

Stratégies Windows – sys 26 – cours -

Stratégies Windows XP et de Domaine

Michel Cabaré - Ver 1.0 - Oct 2006-

http://<u>WWW.CABARE.NET</u>©

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	5
TYPES DE STRATEGIE :	5
Stratégies sur un ordinateur local ( cf microsoft GPO hors AD):	5
Stratégies de Groupe GPO (cf microsoft GPO dans AD):	5
CONFIGURER DES STRATEGIES LOCALEMENT :	6
CONTENU DES PARAMETRES LOCAUX DE SECURITE :	7
STRATEGIES LOCALES - AUDIT	10
AUDIT EVENEMENT - RESSOURCE:	
AUDIT SUR EVENEMENT:	11
LIRE LE JOURNAL DE SECURITE:	
Installer un Audit sur des ressources:	
Audit sur un dossier	
Audit sur une imprimante	
STRATEGIES DE DOMAINE	14
STRATEGIES DE DOMAINE :	14
PROPAGATION STRATEGIES DE DOMAINE :	
STRATECIES CONTROL FUR DE DOMAINE	17
STRATEGIES CONTROLEUR DE DOMAINE ·	17
STRATEOIES DE CONTROLEOR DE D'OMAINE	
MODELE DE STRATEGIES.	
LES MODELES DE STRATEGIE DE SECURITE:	
CREATION D'UN MODELE:	
CREATION D'UNE BASE LOCALE DE SECURITE:	
VERIFICATION MODELE - POSTE:	
APPLICATION DU MODELE SUR LE POSTE	
MODIFICATION DU MODELE	
MODELES PRE DEFINIS	
CLES DE REGISTRE D'UNE STRATEGIE	23
KESUME	24
GPO D'UNITE ORGANISATIONELLE	
TYPES ET NIVEAUX DE STRATEGIE :	25
NIVEAU DE MODIFICATION DANS LA BASE DE REGISTRE	
STRATEGIES PREDEFINIES EXISTANTES :	
DEFINIR UNE STRATEGIE DE GROUPE SUR UNE U.O :	
HIERARCHIE DES STRATEGIES	
ORDRE FINAL D'APPLICATION DES STRATEGIES :	
L'UTILITAIRE EN LIGNE SECEDIT (2000)	
L'UTILITAIRE EN LIGNE GPUPDATE (XP - 2003)	
LIAISON - HERITAGE – BLOCAGE - FORCER DES GPO	
LIAISON DE GPO :	
GESTION DES LIAISONS DE GPO:	
HERITAGE ET BLOCAGE D'HERITAGE:	
INTERDIRE LE BLOCAGE D'HERITAGE :	35
L'UTILITAIRE GPRESULT.EXE DU KIT DE RESSOURCE	
GESTION STRATEGIES 2003 - RSOP	
CONSOLE GESTION STRATEGIE DE GROUPE ET RSOP SUR XP ET SERVEUR 2003	
AUTORISATION AVEC XP-SP2	
UTILISATION DE RSOP SP1 POUR 2003	
Sur un ordinateur (par exemple)	
CONSOLE GPMC ET GESTION DES STRATEGIES DE GROUPES	



P

GPO - MODELES D'ADMINISTRATION	
Les Modeles presents	40
METHODOLOGIE DE MISE EN OEUVRE	41
CDO DEDIDECTION DOSSIEDS	12
CONFIGURATION LITH RATEUR	
REDIDICED MES DOCUMENTS	
REDIRIGER BUREAU APPLICATION DATA DEMARRER	43
GPO - SCRIPTS	
SCRIPTS DE DEMARRAGE – ARRET – FIN DE SESSION :	
SCRIPTS DE FIN DE SESSION :	
Copier le script dans la GPO	
Utiliser le script dans la GPO	
TEST ET VISUALISATION :	
GPO - INSTALLATION DE LOGICIELS	48
Les 3 elements Winstaller – GPO - AD	48
WINDOWS INSTALLER ET FICHIERS MSI	48
PROCEDURE D'INSTALLATION ET DE MAINTENANCE LOGICIELS	49
CREATION DU POINT D'INSTALLATION DE LOGICIEL	49
ATTRIBUTION - PUBLICATION DE LOGICIEL	
STRATEGIE DE DEPLOIEMENT DE LOGICIEL	
STRATEGIE DE DESINSTALLATION DE LOGICIEL	51
GPEDIT	52
STRATEGIE LOCALE / RESEAU:	52
Editeur de strategie locale :	
STRATEGIES SYSTEME CLIENTS NON-2000+ "POLEDIT"	53
OUE SONT LES STRATEGIES SYSTEME .	53
Installer l'editeur de strategie :	
Sur un serveur Windows NT :	
Sur un client Workstation NT :	
Sur un poste Windows 95-98 :	
STRATECIE LOCALE OU MODELE	56
STRATEGIE LOCALE OU "MODELEE	56
FICHIER DE STRATEGIE OU "MODE STRATEGIE":	
STRATEGIE SOUS WINDOWS NT4.0	
NOM ET EMPLACEMENT :	
STRATEGIE D'ORDINATEUR:	60
STRATEGIE D'UTILISATEUR:	60
LOGIQUE DE GESTION DES STRATEGIES D'UTILISATEUR :	
PEMADOLIES SUD LES STRATEGIES ·	
KEMARQUES SUR LES STRATEOILS	
STRATÉGIE SOUS WINDOWS 95-98	64
NOM ET EMPLACEMENT :	64
STRATEGIE D'ORDINATEUR:	
STRATEGIE D'UTILISATEUR:	64
ANNEXE : STRATÉGIES WIN 98	65
Strategies d'Ordinateur Windows 98 :	65
STRATEGIES D'UTILISATEUR WINDOWS 98 :	66
ANNEXE : STRATEGIES NT 4.0	68
STRATEGIES D'ORDINATEUR WINDOWS NT :	
STRATEGIES D'UTILISATEUR WINDOWS NT :	



E 

# **STRATEGIES LOCALES 2000-XP**

#### Types de stratégie :

Arbre

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

a	tion / Stratégies de sé	ecurités locales,
3	Ê	
	Nom	Description
1	Stratégies de comptes	Stratégies de mot de passe et de verrouillage de c…
	Stratégies locales	Stratégies des options d'audit, de droits d'utilisateu
	Stratégies de clé publique	
	🕄 Stratégies de sécurité IP sur	Administration de la sécurité du protocole Internet

Ces stratégies locales sont disponibles sur

Paramètres de sécurité locaux

Paramètres de sécurité P-00 Stratégies de comptes P-00 Stratégies locales P-00 Stratégies de clé publique

| Action Affichage || ← → | 🛅 💽 | 🗙 🞚

🗄 🜏 Stratégies de sécurité IP sur Ordinateur local

- 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:

Arbre

🖥 Paramètres de sécurité locaux

Stratégie de mot de passe
Stratégie de verrouillage du compte

Paramètres de sécurité É- 🖻 Stratégies de comptes

Stratégies locales

Action Affichage 🛛 🗢 🔿 🛍 🔃 🗙 🗔

• Stratégies de compte

(~gestion utilisateur)

• Stratégies locales

(~qui peut ouvrir session locale)

• Stratégies de clé publique

(agent de récupération)

#### • Stratégies IPSEC

tion)

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

#### Interface Windows 2000

(cryptage IP)

🖥 Paramètres de sécurité locaux			_ 🗆 🗙
$   \underline{A}ction  Affichage    \Leftarrow \rightarrow   \textcircled{1} \boxed{\texttt{II}}   \times \boxed{\texttt{II}}   $	Ê		
Arbre	Stratégie 🔺	Paramètre local	Paramètre en cours
Paramètres de sécurité	Conserver l'historique des mots de	0 mots de passe mé	0 mots de passe mé
🖆 👜 Stratégies de comptes	Durée de vie maximale du mot de	42 Jours	42 Jours
	Burée de vie minimale du mot de p	0 Jours	0 Jours
🛄 Stratégie de verrouillage du compte	Les mots de passe doivent respect	Désactivé	Désactivé
🖻 🕮 Stratégies locales	Blongueur minimale du mot de passe	0 Caractères	0 Caractères
- 🕮 Stratégie d'audit	Stocker le mot de passe en utilisan	Désactivé	Désactivé
Attribution des droits utilisateur			
Options de sécurité			
🛱 🖳 🛄 Stratégies de clé publique			
Agents de récupération de données cryptées			
Stratégies de sécurité IP sur Ordinateur local			

#### Interface Windows XP

Paramètres de sécurité locaux		
Fichier Action Affichage ? ← → 1 🗈 📴 😰	Purch faster (	Duran Shar da a faran 1
<ul> <li>Paralites de securite</li> <li>Stratégies de comptes</li> <li>Stratégie de mot de passe</li> <li>Stratégie de verrouillage du compte</li> <li>Stratégie locales</li> <li>Stratégie d'audit</li> <li>Attribution des droits utilisateur</li> <li>Options de sécurité</li> <li>Stratégies de clé publique</li> <li>Système de fichiers EFS (Encrypting File System)</li> <li>Stratégies de sécurité IP sur Ordinateur local</li> </ul>	Strategie // Conserver l'historique des mots de p Durée de vie maximale du mot de passe Durée de vie minimale du mot de passe Le mot de passe doit respecter des Longueur minimale du mot de passe Stocker le mot de passe en utilisant l	Parametre de securite O mots de passe mémorisés 42 Jours O Jours Désactivé O Caractères Désactivé





Stratégies Windows XP - Domaine Cabaré Michel

Cabaré Michel Page 6 www.cabare.net©

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

Paramètres de sécurité locaux	
$ $ Action Affichage $ $ $\Leftrightarrow \Rightarrow  $ $\textcircled{E}$ $\boxed{\blacksquare}   \times \textcircled{E}  $	Ê
Arbre	Stratégie 🛆
🔁 Paramètres de sécurité	Durée de verrouillage des comptes
🛱 🕮 Stratégies de comptes	BigRéinitialiser le compteur de verrouillages du compte après
- 🖼 Stratégie de mot de passe	Seuil de verrouillage du compte
Strategie de verrouillage du compte	
	Descendante de stantistica de stantistica de la secondational de la secondational de la secondation de
	Seuil de verrouillage du compte
Sur lequel un double-clic amène	Paramètres de la stratégie actuelle
	Le compte ne sera pas verrouillé :
	Paramètre de stratégie locale
	Le compte ne sera pas verrouillé :
	tentatives d'ouvertures de session non valides
	Ci des paramètres de stratégie cont définis au siyaay du deraine ils
	remplacent les paramètres de stratégie locale.
	templaterit ite parametres as strategie locale.

### Contenu des Paramètres locaux de sécurité :

#### Stratégies de comptes

COLOR STRAT	égies de comptes tratégie de mot de passe tratégie de verrouillage du compte Stratégies de mot de passe					
	Stratégie 🛆					
	B Conserver l'historique des mots de passe					
	BDurée de vie maximale du mot de passe					
	B Durée de vie minimale du mot de passe					
<b>→</b>	避Les mots de passe doivent respecter des exigences de complexité					
	题Longueur minimale du mot de passe					
	🕮 Stocker le mot de passe en utilisant le cryptage réversible pour tous les utilisateurs du domaine					
Stratégies de verrouillage du compte						
	Stratégie 🛆					
<b></b>	Burée de verrouillage des comptes					
	🕮 Réinitialiser le compteur de verrouillages du compte après					
	យឿSeuil de verrouillage du compte					

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



#### Stratégies locales 💼 Stratégies locales 📴 Stratégie d'audit Attribution des droits utilisateur 🔟 Options de sécurité Stratégie d'audit Stratégie BAuditer la gestion des comptes 🕮 Auditer l'accès au service d'annuaire Auditer l'accès aux objets 🕮 Auditer le suivi des processus Auditer les événements de connexion B Auditer les événements de connexion aux comptes Auditer les événements système Relations de stratégie Real Auditer l'utilisation des privilèges Attribution des droits utilisateurs Stratégie 🕮 Accéder à cet ordinateur depuis le réseau 🕮 Agir en tant que partie du système d'exploitation 避 Ajouter des stations de travail au domaine 🕮 Arrêter le système Augmenter la priorité de planification Augmenter les quotas 🕮 Autoriser que l'on fasse confiance aux comptes ordinateur et utilisateur pour la délégation 🕮 Charger et décharger des pilotes de périphériques Créer des objets partagés permanents Créer un fichier d'échange 🛯 🕮 Créer un objet-jeton BDéboguer des programmes B Forcer l'arrêt à partir d'un système distant Générer des audits de sécurité BGérer le journal d'audit et de sécurité Modifier les valeurs d'env. de microprogrammation Modifier l'heure système BOptimiser les performances système Coptimiser un processus unique Outrepasser le contrôle de défilement BOUVRING OUVRING SESSION ON LAND QUE SERVICE 🕮 Ouvrir une session en tant que tâche Ouvrir une session localement Options de sécurité Stratégie 🕮 Arrêter immédiatement le système s'il n'est pas possible de se connecter aux audits de sécurité BB Auditer l'accès des objets système globaux 📖 Auditer l'utilisation des privilèges de sauvegarde et de restauration Canal sécurisé : crypter numériquement les données des canaux sécurisés (lorsque cela est pos 🕮 Canal sécurisé : crypter ou signer numériquement les données des canaux sécurisés (toujours) 🕮 Canal sécurisé : nécessite une clé de session forte (Windows 2000 ou ultérieur) 📆 Canal sécurisé : signer numériquement les données des canaux sécurisés (lorsque cela est possi 🕮 Comportement d'installation d'un fichier non-pilote non signé Comportement d'installation d'un pilote non signé 🕮 Comportement lorsque la carte à puce est retirée 🕮 Console de récupération : autoriser la copie de disquettes et l'accès à tous les lecteurs et dossie Console de récupération : autoriser l'ouverture de session d'administration automatique 📖 Contenu du message pour les utilisateurs essayant de se connecter 题Créer un fichier d'échange de mémoire virtuelle lors de la fermeture du système BDésactiver la combinaison de touches Ctrl+Alt+Suppr. lors de l'ouverture de session BDurée d'inactivité avant la déconnexion d'une session 题Empêche la maintenance par le système du mot de passe du compte ordinateur Empêcher les utilisateurs d'installer des pilotes d'imprimante 🕮 Envoyer un mot de passe non crypté pour se connecter aux serveurs SMB tierce partie 📲 Fermer automatiquement la session des utilisateurs à l'expiration du délai de la durée de session Ne pas afficher le dernier nom d'utilisateur dans l'écran d'ouverture de session BBNe permettre l'accès au CD-ROM qu'aux utilisateurs connectés localement 🕮 Ne permettre l'accès aux disquettes qu'aux utilisateurs connectés localement. 🕮 Niveau d'authentification Lan Manager 📖 Nombre d'ouvertures de session précédentes dans le cache (au cas ou le contrôleur de domaine



#### Stratégies de clé publique

🗟 Stratégies de clé publique

Agents de récupération de données cryptées

#### Stratégies de sécurité IP

畏 Stratégies de sécurité IP sur Ordinateur local



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:

Г

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 II faut développer la clé

#### Stratégies locales / Stratégies d'audit

Arbre       Stratégie       Paramètre local       Paramètre en cours         Paramètres de sécurité       Bill Auditer la gestion des comptes       Paramètre local       Paramètre en cours         Stratégies de comptes       Bill Auditer la gestion des comptes       Pas d'audit       Pas d'audit         Stratégies locales       Bill Auditer l'accès aux objets       Pas d'audit       Pas d'audit         Stratégies de comptes       Bill Auditer l'accès aux objets       Pas d'audit       Pas d'audit         Stratégies de faudit       Bill Auditer l'accès aux objets       Pas d'audit       Pas d'audit         Attribution des droits utilisateur       Bill Auditer les événements de connex       Pas d'audit       Pas d'audit         Options de sécurité       Bill Auditer les événements de connex       Pas d'audit       Pas d'audit         Stratégies de clé publique       Bill Auditer les événements de connex       Pas d'audit       Pas d'audit         Stratégies de sécurité IP sur Ordinateur local       Bill Auditer les modifications de stratégie       Pas d'audit       Pas d'audit         Auditer l'utilisation des privilèges       Pas d'audit       Pas d'audit       Pas d'audit	Paramètres de sécurité locaux	3 B			>
Image: Autobulon des droits duits d	Arbre	Stratégie A Stratégie A Auditer la gestion des comptes Auditer l'accès au service d'annuaire Auditer l'accès aux objets Auditer le suivi des processus Manditer le suivi des processus	Paramètre local Pas d'audit Pas d'audit Pas d'audit Pas d'audit Das d'audit	Paramètre en cours Pas d'audit Pas d'audit Pas d'audit Pas d'audit Pas d'audit	
	Actributor des droits duisateur     Actributor des droits duisateur     Actributor des écurité     ⊡    Stratégies de sécurité IP sur Ordinateur local	Moulter les événements de connex           副 Auditer les événements de connex           副 Auditer les événements système           副 Auditer les modifications de stratégie           副 Auditer les modifications de stratégie           副 Auditer l'utilisation des privilèges	Pas d'audit Pas d'audit Pas d'audit Pas d'audit	Pas d'audit Pas d'audit Pas d'audit Pas d'audit Pas d'audit	-

par exemple sur <b>connexion</b>	1 The second sec
et en demandant d'auditer les réussites et/ou les échec	Paramètre de stratégie de sécurité locale       ? ×         Auditer les événements de connexion       Paramètres de la stratégie en cours :         Paramètre de stratégie en cours :       Paramètre de stratégie locale         Auditer ces essais :       •         Muditer ces essais :       •         Essais ayant réussi       •         Essais ayant échoué       Si des paramètres de stratégie sont définis au niveau du domaine, ils remplacent les paramètres de stratégie locale.         OK       Annuler

L'audit étant posé , mais non enregistré \_\_\_\_\_

Auditer les événements de connexion Opération réussie, Échec Pas d'audit

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

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

Auditer les événements de connexion Opération réussie, Échec Opération réussie, Échec





#### Lire le journal de sécurité:

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

Action Affichage	Action Affichage $4 \Leftrightarrow \Rightarrow 1 \boxdot 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 $							
Arbre	Journal sécurité 7 (	événement(s)						
🗊 Observateur d'évéi	Туре	Date	Heure	Source	Catégorie	Évén	Utilisateur	Ordinateur
Journal applical	Audit des succès	24/05/2002	08:56:10	Security	Ouverture/Fermeture de session	528	Administrateur	CLIENT2KP8
🗊 Journal sécurite	🔒 Audit des échecs	24/05/2002	08:56:06	Security	Ouverture/Fermeture de session	529	SYSTEM	CLIENT2KP8
🄤 Journal systèm	Audit des succès	24/05/2002	08:56:03	Security	Ouverture/Fermeture de session	538	bob	CLIENT2KP8
	audit des échecs	24/05/2002	08:56:01	Security	Ouverture/Fermeture de session	529	SYSTEM	CLIENT2KP8
	Audit des succès	24/05/2002	08:55:57	Security	Ouverture/Fermeture de session	538	Administrateur	CLIENT2KP8
	Audit des succès	24/05/2002	08:54:55	Security	Ouverture/Fermeture de session	528	Administrateur	CLIENT2KP8
	Audit des succès	24/05/2002	08:54:07	Security	Ouverture/Fermeture de session	528	bob	CLIENT2KP8

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

Audit succès	Audit Echec
Propriétés de Événement	Propriétés de Événement         ? ×
Événement	Événement
Date :       24/05/2002       Source :       Security         Heure :       08:56       Catégorie :       Ouverture/Fermeture de         Type :       Audit des       ID événement :       528         Utilisateur :       CLIENT2KP8VAdministrateur       Image: CLIENT2KP8	Date :       24/05/2002       Source :       Security         Heure :       08:56       Catégorie :       Ouverture/Fermeture de         Type :       Audit des       ID événement :       529         Utilisateur :       AUTORITE NTASYSTEM       Image: CLIENT2KP8
Description : Sessions acceptées : Nom de l'utilisateur : Administrateur Domaine : CLIENT2KP8 N <sup>g</sup> de la session : (0x0,0x3A1C3) Type de session : 2 Processus d'ouverture de session : User32 Package d'authentification : Negotiate	Description :

#### 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...ll 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

ll 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...)

Paramètre	s du contrôle d'accès pour data			? ×
Autorisatio	ns Audit Propriétaire			
Entrées	d'audit :			
Туре	Nom Accè	s Ap	opliquer à	
<b>R</b> Éch	ec pierre (pierre@domaine1.edu) Supp	rimer Ce	e dossier, les sous	s-dossiers
ll faut corresp	ensuite ajouter <u>pou</u> oondant à	<u>r qui</u> e	et <u>quel t</u>	<u>type d'Audit</u> l'on veut
	Audit de l'entrée pour data Objet		? ×	
	Nom : pierre (pierre@domaine1.edu		Modifier	
	Appliquer à : Ce dossier, les sous-dos	siers et les fichie	ers 💌	
	Acces : Parcourir le dossier/Exécuter le fichi Liste du dossier / Lecture de donné Attributs de lecture Lire les attributs étendus Création de fichiers / Écriture de don Création de dossiers / Ajout de donn Attributs d'écriture			Les type d'audit en tentative d'accès peuvent être obtenu par <b>Parcourir le dossier</b>
	Écriture d'attributs étendus Suppression de sous-dossiers et de Supprimer Autorisations de lecture Modifier les autorisations Appliquer ces entrées d'audit aux o et/ou aux conteneurs à l'intérieur d conteneur uniquement	iich	Effacer tout	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 :

ll 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

Audit de l'entrée pour HP LaserJe	et 6P	?
Objet		
Nom : Tout le monde		<u>M</u> odifier
Appliquer à : Cette imprimante et le	es documents	•
Accè <u>s</u> :	Réussite	Échec
Imprimer Gestion d'imprimantes Gestion des documents Autorisations de lecture Modifier les autorisations Appropriation		

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 <u>à toutes les machines de notre domaine</u>.

- 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 <u>client 2000 du domaine</u>, voila l'aspect de la **stratégie locale** concernant qui peut mettre à l'heure la machine....

Paramètre	de stratégie de sé	curité locale	<u>?</u> ×
F	Modifier l'heure systè	me	
Attribué à	Param	Local ètre de stratégie	Effectif Paramètre de stratégie
Administ	rateurs		$\checkmark$
Utilisate	urs avec pouvoir		Ø

Sur le <u>client XP du domaine</u>, la stratégie locale ne montre qu'une seule colonne

📴 Paramètres de sécurité 🛛 🔺	Stratégie 🛆	Paramètre de sécurité
🕀 📴 Stratégies de comptes	B Modifier les valeurs d'env. de microprogrammation	Administrateurs
E Stratégies locales	Modifier l'heure système	Administrateurs, Utilisateurs avec pouvoir
Stratégie d'audit	Optimiser les performances système	Administrateurs
Attribution des droits utilisateur	Contimiser un processus unique	Administrateurs. Itilisateurs avec nouvoir

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



📅 Paramètres de sécurité du domaine par défaut Fichier Action Affichage ? ⇔ ⇒ | 🖮 Paramètres Windows Stratégie 🦯 Paramètres de stratégie ۰ 🗐 Scripts (démarrage/arrêt) Interdire l'ouverture de session en tant que .... Non défini Paramètres de sécurité 🕮 Interdire l'ouverture de session par les servi... Non défini 🗄 🛃 Stratégies de comptes 🕮 Interdire l'ouverture d'une session locale Non défini 🖻 🚽 🚮 Stratégies locales 🛍 Modifier les valeurs d'env. de microprogram... Non défini 🗄 🚽 🚮 Stratégie d'audit Modifier l'heure système Non défini 🗄 🖅 🛃 Attribution des droits utilisateur 🛛 🕮 Optimiser les performances système Non défini 🗄 📲 Options de sécurité 20 Optimicor un pr Non défini

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







#### Sur le <u>client 2000 du domaine</u>

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

	Arbre		Stratégie A		Paramètre local		Paramètre en cours
	🗐 Daram	atros do sócuritó	Gérer le journal d'a	udit et de sécurité	Administrateurs		Administrateurs
	i jeraian i i ⊡i i i i i i i i i i i i i i i i i	ratégies de comptes	Modifier les valeurs	s d'env. de micr…	Administrateurs		Administrateurs
	🖻 🛄 St	ratégies locales	Modifier l'heure sys	stème	Utilisateurs avec pouv	oir,Administrateurs	MANUEL\bob
	÷.	Stratégie d'audit	Optimiser les perfo	rmances système	Administrateurs		Administrateurs
	····	SPAttribution des droits utilisateur	Inglopamiser un proce	ssus unique	Utilisateurs avec pouv	oir, Administrateurs	utilisateurs avec po
	avec						
		Paramètre de stratégie de	sécurité locale		?   X		
		Medifier l'hours s	webèren				
			ysteme				
Pas	de		Local	Effectif		Mais ici	on a
changemen	it .	Attribue a Pa	rametre de strategie	Parametre de strati	egie	récupéré	la
localement	, c	MANUEL\bob				stratégie	de
localement		Administrateurs		H		domaine	
						e. e i i i i i i i i i i i i i i i i i i	
	Sur le propa d'une locale	e <u>client XP du de</u> ager, normalemen e icône indiquar ement.	<u>omaine</u> , Lors It la visualisa <sup>:</sup> nt qu'elle v	que la str tion de la /ient du	ratégie de <b>stratégie lo</b> Domaine,	domaine à c <b>ale</b> sera m et no	pu se iarquée on pas
	📴 Param	iètres de sécurité	Stratégie 🛆		Paramètre de sécur	ité	
	_ ⊕ <b>⊡ਉ</b> St	ratégies de comptes ratégies locales	Modifier les valeu	urs d'env. de micr…	. Administrateurs		
		Stratégie d'audit	Modifier l'heure s	système formances système	MANUEL\bob		
		Attribution des droits utilisateur	St Optimiser up pro	cassus uniqua	Administrateure I Iti	li	
	Avec						
		Propriétés de Modifier l'	heure système	1	?   X		
		Paramètro de sécurité locale	1				
		Farametre de securite locale					
		Modifier l'heure sy	stème				
		MAROLLIDOD			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, <u>depuis le client</u> sur lequel on veut effectuer la propagation

Sous Windows 2000 :

Secedit /refreshpolicy machine\_policy



Sous Windows XP

Gpupdate /force

C:\Documents and Settings\Administrateur.SRV1-2003.000>gpupdate /force Actualisation de la stratégie
L'actualisation de la stratégie utilisateur s'est terminée. L'actualisation de la stratégie ordinateur s'est terminée.
Pour vérifier des erreurs dans le traitement de la stratégie, consultez l'Observateur d'événements.

Par exemple

effectivement, dans le journal on peut observer

Propriétés de Événement	:		? ×
Événement			
Date : 16/12/2002 Heure : 21:20 Type : Informations Utilisateur : MZ Ordinateur : CLIENT1R1	Source : Catégorie : ID événement :	SceCli Aucun 1704	<ul> <li>↑</li> <li>↓</li> <li>↓</li> </ul>
Description : La stratégie de sécurité d correctement.	lans les objets Stra	tégie de groupe est appli	quée

(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 :

Paramètre de stratég	gie de sécurité locale	? X	Paramètre	de stratégie de sécurité locale	? X
Ouvrir une	session localement		E	Modifier l'heure système	
Attribué à	Local Paramètre de stratégie	Effectif Paramètre de stratégie	Attribué à	Local Paramètre de stratégie	Effectif Paramètre de stratégie
Opérateurs d'impress Opérateurs de serve	ion 🗌 ur 🔲		Opérate DOMAIN Administ	urs de serveur	
IUSR_SERVEUR DOMAINE1\marie DOMAINE1\IUSR_S			Utilisate	urs avec pouvoir	ä

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

🐂 Paramètres de sécurité du contrôleur de	domaine par défaut	
Eichier Action Affichage ?		
📄 Paramètres Windows 📃	Stratégie 🔺	Paramètres de stratégie
- 🗐 Scripts (démarrage/arrêt)	BModifier les valeurs d'env. de microprogram	Administrateurs
🖻 🖓 Paramètres de sécurité	BB Modifier l'heure système	Administrateurs, MANUEL \marie, Opérateurs de se 🥌
Stratégies de comptes	BOptimiser les performances système	Administrateurs
🖃 🚮 Stratégies locales	BOptimiser un processus unique	Administrateurs
⊡ 🚰 Stratėgie d'audit	🕮 Outrepasser le contrôle de défilement	Tout le monde, Administrateurs, Utilisateurs authe
Attribution des droits utilisateu	Ouvrir une session en tant que service	
Options de securité	BOuvrir une session en tant que tâche	
H · · · · · · · · · · · · · · · · · · ·	Permettre l'ouverture d'une session locale	Administrateurs,MANUEL\marie,Opérateurs de co 🗲



# **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

	x	Nom 🛆	Taille	Туре	Modifié le
🗄 💼 security		policies		Dossier de fichiers	30/05/2002 21:15
Database		🗟 basicdc.inf	16 Ko	Informations de configuration	16/12/1999 02:15
logs		🐻 basicsv.inf	275 Ko	Informations de configuration	16/12/1999 02:15
🗄 📼 templates		🗟 basicwk.inf	252 Ko	Informations de configuration	16/12/1999 02:15
🛄 ShellNew		🗟 compatws.inf	53 Ko	Informations de configuration	16/12/1999 02:15
🛄 Speech		📓 hisecdc.inf	7 Ko	Informations de configuration	16/12/1999 02:15
system		📓 hisecws.inf	18 Ko	Informations de configuration	16/12/1999 02:15
⊡		🗟 ocfiless.inf	765 Ko	Informations de configuration	16/12/1999 02:15
⊡ CatRoot		🐻 ocfilesw.inf	479 Ko	Informations de configuration	16/12/1999 02:15
Com		🐻 securedc.inf	7 Ko	Informations de configuration	16/12/1999 02:15
conrig		🗟 securews.inf	7 Ko	Informations de configuration	16/12/1999 02:15
dlicache		setup security.inf	511 Ko	Informations de configuration	15/10/2001 17:45

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

×	Nom 🛆	Taille	Туре	Modifié le
security     Database	🔊 secedit.sdb	3 080 Ko	Fichier SDB	30/05/2002 21:15

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:

Modèles de sécurité

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

Lien vers une adresse Web Modèles de sécurité	
📰 Modèles de sécurité 🛛 👘 Micr	
	osoft Corporation
Observateur d'événements Micro	osoft Corporation
Service d'indexation Micr	osoft Corporation, I
🖏 Services Micr	osoft Corporation
😰 Services de composants 🛛 🛛 Micr	osoft Corporation
🕵 Stratégie de groupe Micr	osoft Corporation
🕵 Utilisateurs et groupes locaux Micr	osoft Corporation

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





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

Dans les stratégies locales / options de sécurité

Contenu du message pour les utilisateurs essayant de se connecter Non défini

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

Titre du message pour les utilisateurs essayant de se connecter

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



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

Configuration	et	analyse	de	la
sécurité —				



🖻 – 🔂 test

<u>0</u>-5

÷

Non défini

Définir la description...

Ouvrir

Enregistrer

Timeloree

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 !

Ouvrir Ouvrir une base de données... Analyser l'ordinateur maintenant... Configurer l'ordinateur maintenant...

2



#### 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 !

Configuration et analyse de la sécurité		
6,	Ouvrir	
	Ouvrir une base de données	
	Analyser l'ordinateur maintenant	
	Configurer l'ordinateur maintenant	│

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**!

🖥 securite gpo - [Racine de la console\Configuration et analyse de la sécurité\Stratégies locales\Options de sécurité] 📃 📕					
🚡 Console Fenêtre ?					
Action Affichage Eavoris $] \Leftrightarrow \Rightarrow   \boxdot   \boxed{\mathbb{R}}   \times \mathbb{E}_{0}   \textcircled{2}$					
Arbre Favoris	Stratégie 🔺	Paramètre de base	Paramètre de l'ordin		
Racine de la console	Refer immédiatement le système s'il n'est pas possibl	Non défini	Désactivé		
Modèles de sécurité	Auditer l'accès des objets système globaux	Non défini	Désactivé		
E:\WINNT\Security\Templates	BAuditer l'utilisation des privilèges de\Configuration (de	Non défini	Désactivé		
🖓 😳 Configuration et analyse de la sécurité	Canal sécurisé : crypter numériquement les données d	Non défini	Activé		
🚊 🛃 Stratégies de comptes	Canal sécurisé : crypter ou signer numériquement les d	Non défini	Désactivé		
🛛 🛃 Stratégie de mot de passe	Canal sécurisé : nécessite une clé de session forte (Wi	Non défini	Désactivé		
🚽 🛃 Stratégie de verrouillage du con	Canal sécurisé : signer numériquement les données de	Non défini	Activé		
🖻 📲 Stratégies locales	Comportement d'installation d'un fichier non-pilote non	Non défini	Réussite silencieuse		
🔤 🚮 Stratégie d'audit	Comportement d'installation d'un pilote non signé	Non défini	Avertir, mais autori		
Attribution des droits utilisateur	Comportement lorsque la carte à puce est retirée	Non défini	Aucune action		
Options de sécurité	Console de récupération : autoriser la copie de disquet	Non défini	Désactivé		
	Console de récupération : autoriser l'ouverture de ses	Non défini	Désactivé		
H Groupes restreints	Contenu du message pour les utilisateurs essayant de	super,bravo !			
E Services systeme	Créer un fichier d'échange de mémoire virtuelle lors de	Non défini	Désactivé		
	Désactiver la combinaison de touches Ctrl+Alt+Suppr	Non défini	Non défini		
Emiliar Systeme de richiers	Off reader and the second seco	NILL 120:1:	1 F		

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,

Configuration et analyse de la sécurit	Groupes restreints	Gr
🗐 🛃 Stratégies de comptes	Ouvrir	
🗍 📰 Stratégie de mot de passe	Ouvrir une base de données	
- 🛃 Stratégie de verrouillage du	Analyser l'ordinateur maintenant	
🗄 🚽 🚮 Stratégies locales	Configurer l'ordinateur maintenant	

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 le	es paramètres	par défaut	(Setup security.in	nf)
-	neuppiiquei r	cs parametres	paraciaat	(Octup Ocountyin	·••),

(Rootsec.inf) Sécuriser la racine du système •

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 xxxx.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 typeversion, 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

🚰 Stratégie de groupe	
$   \underline{A}ction  Affichage    \Leftrightarrow \Rightarrow   \blacksquare \boxed{\blacksquare} \boxed{\blacksquare}   \blacksquare $	Ê
Arbre Stratégie pour commerciaux [serveur2.domaine2.edu] Configuration ordinateur	Nom Configuration ordinateur Configuration utilisateur
🗄 🚛 Configuration utilisateur	

• 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

Configuration ordinateur Paramètres logiciel Installation de logiciel Paramètres Windows Scripts (démarrage/arrêt) Paramètres de sécurité Stratégies de comptes Stratégies locales Journal des événements Groupes restreints Services système Paramètres de sécurité Stratégies de clé publique Stratégies de clé publique Stratégies de sécurité IP sur Active Dire-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 : SI on regarde dans Utilisateur et ordinateurs Active Directory 🔏 Utilisateurs et ordinateurs Active Directory [serveu 🖻 🗊 domaine2.edu 🗄 🖾 🛄 Builtin Computers Il existe une GPO 🕘 Domain Controllers -Et II existe une GPO pour pour le Domain **Domain Controllers** 🗄 💼 ForeignSecurityPrincipals 🕘 commerciaux (ici le pointeur) (ici le pointeur) 🕂 🗐 Users 🙆 secretaires Propriétés de Domain Controllers ? × Propriétés de domaine2.edu ? × Général Géré par Stratégie de groupe Général Géré par Stratégie de groupe Liaisons de l'objet Stratégie de groupe actuel pour domaine2 Liaisons de l'objet Stratégie de groupe actuel pour Domain Controllers Liaisons de l'objet Stratégie de groupe Ne pas passer outre Désactivé Liaisons de l'objet Stratégie de groupe Ne pas pas... Désacti... Default Domain Policy 🚮 Default Domain Controllers Policy . Plus un objet Stratégie de groupe est haut dans la liste, plus sa priorité est élevée. Plus un objet Stratégie de groupe est haut dans la liste, plus sa priorité est élevée. Cette liste a été obtenue à partir de : serveur2.domaine2.edu Cette liste a été obtenue à partir de : serveur2.domaine2.edu Modifier Modifier Nouveau Aiouter. Nouveau Ajouter.. Options... Descendre Options. Supprimer. Propriétés Descendre Supprimer. Propriétés Propriétés de Default Domain Policy ? × Propriétés de Default Domain Controllers Policy ? X Général Liaisons Sécurité Général Liaisons Sécurité Default Domain Policy [serveur2.domaine2.edu] Default Domain Controllers Policy [serveur2.domaine2.edu] Résumé Résumé 11/05/2002 09:45:03 11/05/2002 09:45:03 Créé le : Créé le : Modifié le : 11/05/2002 09:58:30 Modifié le : 29/05/2002 02:14:52 3 (Ordinateur), 1 (Utilisateur) Révisions : 14 (Ordinateur), 0 (Utilisateur) Révisions : domaine2.edu Domaine : domaine2.edu Domaine : Nom unique : {31B2F340-016D-11D2-945F-00C04FB984F9} Nom unique : {6AC1786C-016F-11D2-945F-00C04/B984F9} Stockées physiquement dans **sysvol** (qui est répliqué entre CD/..) 🖻 🔄 SYSVOL 🗄 🛄 domain 🗄 🛄 sysvol 🚊 🛅 domaine2.edu DO\_NOT\_REMOVE\_NtFrs\_PreInstall\_Directory Dicies 🛄 scripts 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...

g# Stratégie de groupe		_ <b>_ _ _ _</b>
Action Affichage $4 \Rightarrow 1$ $1 \Rightarrow 1$		
Action       Affichage       Image: The transmission of the second seco	Stratégie Straté	Paramètre de l'ordinateur  Non défini
Paramètres du journal des événement     Groupes restreints     Services système     Begistre     Système de fichiers     Stratégies de sécurité IP sur Active Directo     Modèles d'administration	Créer un fichier d'échange de mémoire virtuelle lors de la Déconnecter automatiquement à la fin de la période de c Déconnecter automatiquement à la fin de la période de c Déconnecter automatiquement à la fin de la période de c Déconnecter la combinaison de touches Ctrl+Alt+Suppr. lo Durée d'inactivité avant la déconnexion d'une session Empêche la maintenance par le système du mot de pass Empêcher les utilisateurs d'installer des pilotes d'imprimante Envoyer un mot de passe non crypté pour se connecter	Non défini Désactivé Non défini Non défini Non défini Non défini

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

Utilisateurs et ordinateurs Active Directory [serveu domaine2.edu Utilisateurs Computers Domain Controllers	En se plaçant sur l'Unité voulue, il faut demander propriété :
Gran Controllers     ForeignSecurityPrincipals	Exemple ici commerciaux
± Isers	
🧖 secretaires	



#### et demander Stratégies de groupe

Propriétés de	comn	nerciaux			? ×
Général Gé	ré par	Stratégie de	groupe		
Liaisons de l'objet Stratégie de groupe actuel pour commerciaux					
Liaisons d	e l'objet	: Stratégie de g	groupe	Ne pas pas	Désacti
) Plus un obie	et Straté	aie de aroune	est haut dans la list	te, plus sa priorit	é est élevée
Cette liste a	été obt	enue à partir c	le : serveur2.domair	ne2.edu	
Nouvea		Ajouter	Modifier		Monter

Il faut se créer une nouvelle stratégie via Nouveau

	Liaisons de l'objet Stratégie de groupe actuel pour commerciaux		
Liaisons d	le l'objet Stratégie de groupe	Ne pas pas	
and the second s			
Selboard	ommerciaux		

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

puis modifier

🚮 Stratégie de groupe	
$ $ Action Affichage $ $ $\leftarrow \rightarrow  $ im $\boxed{\mathbb{R}}$ $\boxed{\mathbb{R}}$	Ê
Arbre	Nom
Stratégie pour commerciaux [serveur2.domaine2.edu]	Configuration ordinateur
E- R Configuration ordinateur	🕵 Configuration utilisateur
🕀 💼 Paramètres logiciel	
庄 💼 Paramètres Windows	
🗄 🚛 Configuration utilisateur	
🕀 💼 Paramètres logiciel	
🗄 🖳 🛄 Paramètres Windows	
	-

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. 🗲

#### stratégie utilisateur

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



#### /enforce

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

#### 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.

#### /loaoff

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 <u>lier une GPO</u>...

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





Et il faut aller dur la GPO qui nous intéresse...

Ajouter une liaison d'objet Stratégie de groupe	?	×
Domaines/unités d'organisation Sites Tous		
Regarder dans : 🗀 commerciaux.domaine2.edu	🔹 🗈 🏩 •	
Domaines, unités d'organisation et objets de stratégie	de groupe liés :	
Nom	Domaine	I
🚮 pour commerciaux	domaine2.edu	I

pour obtenir finalement

Propriétés de vrp	٤
Général   Géré par   Objet   Sécurité Stratégie de groupe	
Liaisons de l'objet Stratégie de groupe actuel pour vrp	
Liaisons de l'objet Stratégie de groupe Ne pas pas Désacti	

- 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** :



#### Gestion des liaisons de GPO:

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

Utilisateurs et ordinateurs Active Directory 🗄 💼 Requêtes sauvegardées 🖻 🗊 manuel.net

Ensuite on travaille simplement avec des liens...



Stratégies Windows XP - Domaine Cabaré Michel - SYS 26- Cours - ver 1.0 -

www.cabare.net©

🗄 🙆 a-stock-GPO

#### héritage et blocage d'héritage:

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



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

oprieces de Pe	rsonnel			
Général 🛛 Géré p	ar Stratégie de gr	oupe		
Lia	isons de l'objet Stra	tégie de group	e actuel pour F	Personnel
Liaisons de l'o	bjet Stratégie de gr	oupe	Ne pas p	as Désacti
Plus un objet SI Cette liste a été	rratégie de groupe e obtenue à partir de	est haut dans k ⊧: serveur2.do	a liste, plus sa maine2.edu	priorité est élevé
Plus un objet SI Cette liste a été Nouveau	ratégie de groupe e obtenue à partir de Ajouter	est haut dans l s : serveur2.do Modifier	a liste, plus sa maine2.edu	priorité est élevé Monter

- 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** 

	Options pour commerciaux
Et demander alors Aucun remplacement —	<ul> <li>Options de liaison :</li> <li>Aucun remplacement : empêche d'autres objets Stratégie de groupe de remplacer l'ensemble de stratégie dans celui-ci</li> <li>Désactiver : l'objet Stratégie de groupe n'est pas appliqué à ce conteneur</li> </ul>
	OK Annuler

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

Propriétés de commerciaux		? ×	1
Général Géré par Stratégie de groupe			.
Liaisons de l'objet Stratégie d commerciaux	e groupe actuel pour		
Liaisons de l'objet Stratégie de groupe	Ne pas passer outre	Désactivé	
g pour commerciaux	~		

### 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

🖾 Invite de commandes
Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-1999 Microsoft Corp.
E:\>gpresult /? Microsoft (R) Windows (R) 2000 Operating System Group Policy Result tool Copyright (C) Microsoft Corp. 1981-1999
This tool displays the result of Group Policy for the current user and computer.
usage: gpresult [/V] [/S] [/C   /V] [/?]
/V Verbose mode /S Super verbose mode /C Computer settings only /V User settings only



# **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.

Console de gestion des stratégies de groupe Service Pack 1

#### **Description rapide**

La console de gestion des stratégies de groupe (GPMC, Group Policy Management Console) Service Pack 1 (SP1) Microsoft uniformise la gestion des stratégies de groupe au sein de l'entreprise.

Sur	cette	page
-----	-------	------

⇒	<u>Détails rapides</u>	$\checkmark$	<u>Présentation</u>
⇒	Configuration minimale	$\checkmark$	Instructions
÷	<u>Ressources associées</u>	÷	<u>Voir ce que les autres personnes</u> <u>téléchargent</u>

#### Télécharger

gpmc.msi
1.0.2
15/06/2004
Français
5.6 Mo

L'installation ou la désinstallation ne pose pas de problèmes

🖓 gpmc.msi 5 719 Ko Package Windows Inst..

Se gérant classiquement via

👸 Ajouter ou supprim	er des programmes		_ 🗆 ×
	Programmes actuellement installés : 🔲 Affic <u>h</u> er les mises à jour Irier par : Nom	1	•
<u>M</u> odifier ou supprimer des	🖻 🚡 Console de gestion de la stratégie de groupe Microsoft avec SP1	Taille	<u>6,30Mo</u>
programmes	Cliquer ici pour obtenir des informations sur le support technique.	Utilisé	<u>rarement</u>
6	Pour modifier ou supprimer ce programme de votre ordinateur, cliquez sur Modifier ou Supprimer.	Modifier	Supprimer

#### 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

🛒 Stratégie Default Domain Policy [srv1-man.manuel.net]	Paramètre	État
🛱 🚚 Configuration ordinateur	Pare-feu Windows : protéger toutes les connexions réseau	Non configuré
🕀 🖓 🛄 Paramètres du logiciel	Pare-feu Windows : n'autoriser aucune exception	Non configuré
🗄 💼 Paramètres Windows	🛱 Pare-feu Windows : définir les exceptions de programmes	Non configuré
🖻 ··· 🧰 Modèles d'administration	🛱 Pare-feu Windows : autoriser les exceptions de programmes locaux	Non configuré
⊡ Composants Windows	🛱 Pare-feu Windows : autoriser l'exception d'administration à distance	Non configuré
⊡ ⊡ Système	🛱 Pare-feu Windows : autoriser l'exception de partage de fichiers e	Non configuré
Erren Keseau	🛱 Pare-feu Windows : autoriser les exceptions ICMP	Non configuré
Client DNS	Propriétés de Pare-feu Windows : autoriser l'exception d'adm	inistration <b>? X</b>
Fichiers hors connexion	Paramètre Expliquer	
🖆 - 🦳 Pare-feu Windows 	Pare-feu Windows : autoriser l'exception d'administration à distance	ce
	O Non configuré	
- SNMP	Activé	
Service de transfert intelligent en arrière-		
Imprimantes		
🖻 📲 Configuration utilisateur	Autoriser les messages entrants non sollicités provenant de :	<u> </u>
🕀 🛄 Paramètres du logiciel		
Parametres Windows		
	Syntaxe :	
	Entrez "" pour autoriser les messages provenant de n'importe quel	réseau, ou
	entrez une liste délimitée par des virgules qui contient	
	n'importe quel nombre ou une combinaison des éléments suivants :	
	Adresses IP, telles que 10.0.0.1	
	Descriptions de sous-réseaux, telles que 10.2.3.0/24	
	La chaîne "localsubnet"	
	Pris en charge sur : Microsoft Windows XP Professionnel avec SP2	2 ou une version
	Autoriser les messages entrants non sollio	cités provenant de :
ii taut indiquer l'adresse ip du serveu	IF 2003 aepuis	
loguallo on compto fairo de l'odministro		

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

A	jout d'un composant logiciel enficha	ble autonome	? X
	Composants logiciels enfichables disponible	es:	
	Composant logiciel enfichable	Fabricant	
	🛺 Gestionnaire d'autorisations	Microsoft Corporation	
	🚇 Gestionnaire de périphériques	Microsoft Corporation	
	🕼 Jeu de stratégie résultant	Microsoft Corporation	
	📓 Journaux et alertes de performance	Microsoft Corporation	



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



### 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

As	ssistant Jeu de stratégie résultant		×
	Sélection des ordinateurs Vous pouvez afficher les paramètres de str ordinateur sur ce réseau.	ratégie pour cet ordinateur ou pour un autre	Ē
	Sélectionnez l'ordinateur pour lequel vous voule	ez afficher les paramètres de la stratégie.	
	C Det ordinateur		
	Un <u>a</u> utre ordinateur :		
	MANUEL\CLIENT-XP	Pag	sourir
As	ssistant Jeu de stratégie résultant		x
	Sélection de l'utilisateur Vous pouvez afficher les paramètres de str l'ordinateur sélectionné.	ratégie pour n'importe quel utilisateur de	
	Afficher les paramètres de la stratégie de :     D Utilisateur actuel     Utilisateur spécifique :		
	CLIENT XPVAdministrateur MANUEL Vadministrateur MANUEL \bob		
<u> </u>	Jeu de stratégie résultant		
9	<u>Fichier Action Affichage Favoris Fe</u>	nêtre <u>?</u>	
-	- →   II   12 <sup>°</sup> IB   12 <sup>°</sup>		
	Administrateur on CLIENT-XP - RSoP Configuration ordinateur Promi Paramètres du logiciel	Administrateur on CLIENT-XP - sélectionnez un élément pour obtenir une description.	R50P Nom Configuration ordinateur

#### Console gpmc et Gestion des stratégies de groupes

Une nouvelle console est utilisable dans les outils Propriétés de Domain Controllers d'administration

#### Gestion des stratégies de groupe

ou à la place de Stratégie de groupe

Général Géré par Objet Sécurité COM+ Stratégie de groupe

Vous avez installé le composant logiciel enfichable Gestion des stratégies de groupe, ce qui rend cet onglet inutile.

Cliquez sur Ouvrir pour ouvrir la console de gestion des stratégies de groupe.

<u>O</u>uvrir..





www.cabare.net©

Page 38

#### Elle donne une interface plus complète

🔊 Gestion des stratégies de groupe	
පිදි Eichier <u>A</u> ction Affic <u>h</u> age Fenêtre <u>?</u>	X
$\Leftrightarrow \rightarrow   \textcircled{1}   \textcircled{1} \times \textcircled{1}   \textcircled{2}$	
Image: Second constraint of the second c	Default Domain Policy         Étendue       Détails       Paramètres       Délégation         Liaisons         Afficher les liaisons à cet emplacement :       manuel.net         Les gites, domaines et unités d'organisation suivants sont liés à cet objet GPO :
Comain Controllers     Gormation     Go	Emplacement       Appliqué       Lien activé       Chemin d'accès         Imanuel.net       Non       Oui       manuel.net         Imanuel.net       Imanuel.net       Imanuel.net         Imanuel.net       Imanuel.net       Imanuel.net

#### On retrouve les stratégies ensuite via Modifier





F

# **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 <b>Démarrer</b> et les options qui rendent le menu <b>Démarrer</b> 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	6

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







www.cabare.net©

	Réseau Fichiers hors connexion Connexions réseau et accès à distance	Réseau Fichiers hors connexion Connexions réseau et accès à distance
Composant <b>Imprima</b>	ante ordinateur Timprimantes	
Composant <b>Menu D</b> e	émarrer barre tâche	utilisateur Menu Démarrer et Barre des tâches
Composant <b>Bureau</b>		utilisateur Bureau Active Desktop Active Directory
Composant <b>Pannea</b>	u de configuration	utilisateur Panneau de configuration Ajout/Suppression de programmes Affichage Imprimantes Options régionales

#### Méthodologie de mise en oeuvre

Il est toujours conseillé de

- Ne jamais modifier las stratégies pré-définies de domaine et de controlleurs de domaine
   Default Domain Policy
   Default Domain Controllers Policy
- Rarement définir des stratégies globales au domaine, mais toujours sur des UO précises

ll est bon aussi de

- stocker toutes les stratégies dans UO spécifique et ensuite d'utiliser des liens
   manuel.net
   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 🗄 🔊 Configuration utilisateur au niveau des utilisateurs

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

- Application Data
- Bureau  $\cap$
- Mes documents 0
- Menu Démarrer 0
- 🗀 bob 🗄 🛅 Application Data 🚞 Bureau Cookies 🗋 Documents de bob 🛨 😪 Favoris 표 🚞 Local Settings 표 🚞 Menu Démarrer



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

#### Genre stock-mesdocs

📕 Gestion de l'ordinateur (local) 🛛 🔺	Nom du partage 🛛 🗠	Chemin du dossier	Туре
🖻 🌇 Outils système	stock-mesdocsp	C:\stock-mesdocs	Windows
🕀 🗊 Observateur d'événemer	SYSVOL	C:\WIN2003\SYSVO	Windows
🖻 😱 Dossiers partagés	atest	C:\test	Windows
Partages 🔽		· ·	

#### **Rediriger mes documents**

Dans la stratégie, on demande les propriétés de

#### dans lesquelles on demande Paramètre

Propriétés de Mes documents	$ \times $
Cible Paramètres	
Vous pouvez spécifier l'emplacement du dossier Mes documents.	
Paramètre : Non configuré	
Cet objet stratégie de groupe n'aura aucun effet sur l'emplacement de ce dossier. Toute redirection existante continuera à s'appliquer même si cet objet de stratégie de groupe est supprimé. Pour s'assurer que le dossier est redirigé vers l'emplacement par défaut d'origine, sélectionnez l'option "Rediriger vers l'emplacement du profil utilisateur local".	



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



Les options par défaut sont les moins dangereuses.

Propriét	és de Mes documents	? X
Cible	Paramètres	
	Sélectionner les paramètres de redirection pour Mes documents.	
	Accorder à l'utilisateur des droits exclusifs sur Mes documents	
	Déplacer le contenu de Mes documents vers le nouvel emplacement.	
_ Sup	pression de stratégie	- 1
•	Conserver le dossier dans le nouvel emplacement lorsque la stratégie sera supprimée.	
0	Rediriger le dossier vers l'emplacement du profil <u>u</u> tilisateur local lorsque la stratégie sera supprimée.	

#### 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 <u>nouveaux type</u> 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,

	Proprietes de D	econnexion	<u></u>
Arbre	Scripts		
Stratégie politique globale [serveur1.domaine1.edu] Sconfiguration ordinateur Paramètres logiciel Installation de logiciel Paramètres Windows Scripts (démarrage/arrêt) Paramètres de sécurité Paramètres de sécurité Configuration utilisateur Paramètres logiciel	Nom	éconnexion Paramètres	Monter Descendre
Paramètres Windows     Paramètres Windows     Maintenance de Internet Explorer     Scripts (ouverture/fermeture de session)     Paramètres de sécurité     Services d'installation à distance     Redirection de dossiers			Modifier
	Pour voir les fi stratégie de g Afficher les	ichiers de scripts stockés dans cet ob roupe, cliquez sur le bouton ci-dessou fichiers	ijet de Is.



0111

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...

Scripts			
	Déconnexion		
Nom		Paramètres	
			Monter
			Descendr
			Ajouter
			Modifier
			Supprime

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





### Utiliser le script dans la GPO

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

Propriétés de Déconnexion	? ×		
Scripts			
Déconnexion			
Nom Paramètres	Monter Descendre		
	Ajouter	▼	
	Supprimer	Ajout d'un Script	? ×
Pour voir les fichiers de scripts stockés dans cet objet de stratégie de groupe, cliquez sur le bouton ci-dessous. Afficher les fichiers		Nom du script : I Paramètres de scripts :	Parcourir
		OK.	Annuler

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

Parcourir		? ×	
Rechercher dans : 🔁 Logoff	+ E 🖄 📰+	-	
Fistorique			

Maintenant on a un script de déconnexion....

Propriétés de Déconnexion	?
Déconnexion	
Nom Paramètres ferme.bat	Monter Descendre
	Ajouter Modifier
Pour voir les fichiers de scripts stockés dans cet objet de stratégie de groupe, cliquez sur le bouton ci-dessous. Afficher les fichiers	Supprimer
OK Annuk	er Appliquer



#### test et visualisation :

Sachant que

- les scripts de déconnexion s'exécutent par défaut en mode caché... 0
- les scripts disposent de 10 minutes pour se réaliser, avant d'être 0 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...)





H

# **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 :

- 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

Dossiers	x	Nom 🛆	Taille	Туре	Modifié le
installsoft		授VSCAN60.MSI	21 469 Ko	Windows Installer Package	10/12/2001 06:01

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 <u>pas d'annonce</u>, 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 <u>annoncé</u> (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 <u>pas d'annonce</u>. 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

🐗 Utilisateurs et ordinateurs Active Directory			
🖉 Console Eenêtre ?			
Action Affichage   ← →   € 💽   X 🗃 🔂 🗔   😭	) 🖞 🖉 🐌 🗸	° 🗟 🐻	
Arbre	bidouilleur 1 objets	i	
Utilisateurs et ordinateurs Active Directory [serveur2.domaine2.edu]	Nom 🛆	Туре	Description
omaine2.edu	📕 client2kp7	Computer	
Ē @ Builtin			
Computers			
🗄 🧭 Domain Controllers			
🗄 📲 ForeignSecurityPrincipals			
±-Ø nouveau			
±@ Personnel			
Users			

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)





nuis	Déploiement du logiciel
	Sélectionnez la méthode de déploiement :
	C Publication
	Attribution
	C Publication ou attribution avancée
	Sélectionnez cette option pour assigner l'application sans modification.
	OK Annuler
obtient finalement	

#### or

f Stratégie de groupe							
Action Affichage $  \Leftrightarrow \Rightarrow  $ $\square$ $\square$ $\square$ $\square$ $\square$							
Arbre	Nom 🛆	Version	État du déplo	Installat	Type de mise	Mise à niveau	Paramètres régio
🛃 Stratégie installation antivirus [serv	🖀 McAfee VirusScan	6.0	Attribué	Oui	Nécessaire	Aucun	Anglais (États-Unis)
🚊 🔊 🔜 Configuration ordinateur	Configuration ordinateur						
Paramètres logiciel           Installation de logiciel							

- 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

Arbre	Type de mis	Mise à niveau	Paramètre	Source	Modifications
Stratégie msi-spyware [serveur1.dc Configuration ordinateur Configuration ordinateur Paramètres logiciel Configuration utilisateur Configuration utilisateur Paramètres logiciel Installation de logiciel Configuration utilisateur Configuration utilisateur	Facultatif	Aucun Attribuer Publier Toutes les Actualiser Propriété Aide	Exerciti ( n automatique tâches	\Serveur1\instalsoft\sna Attribuer Publier Supprimer Redéploiement des applica	tions

#### et là on peut choisir

Suppression de logiciel	? X
Sélectionner la méthode de suppression :	
C Désinstaller immédiatement le logiciel des utilisateu des ordinateurs	ırs et
C Autoriser les utilisateurs à continuer à utiliser le log mais interdire de nouvelles installations	iciel,
OK Annu	er



### 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 :

🖥 Paramètres de sécurité locaux 📃 🗖 🗵							
$   \underline{A}ction  Affichage    \Leftrightarrow \Rightarrow   \textcircled{1} \boxed{\texttt{II}}   \times \boxed{\texttt{II}}   $	Ê						
Arbre	Stratégie 🔺	Paramètre local	Paramètre en cours				
Paramètres de sécurité	Conserver l'historique des mots de passe	O mots de passe mémorisés	O mots de passe mé				
🖆 📾 Stratégies de comptes	BBDurée de vie maximale du mot de passe	42 Jours	42 Jours				
⊡ - 💼 Stratégie de mot de passe	BDurée de vie minimale du mot de passe	0 Jours	0 Jours				
🕀 🛄 Stratégie de verrouillage du compte	Les mots de passe doivent respecter des exigences de co	Désactivé	Désactivé				
🖻 🕮 Stratégies locales	E Longueur minimale du mot de passe	0 Caractères	0 Caractères				
🕀 🛄 Stratégie d'audit	Stocker le mot de passe en utilisant le cryptage réversible	Désactivé	Désactivé				
🕀 🕮 Attribution des droits utilisateur							
😟 📴 Options de sécurité							
🚊 💼 Stratégies de clé publique							
Agents de récupération de données cryptées							
🗄 🗐 Stratégies de sécurité IP sur Ordinateur local							

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

🛃 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**,

	Installe	r à par	tir de la disquette	;				×
		Insérez dans le	: le disque d'installation : lecteur sélectionné	on du et cliq	constructeur uez sur OK.	0	)K	
						Ani	nuler	
		Copier	les fichiers construct	eur à j	partir de :			
		<u>A:</u> N			<u> </u>	Parc	ourir	
• pour   <b>ADM</b>	windows	95 <b>LS\F</b>	procédez POLEDIT	à	l'installa	ation	à	partir
		00		2	l'un at a llu	-	2	us suttin

 pour windows 98 procédez à l'installation à partir du répertoire TOOLS\RESKIT\NETADMIN\POLEDIT

du répertoire



Dans l'installation cocher les deux cases	bien	Disquette fournie Pour ajouter un composant, sélectionnez la c. côté du composant. Décochez la case si vou inclure le composant. Composants : ☑ ◆ Editeur de stratégie système ☑ ◆ Stratégies de groupe	ase à cocher située à is ne voulez pas 0,3 Mo 0,0 Mo
Désormais l'éditeur stratégie est dispo dans le menu	de nible	Espace nécessaire : Espace disponible sur le disque : Description Prise en charge par groupe des stratégies s	0,2 Mo 454,3 Mo ystème.

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

|--|

Lorsqu'on le lance, on obtient

🛃 Editeur de stratégie système 📃 🗖 🛛 🔀
<u>Fichier</u> <u>Edition</u> <u>Affichage</u> <u>Options</u> <u>?</u>

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



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





 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) 

 Modification des mots de passe

 Administration distante
 Profils utilisateur

 Image: Administration distante
 Administration distante

 Activer l'administration distante de ce serveur
 Permet à d'autres utilisateurs de gérer vos fichiers et vos imprimantes à partir d'un ordinateur distant.

 Mot de passe :
 Image: Confirmer le mot de passe :

? X

2.	Le service <b>Registre distant</b> soit installé, via le menu contextuel de <b>voisinage</b> <b>réseau / propriété /</b> dans lequel on demande d'ajouter un service	Sélection de : Service réseau       Image: Service réseau que vous souhaitez installer et cliquez ensuite sur DK. Si vous avez une disquette d'installation pour ce périphérique, cliquez sur Disquette fournie.         Modèjes :
	spécifique, que l'on prends via "disquette fournie"	Partage des fichiers et imprimantes pour les réseaux Microsoft Partage des fichiers et imprimantes pour les réseaux NetWare Service pour NDS

Propriétés de Mots de passe

• dans le dossier TOOLS\RESKIT\NETADMIN\REMOTEREG

		Ouvrir		? ×
		<u>N</u> om de fichier : regsrv.inf	<u>D</u> ossiers : n:\tools\reskit\net\remotreg	ОК
Uniquement	sur	regsrv.inf	n:\	
windows 98	301	•	a reskit	<u>H</u> eseau
		T	er remotreg	
		_	Lecteurs :	

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
- I'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

On cré un fichier de stratégie comprenant 2 entrées:	-
l'Utilisateur par défaut	
ou l' <b>Ordinateur par défaut</b>	
2 entrées	li.

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

No <u>m</u> :	
<u>T</u> ype :	Stratégies (*.POL)



# **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** 



#### 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	Ajouter un ordinateur
rentrer le nom de la machine à traiter différemment	Entrez le nom de l'ordinateur à ajouter :       OK         Annuler
	Parcourir à la recherche d'un ordinateur 🔹 🏾 🕄
	Sélectionnez l'ordinateur que vous voulez ajout
	<ul> <li>☐ - ☐ Voisinage réseau</li> <li>☐ - ④ Tout le réseau</li> <li>☐ Serveur_simple</li> <li>↓ Wks_simple1</li> </ul>

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



	🛃 Propriétés de Ordinateur par défaut	×
Les stratégies possible apparaissent alors listées:	Stratégies	
3 valeurs peuvent être prises par les	Acces distant windows NT     Interpréteur de commandes Windows NT     Système Windows NT     Profils utilisateurs Windows NT	

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	Ajouter un utilisateur
rentrer le nom de l'utilisateur à traiter différemment	Entrez le nom de l'utilisateur à ajouter : Annuler
Ajout d'utilisateurs	×
Lister les noms de : By SIMPLE* <u>N</u> oms :	
Administrateur Albert Bertrand Camille Daniel Eric	Compte d'utilisateur d'administration
pour gérer un groupe différemment	t il faut dans le menu
Modifier / Ajouter un groupe	ijout d'un groupe 🛛 🗙
rentrer le nom du groupe à traiter différemment	Entrez le nom du groupe à ajouter : OK Annuler Parcourir

Ajout de groupes		×
Lister les noms de :	B SIMPLE*	<b>_</b>
<u>N</u> oms :		
🙀 Admins du doma	ine	Administrateurs désignés du domaine
Commerciaux C Invités du domain	ne	Tous les invités du domaine
		Priorité du groupe

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

un utilisateur appartient à des groupes qui ont différer la même stratégie, les paramètres du groupe ayant la auront préséance.	nts paramètres pour plus haute priorité
<u>O</u> rdre de groupe :	
Commerciaux C NOUS	<u>M</u> onter Descendre
OK	Annuler

Les groupes situés dans la haut de la liste ont la priorité la plus haute. Si

Ordonner les groupes par ordre de priorité.

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



.

X



Les stratégies possible apparaissent alors listées:

itratégie	s
ç Ui	isateur par défaut
Ē. 🕉	Panneau de configuration
⊡ ♦	Bureau
	Shell
÷.	Système
÷.	Interpréteur de commandes Windows NT
1 i 👗	Sustème Windows NT

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

C	cochée :	la stratégie est implémentée
Ç	grise :	la clé de registre n'est pas modifiée
k	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** 



#### 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 :
Dásoou	📕 Ordinateur par défaut
Reseau	🖻 🕔 Réseau
	🖻 🛄 Contrôle d'accès
	🔤 🔣 Contrôle d'accès au niveau utilisateur
	🖨 🐙 Ouverture de session
	🔤 💹 Bannière d'ouverture de session
	🔤 Nécessite une validation par réseau pour l'accès Window:
	🖨 🛄 Client Microsoft pour réseaux NetWare
	🔤 📰 Serveur par défaut
	🔤 📰 Prend en charge des noms longs de fichiers
	🔤 🔤 Mode de recherche
	🔤 Désactiver l'ouverture automatique de session NetWare
	🖨 🔟 Client Microsoft pour réseaux Windows
	🔤 🖩 Ouverture de session sur Windows NT
	🔤 🔤 Groupe de travail
	🔤 Autre groupe de travail
	🖨 🔟 Imprimante et fichier partagés pour les réseaux NetWare
	Désactiver annonce SAP
	🚊 🛄 Mots de passe
	🔤 Masquer les mots de passe de partage par des astérisque:
	🔤 🔤 Désactiver la mise en antémémoire du mot de passe
	🔤 Mécessite un mot de passe alphanumérique d'ouverture de
	🔤 Longueur minimale du mot de passe Windows
	🖨 🔟 Accès réseau à distance
	Désactiver la réception d'appel
	🚊 🔟 Partage
	🔤 🔤 Désactiver le partage de fichiers
	Désactiver le partage d'imprimante
	🚊 🛄 SNMP
	🔤 🔤 Communautés
	🔤 🖩 📰 Gestionnaires permis
	🔤 Intercepte communauté 'Publique'
	Internet MIB (RFC1156)
	🖻 🛄 Mettre à jour
	🔤 Mise à jour distante
Système	Ordinatour par défaut
	E Ordinateur par deraut
	Emilia <u>Sovience</u>
	Mutrer les prons d'unisateurs
	Chemin d'accès réseau pour l'unitation de Wilhouws
	Enternin a acces reseau pour windows rour
	Executer une rois



#### Stratégies d'Utilisateur Windows 98 :

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





#### Système







# **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 :







#### Stratégies d'Utilisateur Windows NT :

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





Stratégies Windows XP - Domaine Cabaré Michel - SYS 26- Cours - ver 1.0 -

www.cabare.net©



