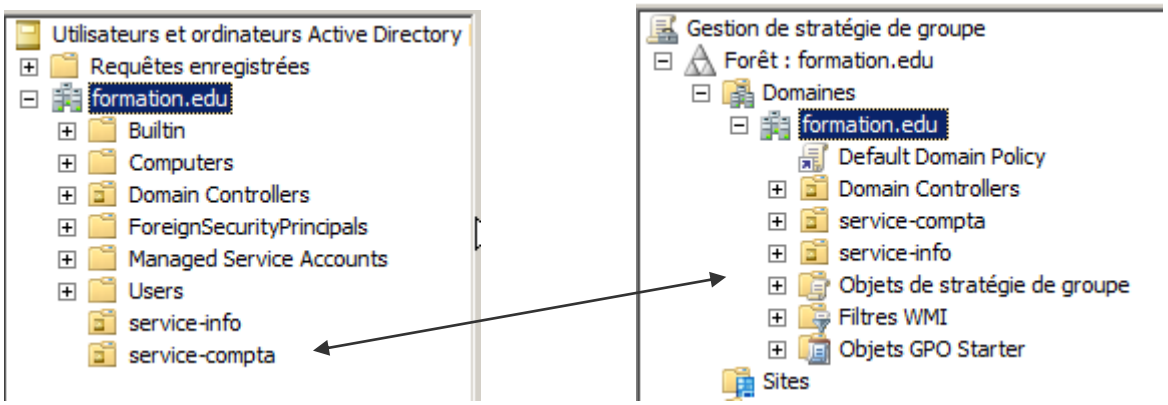




Les **Objets de stratégie de groupe** représentent l'endroit **logique** de stockage de toutes les stratégies de groupe,

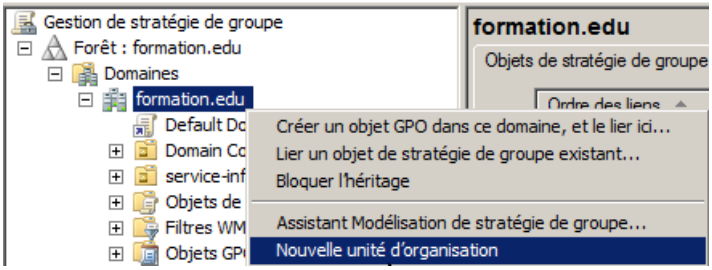
Seule l'UO prédéfinie **Domain Controllers** et le **Domaine** Entier apparaissent par défaut

De manière générale, Si une **UO** à été Crée dans **Utilisateurs et Ordinateurs Active Directory**, elle apparaîtra dans la **Gestions des stratégies de groupe**



Même si pour l'instant on n'en voit pas encore bien l'utilité, le principe est que par **Utilisateur et Ordinateurs Active Directory**, on gère les **UO**... mais pas les **Stratégie**s...

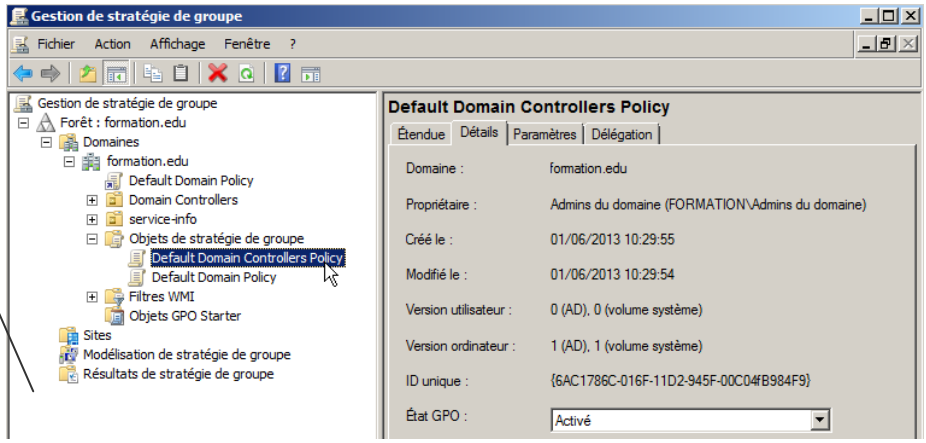
par **Gestion des stratégies de groupe**, on gère évidemment les **stratégies de groupe**, mais on peut aussi créer (et principalement uniquement créer) de nouvelles **UO**...via un clic droit.



Plaçons nous sur la stratégie **Default Domain Controller**

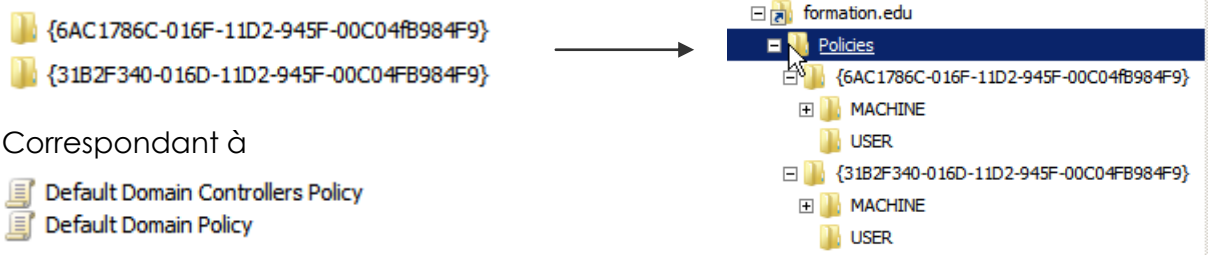
onglet **Détails**,

on voit alors le GUID de la stratégie



Correspondant **physiquement** au dossier **%Windir%\sysvol\sysvol***domaine***\Policies**

Dans lequel on y trouvera nos stratégies



Correspondant à

Default Domain Controllers Policy
Default Domain Policy

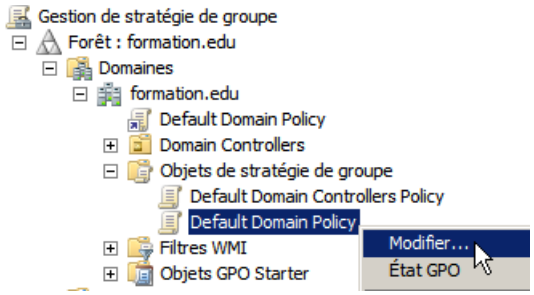
Il existe 2 GUID connus :

Default Domain Policy : **{31B2F340-016D-11D2-945F-00C04FB984F9}**.

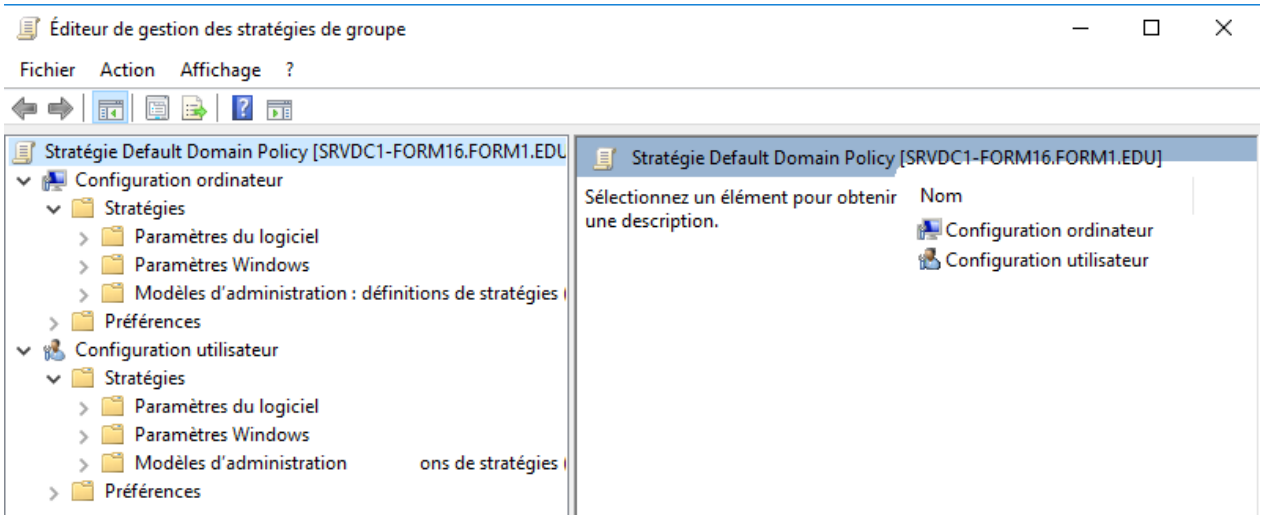
Default Domain Controllers Policy: **{6AC1786C-016F-11D2-945F-00C04fB984F9}**.

Modifier la Stratégie de Domaine :

via la **Gestion des stratégies de groupe** dans les **Outils d'Administration**



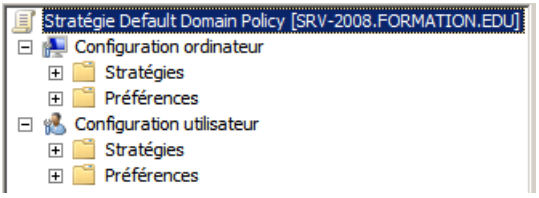
On demande **Modifier…** la **Default Domain policy**



Stratégie Ordinateur, Utilisateur:

A ce niveau là, les options indiquées dans la section **Configuration ordinateur** s'appliquent à tous les postes du Domaine… Y COMPRIS LES CD !

A ce niveau là, les options indiquées dans la section **Configuration utilisateur** s'appliquent à tous les users du Domaine… Y COMPRIS L'ADMIN DE DOMAINE !



Ce qui veut dire que la portée de la **Default Domain Policy** c'est TOUT le domaine !

Propagation Stratégies de Domaine :

Les stratégies sous 2003-XP étaient gérées par le service **Netlogon.** Depuis 2008 Seven elles sont gérées par un service **NlaSVC/** (connaissance des emplacements réseau), plus réactif et gérable (par stratégie !). Depuis 2008R2 elles sont gérées par DFRS pour améliorer encore la réplication.

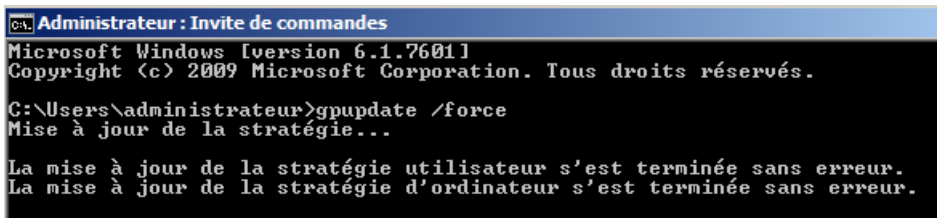
Normalement une stratégie se propage à **chaque démarrage de poste**, puis **toutes les 5 à 60 voire 90 minutes + (delta de +/-30mn)**

Il est bien sûr toujours possible de forcer le rafraîchissement mais en partant du principe que l'on tire la propagation de la stratégie vers soi (donc depuis un client on va chercher sur le serveur) mais on ne peut pas pousser la propagation (depuis le serveur vers les clients)

Pour forcer la propagation d'une stratégie, on effectue une commande depuis le client sur lequel on veut effectuer la propagation (on tire la stratégie vers soi !)

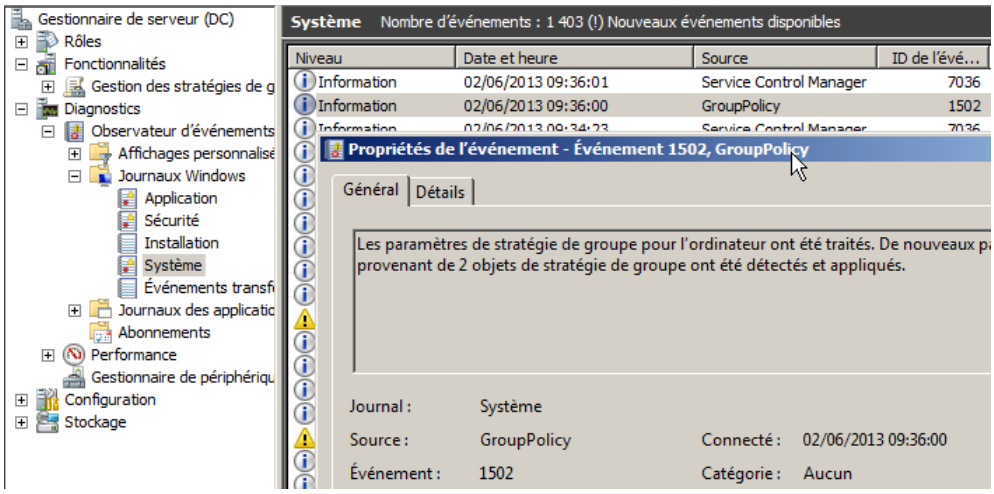
Depuis **Windows Seven - XP**

Gpupdate /force

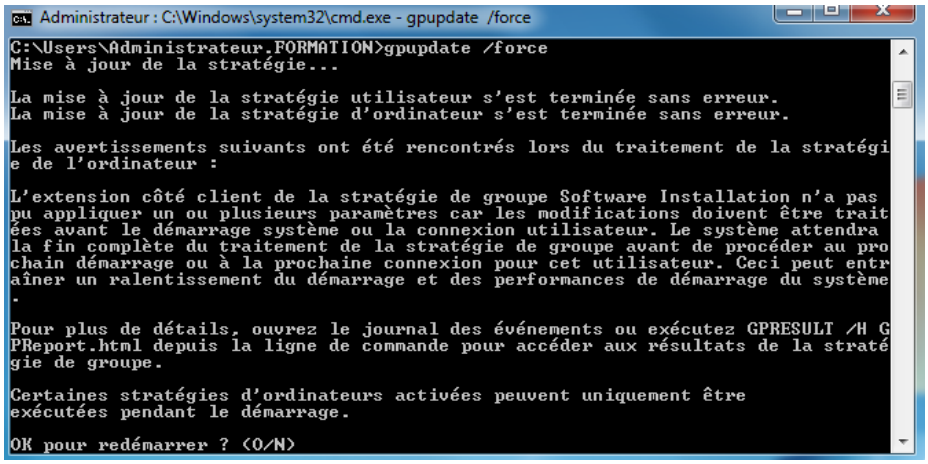


Par exemple

Effectivement, dans le journal on peut observer

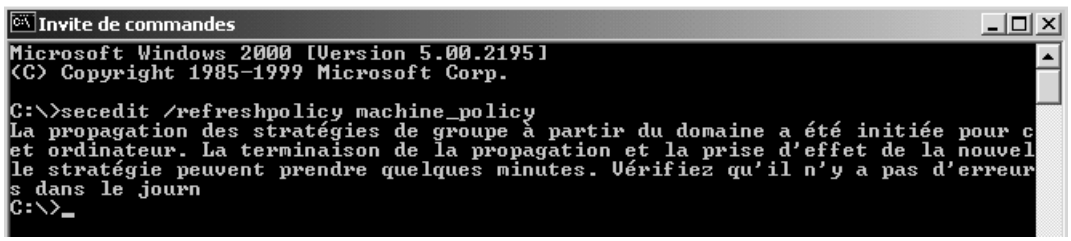


Sous 7 (rappel) un **gpupdate** peut nous suggérer 1 re-démarrage



Pour mémoire sous **Windows 2000** :

Secedit /refreshpolicy machine_policy



Et / ou Secedit /refreshpolicy user_policy

L'utilitaire en ligne Gpupdate (Depuis Seven XP – 2008 2003)

Cette commande force la propagation des stratégies. Normalement une stratégie se propage à **chaque démarrage de poste**, puis **toutes les 5 à 60 voire 90 minutes**, et lorsque les paramètres de sécurité locale sont modifiés…

Gpupdate

Permet d'actualiser les paramètres de stratégie de groupe locaux et Active Directory, y compris les paramètres de sécurité. Cette commande remplace l'option désormais caduque **/refreshpolicy** de la commande **secedit**.

Syntaxe

gpupdate [**/target:**{**ordinateur**|**utilisateur**}] [**/force**] [**/wait:***valeur*] [**/logoff**] [**/boot**]

/target:{**ordinateur**|**utilisateur**}
Permet de traiter uniquement les paramètres de l'*ordinateur* ou les paramètres de l'*utilisateur* courant. Par défaut, sont traités à la fois les paramètres de l'ordinateur et de l'utilisateur.

/force
Permet à la fonction d'actualisation d'ignorer toutes les optimisations et de réappliquer tous les paramètres.

/logoff
Permet de mettre fin à la session une fois l'actualisation terminée. Ce paramètre est obligatoire pour les extensions de stratégies de groupe côté client qui ne sont pas exécutées dans le cadre d'un cycle d'actualisation en arrière-plan mais qui sont appliquées lorsque l'utilisateur ouvre une session, telles que les stratégies d'installation de logiciel et de redirection de dossier traitées au niveau de l'utilisateur. Cette option est sans effet si, parmi les extensions appelées, aucune ne demande à l'utilisateur de mettre fin à la session ouverte.

/boot
Permet de redémarrer l'ordinateur une fois l'actualisation terminée. Ce paramètre est obligatoire pour les extensions de stratégies de groupe côté client qui ne sont pas exécutées dans le cadre d'un cycle d'actualisation en arrière-plan mais qui sont appliquées au démarrage de l'ordinateur, telles que les stratégies d'installation de logiciel traitées au niveau de l'ordinateur. Cette option est sans effet si, parmi les extensions appelées, aucune n'exige le redémarrage de l'ordinateur.

L'utilitaire en ligne Secedit (2000)

Cette commande force la propagation des stratégies. Normalement une stratégie se propage à **chaque démarrage de poste**, puis **toutes les 5 à 60 voire 90 minutes**, et lorsque les paramètres de sécurité locale sont modifiés…

Actualiser les paramètres de sécurité

secedit /refreshpolicy

Cette commande actualise la sécurité du système en appliquant à nouveau les paramètres de sécurité à l'objet Stratégie de groupe.

Syntaxe

secedit /refreshpolicy {**stratégie_ordinateur** | **stratégie_utilisateur**} [**/enforce**]

Parameters

stratégie_ordinateur
Actualise les paramètres de sécurité pour l'ordinateur local. ←

N.B: erreur doc **machine_policy**

stratégie_utilisateur
Actualise les paramètres de sécurité pour le compte d'utilisateur local qui conduit actuellement une session sur l'ordinateur. ←

N.B: erreur doc **user_policy**

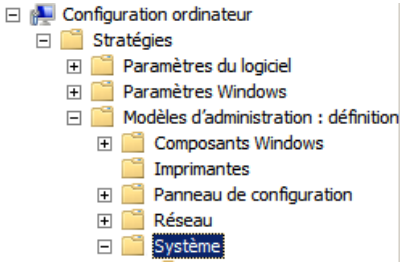
/enforce
Actualise les paramètres de sécurité, même si aucune modification n'a été apportée aux paramètres de l'objet Stratégie de groupe.

Gestion Propagation des Stratégies de Domaine :

Lorsque un client Windows contacte son DC pour récupérer une stratégie, si un problème se passe, il ne le re-contactera pas avant le prochaine cycle normal… depuis 2008 et Seven; le service **NlaSVC** interroge et reprends contact avec le DC dès la remise en disponibilité de celui-ci.

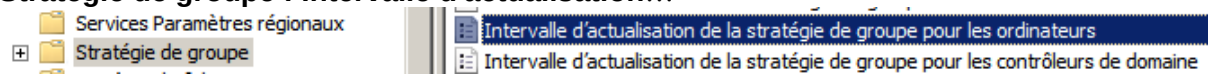
De plus 2 nouvelles stratégies désormais existent permettant d'affiner la vitesse de propagation des GPO qui est par défaut on le rappelle **chaque démarrage de poste**, puis **toutes les 5 à 60 voire 90 minutes + (delta de +/- 30mn)**

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

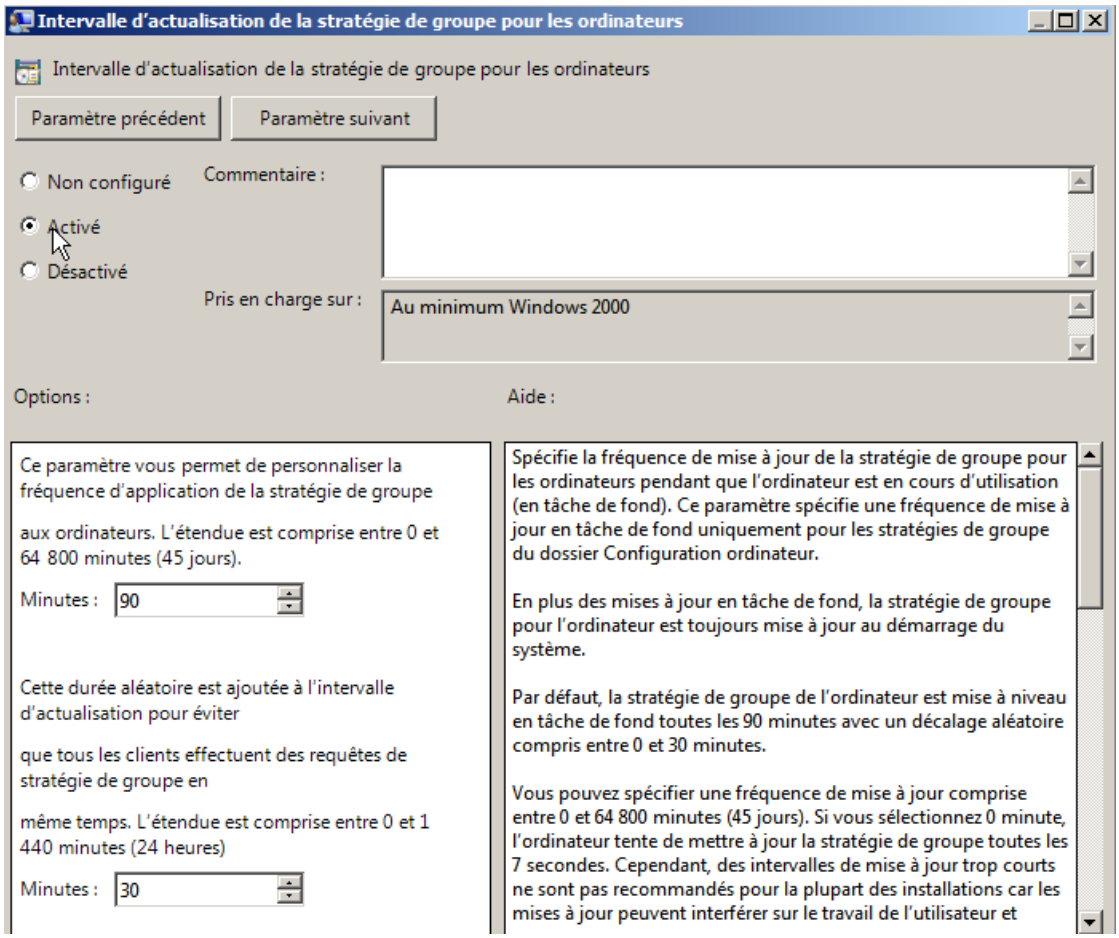


on trouve

Stratégie de groupe : Intervalle d'actualisation…



Donnant

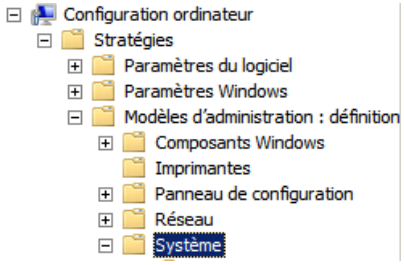


N.B: et bien sur se réglage se trouve également dans **Configuration Utilisateur / Stratégies / Modèles d'administration / Système**

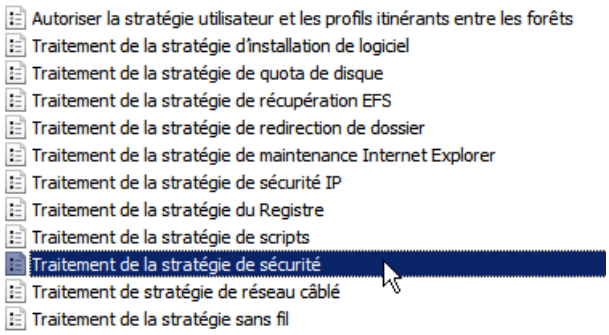
Mais il faut bien voir qu'en plus, certaines stratégies ne sont ré-appliquées localement que si elles ont été modifiées… (afin d'optimiser le temps de réaction des clients)

Cela peut également se modifier, toujours dans la même stratégie globale

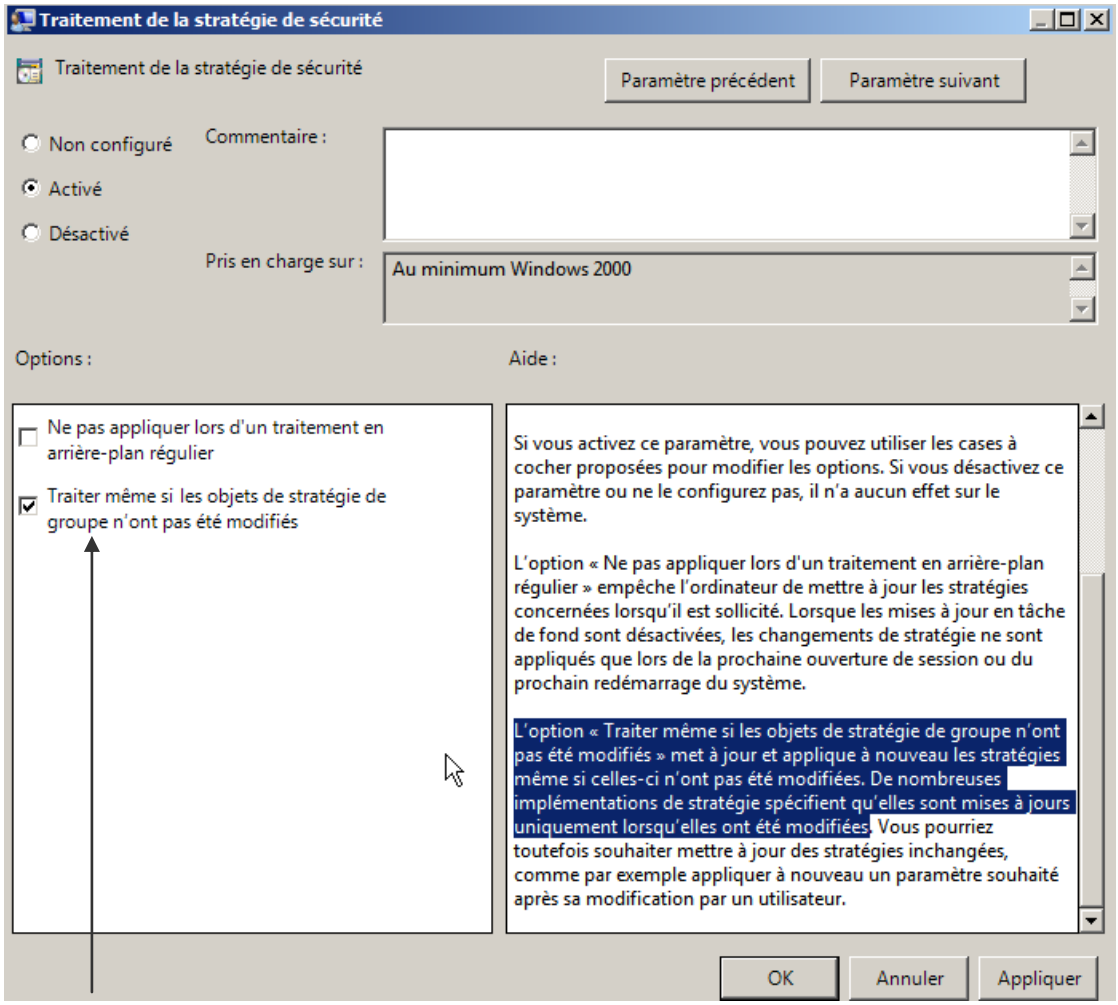
Ordinateur / Stratégies / Modèles d'administration / Système



Mais là on trouve tout un paquet de stratégies :



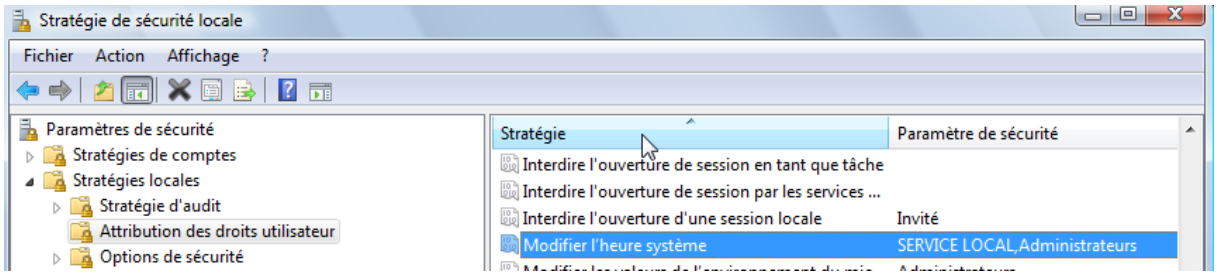
Et lorsque l'on active une stratégie pour un groupe, par exemple ici "Sécurité"



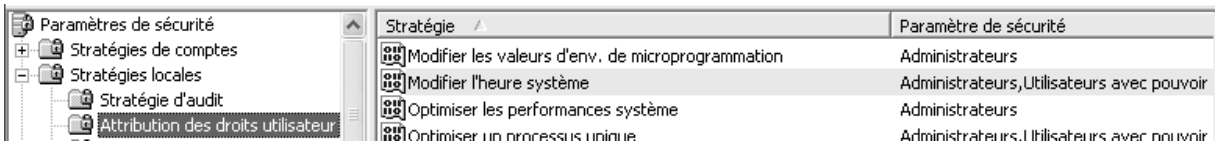
L'option « **Traiter même si les objets de stratégie de groupe n'ont pas été modifiés** » met à jour et applique à nouveau les stratégies même si celles-ci n'ont pas été modifiées.

Exemple : Attribution droits Utilisateur Modifier l'heure système :

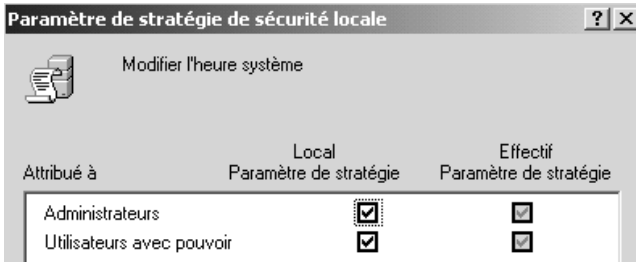
Depuis les clients Windows 7du domaine, la **stratégie locale** ne montre qu'une seule colonne, (le **service local** remplace les **utilisateurs avec pouvoir**…)



Sur un client XP du domaine, la **stratégie locale** montre une seule colonne

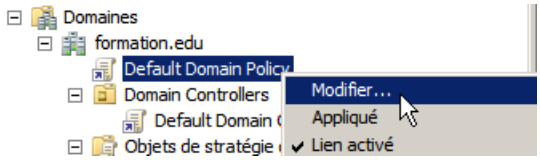


Sur un client 2000 du domaine, voila l'aspect de la **stratégie locale** concernant qui peut mettre à l'heure la machine.... (on voyait mieux quel niveau disait… quoi…)

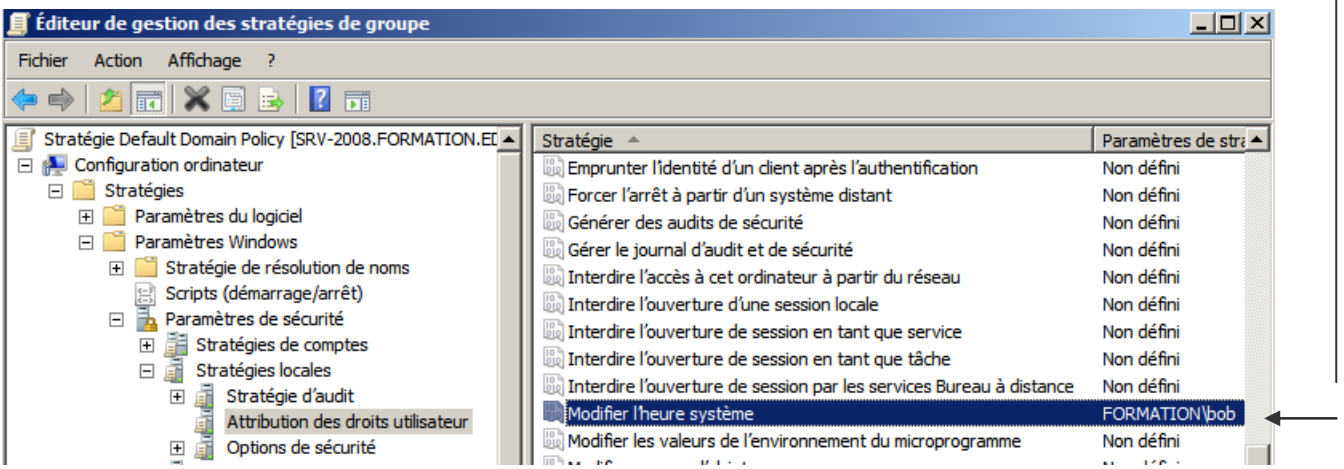


Sur le Contrôleur de Domaine, on définit une **Stratégie de sécurité du domaine** pour **Modifier l'heure système** (qui par défaut est non activée)

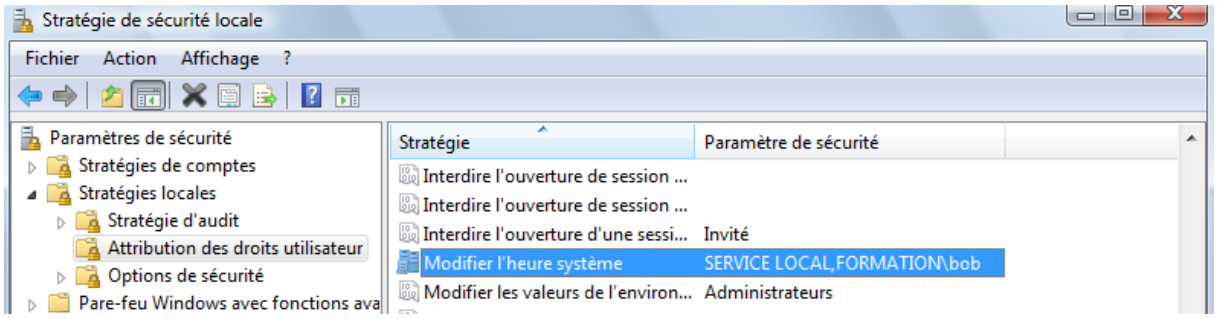
On modifie donc la **Default Domain Policy**



Pour ajouter un utilisateur "bob" ayant ce privilège de changer l'heure système…

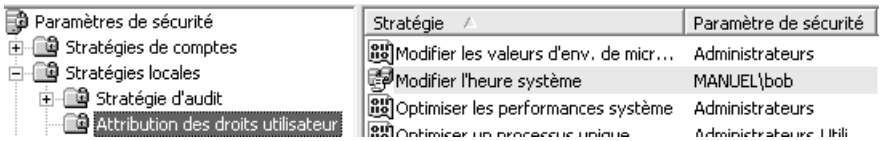


Sur le client Windows du domaine, la **stratégie locale** ne montre qu'une seule colonne, (le service local est maintenu !) et bob est ajouté…

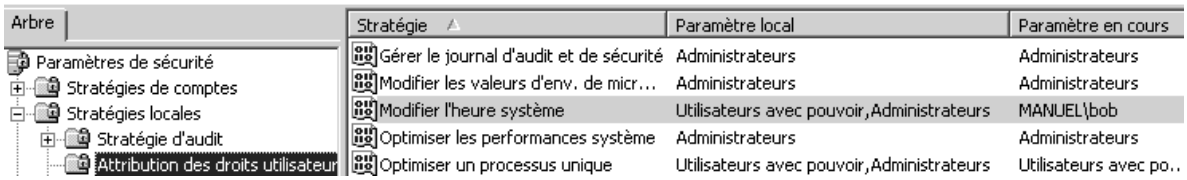


Lorsque la stratégie de domaine s'est propagée, la visualisation de la **stratégie locale** sera marquée d'une icône indiquant qu'elle vient du Domaine,  ou localement. 

Sous XP il n'y a plus que bob

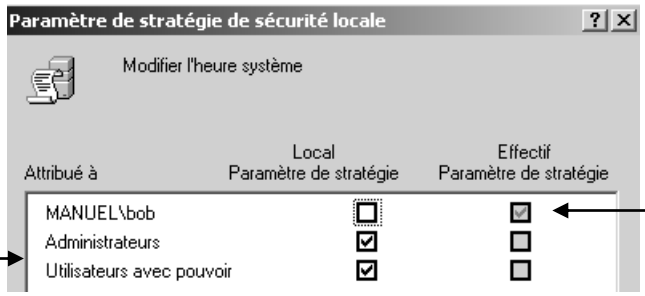


Sur le client 2000 du domaine on a les deux informations



Avec bob uniquement

Pas de changement localement



Mais ici on a récupéré la stratégie de domaine

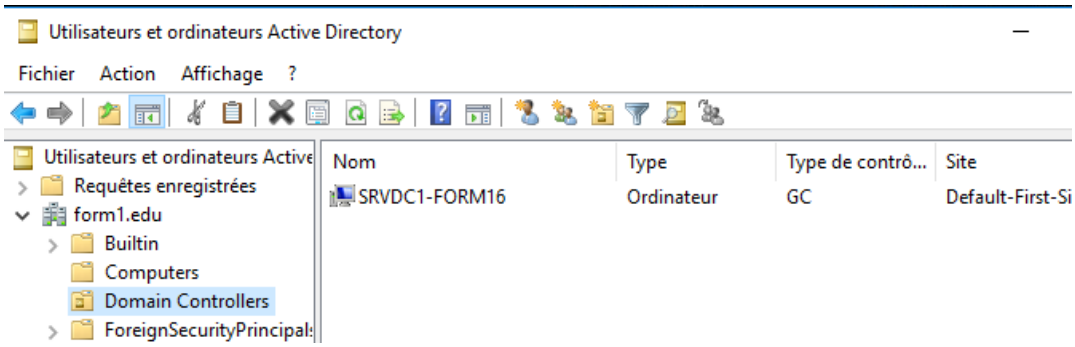
Et sur le Contrôleur de Domaine ???

STRATEGIES CONTROLEUR DOMAINE

Stratégies de Contrôleur de Domaine :

Une **Stratégie de Domaine** s'applique sur notre contrôleur de Domaine, mais elle peut être écrasée par une **Stratégie de Contrôleur de Domaine**.

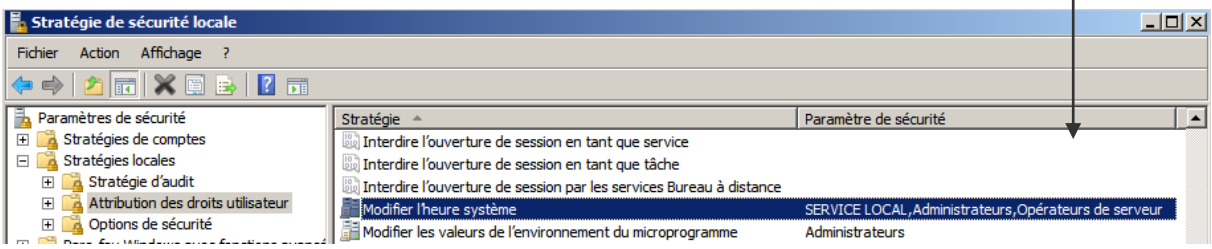
Lorsque l'on configure une stratégie de **Contrôleur de domaine**, cela signifie que l'on souhaite que cette stratégie s'applique à toutes les machines ayant ce rôle, et uniquement celles-ci. Cela peut représenter uniquement notre serveur CD, mais cela peut aussi en représenter plusieurs… (visibles dans l'UO **Domain Controllers**)



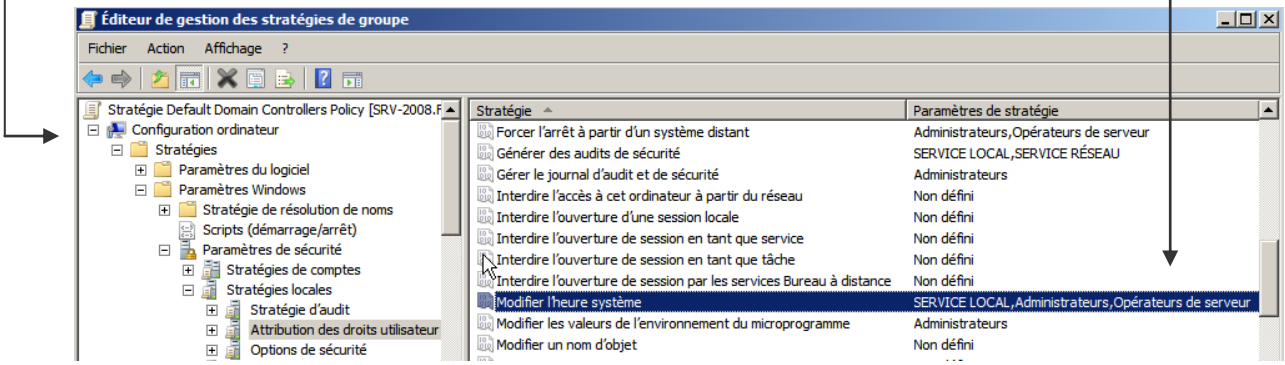
La stratégie de **Contrôleur de Domaine** existe, et elle possède plusieurs réglages actifs, qui risquent de s'opposer à ceux de la **stratégie de Domaine** !

Regardons l'exemple de l'attribution du droit "modifier l'"heure"…

- On sait que par défaut la stratégie de domaine ne dit rien a ce propos, (et nous on a peut être spécifié "bob" dans le chapitre précédant…)
- Si on vérifie sur notre Contrôleur de Domaine les valeurs via les stratégies locales voilà ce que l'on obtient…
  ce n'est pas la stratégie de domaine (par défaut ou modifiée…)

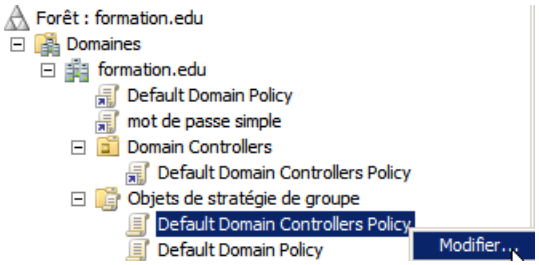


En fait la **Default Domain Controller policy** est active…



Modifier la Stratégie des Contrôleur de Domaine :

via la **Gestion des stratégies de groupe** dans les **Outils d'Administration**



On demande **Modifier…** la **Default Domain Controllers policy**

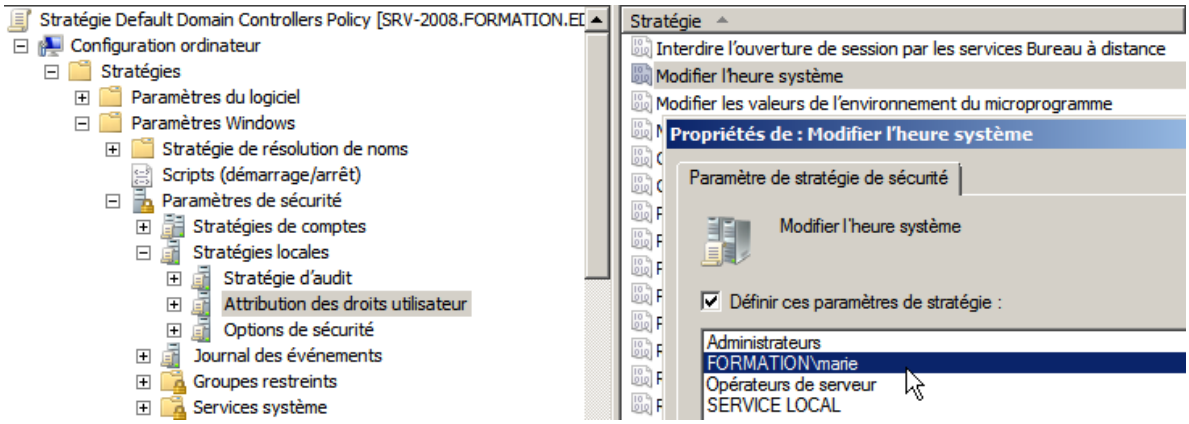
Exemple : Attribution droits Utilisateur Modifier l'heure DC :

Par exemple on souhaite que l'utilisateur "marie" puisse mettre à l'heure les contrôleurs de Domaine, mais sans pour autant être opérateur de serveur, ou appartenir à d'autres groupes pré-définis. Il faut donc lui donner les deux droits utilisateurs suivants

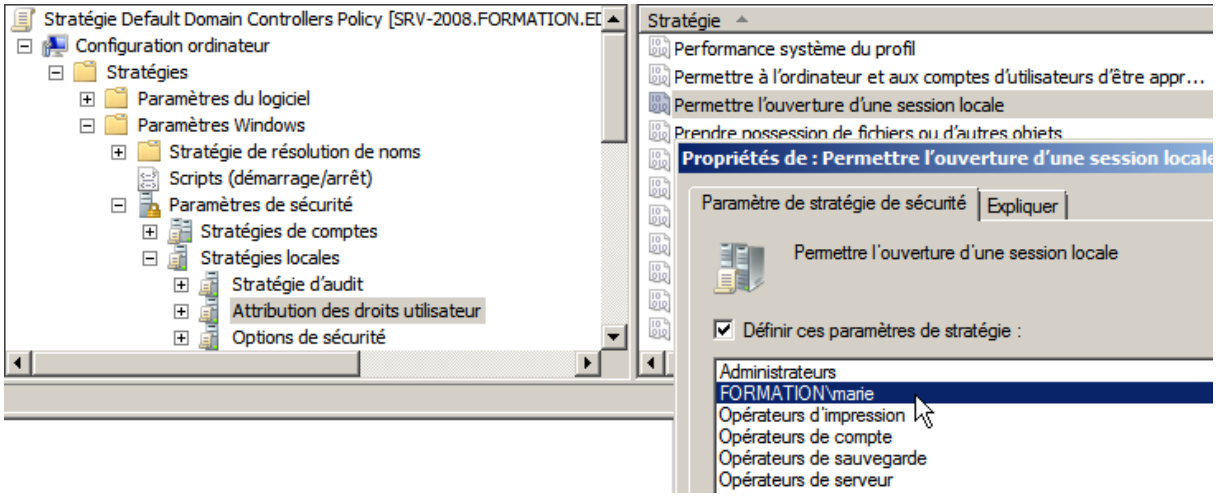
- **Modifier l'heure système**
- **Permettre l'ouverture d'une session locale**

Sur le (un) Contrôleur de Domaine, on modifie la **Stratégie de sécurité du contrôleur de domaine** : **Default Domain Controllers policy**

en spécifiant que l'utilisateur **marie** a ce droit de **Modifier l'heure système**

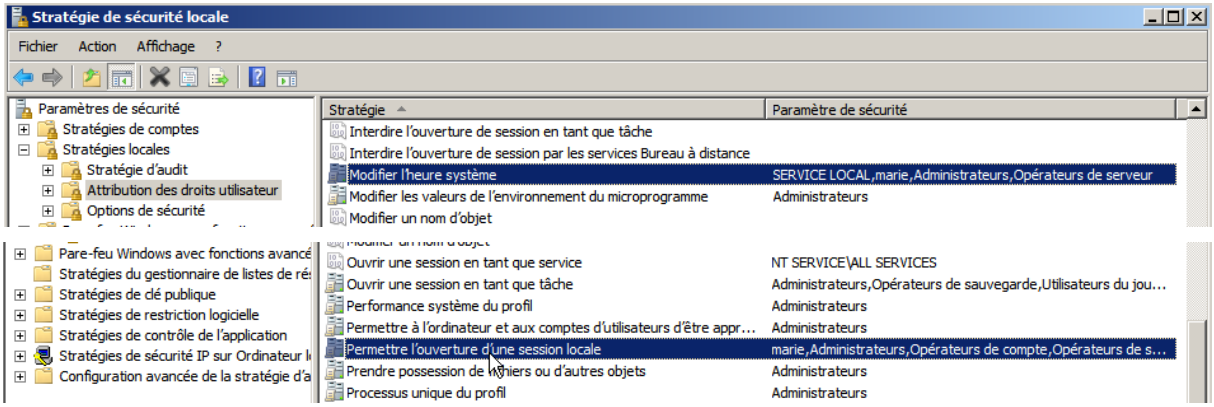


Et que l'utilisateur **marie** dispose aussi du droit d'**ouvrir une session localement**



Vérification :

Sur le serveur les stratégies locales montrent bien

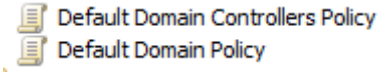


N.B : si on a plusieurs CD penser à propager la stratégie sur tous les CD…

BEST PRACTICE GPO DOMAINE ET CD

Ne pas modifier les GPO par défaut:

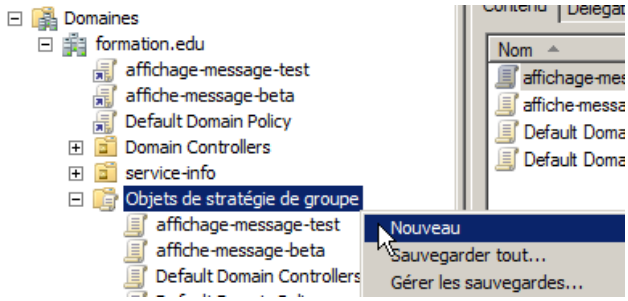
Elles représentent la base sur laquelle il est bon de pouvoir revenir



il faut les sauvegarder plus ou moins régulièrement, car certaines installations peuvent les modifier... et ne pas les modifier

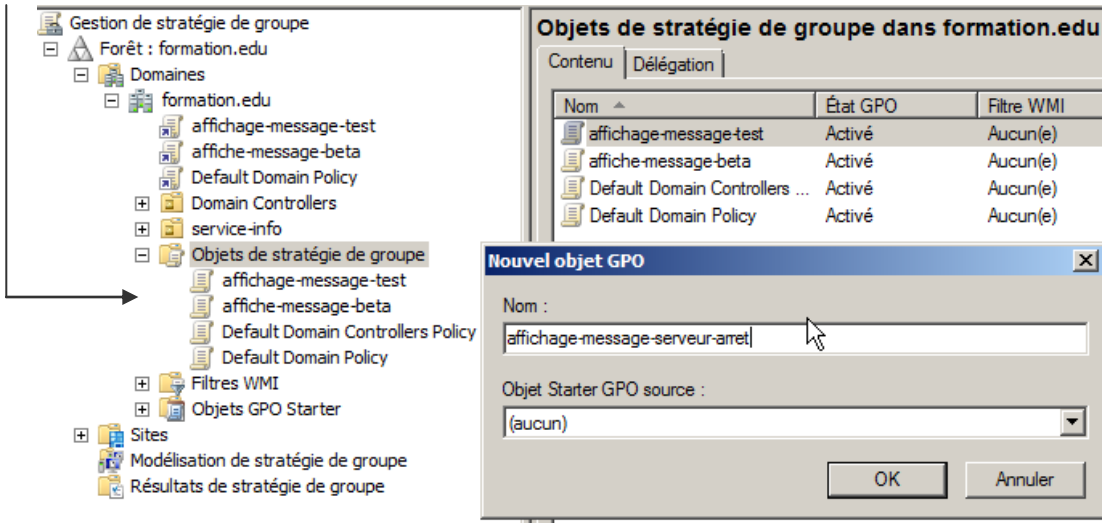
1 GPO = 1 action :

il faut se créer dans notre stockage **Objets de stratégies** de groupe autant de GPO que d'actions diverses que l'on souhaite :



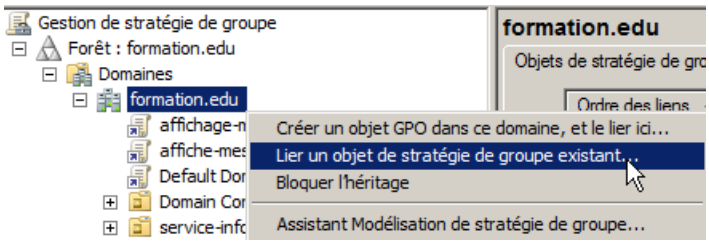
en leur donnant un titre explicite

on se crée une "bibliothèque...

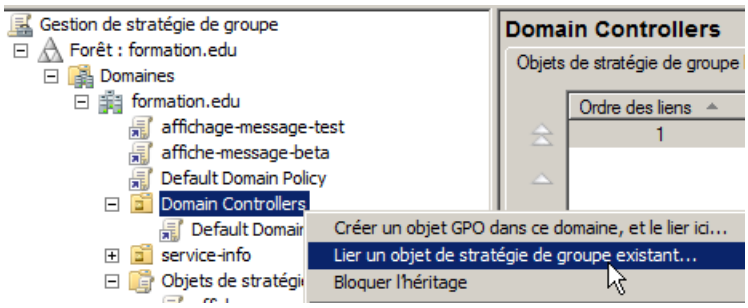


liaison - portée :

Et on lie la **GPO** au niveau souhaité, ici pour le **Domaine** complet



Pour le-les Contrôleur de Domaine



Propagation et Test :

Une fois la **GPO** propagée...

- il faut effectuer un **gpupdate / force** avec un compte de domaine
- la **GPO** ne doit pas être en "modification" sur le serveur

on la teste

- cela peut nécessiter re-ouverture de session ou re-démarrage du poste

en cas de problème on pense à :

Des problèmes de « propagation »

- vérification **DNS**
- outils **gpresult**

Des problèmes de « sécurité »

- vérification **Droits**

Des problèmes de « logique » dans la hiérarchie des GPO

- écrasement **GPO** par une autre de niveau hiérarchique supérieur (pour l'instant une GPO local par une GPO de domaine, et/ou une **GPO de domaine** par une **GPO de Contrôleur de Domaine**)
- contradiction entre 2 GPO au même niveau, si 2 GPO modifient la même clé, la même notion, l'effet n'est pas "cumulatif", mais une seule des 2 GPO sera effective, la dernière appliquée. (pour l'instant on évite de donner 2 GPO de même but au même niveau...)

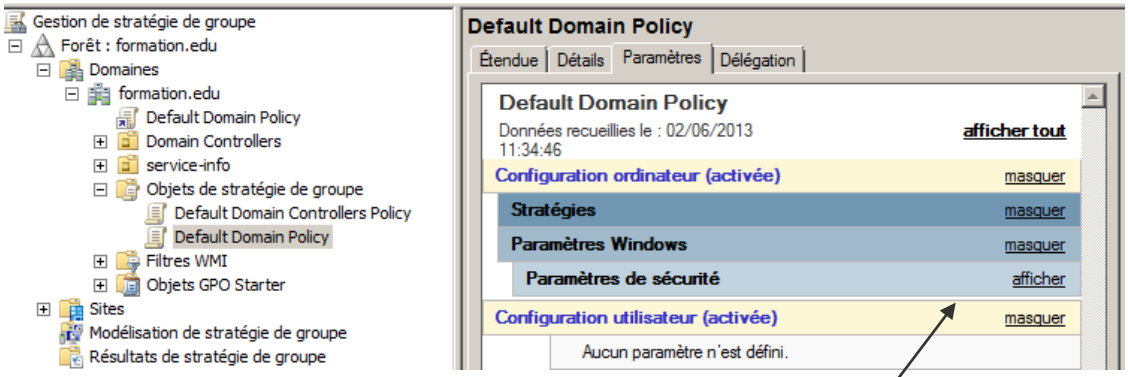
un chapitre complet **liaisons – priorité – heritage** traitera plus loin dans ce support les soucis de type « logique)

GESTION ET SAUVEGARDE DES GPO

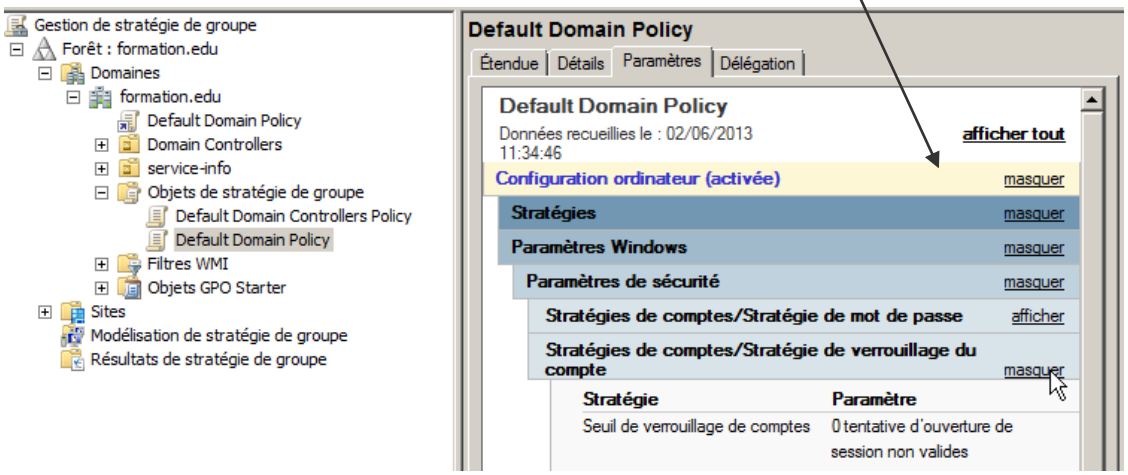
"Visualisation" en direct de la stratégie :

Il est possible d'avoir une idée (documentation) de ce que fait une stratégie.

on se place sur la stratégie, par exemple la **Default Domain Policy**, et on demande **Paramètres**



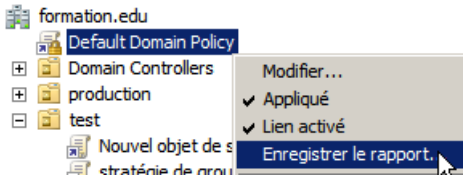
un jeu d'affichage assez intuitif est disponible



fichier de "Visualisation" de la stratégie :

On peut garder ces informations dans un fichier, pour les consulter ensuite a tout moment avec un simple navigateur (IE) acceptant les ActiveX...

Cela se demande, une fois placés sur la **GPO** via le bouton droit : **Enregistrer le rapport…**

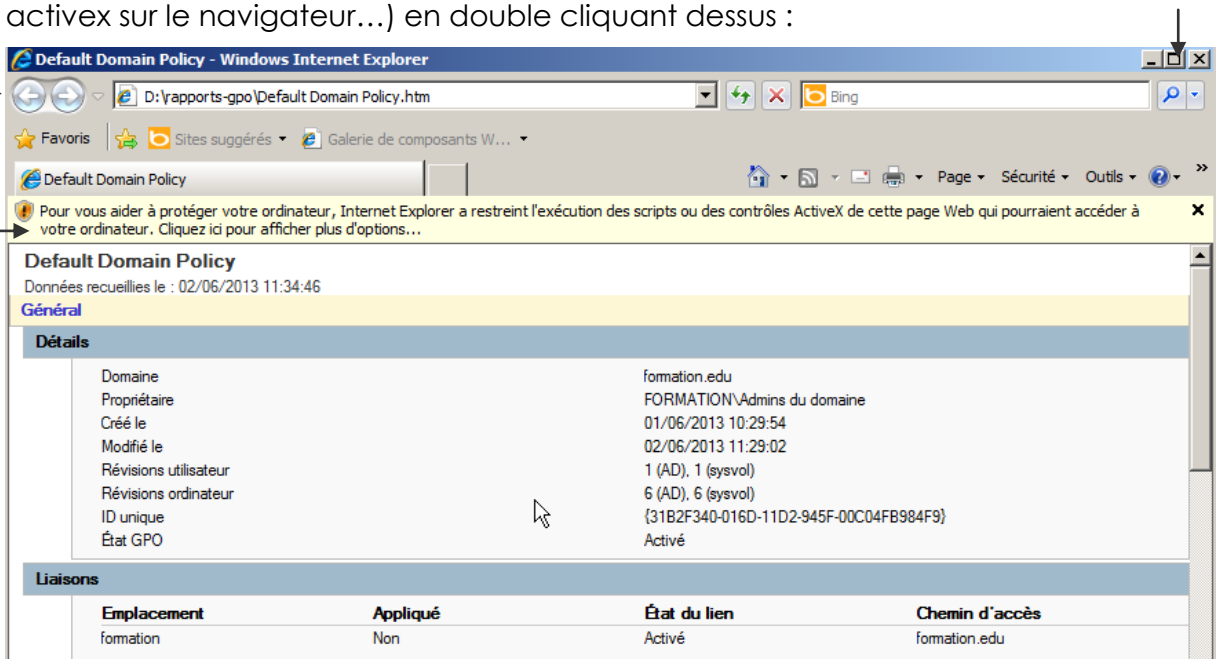


Et on indique ensuite un dossier et un nom de fichier (au format HTML) par défaut le nom de la GPO est proposé

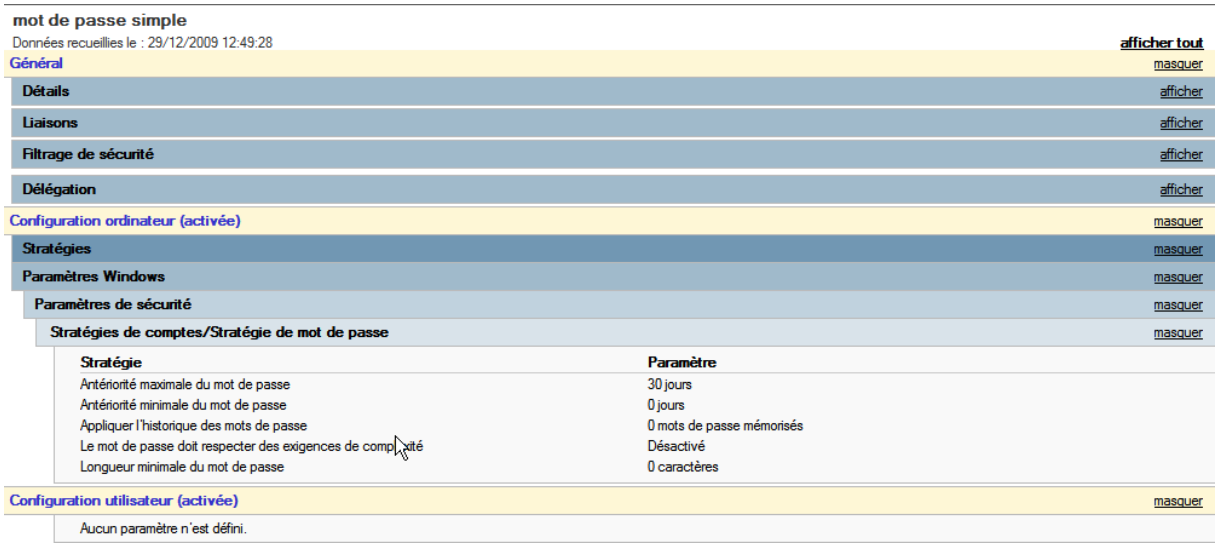
on peut du coup avoir ce genre de liste...

Default Domain Controllers Policy.htm	01/12/2009 09:32	Document HTML
Default Domain Policy 2.htm	29/12/2009 12:37	Document HTML
Default Domain Policy.html	01/12/2009 09:33	Document HTML
fermeture de session.htm	28/12/2009 13:03	Document HTML
mot de passe simple.htm	29/12/2009 12:49	Document HTML

Ces fichiers sont ensuite facilement visualisables (à condition d'autoriser les activex sur le navigateur...) en double cliquant dessus :



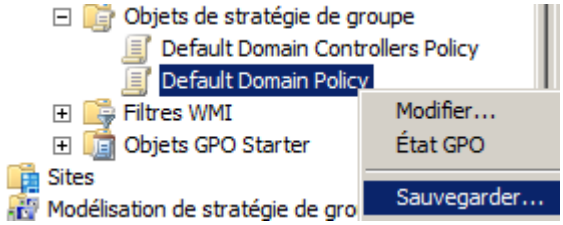
on autorise les ActiveX... et sur la droite apparaît la fonction **Afficher / Masquer**



Sauvegarder une ou toutes les stratégies :

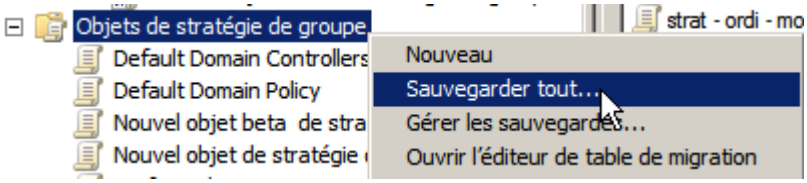
On peut se placer dans le dossier **Objets de stratégies de groupe**

Sur la stratégie que l'on souhaite sauvegarder, et demander **Sauvegarder…**

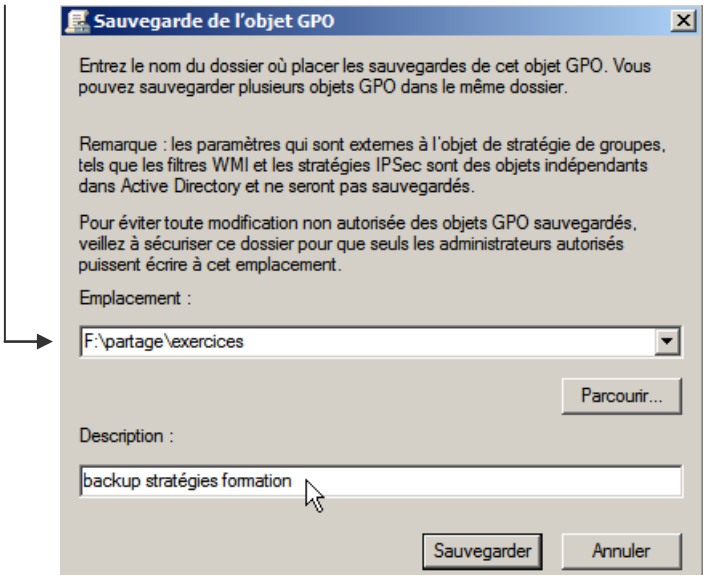


On peut se placer sur le dossier **Objets de stratégies de groupe**

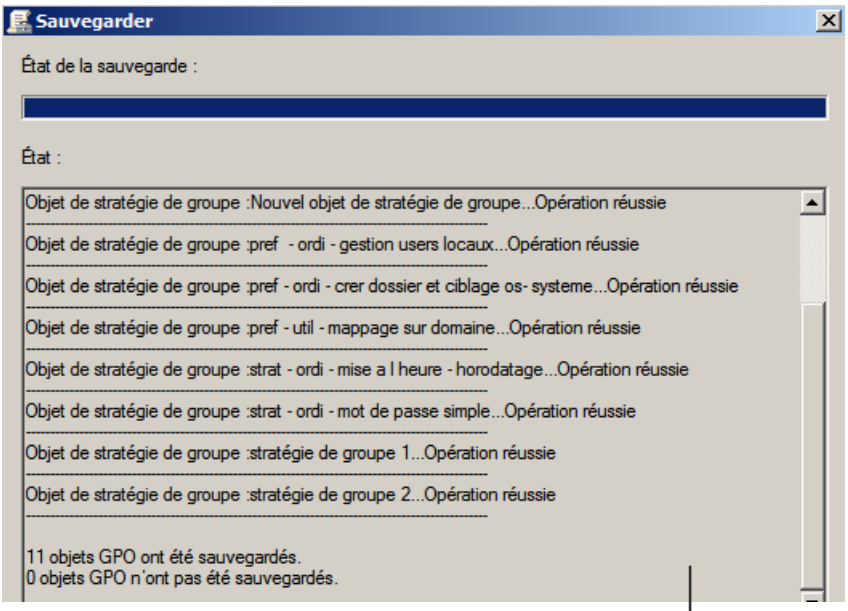
et demander **Sauvegarder tout…**



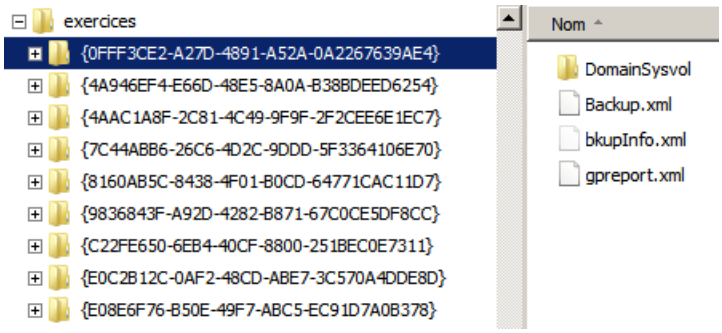
Il faut indiquer un emplacement



on a une confirmation



et voila…

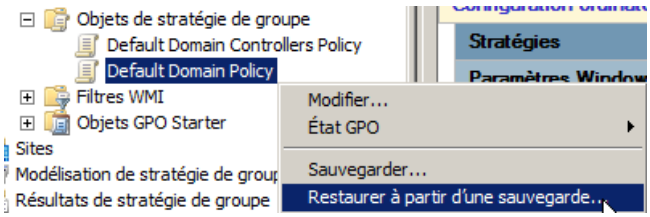


Restaurer les stratégies :

Dans la même logique soit

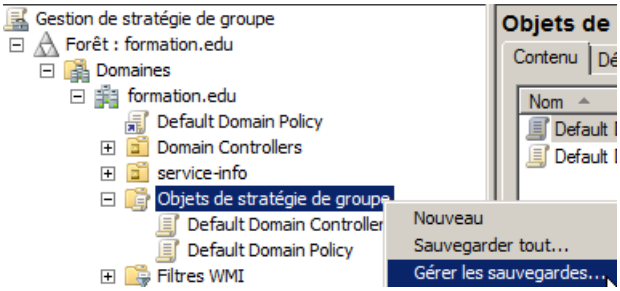
on veut restaurer une seule stratégie:

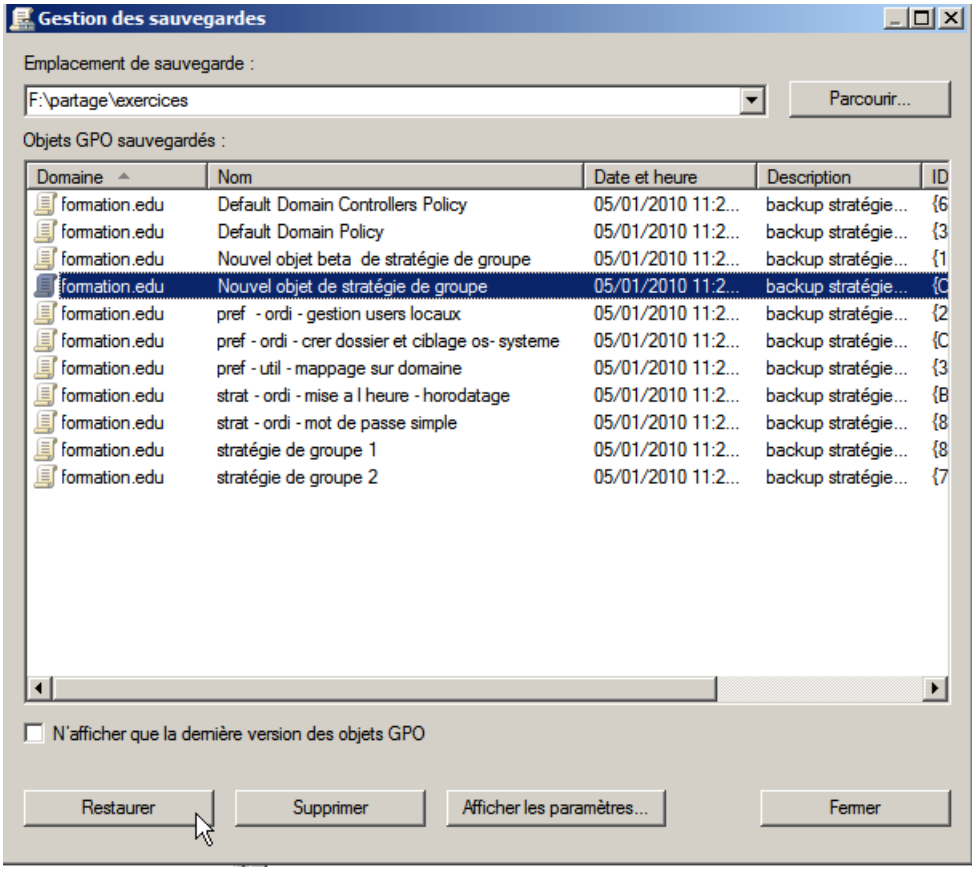
on se place dessus, puis **Restaurer à partir d'une sauvegarde**...



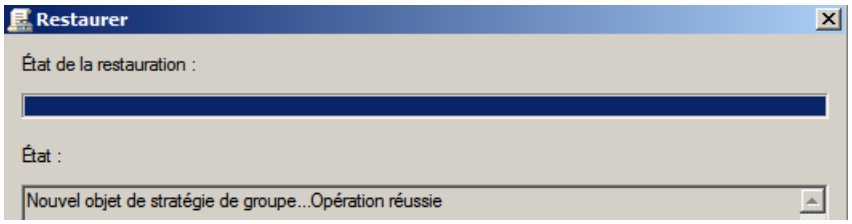
ou bien on se place sur le dossier **Objets de stratégies de groupe**

et on demande **Gérer les sauvegardes…**





On sélectionne la stratégie à restaurer, puis on demande **Restaurer**

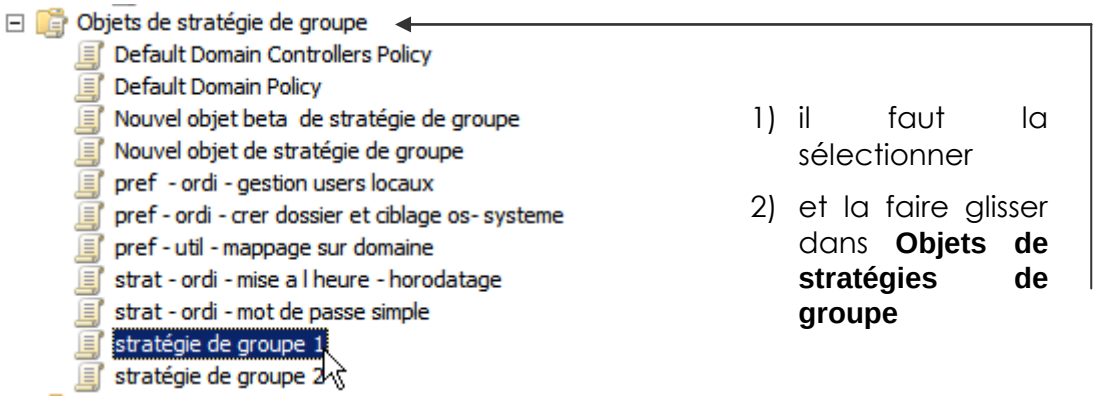


N.B: par contre les liaisons ne sont pas recrées !

Copier une stratégie :

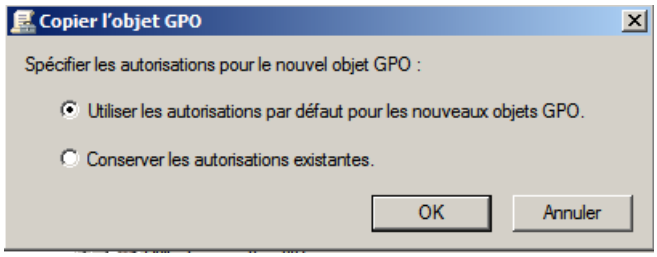
Si on souhaite copier une stratégie, pour repartir de cette base et la retravailler, par exemple on veut copier la "stratégie de groupe 1"

Il faut la copier – coller dans l'objet **Objets de stratégies de groupe**



1) il faut la sélectionner
2) et la faire glisser dans **Objets de stratégies de groupe**

Alors on réponds



On a confirmation, et voila…

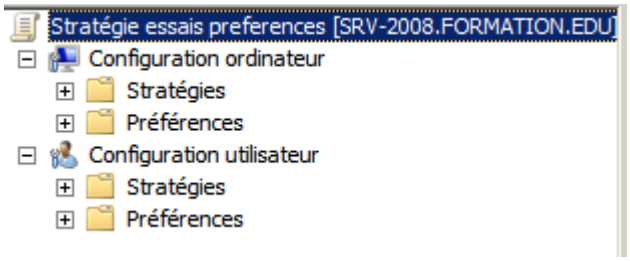
Sauvgarde des Stratégies par défaut :

Bine penser à effectuer une sauvegarde des **defaults domain policy** et **default domain controller policy**…

STRATEGIES ET PREFERENCES

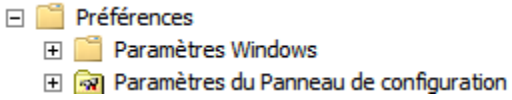
Les préférences depuis 2008 :

Les préférences sont une nouveauté disponible depuis 2008 et uniquement a destination des client depuis Seven (natif) ou Vista - Xp dotés des… **Clients Side Extensions**.



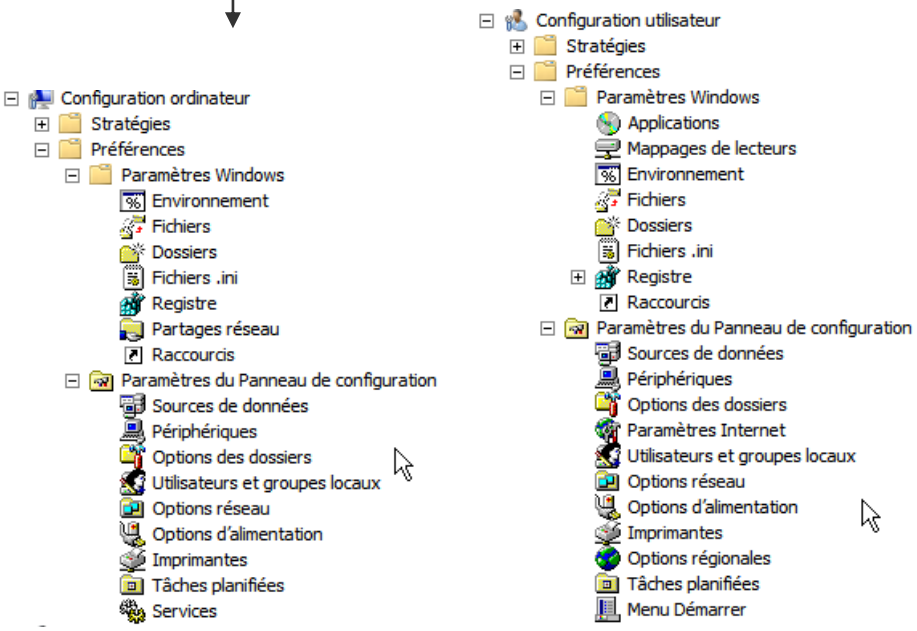
La différence fondamentale (s'il faut en trouver une) entre les **préférences** et les **stratégies**, réside dans le fait qu'une **stratégie** est toujours strictement appliquée, alors qu'une **préférence** peut être modifiée par l'utilisateur.

Donc comme certains paramètres sont disponibles aussi bien au niveau des préférences que des stratégies, à nous de choisir…



- Donnés via les **stratégie**s, ces paramètres ne sont pas modifiables par l'utilisateur…
- Donnés via les **préférences**, ces paramètres sont modifiables par l'utilisateur…

Les préférences sont nombreuses soit au niveau **ordinateur**, soit au niveau **utilisateur**



Client Side Extension pour XP SP2-Sp3 & Vista:

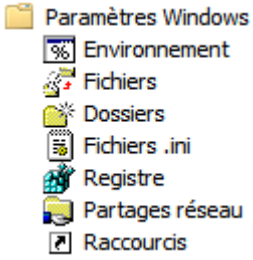
Côté client, vous devez déployer CSE : **Client-Side Extension** sur les systèmes suivants : (dans WSUS c'est un feature pack…)

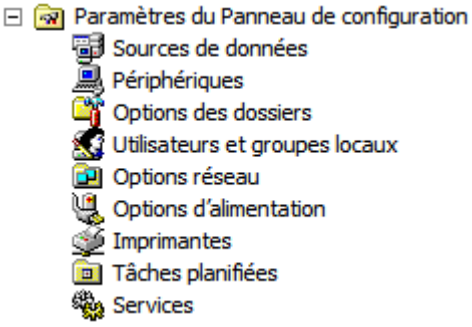
XP Sp2 – Sp3

Vista

Principales Préférences Ordinateur :

On y trouve surtout

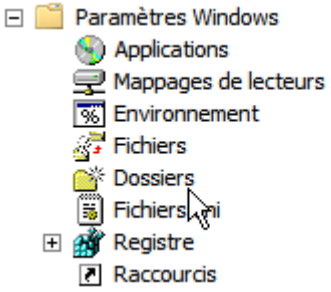


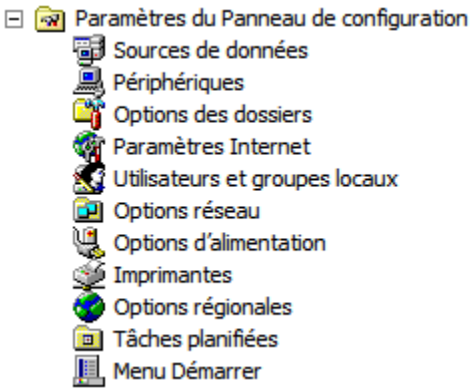


Mais principalement :

Principales Préférences Utilisateur :

On y trouve surtout





Mappages de lecteurs

Possibilité de gérer la connexion de lecteur réseau sur les postes de travail sans passer par des scripts de logon. Il faut le chemin UNC du partage, son nom d'apparition, sa lettre de lecteur et de choisir la cible du paramètre.

Fichiers

Possibilité de copier des fichiers, les déplacer, les renommer, modifier leur attribut sur les ordinateurs cibles par GPO sans le moindre script. Pour une copie, indiquez la source (généralement un partage) puis le chemin de destination. Si vous copiez le fichier dans un répertoire inexistant, ce dernier sera automatiquement créé.

N.B: il est obligatoire de retaper le nom du fichier complet dans le chemin de destination pour que la copie s'effectue correctement

Dossiers

Possibilité de créer, modifier, remplacer et supprimer des dossiers sur les ordinateurs cibles. Lors de la suppression d'un dossier, plusieurs options sont alors envisageables : Supprimer le dossier s'il est vide, supprimer également tous les sous dossiers s'ils sont vides également mais aussi supprimer tous les fichiers à l'intérieur de ce dossier et autoriser la suppression de fichiers/dossiers en lecteur seul.

Raccourcis

Possibilité d'effectuer des raccourcis vers des applications, des URL ou des objets Shell…

Périphériques

Possibilité d'activer ou désactiver des périphériques à distance soit au niveau ordinateur soit au niveau utilisateur.

Option des dossiers

Possibilité de modifier les options de dossiers (pour Windows XP et pour Windows Seven) comme par exemple activer l'affichage des fichiers et dossiers cachés. On peut également cacher l'affichage des extensions des fichiers connus …

Utilisateurs et groupes locaux

Possibilité de créer des utilisateurs et groupes locaux sur vos ordinateurs réseaux mais également les modifier. Il devient donc très facile de renommer et/ou modifier le mot de passe du compte administrateur local de toutes les machines. La gestion des groupes locaux est tout aussi puissante. Vous pouvez ajouter ou supprimer des membres à un groupe existant mais aussi en créer des nouveaux et les remplir…

Imprimantes

Possibilité de déployer une imprimante partagée / Locale et même réseau sur vos postes de travail.

menu Démarrer

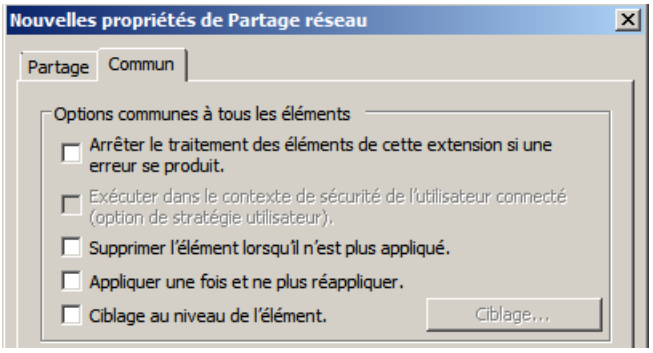
Possibilité de personnalisé le menu Démarrer des utilisateurs en paramétrant leurs propriétés. Il s'agit exactement des mêmes propriétés que vous retrouvez en local pour les postes sous Windows XP ou Windows Seven.

Services

Possibilité de gérer les services sur les postes distants et modifier leurs propriétés en choisissant le type de démarrage.

Options Communes des Préférences :

De nombreux éléments de préférence de stratégie de groupe partagent des options. Elles sont affichées dans l'onglet **Commun** de chaque élément de préférence. Les options communes sont identiques dans les différentes extensions de préférence. Par exemple si on à crée un partage réseau, alors on pourra accéder à



Les principales étant

Exécuter dans le contexte de sécurité de l'utilisateur connecté:

Par défaut, les stratégies de groupe de préférence utilisent le compte **local System** ce qui permet d'accéder aux variables d'environnement système et aux ressources locales. Pour accéder à l'environnement utilisateur et ses ressources réseaux (lecteurs réseaux) vous devez cocher cette case.

Supprimer l'élément lorsqu'il n'est plus appliqué:

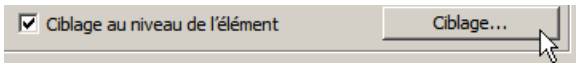
Contrairement aux paramètres de stratégies de groupes classiques qui sont retirés lorsque la GPO est supprimée, les préférences restent. Il est donc possible en cochant cette case d'obtenir le même comportement.

Appliquer une fois et ne plus réappliquer :

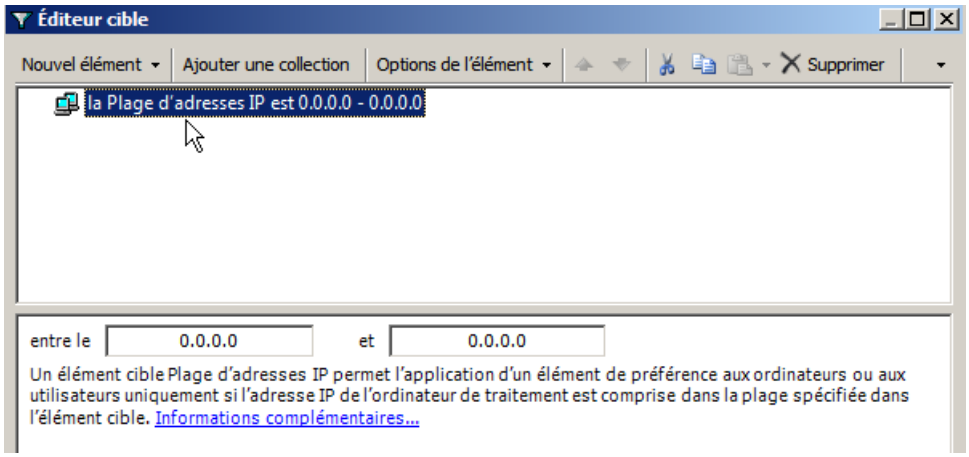
Les préférences sont actualisées toutes les 90 minutes par défaut (comme les stratégies). Du coup, si un utilisateur modifie les préférences, celles-ci seront remodifiées par la stratégie. Pour éviter ce comportement, cochez cette case pour que la stratégie ne s'applique qu'une seule fois.

Ciblage des Préférences :

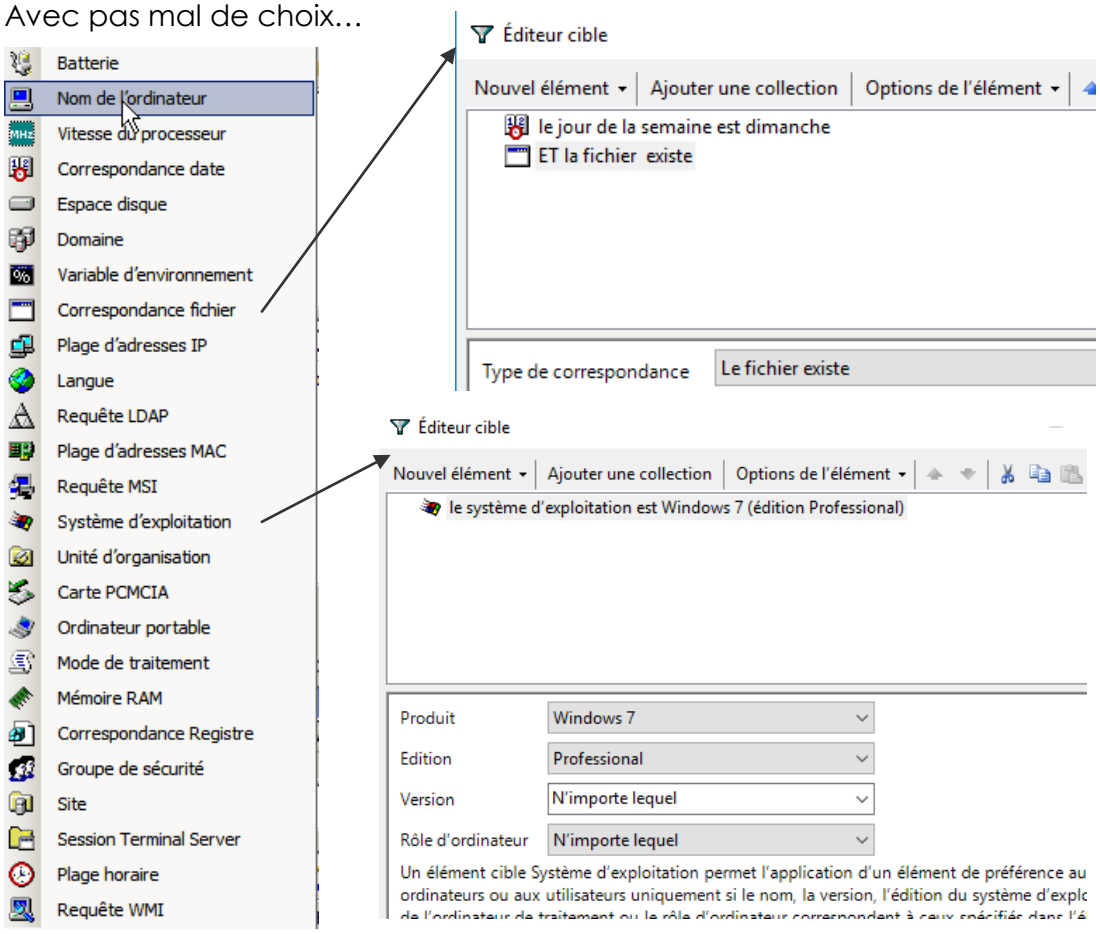
Ciblage au niveau de l'élément :



Permet de construire une requête…



Avec pas mal de choix…



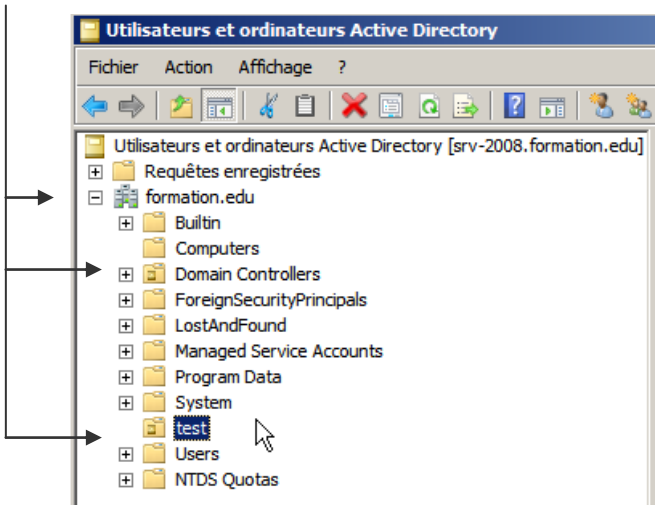
GPO D'UNITE ORGANISATIONELLE

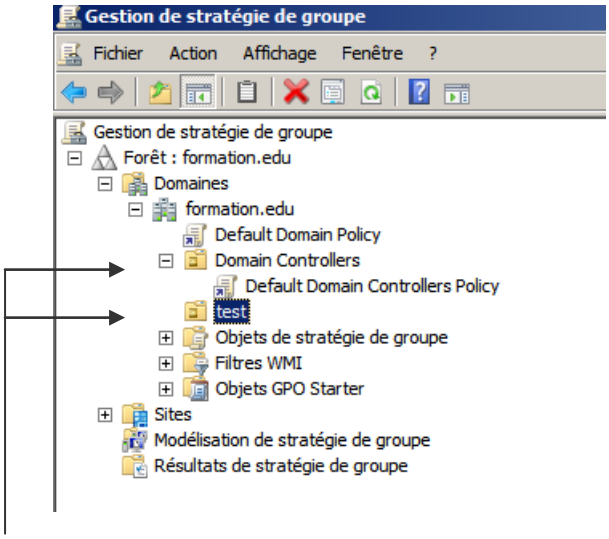
Types et niveaux de stratégie :

GPO signifie **Group Policy Object**

On l'a déjà dit mais rappelons que l'on peut poser des s**tratégies** à différents niveaux, et donc les **GPO** sont des modèles de stratégies posées au niveau des **Unité organisationnelles** de **Active Directory**

Ces **Unités Organisationnelles** peuvent être crées dans la console gestion **AD Utilisateurs et Ordinateurs Active Directory…**

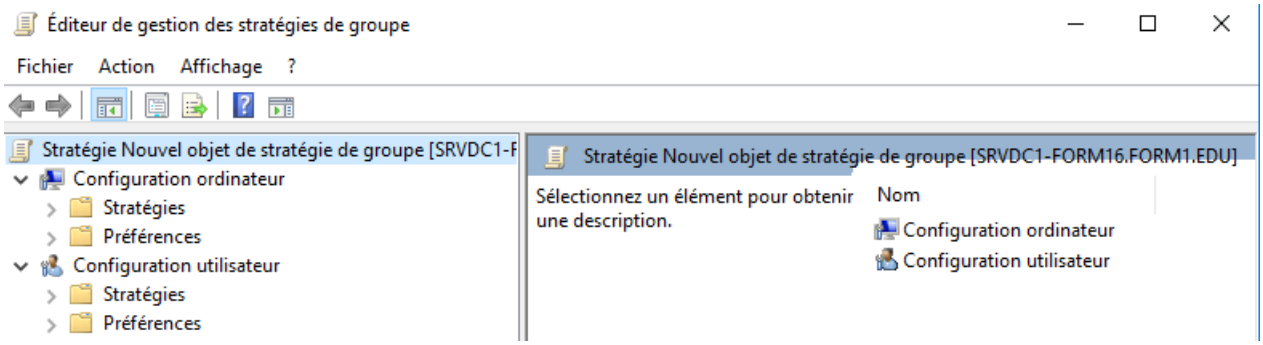




On les retrouvera dans la console **Gestion des stratégies de groupe !**

N.B: il est possible de créer des UO directement depuis la **gestion des stratégies de groupe,** mais cela n'est pas une bonne habitude…

Comme Les **GPO de domaine** Les **GPO d'Unités Organisationnelles** se décomposent en deux catégories



- Les paramètres de **stratégie de groupe pour les ordinateurs**
- Les paramètres de **stratégie de groupe pour les utilisateurs**

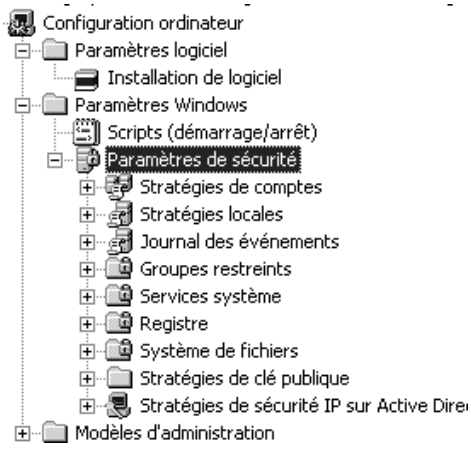
Par défaut, les stratégies de groupes ont un traitement synchrone, c'est à dire :

- les **stratégies de groupe pour les ordinateurs** s'exécutent avant que le message de bienvenue dans windows ne s'affiche.
- les **stratégies de groupe pour les utilisateurs** s'exécutent avant que l'interpréteur de commande du système ne soit activé et mis à la disposition de l'utilisateur.
- Les questions de propagations sont les mêmes que pour les stratégies de Domaine

N.B: Dans le cas où l'on définirait des stratégies contradictoires, il faut savoir que normalement les stratégies ordinateurs prennent le pas sur les stratégies utilisateurs.

Les ajouts notables dans les **stratégies de groupe pour les ordinateurs** sont:

1. les scripts de machine, avec les scripts de démarrage et les scripts d'arrêt…
2. l'installation de logiciel
3. Modèles d'administration

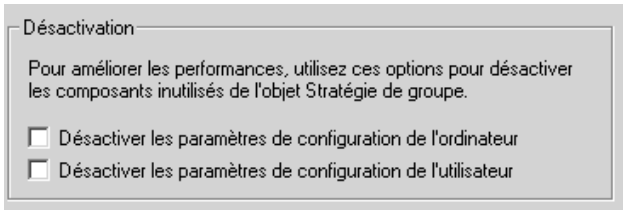


Les ajouts notables dans les **stratégies de groupe pour les utilisateurs** sont:

1. Les installations de logiciels
2. les scripts d'ouverture et de fermeture de session (doublon avec compte util…)
3. redirection de dossier
4. Modèles d'administration

N.B: les scripts qui sont gérés par les stratégies ne sont pas récupérés par les clients antérieurs à windows 2000

N.B: Dans une stratégie on peut au niveau de ses propriétés invalider la catégorie que l'on ne pense pas utiliser (amélioration de la vitesse de connexion)



Niveau de modification dans la base de registre

Lorsque l'on manipule les paramètres de **stratégies de sécurité locale**, (ce qui ne peut se faire que depuis le poste, comme on l'a vu dans le chapitre des stratégies locales…) on fixe les modifications dans la base de registre au niveau des clés

HKEY_LOCAL_MACHINE Et **HKEY_CURRENT_USER**

Ces modifications sont permanentes sur la machine, que cette machine soit membre d'un domaine ou non. C'est pour cette raison que ces **stratégies de sécurité locale** sont le seul moyen de gérer la sécurité sur des machines seules, hors domaine.

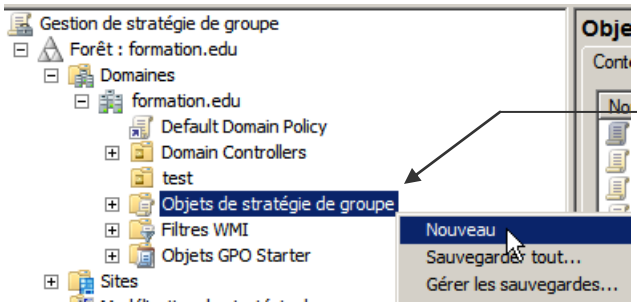
Lorsque l'on manipule les paramètres de **stratégies de sécurité de groupe**, on fixe les modifications dans la base de registre au niveau des clés qui seront effacées si la GPO ne s'applique plus. Donc en clair si les paramètres de stratégies GPO ne s'appliquent plus, on retrouvera les paramètres de stratégie locale.

Créer une Stratégie de Groupe:

Cela repose sur 3-4 étapes

1) Création de la stratégie en elle-même
2) Lier la stratégie sur l'UO cible
3) Vérification des éléments de l'UO (ordinateurs et / ou utilisateurs)
4) Propagation / test

Ayant ouvert une session sur un serveur contrôleur de domaine, il faut lancer la mmc **Gestion des stratégies de groupe**



En se plaçant sur **Objets de stratégie de groupe**

On demande **Nouveau**

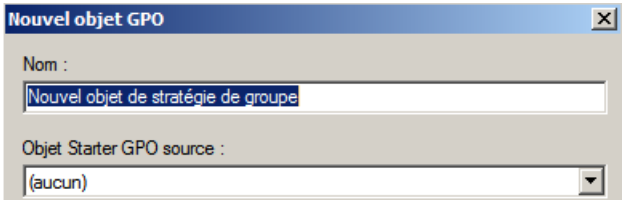
On lui donne un nom explicite avec une convention utile, par exemple

strat = stratégie

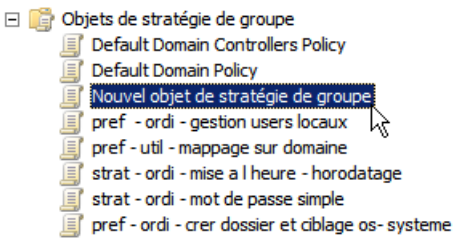
pref = préférence

o = ordinateur

u = utilisateur



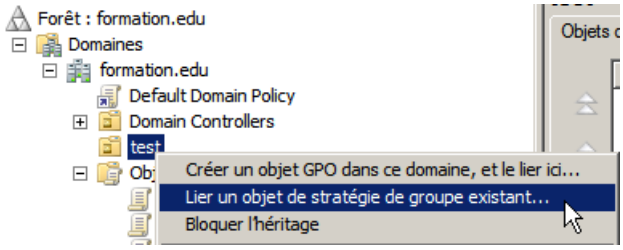
et on la modifie clic – droit / **Modifier**



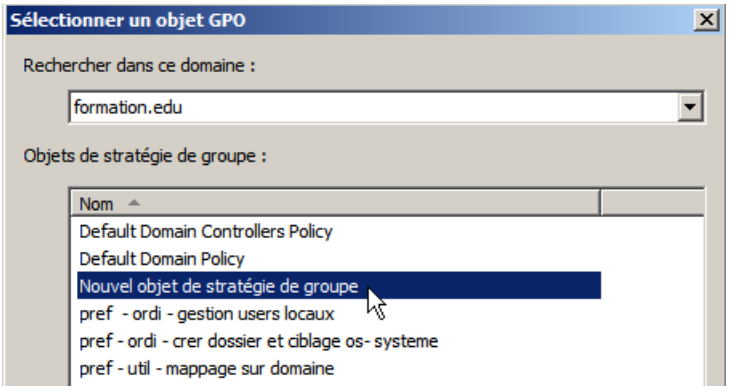
N.B: les tp suivant porteront sur le "contenu"… d'une stratégie…

Lier une Stratégie de Groupe sur une U.O :

Ensuite on lie la stratégie en se plaçant sur l'UO voulue, (voire le domaine) et clic **droit Lier un objet de stratégie de groupe existant…**

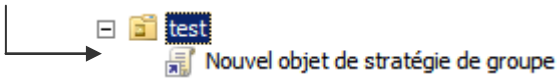


Tous les objets apparaissent



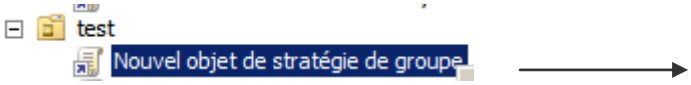
ok

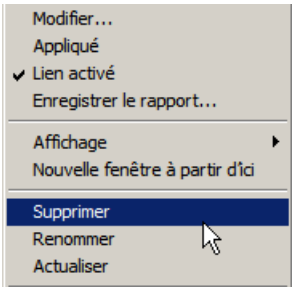
Et un pointeur (indiquant un lien) se crée :



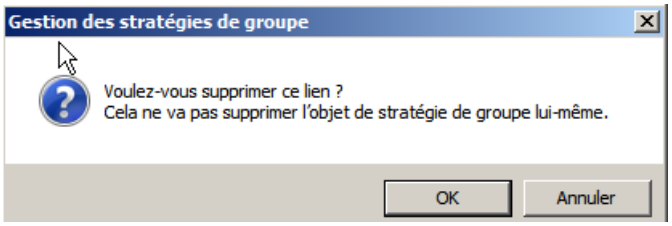
N.B: une stratégie peut être liée sur plusieurs UO, c'est bien le principe même… par conséquent son nom ne doit jamais mentionner l'UO sur laquelle elle s'applique, mais toujours sa nature (stratégie, préférence… ordinateur, utilisateur…), et son objectif (son action…)

Si on veut supprimer un lien, il suffit de sélectionner le pointeur (le lien) et demander **Supprimer**



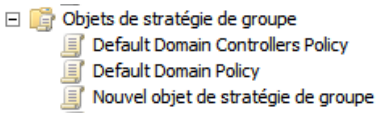


Cela supprime le lien sur cette **UO**

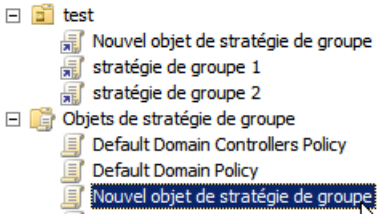


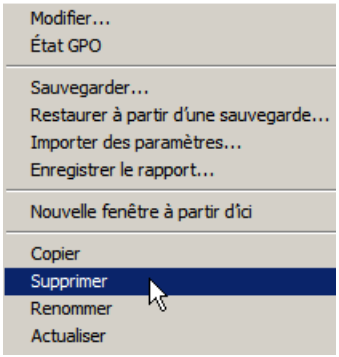
(par défaut OUI)

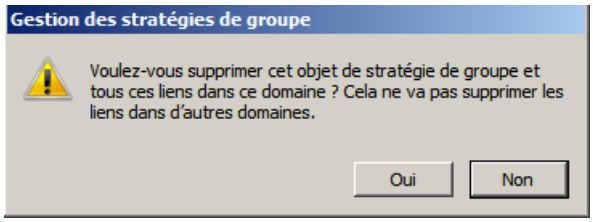
Mais la stratégie reste disponible



Pour supprimer la stratégie (et non pas le lien) il suffit de la sélectionner la stratégie et demander **Supprimer**







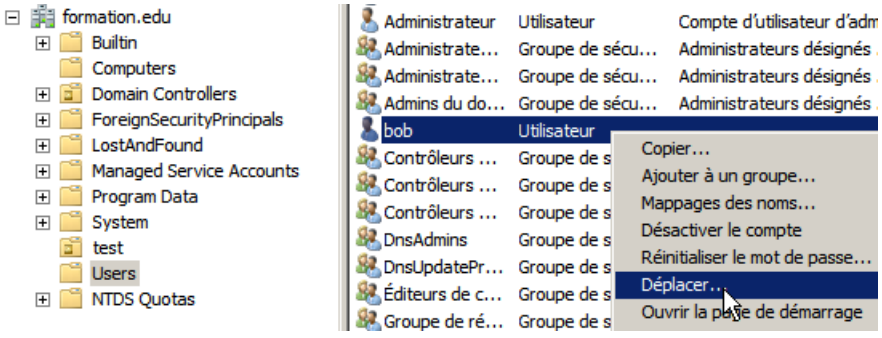
(par défaut NON)

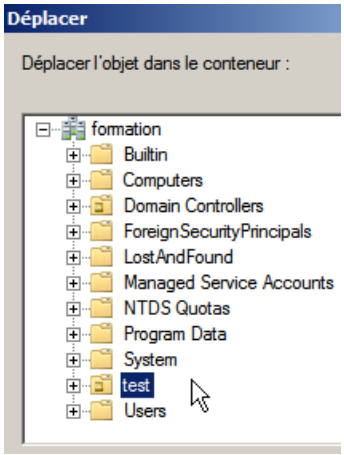
Et on supprime la Stratégie, et aussi tous les liens qu'elle pouvait avoir…

Vérification des éléments de l'UO:

La gestion des UO ne se fait pas depuis la mmc Gestion des stratégies de groupe, mais bien sur depuis la mmc **Utilisateurs et Ordinateurs Active Directory**

L'**UO** "test" étant vide actuellement, on peut y placer selon notre objectif, un utilisateur, ici dans l'exemple bob…



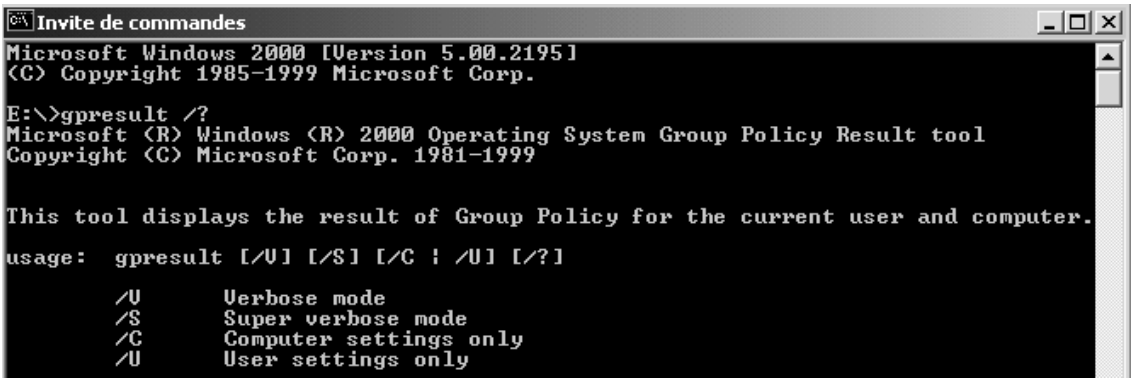


Et de même un compte ordinateur…

N.B: Il est toujours déconseillé de travailler au niveau des UO pré-définies, (**Domaine**, **Contrôleur de Domaine**) car leur portée est énorme… alors que si on se trompe de stratégie en test, seul **bob** et/ou la machine **pc-seven** en sont affectés !

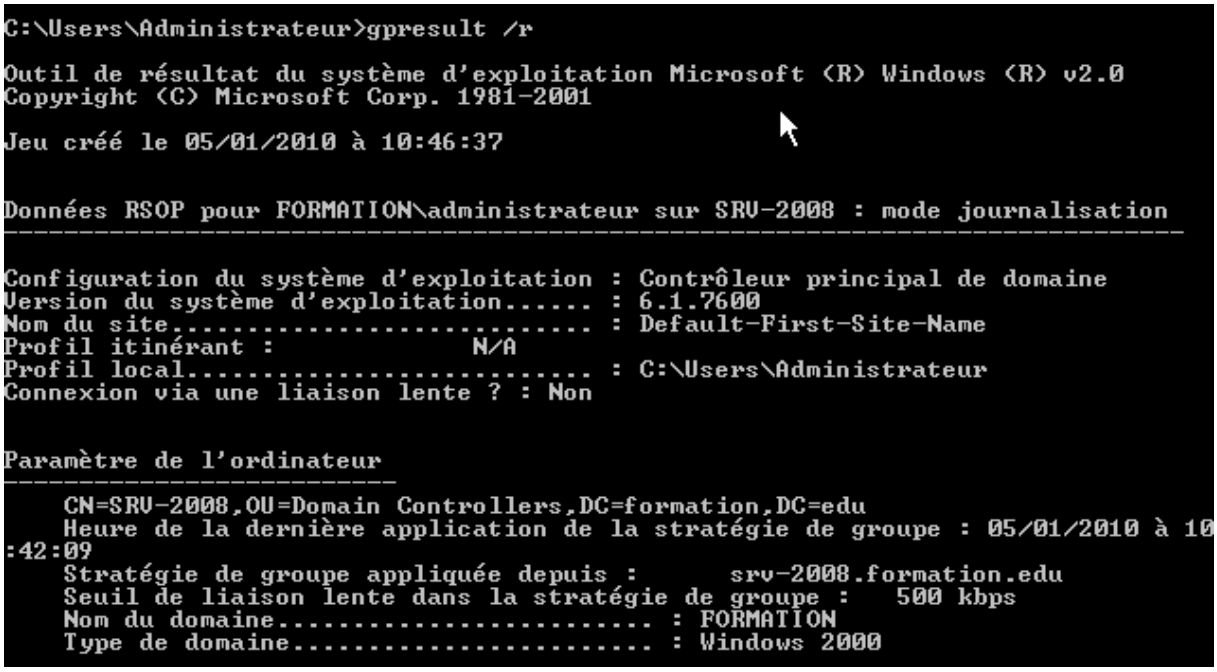
Gpresult.exe 10 - 7 - Xp

Il existe un utilitaire Disponible depuis XP (par le du kit de ressource technique et natif sous les versions récentes permettant d'avoir un compte rendu sur une machine des GPO sui se sont appliquées. Depuis Xp Sp3, (natif) et 2000 avec le Kit de ressource technique, appel par la ligne de commande **gpresult.exe**



Depuis Vista, et Seven (et 2008 Serveur) il faut obligatoirement ajouter une option

gpresult /R suffira au quotidien (fonctionne aussi sous XP-Sp3)



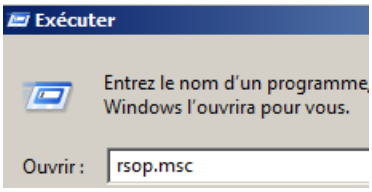
L'option **/V** est très complète…

N.B: penser que selon le compte qui est en session, **Gpresult** peut ne pas afficher les paramètres ordinateurs, mais uniquement les paramètres utilisateurs…

RSOP JEU DE STRATEGIE RESULTANT

RSop.msc resultant set of policy (local)

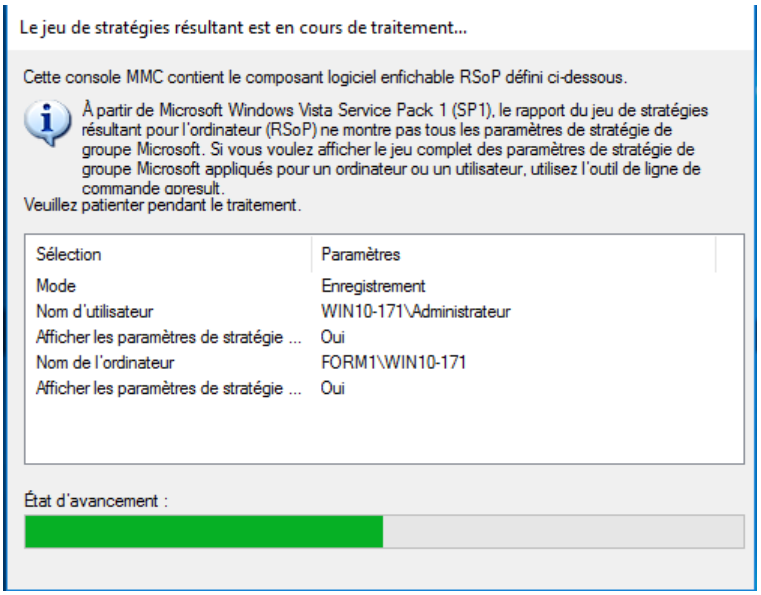
Il existe un utilitaire disponible depuis seven que l'on peut lancer en invite de commande



rsop.msc

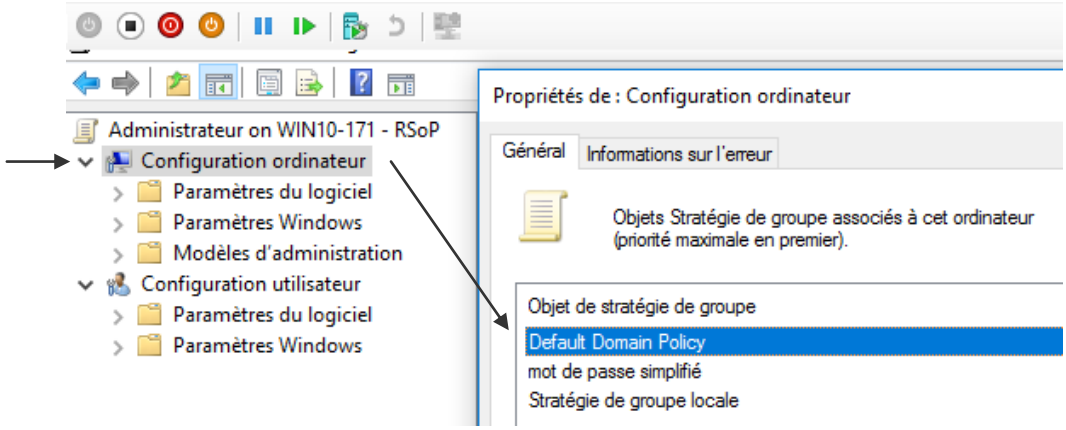
Il permet de donner la situation, par défaut,

- pour l'ordinateur sur lequel on se trouve,
- et l'utilisateur en cours de session...

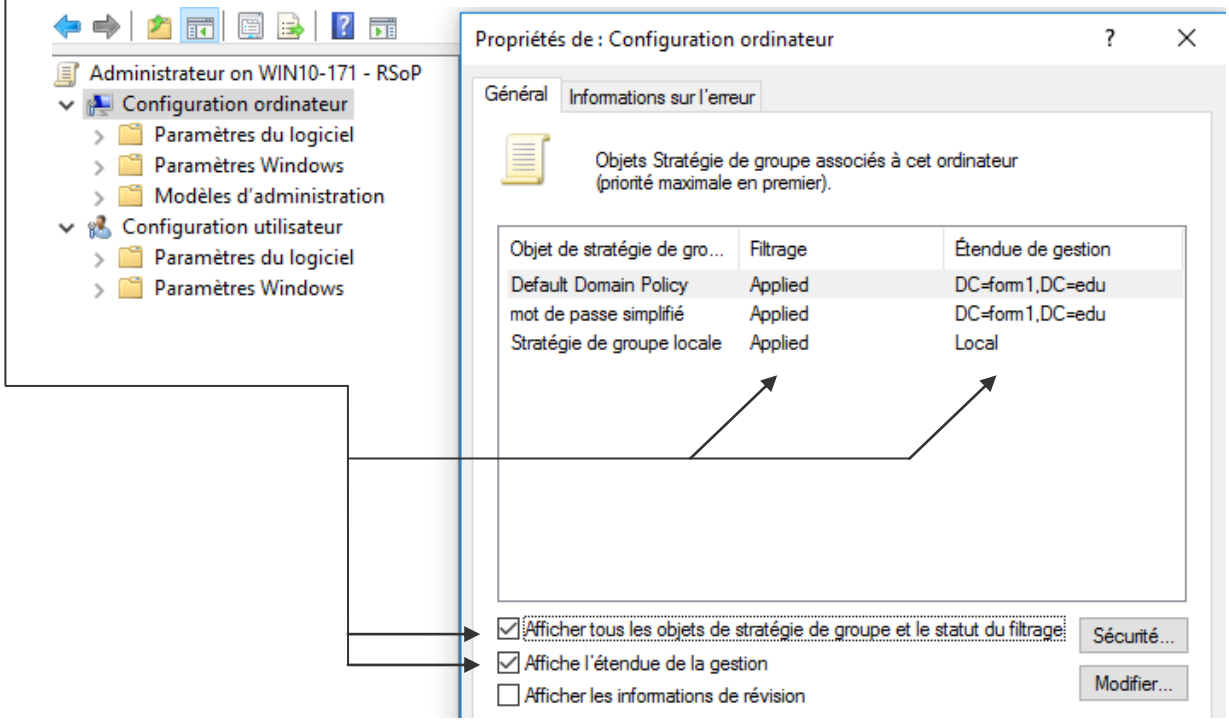


N.B: penser que selon le compte qui est en session, **Rsop** peut ne pas afficher les paramètres ordinateurs, mais uniquement les paramètres utilisateurs…

Si on demande les **propriétés** de la **Configuration Ordinateur** (ou **Configuration Utilisateur**) on à la liste des **GPO** qui s'appliquent, et dans quel ordre…



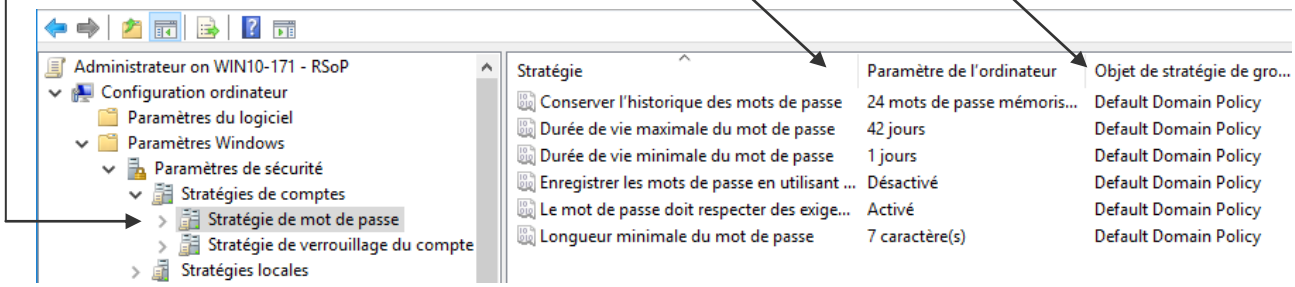
Si on veut plus d'informations, on peut demander d'afficher **les filtrages** éventuels, et **l'UO – l'étendue** d'appartenance



Mais surtout

Si on se met sur un paramètre de la GPO

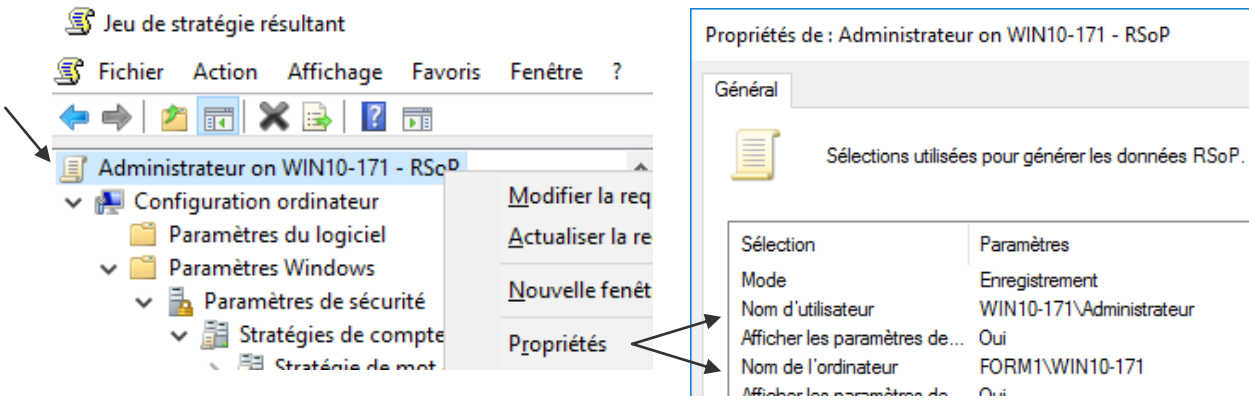
on voit alors la valeur finale-resultante et qui l'a générée



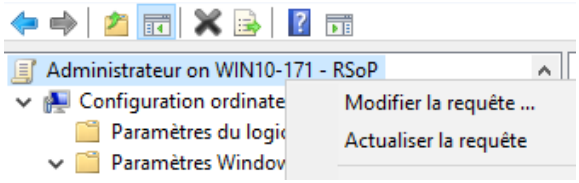
RSop.msc autre utilisateur - ordinateur

On a dit que par défaut RSOP donnait les indication pour l'ordinateur sur lequel on lance la commande RSOP et pour l'utilisateur connecté.

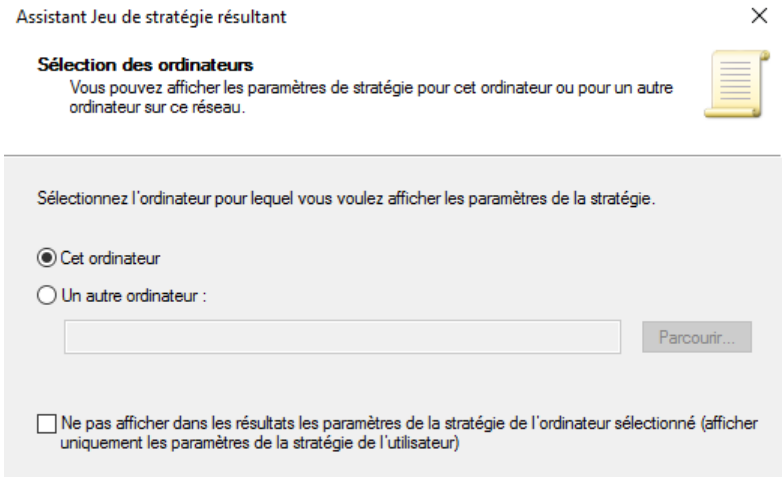
Cela peut se vérifier en demandant les **Propriétés** sur la **racine** de **RSOP**



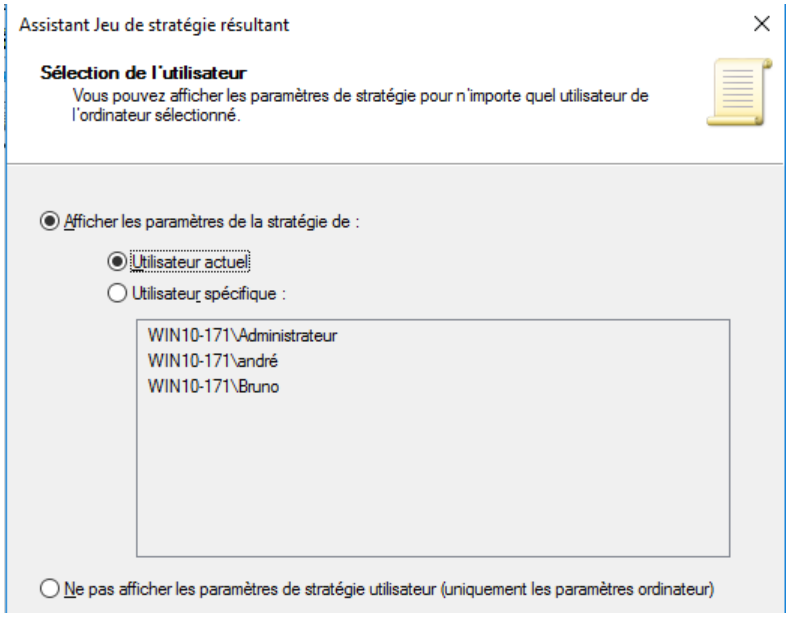
On peut changer cela, en fonction des droits avec lesquels on est connecté, en demandant **Modifier la requête…**



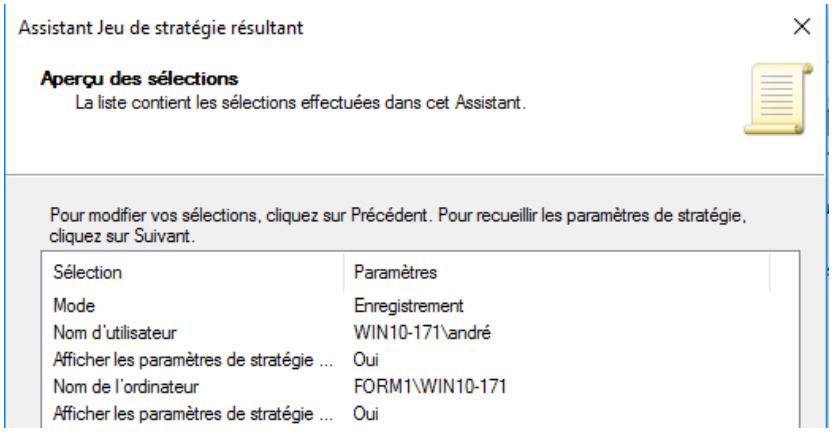
On peut choisir un **compte machine**



Et un **compte Utilisateur**

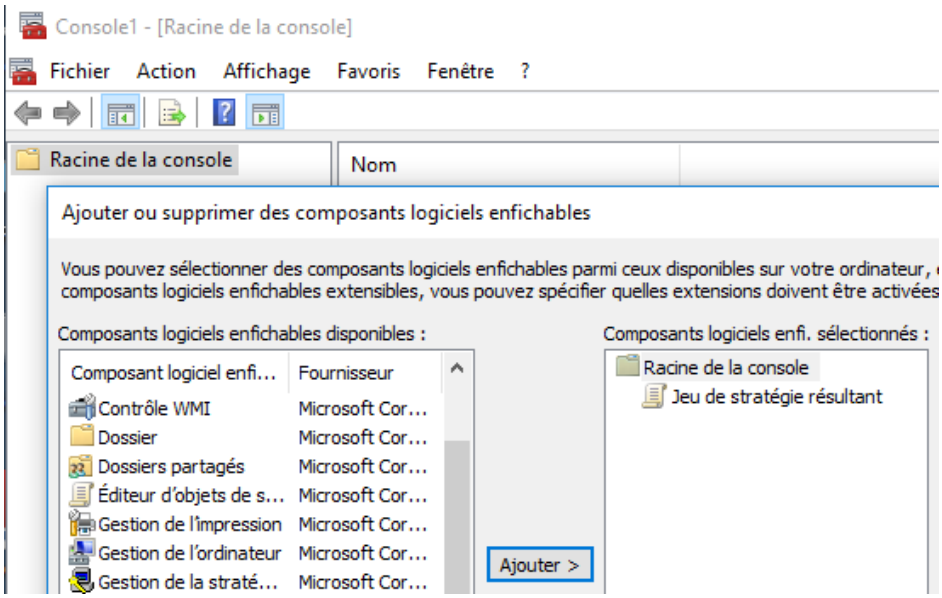


Et on affichera ensuite les **données RSOP** pour ce « couple »

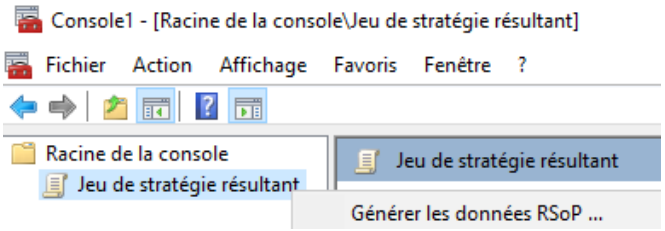


Mmc Jeu de stratégie résultant

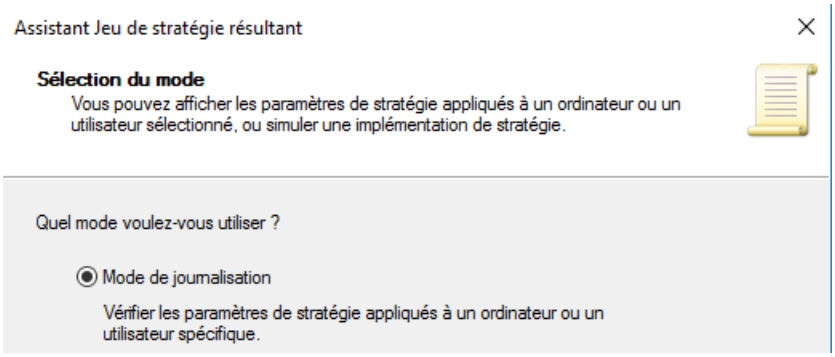
N.B : C'est ce qui se passera si on lance une mmc avec l'ajout du composant logiciel enfichable **Jeu de stratégie résultant**



Et dans lequel on demande **Générer les données RSOP…**

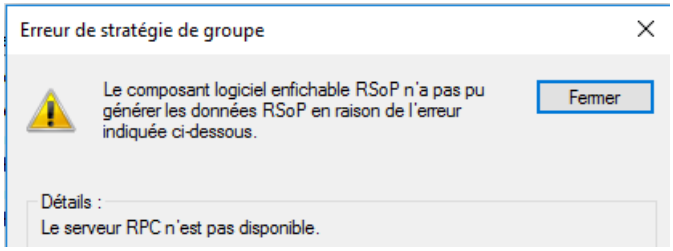


En **Mode Journalisation**



Erreur RPC – changement d'ordinateur

Lorsque l'on demande d'exécuter un **RSOP** sur une autre machine que celle sur laquelle on est connecté, on a souvent une erreur **RPC**

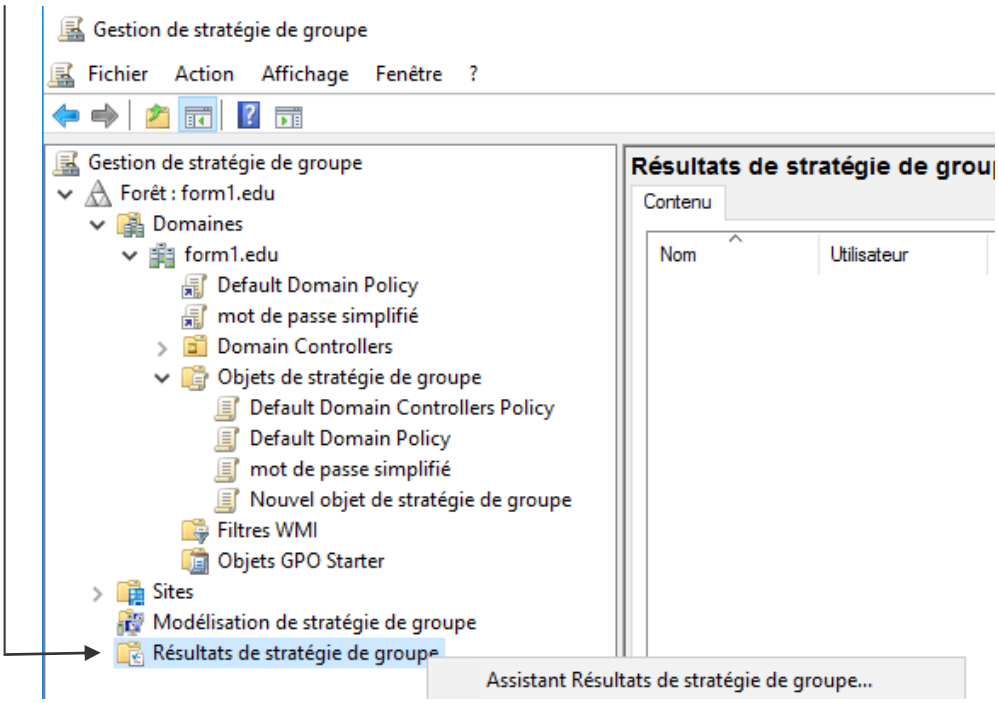


Il faut penser à ouvrir dans le **Pare-feu** les accès **administration distante** et **WMI**

Rsop dans la console Gestion de stratégie de groupe

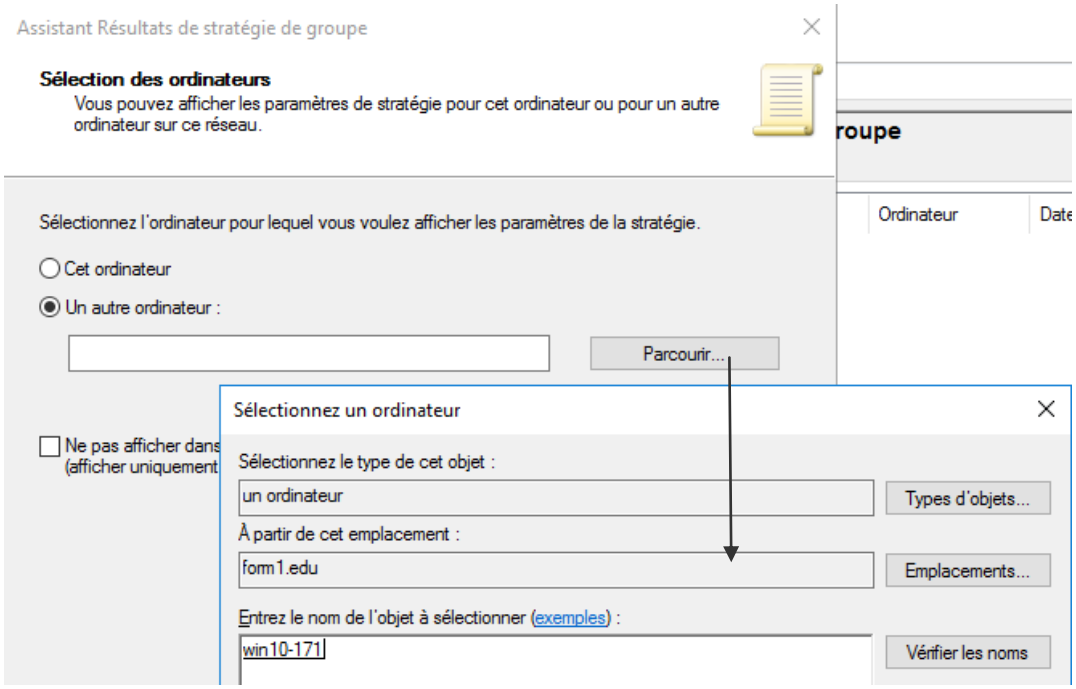
Dans la console gestion de stratégies de groupe, on a la possibilité de construire plusieurs requêtes **RSOP** et de les visualiser très simplement

On se place sur **Résultats de stratégie de groupe**, et on demande **Assistant résultats de stratégie de groupe**

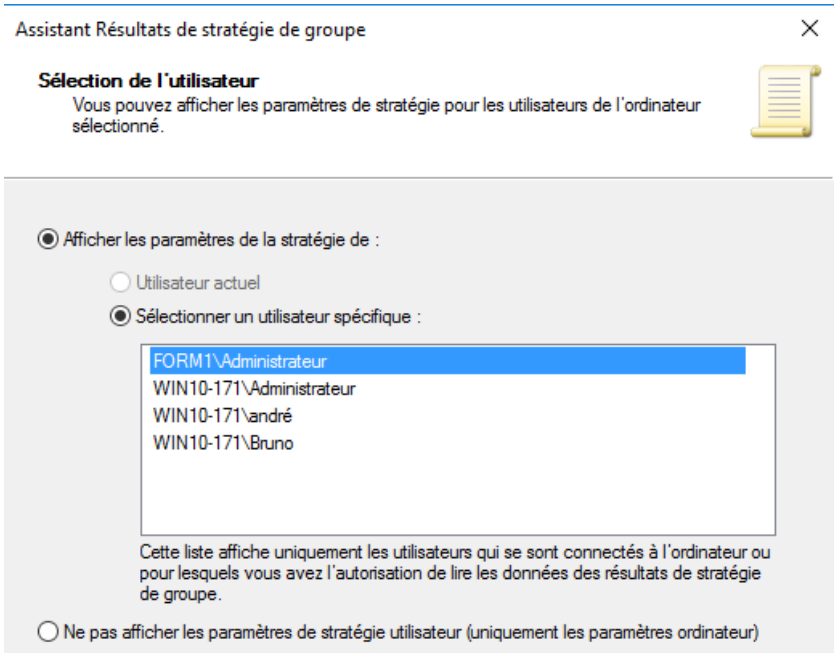


Un assistant se déclanche

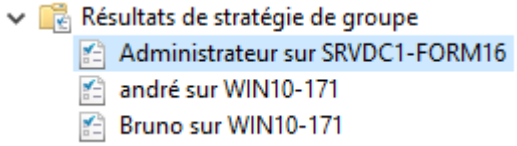
On peut indiquer n'importe quel ordinateur du Domaine



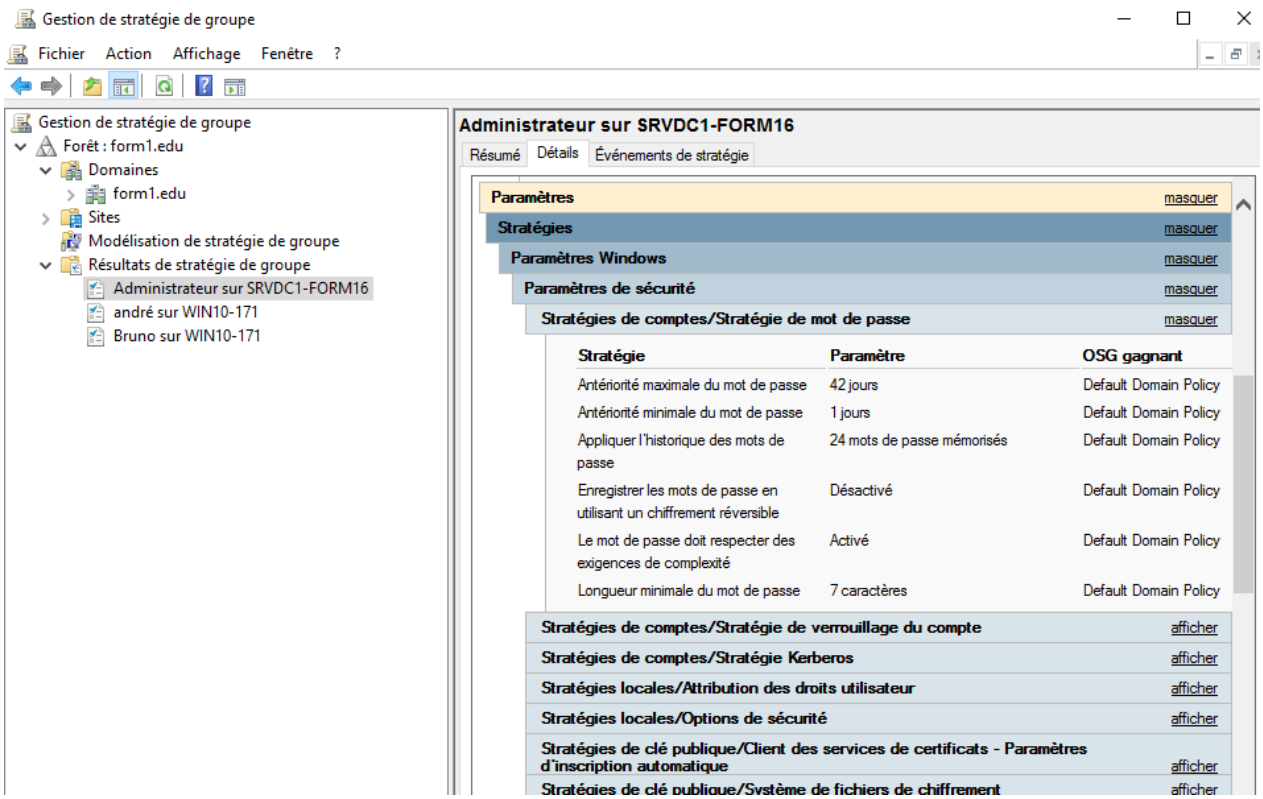
Et un utilisateur souhaité



On peut donc se construire un ensemble de test…



Et la lecture pour chacun est détaillée



HIERARCHIE DES STRATEGIES

Ordre final d'application des stratégies :

Pour être complet, on dira donc les paramètres modifiables par stratégies le sont dans cet ordre (sauf blocage spécifique au niveau de l'héritage)

Clients Hors Domaine

- Pour des clients 10 SEVEN XP(PRO) ou serveur 2008R2-2008-2003

  stratégies locales - & MLGPO

Clients du Domaine Hors Contrôleurs de Domaine

- Pour des client 10 SEVEN XP(PRO) ou les serveurs 2016 – 2012 -2008R2 membres:

  stratégies locales / stratégies de domaine

  et si des GPO sont données sur des UO alors on a

  stratégies locales / stratégies de domaine / GPO d'UO

  et si la notion de site est activée

  stratégies locales / stratégies de site / stratégies de domaine / GPO d'UO

Contrôleurs de Domaine

- Pour des serveurs 2016 2012r2 -2008R2

  stratégies locales / stratégies de domaine / stratégies de CD

  et si la notion de site est utilisée

  stratégies locales / stratégies de site / stratégies de domaine / stratégies de CD

- Pour des serveur 2003 (les stratégies locales sont dévalidées, pour les manipuler il faut passer par **secpol.msc /s**)

  stratégies de domaine / stratégies de CD

  et si la notion de site est utilisée

  stratégies de site /stratégies de domaine / stratégies de CD

N.B: toutes les stratégies définies par défaut dans la GPO de domaine, s'appliquent à la GPO des Contrôleurs de Domaine. **SI ON VEUT QUES LES STRATEGIES DE DOMAINE NE S'APPLIQUENT PAS AUX CD IL FAUT BLOQUER L'HERITAGE**

N.B: Dans le cas où l'on définirait des stratégies contradictoires, il faut savoir que normalement les **stratégies ordinateurs** prennent le pas sur les **stratégies utilisateurs**.

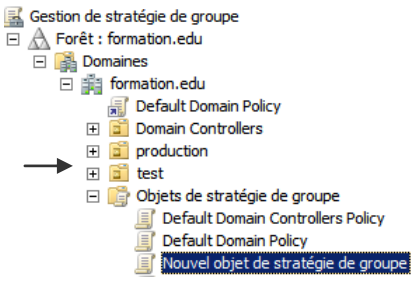
LIAISONS MULTIPLES - PRIORITE - HERITAGE -GPO

Liaison de GPO :

On a compris que lorsque l'on définissait une **GPO** sur une **UO**, celle-ci s'appliquait à tous les éléments posés dans l'**UO**.

On a aussi vu que l'on pouvait appliquer la même **GPO** à deux **UO** différentes…

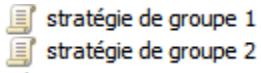
Créons une UO "production" sur laquelle on applique la même GPO …

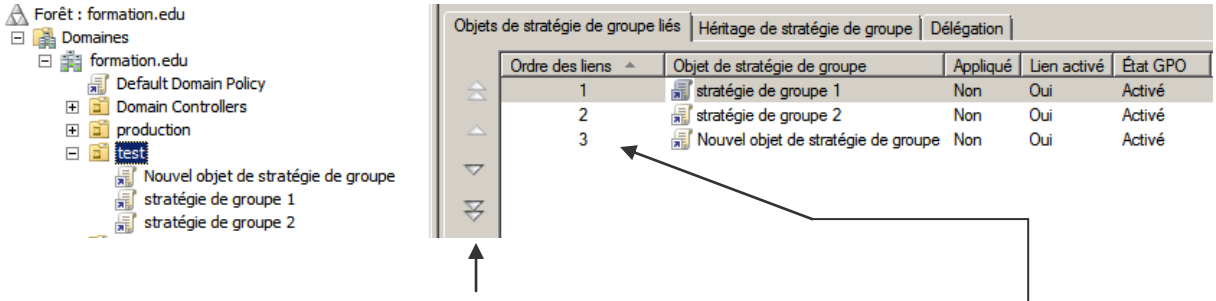


N.B: il est donc immédiat dans **Etendue** de savoir "*si une GPO est utilisée sur d'autres UO que celle sur laquelle on pointe*

Priorité de GPO :

Créons deux autres GPO nommées "stratégie de groupe 1" et "stratégie de groupe 2" et relions les sur l'UO "test" (qui au final reçoit 3 stratégies…)



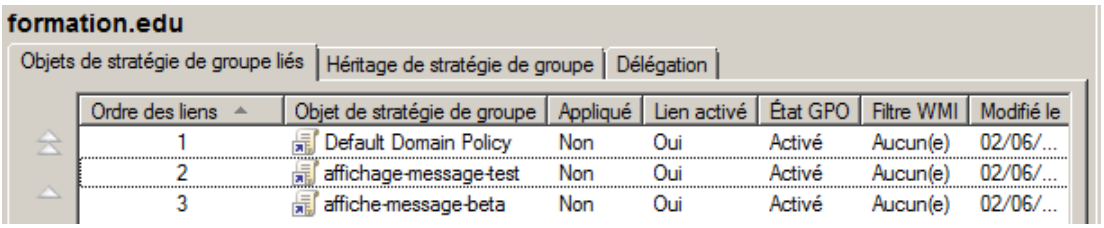


On peut modifier l'ordre des liens avec les boutons de défilement

N.B: L'**Ordre des liens** permet de comprendre de la priorité d'une GPO (c'est toujours le lien d'ordre 1 qui aura le dernier mot sur l'ordre 2 qui lui aura le dernier mot sur l'ordre 3…)

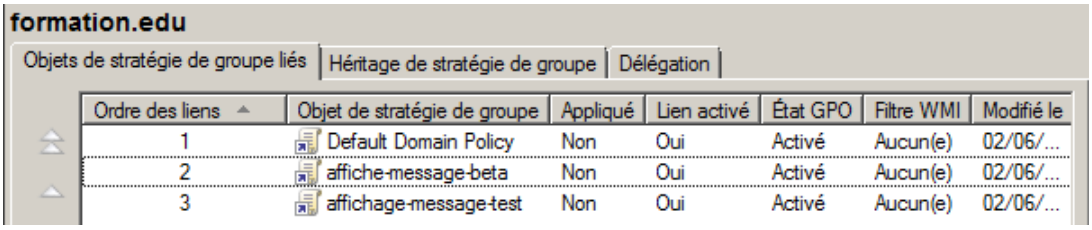
Si par exemple on souhaite que la stratégie de groupe 2 soit celle qui prenne le pas sur toutes les autres, alors il faut la passer en ordre 1…

dans l'exemple ci-dessous



les machines affichent le message "TEST" car la défaut policy elle , ne fait rien afficher..

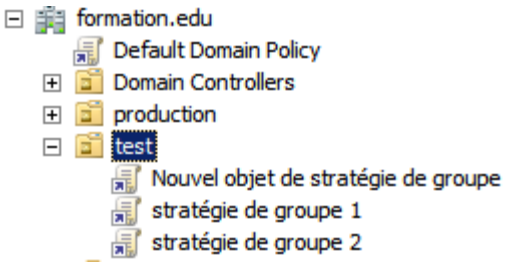
pour que les machines affichent le message "BETA" il faut élever l'ordre du lien de la GPO beta, comme ci-dessous



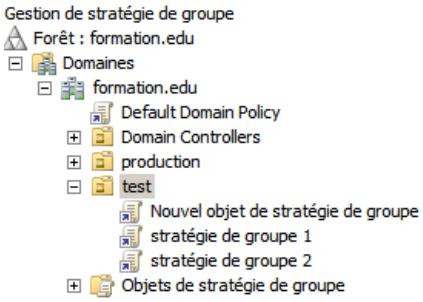
héritage – bloqué :

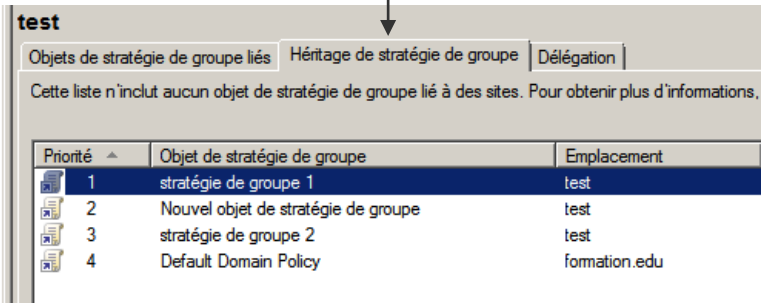
En plus de l'ordre des stratégies dans une UO, la notion d'héritage existe pour l'arborescence d'AD…

ainsi par "héritage", notre stratégie de Domaine **Default Domain Policy** se propage dans notre UO test

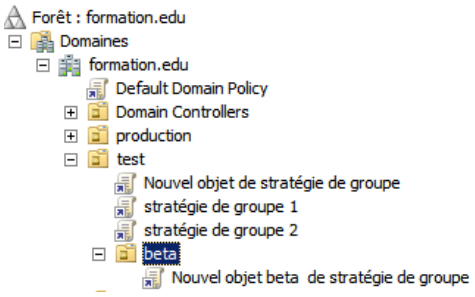


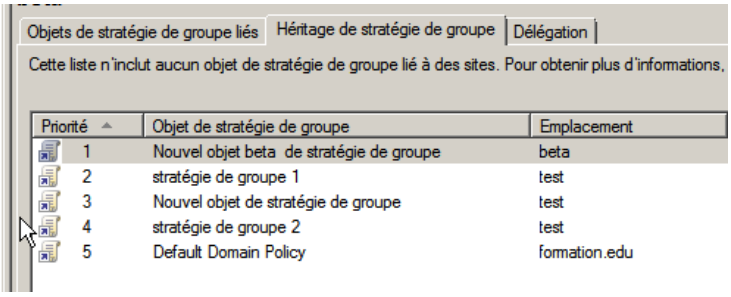
Ce que l'on peut constater dans l'onglet **Héritage de stratégies de groupe**





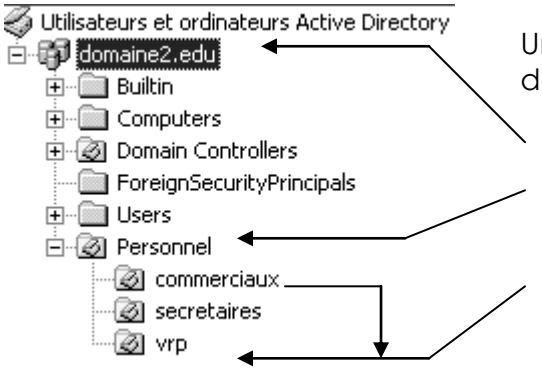
Et ainsi de suite





N.B: L'**Ordre des liens** permet de comprendre de la priorité d'une GPO (c'est toujours le dernier qui cause qui a raison…)

Donc, lorsque l'on crée des **UO**, les **GPO** s'appliquent de manière hiérarchique.

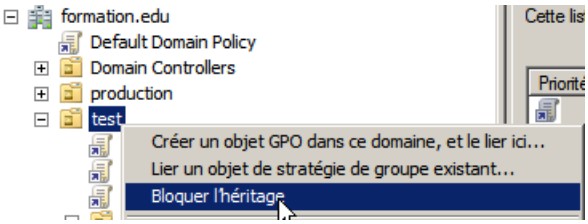


Un élément placé dans l'UO **vrp** reçoit donc ici :

- la GPO de domaine par défaut
- La GPO de Personnel (si elle existe)
- La GPO de vrp et celles liées (par exemple celle de commerciaux

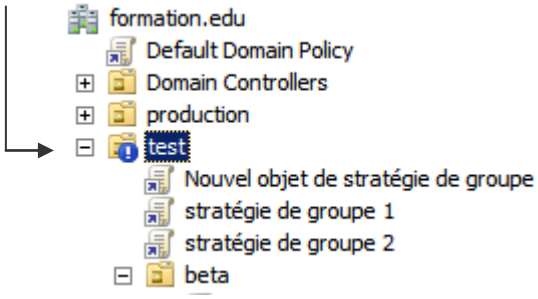
N.B: En cas de conflit sur un même élément défini à différents niveaux, le principe étant de dire "c'est le dernier qui cause, qui a raison" une exception, lorsque les paramètres qui rentrent en conflits sont exprimés dans des paramètres utilisateurs, et des paramètres ordinateurs. Dans ce cas, généralement les paramètres d'ordinateurs priment ! mais cela doit être vérifié dans les explications des propriétés…

Il est possible de bloquer l'héritage au niveau d'une UO, il suffit simplement de demander sur cette UO, **Bloquer l'héritage**:

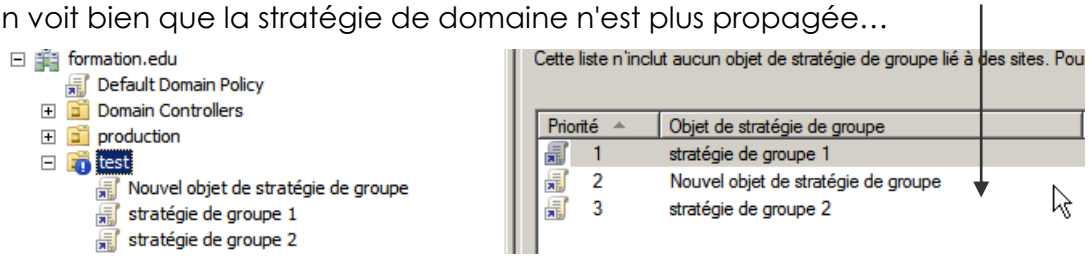


par exemple sur l'UO test

Cela se traduit par un Point d'exclamation !



Et l'on voit bien que la stratégie de domaine n'est plus propagée…



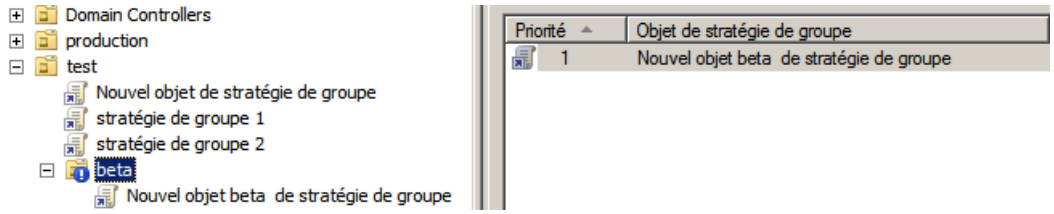
N.B: On ne peut pas bloquer l'héritage des stratégies de domaine pour l'UO prédéfinie Users… **par conséquent toutes les stratégies de domaine s'appliquent aussi aux utilisateurs, y compris l'administrateur de Domaine**

N.B: lorsque l'on bloque un héritage, on bloque cet héritage pour toutes les stratégies qui pourraient venir… sauf celles qui ont été spécifiées avec la mention "**Appliqué**" (cf chapitre suivant)

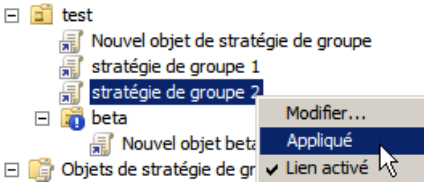
héritage - appliqué:

Il est possible dans une stratégie de spécifier que cette stratégie ne peut pas être bloquée par une stratégie ultérieure (on peut donc forcer l'héritage…)

Dans l'exemple on a bloqué l'héritage, au niveau de l'**UO** beta…

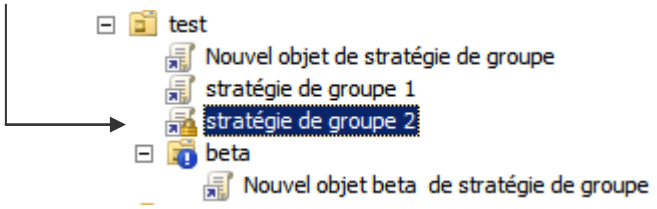


Mais on décide que la stratégie de groupe 2 doit s'appliquer tout le temps dans toutes les conditions…

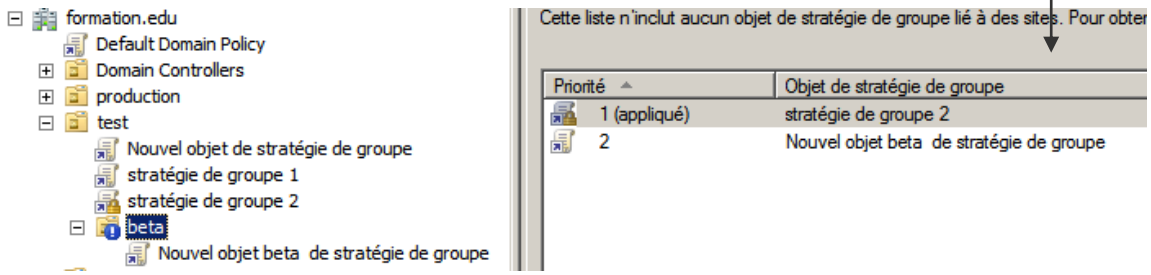


On se place dessus et on demande clic-droit **Appliqué**

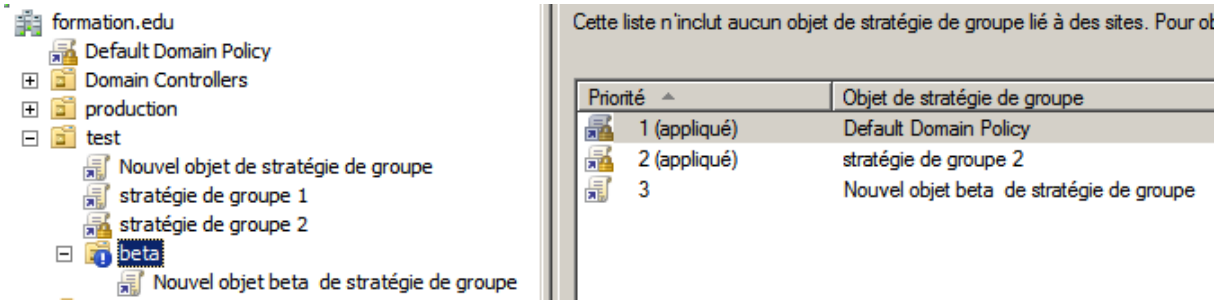
Cela se traduit par un Cadenas !



Et l''on voit bien que la stratégie est de nouveau propagée…



On peut procéder de même pour la **Default Domain Policy**…



GPO - MODELES D'ADMINISTRATION

Les Modèles présents

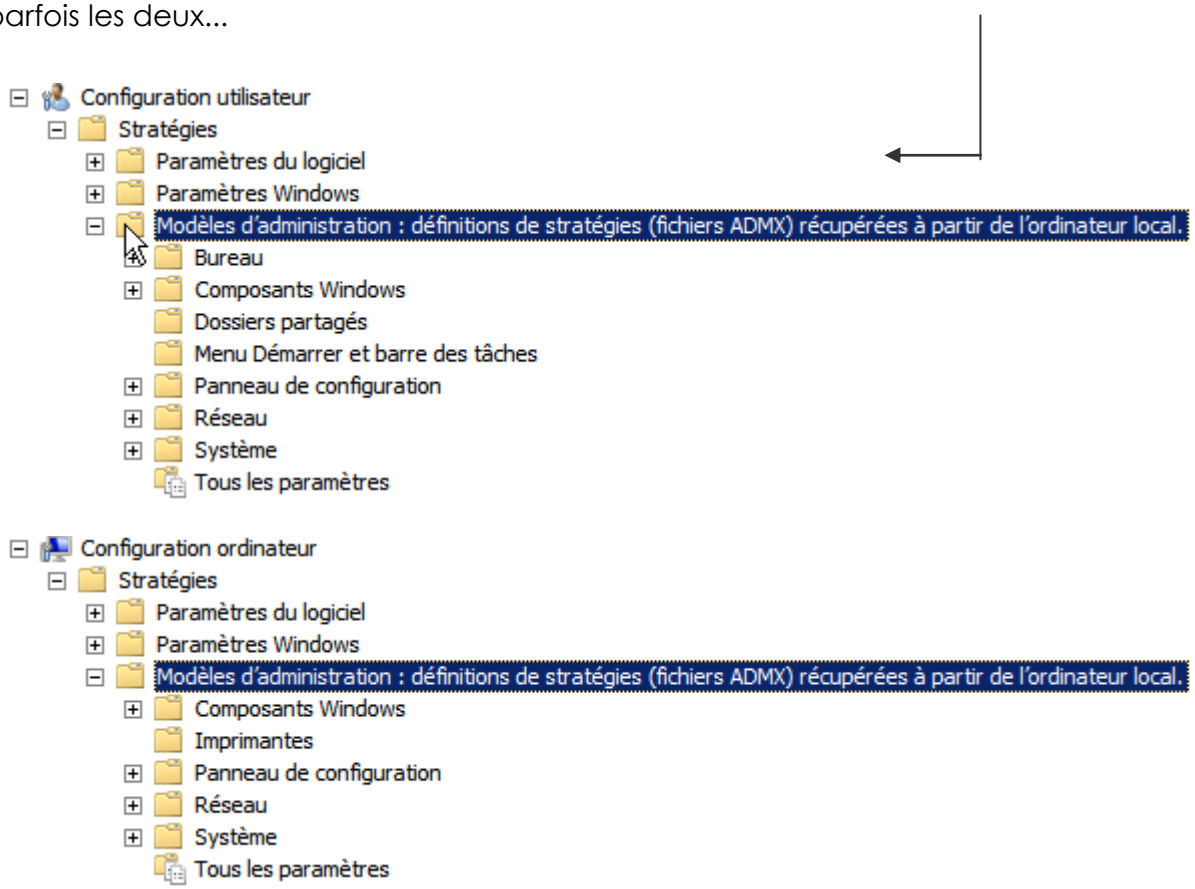
Maintenant que l'on a compris comment donner et faire appliquer des **GPO** sur des **UO** ou dans un domaine, on peut regarder de plus près ce qui leur est spécifique, par rapports aux sécurités locales.

Les premiers fichiers des modèles d'administration sous Windows Server 2003 (également appelés **fichiers ADM**) n'étaient du format XML

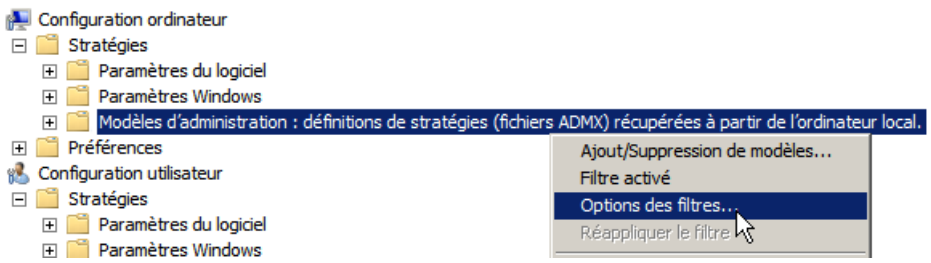
La version actuelle des fichiers des modèles d'administration depuis 2008 ou Seven (appelés **fichiers ADMX**) est créée à l'aide du format XML.

L'Éditeur **d'objets de stratégie de groupe** affiche ces paramètres sous le nœud **Modèles d'administration**

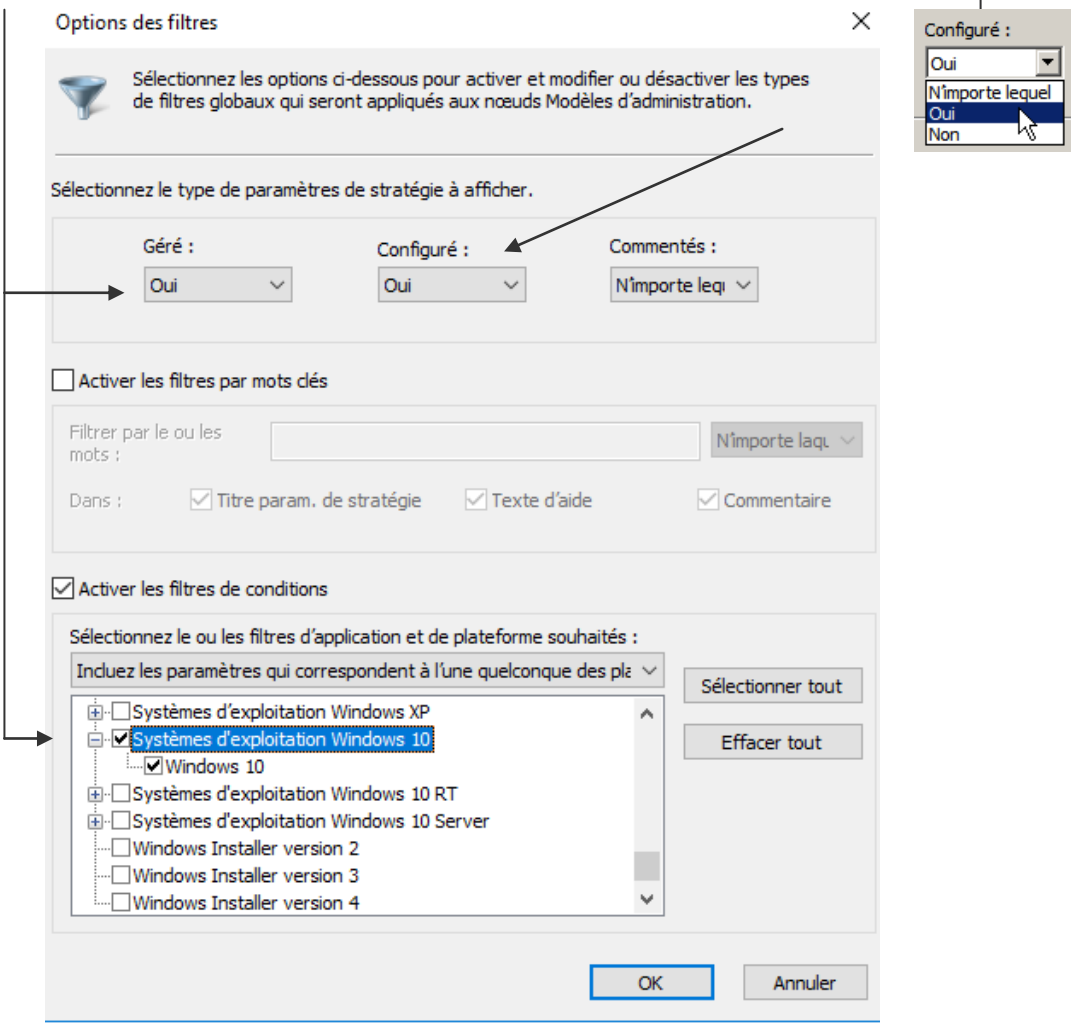
On a regroupé dans les **modèles d'administration**, toute une série de paramètres, disponibles tantôt uniquement pour la partie **ordinateur**, pour la partie **utilisateur**, ou parfois les deux...



Le choix est vaste, on peut **filtrer** les **modèles d'administration** avec **Options des filtres…**



Notamment pour cibler un **système**, ou garder que les valeurs **Configurées**



Rappels Méthodologie de mise en œuvre

Il est toujours conseillé de

- Ne jamais modifier las stratégies pré-définies de domaine et de contrôleurs de domaine 

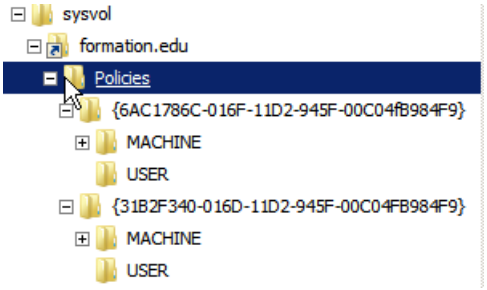
- Rarement définir des stratégies globales au domaine, mais toujours sur des UO précises
- donner des noms aux stratégies par rapport à leur action, et non pas par rapport aux objets sur lesquelles elles s'appliquent
- d'avoir une UO de test, dans laquelle on va faire glisser un compte ordinateur et ou un compte utilisateur, ce qui limite les risques à ce seul poste, ce seul utilisateur
- Le compte administrateur (ou son double) doit être stocké dans une UO séparée, avec un héritage bloqué permettant de le protéger…

Stockage des Modèles de GPO – sur chaque DC

Regardons de plus près la gestion de stockage des Modèle de ces GPO.

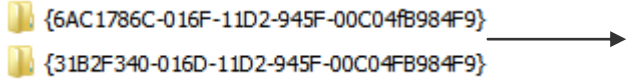
N.B : Ne pas confondre les **GPO** et les **modèles de GPO** à partir desquelles elles sont crées

On l'a déjà dit, les **GPO** sont stockées par défaut **physiquement** dans le dossier **%Windir%\sysvol\sysvol*domaine*\Policies** dans lequel on retrouvera au minimum par exemple nos 2 stratégies de base

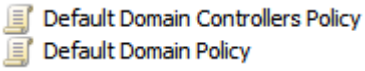


Default Domain Controllers Policy

Default Domain Policy



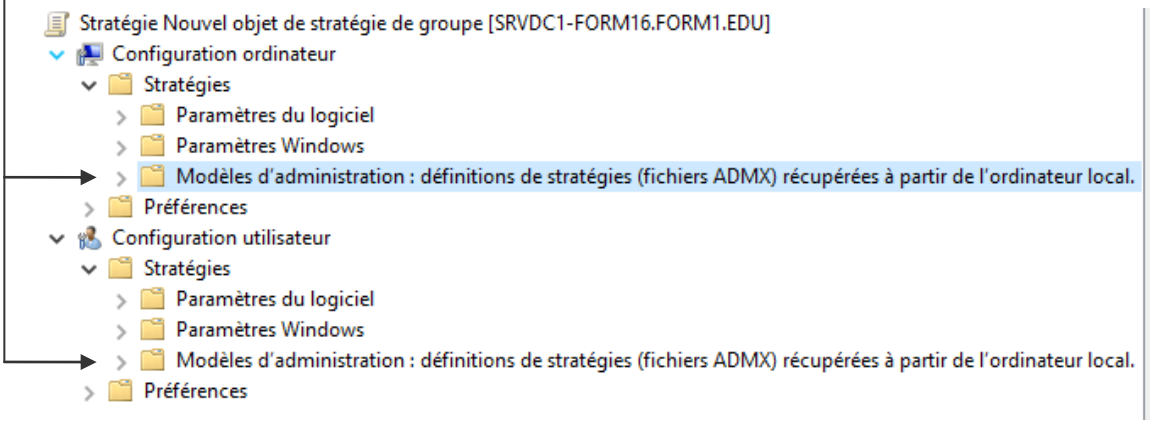
Correspondant à



Elles sont stockées sur chaque **Contrôleur de domaine**, et elles sont ensuite répliquées entre tous les **CD.**

Par contre les **modèles de GPO**, à partir desquels nos GPO sont construites, sont stockés eux dans le dossier **C:\Windows\Policydefinitions**

N.B : On peut se rendre compte lorsque l'on modifie dans une **GPO** un réglage en provenance d'un **modèle d'administration**, par l'apparition de la mention « **définition de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local »**



Pourquoi cela peut poser probleme :

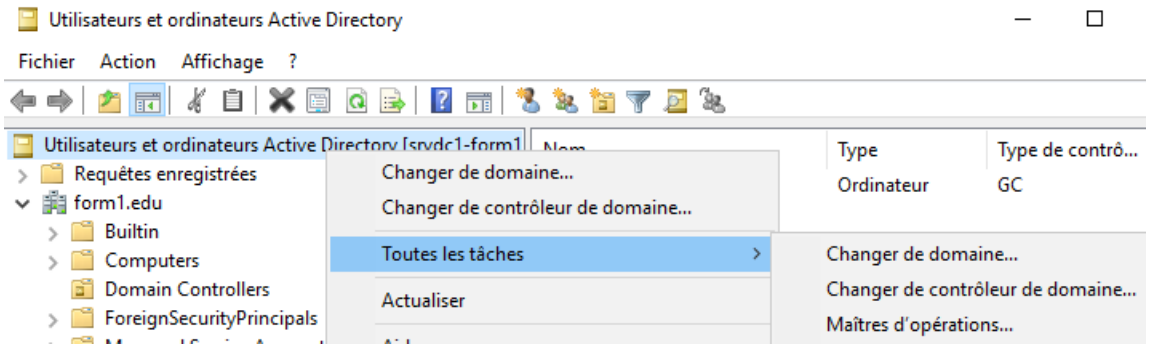
Soit 2 DC dans un Domaine, **DC1** et **DC2**

Si on ajoute un modèle de **GPO** sur un **DC1** , et que l'on crée une **GPO** à partir de ce modèle, alors si le nouveau modèle n'existe pas sur le **DC2** on ne pourra modifier cette **GPO** que depuis la console **gestion des stratégie de groupe** présente sur le **DC1**,

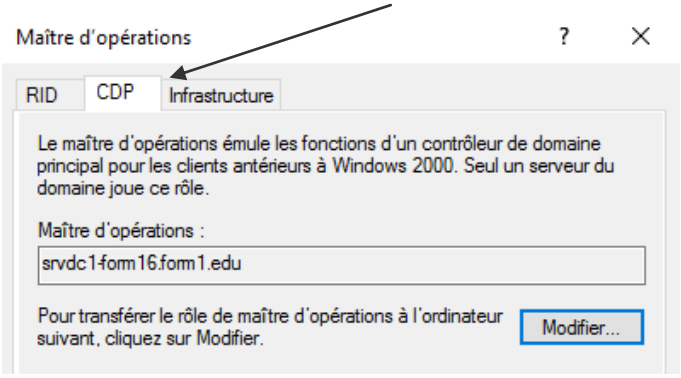
Pour centraliser le stockage des **modèle de GPO** il faut et suffit de créer un dossier supplémentaire dans le dossier partagé **Sysvol**, sur le **DC** ayant le rôle de **PDC.** Ce dossier doit s'appeler obligatoirement **Policydefinitions**

Trouver le DC ayant le rôle PDC

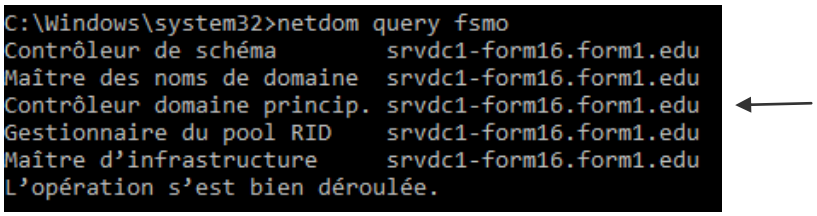
Dans **Utilisateur et ordinateurs Active Directory** on demande via clic droit **maître d'opérations**…



Et on regarde qui est **CDP Controlleur de domaine Principal**

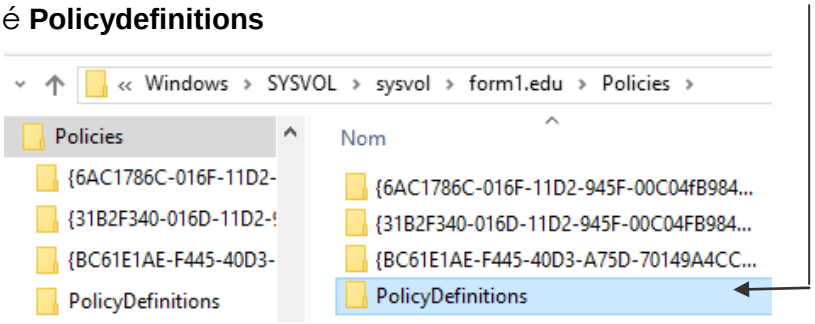


Ou bien on tape la commande **Netdom query fsmo** pour trouver le **Controlleur de domaine Principal**



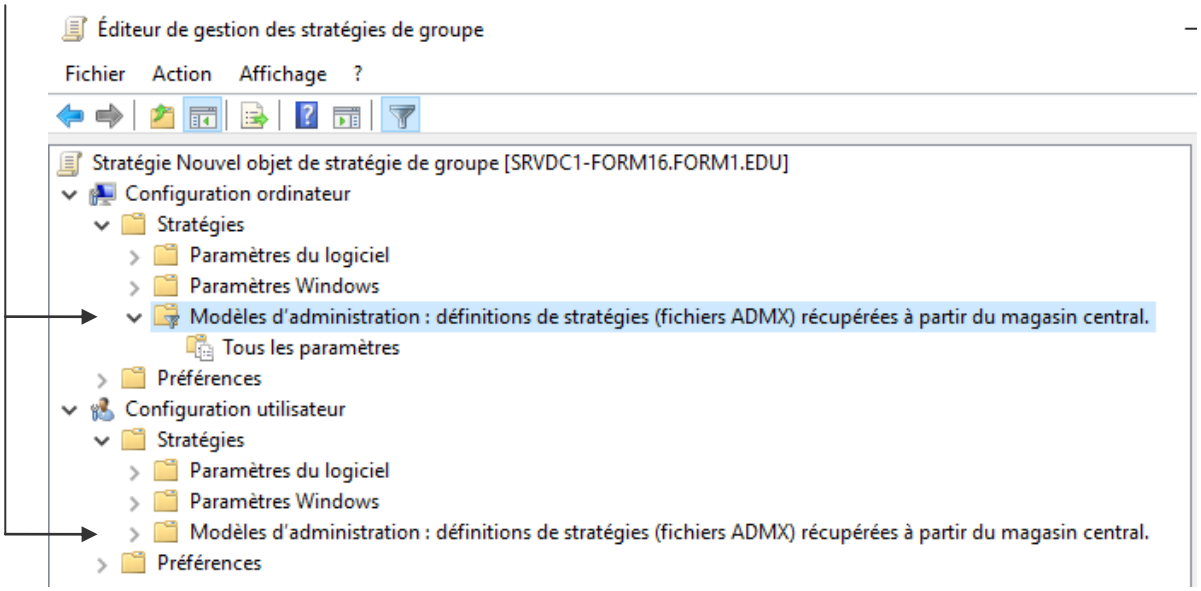
Création du dossier PolicyDefinitions

Dans le dossier **%Windir%\sysvol\sysvol***domaine***\Policies** on se crée un dossier nommé **Policydefinitions**



Après un petit délai, les **Modèles de GPO** sont désormais automatiquement pris dans le **magasin central**, et non plus dans le dossier de stockage local de l'ordinateur

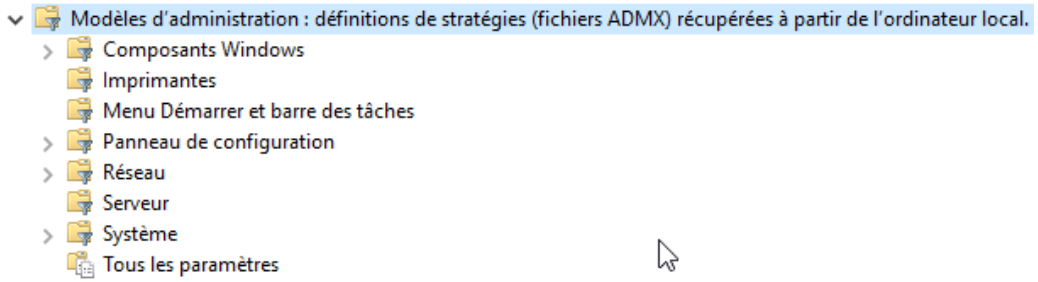
N.B : On peut se rendre compte lorsque l'on modifie dans une **GPO** un réglage en provenance d'un **modèle d'administration**, par l'apparition de la mention « **définition de stratégies (fichiers ADMX) récupérées à partir du magasin central »**



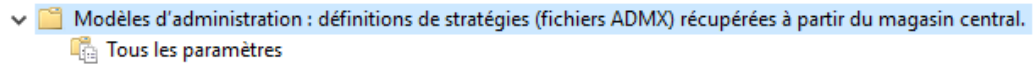
Copier les modèles de GPO

Lorsque l'on met en oeuvre le **Magasin Central**, alors on s'aperçoit que les modèles de GPO à disposition, sont… rares ! Forcément, le dossier est vide !

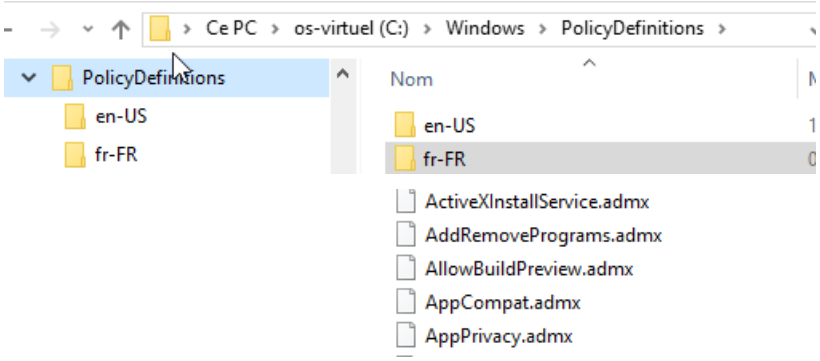
Au lieu de tous les modèles (anciennement)



On a maintenant 0 modèles, dans le **Magasin Central**…



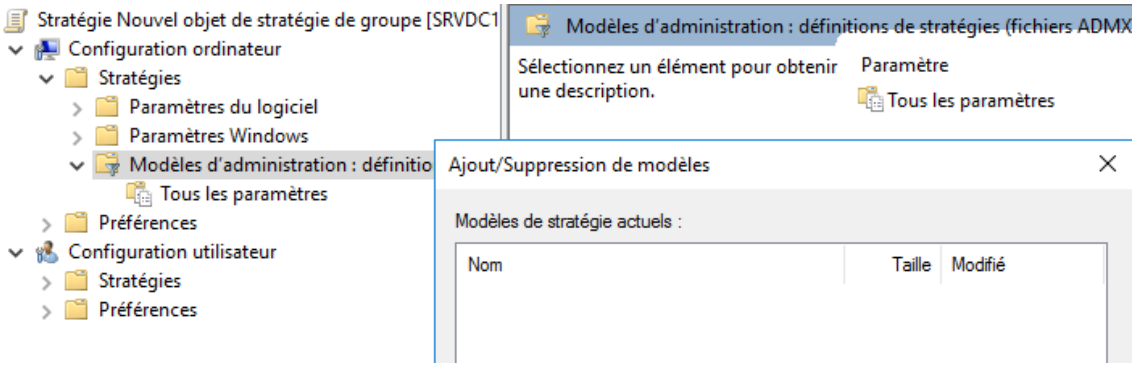
Pour copier nos **Modèles ADMX** il suffit de copier la totalité de l'ancien répertoire de stockage local **C:\Windows\Policydefinitions** dans notre nouveau magasin **%Windir%\sysvol\sysvol***domaine***\Policies\Policydefinitions**



Ajout suppression des Modèles de GPO

- Pour les nouveaux Modèles a base de **fichier ADMX** il faut copier les fichiers dans le dossier de stockage, donc soit
  - le dossier local de la machine
  - le magasin central dans sysvol

- Pour les anciens Modèle a base de **fichier ADM**, on pouvait demander via un clic droit sur la console, **Modèle D'administration / Ajout Suppression de modèles…**



Dans l'exemple ici aucun modèle n'apparait… car on n'a pas d'anciens Modèle ADM

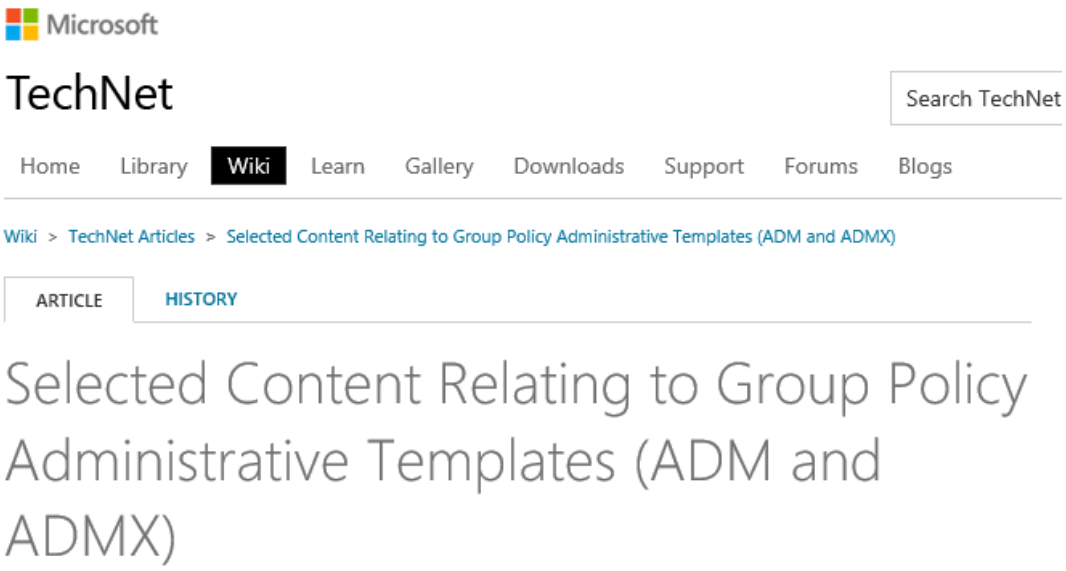
Trouver des Modèles de GPO – technet WIKI

On peut trouver des modèles un peu… partout

L'idée est de faire le bon choix sur la « qualité » des templates, et à ce titre **technet** semble une bonne solution

1 Sélection - Technet WIKI

Faire une recherche sur google avec le titre du WIKI



Avec un choix sélectif, mais vaste !

NB: as of 2015/2016, I've noticed that recently released Security Updates or Cumulative Updates, for Windows and/or Internet Explorer, are shipping updated ADMX/ADML files e.g. inetres.admx/adml for IE. So, if you can't find the setting you're looking for in the downloads section, you might need to grab the latest CU for Windows or IE to get the freshest ADMX/ADML. This concept also seems to apply to Win10 upgrades (e.g. 1507 -> 1511 -> 1607)...

ADM and ADMX Downloads for Windows
Administrative Templates (.admx) for Windows 10 Fall Creators Update (1709)
Administrative Templates (.admx) for Windows 10 Creators Update (1703)
Administrative Templates (.admx) for Windows 10 1607 and Windows Server 2016
Administrative Templates (.admx) for Windows 10 1507 and 1511
Administrative Templates (.admx) for Windows 8.1 Update and Windows Server 2012 R2 Update
Administrative Templates (.admx) for Windows 8.1 and Windows Server 2012 R2
Administrative Templates (.admx) for Windows 8 and Windows Server 2012
Administrative Templates (ADMX) for Windows Server 2008 R2 and Windows 7
Administrative Templates (ADMX) for Windows Server 2008
Administrative Templates (.admx) for Windows Vista
Group Policy ADM Files

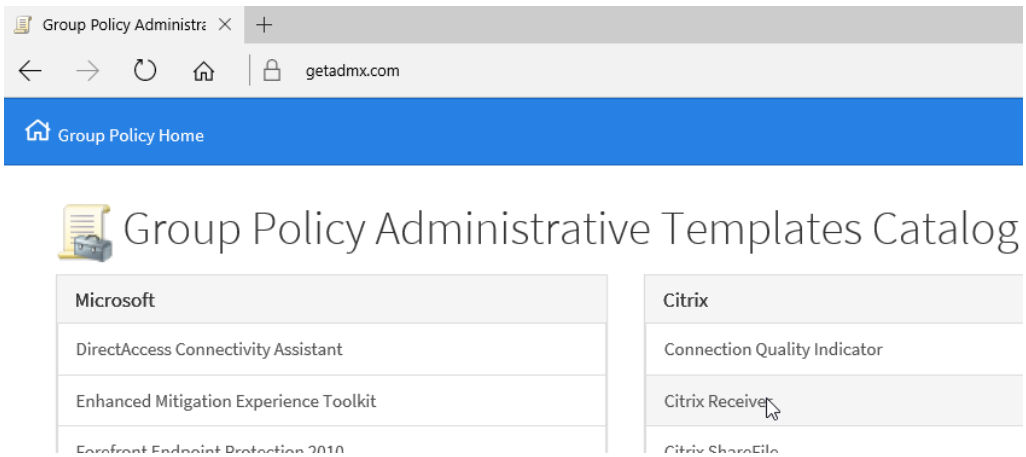
ADM and ADMX Downloads for MS Internet Explorer
Administrative Templates for Internet Explorer 11 This page provides the Group Policy Administrative Template files for Internet Explorer 11.
Administrative Templates for Windows Internet Explorer 10 This page provides the Group Policy Administrative Template files for Windows Internet Explorer 10. **** Warning: IE10 deprecates/removes the IEM methods.** Refer: AskIEBlog
Administrative Templates for Windows Internet Explorer 9 This page provides the Group Policy Administrative Template files for Windows Internet Explorer 9
Administrative Templates for Internet Explorer 7 for Windows This page provides the Group Policy Administrative Template file for Internet Explorer 7 for Windows.

Blocker Toolkits for MS Internet Explorer
Toolkit to Disable Automatic Delivery of Internet Explorer 11 The Internet Explorer 11 Blocker Toolkit enables users to disable automatic delivery of Internet Explorer 11 as an important class update via Automatic Updates (AU) feature of Windows Update (WU).
Toolkit to Disable Automatic Delivery of Internet Explorer 10
Toolkit to Disable Automatic Delivery of Internet Explorer 9
Toolkit to Disable Automatic Delivery of Internet Explorer 8
Toolkit to Disable Automatic Delivery of Internet Explorer 7

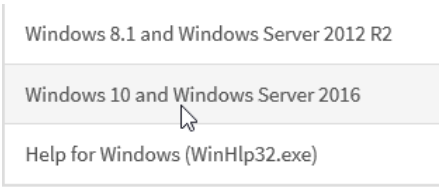
ADM and ADMX Downloads for MS Office
Office 2016 Administrative Template files (ADMX/ADML) and Office Customization Tool This download includes Group Policy Administrative Template (ADMX/ADML) and Office Customization Tool (OPAX/OPAL) files for Microsoft Office 2016.
Office 2013 Administrative Template files (ADMX/ADML) and Office Customization Tool This download includes Group Policy Administrative Template (ADMX/ADML) and Office Customization Tool (OPAX/OPAL) files for Microsoft Office 2013.
Office 2013 Help Files: Office Fluent User Interface Control Identifiers This download details the ControlIDs needed for OFF2013, if you want to disable specific UI controls, buttons, menu items, via a registry policy.

1 Liste exhaustive - getadmx.com

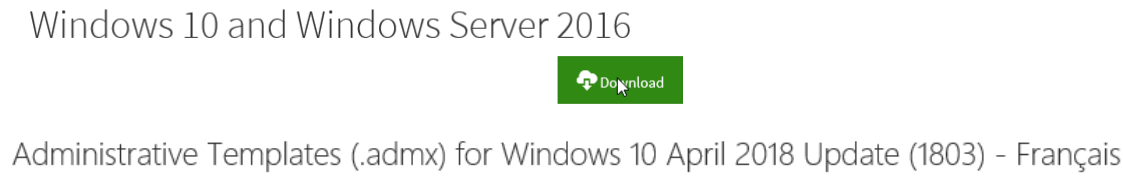
Un autre moyen de trouver des Templates, c'est le site **getadmx.com**

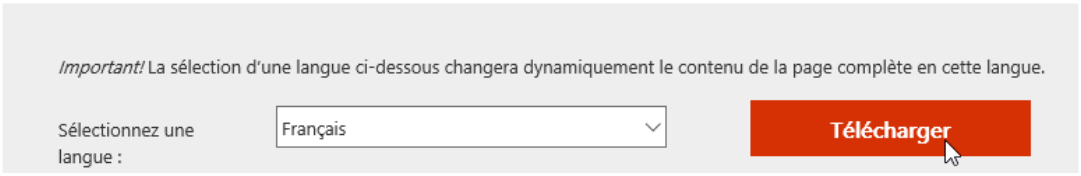


Dans lequel on va trouver soit le téléchargement possible d'un templates ADMX qui nous interesse, par exemple Windows 10



Il n'y a plus qu'à demander le téléchargement, qui nous renverra en fait sur le site de Microsoft.



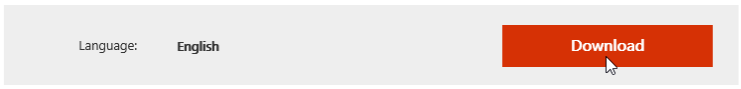


N.B: il est possible en ligne de parcours latotalité des composants, et de trouver la documentation correspondante…en anglais ET en français et de trouver des templates autres que Microsoft !

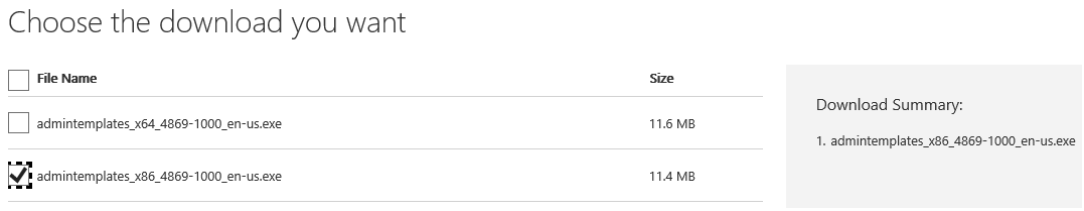
Télécharger et installer un Modèles de GPO – office 2013

Essayons de télécharger et installer un templates pour office 2013

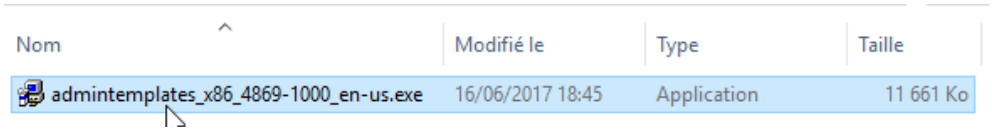
Office 2013 Administrative Template files (ADMX/ADML) and Office Customization Tool



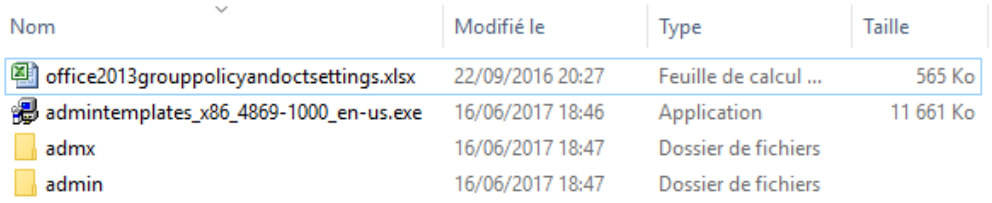
Et on télécharge un fichier (la version pour office x86)



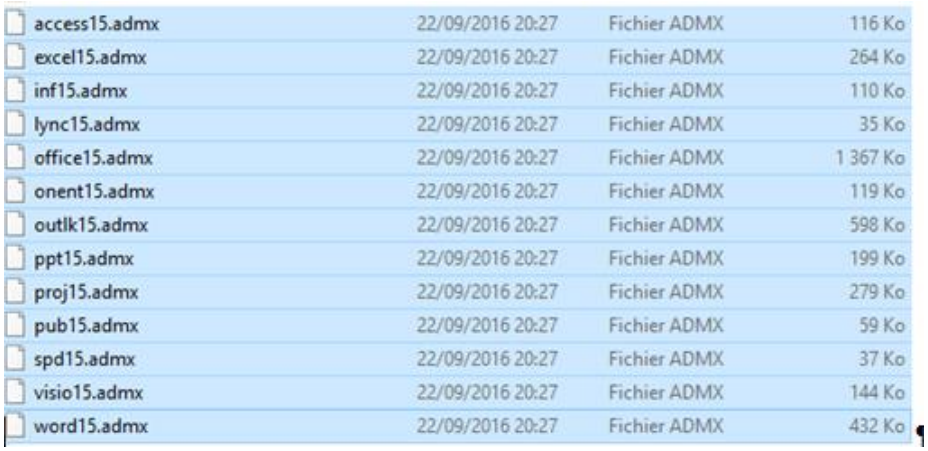
Il faut le désarchiver, et l'executant



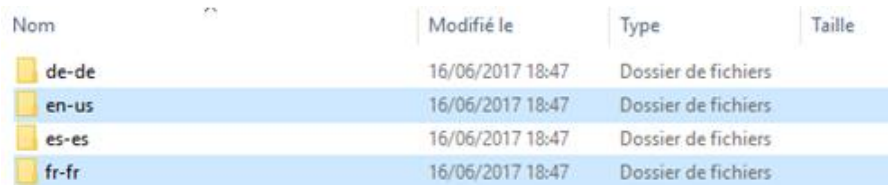
Pour obtenir



Dans le dossier **admx**, qui nous intéresse on trouve tous les modèles **admx** et les

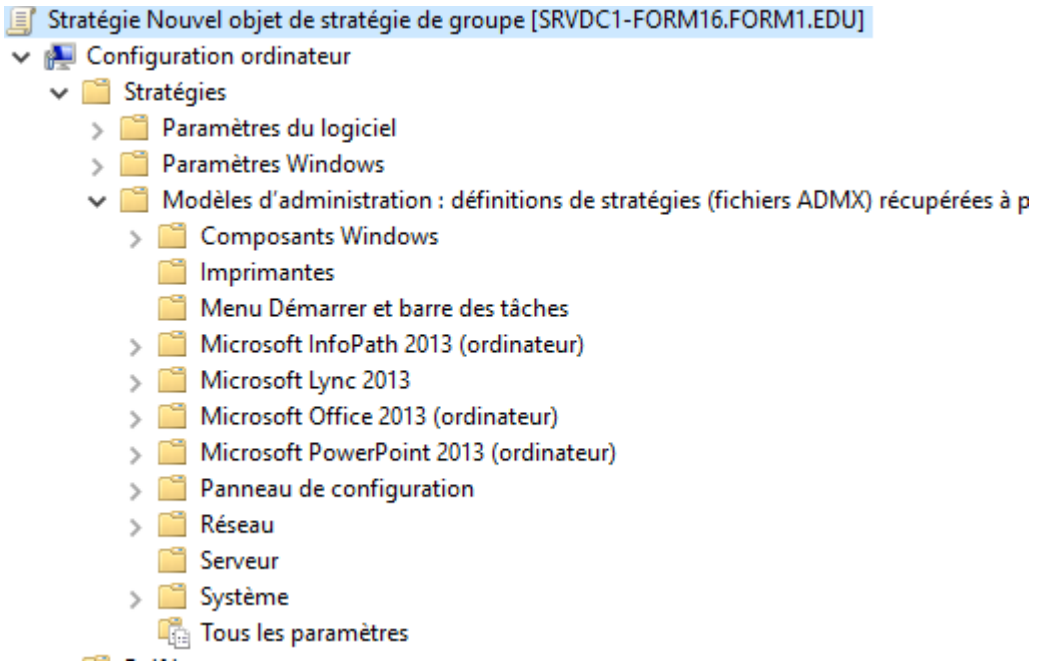


dossiers de langue **fr-fr** et **en-us**

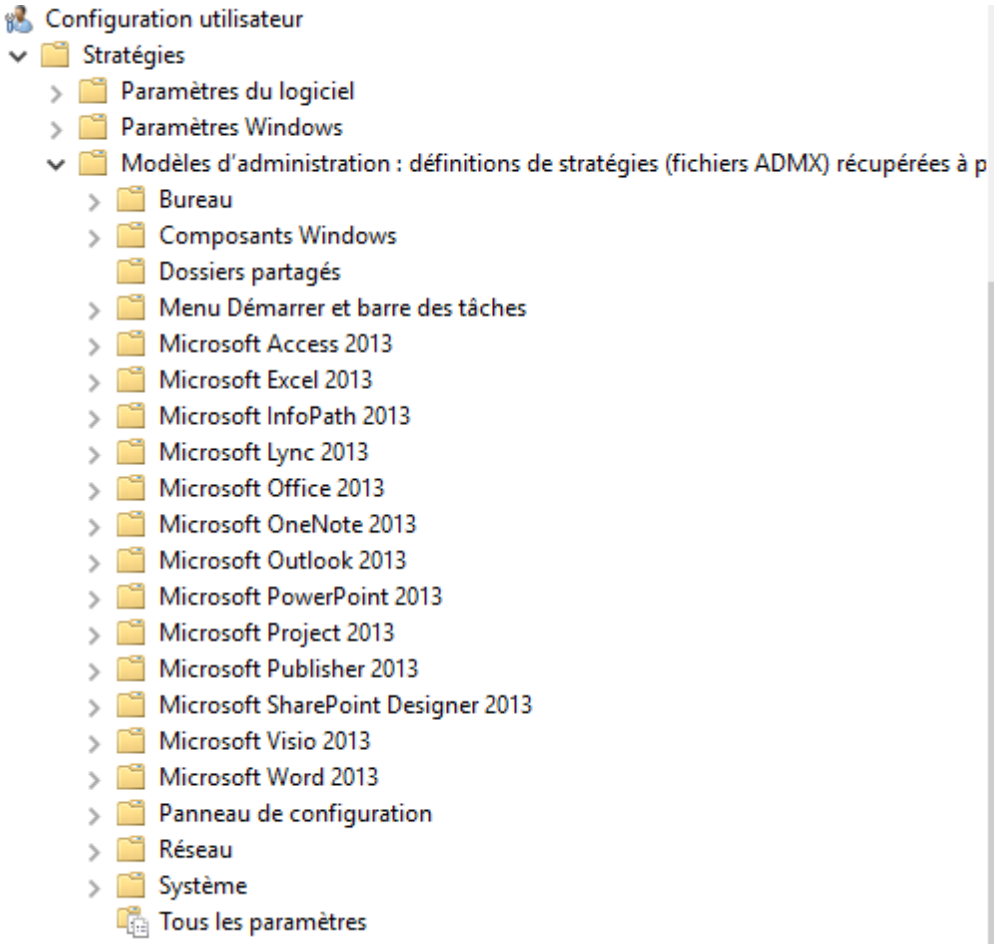


Il faut copier tout cela dans notre **Magasin Central**

Du coup on aura désormais



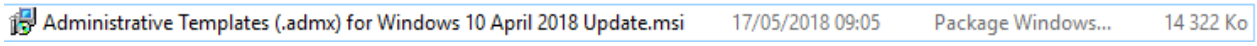
Et



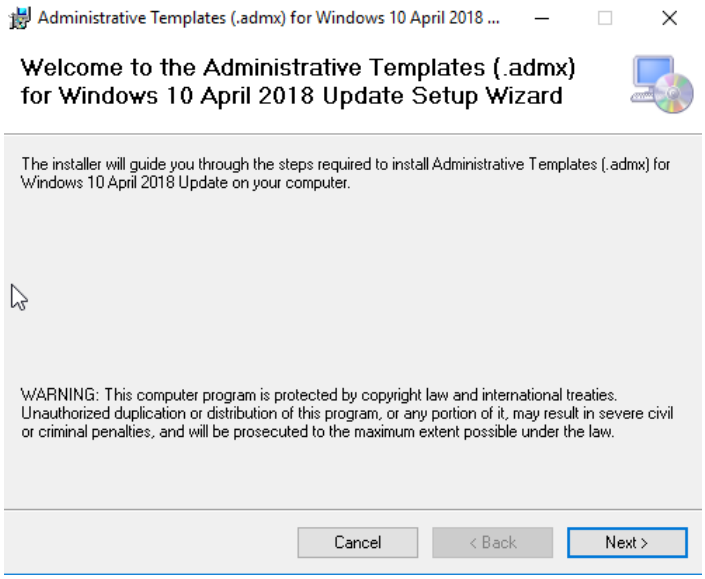
N.B : Pour désinstaller ces GPO il suffit de les supprimer du **Magasin Central**

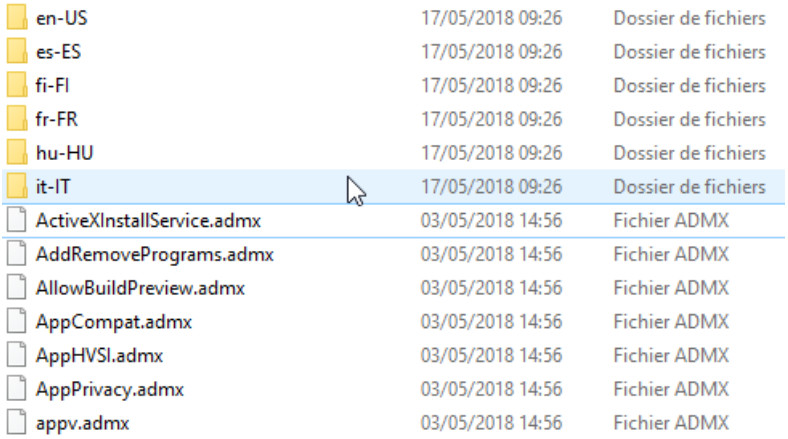
Télécharger et installer un Modèles de GPO – Windows 10 v1803

Essayons de télécharger et installer un **templates** pour **Windows 10 v1803** sur le site **getadmx.com**. Il faut le désarchiver, et l'executant



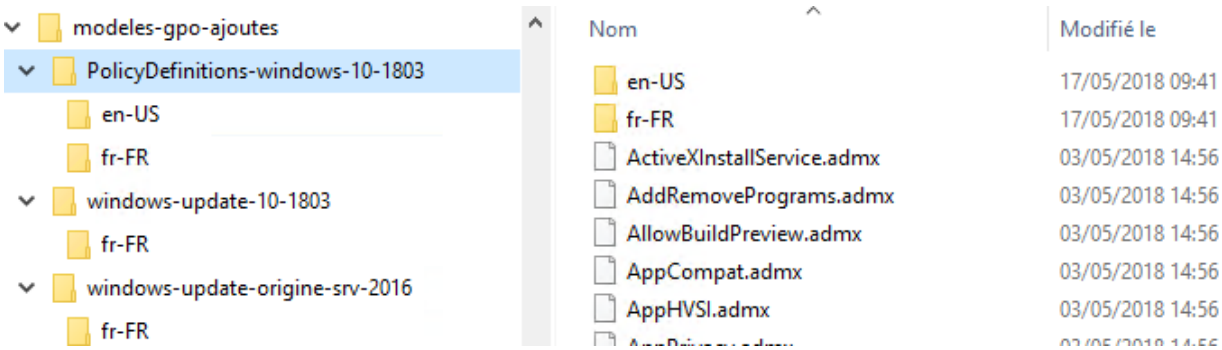
Pour obtenir





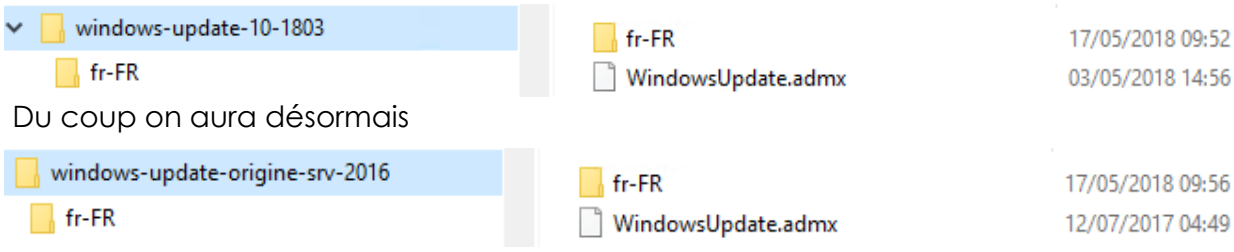
Dans le dossier **de désarchivage** on trouve tous les modèles **admx** et les dossiers de langue (au minimum) **fr-fr** et **en-us**

Il faut copier soit tout cela, soit uniquement ce qui nous intéresse dans notre **Magasin Central**



L'idée est que par rapport à un ebsemble de mises à jour disponibles, comme ici à la sortie d'une nouvelle version de l'OS windows 10 v1803, on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx…

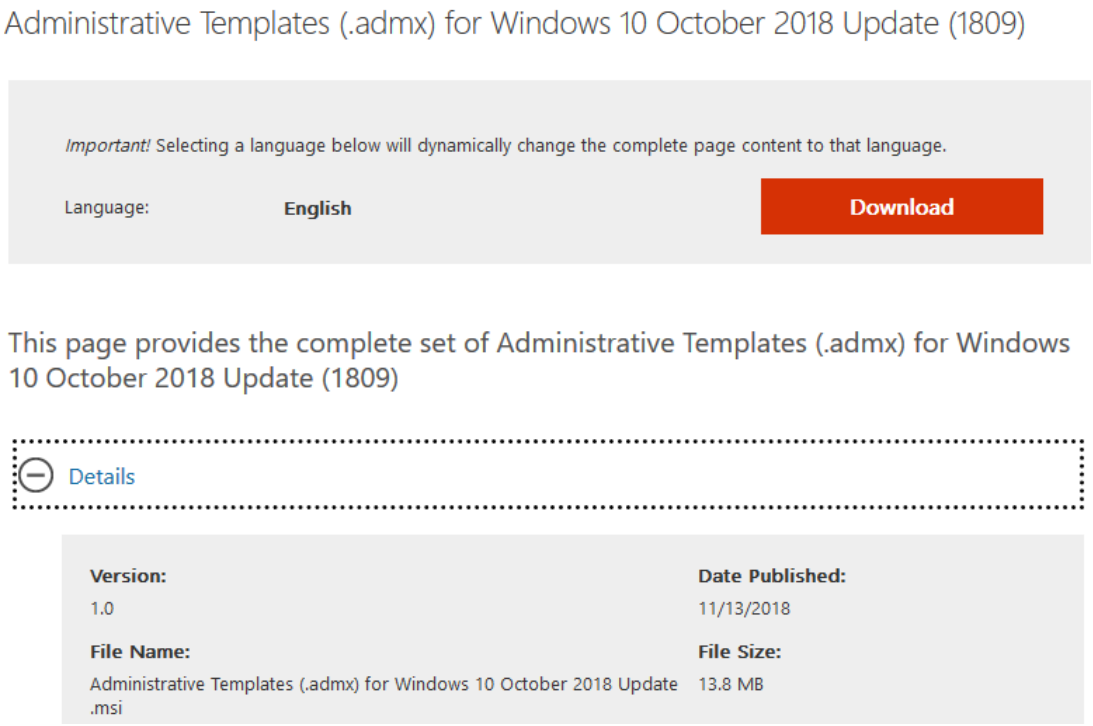
On remplace donc juste un admx et son fichier de langue, tout en gardant l'ancien…



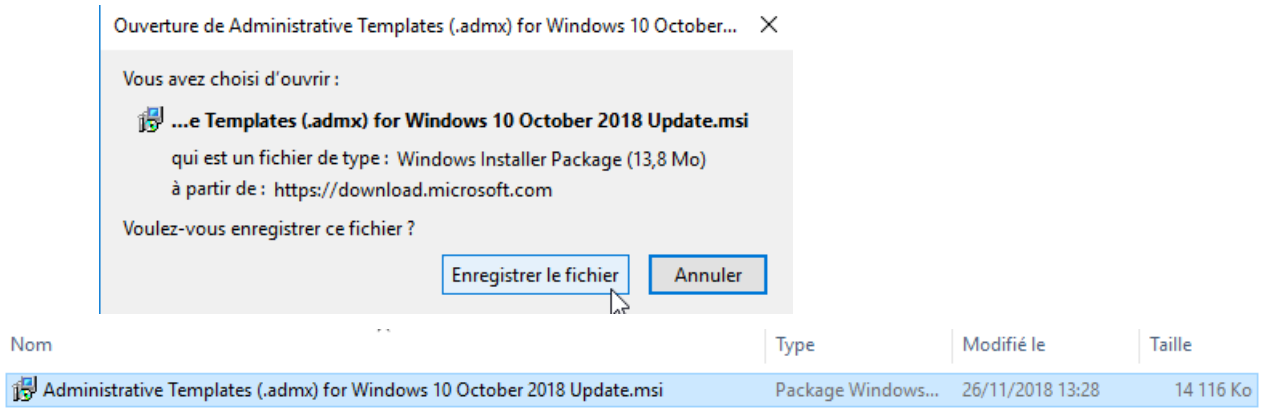
Du coup on aura désormais

Télécharger et installer un Modèles de GPO – Windows 10 v1809

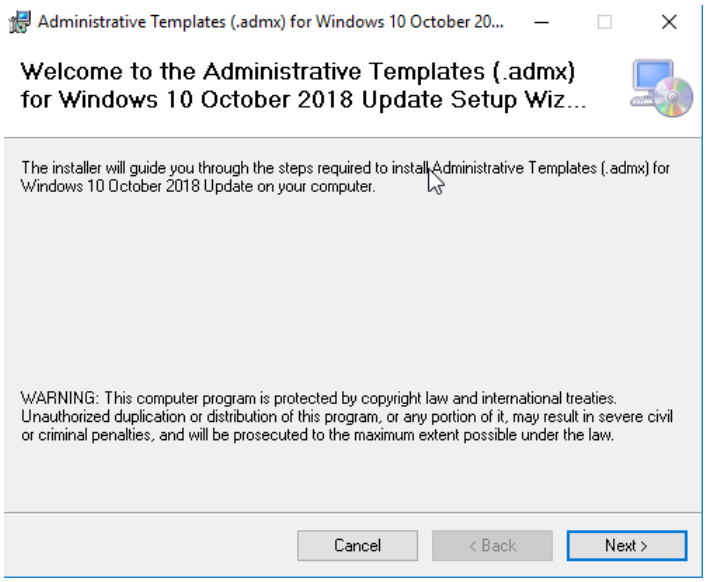
Essayons de télécharger et installer un **templates** pour **Windows 10 v1809 depuis le site de microsoft**

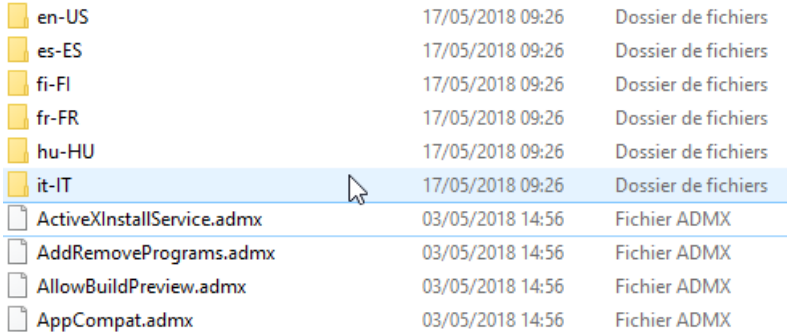


On télécharge le fichier



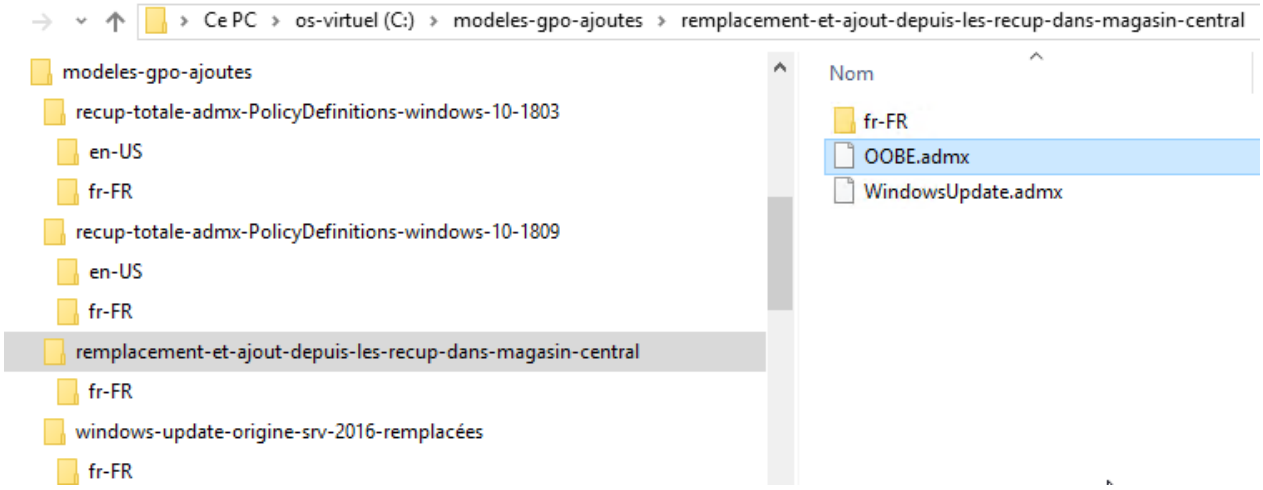
Et on l'installe





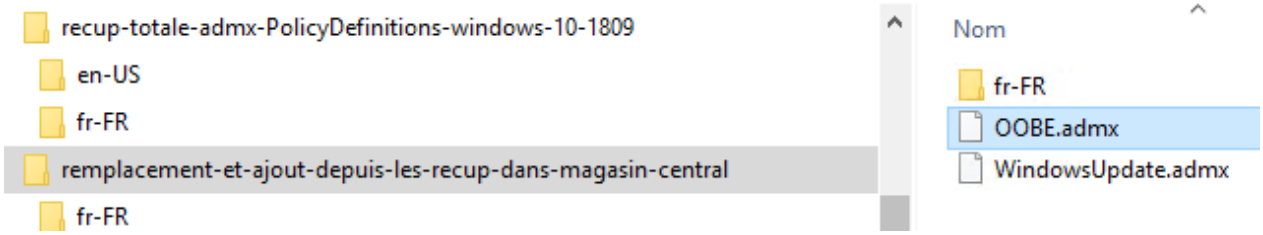
Dans le dossier **de désarchivage** on trouve tous les modèles **admx** et les dossiers de langue (au minimum) **fr-fr** et **en-us**

Il faut copier soit tout cela, soit uniquement ce qui nous intéresse dans notre **Magasin Central**



L'idée est que par rapport à un ebsemble de mises à jour disponibles, comme ici à la sortie d'une nouvelle version de l'OS windows 10 v1803, on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx…

On remplace donc juste un admx et son fichier de langue, tout en gardant l'ancien…



FILTRES WMI

Objectifs des Filtres WMI sur les GPO

L'idée est de pouvoir moduler l'application d'un **GPO** par un certain nombre d'interrogation portant sur des primitives accessible via **WMI**.

La pricédure se fait en 2 temps :

- On crée paramètre dans un premier temps son **filtre WMI**
- , puis on l'applique sur la **GPO**

Les filtres les plus utilisés chez les clients permettent de déterminer entre autres la version de Windows installée sur l'ordinateur, le type de PC (Portable/Poste fixe). le modèle/marque du PC…

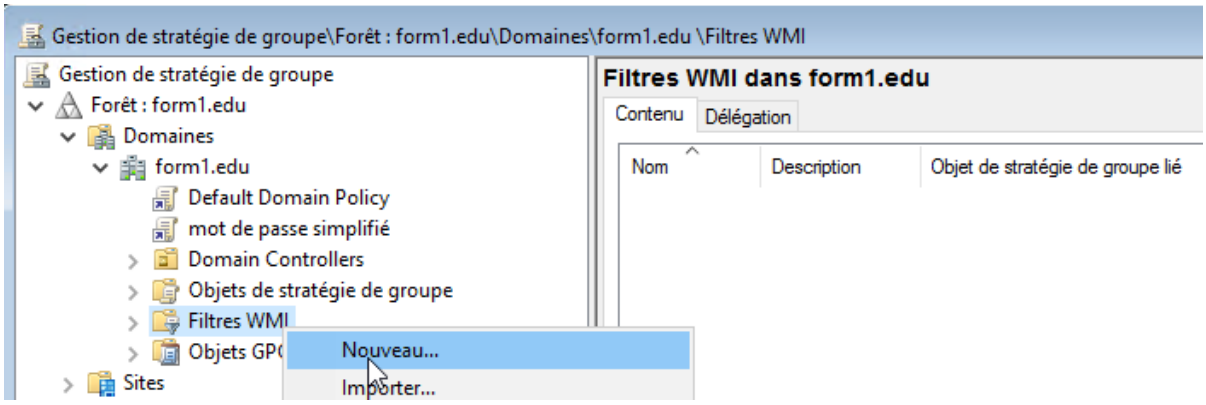
Cependant, l'utilisation de **filtres WMI** sur les **GPO** va impacter les performances au démarrage. En effet, l'ordinateur doit évaluer si le filtre est vrai ou faux. En fonction du contenu de la requête WQL, l'évaluation du filtre prend plus de temps, ce qui retarde le processus d'application des GPOs. (le service **Client Stratégie de groupe** doit attendre que le service **WinMgmt** démarre et initialise la couche **WMI**. Une fois que la couche **WMI** est initialisée, un processus **WMIPrvSe** est créé et la requête est évaluée.)

N.B : Il est également possible de filtrer les **Préférences** avec le **ciblage** qui utilise des **API** natives de **Windows** et n'utilise pas de **WMI** (sauf si la condition du ciblage est effectuée avec une requête WQL). Les performances de ciblage sont meilleures !

Si vous utilisez des Préférences, il est recommandé de choisir un ciblage au lieu d'utiliser un filtre WMI sur l'objet GPO.

Création du filtre WMI

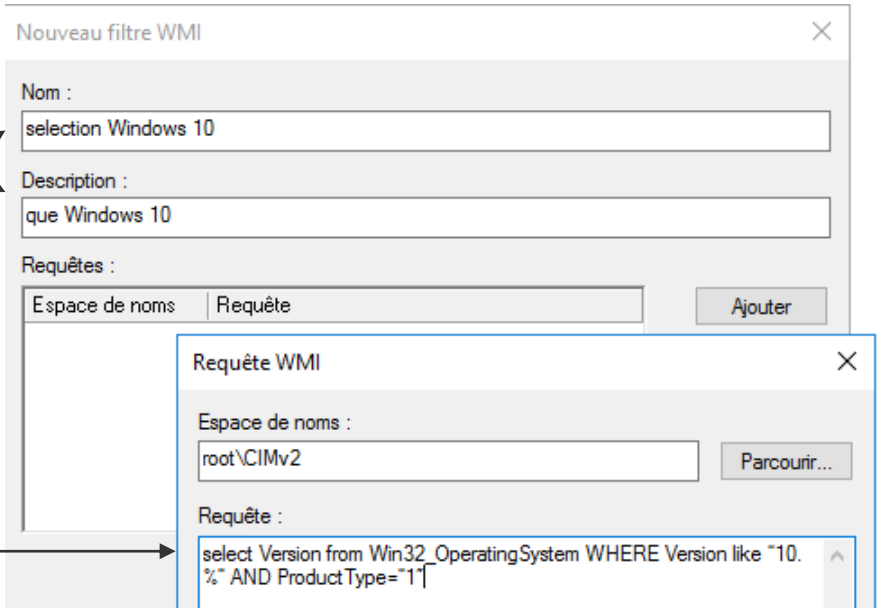
Dans la console **Gestion des stratégies de groupe**, on se place sur **Filtres WMI** et on demande via clic droit / **Nouveau…**



Dans la boite de dialogue, il faut

nommer le script,

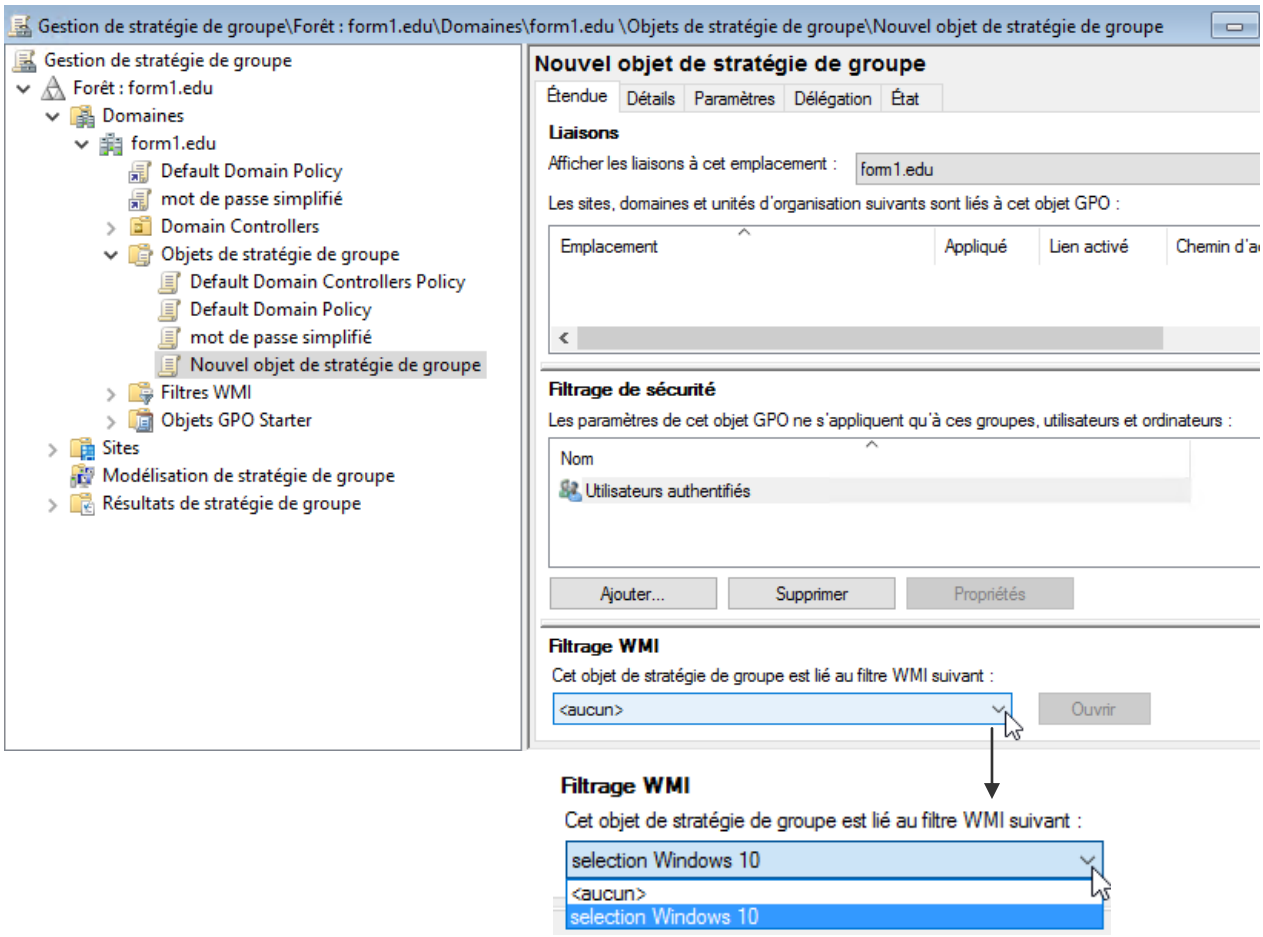
et surtout écrire la requête qui correspondra à notre recherche



select Version from Win32_OperatingSystem WHERE Version like “10.%” AND ProductType=1”

Lier la GPO et le filtre WMI

Il suffit maintenant de seléctionner notre GPO et dans la partie Filtrage WMI de choisir le filtre à appliquer parmis ceux disponibles



N.B : le **filtrage WMI** s'applique à une **GPO**, et reste identique quelles que soient les liens posés sur les differentes UO

Autrement dit on ne peut pas selon les liens GPO-UO choisir en plus le filtre WMI

Test wmi via powershell

GPO WMI filters can get screwed up when edited. Quick way of testing a WMI filter is available using Powershell:

1.Grab the GPO WMI filter from GPMC and put it into clipboard

2.in Powershell console: gwmi -Query 'Paste your WMI filter here'

gwmi -Query 'SELECT ProductType, CSName FROM Win32_OperatingSystem WHERE (ProductType = "1") AND Not CSName = "CB002021")'

When any results are returned WMI filter evaluates to $true (GPO applies), else $false (GPO does not aplly)

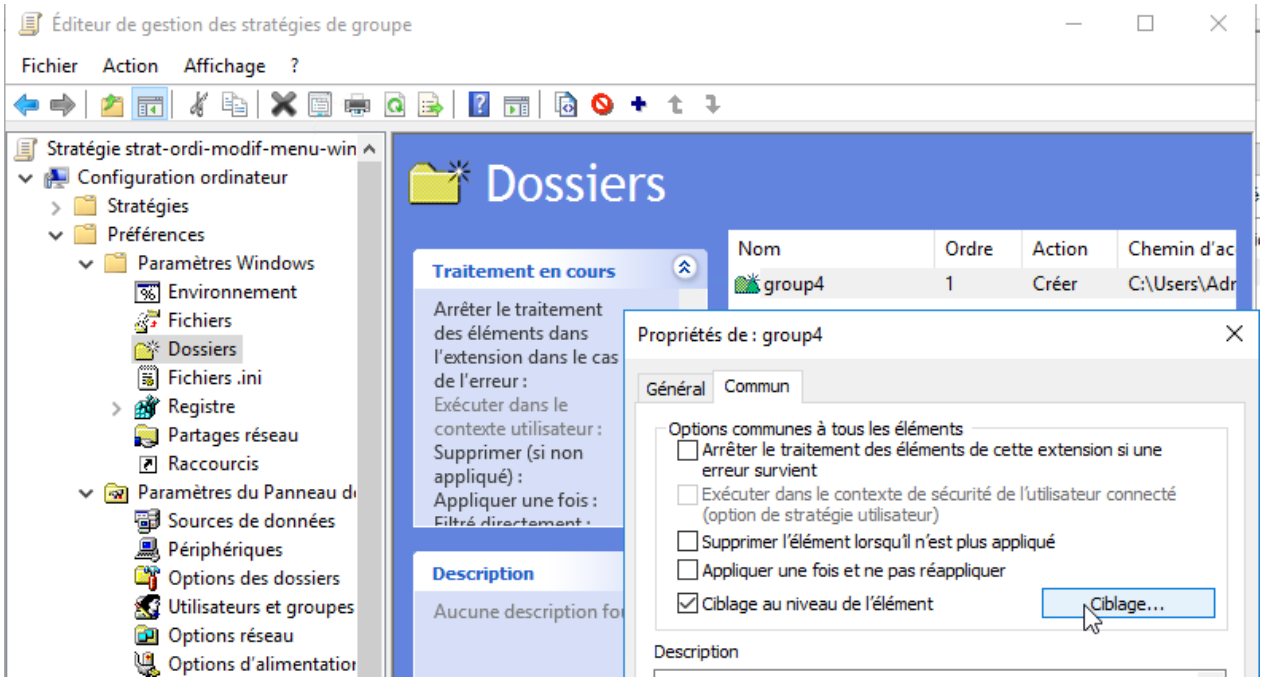
Don't forget that you get the luxury to test against multiple computer just by adding the -Computername parameter:

gwmi -Query 'SELECT ProductType, CSName FROM Win32_OperatingSystem WHERE (ProductType = "1") AND Not CSName = "CB002021")' -Computername PC01,PC02

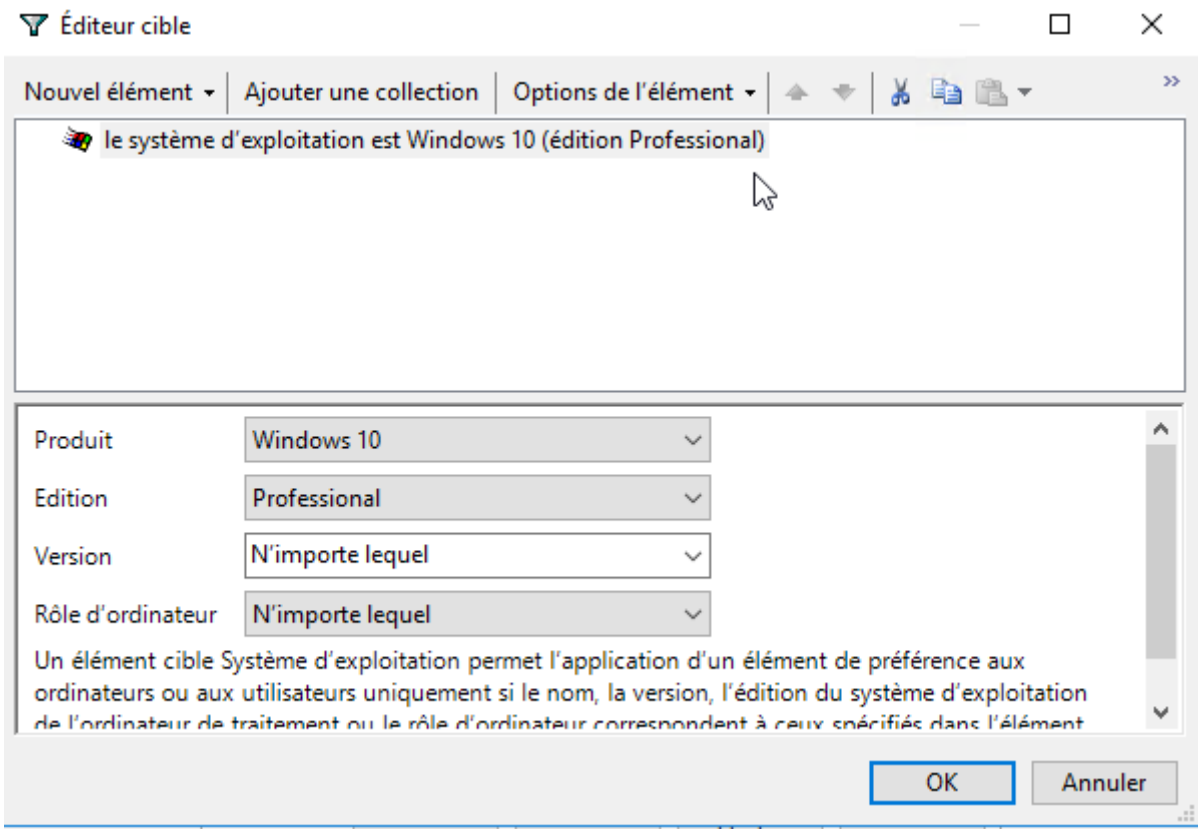
Ciblage de préférence

Si on a une préférence, il est possible lorsque l'on est sur la préférence, de demander les propriétés, puis onglet commun, Ciblage au niveau de l'élément

Cela permet de choisir le filtre à appliquer parmis ceux disponibles



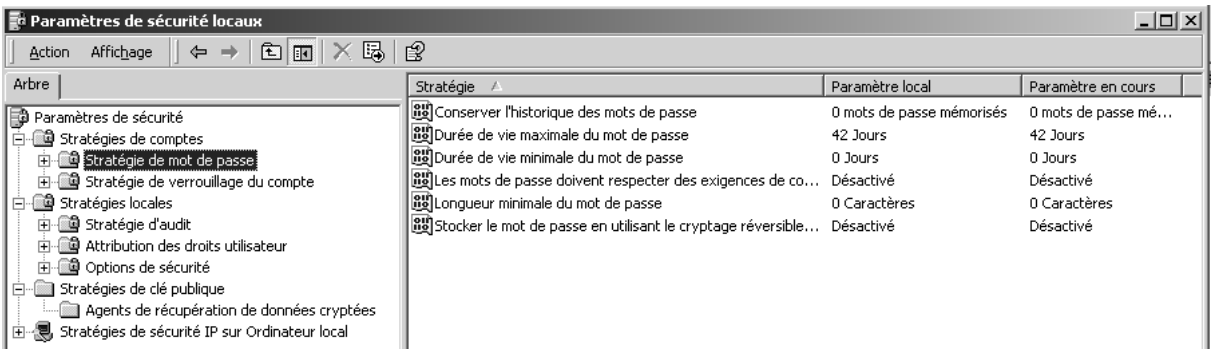
Par exemple


Éditeur cible
Nouvel élément
Ajouter une collection
Options de l'élément
le système d'exploitation est Windows 10 (édition Professional)
Produit
Windows 10
Edition
Professional
Version
N'importe lequel
Rôle d'ordinateur
N'importe lequel
Un élément cible Système d'exploitation permet l'application d'un élément de préférence aux ordinateurs ou aux utilisateurs uniquement si le nom, la version, l'édition du système d'exploitation
OK
Annuler

Secpol.msc - Rappel stratégies locales et GPo de domaine

Les stratégies locales se lancent depuis les outils d'administration, à travers **stratégie de sécurité locale**

ce qui donne ensuite accès aux paramètres suivants :



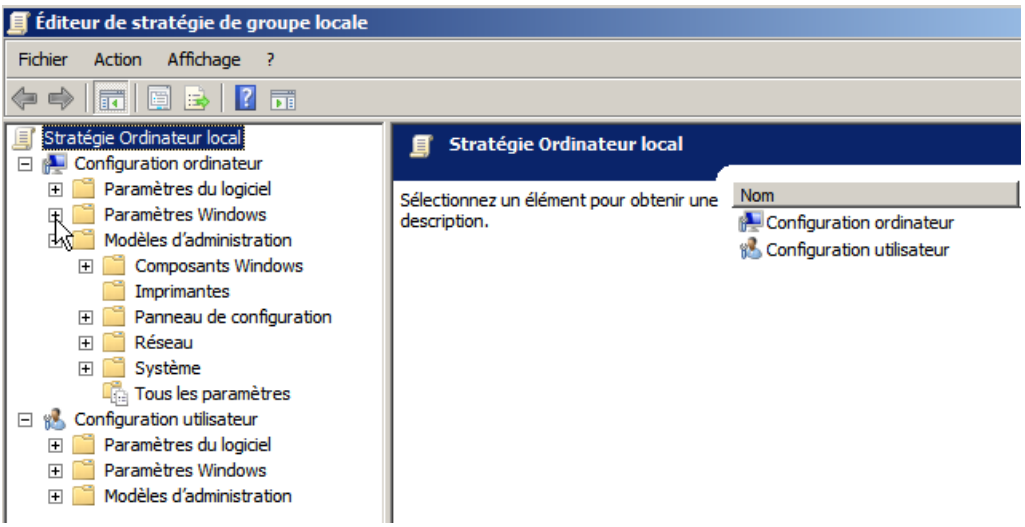
Les **GPO** ou **stratégies de domaine/réseaux** elles sont en général utilisées à travers le réseau (pour tout le domaine ou une partie à travers les UO...)

A ce stade, on ne confond plus les « réglages des stratégies locales » avec le fait de passer ces réglages localement via **secpol.msc** (ou **le panneau de configuration / stratégies locales**) ou via une **GPO** de **domaine**

Gpedit.msc - editeur de stratégie de domaine "locale" ! :

Il est cependant possible de modifier localment les stratégies d'une machine Windows avec les options normalement réservées aux stratégies de domaine /réseau, ARG !

Il faut passer par une console personnalisée **gpedit.msc** que l'on lance depuis **démarrer / executer**…

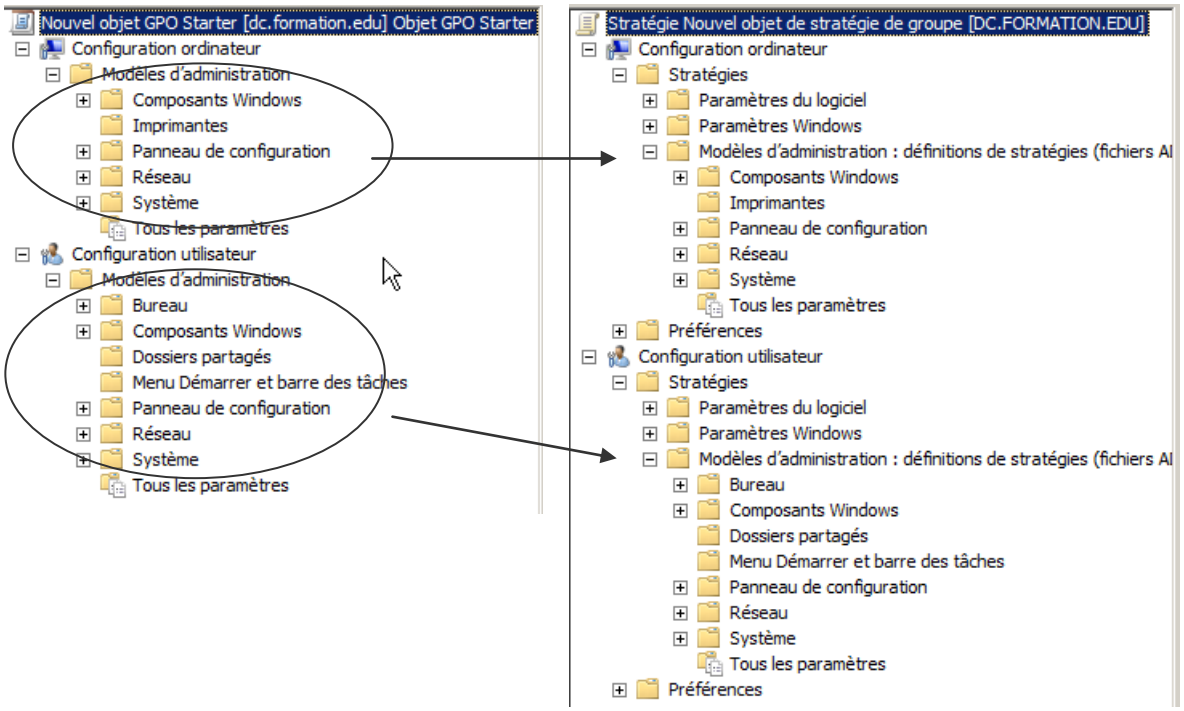


N.B: Evidemment on ne choisit pas sur qui cela s'applique…!

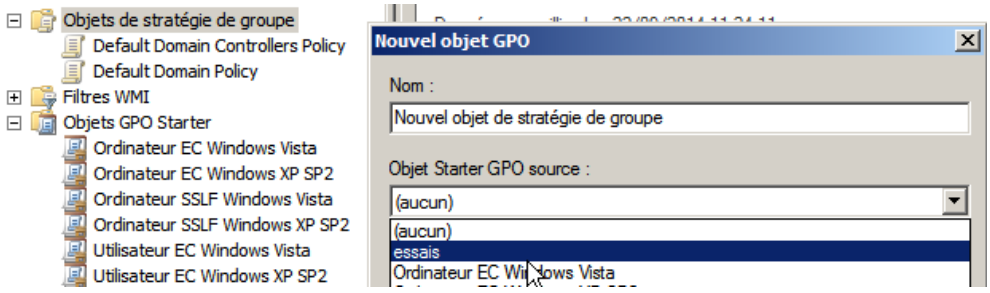
Objets GPO starter

pour avoir des modèles reproductibles de GPO, mais bases uniquement sur la partie "Modèles d'Administration" des stratégies Ordinateurs ou Utilisateurs.

GPO Starter **GPO complète**



Permet la création de GPO à partir de ces templates facilement



Permet l'exportation de ces modèles sous forme de **fichier CAB**, que l'on peut ré-importer dans un autre Domaine (on fait des **GPO** sur un site de test, puis on les implantes ailleurs...

N.B: si on veut effectuer la même chose pour des GPO complètes, c'est à dire incluant des paramètres du logiciels, des Paramètres Windows ou des préférences, il faut utiliser 2 techniques :

- faire du scripting en **powershell**
- Utiliser un outil **AGPM Advanced Group Policy Management** faisant parti d'un ensemble nommé **MDOP Microsoft Desktop Optimization Pack**