Stratégies Windows
– sys 26 – cours -

Stratégies Windows XP et de Domaine

Michel Cabaré – Ver 1.0 – Oct 2006-

http://WWW.CABARE.NET©

La formation que vous suivez, à pour but de vous initier avec le logiciel Microsoft Windows NT-2000-XP-2003 (version 4.0-5.x) sur environnement P.C.

Ce Support a 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 2000-XP

Types de stratégie :

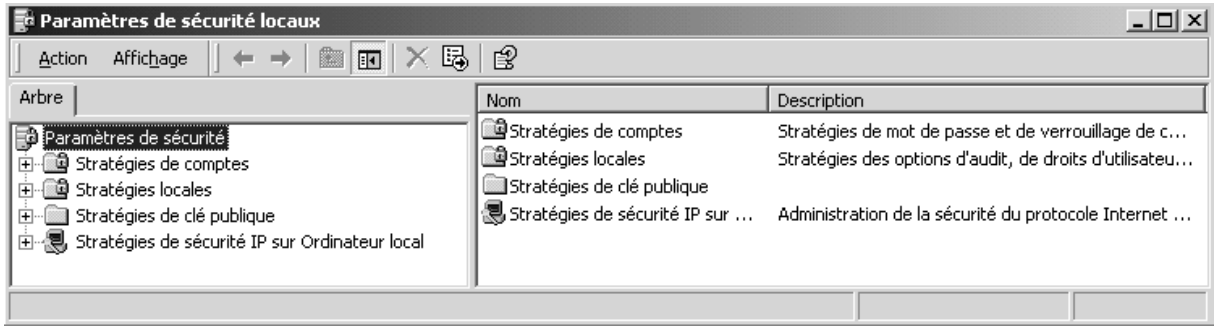
Les stratégies de sécurité permettent d'éviter que des utilisateurs modifient involontairement (ou volontairement) la configuration d'un ordinateur.

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).

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:

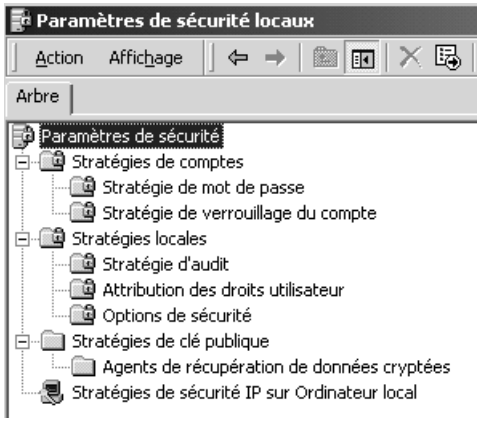
- **Stratégies de compte**

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

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

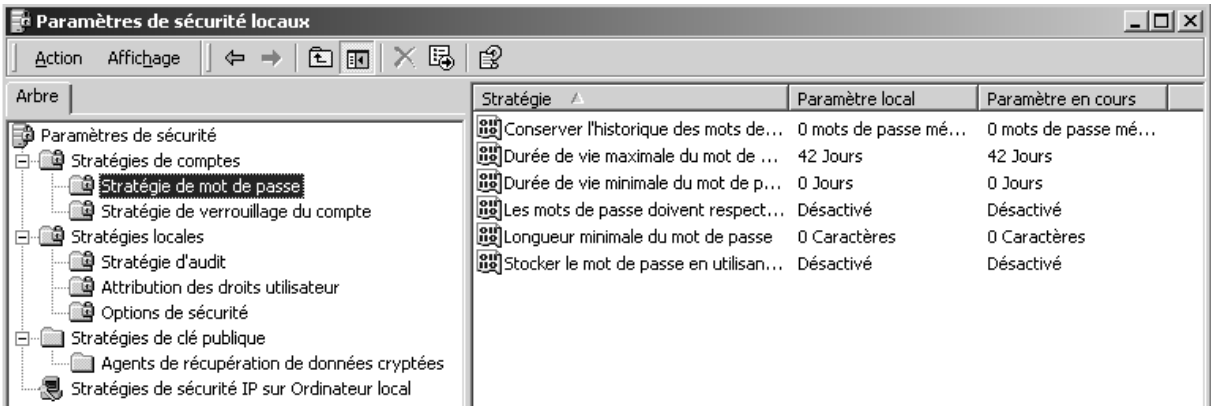
  (agent de récupération)
- **Stratégies IPSEC**

  (cryptage IP)

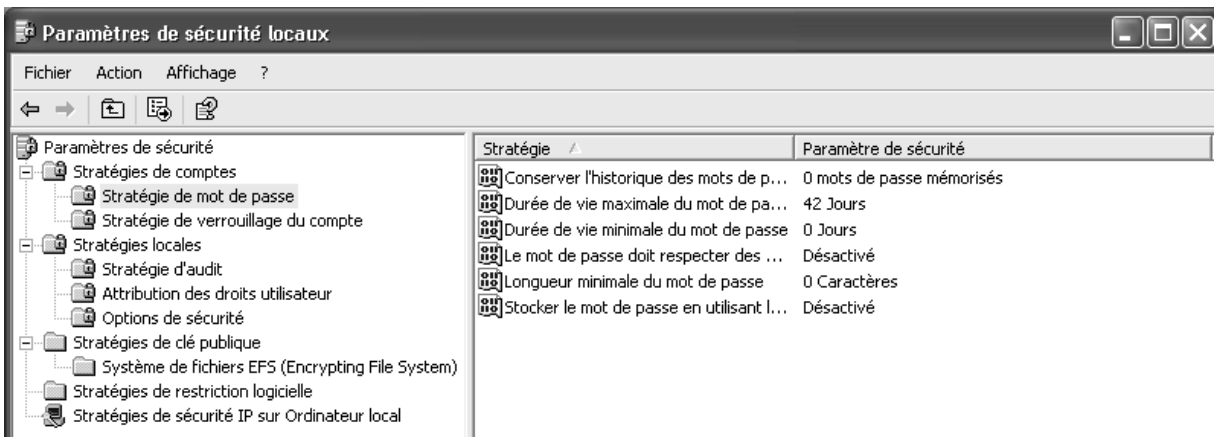


Dans l'arborescence, on visualise à droite les différentes composantes...

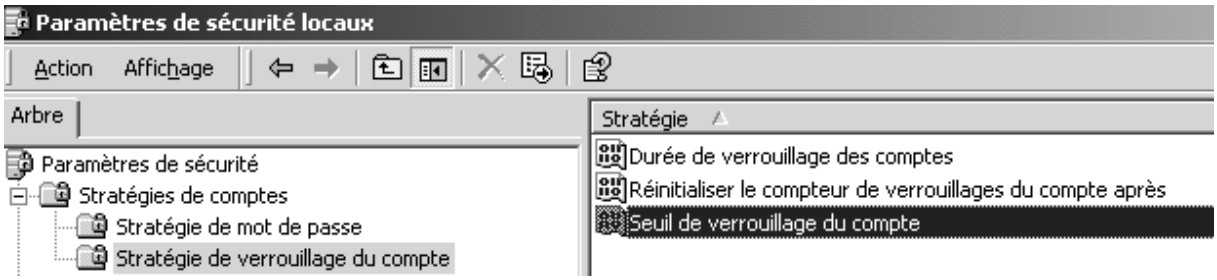
Interface **Windows 2000**



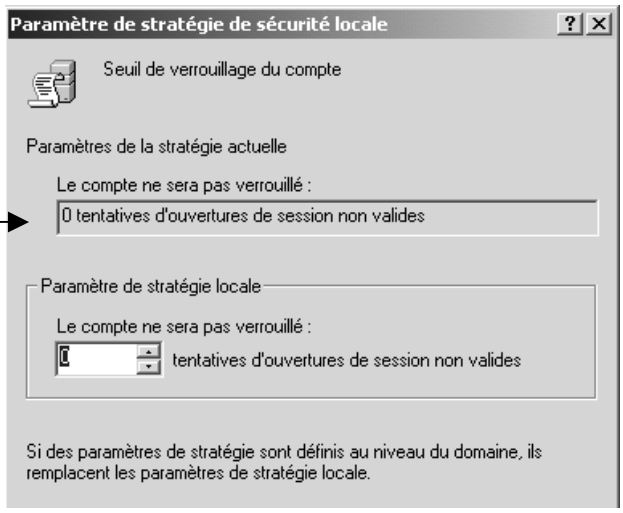
Interface **Windows XP**



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

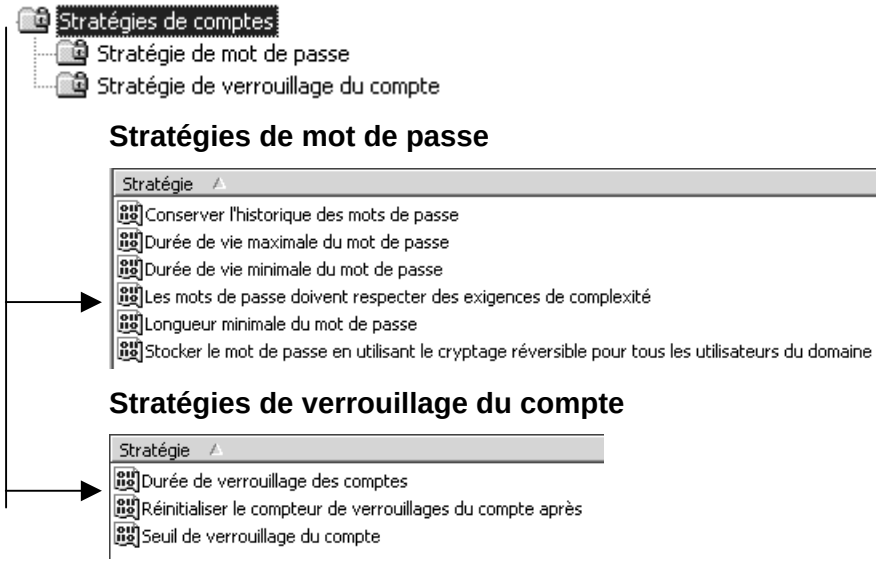


Sur lequel un double-clic amène



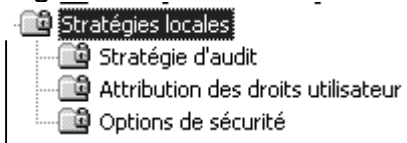
Contenu des Paramètres locaux de sécurité :

Stratégies de comptes

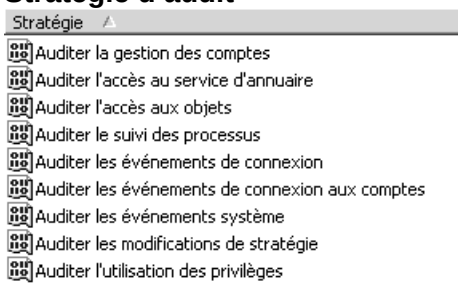


N.B : concernant la gestion des mots de passe, si un domaine existe, alors il serait bon de gérer ces stratégies essentiellement au niveau du Domaine, et jamais à un niveau inférieur, sous peine d'avoir des incohérences et des problèmes d'accès !

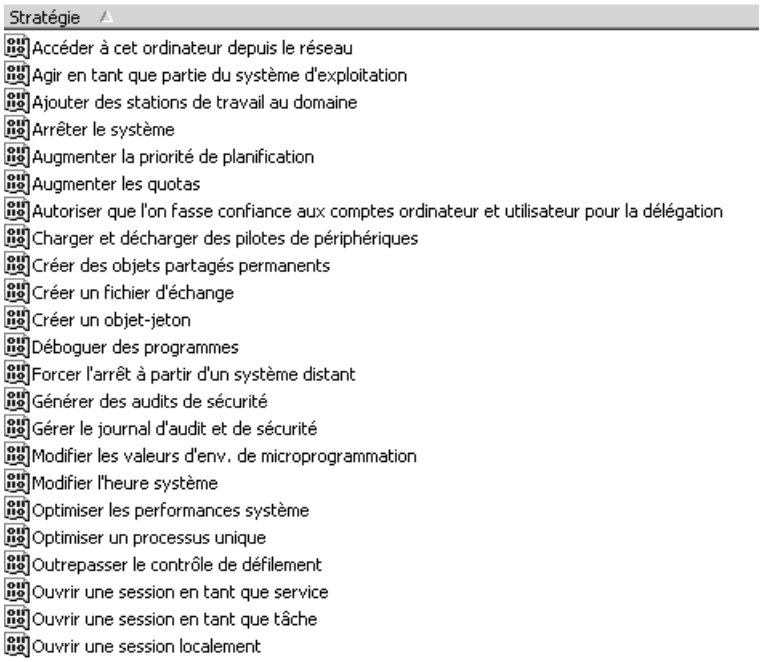
Stratégies locales



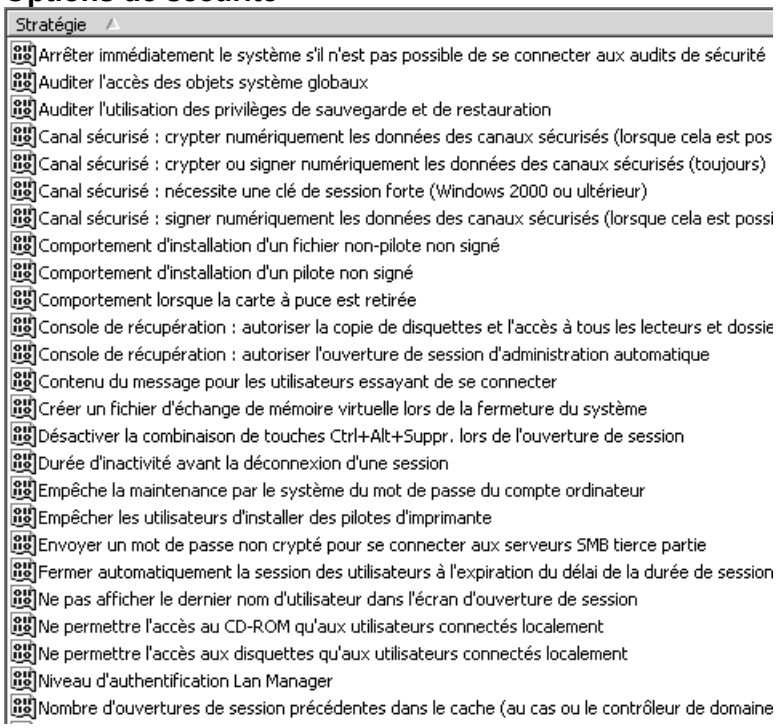
Stratégie d'audit



Attribution des droits utilisateurs



Options de sécurité



Stratégies de clé publique

Stratégies de sécurité IP

Stratégies de restriction logicielle (uniquement sous XP)

STRATEGIES LOCALES - AUDIT

Audit évènement - 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.**

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

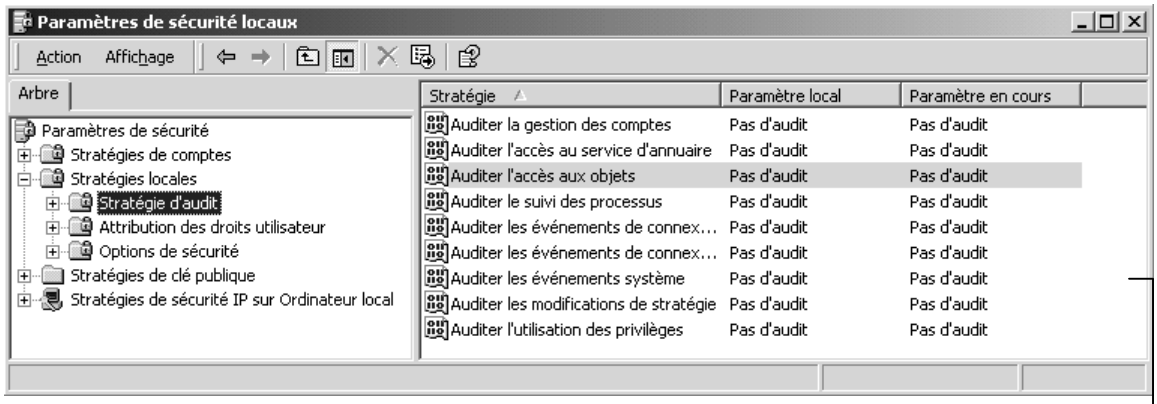
Audit sur évènement:

Lorsque l'on veut auditer un évènement, on eut 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**,

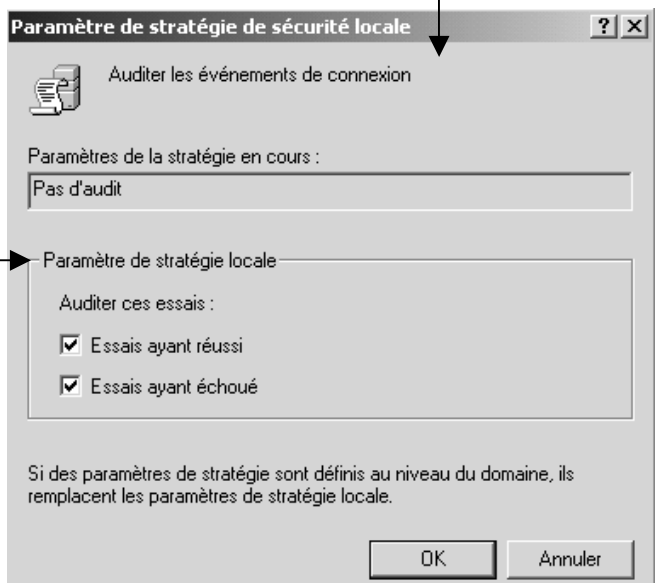
dans laquelle Il faut développer la clé

Stratégies locales / Stratégies d'audit



par exemple sur **connexion**

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



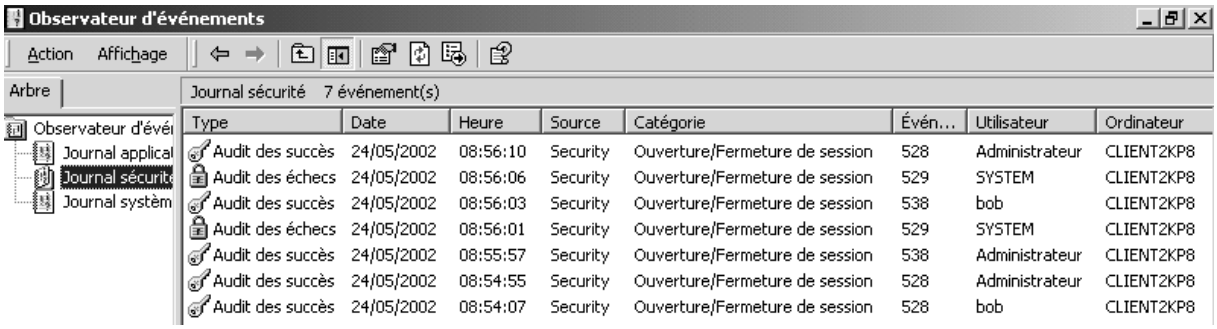
L'audit étant posé , mais non enregistré

il faut fermer la console pour que les modifications soient prises en compte et re-démarrer

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

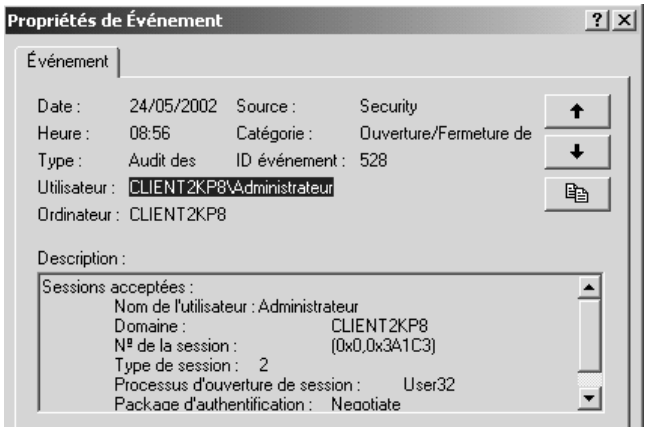
Lire le journal de sécurité:

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



Dans lequel un double clic sur l'événement donne le détail

Audit succès



Audit Echec

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

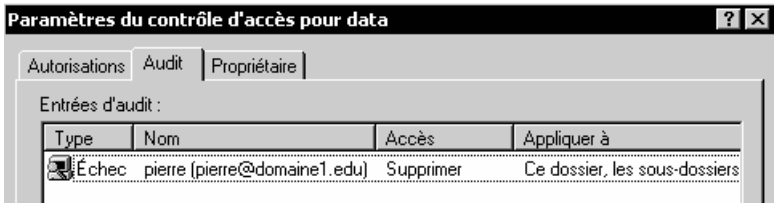
Audit sur un dossier

Il faut

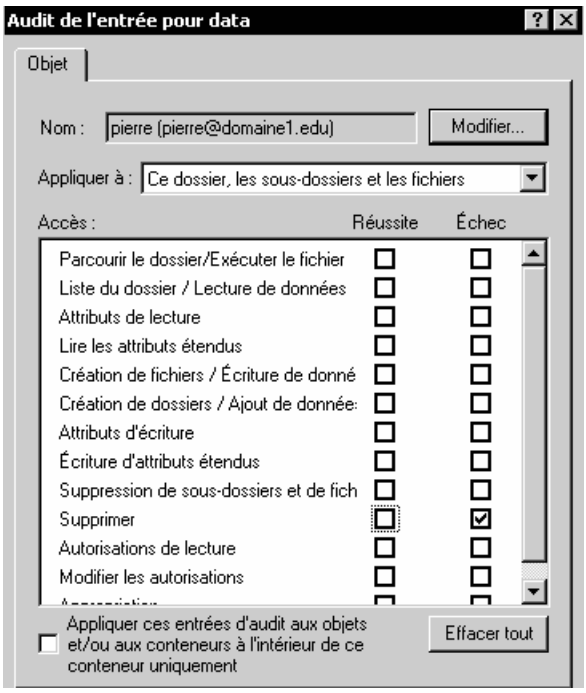
1. activer l' Audit "**Accès aux objets**"dans les stratégies locales de l'ordinateur sur lequel le dossier se trouve
2. sur ce même dossier ensuite demander les **propriétés**, onglet **sécurité**, via les **Paramètres avancées NTFS** et demander **Audit** ...

Exemple :

Audit accès en échec pour le dossier de pierre (on cherche à savoir qui essaye d'effacer le dossier de pierre…)



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



Les type d'audit en tentative d'accès peuvent être obtenu par **Parcourir le dossier**

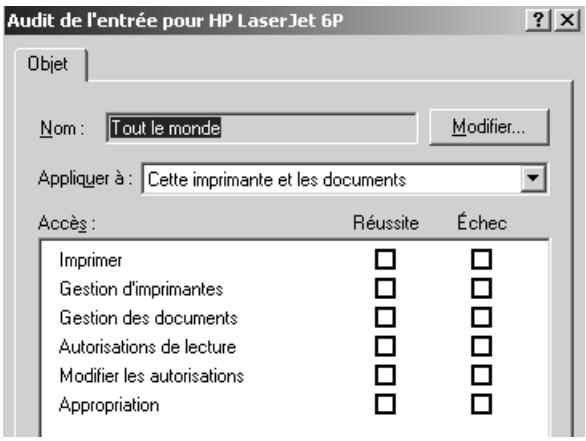
N.B : Ne pas cocher tous les accès car cela génère autant d'évènements de plus !!!

Audit sur une imprimante

On veut savoir qui utilise l'imprimante :

Il faut

1. activer l' Audit "**Accès aux objets**"dans les stratégies locales de l'ordinateur sur lequel l'imprimante est connectée
2. sur cette imprimante demander par les **Propriétés avancées NTFS** Audit pour tout le monde en réussite



Les type d'audit en tentative 'impression » peuvent être obtenu par **Imrimer**

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

STRATEGIES DE DOMAINE

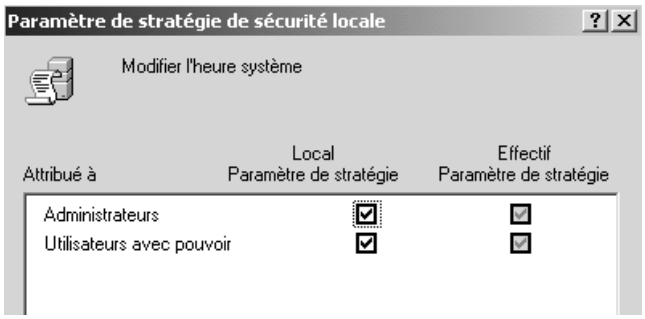
Stratégies de Domaine :

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.

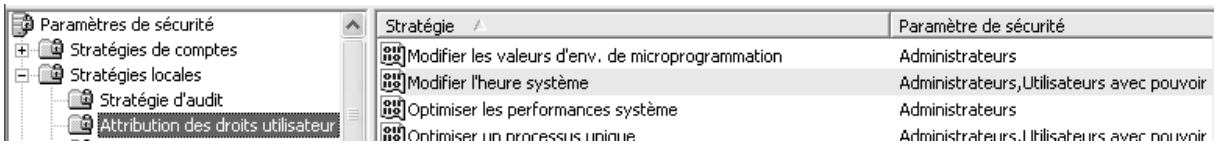
- les contrôleurs de domaine 2003 en font partie
- les contrôleurs de domaine 2000 n'en font pas partie)

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

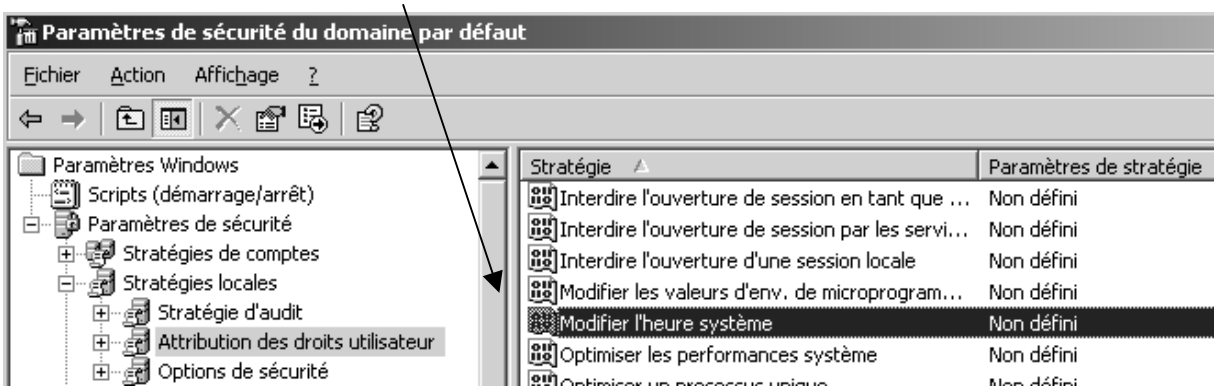
Sur le client 2000 du domaine, voila l'aspect de la **stratégie locale** concernant qui peut mettre à l'heure la machine....



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

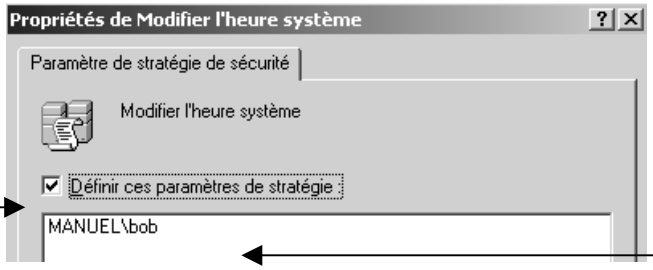


Sur le serveur de Domaine, on définit une **Stratégie de sécurité du domaine** pour **Modifier l'heure système** (qui par défaut est non activée)



en spécifiant que l'utilisateur bob a ce droit de mise à l'heure...

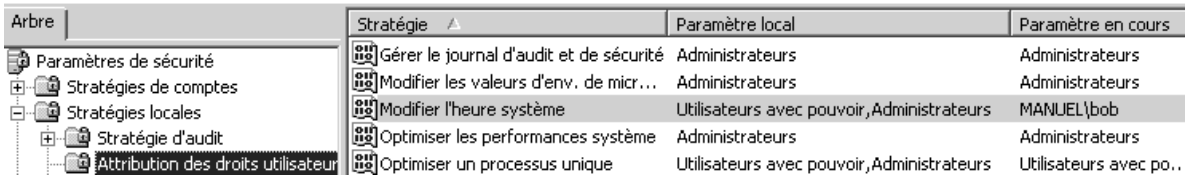
N.B : On active cette stratégie



Avec un utilisateur

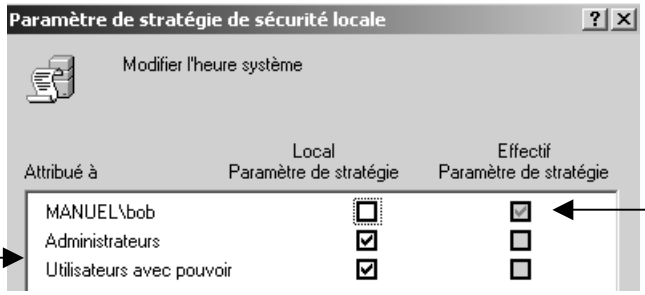
Sur le client 2000 du domaine

Lorsque la stratégie de domaine à pu se propager, normalement la visualisation des stratégies locales devrait donner :



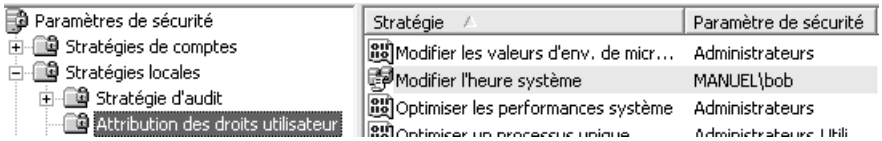
avec

Pas de changement localement

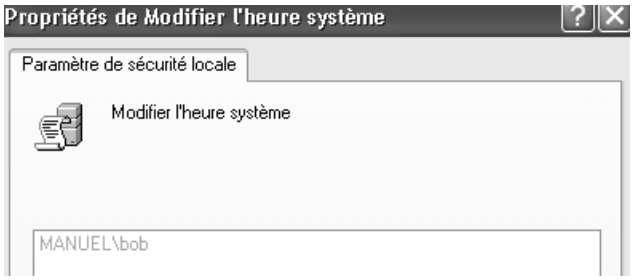


Mais ici on a récupéré la stratégie de domaine

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



en grisé

Propagation Stratégies de Domaine :

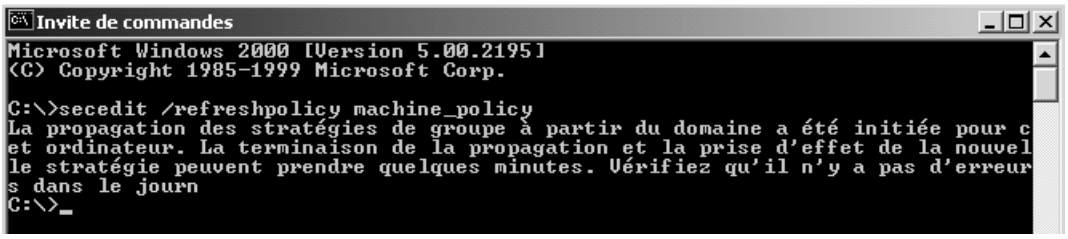
Normalement une stratégie se propage à **chaque démarrage de poste**, puis **toutes les 5 à 60 voire 90 minutes**, et lorsque les paramètres de sécurité locale sont modifiés...

Il est bien sûr toujours possible de forcer le rafraîchissement mais en partant du prinvipe 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, il est donc possible, depuis le client sur lequel on veut effectuer la propagation

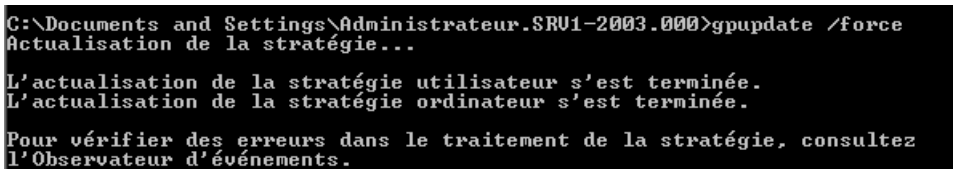
Sous **Windows 2000** :

Secedit /refreshpolicy machine_policy



Sous **Windows XP**

Gpupdate /force



Par exemple

effectivement, dans le journal on peut observer

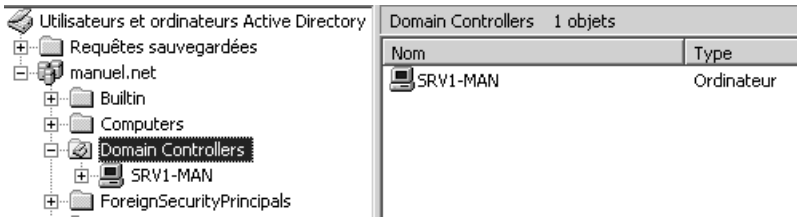
(Voir détail de ces commandes **secedit** et **gpupdate** dans le chapitre sur les GPO d'unité organisationnelle…)

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**)



Par exemple on souhaite que l'utilisateur marie puisse mettre à l'heure les contrôleurs de Domaine, mais ans pour autant être opérateur de serveur, ou appartenir à d'autres groupes pré-définis.

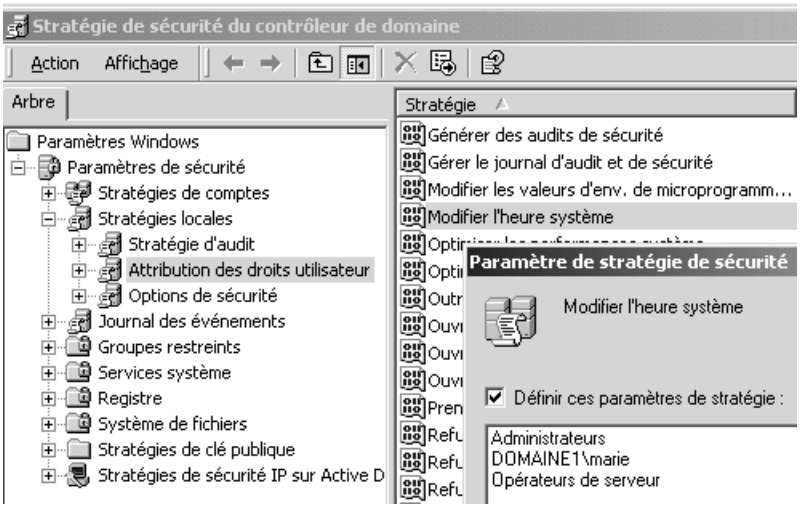
Il faut donc lui donner les deux droits suivants

- **Modifier l'heure système**
- **Ouvrir une session localement**

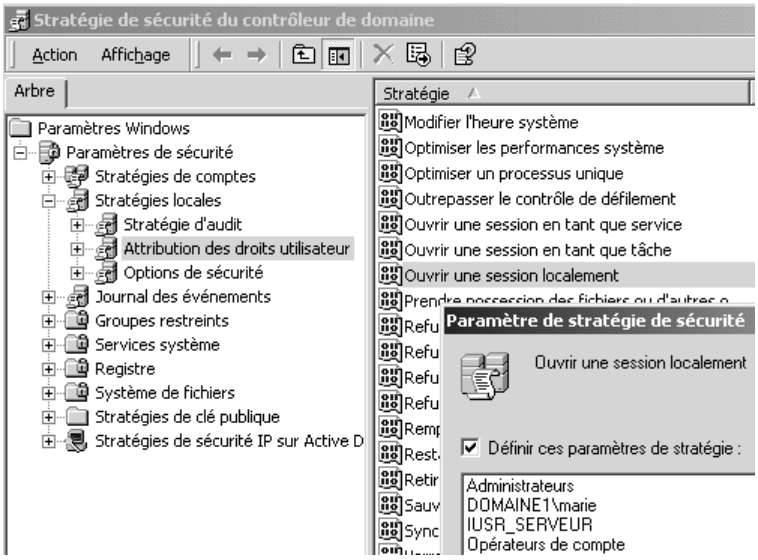
Sur le (un) serveur contrôleur de Domaine, on définit une **Stratégie de sécurité du contrôleur de domaine**

Sur le serveur de Domaine, on définit une **stratégie de contrôleur de domaine** qui par défaut est non activée

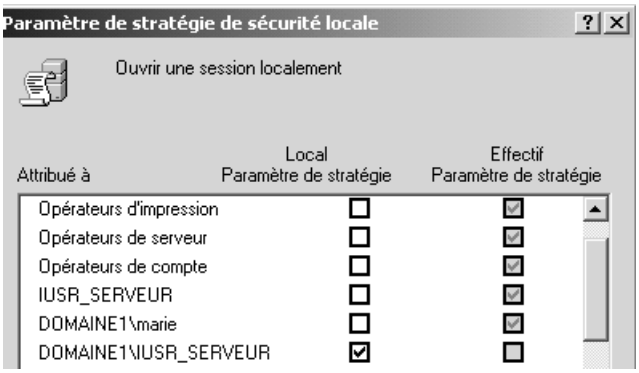
en spécifiant que l'utilisateur **marie** a ce droit de **Modifier l'heure système**

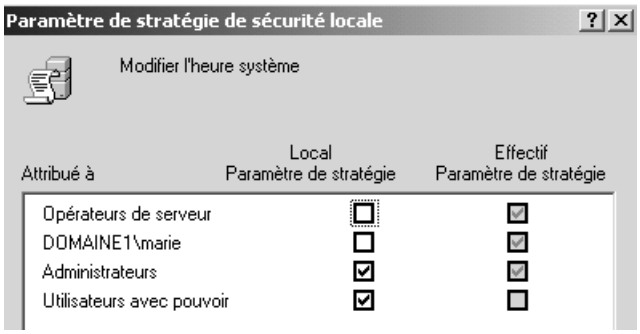


Mais qu'elle dispose aussi du droit d'**ouvrir une session localement**

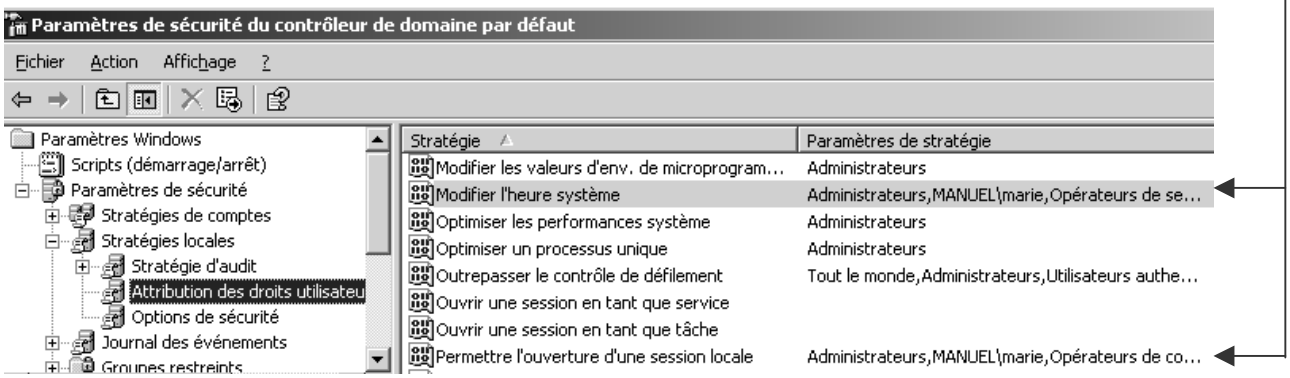


Sur le serveur de Domaine 2000, on visualise alors les paramètres de **stratégie locale** qui montrent les options reçues au niveau du CD :





Sur le serveur de Domaine 2003 les stratégies locales sont dévalidées... et seules les stratégies de sécurité du contrôleur de Domaine sont visibles!



MODELE DE STRATEGIES

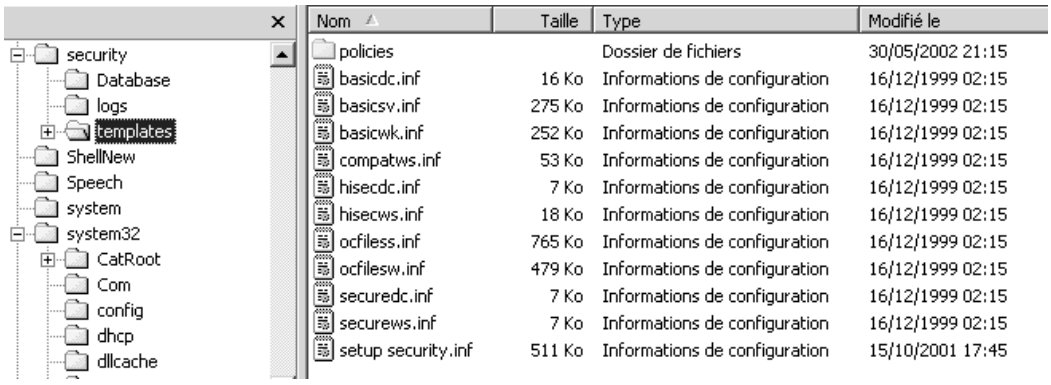
Les modèles de stratégie de sécurité:

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 sont définis dans des fichiers xxxx**.inf** stockés en général dans **Winnt\Security\Templates**



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**

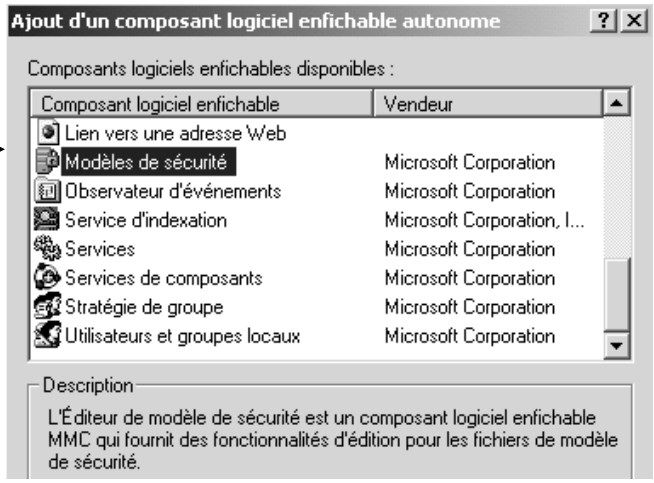
Il va falloir :

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:

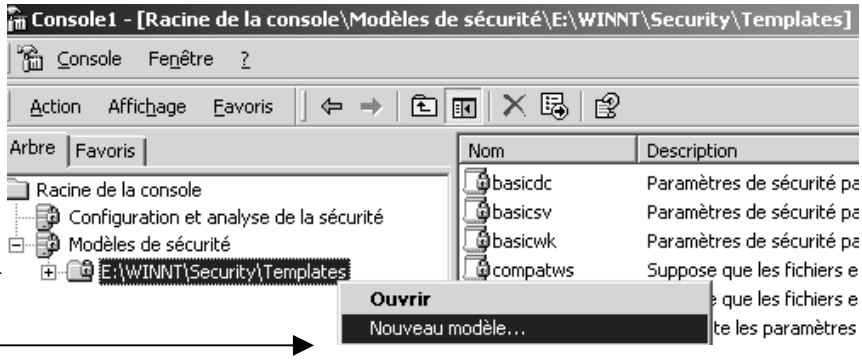
Il faut avoir une mmc permettant de gérer les modèles, cette mmc se nomme

Modèles de sécurité



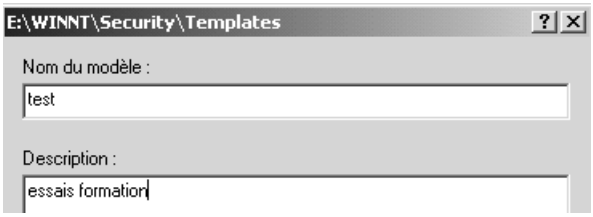
Dans cette mmc tous les modèles prédéfinis apparaissent évidemment on décide de se créer un modèle personnalisé

Clic droit sur le dossier dans lequel les modèles sont stockés



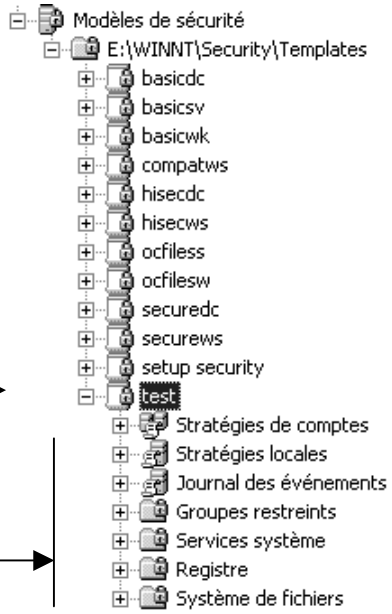
puis

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**

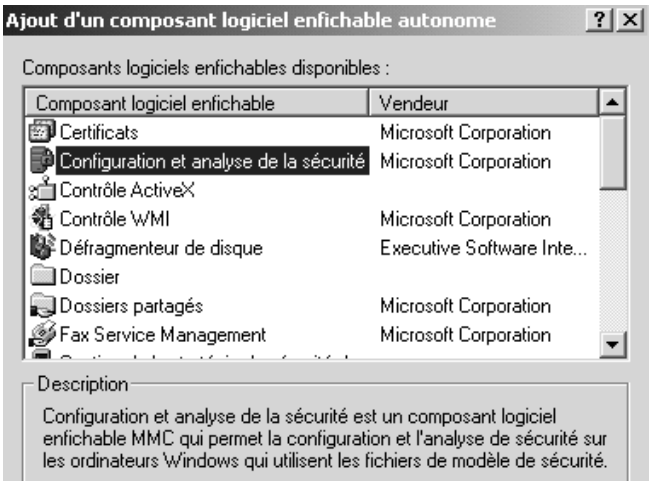
on prévoit de donner un message :"*strategie modele*", sans oublier le titre

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**

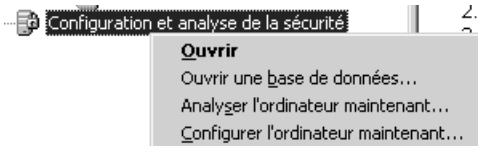
Pour créer une nouvelle base de données

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

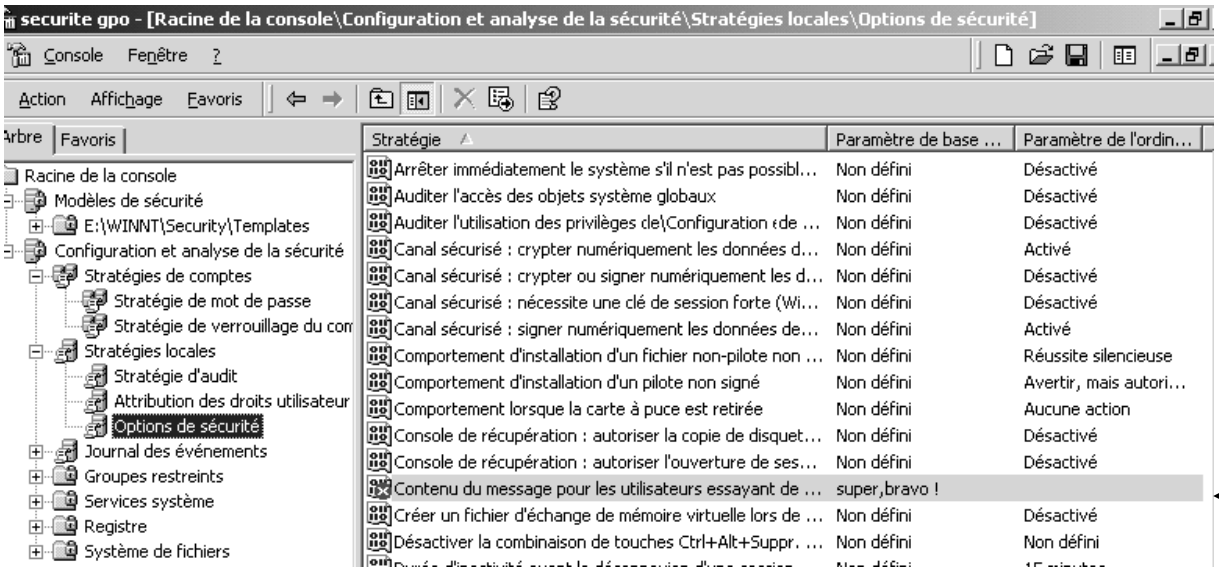
Maintenant nous avons une base de donnée crée avec un modèle chargé ! et les commandes **Analyser** ... **Configurer** sont disponibles !



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**!

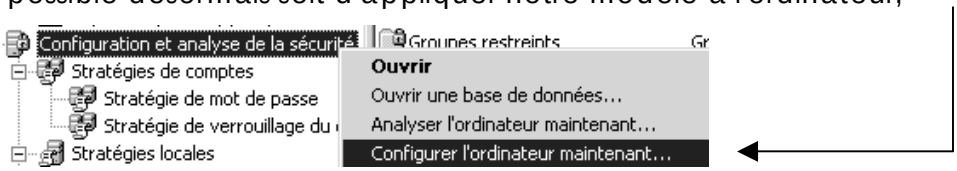


NB: toutes les différences sont marquées d'une croix rouge

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 modification 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 pieds...

Modèles pré définis

Les modèles de sécurité prédéfinis sont les suivants sous 2000:

- 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)

Les modèles de sécurité prédéfinis sont les suivants sous 2000 SRV et client XP:

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

Et de nouvelles versions de

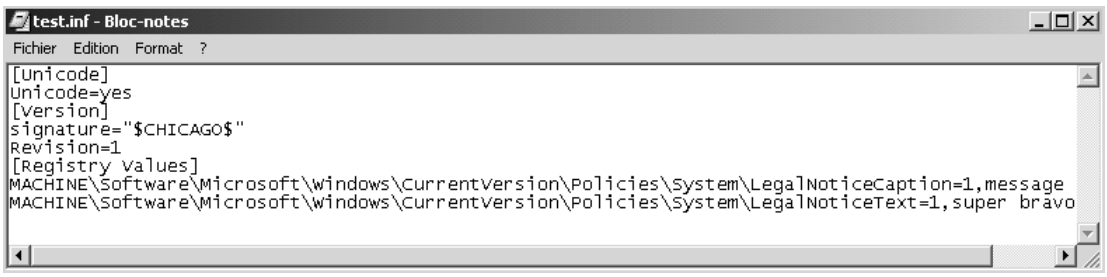
- environnement hautement sécurisé natif Windows® 2000 (Hisecws.inf et Hisecdc.inf),
- Implémenter un environnement à sécurité renforcée (Securews.inf et Securedc.inf),
- Implémenter un environnement considéré non sécurisé, mais plus compatible (Compatws.inf).(Ne pas utiliser sur un Contrôleur de Domaine),

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

Clés de registre... d'une stratégie

On peut avoir une idée des modifications apportées au niveau de la base de registre, en visualisant le contenu de notre modèle...



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…

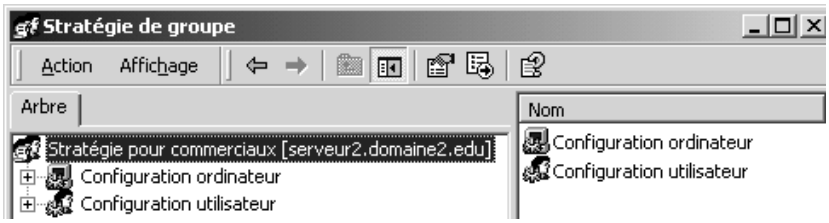
GPO D'UNITE ORGANISATIONELLE

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

Les GPO de domaine (ou d'Unité Organisationnelle) se décomposent en deux catégories



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

  valables a la mise sous tension du poste, puis lors de rafraîchissement périodiques... (cf secedit / gpupdate...)

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

  valables a chaque ouverture de session puis lors de rafraîchissement périodiques... (cf secedit / gpupdate...)

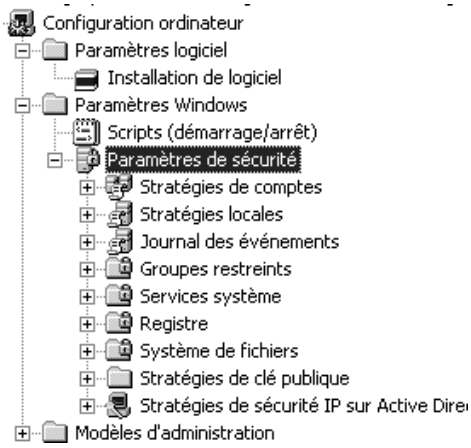
Par défaut, les stratégies de groupes ont un traitement synchrone, c'est à dire :

- 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.

N.B: Dans le cas ou l'on définirait des stratégies contradictoires, il faut savoir que normalement les stratégies ordinateur 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

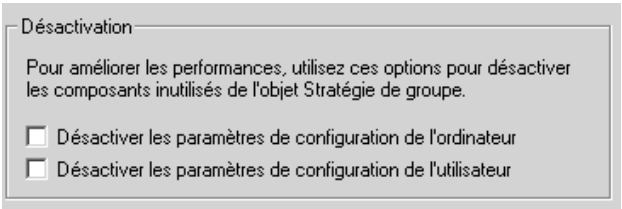


Les ajouts notables dans les **stratégies de groupe pour les utilisateurs** sont:

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 autres que 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

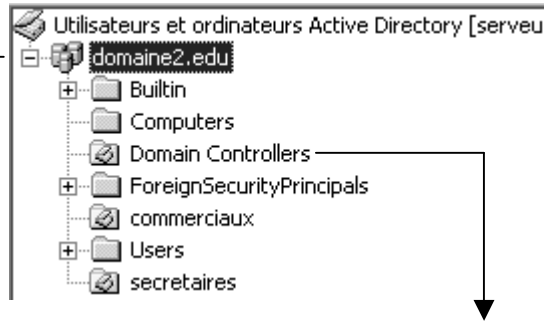
HKEY_LOCAL_MACHINE Et **HKEY_CURRENT_USER**

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.

Stratégies Prédéfinies existantes :

Sl on regarde dans **Utilisateur et ordinateurs Active Directory**

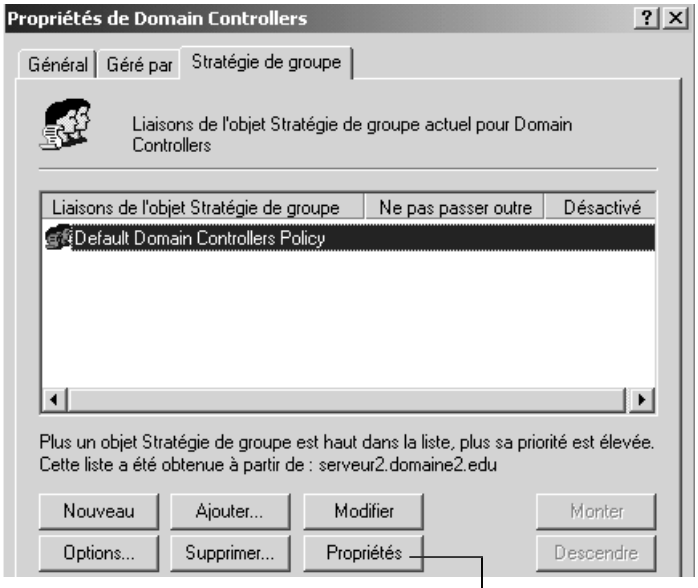


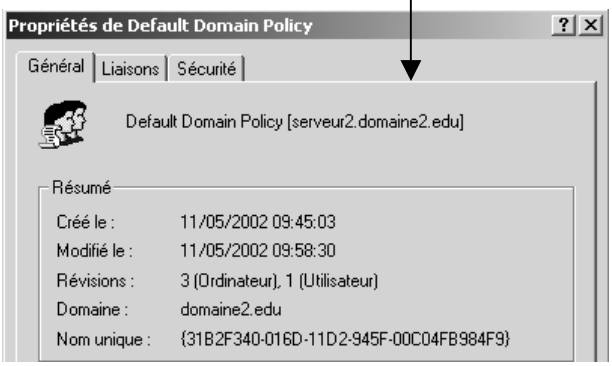
Il existe une GPO pour le **Domain**

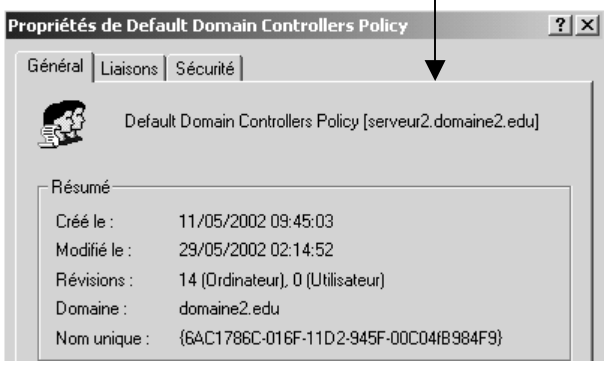
(ici le pointeur)

Et Il existe une GPO pour **Domain Controllers**

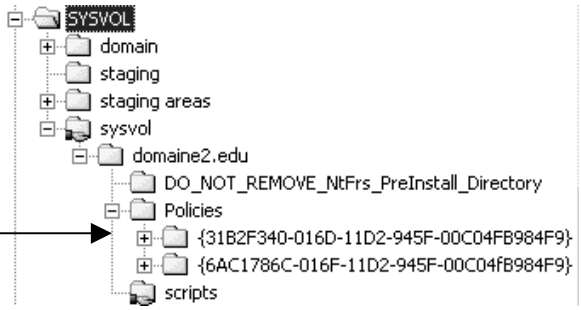
(ici le pointeur)





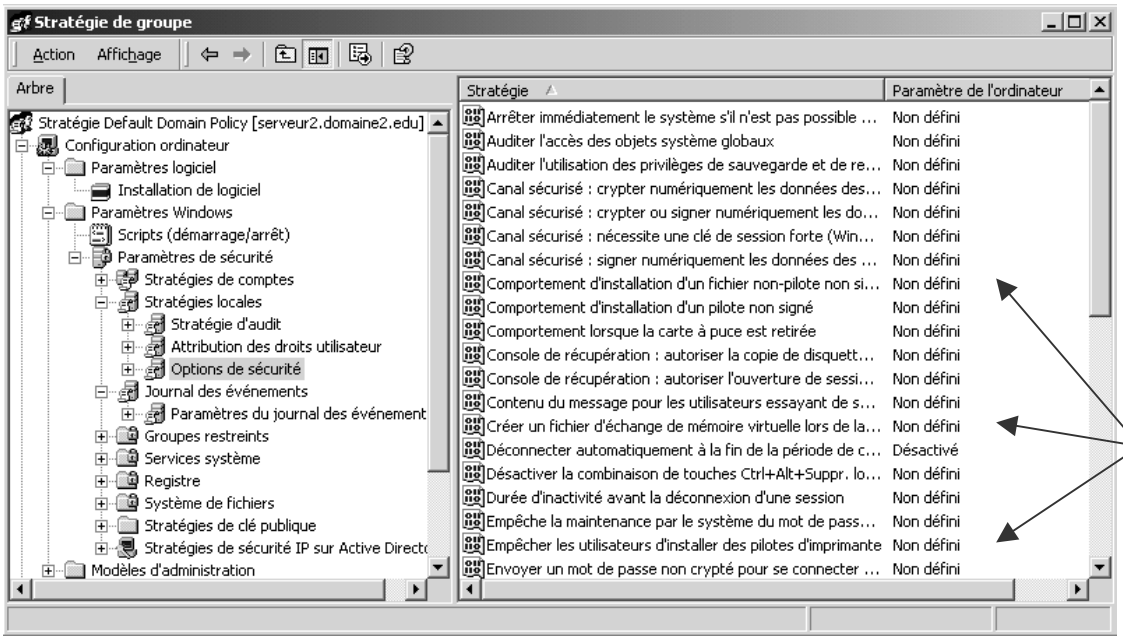


Stockées physiquement dans **sysvol** (qui est répliqué entre CD...)



N.B: les stratégies de groupes sont aussi visibles depuis la mmc **Utilisateur et ordinateurs Active Directory** en demandant **Affichage / fonctionnalité avancées**, dans le conteneur **Domaine, System, Policies** (il s'agit en fait de pointeurs sur les **GPO** physiquement stockées dans **sysvol**)

Ces stratégies existent, mais sont très permissives, dans le sens ou la plupart de leur composant sont non spécifiés...voire spécifié avec une valeur désactivée...



Si on modifie ou ajoute une stratégie au niveau du domaine ou des contrôleurs de domaine, ceux-ci doivent attendre 5 minute avant d'en recevoir les effets...

On force le rafraîchissement à l'aide de la commande

Sous **Windows 2000 Pro-Srv**

Secedit /refreshpolicy machine_policy

ou

Secedit /refreshpolicy user_policy

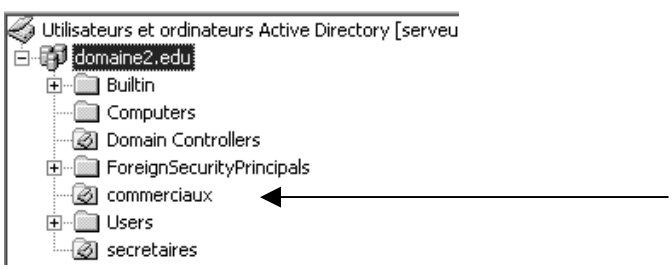
Ssous **Windows XP – Srv 2003**

Gpupdate /force

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** (cf chapitre suivant)

Définir une Stratégie de Groupe sur une U.O :

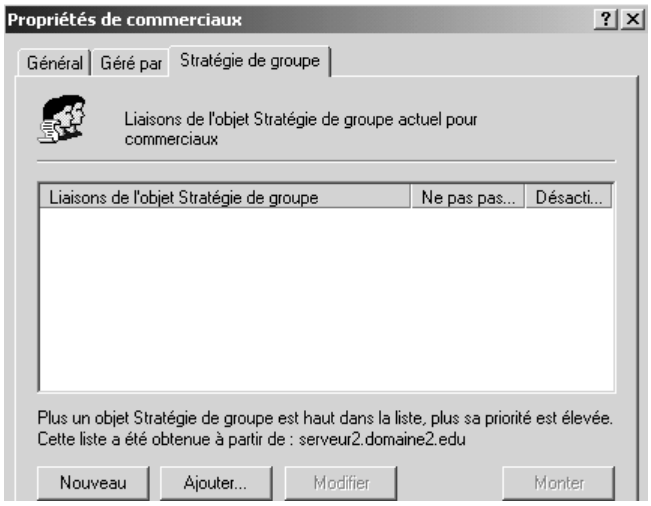
Ayant ouvert une session sur un serveur contrôleur de domaine, il faut lancer la mmc **Utilisateur et ordinateurs Active Directory**



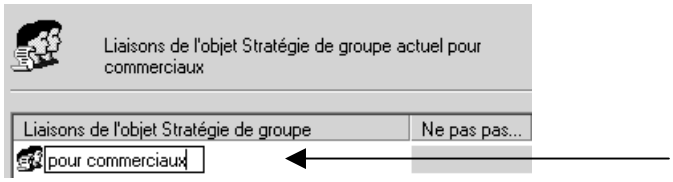
En se plaçant sur l'Unité voulue, il faut demander propriété :

Exemple ici commerciaux

et demander **Stratégies de groupe**

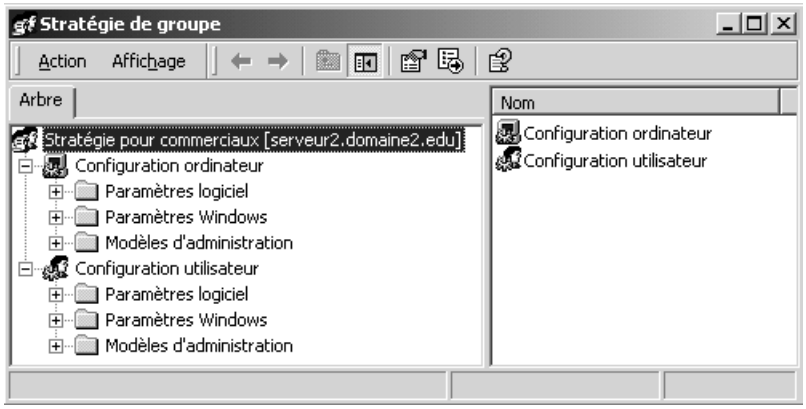


Il faut se créer une nouvelle stratégie via **Nouveau**



De préférences lui donner un nom en relation avec l'UO qu'elle gère par exemple ici "pour commerciaux"

puis modifier



Il faut enfin déplacer (ou créer si besoin) dans l'UO les éléments dont on veut qu'ils héritent la stratégie...par exemple un compte ordinateur si la stratégie travaille dans le registre configuration ordinateur.

N.B: il est toujours déconseillé de poser des stratégies au niveau des **OU** prédéfinies, il vaut mieux créer ses propres **OU** et poser des stratégies dessus.

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 2000 XP(PRO) serveur 2000-2003 Hors Domaine:

  stratégies locales

- Pour des client 2000 XP(PRO) serveur 2000-2003 membres non CD En Domaine:

  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 serveur 2000 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: (stratégies locales dévalidées)

  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 ordinateur** prennent le pas sur les **stratégies utilisateurs**.

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. ←

Non erreur doc: **machine_policy**

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

Non erreur doc: **user_policy**

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

L'utilitaire en ligne Gpupdate (XP - 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.

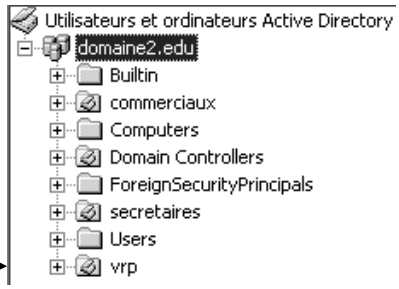
LIAISON - HERITAGE – BLOCAGE - FORCER DES GPO

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**.

Si on souhaite appliquer la même **GPO** à deux **UO** différentes, il semble inutile de créer deux **GPO** différentes, (avec tous les risques de fausse manipulation...) avec les mêmes paramètres, s'appliquant chacune à une UO différente.

Il est possible de spécifié pour une UO d'utiliser une GPO déjà existante, c'est ce que l'on appelle lier une GPO...

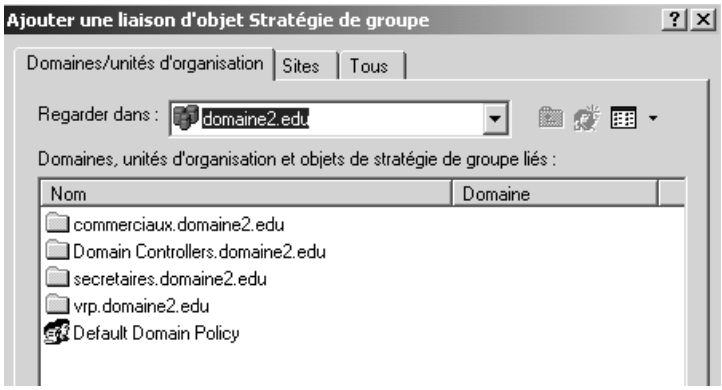


Imaginons que nous devions créer une nouvelle UO pour les **VRP**, celle-ci devant suivre les même consigne de stratégie que les commerciaux...

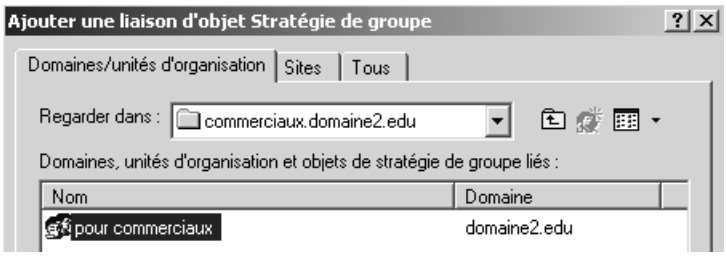
Lorsque je demande les **Stratégies de groupe** pour cette UO

On ne demande pas Nouveau, mais **Ajouter...**

La liste de toutes les **GPO** de domaine et d'UO apparaît



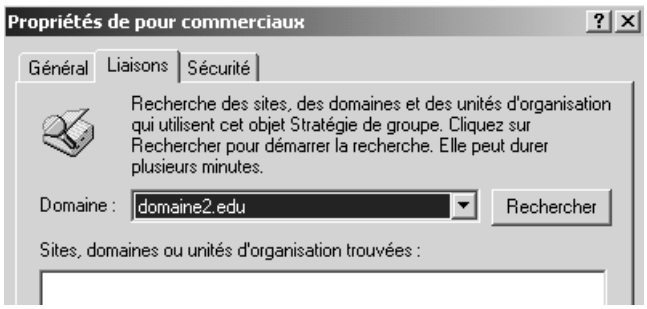
Et il faut aller dur la **GPO** qui nous intéresse…



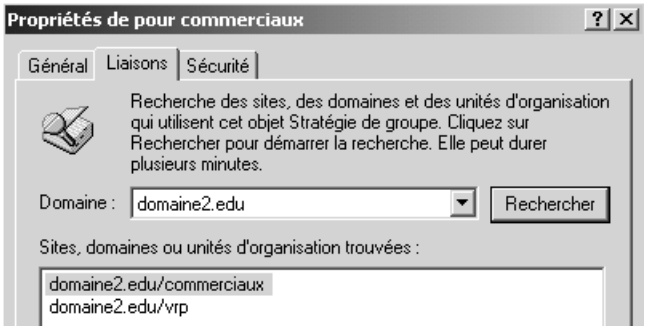
pour obtenir finalement

N.B: Attention, a partir de maintenant, toute modification de la **GPO** intitulé "pour commerciaux" et posée initialement sur l'**UO** commerciaux, s'applique bien sûr aussi à l'**UO** VRP

N.B: Rien ne permet facilement de savoir "*si une GPO est utilisée sur d'autres UO que celle sur laquelle elle est crée*".
Le seul moyen de le savoir, c'est de se placer sur la GPO, pour nous ici "pour commerciaux" dans l'UO commerciaux, et demander **propriétés** :



Puis on demande **Rechercher**



On a la liste de toutes les **UO** utilisant cette **GPO**

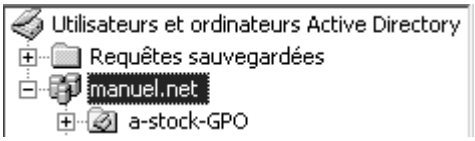
évidemment l'UO **commerciaux** utilise cette GPT

mais aussi l'UO **vrp** !

Gestion des liaisons de GPO:

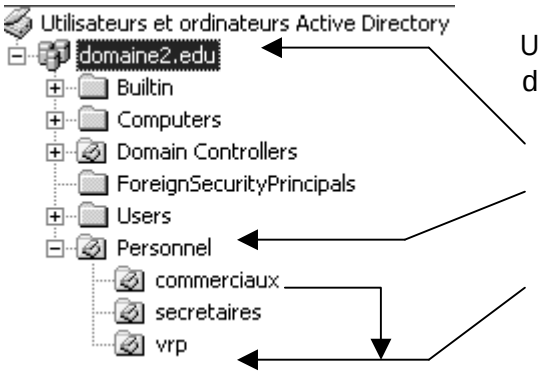
On peut créer un UO « vide » et servant simplement de receptacle à toutes les GPO

Ensuite on travaille simplement avec des liens…



héritage et blocage d'héritage:

On le sait, 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'un objet GPO, il suffit simplement de demander sur cet objet "**bloquer l'héritage**":

N.B: On ne peut pas bloquer l'héritage des stratégies de domaine pour l'UO prédéfinie Domain Controller... **par conséquent toutes les stratégies définies au niveau du domaine s'appliquent aussi aux controlleurs** !

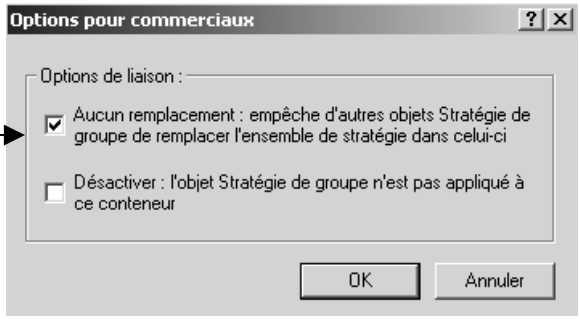
N.B: lorsque l'on bloque un héritage, on bloque cet héritage pour toutes les stratégies qui pourraient venir... sauf celles qui ont été spécifiées avec la mention "**aucun remplacement**" (cf chapitre suivant)

Interdire le blocage d'héritage :

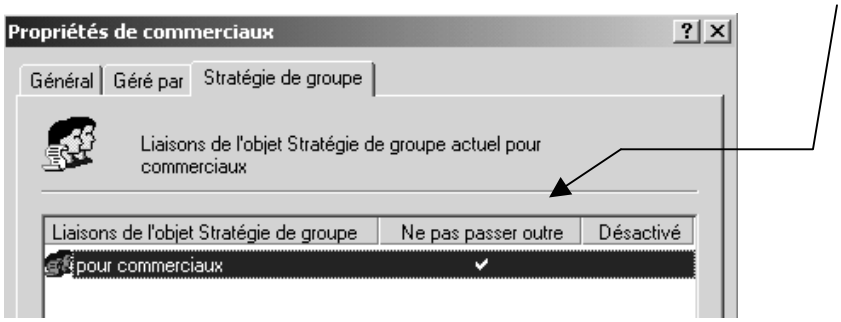
Il est possible dans une stratégie de spécifier que cette stratégie ne peut pas être bloquée par une stratégie ultérieure (on peut donc forcer l'héritage...)

Pour forcer une stratégie à être appliquée, on peut donc demander sur cette stratégie, **Option**

Et demander alors **Aucun remplacement**



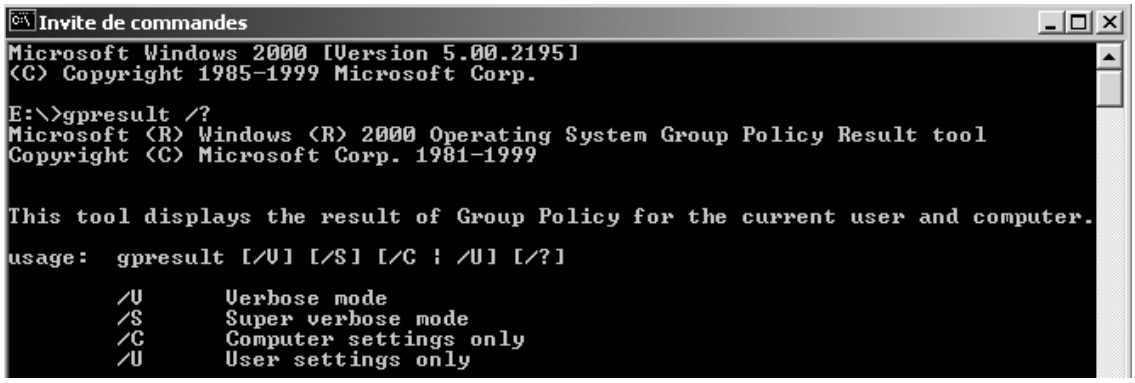
Cela se visualise ensuite sous la forme d'une coche **Ne pas passer outre**



L'utilitaire Gpresult.exe du kit de ressource

Il existe un utilitaire du kit d ressource technique permettant d'avoir un compte rendu sur une machine des GPO sui se sont appliquées

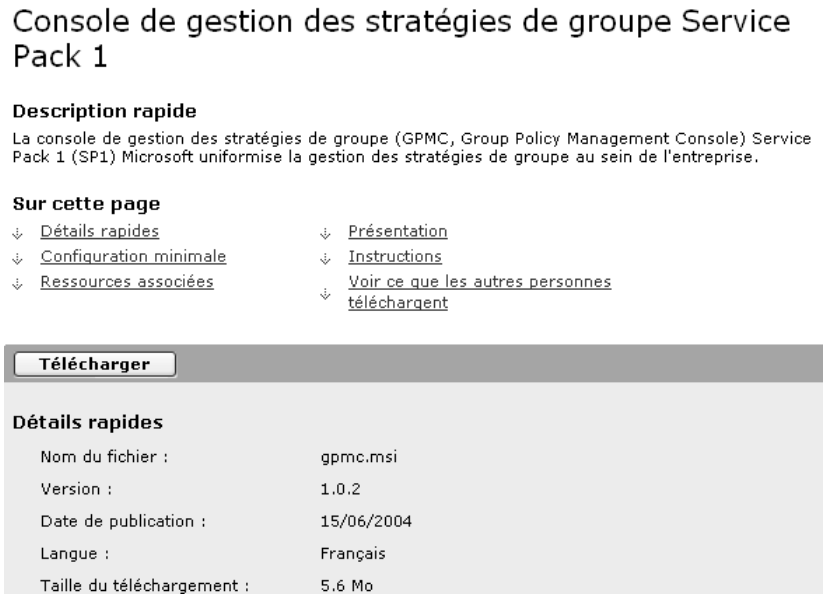
Il se lance en ligne de commande par **gpresult.exe**



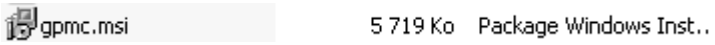
GESTION STRATEGIES 2003 - RSOP

Console Gestion stratégie de groupe et RSOP sur XP et serveur 2003

Il existe un utilitaire disponible à partir des serveurs 2003 et pour des clients XP. Cet outils permet d'avoir une idée du jeux de stratégie final résultant, pour un ordinateur ou un utilisateur.



L'installation ou la désinstallation ne pose pas de problèmes



Se gérant classiquement via

Autorisation avec xp-sp2

La version de base nécessite parfois que les pare-feu Xp-sp2 soit désactivé (alors que normalement l'autorisation de l'exception bureau à distance devrait suffire.), ce qui motive le téléchargement de sa mise à jour SP1…

Si on veut utiliser RSOP en laissant activer le Pare-feu sur les clients XP, il faut encore implémenter une stratégie de domaine (ou une stratégie uniquement pour les machines sur lesquelles on souhaite pouvoir utiliser RSOP…)

Cette stratégoe doit permettre d'utiliser **l'administration à distance** . depuis l'adresse ip… du serveur…

Configuration ordinateur

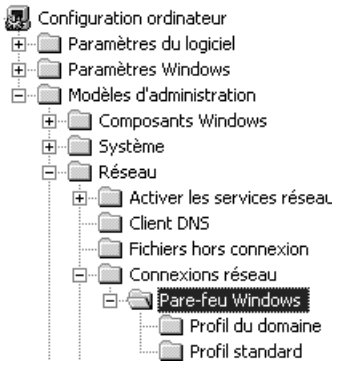
/ Modèles d'administration

/ Réseau

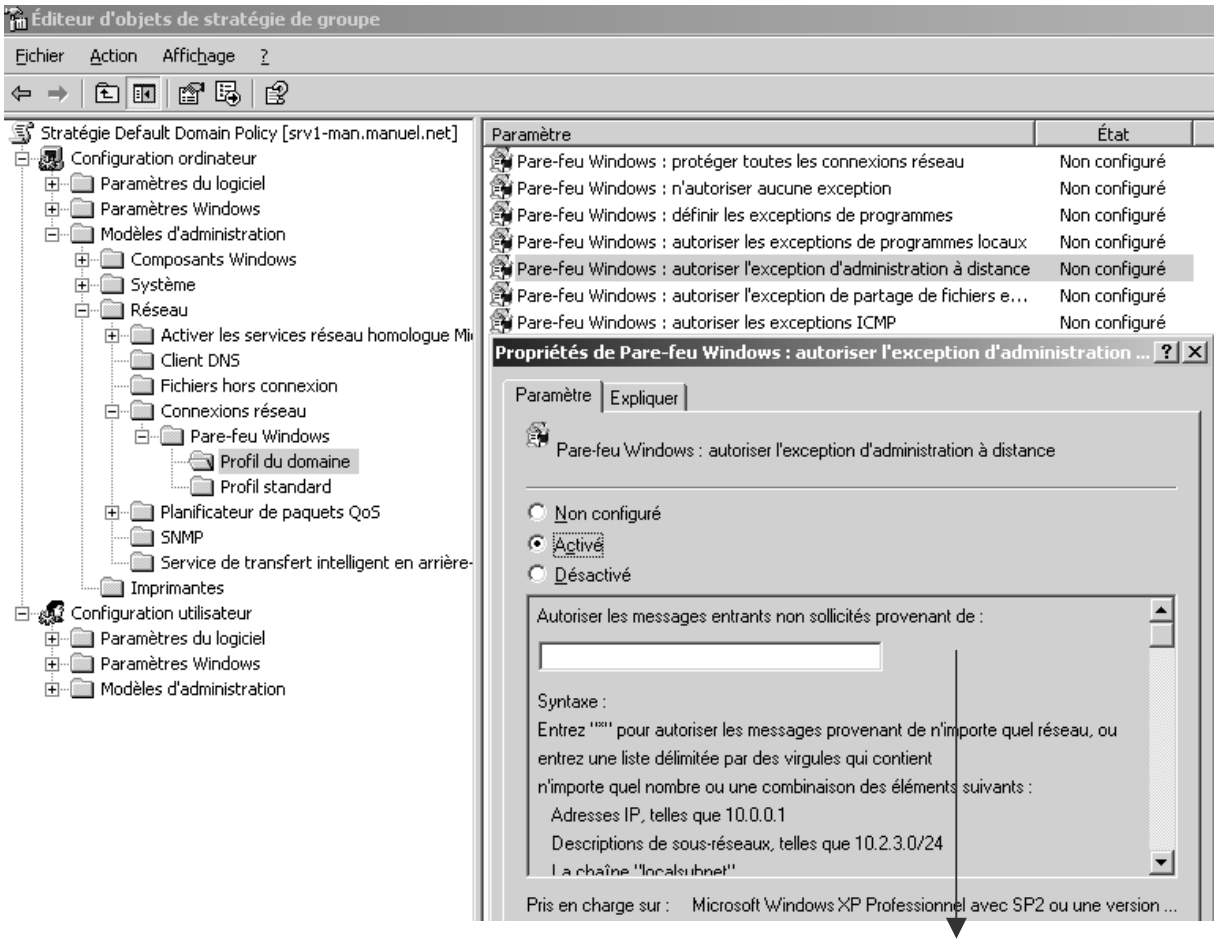
/ Connexions réseau

/ Pare-feu Windows

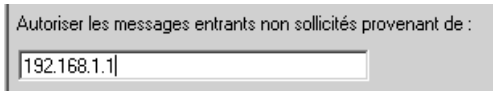
Profil du domaine



donnant



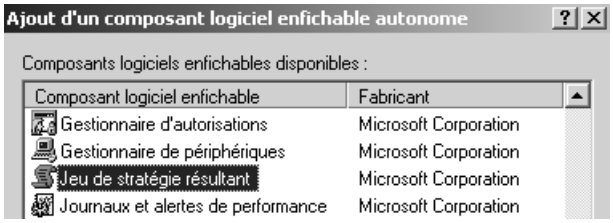
Il faut indiquer l'adresse IP du serveur 2003 depuis laquelle on compte faire de l'administration



Et propager sur reboot des pc client (car c'est une **stratégie d'ordinateur**)

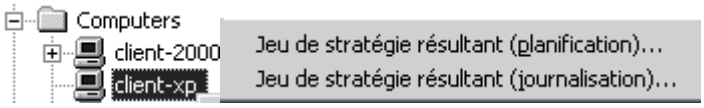
Utilisation de RSOP sp1 pour 2003

On peut faire appel à cet utilitaire directement depuis une mmc

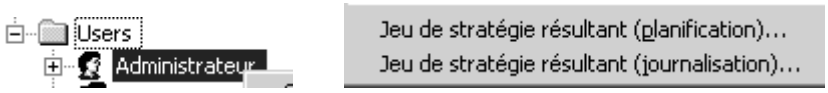


ou depuis la console **Utilisateur et Ordinateurs Active Directory** en demandant **Toutes les taches**

sur un ordinateur



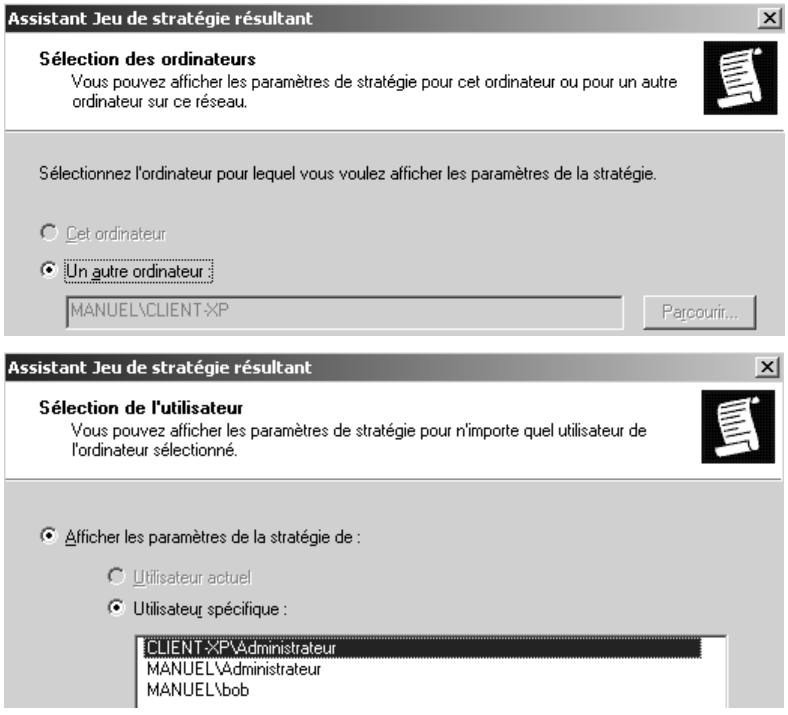
ou un utilisateur



Sur un ordinateur (par exemple)

Si on se place sur l'ordinateur **client-xp** et que demande

Jeu de stratégie résultant (journalisation)... alors on obtient

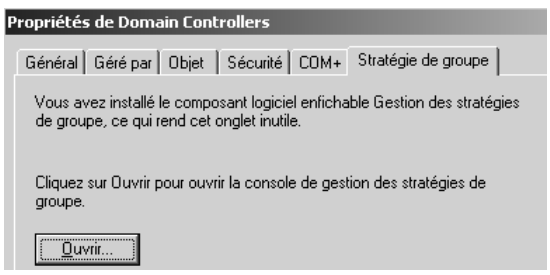


Console gpmc et Gestion des stratégies de groupes

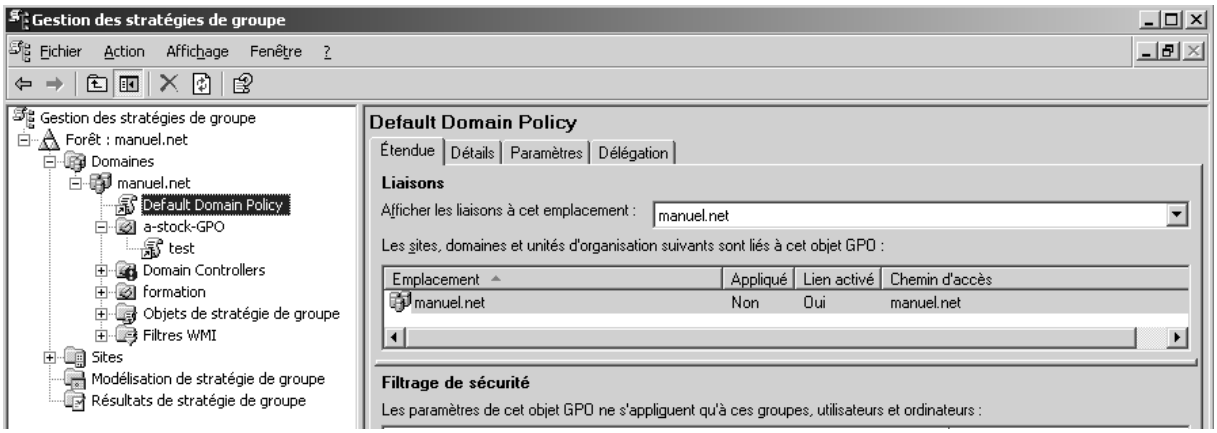
Une nouvelle console est utilisable dans les outils d'administration

Gestion des stratégies de groupe

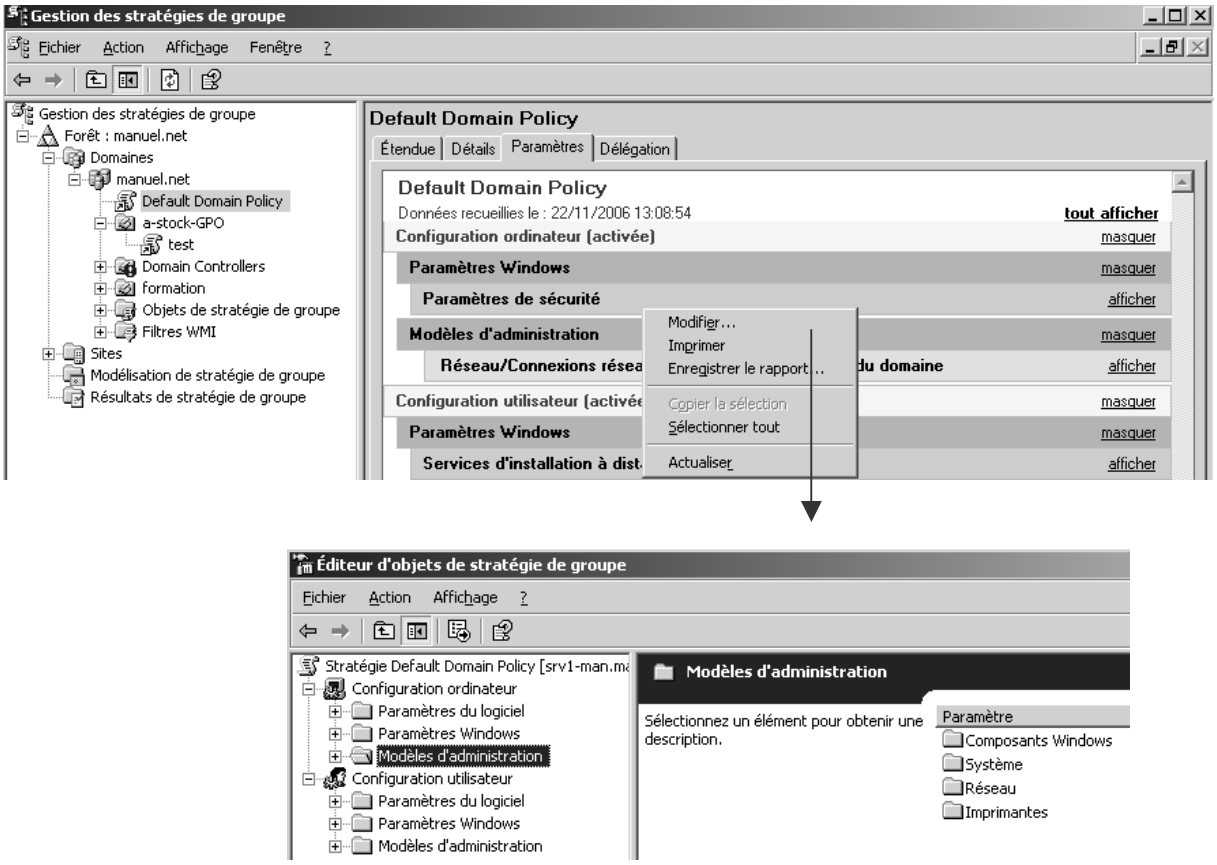
ou à la place de **Stratégie de groupe**



Elle donne une interface plus complète



On retrouve les stratégies ensuite via **Modifier**



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.

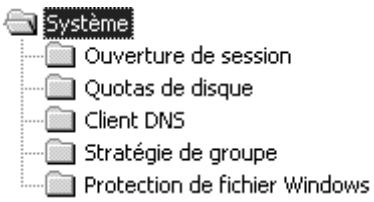
On a regroupé dans les **modèles d'administration**, toute une série de paramètres, disponibles tantôt uniquement pour la partie **ordinateur**, pour la partie **utilisateur**, ou parfois les deux...

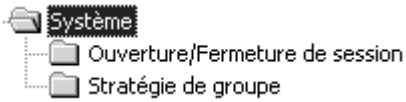
Type de paramètre	Éléments contrôlés	Disponible pour
Composants Windows	Les parties de Windows 2000 et ses outils et composants auxquels les utilisateurs peuvent accéder, y compris la console MMC	
Système	Les procédures d'ouverture et de fermeture de session, la console Stratégie de groupe, les quotas de disque et le traitement par boucle	
Réseau	Les propriétés des connexions réseau et des connexions d'appel entrant	
Imprimantes	Les paramètres d'imprimante qui peuvent obliger les imprimantes à être publiées dans Active Directory et désactiver l'impression à partir d'un navigateur Web	
Menu Démarrer et barre des tâches	Les fonctionnalités auxquelles les utilisateurs peuvent accéder à partir du menu **Démarrer** et les options qui rendent le menu **Démarrer** en lecture seule	
Bureau	Le bureau Active Desktop, y compris ce qui apparaît sur les bureaux, et ce que les utilisateurs peuvent faire avec le dossier Mes documents	
Panneau de configuration	L'utilisation des applications Ajout/Suppression de programmes, Imprimantes et Affichage du Panneau de configuration	

allez regarder un peu l'éventail des possibilités...

Composant **Windows** ordinateur utilisateur

Composant **Système** ordinateur utilisateur





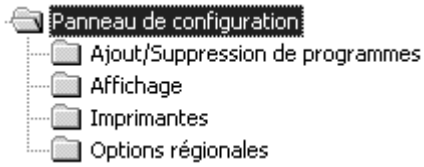
Composant **Réseau** ordinateur utilisateur

Composant **Imprimante** ordinateur

Composant **Menu Démarrer barre tâche** utilisateur

Composant **Bureau** utilisateur

Composant **Panneau de configuration** utilisateur



Méthodologie de mise en oeuvre

Il est toujours conseillé de

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

- Rarement définir des stratégies globales au domaine, mais toujours sur des UO précises

Il est bon aussi de

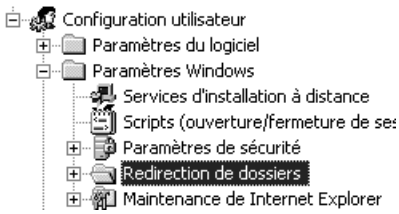
- stocker toutes les stratégies dans UO spécifique et ensuite d'utiliser des liens pour les mises en œuvres sur les autres UO 

- 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 - REDIRECTION DOSSIERS

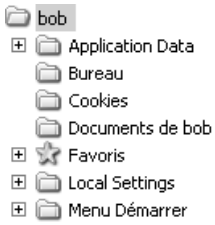
Configuration Utilisateur

Il semble normal que la redirection de dossier se fasse au niveau des utilisateurs



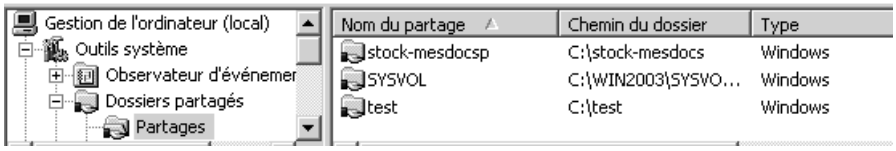
Cette stratégie permet de rediriger au choix 4 dossiers du profil d'un utilisateur

- **Application Data**
- **Bureau**
- **Mes documents**
- **Menu Démarrer**



On prendra le soin de préparer un dossier de stockage sur le serveur...

Genre **stock-mesdocs**

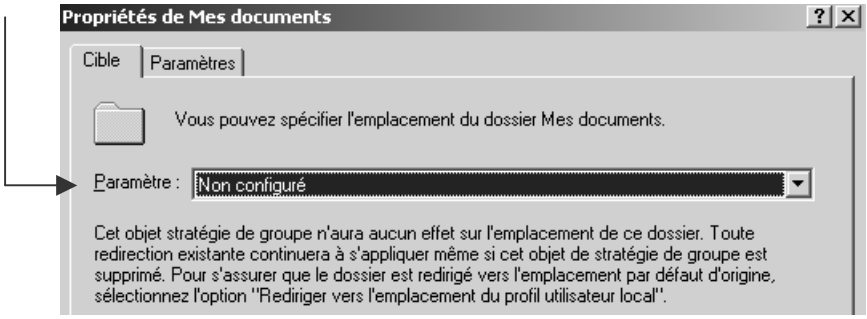


Rediriger mes documents

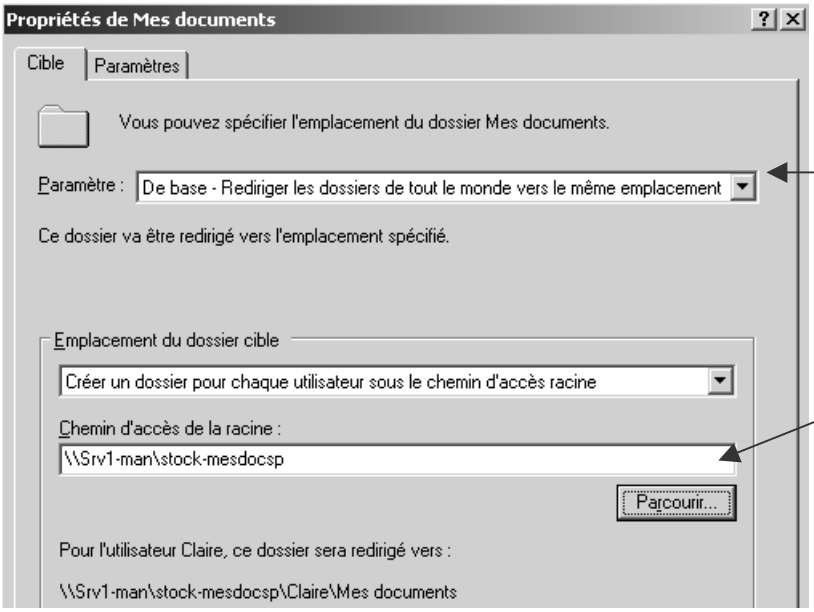
Dans la stratégie, on demande les propriétés de

Redirection de dossiers / Mes documents

dans lesquelles on demande **Paramètre**



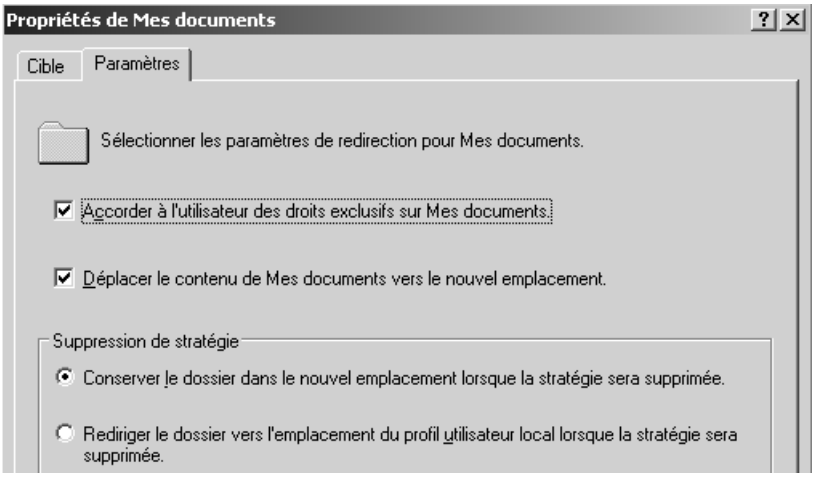
Le paramètre **De base** amène alors deux onglets supplémentaires



De base

Et On indique le dossier de stockage crée...

Les options par défaut sont les moins dangereuses.



Rediriger bureau application data démarrer

La redirection des 3 autres dossiers se construit de même

Sur le serveur pour chaque utilisateur on aura

Et sur le client un message de synchronisation apparaît lors de chaque fin de session

N.B : il vaut mieux avec cette technique éviter les sessions multiples pour un même utilisateur...

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 type 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

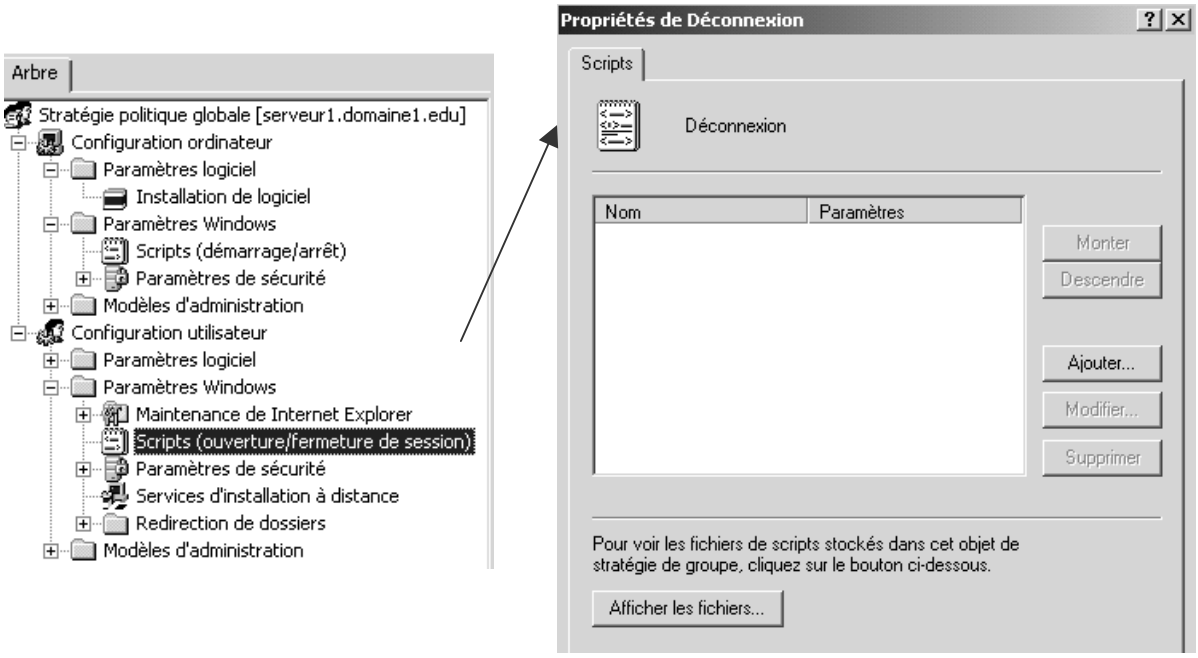
- Script d'ouverture de session : s'exécute lors d'une ouverture de session

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 :

pour utiliser un script de fin de session dans une **GPO**, le script étant déjà écris dans un fichier **.bat** ou **.vbs**,

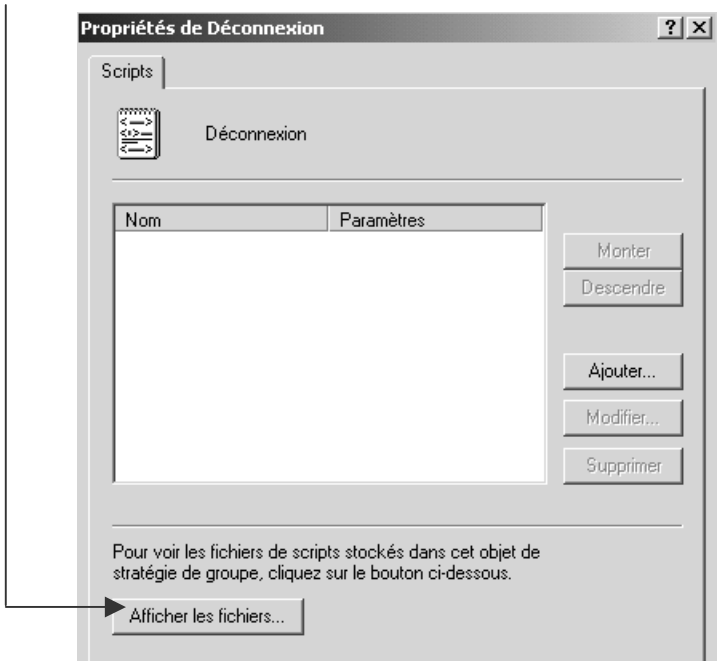


Il faut effectuer une manœuvre en deux temps :

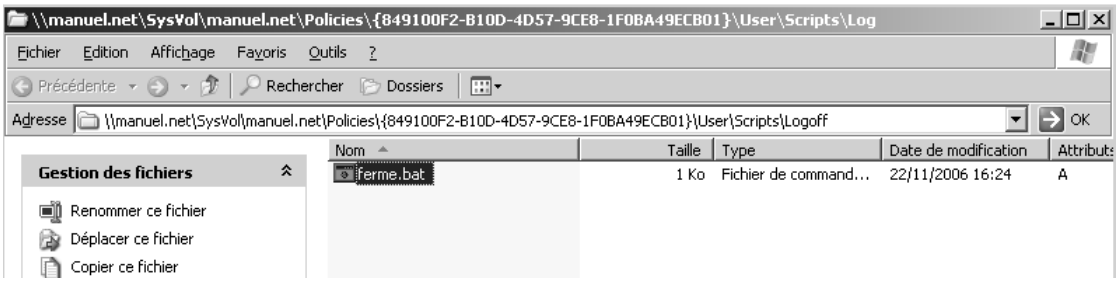
1. D'abords il faut copier le script dans la **GPO**
2. Puis il faut dire à la **GPO** d'utiliser ce script…

Copier le script dans la GPO

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

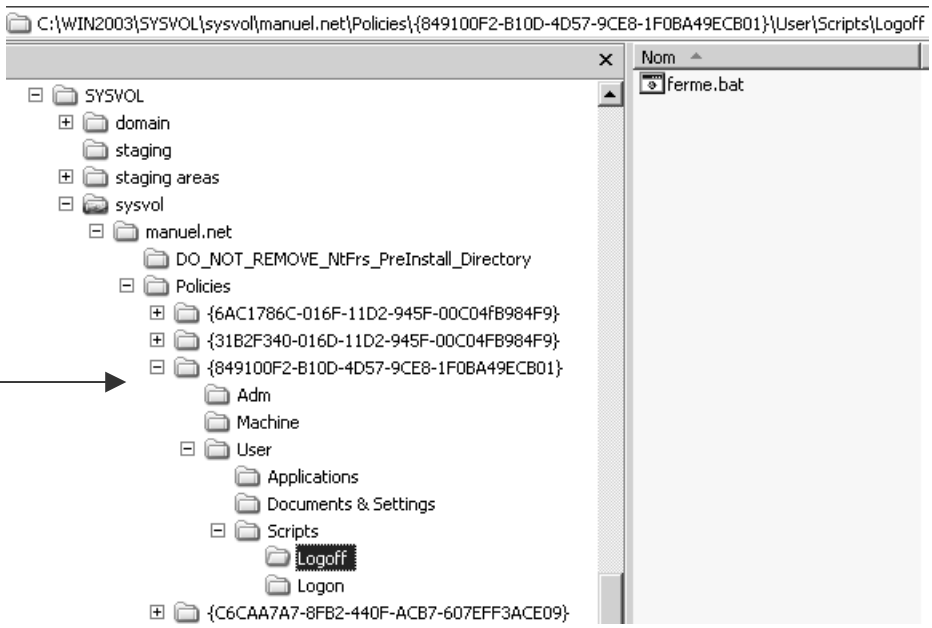


Une fenêtre s 'ouvre dans laquelle il faut copier notre script (ici **ferme.bat**)



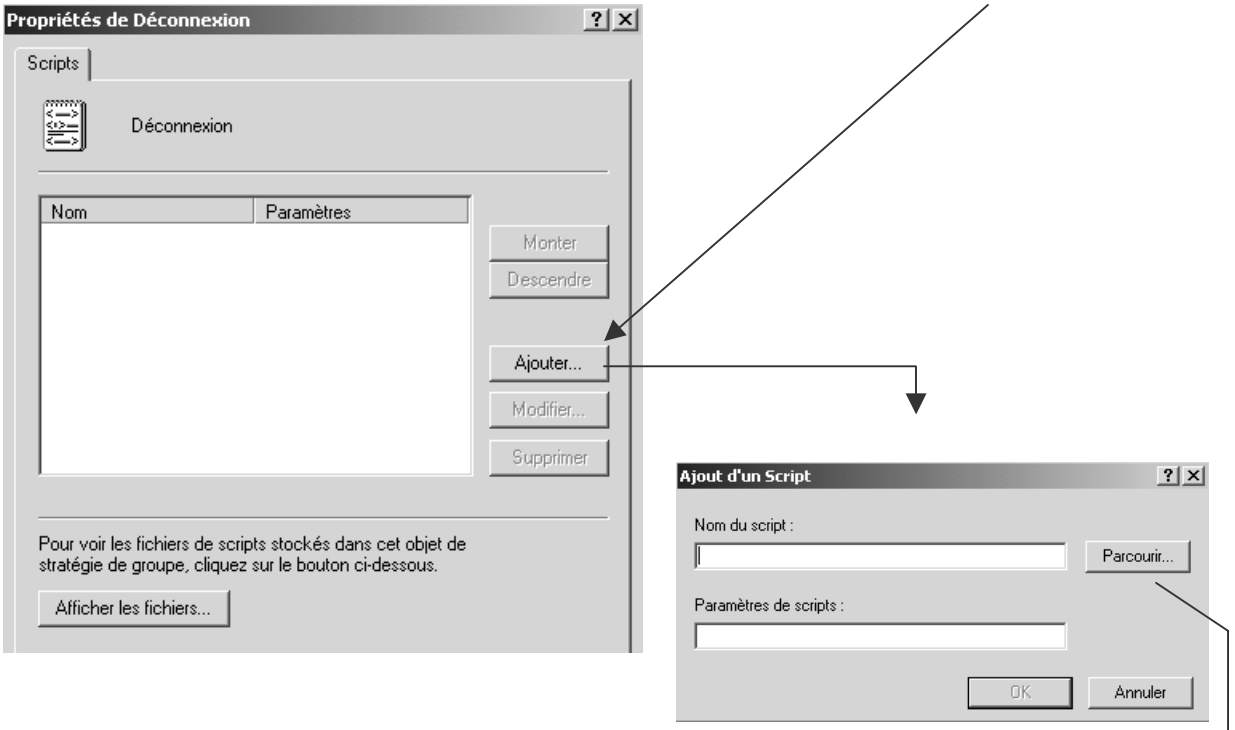
N.B : cette opération a simplement pour but de stocker dans notre **GPO** une copie du script, qui physiquement se trouve dans la stratégie

{849100F2-B10D…}



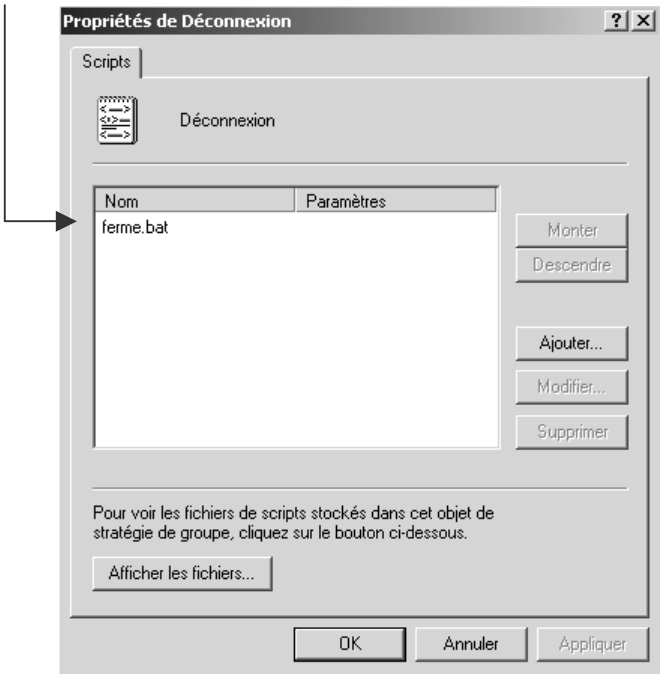
Utiliser le script dans la GPO

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



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

Maintenant on a un script de déconnexion....



test et visualisation :

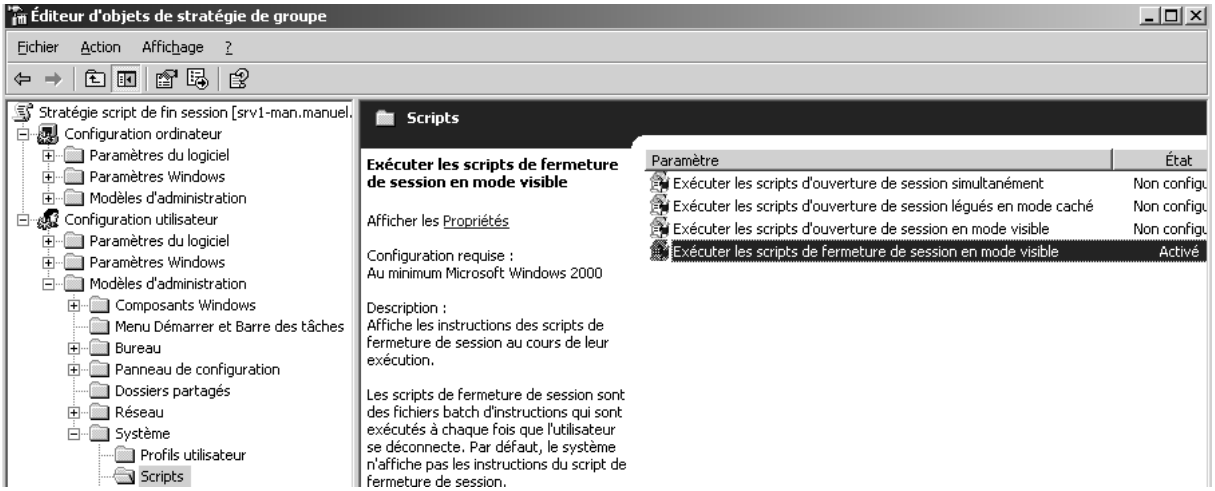
Sachant que

- 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 bête commande **pause**, dans un script de déconnexion, provoque le blocage du poste pendant 10mn, puisque personne ne peut appuyer sur la touche fatidique...

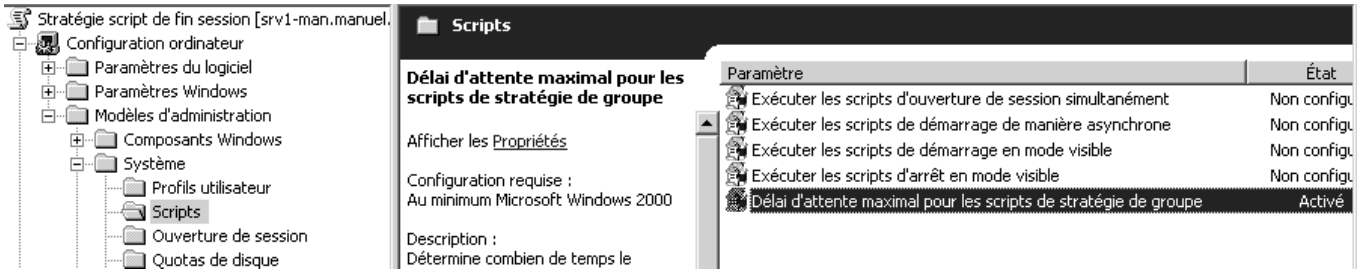
Il existe un modèle de **stratégie utilisateur**,

permettant **d'exécuter les scripts de fermeture de session en mode visible**...



Il existe un modèle de **stratégie ordinateur**,

permettant de paramétrer le **délai d'attente maximal pour les scripts** (tous les scripts) (et 0 donnera une attente infinie...)



GPO - INSTALLATION DE LOGICIELS

Les 3 éléments Winstaller – GPO - AD

Un nouveauté de windows 2000-2003 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 demande 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, et il y en à 1 livré dans le dossier du CD de 2000 serveur

\ValueADD\3RDPARTY\MGMT\WINSTLE

Procédure d'installation et de maintenance logiciels

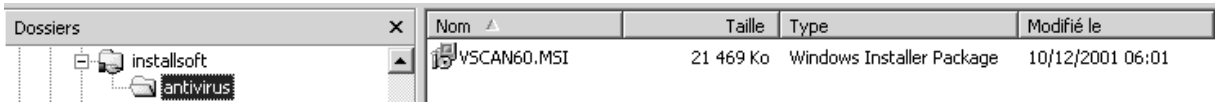
Il va falloir exécuter les étapes suivantes :

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.

Dossier sur lequel on peut si on veut donner des permissions en lecture seule..., partager le dossier de manière administrative ($), pour le rendre invisible...

Attribution - Publication de logiciel

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)

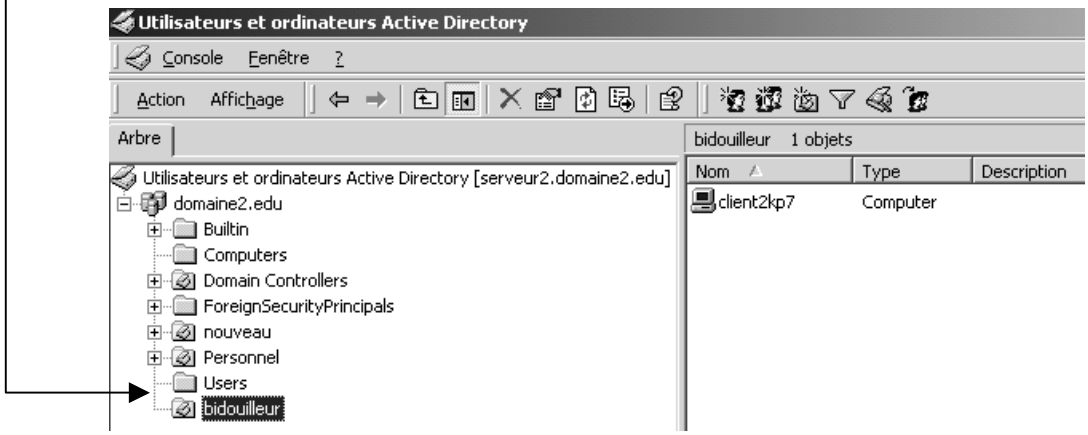
- Si on les affectent à des **utilisateurs** : lorsque l'utilisateur ouvre un session, le logiciel est annoncé (raccourcis présents) , mais l'installation ne débute réellement que si l'utilisateur clique sur l'application ou double-clique sur un fichier associé.

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.

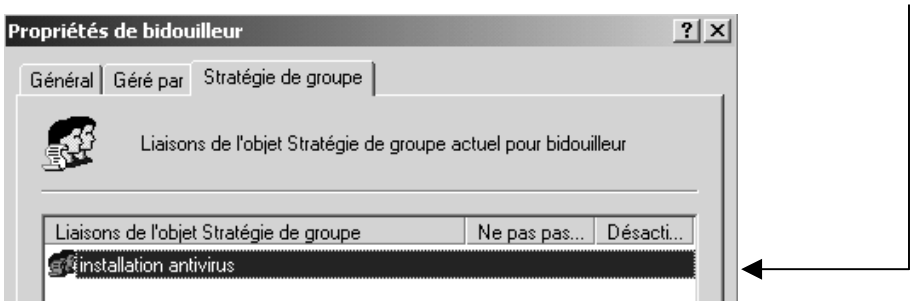
En effet lors de la publication de logiciels, il n'y a pas d'annonce. L'utilisateur peut installer l'application en passant par ajout/suppression programme, ou l'installation se fait automatiquement via un double clic sur un fichier associé

Stratégie de déploiement de logiciel

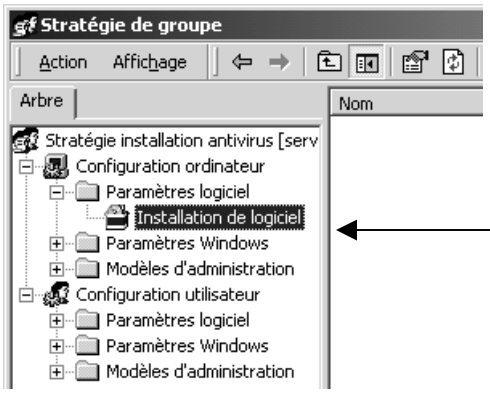
On va créer une **GPO** sur une **OU** contenant les machines des **bidouilleurs**, et leur installer un antivirus dès le démarrage du poste



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

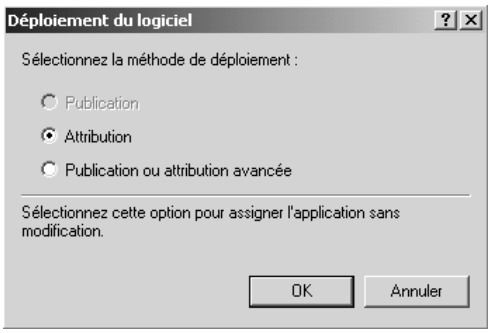


Cette GPO contient une définition de **Paramètres logiciel** dans **Configuration d'utilisateur (ou ordinateur)**

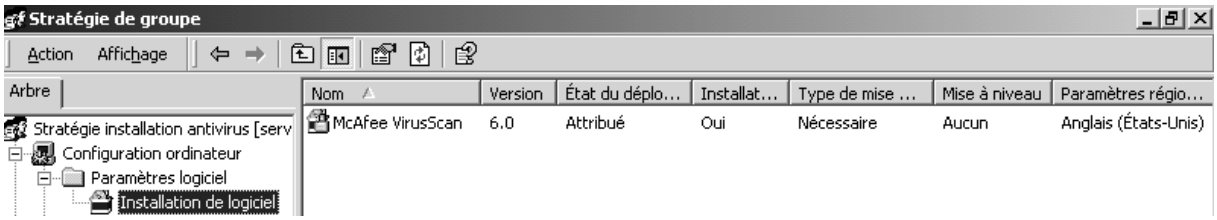


Pour laquelle on demande via un clic droit **nouveau package** et on va chercher le chemin du dossier de distribution (via le réseau bien sûr)

puis



on obtient finalement

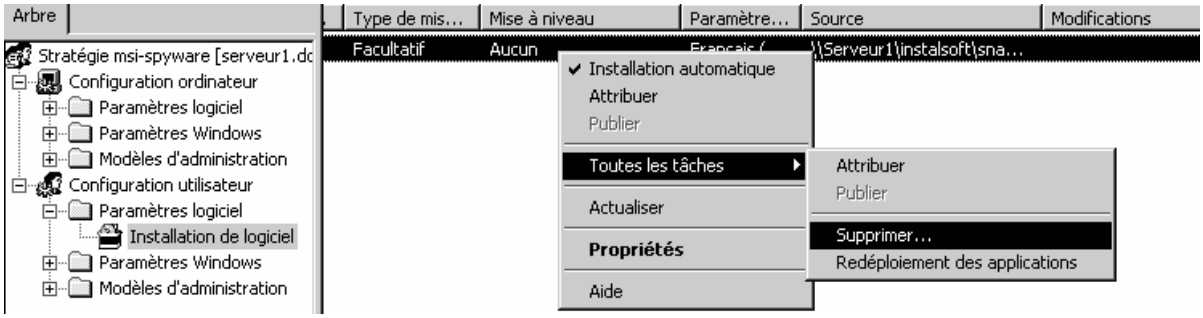


NB: si on travaille au niveau de la configuration d'utilisateur, à l'ouverture de session on récupère le MSI

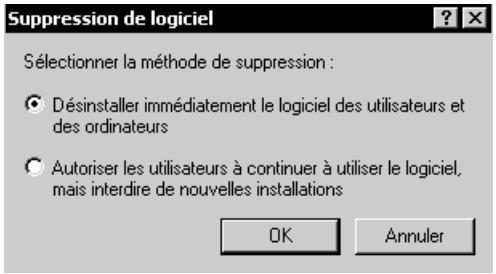
NB: si on travaille au niveau de la configuration d'ordinateur, il faut arrêter et re-démarrer le poste pour récupérer le MSI

Stratégie de désinstallation de logiciel

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



et là on peut choisir



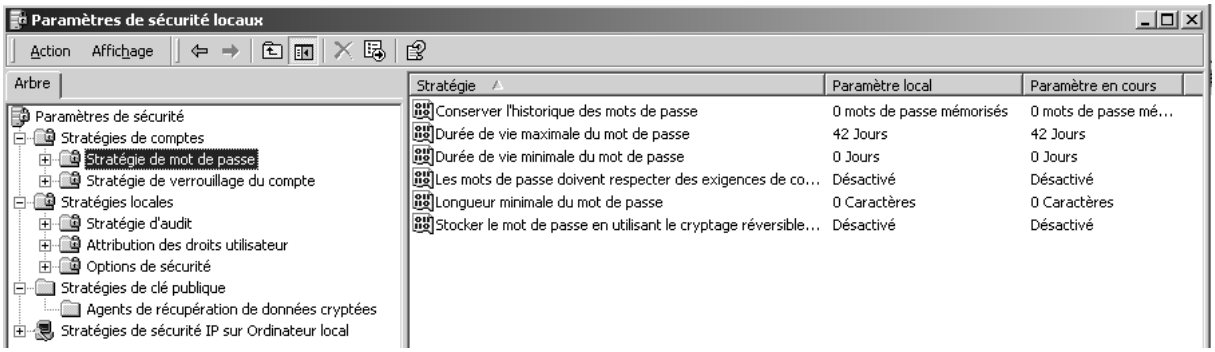
GPEDIT

Stratégie locale / réseau:

Les stratégies permettent de modifier profondément le paramétrage d'un poste 2000-xp, il existe des stratégies que l'on peut modifier localement depuis le poste, et des stratégies que l'on peut modifier à travers le 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 :

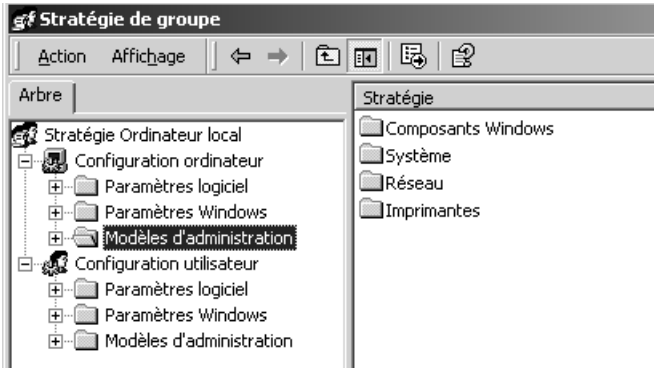


Les stratégies réseaux elles sont en général utilisée à travers le réseau (pour tout le domaine ou une partie à travers des stratégies de GPO...

Editeur de stratégie locale :

Il est cependant possible de modifier les stratégies d'une machine 2000-xp avec les options normalement réservées au stratégies de réseau, et ce localement...

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



STRATEGIES SYSTEME CLIENTS NON-2000: "POLEDIT"

Que sont les stratégies système :

Une stratégie système est une restriction imposée à un utilisateur ou à l'ordinateur d'un utilisateur pour limiter sa capacité à accéder aux ressources ou à configurer l'ordinateur. (ne plus pouvoir accéder au panneau de configuration, enlever la commande exécuter du menu démarrer, etc etc...

Ces restrictions sont obtenues via la modification de la base de registre de la machine sur laquelle la session est ouverte, et l'utilitaire **POLEDIT** permet de modifier la base de registre en utilisant une interface graphique...

Mais même si POLEDIT permet de modifier la base de registre locale, (et à fortiori une base de registre quelconque de n'importe qu'elle machine du domaine) POLEDIT devrait être utilisé essentiellement pour créer une fichier de configuration. Ce fichier de configuration sera stocké sur le serveur, et téléchargé sur chaque client à l'ouverture de session : il prévaudra alors sur les inscriptions locales de la base de registre locale !

Il existe fondamentalement deux type de stratégies système, :

la stratégies système des utilisateurs

la stratégies système des ordinateurs

La stratégie système des utilisateurs :

remplace les paramètres définis dans la zone relative à l'utilisateur courant du registre (HKEY_CURRENT_USER), elle s'applique par défaut à tous les utilisateurs, et par conséquent aussi à l'administrateur.

La stratégie système des ordinateurs :

remplace les paramètres définis dans la zone relative à l'ordinateur local (HKEY_LOCAL_MACHINE), elle s'applique par défaut à toutes les machines, même les serveurs, quel que soit l' utilisateur qui ait ouvert la session.

N.B: On peut donc considérer les stratégies système d'ordinateur par défaut comme un ensemble de stratégies à plus petit dénominateur commun.

Installer l'éditeur de stratégie :

ATTENTION : l'éditeur de stratégies est un outils puissant, son emplois doit être limité aux seuls administrateurs des machines

Il faut donc limiter son emplois en ne **l'installant pas sur toutes les machine !**

par précaution on peut toujours sauvegarder les fichiers User.dat et system.dat dans \windows (base de registre)

Pour installer l'éditeur, la situation n'est pas la même selon que l'on se trouve sur une machine NT ou Windows 95-98

Sur un serveur Windows NT :

Sur un **serveur NT** l'installation se fait en standard, et on peut lancer l'éditeur de stratégies système via

… / Programme / Outils d'administration (commun) / Editeur de stratégie système

Sur un client Workstation NT :

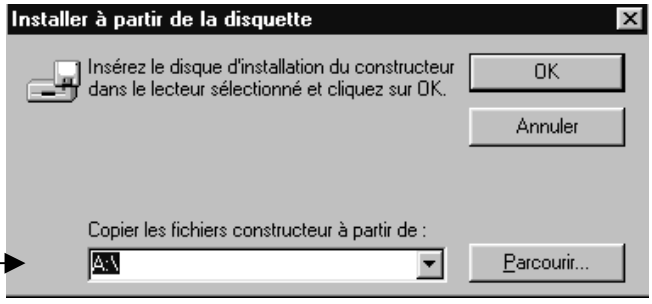
Sur une **workstation NT** il faut le récupérer soit depuis le CDROM NT serveur, mais il faut le décompresser, soit en copiant simplement les fichiers depuis le serveur **Poledit.exe** et éventuellement **Poledit.hlp**

On peut ensuite bien sûr se créer se créer un raccourci …

Pour la désinstallation il suffit de supprimer les deux fichiers en question…

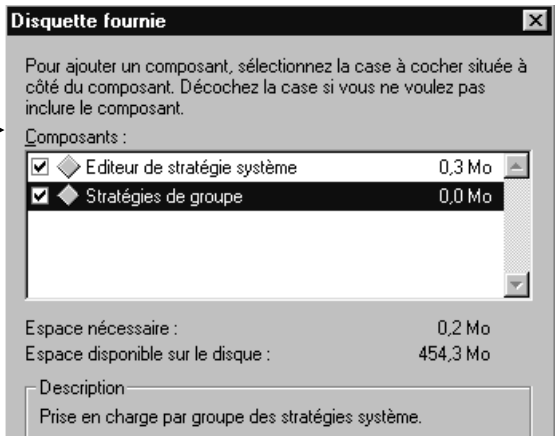
Sur un poste Windows 95-98 :

Pour installer cet outil sur votre disque dur local, ou pour installer le support pour les stratégies de groupe, utilisez l'option **Ajout/Suppression** de programmes du **Panneau de configuration**, sélectionnez l'onglet **Installation de Windows**, et cliquez sur le bouton **Disquette fournie**,



- pour windows 95 procédez à l'installation à partir du répertoire **ADMIN\APPTOOLS\POLEDIT**
- pour windows 98 procédez à l'installation à partir du répertoire **TOOLS\RESKIT\NETADMIN\POLEDIT**

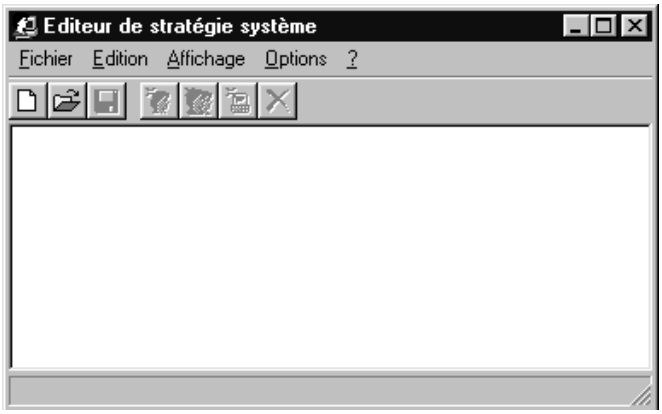
Dans l'installation bien cocher les deux cases



Désormais l'éditeur de stratégie est disponible dans le menu

... / Programme / Accessoires / outils systèmes / Editeur de stratégie système

Lorsqu'on le lance, on obtient



Pour plus d'informations sur les stratégies système et sur cet éditeur, consultez les rubriques correspondantes dans le Kit de ressources Windows 95 (**WIN95RK.HLP**) ou Windows 98 (**WIN98RK.HLP**).

Pour la désinstallation il suffit de demander le menu
Démarrer / panneau de configuration / Ajouter / suppression programme
Une entrée libellée "éditeur de stratégies système" apparaît
il suffit de demander de la désinstaller

STRATEGIE LOCALE OU MODELE

POLEDIT permet de modifier la base de registre locale, (et à fortiori une base de registre quelconque de n'importe qu'elle machine du domaine)

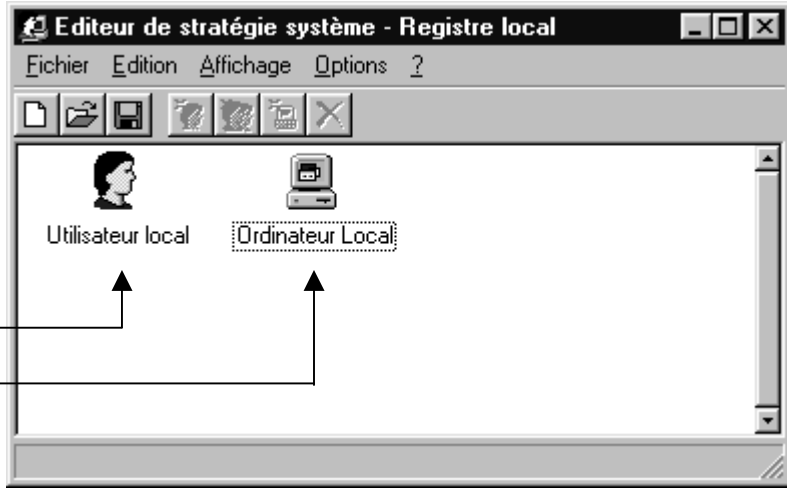
POLEDIT peut aussi créer un fichier de configuration. Ce fichier de configuration sera stocké sur le serveur, et téléchargé sur chaque client à l'ouverture de session : il prévaudra alors sur les inscriptions locales de la base de registre locale

Stratégie locale ou "mode registre" :

En mode registre, on édite donc directement le registre, et les modifications sont à priori directement visualisables

il n'est pas nécessaire de fermer la session en cours ou de re-démarrer l'ordinateur pour visualiser les effets

par le menu :
Fichier / Ouvrir la base de registre

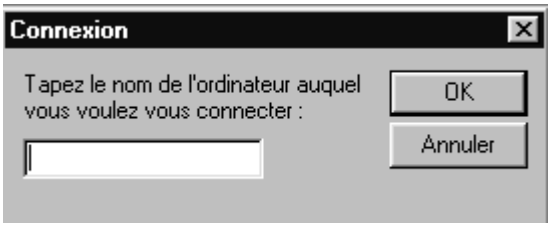


on édite la base de registre locale à travers :

l'**Utilisateur local**

ou l'**Ordinateur local**

par le menu :
Fichier / Connecter

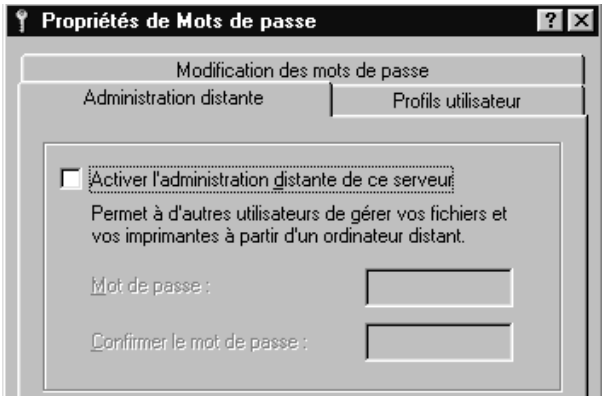


on peut éditer le registre d'une machine distante, à condition que sur cette machine un certain nombre de manipulation ait été faites :

1. l'**Administration distante** doit avoir été activée , via le menu

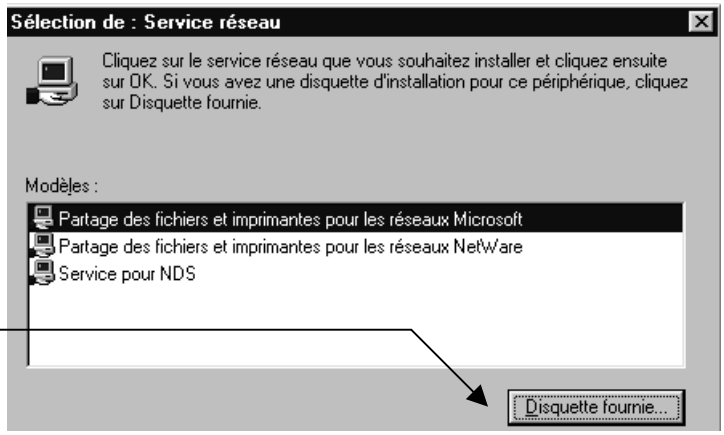
/démarrer / panneau de configuration / Mot de passe

onglet **Administration distante**



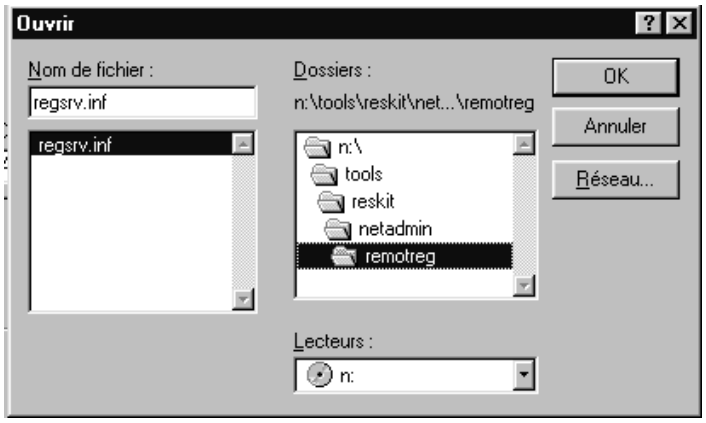
(ce qui est fait de manière implicite si on est Administrateur d'un domaine et que le client 98 est rattaché au domaine)

2. Le service **Registre distant** soit installé, via le menu contextuel de **voisinage réseau / propriété /** dans lequel on demande d'ajouter un service spécifique, que l'on prends via "disquette fournie"



- dans le dossier **TOOLS\RESKIT\NETADMIN\REMOTEREG**

Uniquement sur windows 98



pour plus re renseignement cf "Paramétrage de l'Administration à distance" du **Kit de ressource technique de windows 98**

N.B: MAIS DE MANIERE GENERALE IL EST DECONSEILLE D'UTILISER LE MODE REGISTRE. SI UNE INCOMPATIBILITE SE PRESENTE SPECIFIQUE A UN ORDINATEUR OU UN UTILISATEUR IL EST RECOMMANDE DE CREER DANS LE DOMAINE UNE STRATEGIE SPECIFIQUE POUR CET ORDINATEUR OU CET UTILISATEUR

Fichier de stratégie ou "mode stratégie":

Vous pouvez créer des fichiers de stratégies ou bien utiliser les exemples qui vous sont fournis dans le dossier ADMIN\RESKIT\SAMPLES\POLICIES.

En mode fichier de stratégie, on édite un fichier caractérisé par le fait que son extension est **xxxxx.POL**

Pour qu'un tel fichier de stratégie soit effectif, il est nécessaire que plusieurs conditions soient requises :

- le fichier de stratégie a été sauvegardé dans le dossier partagé du serveur NT CPD nommé **Netlogon**, sous le nom réservé :
  - ✓ **Ntconfig.pol** s'il a été crée via l'éditeur de stratégie NT et se destine à gérer tous les clients NT ouvrant leur session sur ce serveur CPD
  - ✓ **Config.pol** s'il a été crée via l'éditeur de stratégie windows 95-98 et se destine à gérer tous les clients windows 95-98 ouvrant leur session sur ce serveur de domaine
- l'utilisateur à ouvert une nouvelle session sur le domaine géré par le CPD depuis que le fichier de stratégie y a été placé

N.B: LES STRATEGIES SYSTEMES CREES SOUS L'EDITEUR DE STRATEGIE NT NE PEUVENT S'APPLIQUER QUE SUR LES MACHINE NT ET JAMAIS SUR DES CLIENTS WINDOWS 95-98.

DE MEME LES STRATEGIES SYSTEMES CREES SOUS L'EDITEUR DE STRATEGIE WINDOWS NE PEUVENT S'APPLIQUER QUE SUR LES MACHINE WINDOWS ET JAMAIS SUR DES CLIENTS NT.

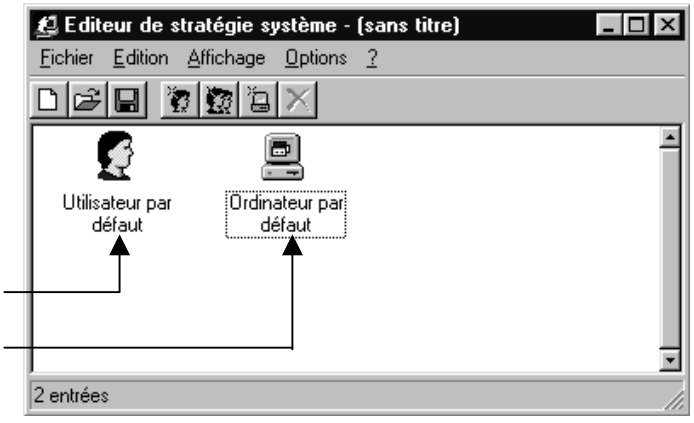
SI ON A UN PARK MIXTE IL FAUT SE CREER 2 FICHIERS DE STRATEGIES DISTINCTS A PARTIR DE L'EDITEUR SPECIFIQUE A CHAQUE ENVIRONNEMENT

par le menu :
Fichier / Nouveau

On cré un fichier de stratégie comprenant 2 entrées:

l'**Utilisateur par défaut**

ou l'**Ordinateur par défaut**



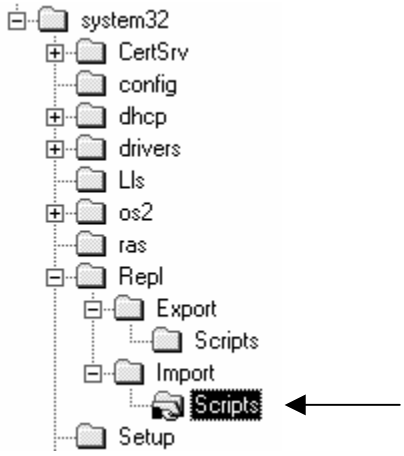
Il faudra bien sûr enregistrer ce fichier avec un nom adéquat ou temporaire classiquement, via le menu **fichier / enregistrer sous**...

STRATÉGIE SOUS WINDOWS NT4.0

Nom et emplacement :

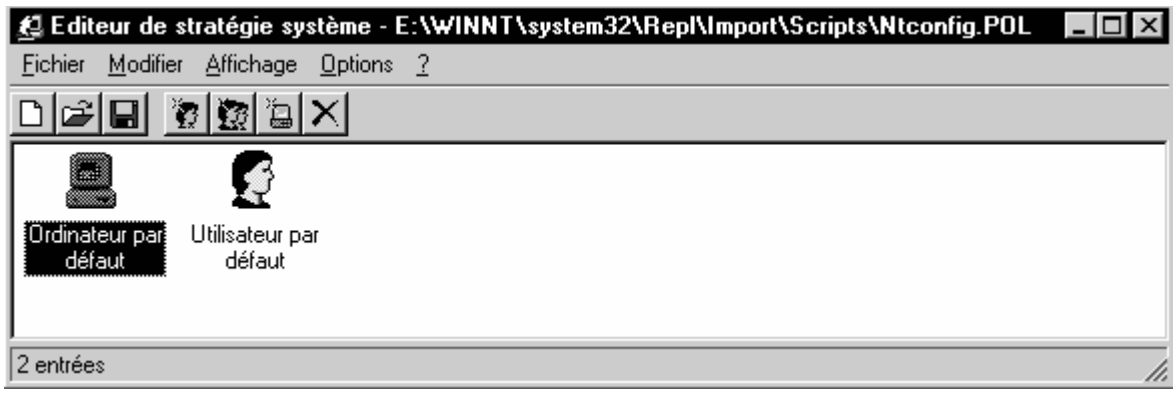
On l'a vu, le fichier de stratégie doit se nommer obligatoirement **Ntconfig.pol** et être sauvegardé dans le dossier partagé du serveur NT CPD nommé **Netlogon**

Le dossier qui apparaît pour les clients sous le nom **NETLOGON** est en fait un dossier situé dans le dossier principal dans lequel windows NT est installé



Winnt\system32\Repl\Import\Scripts

POLEDIT permet de se créer autant de fichier de stratégie que l'on souhaite, mais seul le fichier nommé **Ntconfig.pol** sera chargé et pris en compte par les clients NT

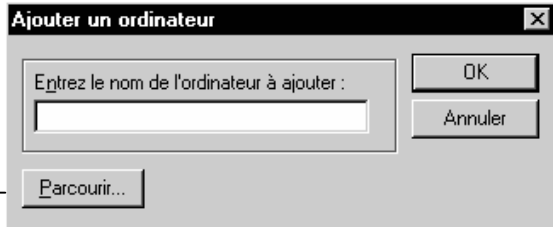


Stratégie d'Ordinateur:

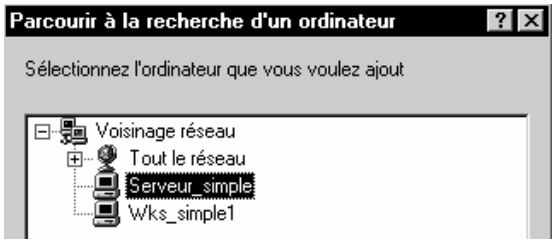
Les stratégies d'ordinateurs s'appliquent à tous les ordinateurs du domaine, et si l'on veut gérer différemment une machine particulière, il faudra inclure "l'exception "dans la stratégie système

pour gérer un poste différemment il faut dans le menu

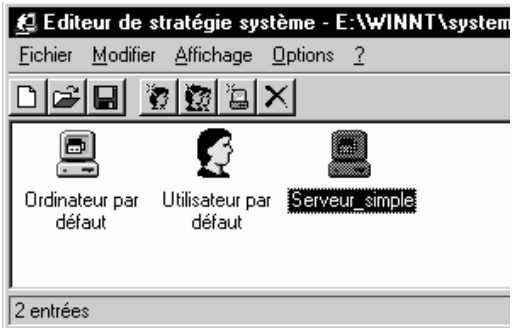
Modifier / Ajouter un ordinateur



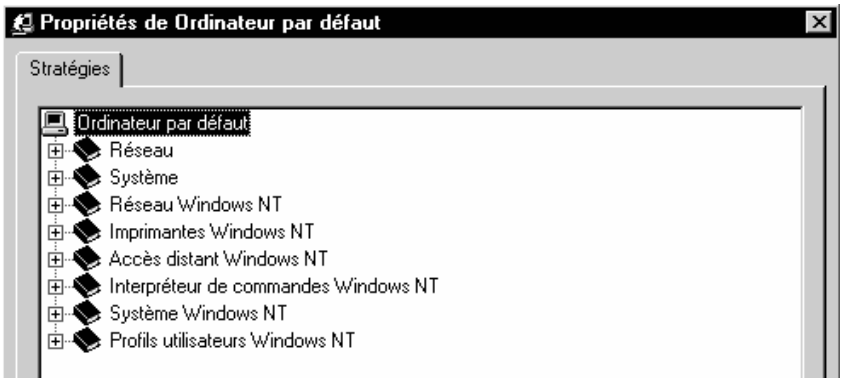
rentrer le nom de la machine à traiter différemment



de manière à visualiser le cas particulier dans l'éditeur de stratégie :



Les stratégies possible apparaissent alors listées:



3 valeurs peuvent être prises par les cases à cocher de l'éditeur de stratégies :

cochée : la stratégie est implémentée

grise : la clé de registre n'est pas modifiée

blanche : la statégie n'est pas implémentée

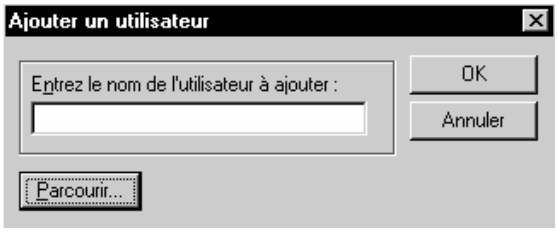
Stratégie d'Utilisateur:

Les stratégies d'Utilisateurs s'appliquent à tous les Utilisateurs du domaine, et si l'on veut gérer différemment un utilisateur

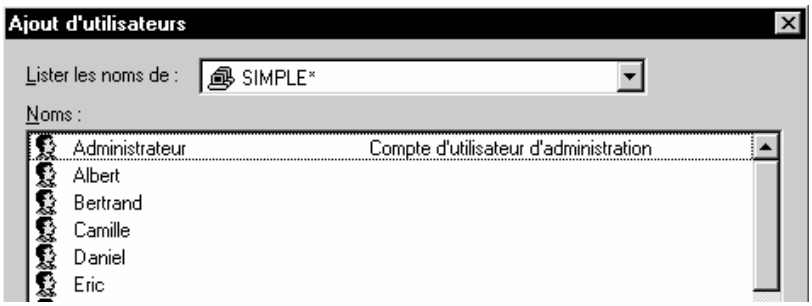
particulier ou un groupe, il faudra inclure "l'exception "dans la stratégie système

pour gérer un utilisateur différemment il faut dans le menu

Modifier / Ajouter un utilisateur

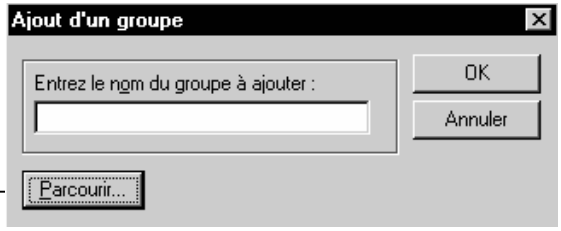


rentrer le nom de l'utilisateur à traiter différemment

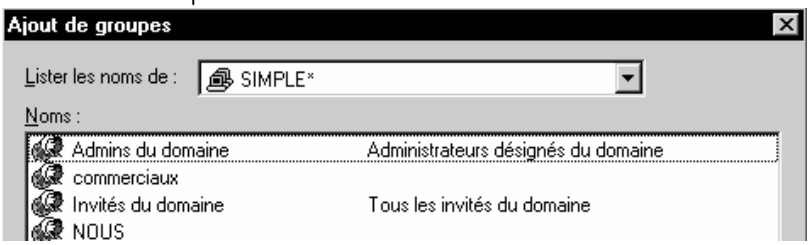


pour gérer un groupe différemment il faut dans le menu

Modifier / Ajouter un groupe



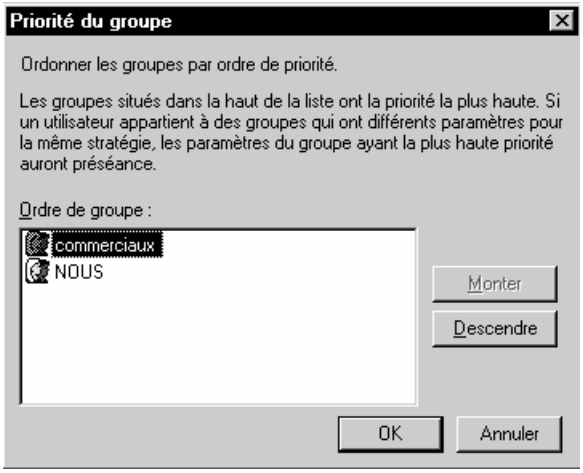
rentrer le nom du groupe à traiter différemment



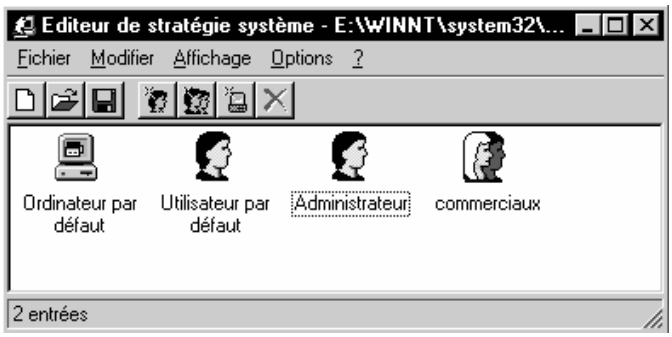
Evidemment un utilisateur pouvant faire partie de plusieurs groupes, on peut définir le groupe dont l'appartenance sera capitale pour décider de la stratégie à utiliser.

En se positionnant sur un groupe dans l'éditeur de stratégie et en demandant le menu **Option / Priorité du groupe**

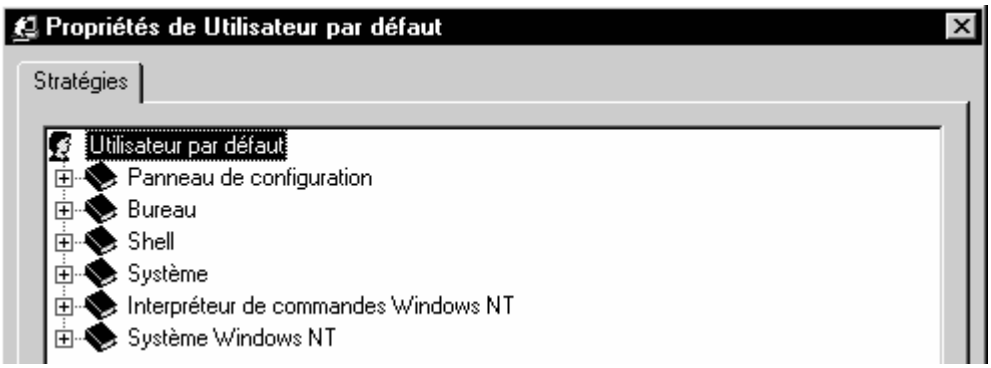
.



On visualise ainsi les cas particuliers dans l'éditeur de stratégie :



Les stratégies possible apparaissent alors listées:



3 valeurs peuvent être prises par les cases à cocher de l'éditeur de stratégies :

☑	cochée :	la stratégie est implémentée
▩	grise :	la clé de registre n'est pas modifiée
☐	blanche :	la statégie n'est pas implémentée

Logique de gestion des stratégies d'Utilisateur :

Lorsque l'utilisateur ouvre une session sur une machine NT :

- le profil éventuel est chargé, puis Windows NT cherche le fichier Ntconfig.pol sur le CPD qui a authentifié l'ouverture de session
- si une stratégie **spécifique à l'utilisateur** a été définie, celle-ci est fusionnée dans la base de registre HKEY_CURRENT_USER, elle à la **priorité sur toutes les autres ! (prendre l'habitude d'en définir une pour l'admin...)**
- si **aucune stratégie d'utilisateur n'a été définie**, mais qu'il y a un stratégie de groupe, on utilise une combinaison de toutes les stratégie de groupe, et si il y a certains conflits sur une stratégie, on applique celle du groupe ayant la plus haute priorité auquel l'utilisateur appartient pour la fusionner dans la base de registre HKEY_CURRENT_USER
- si aucune stratégie spécifique n'est définie, la stratégie de l'utilisateur par défaut est fusionnée dans la base de registre HKEY_CURRENT_USER

Logique de gestion des stratégies d'Ordinateur :

Lorsque l'utilisateur ouvre une session sur une machine NT :

- le profil éventuel est chargé, puis Windows NT cherche le fichier Ntconfig.pol sur le CPD qui a authentifié l'ouverture de session
- si une stratégie spécifique à l'Ordinateur a été définie, celle-ci est fusionnée dans la base de registre HKEY_LOCAL_MACHINE
- si aucune stratégie d'Ordinateur particulière n'a été définie, on utilise la stratégie de l'Ordinatuer par défaut qui est fusionnée dans la base de registre HKEY_LOCAL_MACHINE

Remarques sur les stratégies :

les stratégies s'ajoutent aux profils, et ont des objectifs de restrictions d'utilisation de la machine pouvant être souvent interprétées comme des disfonctionnement du poste de la part de l'utilisateur

Il peut être bon lors de l'utilisation de stratégies d'informer systématiquement l'utilisateur lors de l'ouverture de la session que des stratégies sont en œuvres...Cependant il faut prévoir un message générique, car la bannière fait partie des stratégies d'ordinateur, donc à moins de prévoir machine par machine qui va ouvrir une session, la personnalisation du message devient difficile...

Attention à ne pas inclure l'administrateur dans un groupe pour lequel une stratégie restrictive aurait été définie, celui-ci en bénéficierais automatiquement... **IL VAUT MIEUX DONC SE CREER UNE STRATEGIE SPECIFIANT TOUS LES DROITS POUR L'ADMINISTRATEUR (TOUTES LES RESTRICTIONS DEVALIDEES) , DE MANIERE A EVITER CETTE ERREUR**

De même faire très attention à ne pas se tromper sur le serveur entre **stratégie locale** et sur **domaine**, car le serveur deviendrait vite inaccessible ! (la stratégie locale modifiant la base de registre locale, donc celle du CPD...) On peut améliorer la sécurité en installant l'éditeur de stratégie sur une autre machine NT et en copiant ensuite le fichier **Ntconfig.pol** dans le dossier **Netlogon** du serveur, ainsi en cas de "plantage" on ne se trouve pas sur le serveur !

Pour annuler une stratégie il ne suffit pas de griser forcément la case correspondante, en effet cela signifie alors que l'on ne veut pas modifier la clé correspondante de la base de registre, et si cette clé avait été modifié précédemment , on ne rétablie pas la situation...

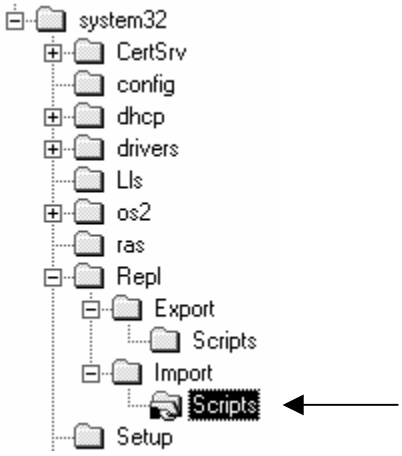
On crée alors facilement une situation confuse, dans laquelle il faut désactiver la clé de cette stratégie, ouvrir une session pour valider cette modification sur chaque client, refermer la session sur chaque client puis revenir dans le fichier de stratégie pour remettre la clé en grisé...

STRATÉGIE SOUS WINDOWS 95-98

Nom et emplacement :

On l'a vu, le fichier de stratégie doit se nommer obligatoirement **Config.pol** et être sauvegardé dans le dossier partagé du serveur NT CPD nommé **Netlogon**

Le dossier qui apparaît pour les clients sous le nom **NETLOGON** est en fait un dossier situé dans le dossier principal dans lequel windows NT est installé



Winnt\system32\Repl\Import\Scripts

POLEDIT permet de se créer autant de fichier de stratégie que l'on souhaite, mais seul le fichier nommé **Config.pol** sera chargé et pris en compte par les clients windows.

Comme ce fichier doit être généré sur une machine Windows, le problème se pose de récupérer ce fichier sur le serveur... En effet les droit en accès au dossier **NETLOGON** sont en **lecture seule**, même pour l'Administrateur... Il faudra alors ouvrir une session sur le serveur et "aller chercher" le fichier sur la machine windows sur lequel il aura été fabriqué !

Stratégie d'Ordinateur:

C'est exactement le même principe que sous NT, aux possibilités près

Stratégie d'Utilisateur:

C'est exactement le même principe que sous NT, aux possibilités près

ANNEXE : STRATÉGIES WIN 98

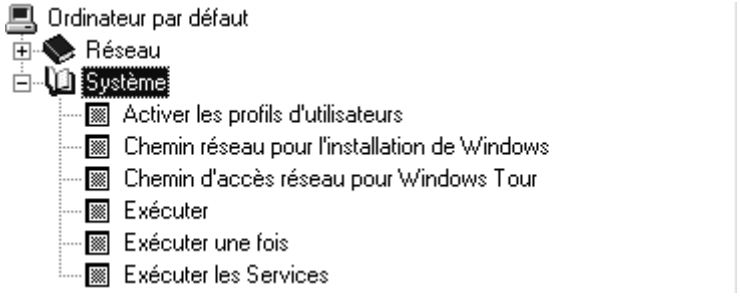
petit descriptif sommaire des stratégies disponibles sous windows 98

Stratégies d'Ordinateur Windows 98 :

L'éditeur de stratégie windows 98 présente au niveau **ordinateur** :

Réseau

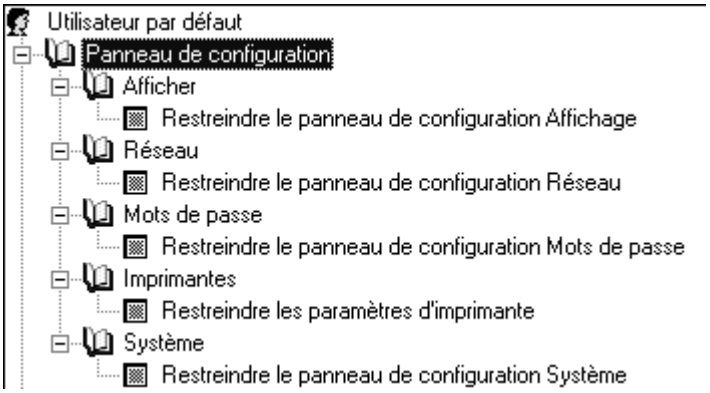
Système



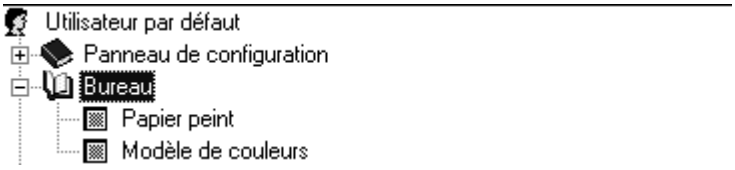
Stratégies d'Utilisateur Windows 98 :

L'éditeur de stratégie windows 98 présente au niveau **utilisateur** :

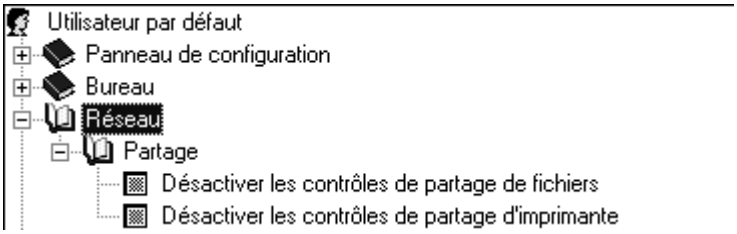
Panneau



Bureau

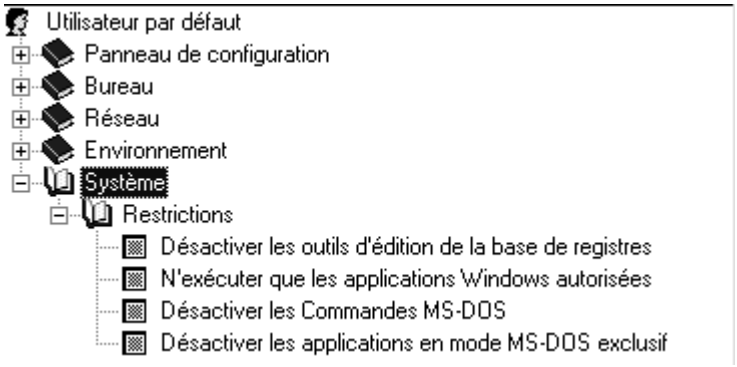


Réseau



Environnement

Système


Utilisateur par défaut
Panneau de configuration
Bureau
Réseau
Environnement
Système
Restrictions
Désactiver les outils d'édition de la base de registres
N'exécuter que les applications Windows autorisées
Désactiver les Commandes MS-DOS
Désactiver les applications en mode MS-DOS exclusif

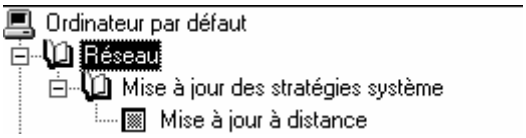
ANNEXE : STRATEGIES NT 4.0

petit descriptif sommaire des stratégies disponibles sous windows NT 4.0

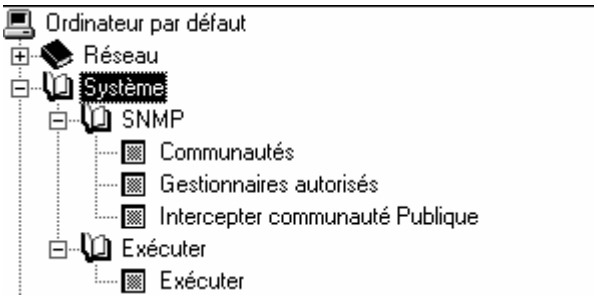
Stratégies d'Ordinateur Windows NT :

L'éditeur de stratégie windows NT présente au niveau **ordinateur** :

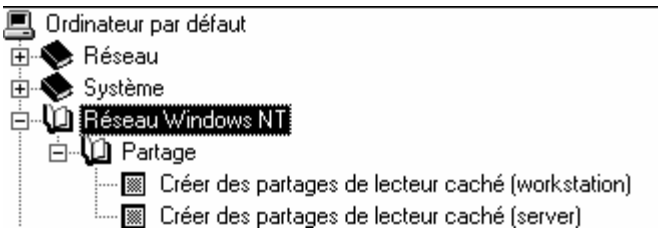
Réseau



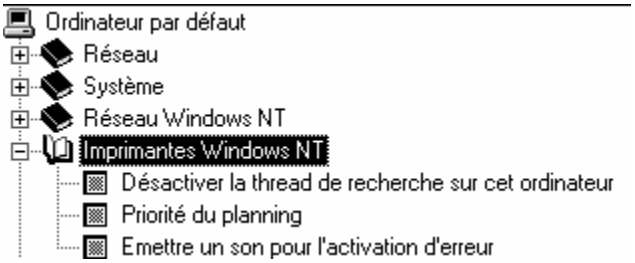
Système



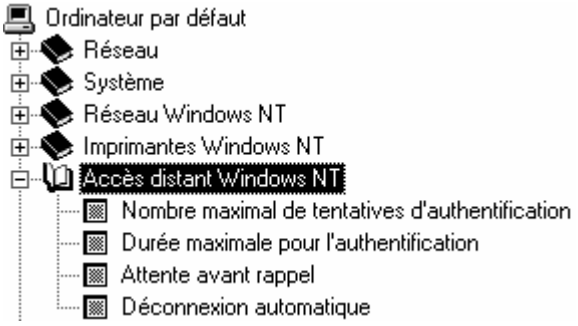
Réseau NT



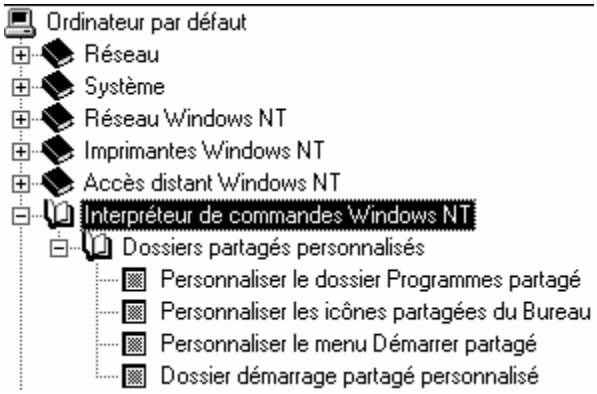
Imprim…



Accès



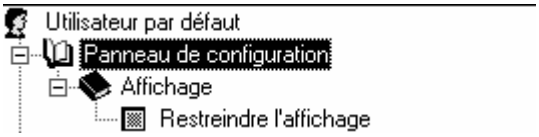
Commande



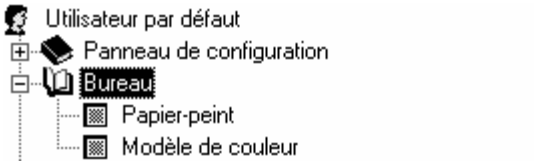
Stratégies d'Utilisateur Windows NT :

L'éditeur de stratégie windows NT présente au niveau **Utilisateur** :

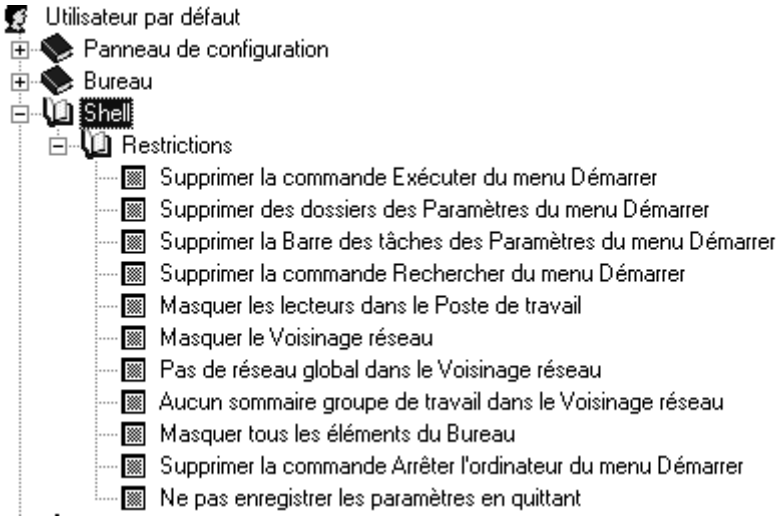
Panneau



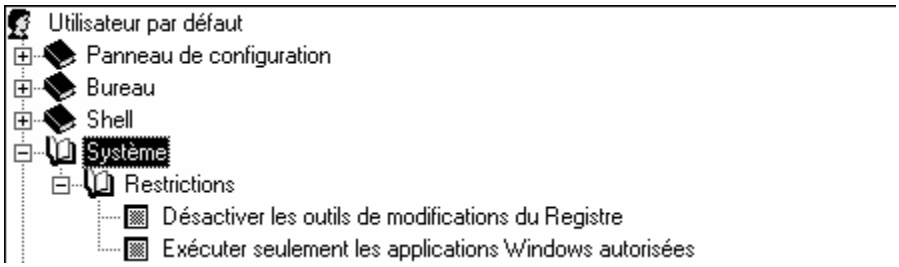
Bureau



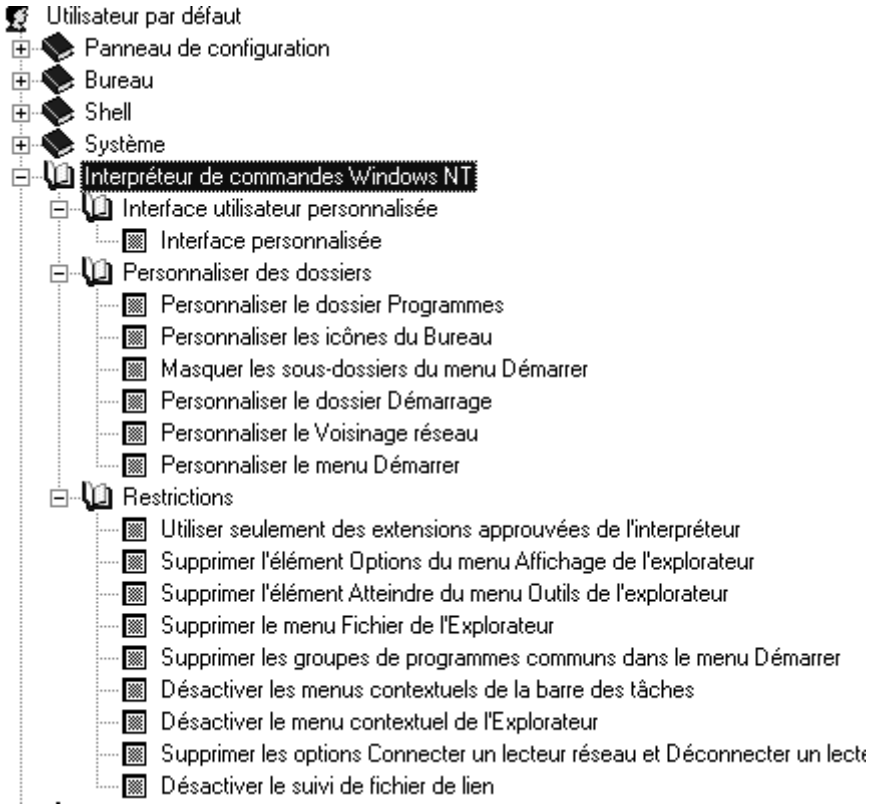
Shell



Système



Commande



Système NT