http://WWW.CABARE.NET ©

Stratégies GPO & AD sous Windows 2008
– sys 26 – cours -

Stratégies Windows & GPO de Domaine 2008

Michel Cabaré – Ver 2.0 – Nov 2009-

La formation que vous suivez, à pour but de vous initier avec le logiciel Microsoft Windows 2008 (version 6.x) sur environnement P.C.

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 XP

Types de stratégie :

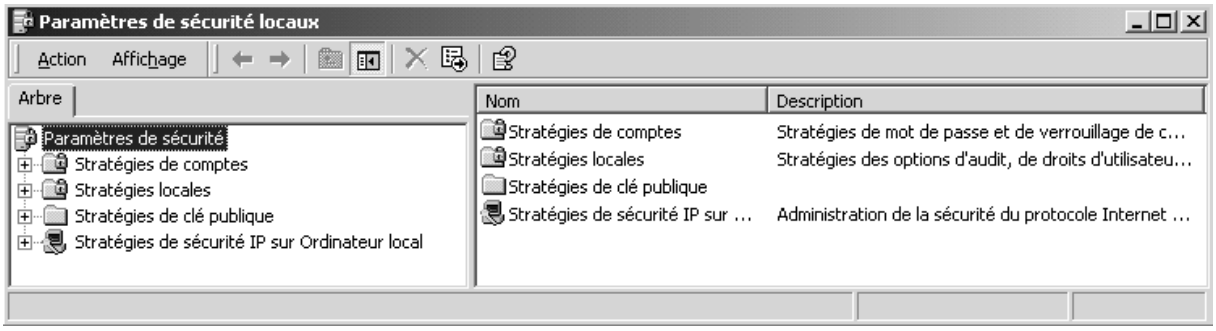
Les stratégies de sécurité permettent d'éviter que des utilisateurs modifient involontairement (ou volontairement) la configuration d'un ordinateur.

il existe essentiellement 2 méthodes pour implémenter des stratégies sur des postes 2000-XP, les **stratégie système locale** appliquée sur un ordinateur unique, ou les **stratégies de groupe** appliquée dans un domaine et déployée sur plusieurs ordinateurs…

Stratégies sur un ordinateur local (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**…

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



Ces stratégies locales sont disponibles sur

- Windows 2000 et Windows -XP,
  (qu'il soit membre d'un domaine ou non)
- Serveur 2000-2003 (s'il n'est pas contrôleur de domaine)-2008.

Lorsque l'on est dans un domaine, ces **stratégies locales** peuvent être écrasées par des stratégies de plus haut niveau.

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

Lorsque un ordinateur appartient à un domaine, on peut alors 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, donc les paramètres locaux sont modifiés dans cet ordre

Stratégies Locales - GPO de Domaine – GPO d'Unité Organisationelle.

Configurer des stratégies localement :

Il ne faut pas confondre "*configurer des stratégies localement*", qui suppose que l'action soit faite localement sur chaque machine, 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 se sécurité locale…

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

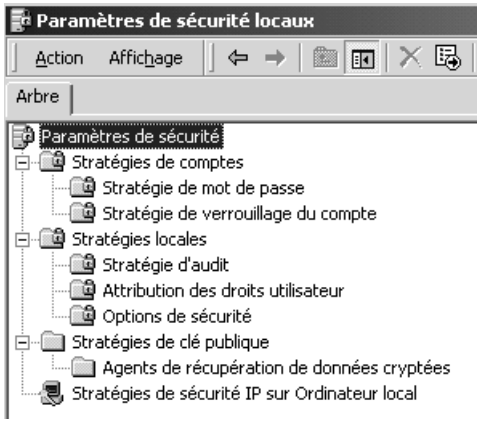
- **Stratégies de compte**

  (~gestion utilisateur)
- **Stratégies locales**

  (~qui peut ouvrir session locale)
- **Stratégies de clé publique**

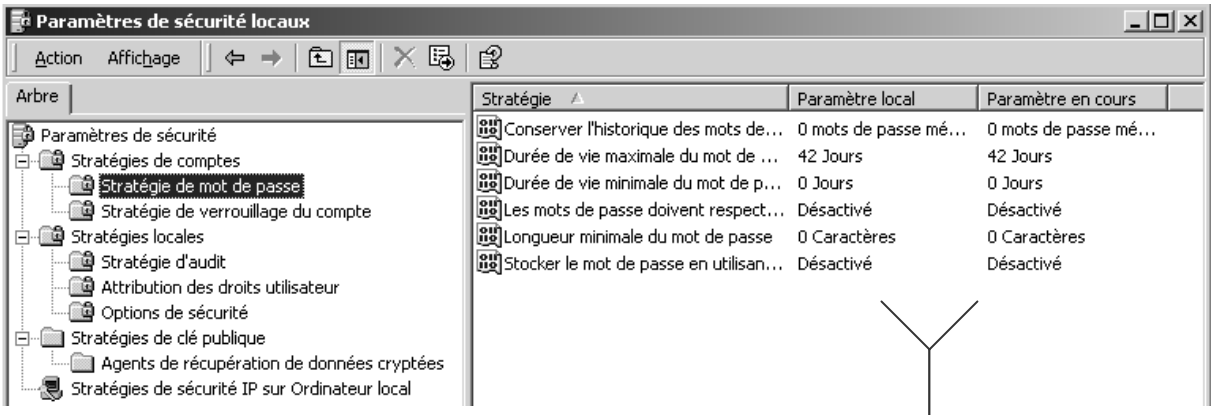
  (agent de récupération)
- **Stratégies IPSEC**

  (cryptage IP)

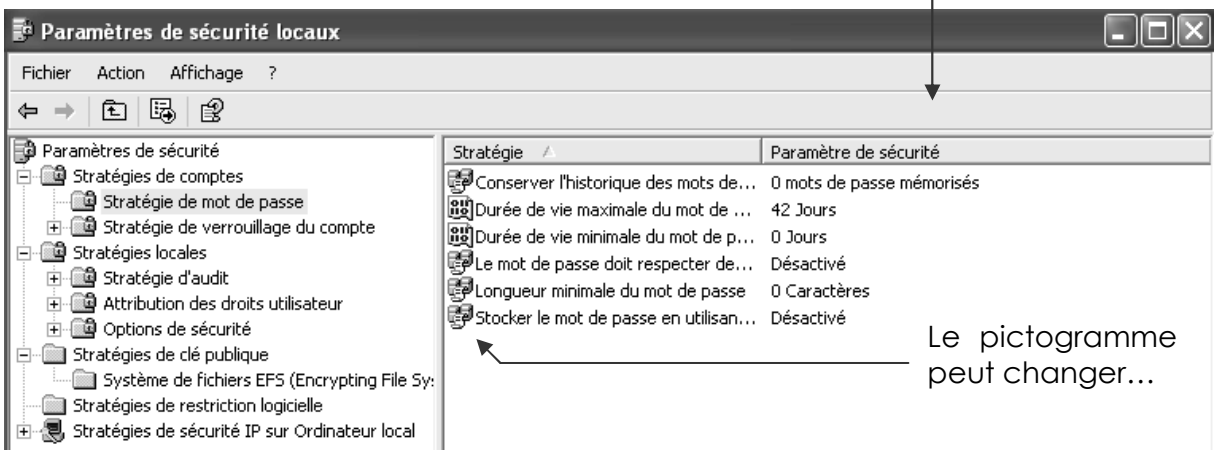


Dans l'arborescence, on visualise à droite les différentes composantes…

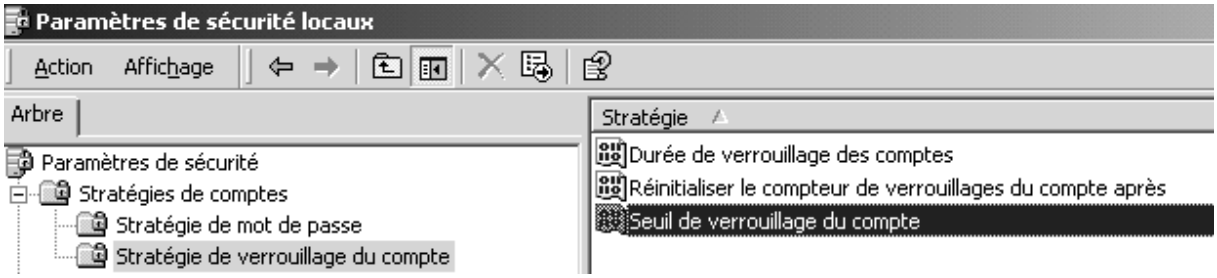
Interface **Windows 2000**



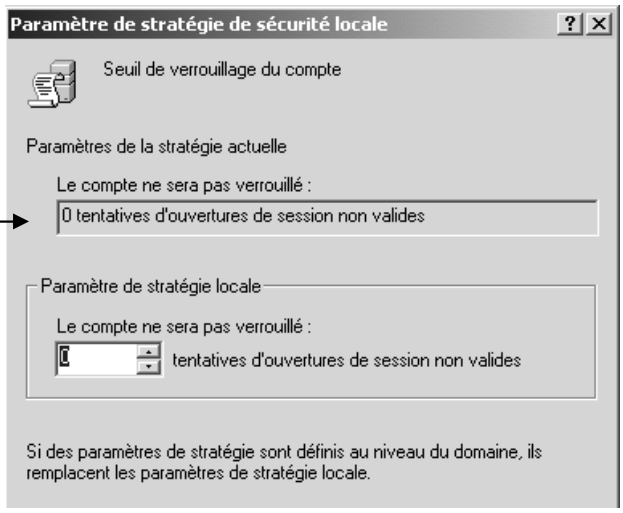
Interface **Seven - Windows XP** (une seule colonne)



Par exemple, dans **Stratégies de compte/ Stratégies de verrouillage du compte**

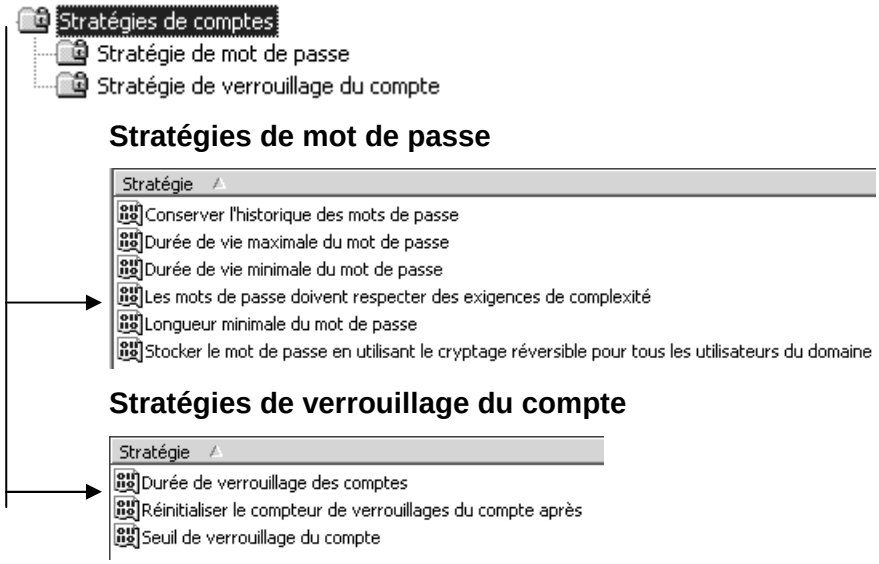


Sur lequel un double-clic amène



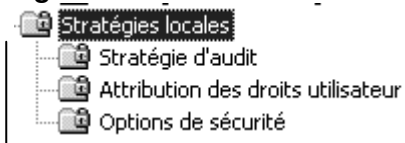
Contenu des Paramètres locaux de sécurité :

Stratégies de comptes

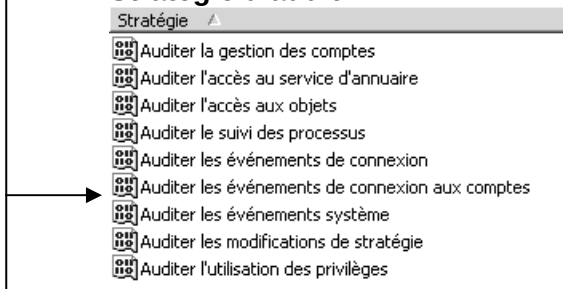


N.B : concernant la gestion des mots de passe, si un domaine existe, alors il serait bon de gérer ces stratégies essentiellement au niveau du Domaine, et jamais à un niveau inférieur, sous peine d'avoir des incohérences et des problèmes d'accès !

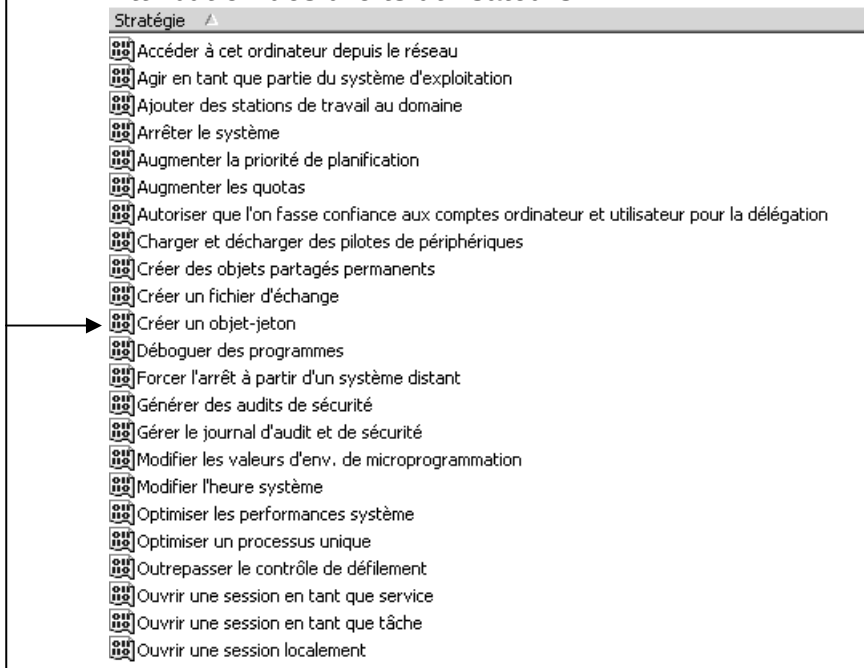
Stratégies locales



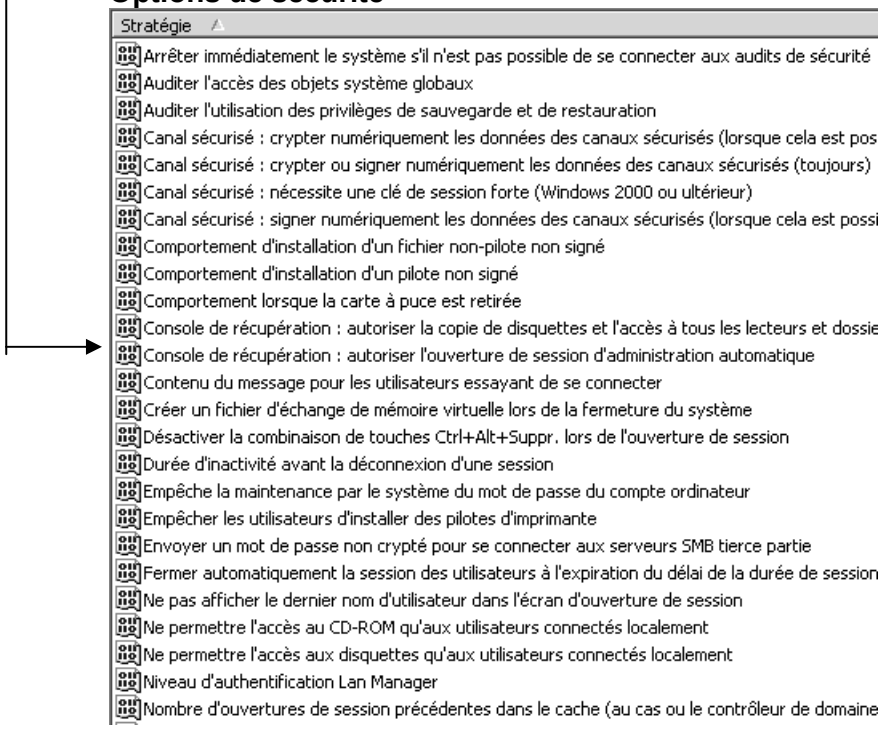
Stratégie d'audit



Attribution des droits utilisateurs



Options de sécurité



Stratégies de clé publique

Stratégies de sécurité IP

Stratégies de restriction logicielle (uniquement sous Seven XP)

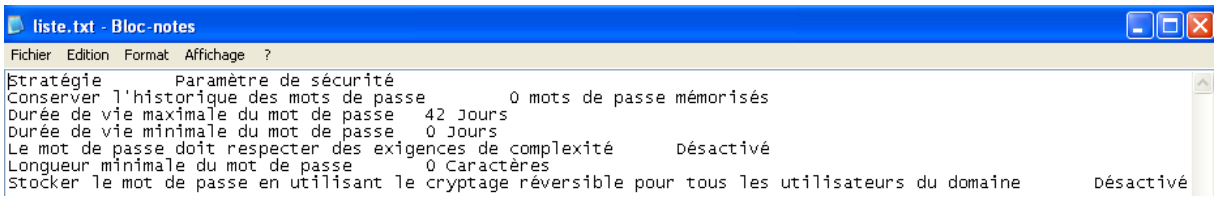
N.B : il faut bien évidemment faire attention à ce que toutes les stratégies ne sont pas disponibles à l'identiques sur toutes les machines, en fonctions des systèmes Seven, Vista Xp et des services packs installés, voir des modules complémentaires spécifiques, les stratégies peuvent varier, parfois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

Imprimer lister les stratégies :

Il est possible lorsque l'on se trouve sur une entrée des stratégies, 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 VISTA SE

Stratégies locales multiples dites LGPO

Avant Vista, 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 :

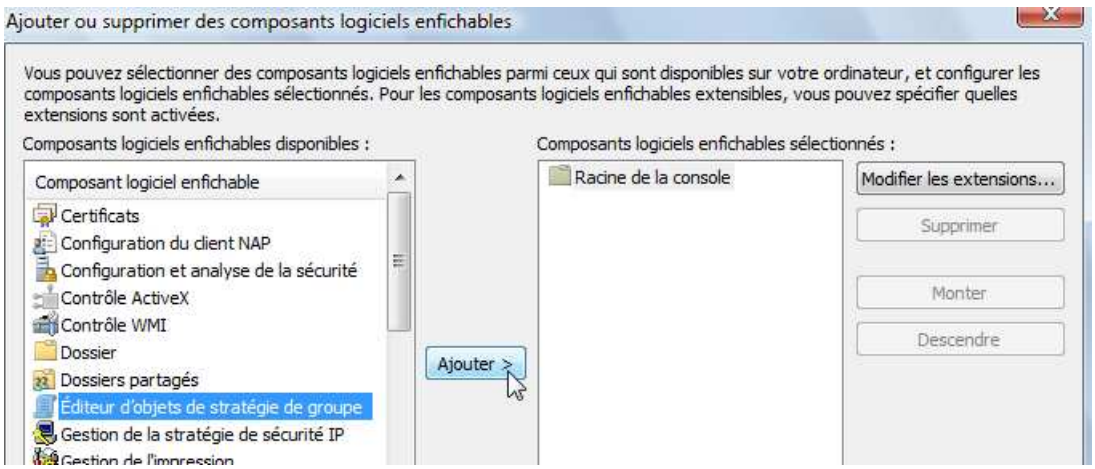
- l'ordinateur, et/ ou
- tous les utilisateurs.

Depuis Vista / Seven il est possible maintenant de définir des stratégies multiples locales **LGPO** dont la portée peut être plus fine…

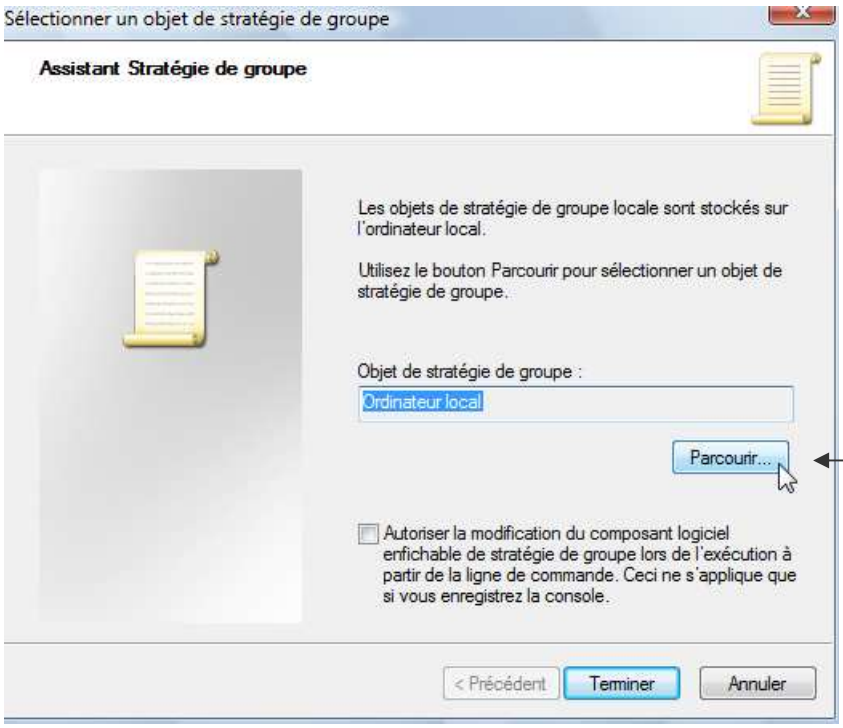
- l'ordinateur, et/ ou
- tous les utilisateurs. (locaux)
- Tous les administrateurs (locaux)
- Touts les non-administrateurs (locaux)
- Un utilisateur local du poste

Définir une LGPO

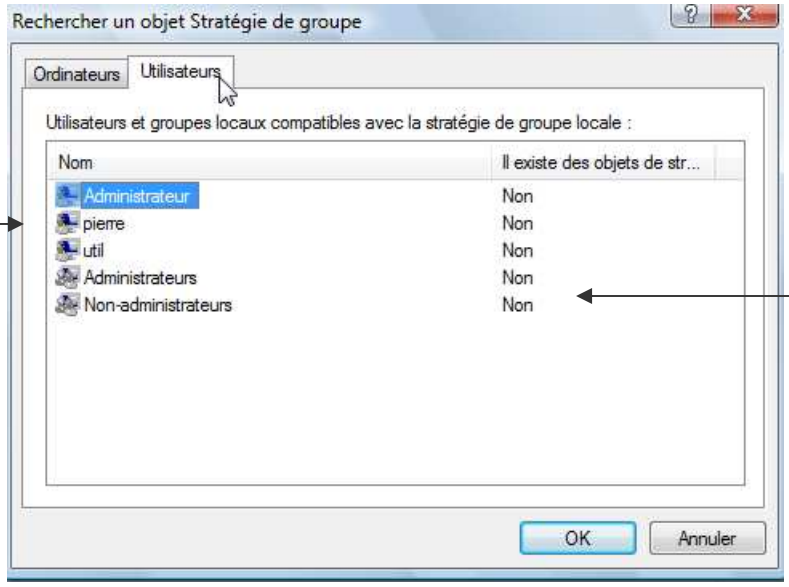
On construit une nouvelle **mmc**, avec **l'Editeur d'objets de stratégie de groupe**



Lorsque on ajoute, On ne demande surtout pas **Terminer**(*), mais **Parcourir**



Et on choisit l'onglet **Utilisateur**

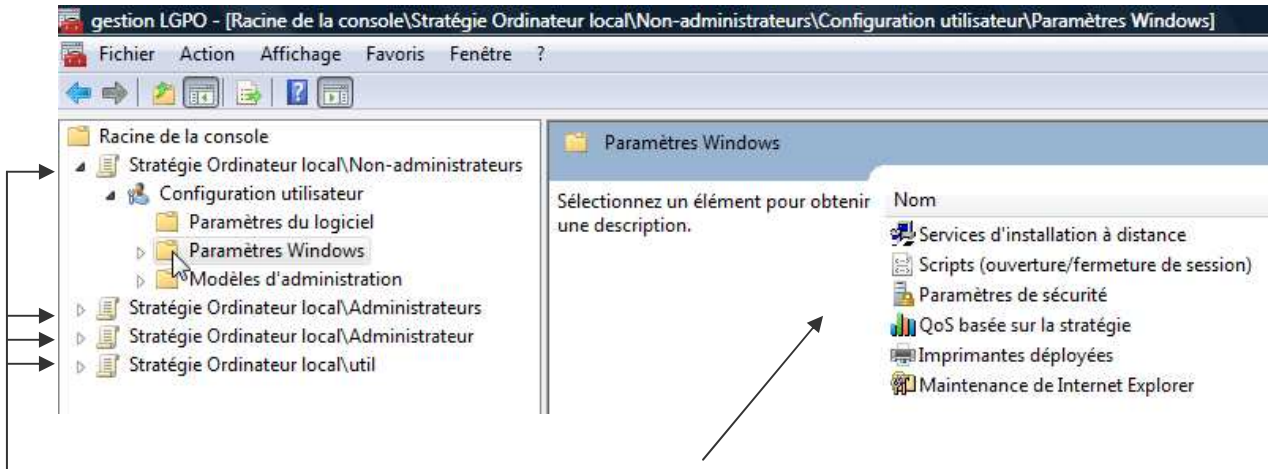


On retrouve ici les choix annoncés

- l'ordinateur, -il aurait fallut faire terminer (*)
- tous les utilisateurs. - il aurait fallut faire terminer(*)
- Tous les administrateurs (locaux)
- Touts 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…

On obtient



Pour chaque Stratégie locale, on effectue les réglages…

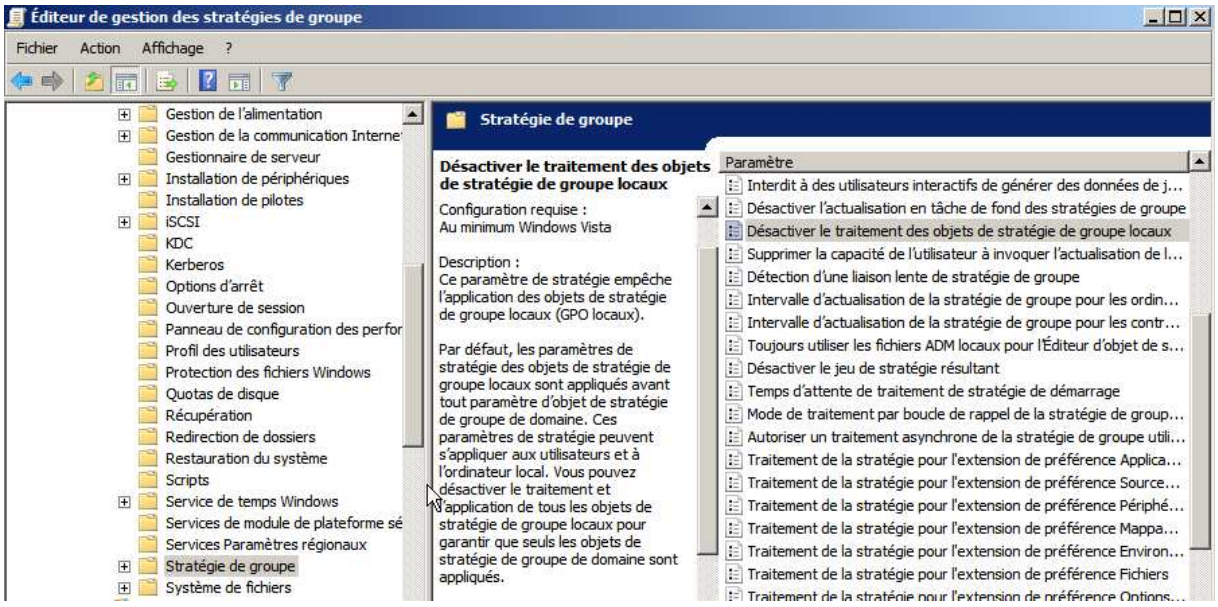
N.B: Attention, à ne pas cumuler plusieurs stratégies locales pour un même utilisateur, autrement dit si on utilise une LGPO de groupe, ne pas utiliser une LGPO pour un utilisateur particulier de ce groupe! L'ordre théorique d'application est le suivant :

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

Désactivation des LGPO

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**\



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

STRATEGIES LOCALES - AUDIT

Audit évènement – audit Ressource:

Il est possible par un audit de suivre les évènements qui surviennent de la part d'un utilisateur, ou du système d'exploitation, sur **une machine donnée**.

Chaque événement est consigné dans un des journaux, appelé **journal de sécurité, qui ne contient pas uniquement les évènements d'AUDIT…**

Une **stratégie d'audit**, peut définir les **types d'événement** à surveiller. Dans la liste suivante les moins importants sont présentés entre parenthèses ():

- **Gestion des comptes** : un administrateur gère un compte ou un groupe, un compte est modifié (mot de passe…)
- **(Suivi des processus)** : uniquement pour les développeurs…
- **(Connexion)** : enregistre les sessions sur le poste, que celle-ci soient locales ou via le réseau, qu'elles utilisent un compte local ou de domaine, (l'audit est posé sur la station)
- **Connexion compte** : enregistre les demandes d'identification. Si la demande d'ouverture de session se fait sur le domaine, elle est reçue par un contrôleur de domaine ,l'audit doit être posé sur le contrôleur. Si elle est locale, l'audit doit être posé localement
- **(Evènements système)** : démarrage ou arrêt du poste…
- **(Modification de stratégie)** : modification aux options de sécurité ou aux stratégies …. D'audit
- **Utilisation de privilèges** : comme la possibilité de modifier l'heure système, ou lorsque un administrateur s'approprie un fichier

Une **stratégie d'audit**, peut définir les **types de ressources** à surveiller

- **Accès à AD** : un utilisateur accède à AD (l'audit doit être posé sur les objets AD)
- **Accès aux objets** : un utilisateur accède à une ressource fichier, dossier, imprimante. (**N.B**: ensuite l'audit doit être posé sur chaque objet à auditer via les permissions NTFS…)

De manière générale donc, pour installer un audit, il va falloir :

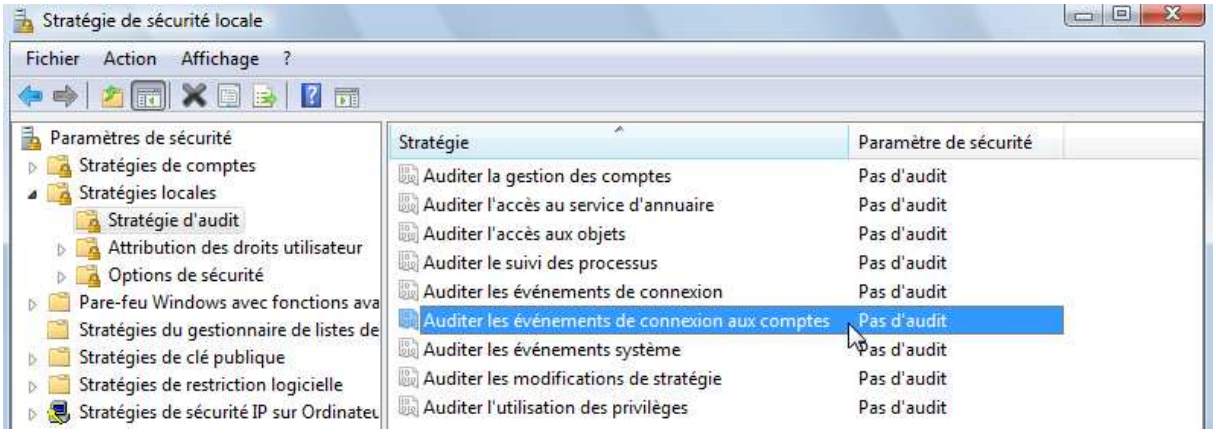
1. Choisir les postes où installer l'audit
2. Déterminer les évènements à auditer
3. Indiquer si on veut auditer les succès ou les échec

Installer un Audit sur évènement - Vista XP

Lorsque l'on veut auditer un évènement, on peut en général auditer aussi bien les **accès réussit**, que les **accès en échec**, les deux n'ont pas la même finalité, et on effectuera toujours un audit minimal afin de faciliter ensuite la lecture du journal d'évènement…

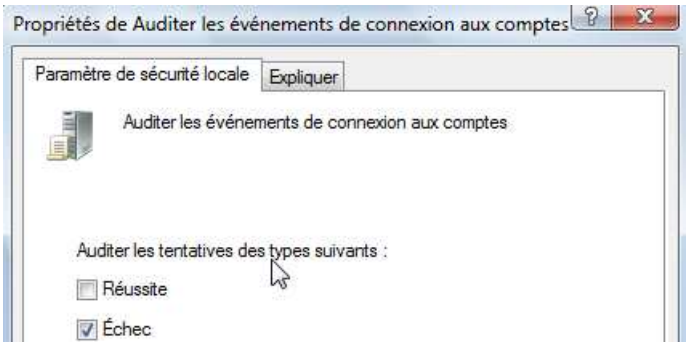
Il faut passer par les **Stratégies de sécurités locales**,

sous VISTA **Stratégies locales / Stratégies d'audit**

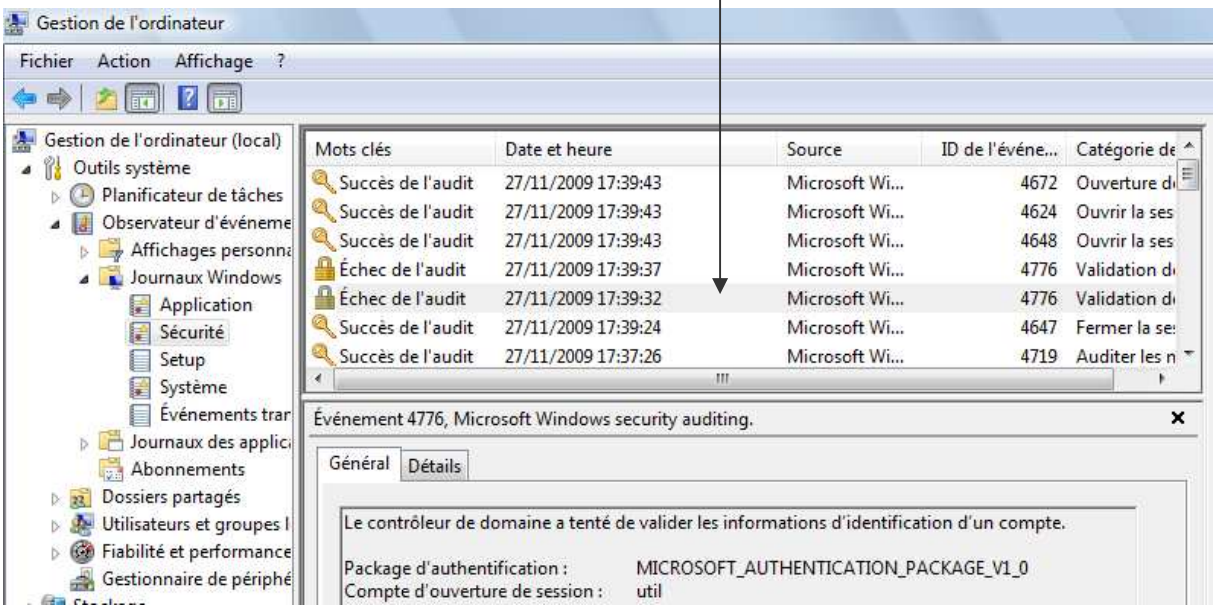


par exemple sur **évènements de connexion aux comptes**

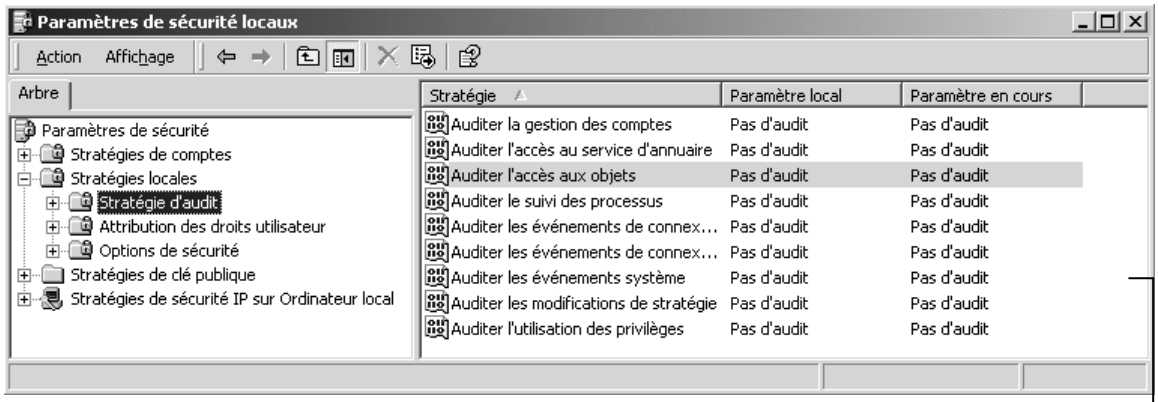
et en demandant d'auditer les **Réussites** et/ou les **Echec**…



par exemple on souhaite ici pister les tentatives d'accès avec un mot de passe erroné… pour obtenir donc après une tentative d'ouverture erronée

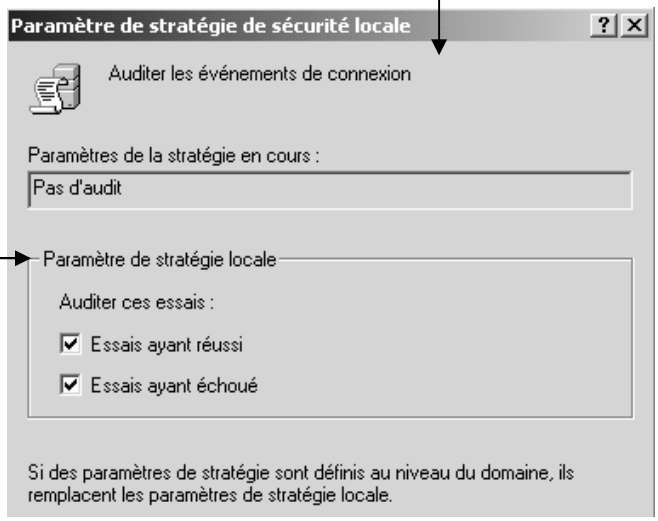


sous 2000 **Stratégies locales / Stratégies d'audit**



par exemple sur **évènements de connexion aux comptes**

et en demandant d'auditer les réussites et/ou les échec…



L'audit étant posé, mais non enregistré

il faut fermer la console pour que les modifications soient prises en compte

…dans ce cas si on re-ouvre la console on voit alors

Installer un Audit via Auditpol - Seven ou 2008

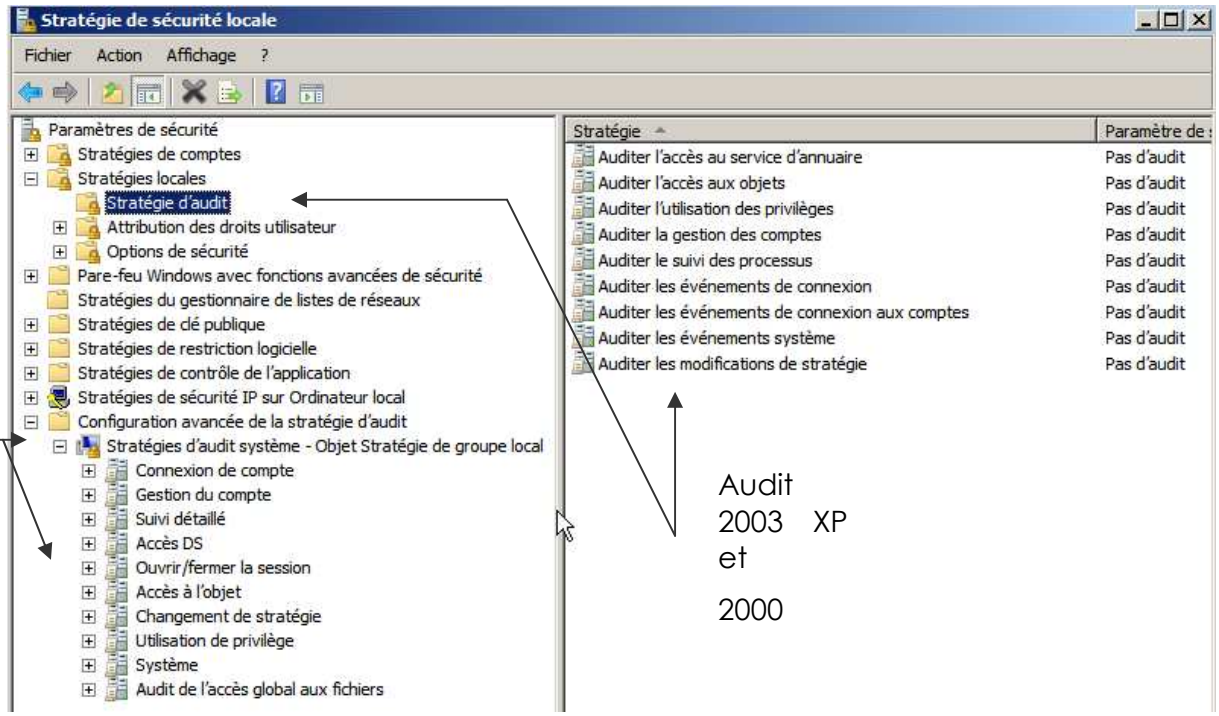
Face à la verbosité des évènements de base, sur SEVEN et Serveur 2008 on a rajouté des options complémentaires augmentant selon Microsoft la granularité de l'Audit

Permettant de ne pas activer simplement les 9 niveaux ou catégories d'audit de base, mais on détaille désormais plus de 52 réglages…

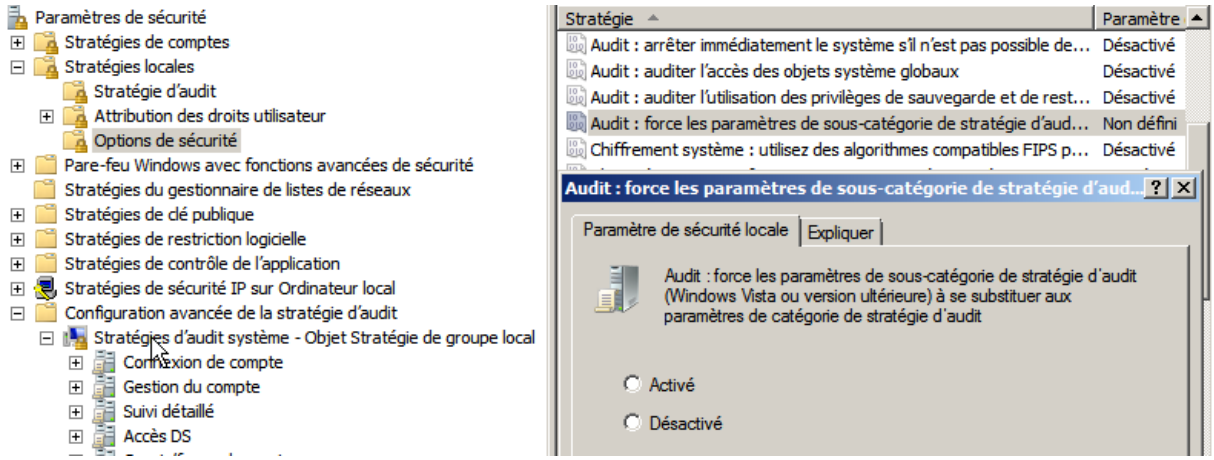
Le problème c'est que ces deux options

- **Stratégies d'audit** : sour XP 2000 et 2003
- **Configuration avancée de stratégies d'audit** : sous SEVEN 2008

sont déclarées incompatibles, et que il faut choisir son camp…



N.B : On peut indiquer via une stratégie **Options de Sécurité** si on veut que les nouvelles stratégies prennent le pas sur les anciennes



N.B vous ne pouvez pas gérer la stratégie d'audit au niveau sous-catégorie en utilisant les stratégies de groupe.. il faut faire cela avec l'outils en invite de commande **auditpol**

Par exemple pour lister les audits **auditpol/get /category :***

```
C:\Users\Administrateur>auditpol/get /category:*
Stratégie d'audit système
Catégorie/Sous-catégorie                    Paramètre
Système
  Extension système de sécurité             Aucun audit
  Intégrité du système                      Succès et échec
  Pilote IPSEC                              Aucun audit
  Autres événements système                 Succès et échec
  Modification de l'état de la sécurité     Opération réussie
Ouverture/Fermeture de session
  Ouvrir la session                         Succès et échec
  Fermer la session                         Opération réussie
  Verrouillage du compte                    Opération réussie
  Mode principal IPsec                      Aucun audit
  Mode rapide IPsec                         Aucun audit
```

Pour changer l'audit d'une sous-catégorie, il faut exécuter **Auditpo**l avec la commande ***/set*** , spécifier la sous-catégorie, et préciser s'il faut activer les événements de réussite et/ou d'échec.

Comme dans

auditpol/set /subcategory:"System Integrity" /failure:enable /success:enable

active la sous-catégorie System Integrity pour les 2 événements réussite / échec.

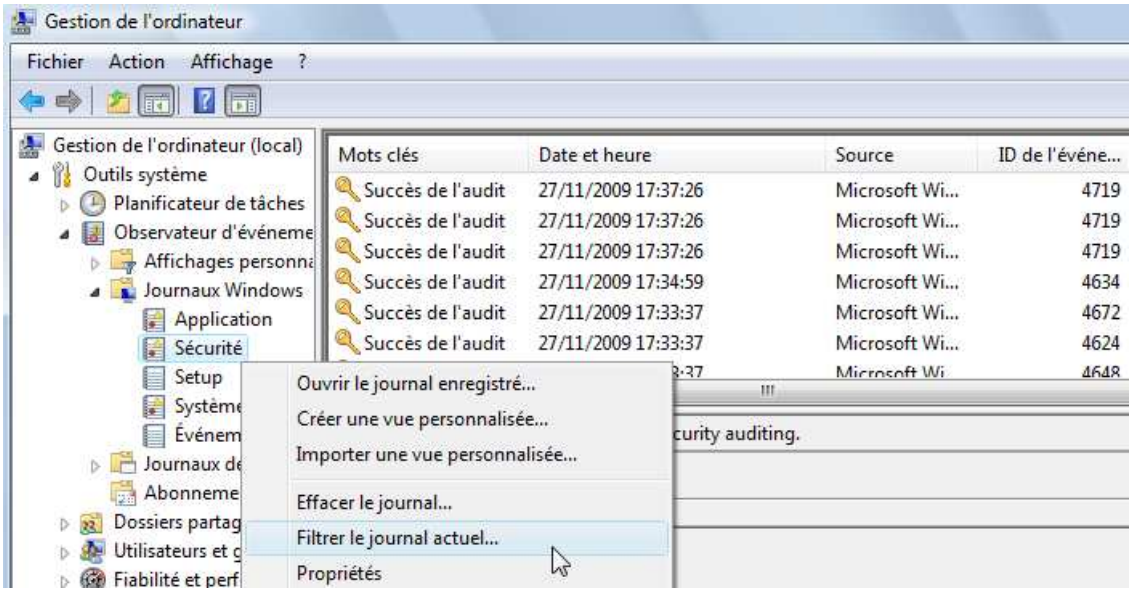
Cet outil ne peut manipuler que les stratégies localement, donc sont déploiement sur un domaine ne pourra se faire que par script…

http://support.microsoft.com/kb/921469/

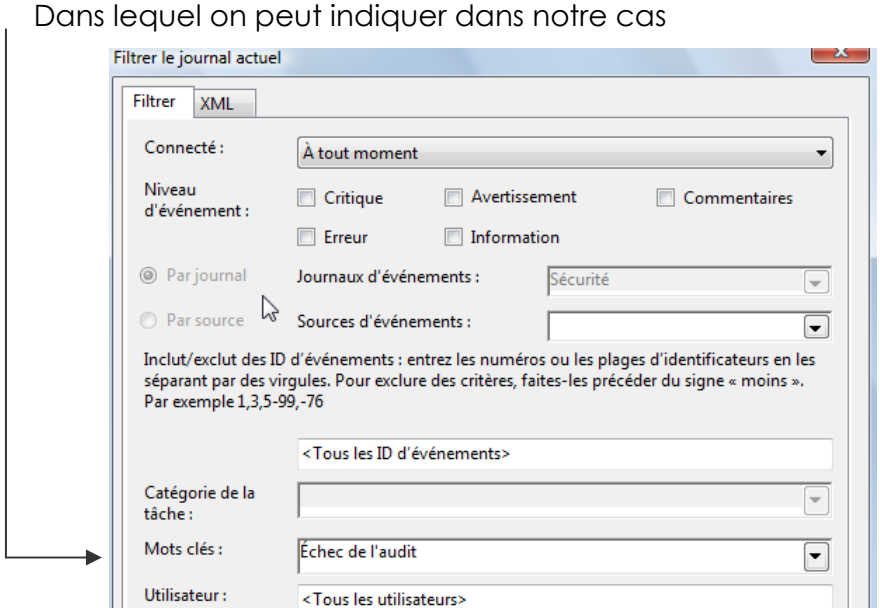
Lire le journal de sécurité:

Ensuite les évènements de sécurité sont consignés dans le journal d'événement

Ce journal est extrêmement verbeux, et pour s'aider on peut le filtrer…



Dans lequel on peut indiquer dans notre cas



Ce qui donne uniquement

Mots clés	Date et heure	Source	ID de l'événe...	Catégorie de l...
Échec de l'audit	27/11/2009 17:39:37	Microsoft Wi...	4776	Validation des ...
Échec de l'audit	27/11/2009 17:39:32	Microsoft Wi...	4776	Validation des ...

Installer un Audit sur des ressources:

Lorsque l'on souhaite installer un **Audit sur des ressources**, l'opération se fait en deux temps. En effet il ne suffit pas de demander d'activer l'audit sur telle ou telle type d'événement (comme cela était le cas pour les session, ou les identification du chapitre précédant), mais il va falloir aussi activer l'audit sur les ressources que l'on veut observer…Il faut donc :

1. activer le type d'audit souhaité, c'est à dire Audit "**Accès aux objets**"dans les stratégies locales de l'ordinateur
2. activer ensuite "**pour chaque ressource**" l'audit particulier (en plus de la sécurité d'accès éventuellement posée

Audit ressource sur un dossier

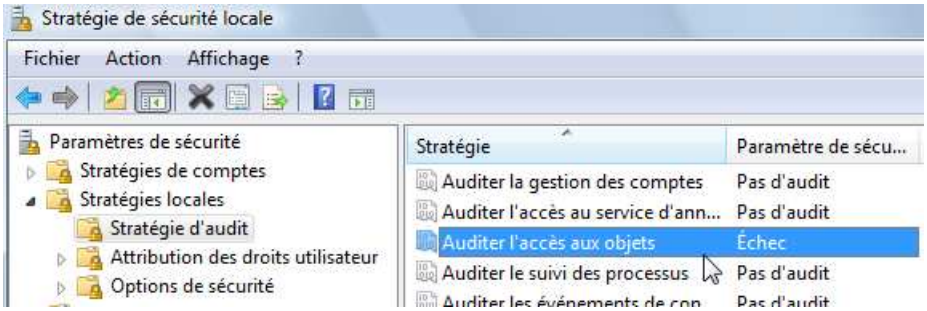
Il faut

1. activer l' Audit "**Accès aux objets**"dans les stratégies locales de l'ordinateur sur lequel le dossier est stocké
2. sur ce dossier ensuite, il fut demander les **propriétés**, onglet **sécurité**, via les **Paramètres avancées NTFS** et demander **Audit** …

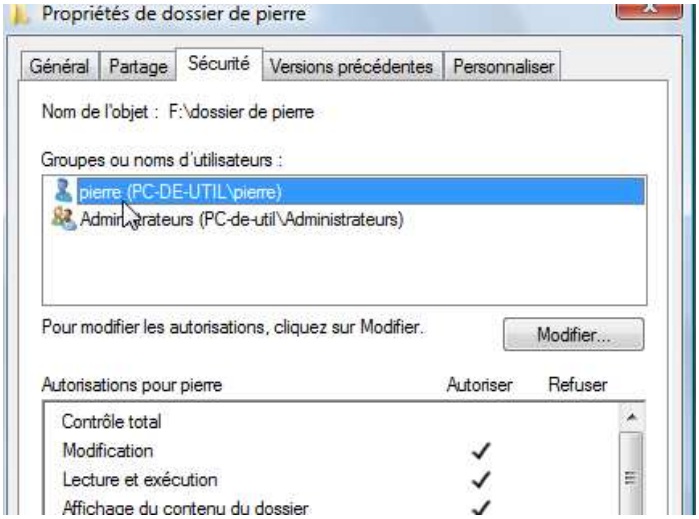
Exemple :

On veut un audit sur les accès en échec pour le dossier de pierre (on cherche à savoir qui essaye d'effacer le dossier de pierre…)

1. Il faut armer les **audits en Echec** sur le poste



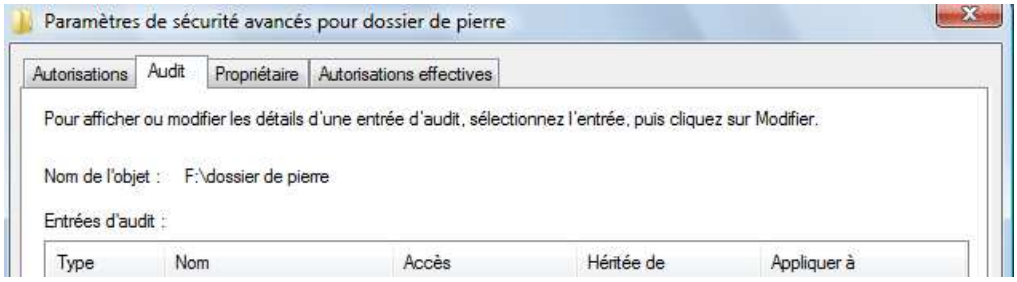
2. Il faut que le dossier de pierre soit protégé en NTFS, bien sûr…



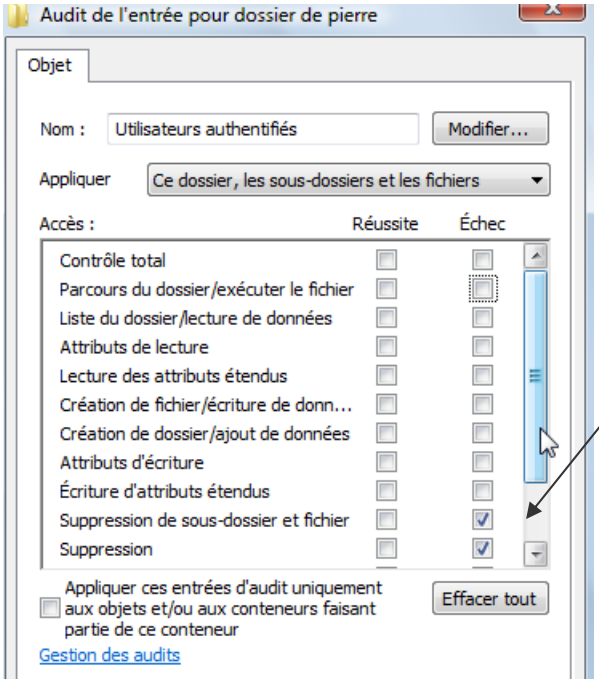
3. puis que l'on pose un audit dessus

via l'onglet **sécurité / avancé** des **propriétés** ce dossier de pierre…

on accès à la boite de dialogue **Paramètre de sécurité avancé pour...**



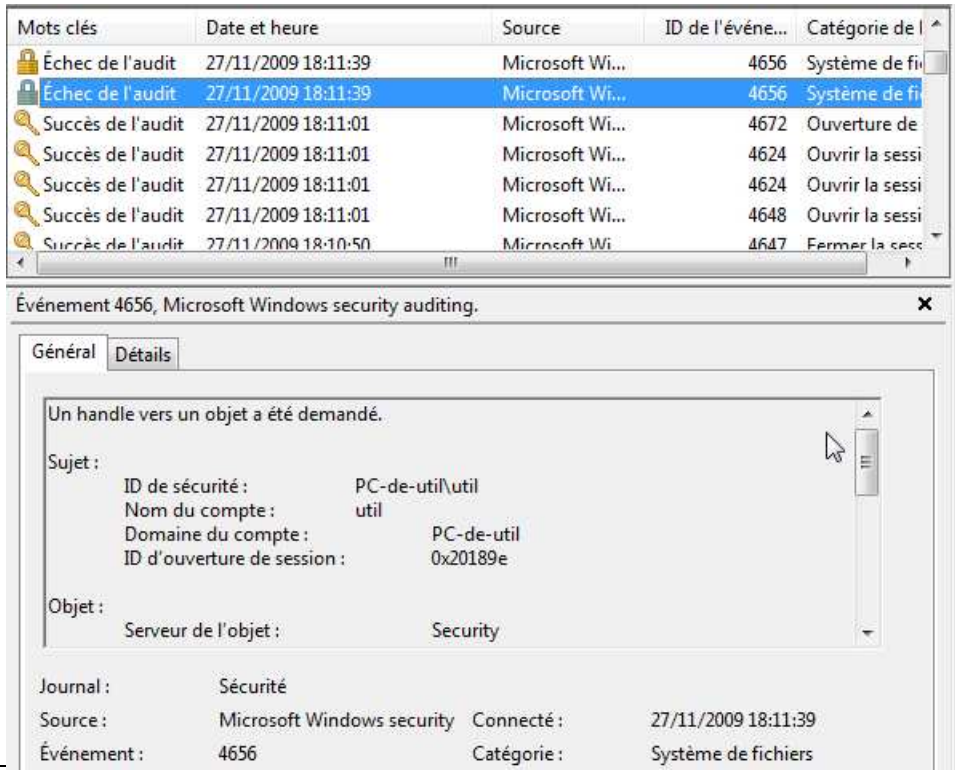
Il faut ensuite ajouter pour qui et quel type d'Audit l'on veut correspondant à



Les types d'audit en tentative de suppresion peuvent être obtenu par **Suppression**

N.B : Ne pas cocher tous les accès car cela génère autant d'évènements de plus !!!

Lorsque ensuite un utilisateur tiers essaye d'effacer le dossier, cela sera tracé…

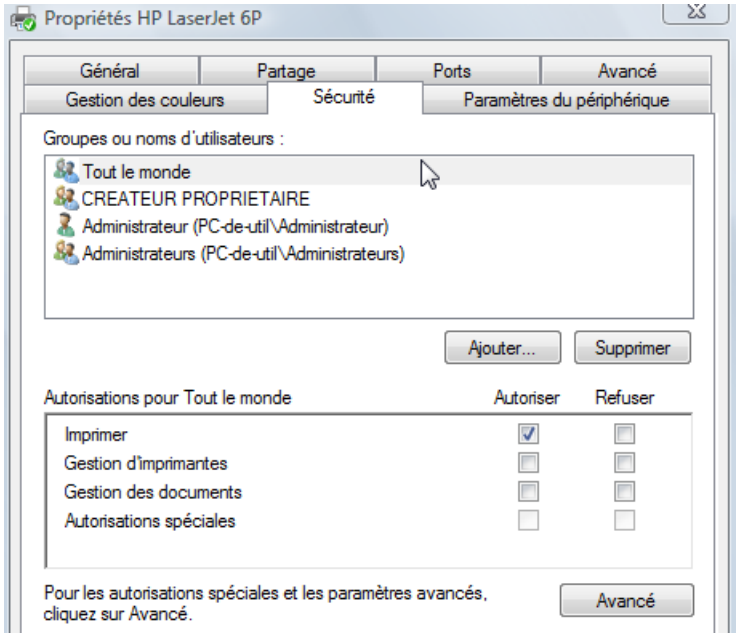


Audit ressource sur une imprimante

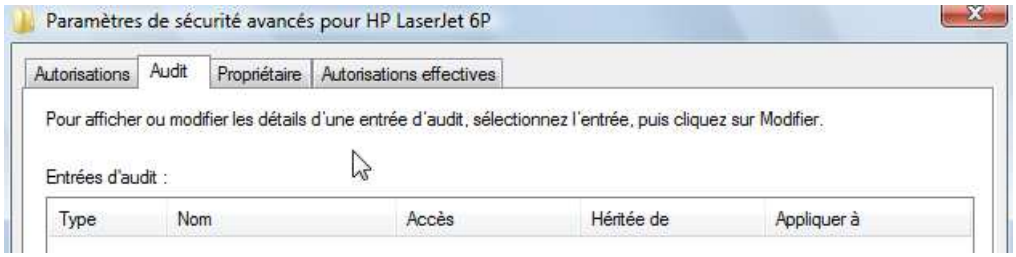
On veut savoir qui utilise l' imprimante réellement :

Il faut

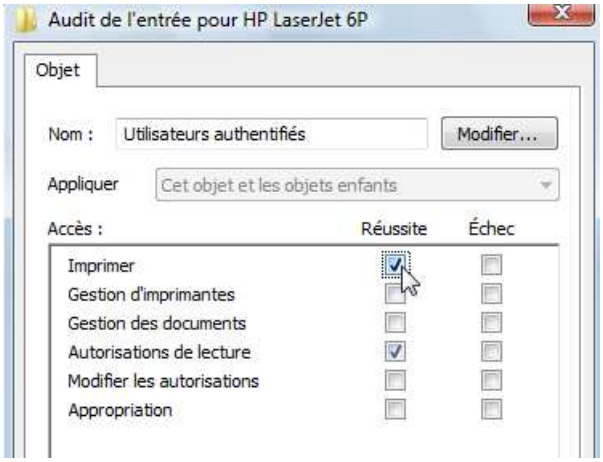
1. activer l' Audit "**Accès aux objets**" en succès dans les stratégies locales de l'ordinateur sur lequel l'imprimante est connectée…
2. sur cette imprimante demander par les **Propriétés avancées NTFS** onglet **Sécurité**, puis bouton Avancé



3. on accès à la boite de dialogue **Paramètre de sécurité avancé pour...**



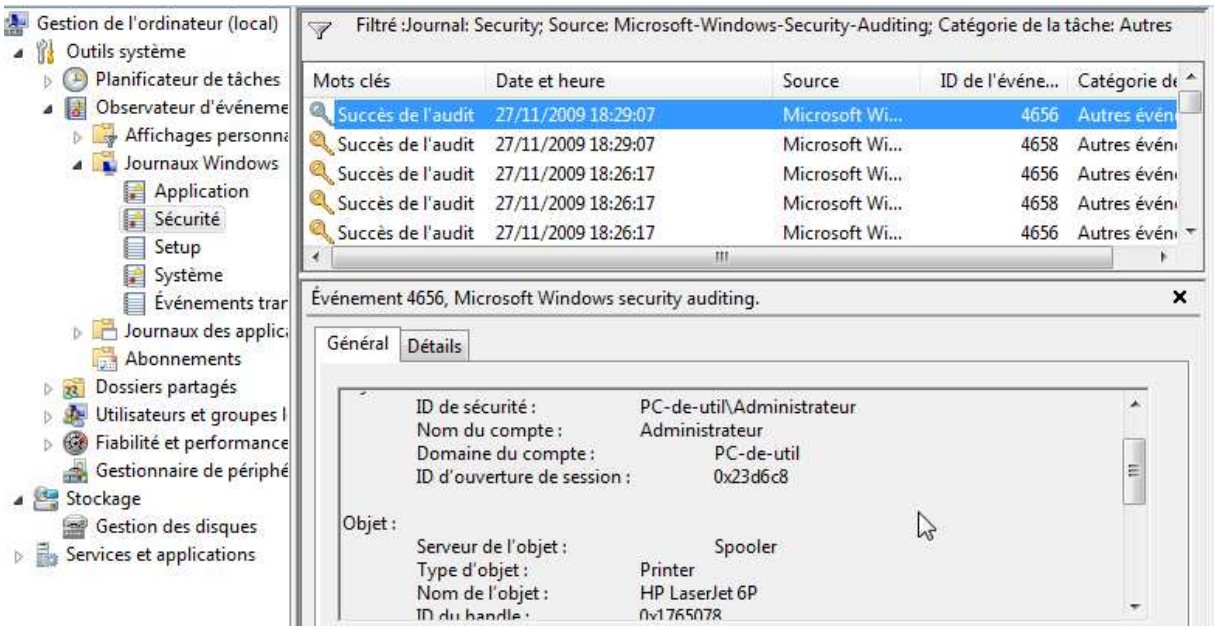
Et il faut indiquer ce que l'on veut auditer



Les types d'audit en tentative 'impression » peuvent être obtenu par **Imprimer**

N.B : Ne pas cocher tous les accès car cela génère autant d'évènements de plus !!!

Ensuite il faut après une impression voir le journal d'évènements…



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 à toutes les machines de notre domaine.

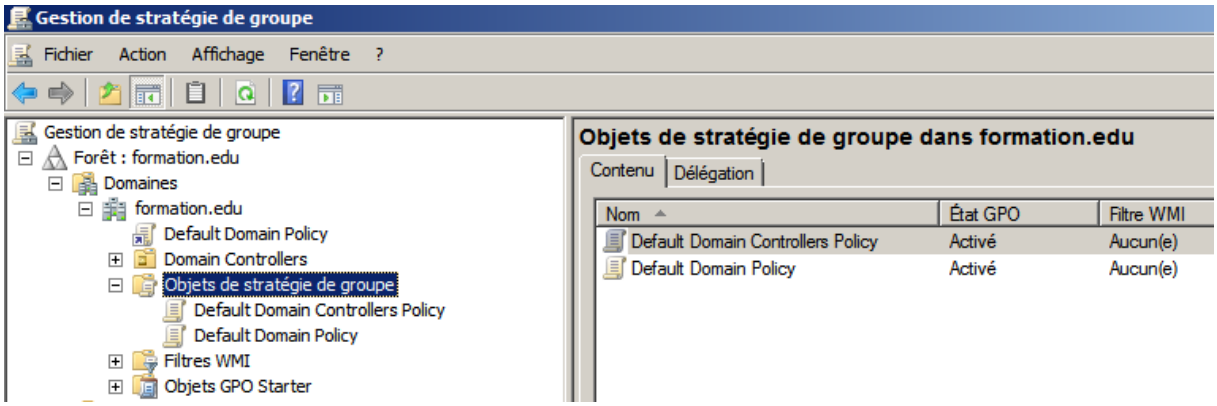
- les contrôleurs de domaine 2008-2003 ou 2000 en font partie

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

La gestion des stratégies de groupe :

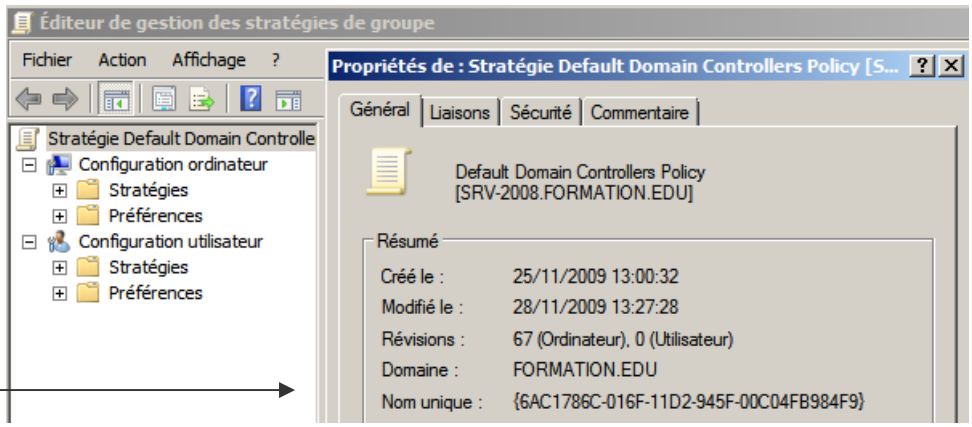
Pour donner une stratégie de domaine, il faut lancer la **Gestion des stratégies de groupe** dans les **Outils d'Administration**

N.B: on n'accède plus aux stratégies via Utilisateur et Ordinateurs AD comme sous 2003, Dans 2008 en effet l'outil GPMC disponible en téléchargement sous 2003 est intégré d'office…



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

Si on demande Modifier / Propriété, on voit alors le GUID de la stratégie

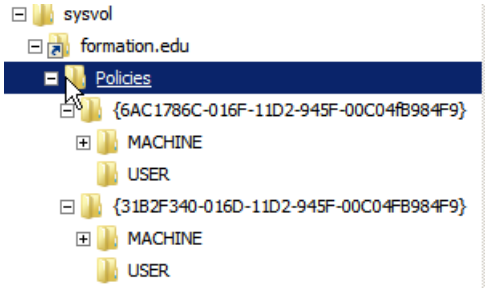


Correspondant **physiquement** au dossier **%Windir%\sysvol\sysvol***domaine***\Policies**

Dans lequel on y trouvera nos stratégies

{6AC1786C-016F-11D2-945F-00C04fB984F9}

{31B2F340-016D-11D2-945F-00C04FB984F9}



Correspondant à

Default Domain Controllers Policy

Default Domain Policy

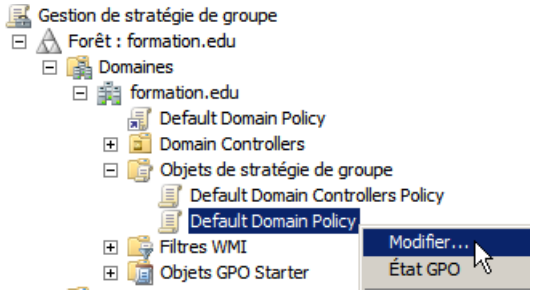
Il existe 2 GUID connus :

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**

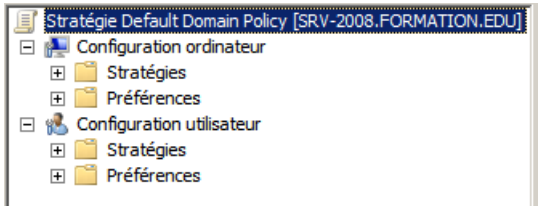


On demande **Modifier…** la **Default Domain policy**

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 d'une **Default Domain Policy** c'est absolument TOUT le domaine !!!

Propagation Stratégies de Domaine :

Les stratégies sous 2003-XP étaient gérées par le service **Netlogon**, Depuis 2008 Seven elle sont gérées par un service **NlaSVC/** (connaissance des emplacements réseau), plus réactif et gérable (par stratégie !)

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 en invite, depuis le client sur lequel on veut effectuer la propagation (on tire la stratégie vers soi !)

Sous **Windows Seven - XP**

Gpupdate /force

```
C:\Documents and Settings\Administrateur.SRV1-2003.000>gpupdate /force
Actualisation de la stratégie...

L'actualisation de la stratégie utilisateur s'est terminée.
L'actualisation de la stratégie ordinateur s'est terminée.

Pour vérifier des erreurs dans le traitement de la stratégie, consultez
l'Observateur d'événements.
```

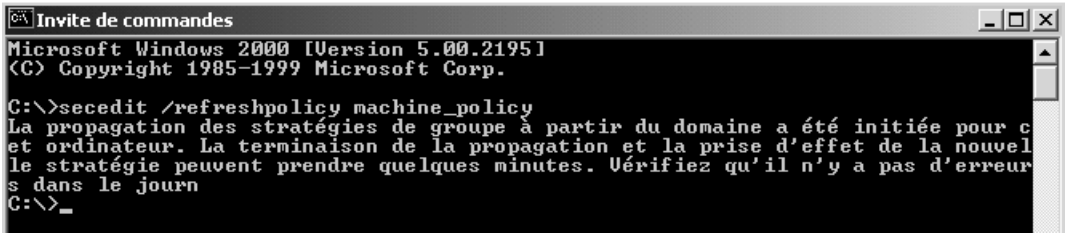
Par exemple

effectivement, dans le journal on peut observer

(Voir détail de ces commandes **secedit** et **gpupdate** dans le chapitre sur les GPO d'unité organisationnelle…)

Sous **Windows 2000** :

Secedit /refreshpolicy machine_policy



Et / ou

Secedit /refreshpolicy user_policy

L'utilitaire en ligne Gpupdate (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. ←

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

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

Non erreur doc: **machine_policy**

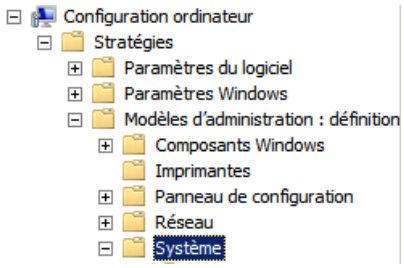
Non erreur doc: **user_policy**

Gestion Propagation des Stratégies de Domaine :

Lorsque un client XP contacte son DC 2003 pour récupérer une stratégie, si un problème se passe, il ne le re-contactera pas avant le prochaine cycle normal… Sous 2008 et Seven; le service **NlaSVC** interroge et reprends contact avec le DC des la remise en disponibilité de celui-ci.

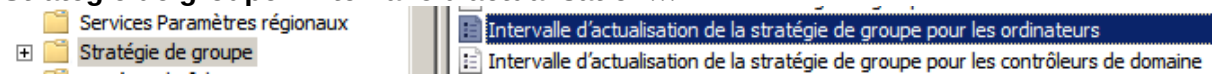
De plus 2 nouvelles stratégies désormais existent permettant d'affiner la vitesse de propagation des GPO qui est par défaut on le rappelle **chaque démarrage de poste**, puis **toutes les 5 à 60 voire 90 minutes + (delta de +/-30mn)**

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

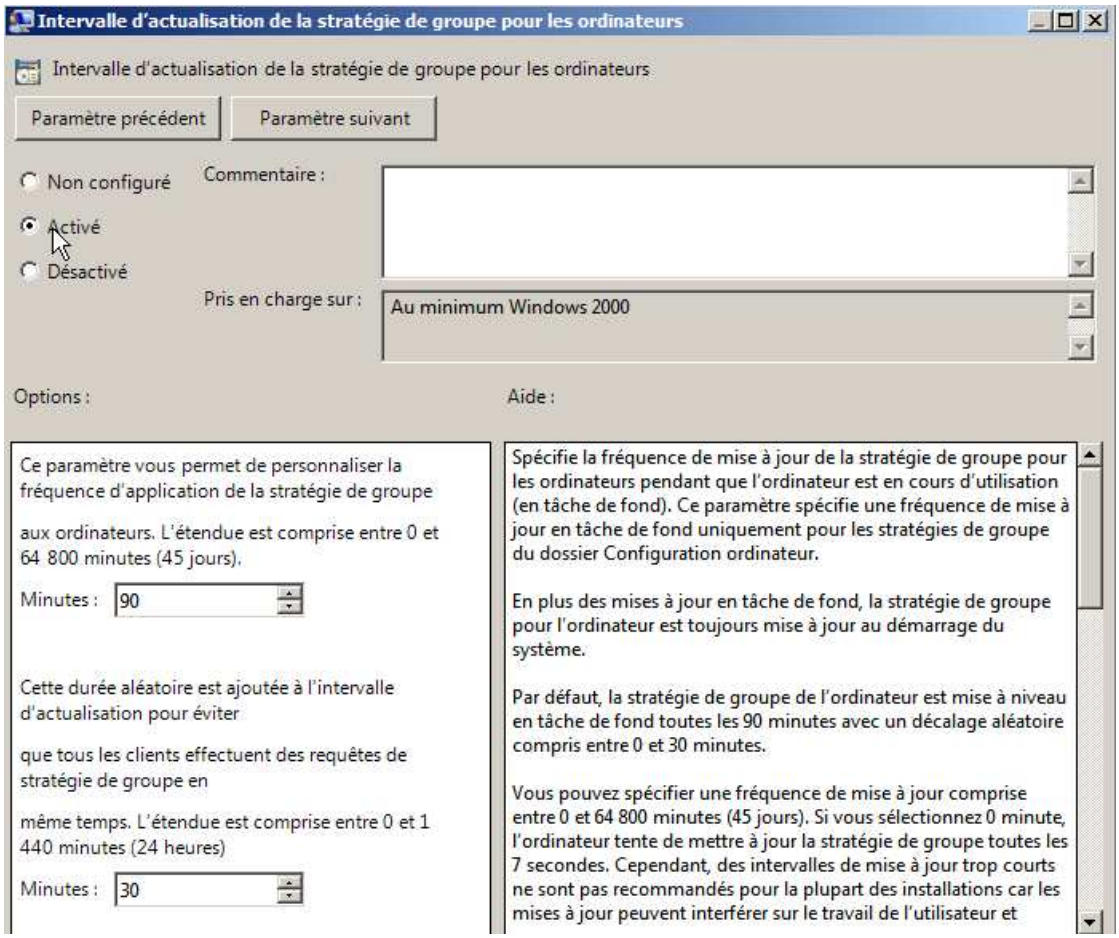


on trouve

Stratégie de groupe : Intervalle d'actualisation…



Donnant

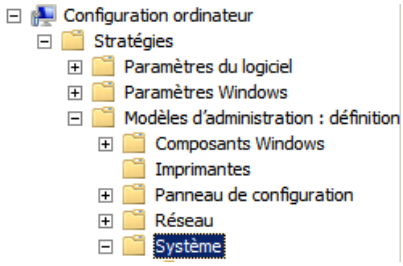


N.B: et bien sur se réglage se trouve également dans **Configuration Utilisateur / Stratégies / Modèles d'administration / Système**

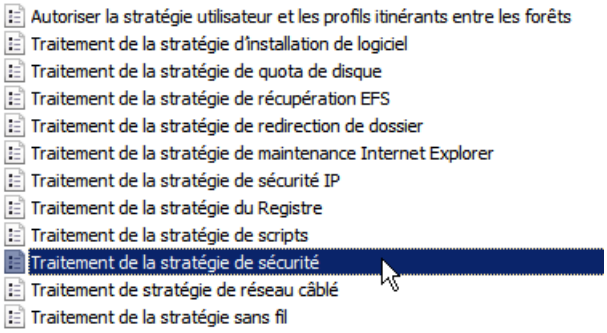
Mais il faut bien voir qu'en plus, certaines stratégies ne sont ré-appliquées localement que si elles ont été modifiées… (afin d'optimiser le temps de réaction des clients)

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

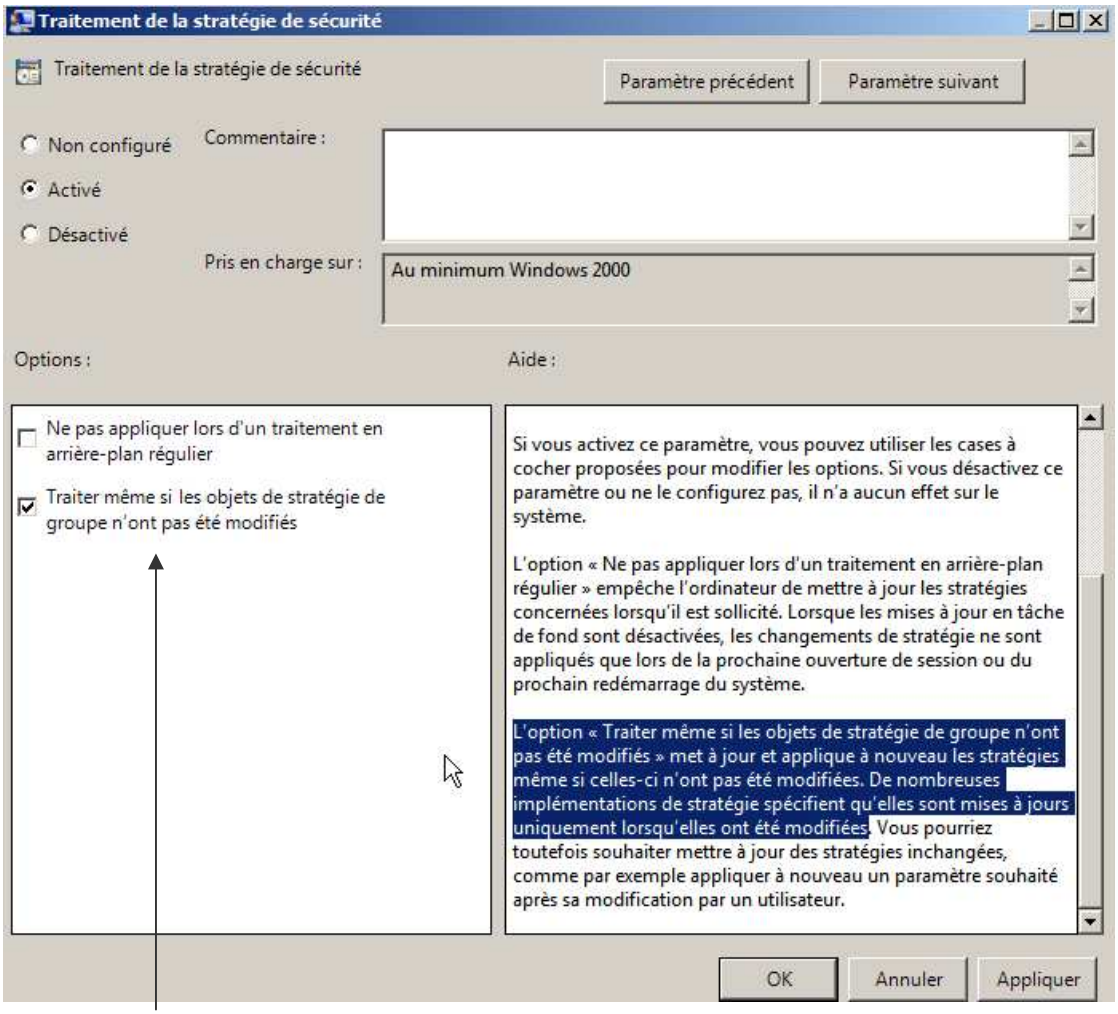
Ordinateur / Stratégies / Modèles d'administration / Système



Mais là on trouve tout un paquet de stratégies :



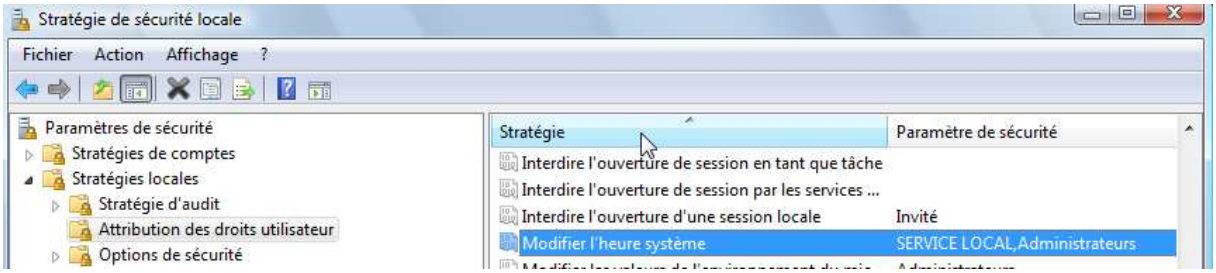
Et lorsque l'on active une stratégie pour un groupe, par exemple ici "Sécurité"



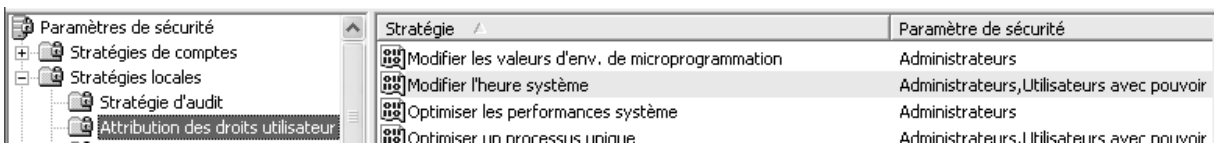
L'option « **Traiter même si les objets de stratégie de groupe n'ont pas été modifiés** » met à jour et applique à nouveau les stratégies même si celles-ci n'ont pas été modifiées.

Exemple : Attribution droits Utilisateur Modifier l'heure système :

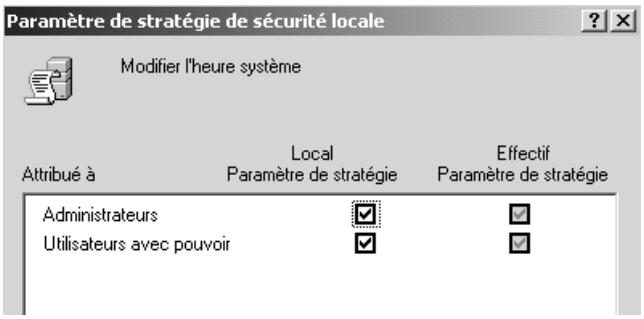
Sur le client Seven – Vista du domaine, la **stratégie locale** ne montre qu'une seule colonne, (le service local remplace les utilisateurs avec pouvoir…)



Sur le client XP du domaine, la **stratégie locale** ne montre qu'une seule colonne

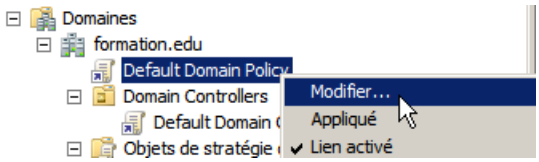


Sur le client 2000 du domaine, voila l'aspect de la **stratégie locale** concernant qui peut mettre à l'heure la machine....

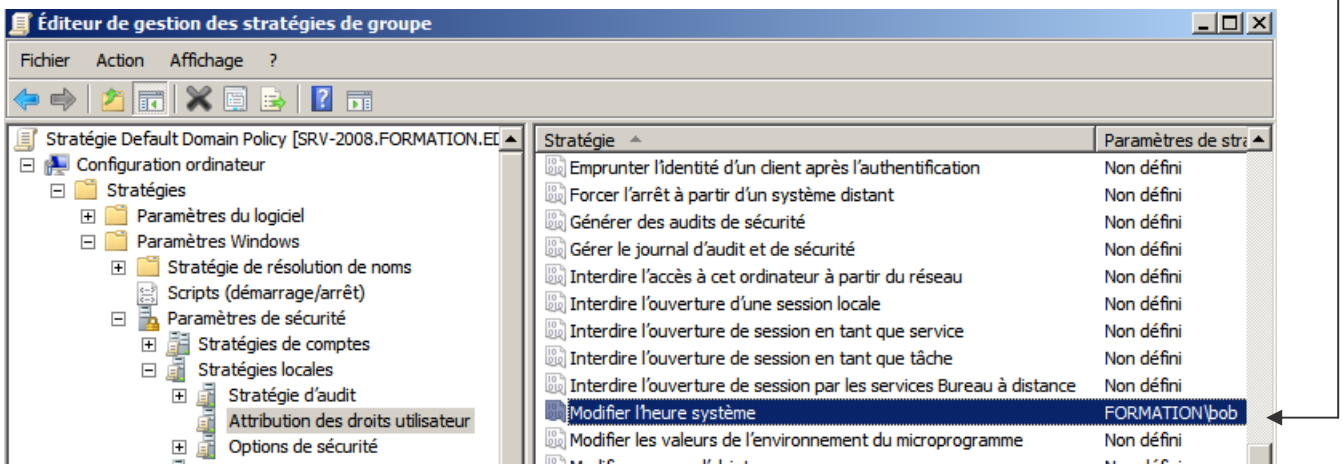


Sur le Contrôleur de Domaine, on définit une **Stratégie de sécurité du domaine** pour **Modifier l'heure système** (qui par défaut est non activée)

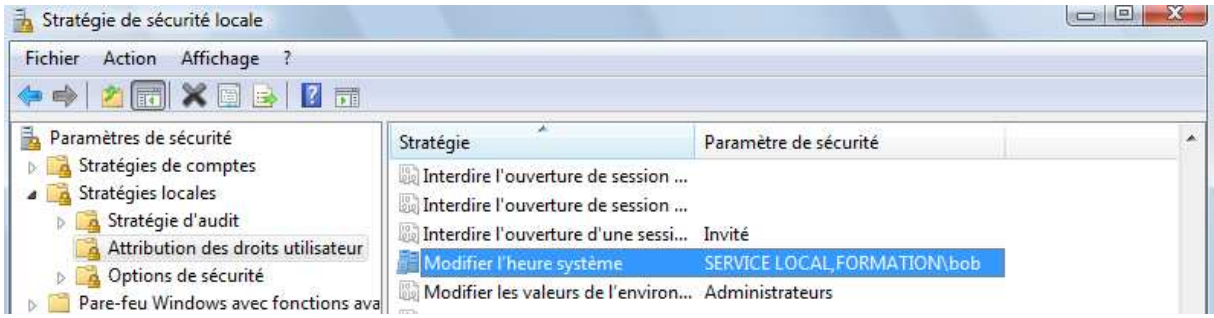
On modifie donc la **Default Domain Policy**



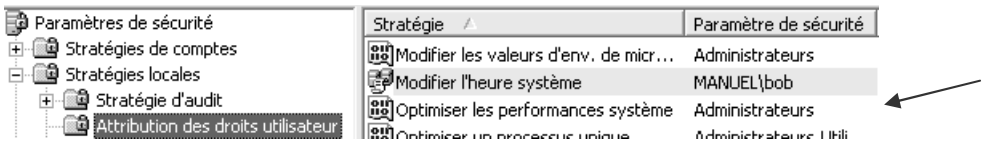
Pour ajouter un utilisateur "bob" ayant ce privilège de changer l'heure système…



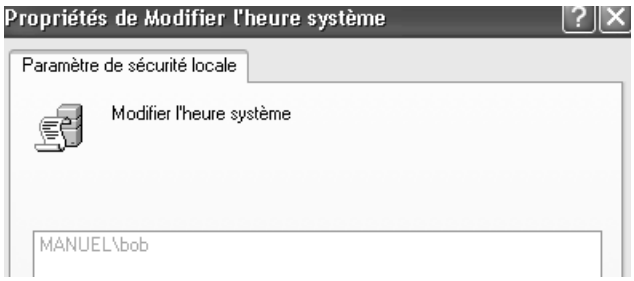
Sur le client Seven – Vista du domaine, la **stratégie locale** ne montre qu'une seule colonne, (le service local est maintenu !) et bob est ajouté…



Sur le client XP du domaine, Lorsque la stratégie de domaine à pu se propager, normalement la visualisation de la **stratégie locale** sera marquée d'une icône indiquant qu'elle vient du Domaine,  et non pas localement. 

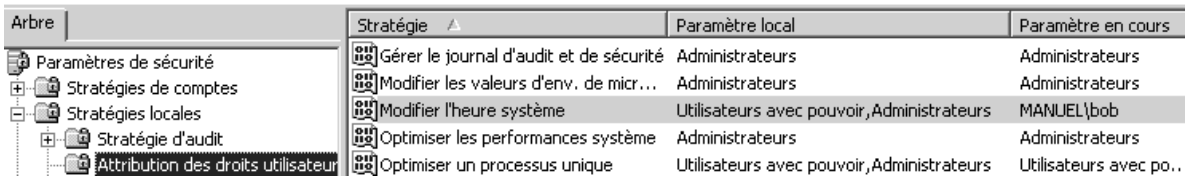


Avec bob uniquement



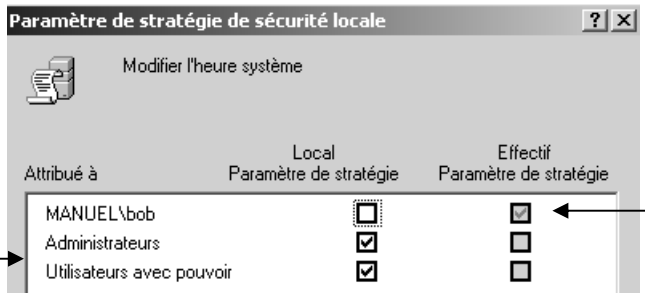
en grisé

Sur le client 2000 du domaine



Avec bob uniquement

Pas de changement localement



Mais ici on a récupéré la stratégie de domaine

STRATEGIES CONTROLEUR DE DOMAINE

Stratégies de Contrôleur de Domaine :

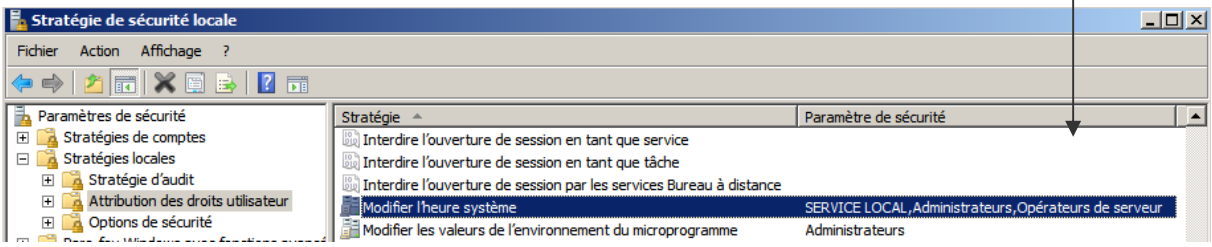
Lorsque l'on configure une stratégie de **Contrôleur de domaine**, cela signifie que l'on souhaite que cette stratégie s'applique à toutes les machines ayant ce rôle, et uniquement celles-ci.

Cela peut représenter uniquement notre serveur CD, mais cela peut aussi en représenter plusieurs… (visibles dans l'UO **Domain Controllers**)

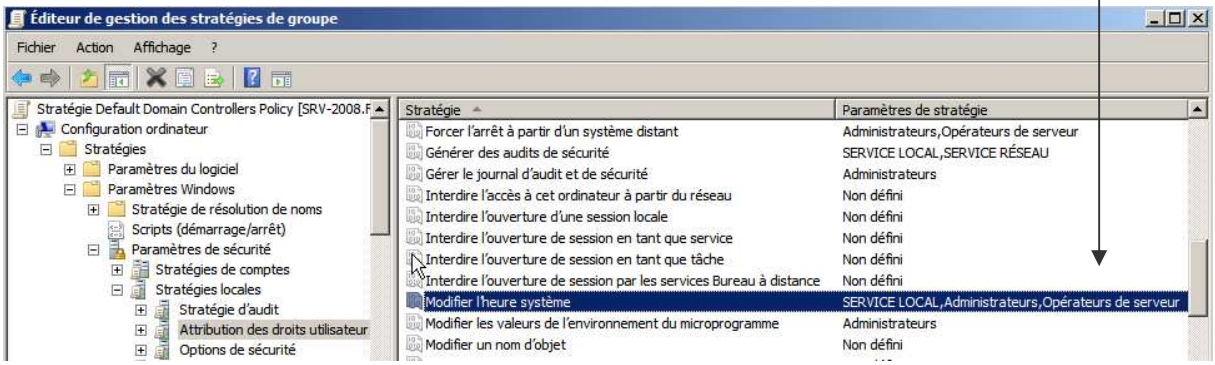
La stratégie de Contrôleur de Domaine existe, et elle possède plusieurs réglages actifs, qui risquent de s'opposer à ceux de la stratégie de Domaine !

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…)

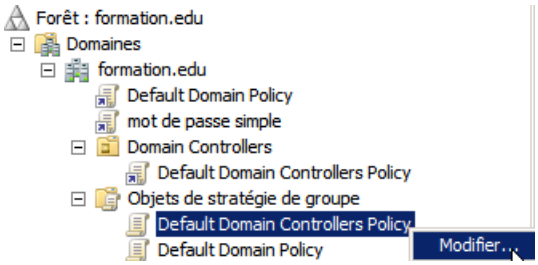


En fait la **Défault Domain Controller policy** est active…



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**

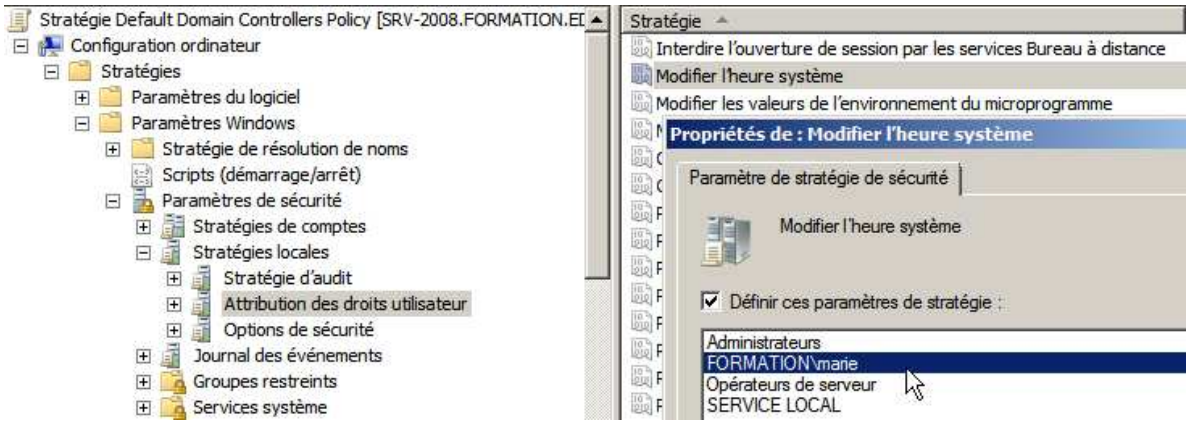
Exemple : Attribution droits Utilisateur Modifier l'heure DC :

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

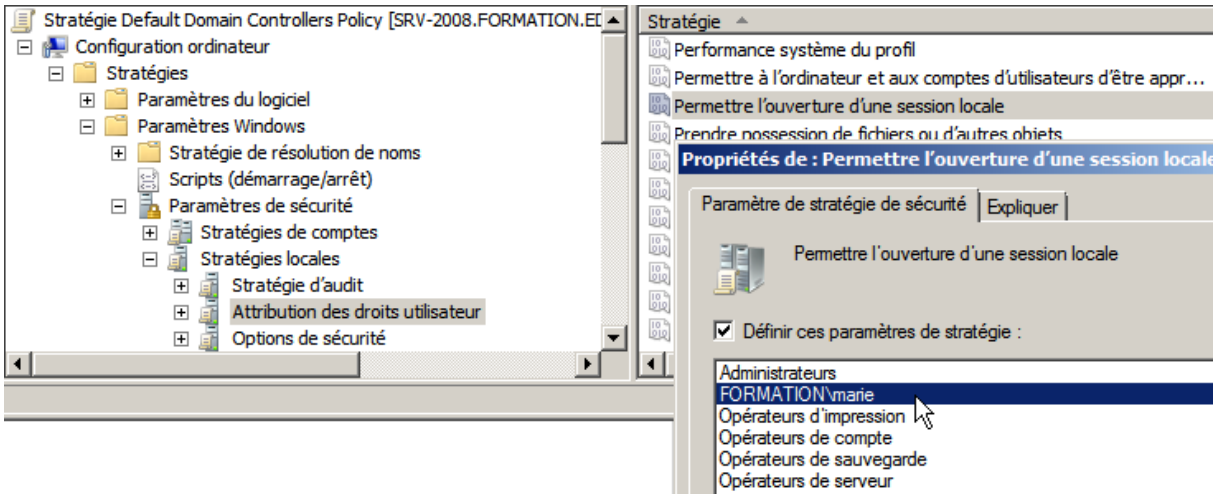
- **Modifier l'heure système**
- **Permettre l'ouverture d'une session locale**

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**

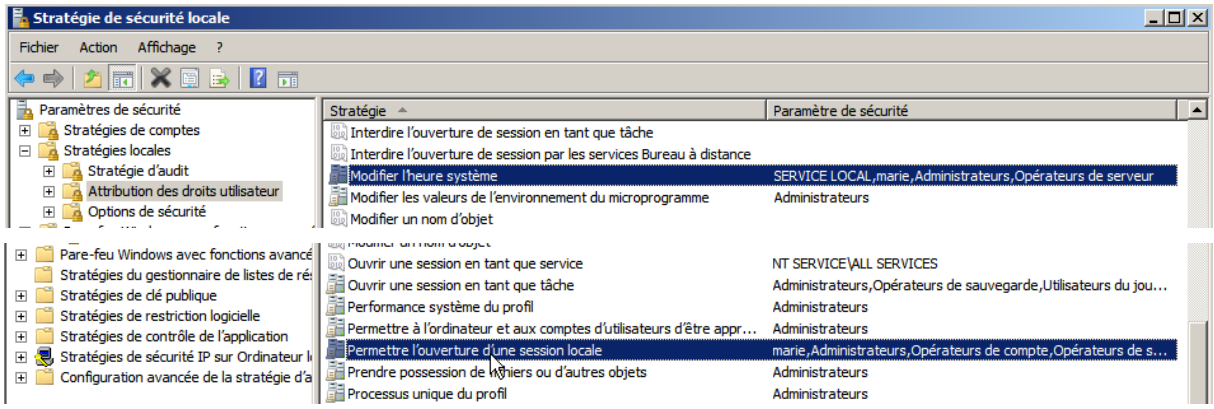


Et que l'utilisateur **marie** dispose aussi du droit d'**ouvrir une session localement**

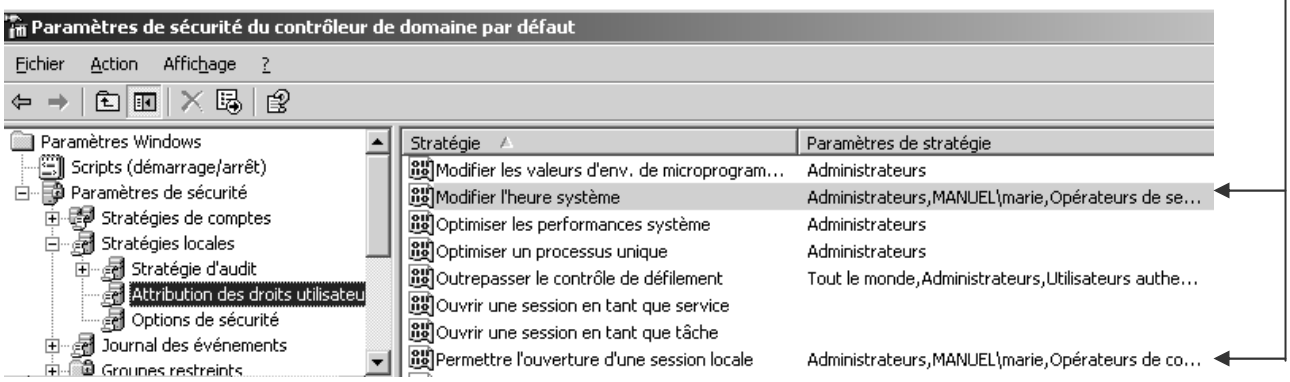


Vérification :

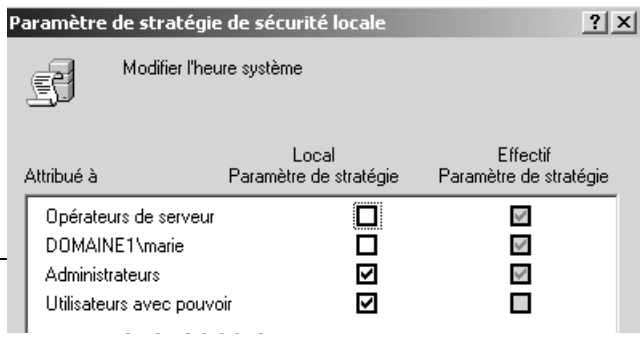
Sur le <u>serveur de Domaine 2008</u> les stratégies locales montrent bien

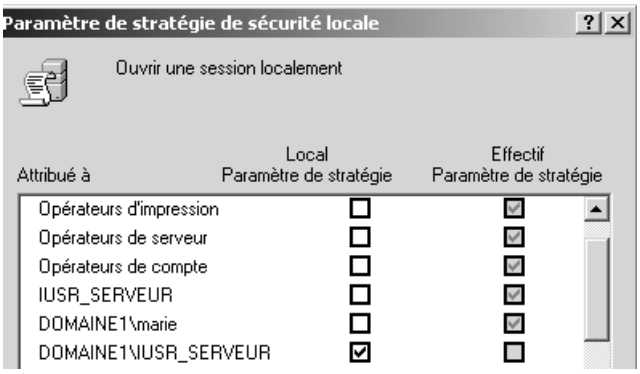


Sur le <u>serveur de Domaine 2003</u> les stratégies locales sont dévalidées… et seules les stratégies de sécurité du contrôleur de Domaine sont visibles!



Sur le <u>serveur de Domaine 2000</u>, on visualise alors les paramètres de **stratégie locale** qui montrent les options reçues au niveau du CD :



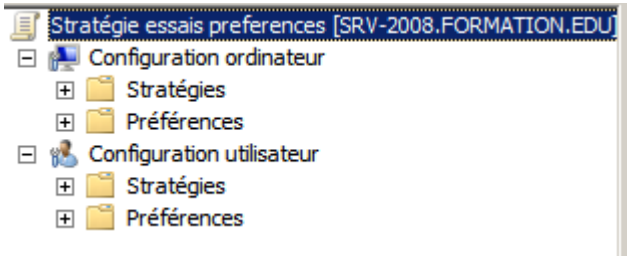


N.B : si on a plusieurs CD penser à propager la stratégie sur tous les CD…

STRATEGIES ET PREFERENCES

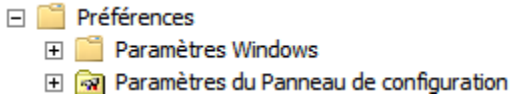
Les préférences 2008 Serveur :

Les préférences sont une nouveauté disponible sous 2008 uniquement sur un client Seven (natif) ou Vista - Xp dotés des… **Clients Side Extensions**.



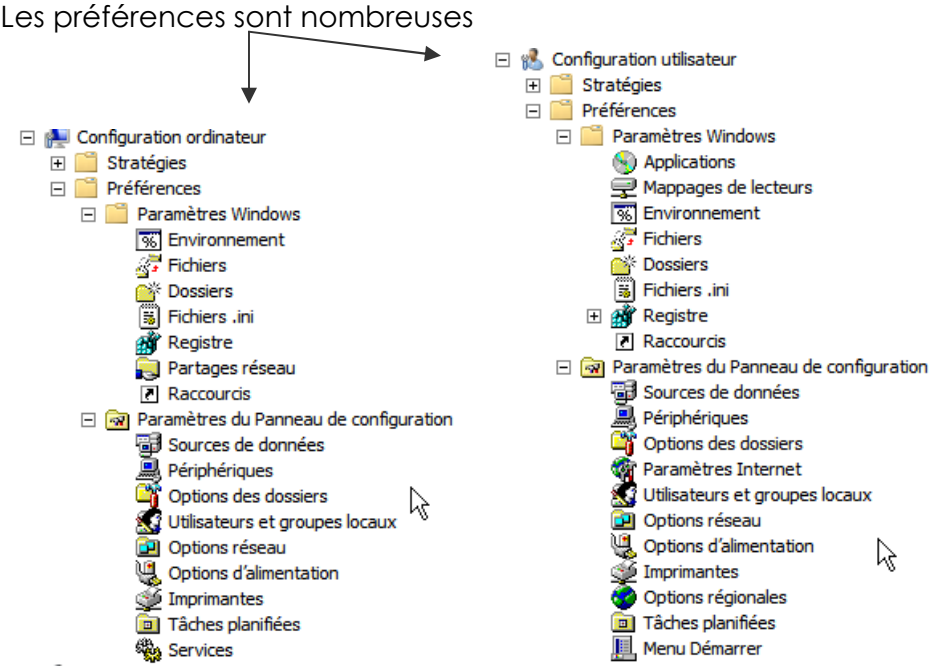
La différence fondamentale entre les préférences et les stratégies, réside dans le fait qu'une stratégie est toujours strictement appliquée, alors qu'une préférence peut être modifiée par l'utilisateur.

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



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

Les préférences sont nombreuses



Client Side Extension pour XP SP2 & Vista:

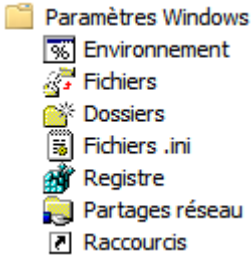
Côté client, vous devez déployer CSE : **Client-Side Extension** sur les systèmes suivants : (dans WSUS c'est un feature pack…)

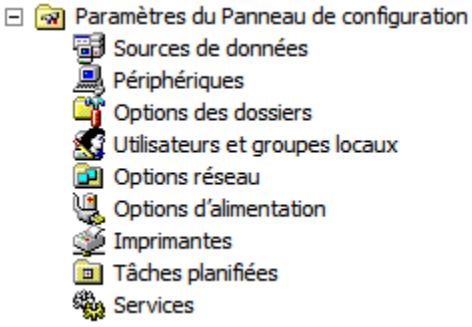
XP SP2

Vista

Principales Préférences Ordinateur :

On y trouve surtout

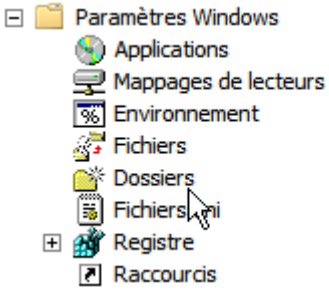


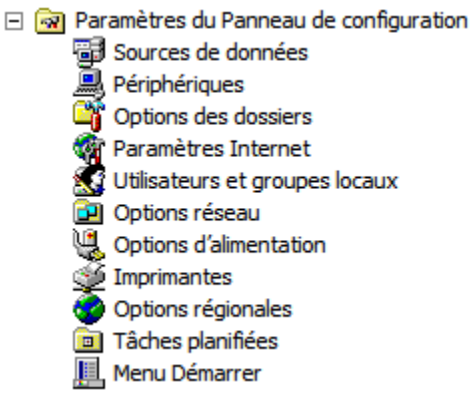


Mais principalement :

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. Vous pouvez agir soit au niveau d'une classe (ensemble d'objets) soit directement au niveau d'un objet. (pour couper l'accès au graveur de CD, désactiver les connexions sans fil.)

Option des dossiers

Possibilité de modifier les options de dossiers (pour Windows XP et pour Windows Vista) 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

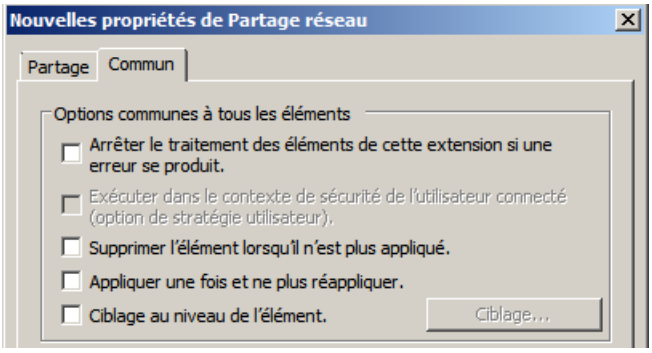
Possibilité de personnalisé le menu Démarrer des utilisateurs en paramétrant leurs propriétés. Il s'agit exactement des mêmes propriétés que vous retrouvez en local pour les postes sous Windows XP ou Windows Vista.

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:

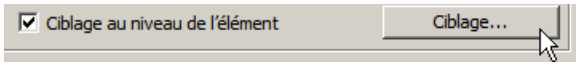
Contrairement aux paramètres de stratégies de groupes classiques qui sont retirés lorsque la GPO est supprimée, les préférences restent. Il est donc possible en cochant cette case d'obtenir le même comportement.

Appliquer une fois et ne plus réappliquer :

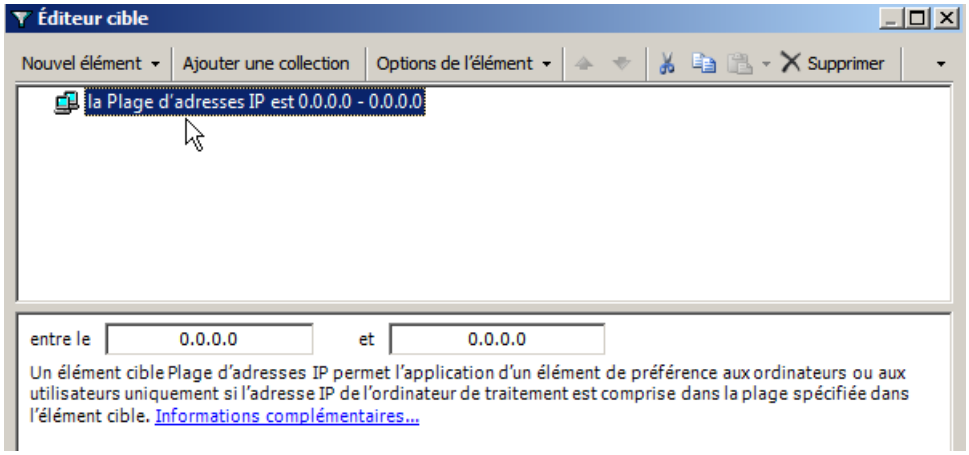
Les préférences sont actualisées toutes les 90 minutes par défaut (comme les stratégies). Du coup, si un utilisateur modifie les

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.

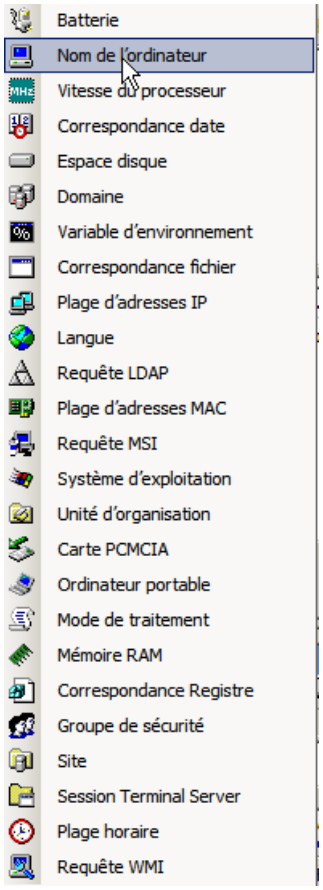
Ciblage au niveau de l'élément :



Permet de construire une requête…



Avec pas mal de choix…



MODELE DE STRATEGIES

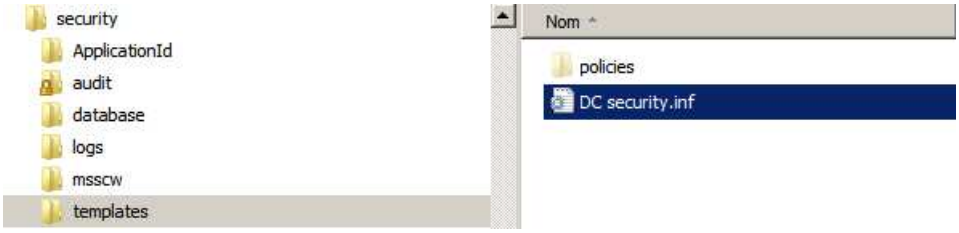
Les modèles de stratégie de sécurité:

N.B: La notion existe déjà sous NT4 avec les fichiers **Ntconfig.pol**, que l'on créait avec le poledit de NT, voire sous win95-98 avec les fichiers **Config.pol** que l'on créait avec le poledit de windows…
on peut continuer à s'en servir en plaçant ces fichiers dans **SYSVOL\Sysvol\domaine\Scripts**…(là où l'on met les scripts de connexion)

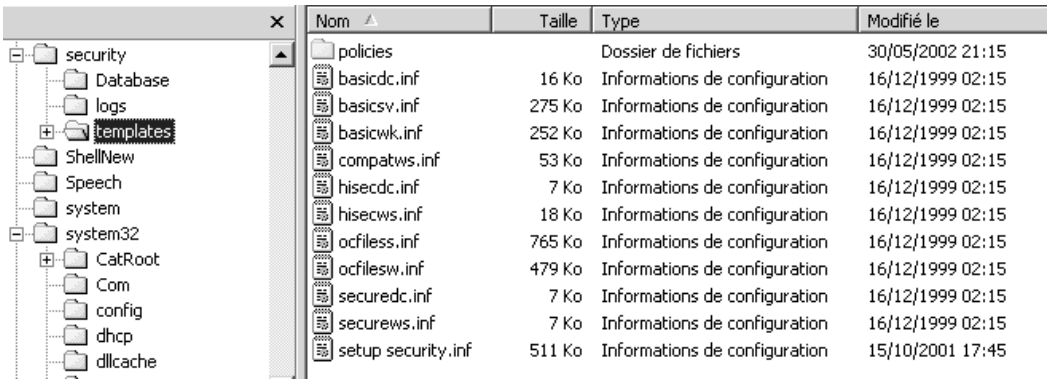
Par rapport aux variables modifiables via les paramètres de sécurité locale, les stratégies de groupes nommées aussi **GPO** fonctionnent avec une notion de modèle. Ce modèle étant exportable, on pourra, dans le chapitre suivant, voir comment créer des **GPO de domaine** , ou **d'Unité Organisationelle**…

Pour l'instant, on va dire que **un modèle de stratégie**, permet **de modifier globalement la sécurité d'une machine par l'application d'un modèle pré-défini** (ou bien défini par nous même), alors que les paramètres de sécurité locale nécessitaient une modification manuelle de chaque valeur…

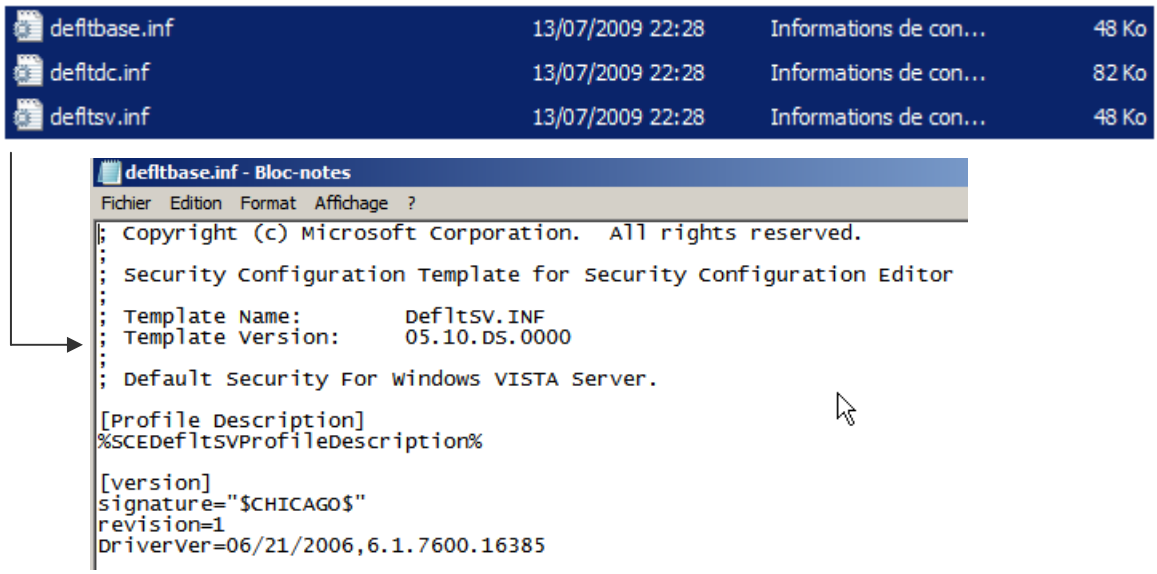
Les modèles de stratégie 2008 sont non- définis ! ou plutôt un seul modèle est crée au moment de la création du domaine dans un fichier **DC Security.inf** stocké en dans **%windir%\security\templates**



Les modèles de stratégie 2003 sont définis dans des fichiers xxxx**.inf** stockés en général dans **%windir%\Security\Templates**



Les modèles de stratégie pour Vista et Seven sont définis dans des fichiers xxxx**.inf** stockés en général dans **%windir%\inf**



La base de donnée dans laquelle on utilise le modèle est unique (une seule base par machine), et se trouve dans un fichiers **xxxxx.sdb** dans le dossier **Winnt\Security\Database**

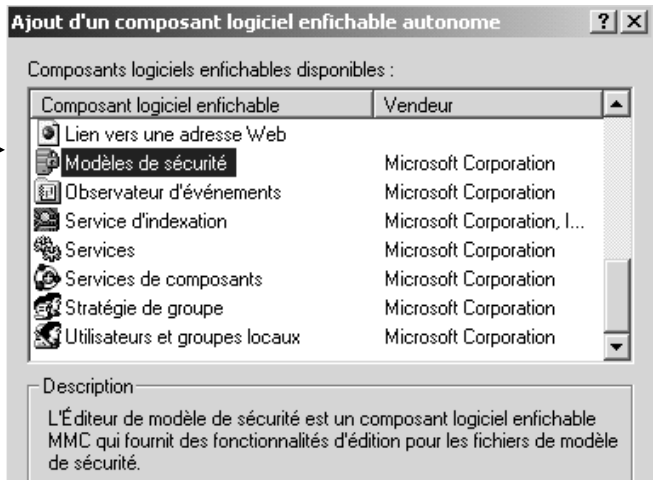
Il va falloir :

1. se créer un modèle (ou prendre un modèle prédéfini)
2. ouvrir le modèle dans la base de donnée de sécurité
3. appliquer la base de sécurité au poste

Création d'un modèle:

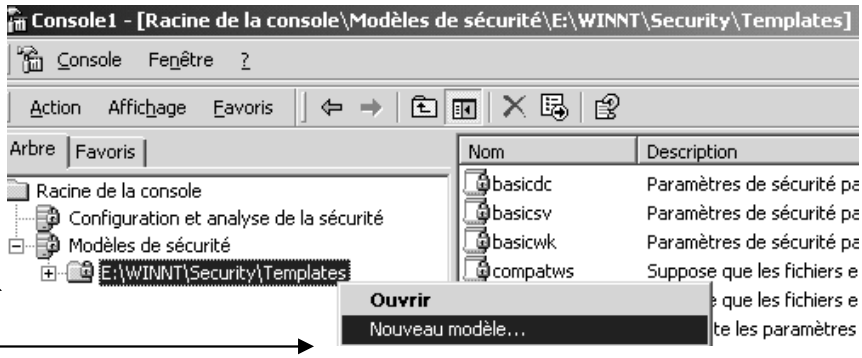
Il faut avoir une mmc permettant de gérer les modèles, cette mmc se nomme

Modèles de sécurité →



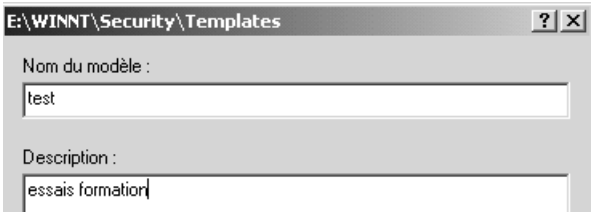
Dans cette mmc tous les modèles prédéfinis apparaissent évidemment on décide de se créer un modèle personnalisé

Clic droit sur le dossier dans lequel les modèles sont stockés



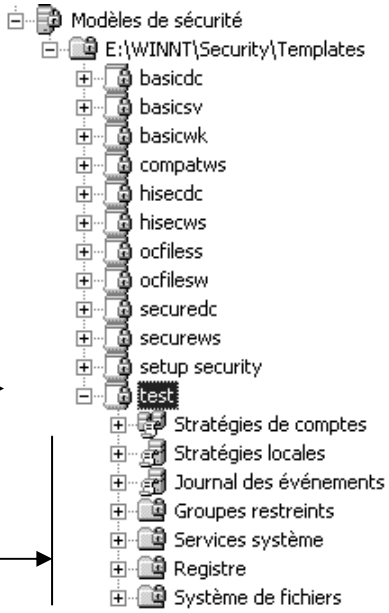
puis

Nouveau modèle



et on lui donne un nom

On obtient alors notre modèle de sécurité



Dans lequel on reconnaît les paramètres de sécurité que l'on modifiait auparavant en local, (ainsi que les autres…)

Effectuons une modification, pour l'instant un peu… futile (mais juste pour repérer notre modèle

Dans les **stratégies locales / options de sécurité**

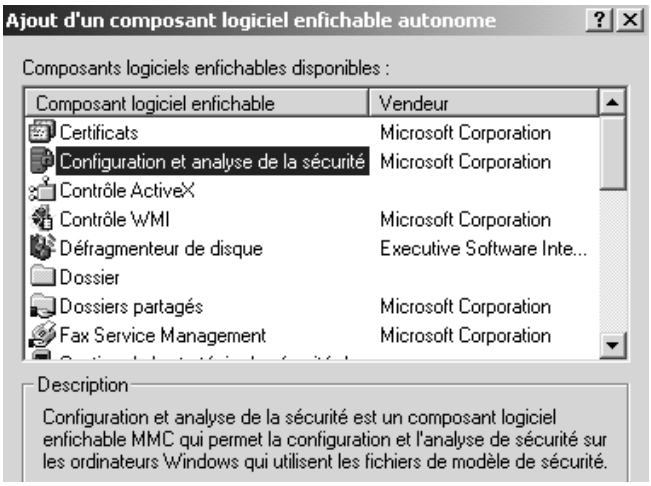
on prévoit de donner un message :"*strategie modele*", sans oublier le titre

Pour enregistrer le modèle, il faut se placer sur le modèle et demander **clic droit, enregistrer…**

Création d'une base locale de sécurité:

Il faut avoir une mmc permettant de gérer les bases, cette mmc se nomme

Configuration et analyse de la sécurité ⟶



Cette console permet d'ouvrir une base de donnée existante (pour la manipuler) ou en crée une nouvelle à l'aide d'un modèle…

Pour ouvrir une base de donnée existante

1. Cliquez-droit sur l'élément étendu de *Configuration et analyse de la sécurité.*
2. Cliquez sur **Ouvrir la base de données**
3. Sélectionnez une base de données et cliquez sur **Ouvrir**

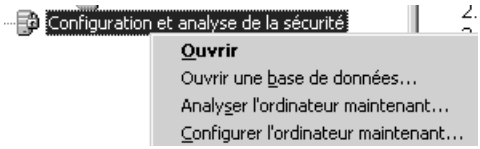
Pour créer une nouvelle base de données

1. Cliquez-droit sur l'élément d'étendue *Configuration et analyse de la sécurité.*
2. Cliquez sur **Ouvrir la base de données**
3. Entrez un nouveau nom de base de données et cliquez sur **Ouvrir**.
4. Sélectionnez un fichier de configuration de sécurité à importer puis cliquez sur **Ouvrir**.

Nous avons besoin de la créer donc on va

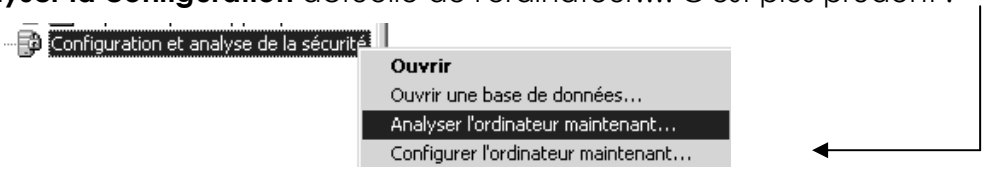
1. Ouvrir la base,
2. lui donner le nom **essais.sdb**
3. sélectionner le fichier **test.inf** crée auparavant…
4. demander ouvrir

Maintenant nous avons une base de donnée crée avec un modèle chargé ! et les commandes **Analyser** … **Configurer** sont disponibles !



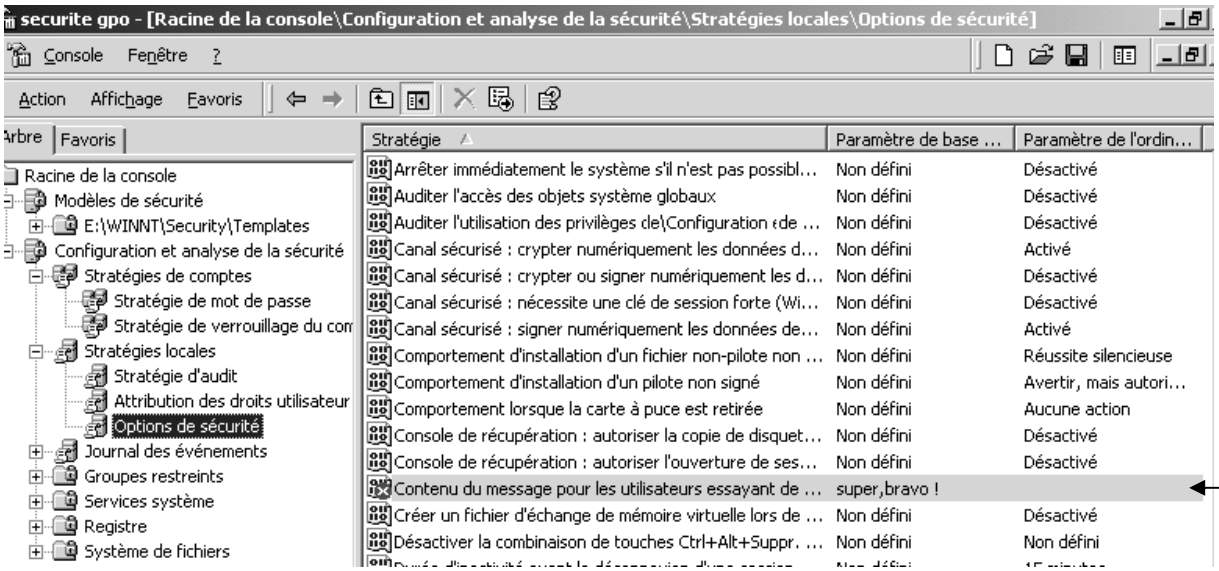
Vérification modèle - poste:

Il est possible désormais soit d'appliquer notre modèle à l'ordinateur, soit de **analyser la configuration** actuelle de l'ordinateur…. C'est plus prudent !



on accepte le chemin du journal par défaut

puis on peut parcourir l'arborescence **pour visualiser les différences entre le modèle chargé, et la configuration actuelle**!

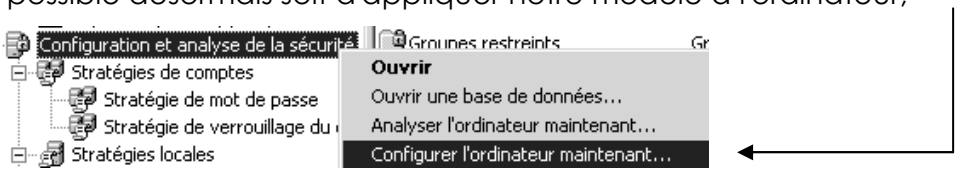


NB: toutes les différences sont marquées d'une croix rouge

Lorsque l'on est content, on peut appliquer notre modèle + base à notre machine

Application du modèle sur le poste

Il est possible désormais soit d'appliquer notre modèle à l'ordinateur,



Si on effectue une vérification après application, les modifications sont marquées d'une coche verte…

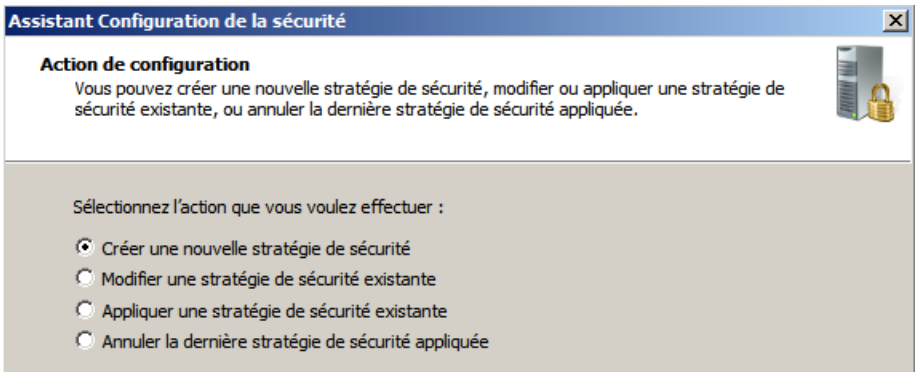
Modification du modèle

Si on souhaite modifier notre structure, on modifie le modèle, puis dans la base actuelle on importe la nouvelle mouture du modèle….

On peut aussi se créer une nouvelle base, pour être sûr de partir sur le bon pied…

Assistant 2008 et Modèles pré définis

Sous 2008 un assistant pour la création de modèle existe, disponible dans le **Panneau de Configuration / Outils d'administration / Assistant Configuration de la Sécurité**



Les modèles de sécurité prédéfinis sous 2003 SRV et client XP sont :

- Réappliquer les paramètres par défaut (**Setup security.inf**),
- Sécuriser la racine du système (**Rootsec.inf**)

Les modèles de sécurité prédéfinis sous 2000 sont :

- Station de travail par défaut (basicwk.inf)
- Serveur par défaut (basicsv.inf)
- Contrôleur de domaine par défaut (basicdc.inf)
- Station de travail ou serveur compatible (compatws.inf)
- Station de travail ou serveur sécurisé (securews.inf)
- Station de travail ou serveur hautement sécurisé (hisecws.inf)
- Contrôleur de domaine sécurisé (securedc.inf)
- Contrôleur de domaine hautement sécurisé (hisecdc.inf)

N.B : chargez le modèle de sécurité **Setup security.inf** sur votre poste de travail, analysez votre machine (mais n'appliquez pas….) que peut on dire ?

Sachez toutefois que ces modèles modifient de manière incrémentielle les paramètres de sécurité par défaut, s'ils sont présents sur l'ordinateur. Ils n'installent pas les paramètres de sécurité par défaut avant d'effectuer les modifications

---

Résumé

On se:	crée un modèle xxxxx.inf	(rien ne se passe)
	On ouvre/crée une base de donnée xxxx.sdb	(rien ne se passe)
	On importe un modèle	(rien ne se passe)
	On analyse différence entre base et registre	(rien ne se passe)
	On configure le poste	(on modifie la base de registre)

N.B: à partir du moment ou l'on a configuré le poste, la base contient des informations différentes du modèle utilisé, car elle est un résultat de (modèle+registre). Dans le doute, refaire une base avec une copie propre du modèle et recommencer. A la limite, appliquer le modèle de sécurité de base, puis ré appliquer le modèle spécifique

N.B: Faire attention aux modèles dans lesquels on ne spécifie rien pour une clé, cela ne rétablira pas la clé dans sa valeur par défaut, mais cela la laissera en l'état

N.B: Faire attention à appliquer des modèles construits sur un OS même type-version, cela peut éviter quelques surprises…

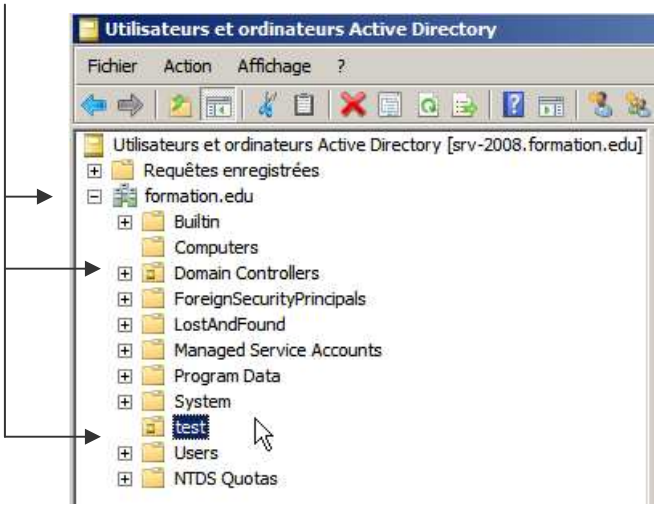
GPO D'UNITE ORGANISATIONELLE

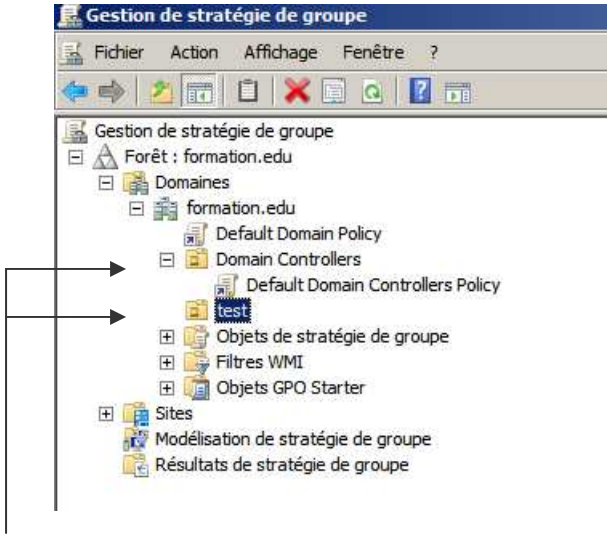
Types et niveaux de stratégie :

GPO signifie **Group Policy Object**

On l'a déjà dit mais rappelons que l'on peut poser des stratégies 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…**

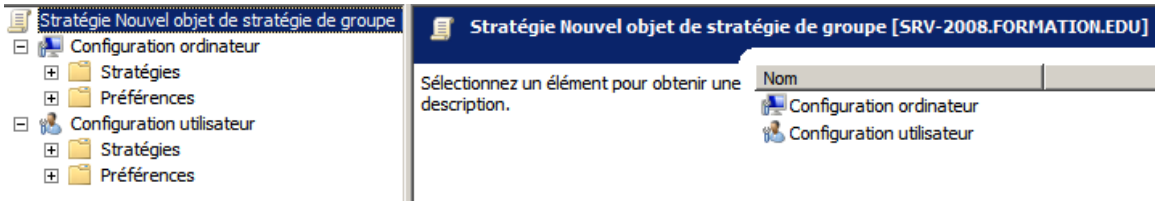




On les retrouvera dans la console **Gestion des stratégies de groupe !**

N.B: il est possible ce 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**

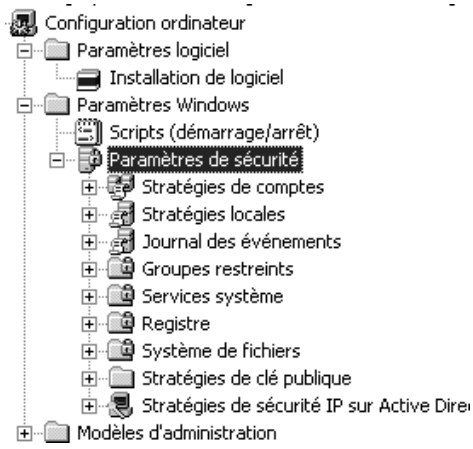
Par défaut, les stratégies de groupes ont un traitement synchrone, c'est à dire :

- 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 ou 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

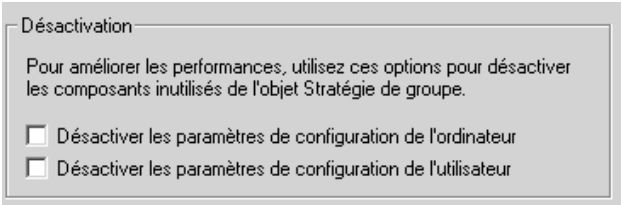


Les ajouts notables dans les **stratégies de groupe pour les utilisateurs** sont:

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 dan 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.

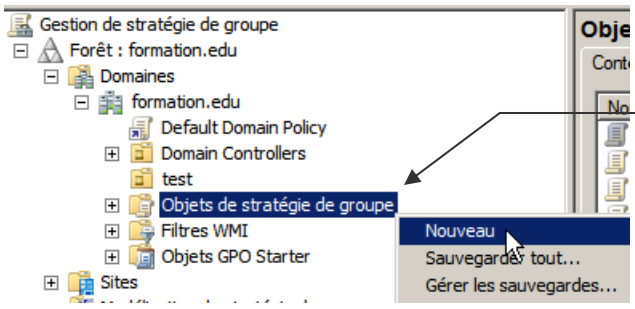
Lorsque l'on manipule les paramètres de **stratégies de sécurité de groupe**, on fixe les modifications dans la base de registre au niveau des clés qui seront effacées si la GPO ne s'applique plus, en clair les paramètres de stratégies GPO ne s'appliquent plus, et on retrouvera les paramètres de stratégie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

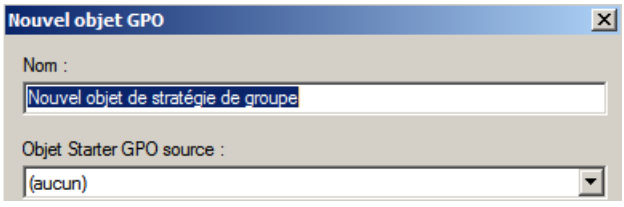
On lui donne un nom explicite avec une convention utile, par exemple

strat = stratégie

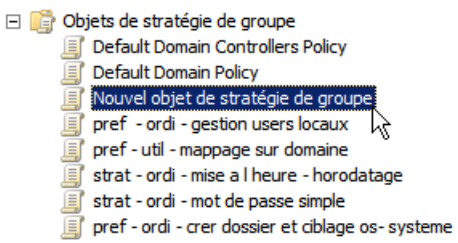
pref = préférence

o = ordinateur

u = utilisateur



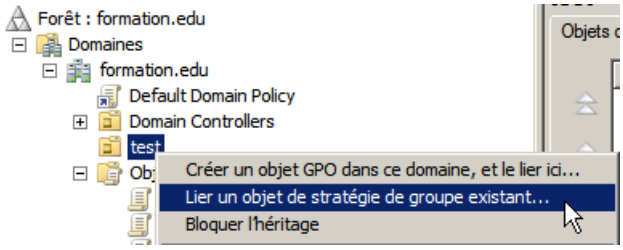
et on la modifie clic – droit / **Modifier**



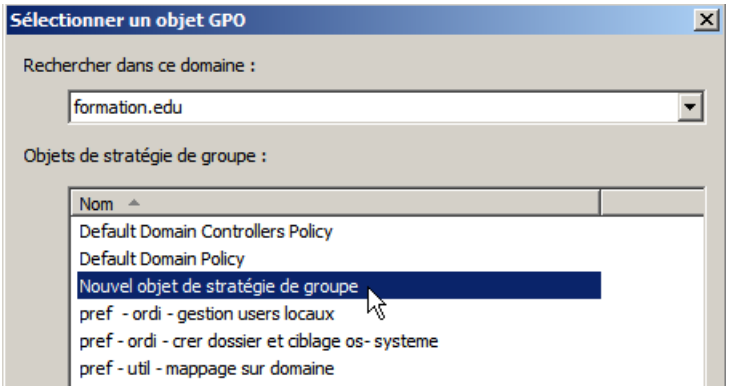
N.B: les tp suivant porteront sur le "contenu"… d'une stratégie…

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…**

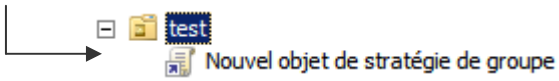


Tous les objets apparaissent



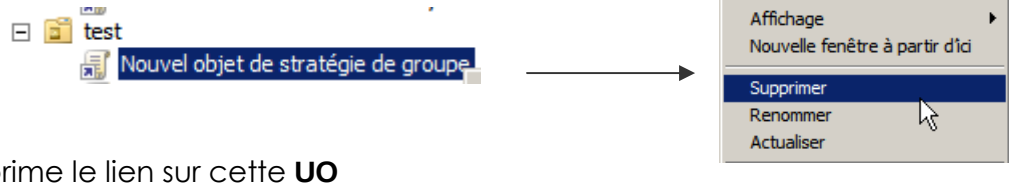
ok

Et un pointeur (indiquant un lien) se crée :

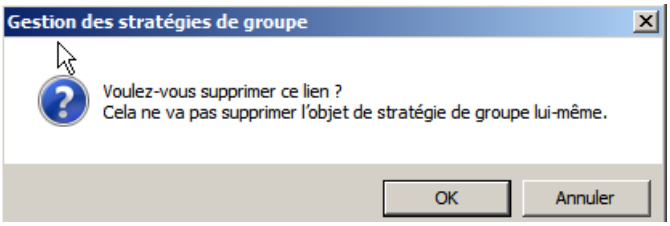


N.B: une stratégie peut être liée sur plusieurs UO, c'est bien le principe même… par conséquent son nom ne doit jamais mentionner l'UO sur laquelle elle s'applique, mais toujours na nature (stratégie, préférence… ordinateur, utilisateur…), et son objectif (son action…)

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

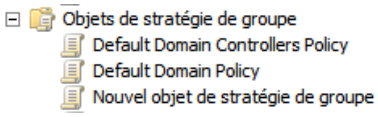


Cela supprime le lien sur cette **UO**

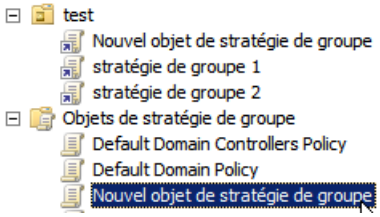


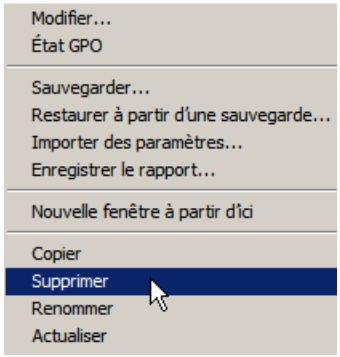
(par défaut OUI)

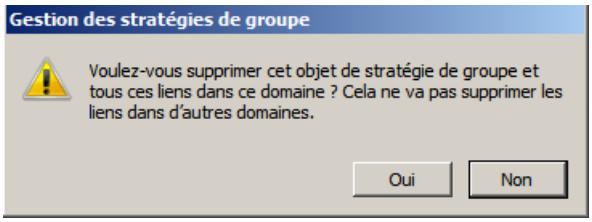
Mais la stratégie reste disponible



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







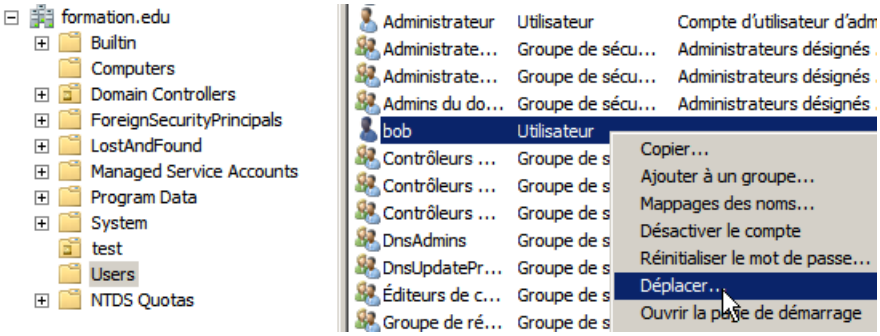
(par défaut NON)

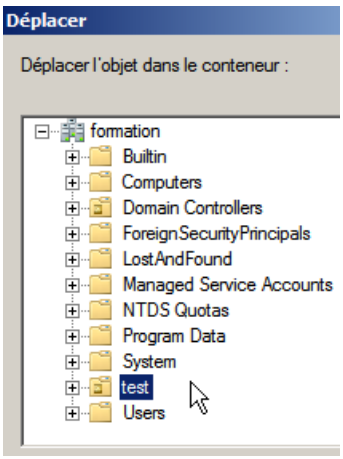
Et on supprime la Stratégie, et aussi tous les liens qu'elle pouvait avoir…

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…





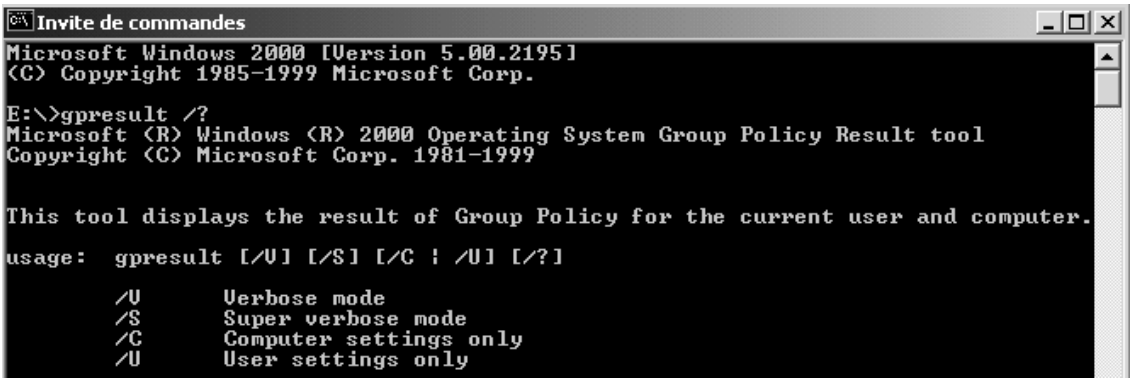
Et de même un compte ordinateur…

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 la machine pc-seven en sont affectés !

Vérification et utilitaire Gpresult.exe

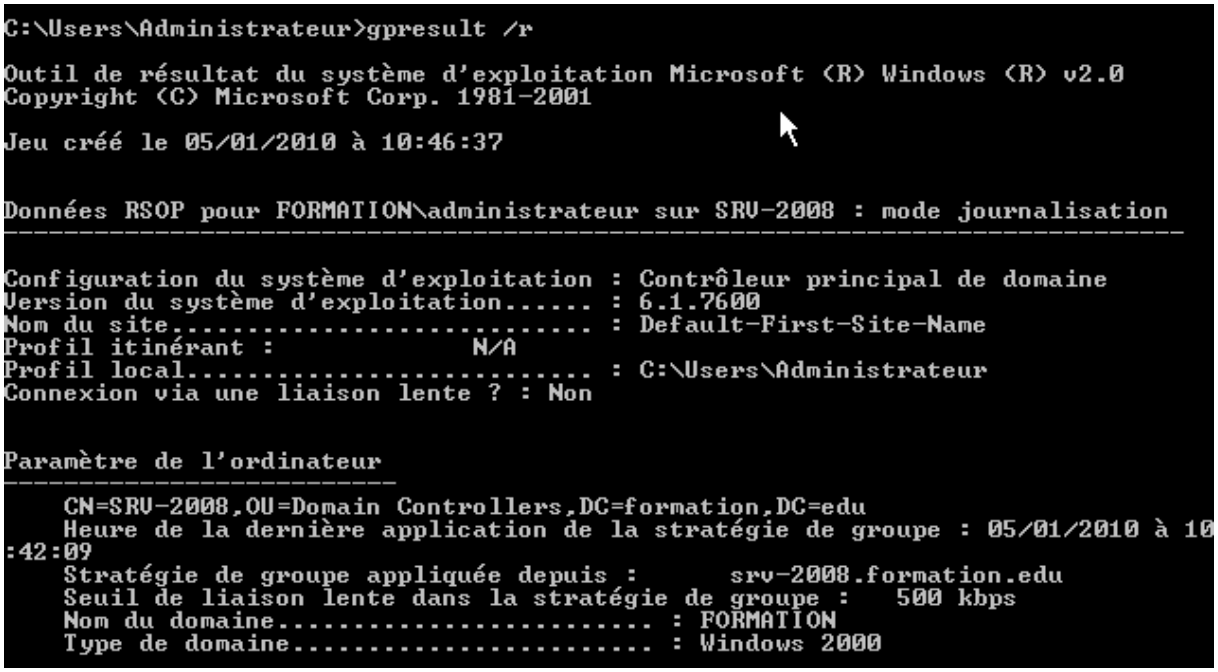
Il existe un utilitaire Disponible depuis XP (par le du kit de ressource technique et natif sous les versions récentes permettant d'avoir un compte rendu sur une machine des GPO sui se sont appliquées

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 utilsiateurs…

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)

- Pour des client SEVEN VISTA XP(PRO) serveur 2000-2003-2008 Hors Domaine:

  stratégies locales

- Pour des client SEVEN VISTA XP(PRO) En Domaine serveur 2000-2003 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

- Pour des serveurs 2000 et 2008 Contrôleurs de Domaine:

  stratégies locales / stratégies de domaine / stratégies de CD

  et si la notion de site est activée

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

- Pour des serveur 2003 Contrôleurs de Domaine: (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 activée

  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 ou l'on définirait des stratégies contradictoires, il faut savoir que normalement les **stratégies ordinateurs** prennent le pas sur les **stratégies utilisateurs**.

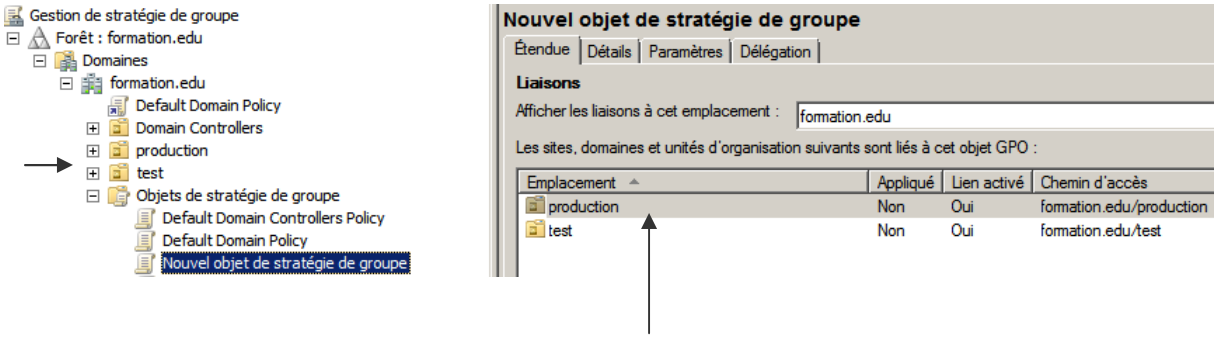
LIAISONS MULTIPLES - PRIORITE - HERITAGE –DES GPO

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**.

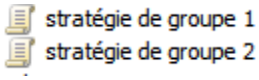
On a aussi vu que l'on pouvait appliquer la même **GPO** à deux **UO** différentes…

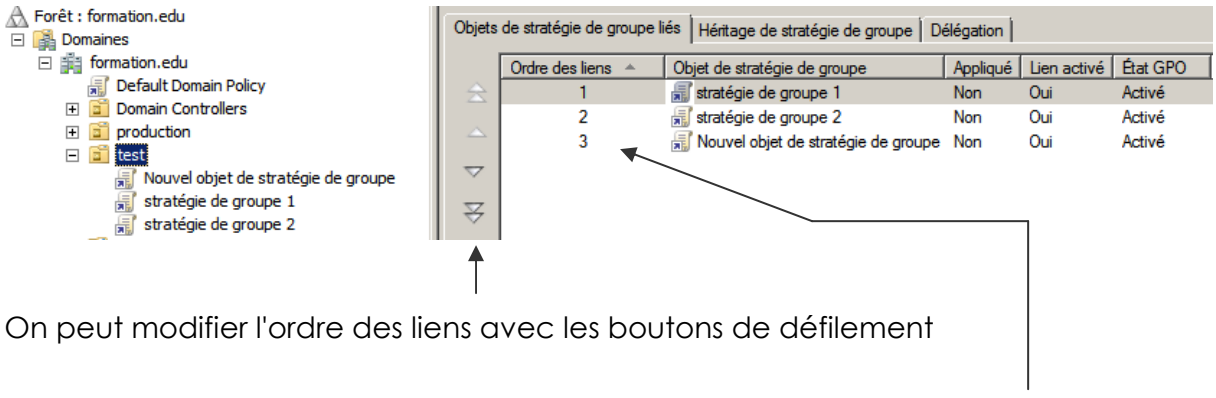
Créons une UO "production" sur laquelle on applique la même GPO …



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*

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…)

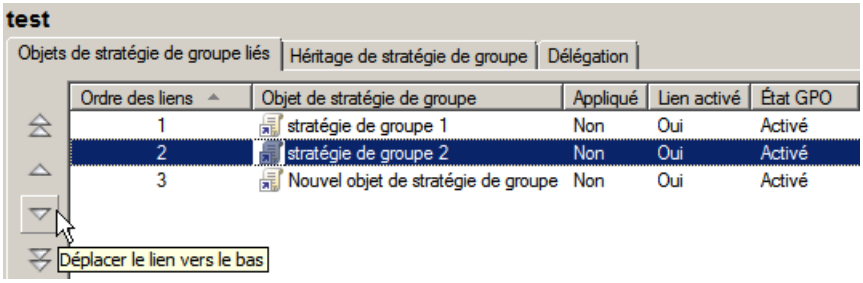




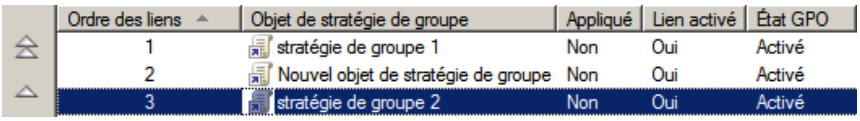
On peut modifier l'ordre des liens avec les boutons de défilement

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

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 3…



Pour obtenir

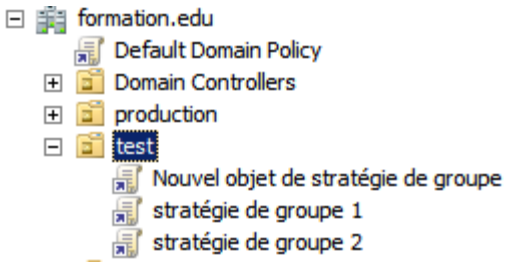


---

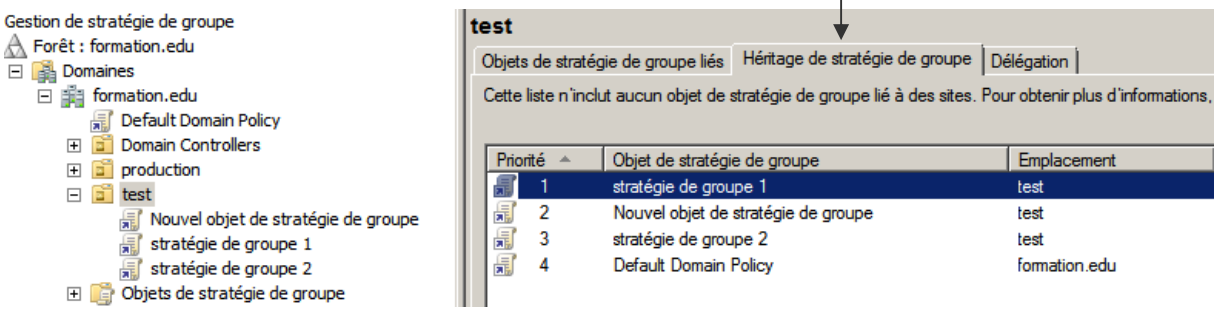
héritage – bloqué :

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

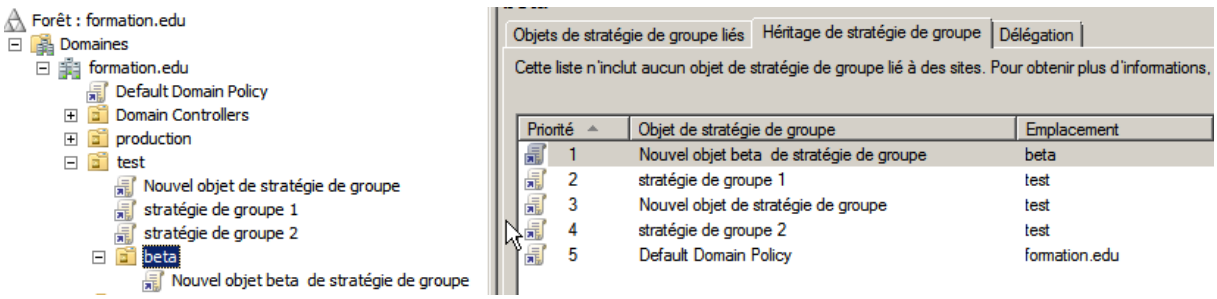
ainsi par "héritage", notre stratégie de Domaine **Default Domain Policy** se propage dans notre UO test



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

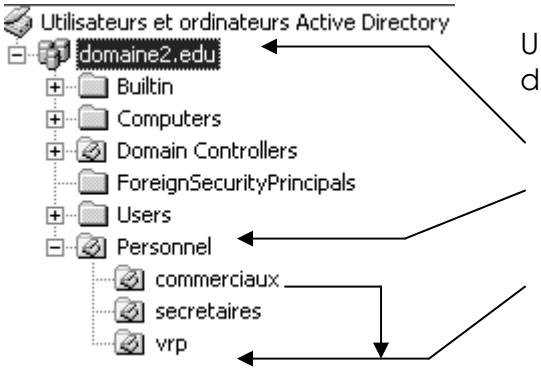


Et ainsi de suite



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.

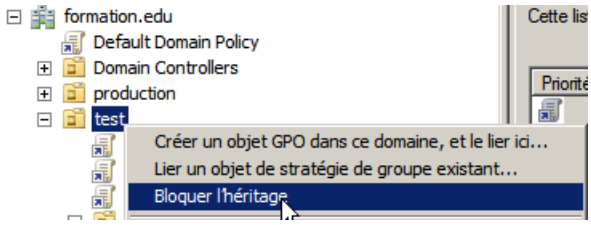


Un élément placé dans l'UO **vrp** reçoit donc ici :

- 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

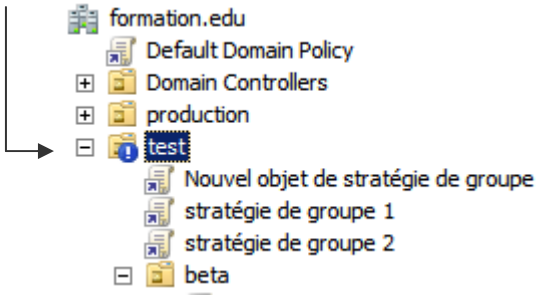
N.B: En cas de conflit sur un même élément défini à différents niveaux, le principe étant de dire "c'est le dernier qui cause, qui a raison" une exception, lorsque les paramètres qui rentrent en conflits sont exprimés dans des paramètres utilisateurs, et des paramètres ordinateurs. Dans ce cas, généralement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

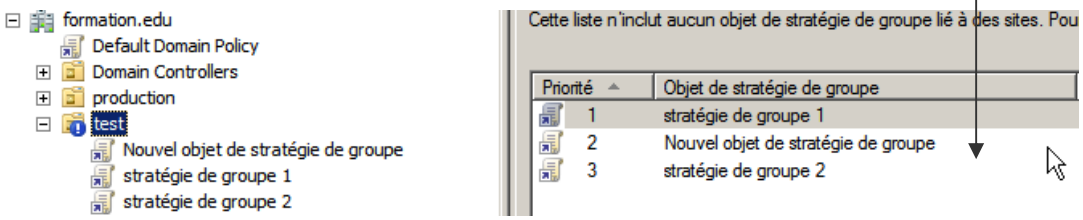


par exemple sur l'UO test

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**

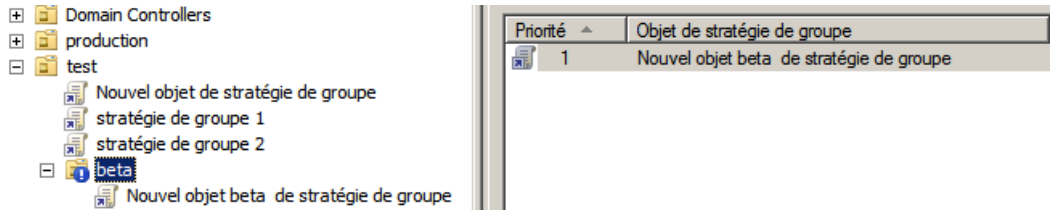
N.B: lorsque l'on bloque un héritage, on bloque cet héritage pour toutes les stratégies qui pourraient venir… sauf celles qui ont été spécifiées avec la mention "**aucun remplacement**" (cf chapitre suivant)

---

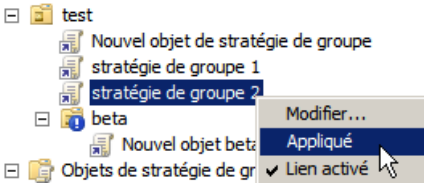
héritage - appliqué:

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…

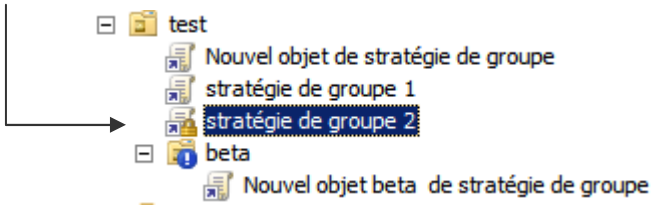


Mais on décide que la stratégie de groupe 2 doit s'appliquer tout le temps dans toutes les conditions…

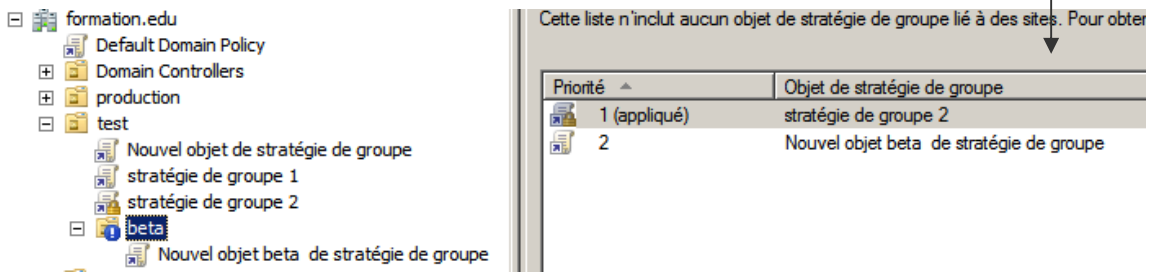


On se place dessus et on demande clic-droit **Appliqué**

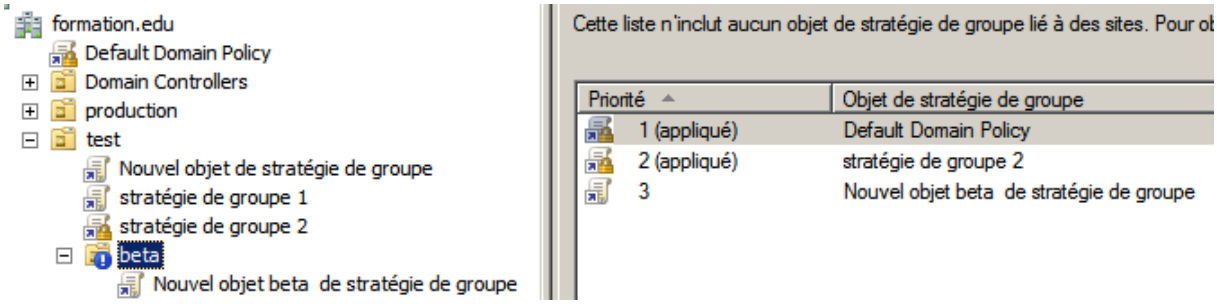
Cela se traduit par un Cadenas !



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

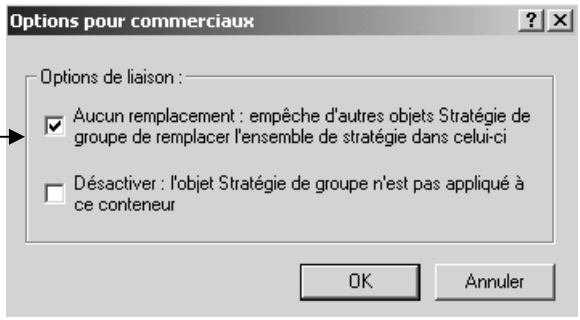


On peut procéder de même pour la **Default Domain Policy**…

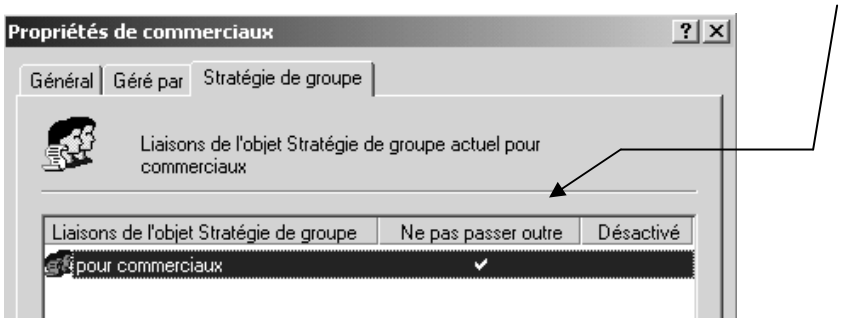


Sous 2003, Pour forcer une stratégie à être appliquée, on devait demander sur cette stratégie, **Option**

Et demander alors **Aucun remplacement**



Cela se visualisait sous la forme d'une coche **Ne pas passer outre**

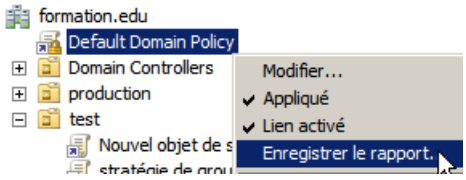


GESTION ET SAUVEGARDE DES GPO

Résumé de la stratégie :

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

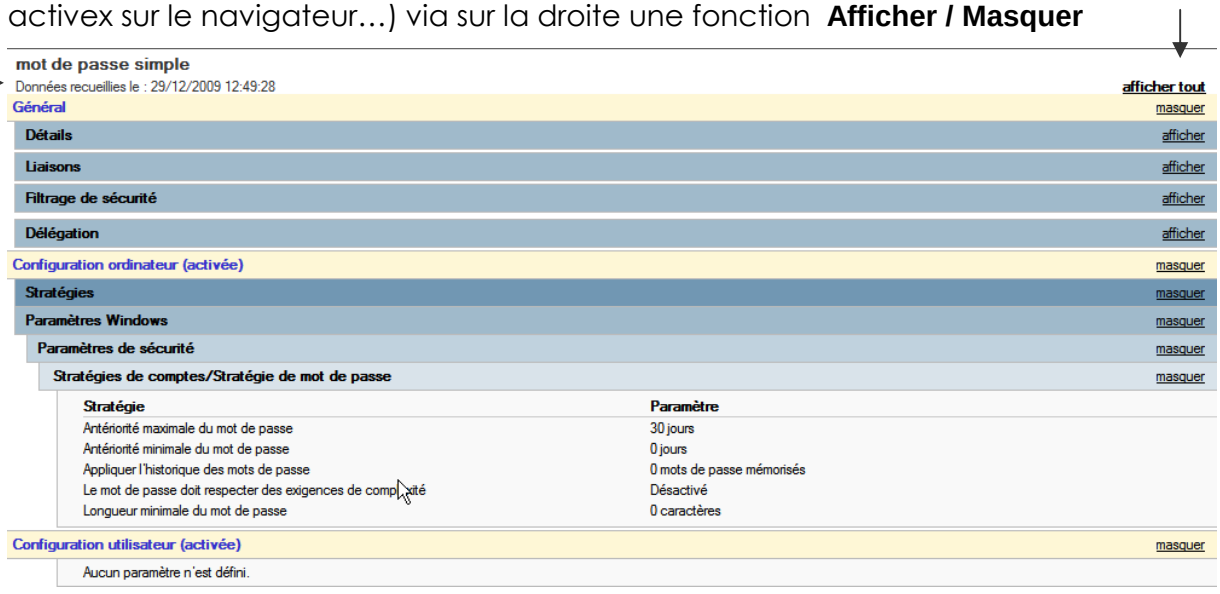
Cela se demande sur une **GPO** via le bouton droit : **Enregistrer le rapport…**



Et on indique ensuite un dossier et un nom de fichier (au format HTML)

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

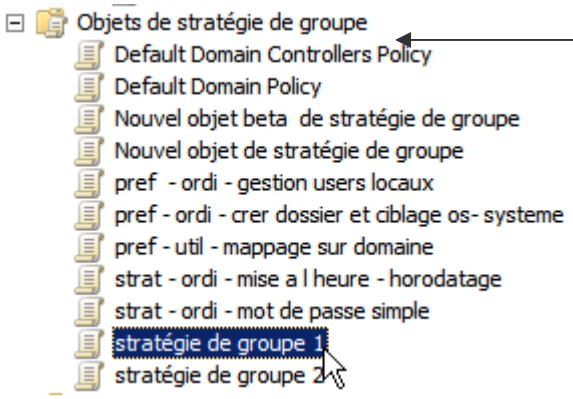
Ces fichiers sont ensuite facilement visualisables (a condition d'autoriser les activex sur le navigateur…) via sur la droite une fonction **Afficher / Masquer**



Copier une stratégie :

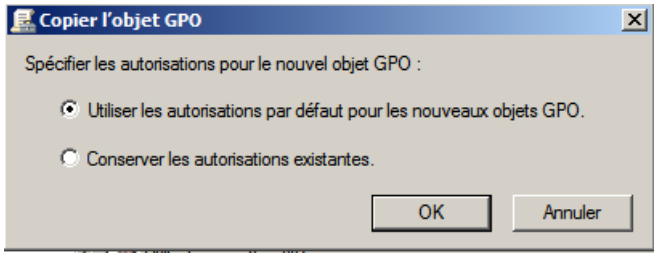
Si on souhaite copier une stratégie, pour repartir de cette base et la retravailler, par exemple on veut copier la "stratégie de groupe 1"

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**

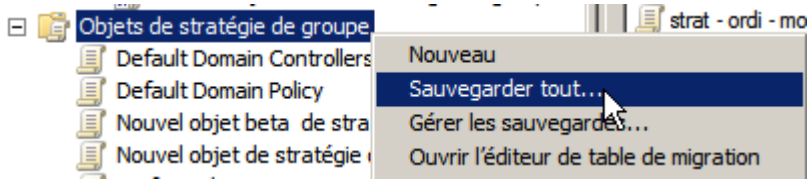
Alors on réponds



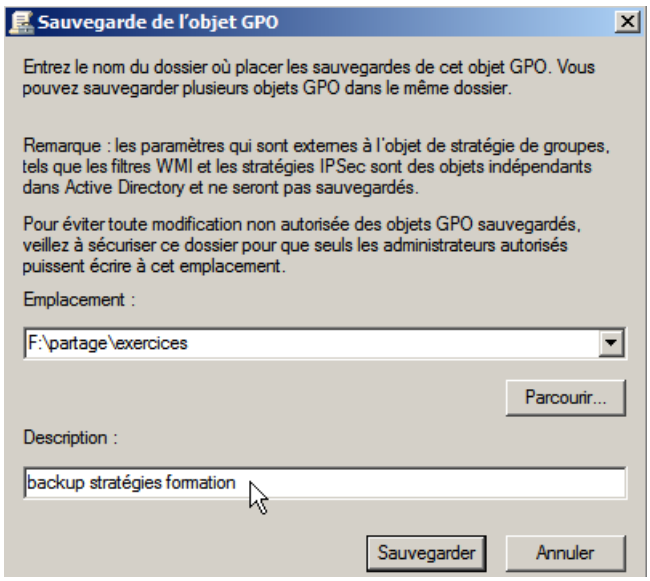
On a confirmation, et voila…

Sauvegarder les stratégies :

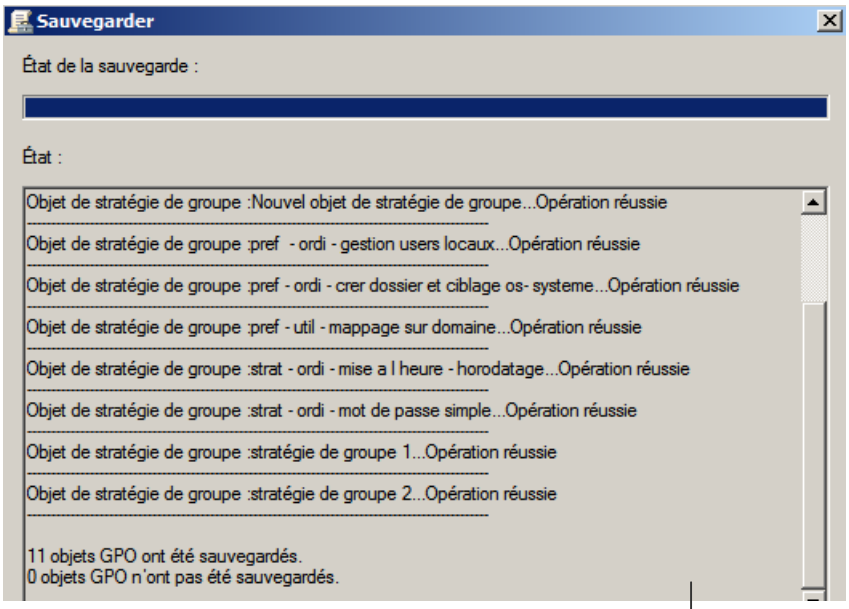
Le plus simple est de se placer sur le dossier **Objets de stratégies de groupe** et demander **Sauvegarder tout…**



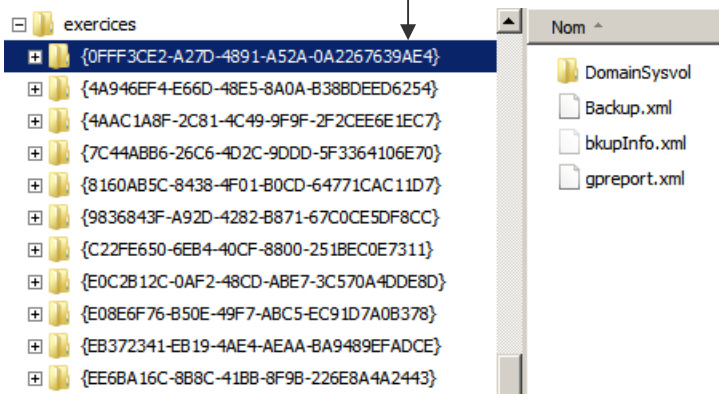
Il faut indiquer un emplacement



on a une confirmation

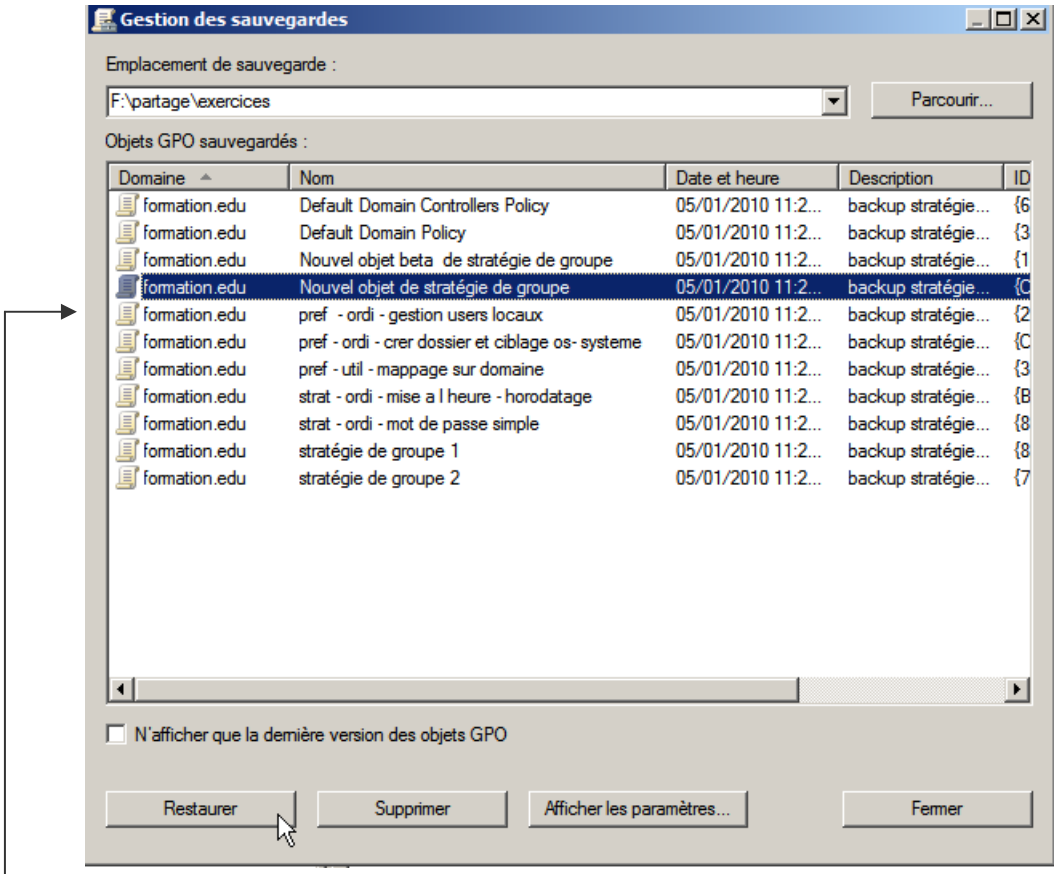


et voila…

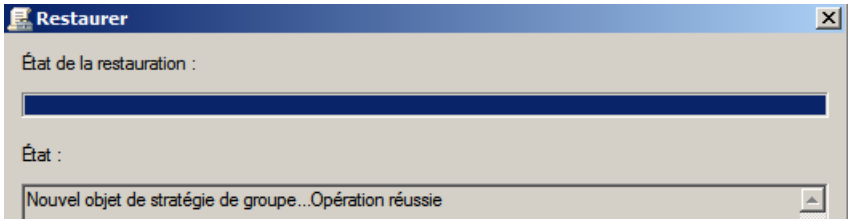


Restaurer les stratégies :

Dans la même logique sur le dossier **Objets de stratégies de groupe** et demander **Gérer les sauvegardes…**



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



une confirmation

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

GPO - MODELES D'ADMINISTRATION

Les Modèles présents

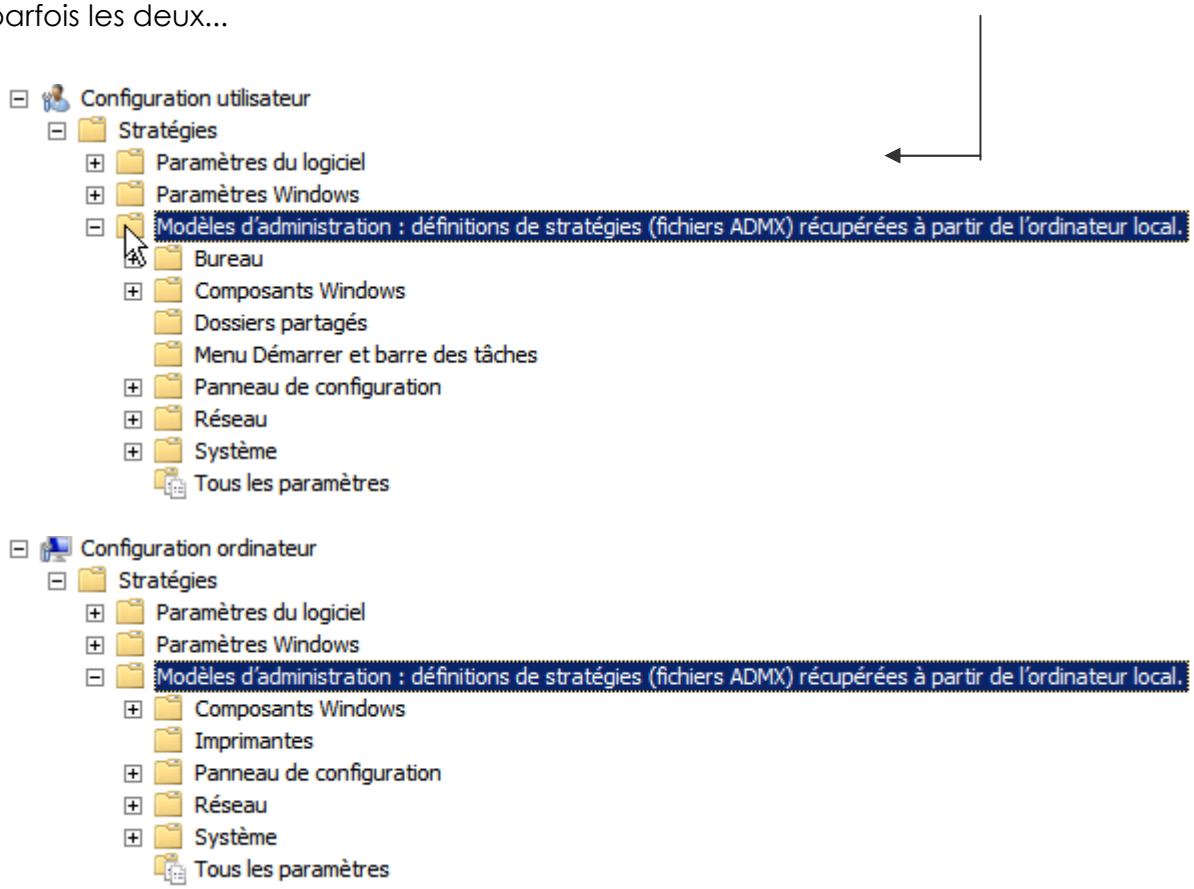
Maintenant que l'on a compris comment donner et faire appliquer des **GPO** sur des **UO** ou dans un domaine, on peut regarder de plus près ce qui leur est spécifique, par rapports aux sécurités locales.

Les fichiers des modèles d'administration classiques sous 2003 (également appelés fichiers ADM) n'étaient du format XML

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

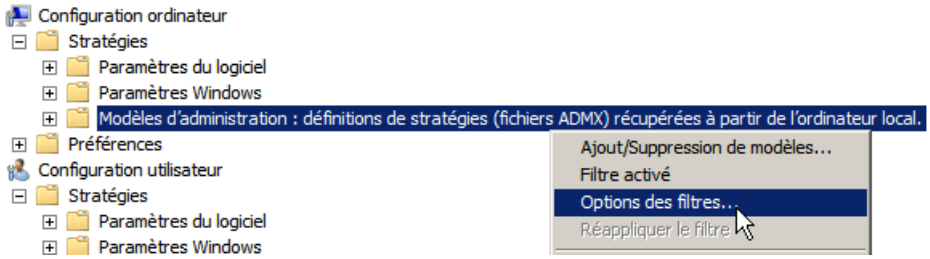
L'Éditeur d'objets de stratégie de groupe affiche ces paramètres sous le nœud **Modèles d'administration**

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...

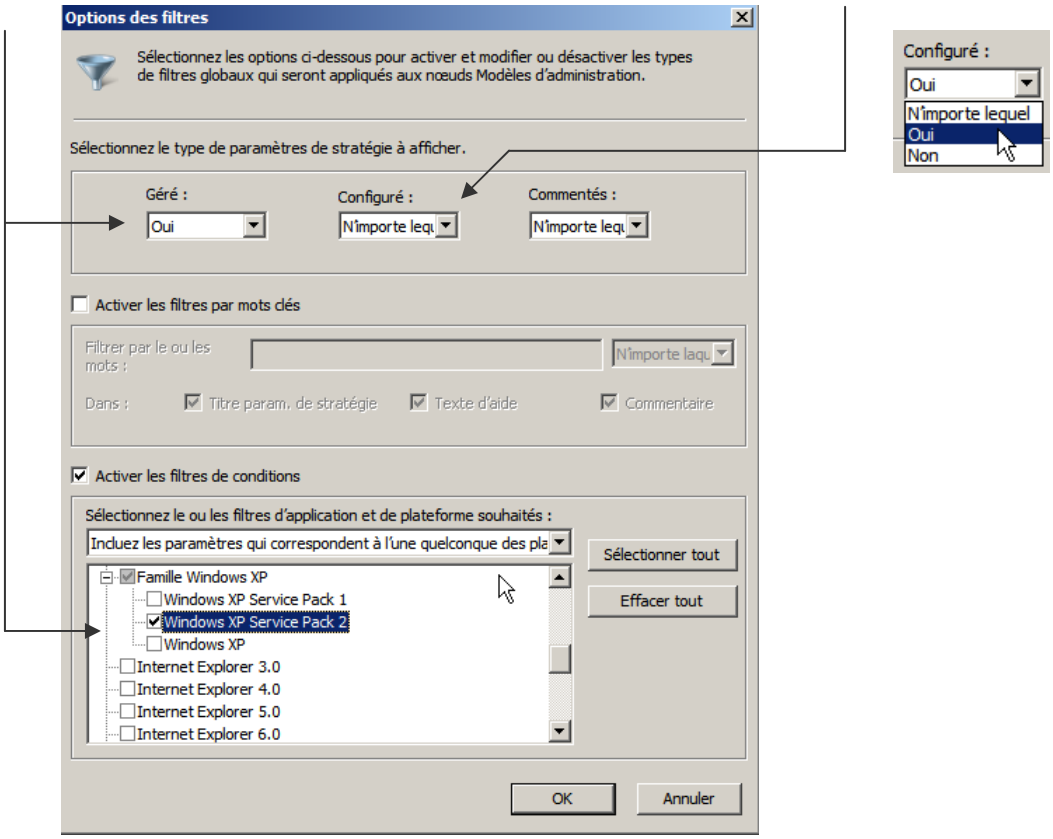


allez regarder un peu l'éventail des possibilités…

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



Notamment pour cibler un système, et 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 a 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…

GPO - SCRIPTS

Scripts de démarrage – arrêt – fin de session :

Lorsque l'on met en œuvre des scripts via les **GPO**, il est possible de placer trois nouveaux types de scripts

- Script de démarrage : s'exécute lors de l'allumage du poste
- Script de fermeture de session : s'exécute lors d'une fermeture de session
- Script d'arrêt : s'exécute lors d'un arrêt de la machine

Mais on peut aussi placer un script de type classique

- Script d'ouverture de session : s'exécute lors d'une ouverture de session

Par défaut chaque script est réalisé avant la fin de l'autre (on parle de traitement synchrone). Les scripts **GPO** sont traités avant les scripts utilisateurs classiques.

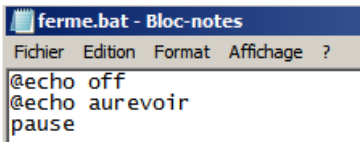
N.B : Par défaut les scripts de démarrage sont masqués.

Scripts de fin de session :

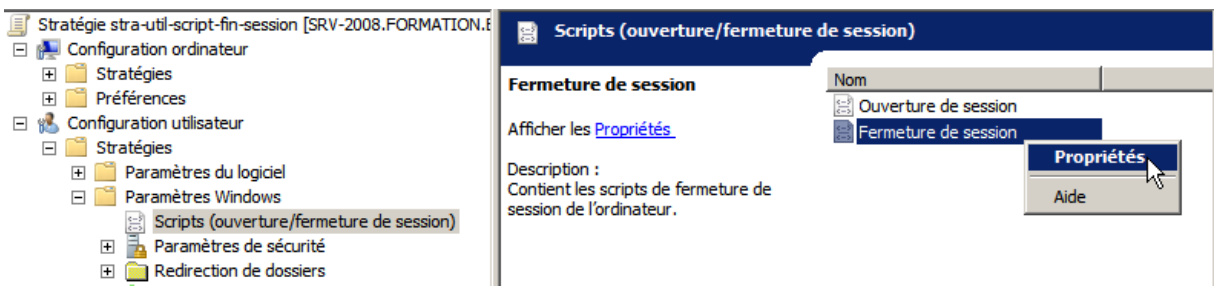
Créons nous une stratégie au nom parlant :

stra-util-script-fin-session stra-util-script-fin-session

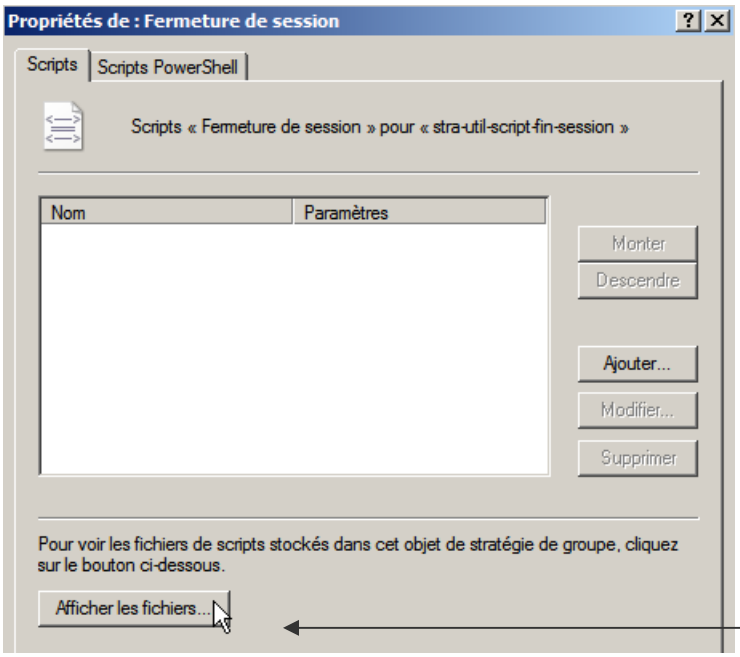
Pour utiliser un script de fin de session dans une **GPO**, (le script étant déjà écrit dans un fichier **.bat** ou **.vbs**, ou en **powershell,** par exemple "ferme.bat"…



Il faut demander les propriétés de **Configuration Utilisateur / Stratégies / Paramètres Windows / Scripts / Fermeture de session**



Pour avoir

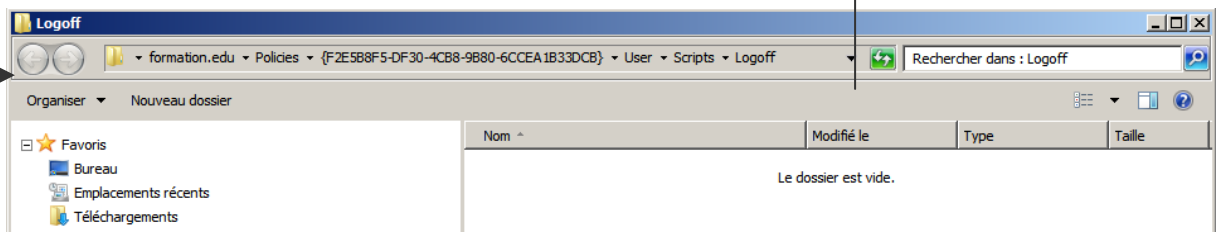


Il faut effectuer une manœuvre en deux temps :

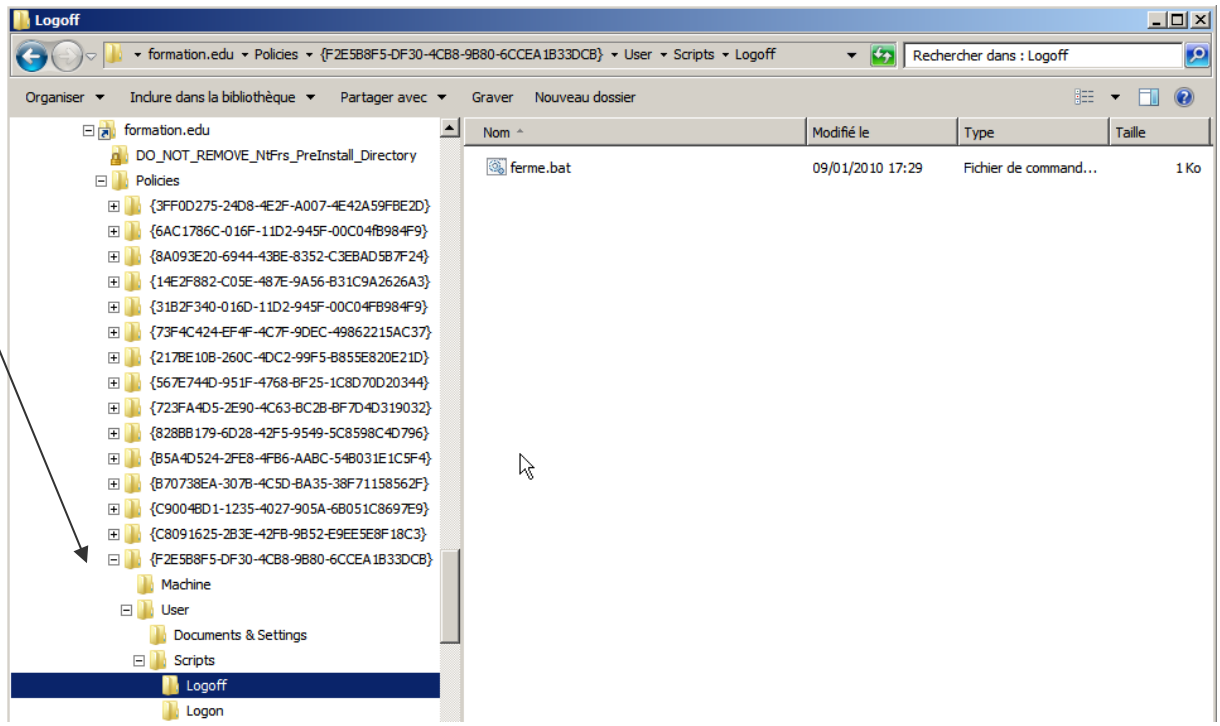
- D'abords il faut copier le script dans la **GPO**
- Puis il faut dire à la **GPO** d'utiliser ce script…

Copier le script dans la GPO : (Afficher…)

depuis la GPO, on demande le bouton **Afficher les fichiers…**



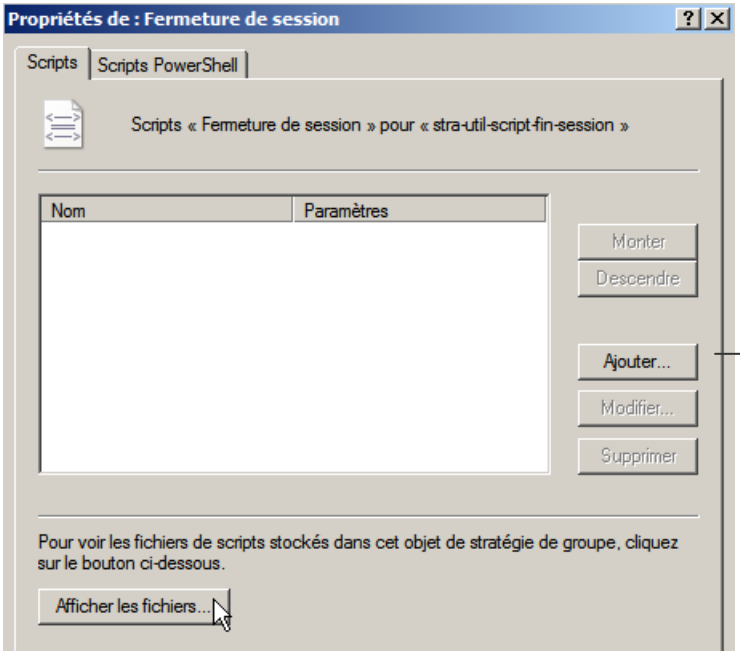
Une fenêtre s 'ouvre dans laquelle il faut copier notre script (donc ici **ferme.bat**)

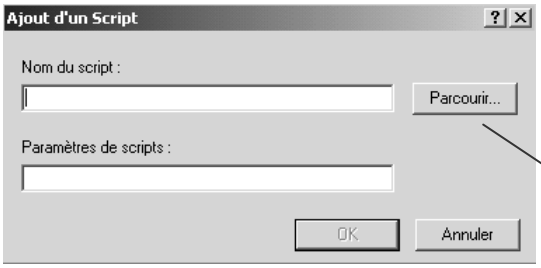


N.B : cette opération a simplement pour but de stocker dans notre **GPO** une copie du script, qui physiquement se trouve dans la stratégie **{F2E588F-DF30**…}

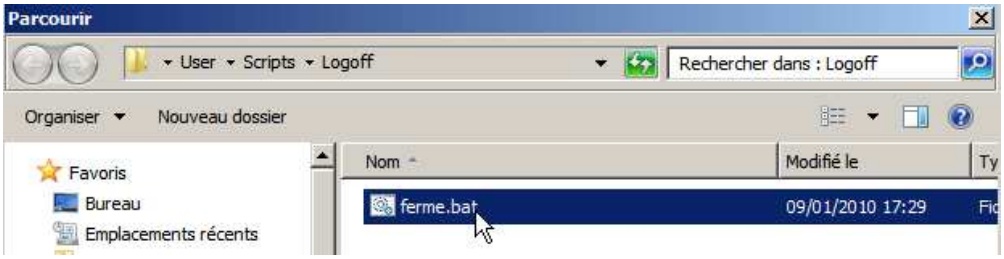
Utiliser le script dans la GPO (Ajouter…)

Pour utiliser le script dans la GPO, depuis la GPO, maintenant on demande le bouton **Ajouter**

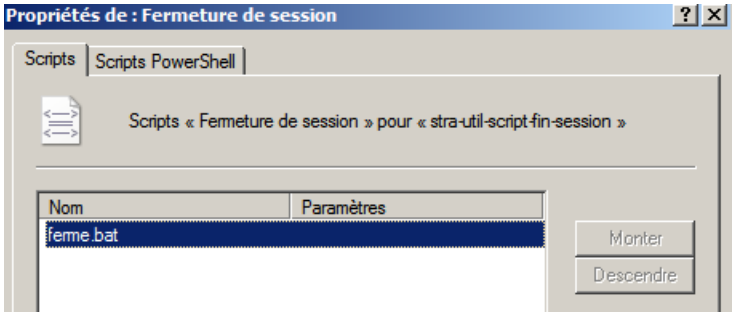




Et via **Parcourir** on prend un script parmi ceux existant dans la GPO (donc parmi ceux précédemment copiés)



Maintenant on a un script de déconnexion….



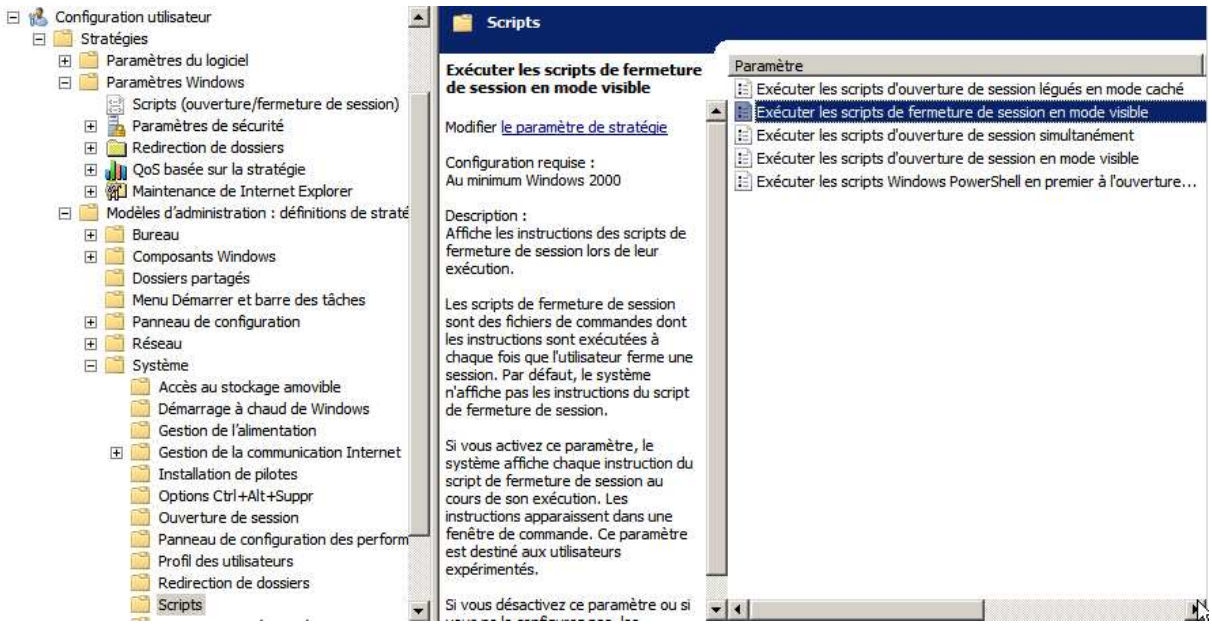
test et visualisation :

Sachant que

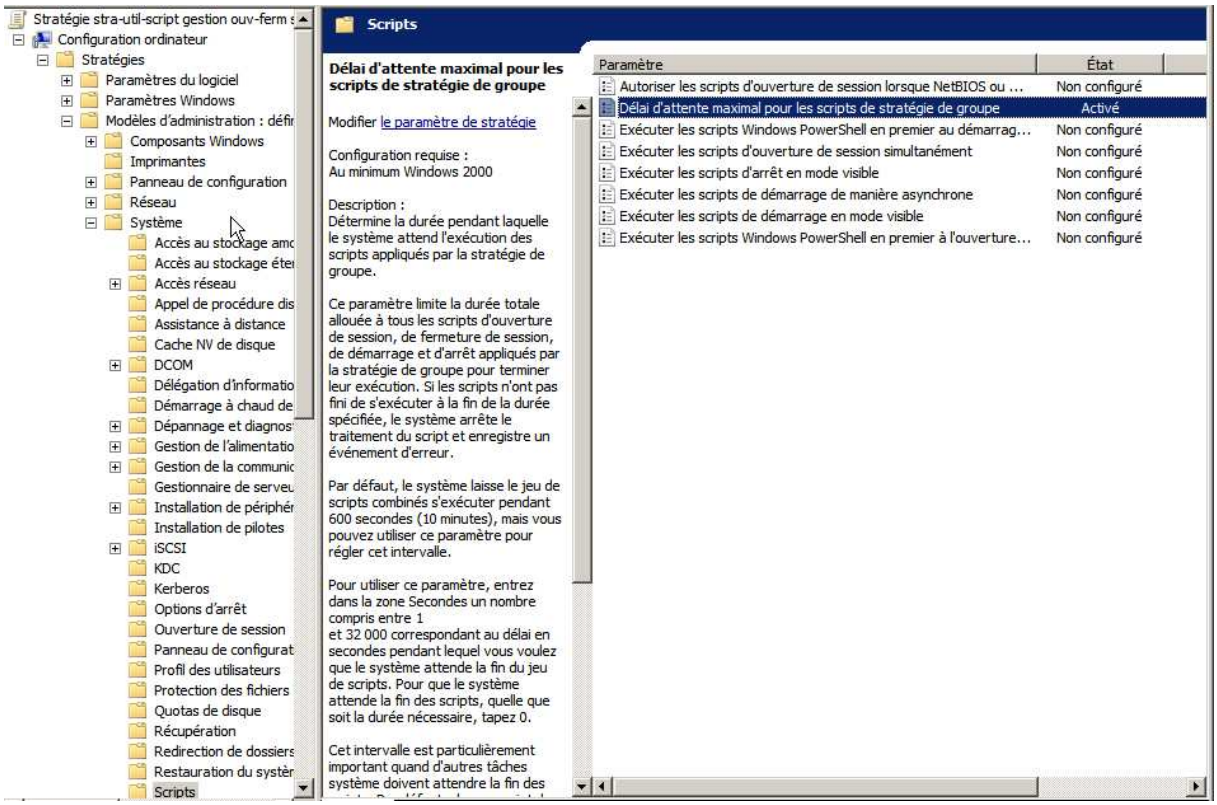
- les scripts de déconnexion s'exécutent par défaut en **mode caché**…
- les scripts disposent de **10 minutes** pour se réaliser, avant d'être interrompus.

Ainsi, une commande **pause**, dans un script de déconnexion, provoque le blocage pendant 10mn, puisque personne ne peut appuyer sur la touche …

Il existe un **Modèle d'administration / Système** de **stratégie utilisateur**, permettant **d'exécuter les scripts de fermeture de session en mode visible**…



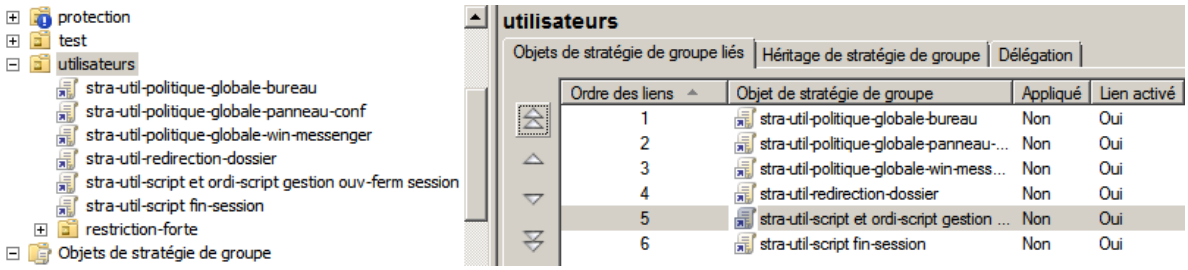
Il existe un **Modèle d'administration / Système** de **stratégie ordinateur**, pour paramétrer le **délai d'attente maximal pour les scripts** (tous les scripts)



On pourrait faire une stratégie ordinateur ET utilisateur pour ces deux réglages…

stra-util-script et ordi-script gestion ouv-ferm session	Activé	Aucun(e)

Du coup, il faut penser à appliquer non seulement notre stratégie de script, mais aussi notre stratégie de réglage…



Et dans le bon ordre…

GPO - INSTALLATION DE LOGICIELS

Les 3 éléments Winstaller – GPO - AD

Un nouveauté de windows 2000-2003 , et maintenue avec 2008 consiste en un système d'installation et de maintenance de logiciel, utilisant **AD** (Active Directory), les **GPO** (stratégies de groupe), et **Windows installer**

L'ordre logique dans lequel ces fonctionnalités vont jouer est le suivant :

1. **Windows Installer** est utilisé pour l'installation de logiciel
2. Les **GPO** sont utilisées pour définir une stratégie quant à cette installation
3. **Active Directory** est là pour déployer cette stratégie

On a déjà suffisamment parlé de **AD** et des **GPO**, la grosse nouveauté ici réside dans **Windows Installer**

Windows installer et fichiers msi

Le service **Windows installer** est un service client automatisant entièrement la procédure d'installation et de désinstallation de logiciel, à condition d'avoir un « package windows installer » correspondant à l'application à installer. Ce package est plus connu sous l'appellation du **fichier MSI** (**Microsoft installer**)

Le fichier **MSI** est donc en fait un package contenant :

- Un fichier de réponse automatisé
- tous les fichiers nécessaires à l'installation de l'application…

Les fichiers **MSI** font aussi des installations **classiques locales** de tout logiciel, grâce à la présence dans l'OS du composant Windows Installer.

- Si l'OS n'a pas **Windows Installer**, une **mise à niveau du système sera nécessaire**
  C'est pour cette raison que certaines installations demandent un redémarrage du poste, car d'abords en fait elles installent **Windows installer**, puis elles font "lire" le fichier **msi** par le **Windows installer** pour installer l'application proprement dite.
- Si l'on **veut une installation réseau**, type installation administrative d'office, les fichiers msi et windows installer **ne savent pas faire**

La présence de **Windows installer** est vérifiable par la présence du fichier **msiexec.exe,** présent en général dans le dossier système.

Aujourd'hui toutes les applications récentes sont livrées avec un fichier **MSI** destiné à être interprété par un Windows installer

Si on n'a pas de fichier **Msi,** il est impossible de se créer une stratégie d'installation automatisée.

Il existe des outils professionnels permettant de créer des fichier msi, notamment *Installshield*, et *Wyse installer*

Procédure d'installation et de maintenance logiciels

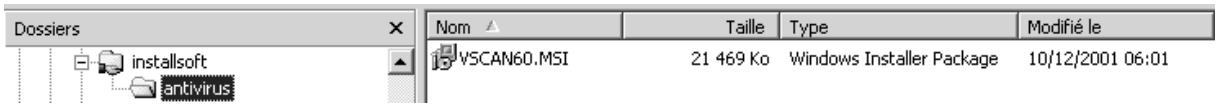
Il va falloir exécuter les étapes suivantes :

1. Il faut créer une GPO qui installe le logiciel sur l'ordinateur, soit lors du démarrage du poste, soit lors du « lancement » de l'application (qui paraît comme disponible) de la part de l'utilisateur.
   cette phase peut être qualifiée de **déploiement** .
2. Le logiciel déployé peut être mis automatiquement à niveau, ou redéployé au démarrage du poste ou lorsqu'un utilisateur lance sa session.
   cette phase peut être qualifiée de **maintenance** .
3. Le logiciel peut être automatiquement supprimé au démarrage du poste ou lorsqu'un utilisateur lance sa session.

Création du point d'installation de logiciel

Il faut copier les package Windows installer, c'est à dire le fichier **msi** vers un **point de distribution** du logiciel.

Par exemple



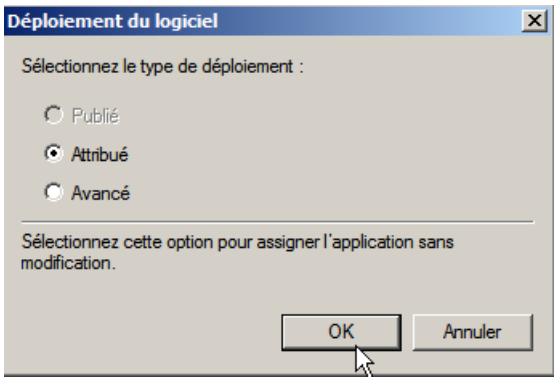
Ce point de distribution est généralement un dossier partagé sur le serveur, mais cela peut être un emplacement réseau quelconque…

C'est en fait simplement un dossier sur lequel on peut si on veut donner des permissions en lecture seule…, partager le dossier de manière administrative ($), pour le rendre invisible…

N.B : il faut impérativement donner un point de distribution réseau, et non pas un chemin local !

Attribution - Publication de logiciel

L'attribution ou la **Publication** sont les deux options de distribution de logiciel possibles



L'attribution permet d'être sur que le logiciel est présent sur l'ordinateur voulu. Avec une attribution on peut affecter les logiciels à des **utilisateurs**, ou a des **ordinateurs**.

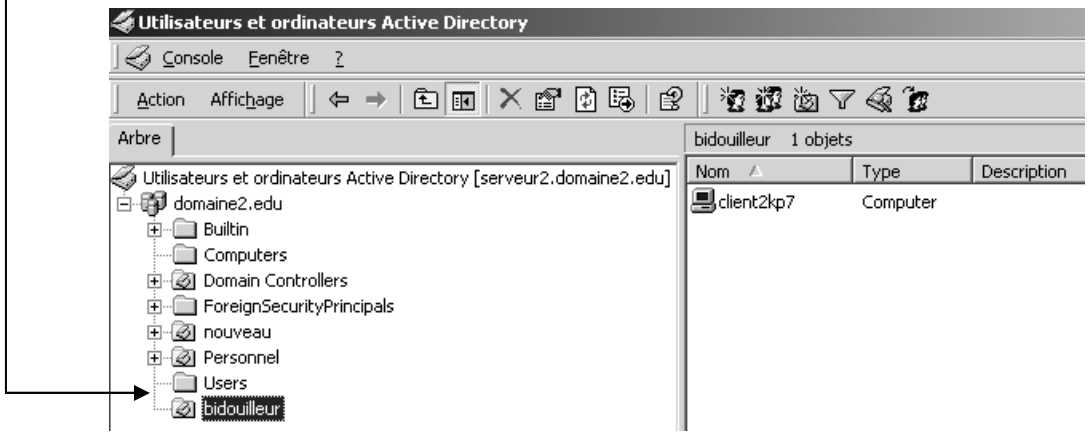
- Si on les affectent à des **ordinateurs** : il n'y a pas d'annonce, le logiciel est automatiquement installé lors de l'allumage du poste. (sauf pour les CD)
- Si on les affectent à des **utilisateurs** : lorsque l'utilisateur ouvre un session, le logiciel est annoncé (raccourcis présents) , mais l'installation ne débute réellement que si l'utilisateur clique sur l'application ou double-clique sur un fichier associé.

La Publication permet que le logiciel soit installable sur l'ordinateur voulu. Avec une publication on peut affecter les logiciels uniquement pour des **utilisateurs**, mais pas pour des ordinateurs.

En effet lors de la publication de logiciels, il n'y a pas d'annonce. L'utilisateur peut installer l'application en passant par ajout/suppression programme, ou l'installation se fait automatiquement via un double clic sur un fichier associé

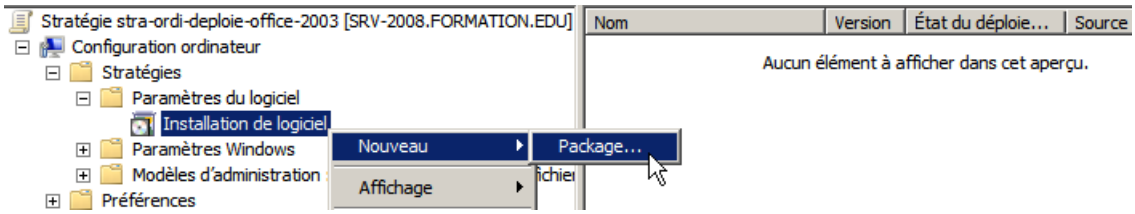
Stratégie de déploiement de logiciel

On va créer une **GPO** sur une **OU** contenant les machines des **bidouilleurs**, et leur installer un antivirus dès le démarrage du poste



Sur cette OU on va poser une GPO que l'on nomme de manière explicite

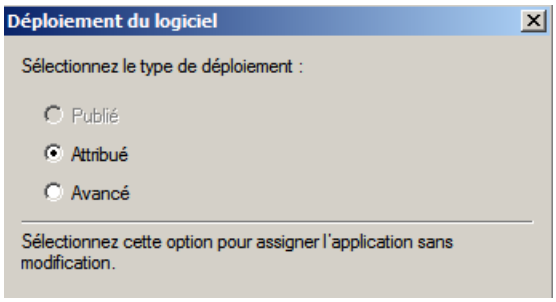
Cette GPO contient une définition de **Paramètres logiciel** dans **Configuration d'ordinateurs (ou utilisateurs)**



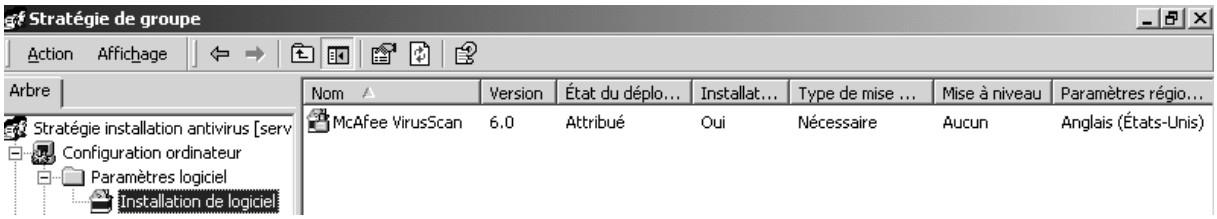
Pour laquelle on demande via un clic droit **Nouveau / Package…**

et on va

1. chercher le chemin du dossier de distribution (via le réseau bien sûr)
2. indiquer le type de déploiement



pour obtenir finalement

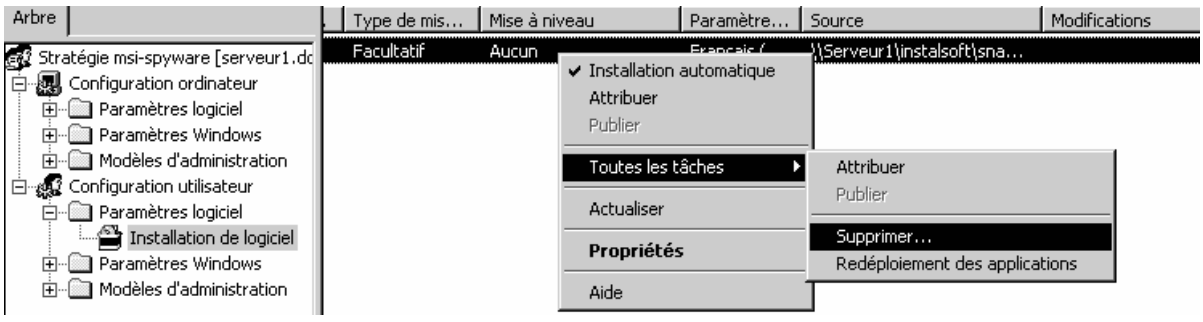


NB: si on travaille au niveau de la configuration d'utilisateur, à l'ouverture de session on récupère le MSI

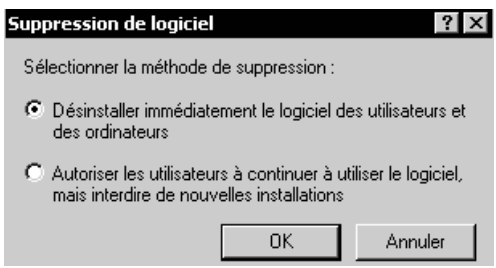
NB: si on travaille au niveau de la configuration d'ordinateur, il faut arrêter et re-démarrer le poste pour récupérer le MSI

Stratégie de re-déploiement / désinstallation

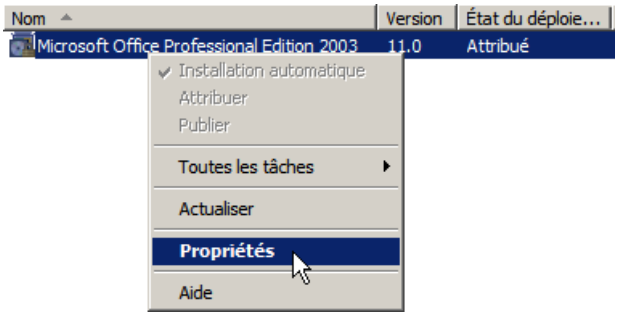
En se plaçant sur la stratégie, on demande **toutes les tâches / supprimer**



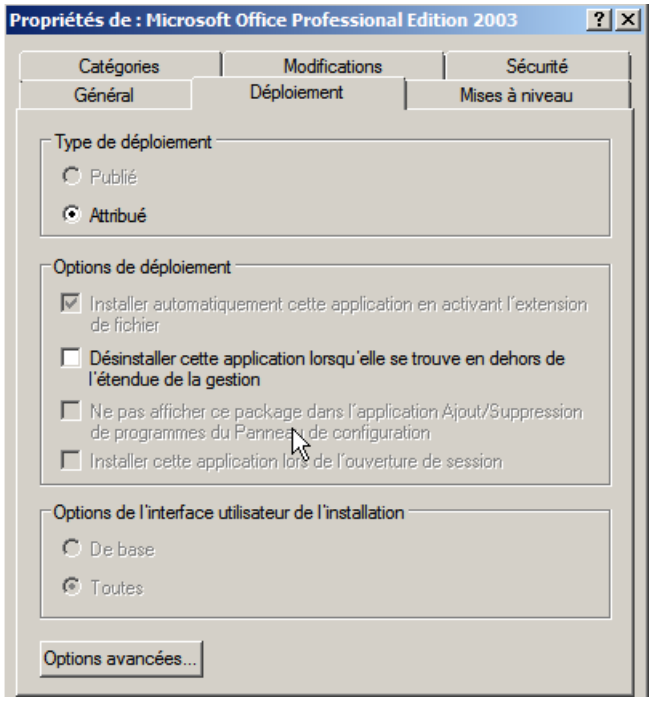
et là on peut choisir



Propriétés de déploiement de logiciel



Donnant

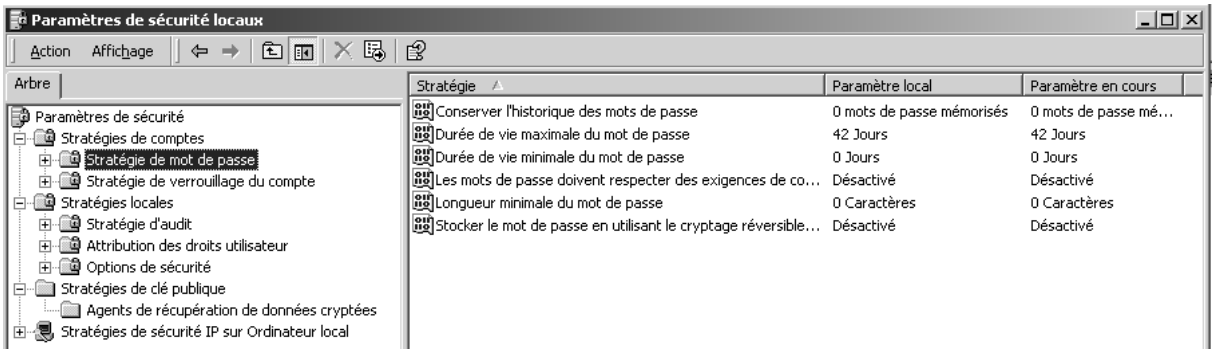


GPEDIT.MSC

Stratégie locale / réseau:

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

ce qui donne ensuite accès aux paramètres suivants :

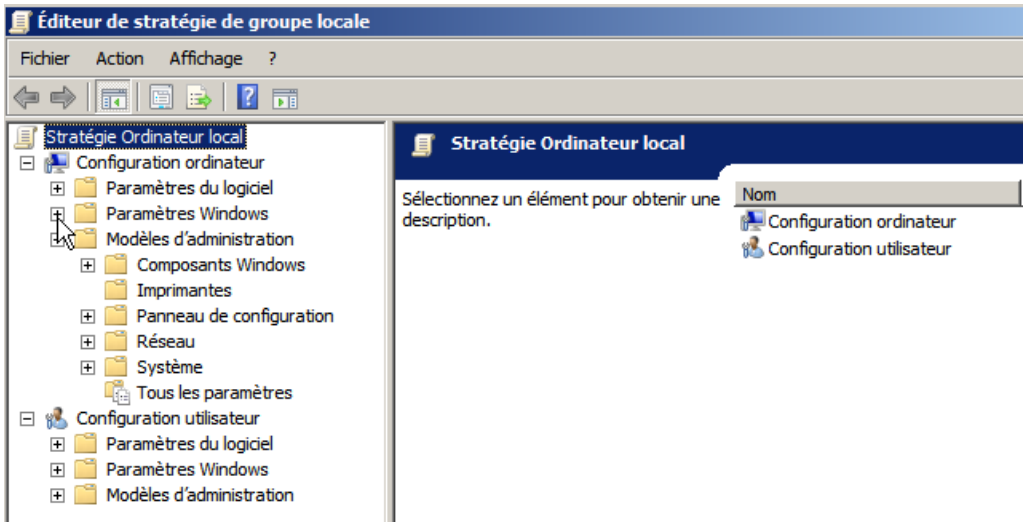


Les stratégies réseaux elles sont en général utilisée à travers le réseau (pour tout le domaine ou une partie à travers des stratégies de GPO...

Editeur de stratégie de domaine "locale" :

Il est cependant possible de modifier les stratégies d'une machine 2000-xp ou Seven Vista avec les options normalement réservées aux stratégies de réseau, et ce localement…

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…!