

http://WWW.CABARE.NET ©

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

Stratégies Windows & GPO de Domaine 2008 Michel Cabaré – Ver 2.0 – Nov 2009La formation que vous suivez, à pour but de vous initier avec le logiciel Microsoft Windows 2008 (version 6.x) sur environnement P.C.

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

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

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

Bon Travail

Michel Cabaré

TABLE DES MATIÈRES

STRATEGIES LOCALES XP	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
IMPRIMER LISTER LES STRATEGIES :	9
STRATEGIES LOCALES MULTIPLES VISTA SEVEN	.10
STRATEGIES LOCALES MULTIPLES DITES LGPO	.10
DEFINIR UNE L'GPO	.10
DESACTIVATION DES LGPO	.12
	10
ALIDIT EVENTEMENT ALIDIT DEGOLIDOE.	.13
AUDII EVENEMENI – AUDII RESSUURCE.	.15
INSTALLER UN AUDIT SUR EVENEMENT - VISTA AP	.14
INSTALLER UN AUDIT VIA AUDITPOL - SEVEN OU 2008	.13
LIKE LE JOURNAL DE SECURITE.	.17
Audit ressource sur un dossier	18
Audit ressource sur une imprimante	20
	.20
STRATEGIES DE DOMAINE	.22
STRATEGIES DE DOMAINE :	.22
LA GESTION DES STRATEGIES DE GROUPE :	.22
MODIFIER LA STRATEGIE DE DOMAINE :	.23
STRATEGIE ORDINATEUR, UTILISATEUR:	.23
PROPAGATION STRATEGIES DE DOMAINE :	.24
L'UTILITAIRE EN LIGNE GPUPDATE (SEVEN $XP = 2008\ 2003$)	.25
L UTILITAIRE EN LIGNE SECEDIT (2000)	.23
CESTION I ROPAGATION DES STRATEGIES DE DOMAINE	.20 28
EXEMPLE . ATTRIBUTION DROTTS UTILISATE OR MODIFIER L HEURE STSTEME	.20
STRATEGIES CONTROLEUR DE DOMAINE	.31
STRATEGIES DE CONTROLEUR DE DOMAINE :	.31
MODIFIER LA STRATEGIE DES CONTROLEUR DE DOMAINE :	.32
EXEMPLE : ATTRIBUTION DROITS UTILISATEUR MODIFIER L'HEURE DC :	.32
STRATEGIES ET PREFERENCES	.35
Les preferences 2008 Serveur :	.35
CLIENT SIDE EXTENSION POUR XP SP2 & VISTA:	.36
PRINCIPALES PREFERENCES ORDINATEUR :	.36
PRINCIPALES PREFERENCES UTILISATEUR :	.36
Options Communes des Preferences :	.38
MODELE DE STRATEGIES	40
Les model es de strategie de securite:	.40
CREATION D'UN MODELE:	.41
CREATION D'UNE BASE LOCALE DE SECURITE:	.43
VERIFICATION MODELE - POSTE:	.43
APPLICATION DU MODELE SUR LE POSTE	.44
MODIFICATION DU MODELE	.44
Assistant 2008 et Modeles pre definis	.44
Resume	.45
ΩΡΩ D'UNITE ODC A NIS A TIONELLE	16
TYPES ET NIVEAUX DE STRATEGIE ·	.40 46
	0





http://www.cabare.net Page 3 - Michel Cabaré -

NIVEAU DE MODIFICATION DANS LA BASE DE REGISTRE	
CREER UNE STRATEGIE DE GROUPE:	
LIER UNE STRATEGIE DE GROUPE SUR UNE U.O :	
VERIFICATION DES ELEMENTS DE L'UO:	
VERIFICATION ET UTILITAIRE GPRESULT.EXE	51
HIERARCHIE DES STRATEGIES	
ORDRE FINAL D'APPLICATION DES STRATEGIES :	
LIAISONS MULTIPLES - PRIORITE - HERITAGE – DES GPO	53
LIAISON DE GPO :	
HERITAGE – BLOQUE :	54
HERITAGE - APPLIQUE:	
GESTION ET SAUVEGARDE DES GPO	58
RESUME DE LA STRATEGIE :	
COPIER UNE STRATEGIE :	
SAUVEGARDER LES STRATEGIES :	
RESTAURER LES STRATEGIES :	60
GPO - MODELES D'ADMINISTRATION	62
Les Modeles presents	
RAPPELS METHODOLOGIE DE MISE EN ŒUVRE	63
GPO - SCRIPTS	64
SCRIPTS DE DEMARRAGE – ARRET – FIN DE SESSION :	64
SCRIPTS DE FIN DE SESSION :	64
Copier le script dans la GPO : (Afficher)	
Utiliser le script dans la GPO (Ajouter)	
TEST ET VISUALISATION :	67
GPO - INSTALLATION DE LOGICIELS	69
Les 3 elements Winstaller – GPO - AD	69
WINDOWS INSTALLER ET FICHIERS MSI	69
PROCEDURE D'INSTALLATION ET DE MAINTENANCE LOGICIELS	
CREATION DU POINT D'INSTALLATION DE LOGICIEL	70
ATTRIBUTION - PUBLICATION DE LOGICIEL	71
STRATEGIE DE DEPLOIEMENT DE LOGICIEL	71
STRATEGIE DE RE-DEPLOIEMENT / DESINSTALLATION	72
PROPRIETES DE DEPLOIEMENT DE LOGICIEL	
GPEDIT.MSC	74
STRATEGIE LOCALE / RESEAU:	74
Editeur de strategie de domaine "locale" :	74





STRATEGIES LOCALES XP

Types de stratégie :

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

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

Stratégies sur un ordinateur local (cf microsoft GPO hors AD):

Lorsque un ordinateur n'appartient à aucun domaine, pour configurer une stratégie il faut obligatoirement passer par une stratégie locale...

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

🖥 Paramètres de sécurité locaux		_ 🗆 ×
$ \underline{A}ction Affic\underline{h}age \leftarrow \rightarrow \blacksquare \overrightarrow{\mathbf{r}} \times \mathbf{E} $	l 🕄	
Arbre	Nom	Description
 Paramètres de sécurité Image: Stratégies de comptes Image: Image: Stratégies locales Image: Image: Imag	Stratégies de comptes Stratégies locales Stratégies de clé publique Stratégies de sécurité IP sur	Stratégies de mot de passe et de verrouillage de c Stratégies des options d'audit, de droits d'utilisateu Administration de la sécurité du protocole Internet
	,	

Ces stratégies locales sont disponibles sur

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

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

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

Lorsque un ordinateur appartient à un domaine, on peut alors utiliser les stratégies de groupes dites **GPO**. On étudiera ces **GPO** ultérieurement, mais il faut savoir que l'on peut poser des stratégies de groupes à différents niveaux, donc les paramètres locaux sont modifiés dans cet ordre

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





Configurer des stratégies localement :

Il ne faut pas confondre "<u>configurer des stratégies localement</u>", qui suppose que l'action soit faite localement sur chaque machine, avec la notion de "<u>paramètres</u> <u>de stratégie locale</u>".

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



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

• Stratégies de compte

(~gestion utilisateur)

• Stratégies locales

(~qui peut ouvrir session locale)

• Stratégies de clé publique

(agent de récupération)

• Stratégies IPSEC

 Action
 Affichage
 ← →
 m
 m
 ×
 w

 Arbre
 Image: Stratégies de comptes
 Image: Stratégies de compte
 Image: Stratégies de compte<

Paramètres de sécurité locaux

(cryptage IP)

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

Interface Windows 2000





http://www.cabare.net Page 6 - Michel Cabaré -

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

Paramètres de sécurité locaux	
$ $ <u>A</u> ction Affichage $ $ $\Leftrightarrow \Rightarrow $ E $ $ \times $ $ $ $	Ê
Arbre	Stratégie 🛆
🗊 Paramètres de sécurité	Durée de verrouillage des comptes
🖻 💼 Stratégies de comptes	Réinitialiser le compteur de verrouillages du compte après
Stratégie de mot de passe	Seuil de verrouillage du compte
Strategie de verrouillage du compte	
	Paramètre de stratègie de securité locale
	Seuil de verrouillage du compte
Sur lequel un double-clic amène	Paramètres de la stratégie actuelle
	Le compte ne sera pas verrouillé :
	O tentatives d'ouvertures de session non valides
	Prove New de strat fair le sele
	Le compte ne sera pas verrouillé :
	tentatives d'ouvertures de session non valides
	Si des paramètres de stratégie sont définis au niveau du domaine, ils
	remplacent les parametres de strategie locale.

Contenu des Paramètres locaux de sécurité :

Stratégies de comptes

Stratu Stratu	égies de comptes tratégie de mot de passe tratégie de verrouillage du compte Stratégies de mot de passe			
	Stratégie 🔺			
	Conserver l'historique des mots de passe			
BDurée de vie maximale du mot de passe				
ImigiDurée de vie minimale du mot de passe ImigiDurée de passe dei vertrestestes des evidences de complexité				
Inglices mous de passe doivent respecter des exigences de complexite				
	📆 Stocker le mot de passe en utilisant le cryptage réversible pour tous les utilisateurs du domaine			
Stratégies de verrouillage du compte				
	Stratégie 🛆			
	Durée de verrouillage des comptes			
•	I题 Réinitialiser le compteur de verrouillages du compte après 認Seuil 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 problèmes d'accès !



Stratégies locales 💼 Stratégies locales 📴 Stratégie d'audit 👜 Attribution des droits utilisateur 🔟 Options de sécurité Stratégie d'audit Stratégie 🕮 Auditer 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 Auditer les événements de connexion aux comptes Auditer les événements système Auditer les modifications de stratégie Auditer l'utilisation des privilèges Attribution des droits utilisateurs Stratégie Contraction de la cet ordinateur depuis le réseau 🕮 Agir en tant que partie du système d'exploitation Ajouter des stations de travail au domaine Arrêter le système B Augmenter la priorité de planification CAUgmenter 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 Déboguer des programmes BBForcer l'arrêt à partir d'un système distant Générer des audits de sécurité Berer le journal d'audit et de sécurité BB Modifier les valeurs d'env. de microprogrammation Modifier l'heure système BOptimiser les performances système BOptimiser un processus unique BOutrepasser le contrôle de défilement 🕮 Ouvrir une session en tant que service BOUVRING Session en tant que tâche BOUVRING UND Session localement Options de sécurité Stratégie 🕮 Arrêter immédiatement le système s'il n'est pas possible de se connecter aux audits de sécurité 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 避 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 🕮 Créer un fichier d'échange de mémoire virtuelle lors de la fermeture du système 题Désactiver la combinaison de touches Ctrl+Alt+Suppr. lors de l'ouverture de session BDurée d'inactivité avant la déconnexion d'une session 🕮 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 🕮 Ne permettre l'accès au CD-ROM qu'aux utilisateurs connectés localement 题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



Agents de récupération de données cryptées

Stratégies de sécurité IP





Stratégies de restriction logicielle (uniquement sous Seven XP)

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

Imprimer lister les stratégies :

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

Exporter la liste...



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

Iiste.txt - Bloc-notes	
Fichier Edition Format Affichage ?	
Stratégie Paramètre de sécurité Conserver l'historique des mots de passe 0 mots de passe mémorisés Durée de vie maximale du mot de passe 42 Jours Durée de vie minimale du mot de passe 0 Jours Le mot de passe doit respecter des exigences de complexité Désactivé Longueur minimale du mot de passe 0 Caractères Stocker le mot de passe en utilisant le cryptage réversible pour tous les utilisateurs du domaine	Désactivé
Ou le travailler (fichier texte délimité par des tabulations)	

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





STRATEGIES LOCALES MULTIPLES VISTA SE

Stratégies locales multiples dites LGPO

Avant Vista, il ne pouvait y avoir qu'une seule stratégie locale, contenant un lot de commandes, valable pour :

tous les utilisateurs....

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

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

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

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

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

Définir une LGPO

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

tensions sont activées. mposants logiciels enfichables disponibles :		(Composants logiciels enfichables s	électionnés :
Composant logiciel enfichable			Racine de la console	Modifier les extensions.
Certificats Configuration du client NAP Configuration et analyse de la sécurité Contrôle ActiveX	щ			Supprimer
Dossier Dossier		Ajouter >		Descendre





http://www.cabare.net Page 10 - Michel Cabaré - Lorsque on ajoute, On ne demande surtout pas Terminer(*), mais Parcourir

Assistant Stratégie de groupe	
	Les objets de stratégie de groupe locale sont stockés sur l'ordinateur local. Utilisez le bouton Parcourir pour sélectionner un objet de stratégie de groupe.
	Objet de stratégie de groupe : Ordinateur local
	Autoriser la modification du composant logiciel enfichable de stratégie de groupe lors de l'exécution à partir de la ligne de commande. Ceci ne s'applique que si vous enregistrez la console.

Et on choisit l'onglet Utilisateur

Rechercher un objet Stratègie de groupe	avec la stratégie de groupe locale :
Nom Administrateur pierre util Administrateurs Non-administrateurs	Il existe des objets de str Non Non Non Non
	OK Annuler
 I'ordinateur, -il a tous les utilisateu Tous les adminis 	urait fallut faire terminer (*) urs il aurait fallut faire terminer trateurs (locaux)
Touts les non-ad	Iministrateurs (locaux)

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



On obtient

Racine de la console Image: stratégie Ordinateur local/Non-administrateurs	📔 Paramètres Windows	y
 Configuration utilisateur Paramètres du logiciel Paramètres Windows Modèles d'administration Stratégie Ordinateur local\Administrateurs Stratégie Ordinateur local\Administrateur Stratégie Ordinateur local\util 	Sélectionnez un élément pour obtenir une description.	Nom Services d'installation à distance Scripts (ouverture/fermeture de sessio Paramètres de sécurité QoS basée sur la stratégie Imprimantes déployées Maintenance de Internet Explorer

Pour chaque Stratégie locale, on effectue les réglages...

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

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

Désactivation des LGPO

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

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



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



STRATEGIES LOCALES - AUDIT

Audit évènement – audit Ressource:

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

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

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

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

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

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

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

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



Installer un Audit sur évènement - Vista XP

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

Il faut passer par les Stratégies de sécurités locales,

sous VISTA Stratégies locales / Stratégies d'audit

🚡 Stratégie de sécurité locale		
Fichier Action Affichage ?		
🗢 \Rightarrow 🖄 🗔 🗙 🗔 😖 🚺 🖬		
Paramètres de sécurité	Stratégie	Paramètre de sécurité
	 Auditer 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 	Pas d'audit Pas d'audit Pas d'audit Pas d'audit Pas d'audit
 Stratégies du gestionnaire de listes de Stratégies de clé publique Stratégies de restriction logicielle Stratégies de sécurité IP sur Ordinateu 	Auditer les événements de connexion aux comptes Auditer les événements système Auditer les modifications de stratégie Auditer l'utilisation des privilèges	Pas d'audit Pas d'audit Pas d'audit Pas d'audit

par exemple sur évènements de connexion aux comptes

	Propriétés de Auditer les événements de connexion aux comptes
et en demandant d'auditer les Réussites et/ou les Echec	Paramètre de sécurité locale Expliquer Auditer les événements de connexion aux comptes
	Auditer les tentatives des types suivants : Réussite Échec

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

Fichier Action Affichage ?					
🔶 🧼 🖄 🖬 🛛 🗖					
Gestion de l'ordinateur (local)	Mots clés	Date et heure	Source	ID de l'événe	Catégorie de ^
 ¹ Outils système Planificateur de tâches Planificateur d'événeme Observateur d'événeme Affichages personna Journaux Windows Application Sécurité Setup 	 Succès de l'audit Succès de l'audit Succès de l'audit Échec de l'audit Échec de l'audit Échec de l'audit Succès de l'audit Succès de l'audit 	27/11/2009 17:39:43 27/11/2009 17:39:43 27/11/2009 17:39:43 27/11/2009 17:39:43 27/11/2009 17:39:37 27/11/2009 17:39:32 27/11/2009 17:39:24 27/11/2009 17:37:26	Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi	4672 4624 4648 4776 4776 4647 4719	Ouverture d Ouvrir la ses Ouvrir la ses Validation d Validation d Fermer la se: Auditer les n
 Systeme Événements trar É Journaux des applica Abonnements Bossiers partagés Witlisateurs et groupes I Misationaire de périphé 	Événement 4776, Micr Général Détails Le contrôleur de d Package d'authen Compte d'ouvertu	osoft Windows security audit omaine a tenté de valider les tification : MICROSOf re de session : util	ing. informations d'identificat	tion d'un compte.	×



sous 2000 Stratégies locales / Stratégies d'audit

$ $ Action Affichage $ $ \Leftrightarrow \Rightarrow 1			
Arbre	Stratégie 🛆	Paramètre local	Paramètre en cours
Paramètres de sécurité	Auditer la gestion des comptes	Pas d'audit	Pas d'audit
E Stratégies de comptes	🕮 Auditer l'accès au service d'annuaire	Pas d'audit	Pas d'audit
🗄 🔟 Stratégies locales	Auditer l'accès aux objets	Pas d'audit	Pas d'audit
庄 💼 Stratégie d'audit	Auditer le suivi des processus	Pas d'audit	Pas d'audit
🕀 🛄 Attribution des droits utilisateur	Auditer les événements de connex	. Pas d'audit	Pas d'audit
庄 📠 Options de sécurité	Auditer les événements de connex	. Pas d'audit	Pas d'audit
🗄 💼 Stratégies de clé publique	Auditer les événements système	Pas d'audit	Pas d'audit
🗄 🗐 Stratégies de sécurité IP sur Ordinateur local	🕮 Auditer les modifications de stratégie	e Pas d'audit	Pas d'audit
	Auditer l'utilisation des privilèges	Pas d'audit	Pas d'audit

par exemple sur évènemen	ts de connexion aux comptes
et en demandant d'auditer les réussites et/ou les échec	Paramètre de stratégie de sécurité locale ? X Auditer les événements de connexion Paramètres de la stratégie en cours : Paramètre de stratégie locale Auditer ces essais : Auditer ces essais : Essais ayant réussi Image: Essais ayant échoué Essais ayant échoué
	Si des paramètres de stratégie sont définis au niveau du domaine, ils remplacent les paramètres de stratégie locale.

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
dans ce cas si on re-ouvre la conse	ole on voit alors	
Auditer les événements de connexion	Opération réussie, Échec	Opération réussie, Échec

Installer un Audit via Auditpol - Seven ou 2008

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

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

Le problème c'est que ces deux options

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

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







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



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

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

C:\Users\Administrateur>auditpol/get /cat	egory:*
Strategie d'audit systeme Catégorie/Sous-catégorie	Paramètre
Système	
Extension système de sécurité	Aucun audit
Intégrité du système	Succès et échec
Pilote IPSEC	Aucun audit
Autres événements système	Succès et échec
Modification de l'état de la sécurité	Opération réussie
Ouverture/Fermeture de session	
Ouvrir la session	Succès et échec
Fermer la session	Opération réussie
Verrouillage du compte	Opération réussie
Mode principal IPsec	Aucun audit
Mode rapide IPsec	Aucun audit
	A 11.

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





http://www.cabare.net Page 16 - Michel Cabaré - Comme dans

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

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

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

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

Lire le journal de sécurité:

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

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

Fichier Action Affichage	2 ?					
🔶 🔿 🔁 🗔 🚺						
Gestion de l'ordinateur (lo	ocal)	Mots clés	Date et heu	ıre	Source	ID de l'événe.
Outils système Dissifications de té		🔍 Succès de l'audit	27/11/2009	17:37:26	Microsoft Wi	471
Planificateur de tac Observateur d'évé	ches	Succès de l'audit	27/11/2009	17:37:26	Microsoft Wi	471
A Affichages per	conni	Succès de l'audit	27/11/2009	17:37:26	Microsoft Wi	471
A 🔂 Journaux Wind	ows	🔍 Succès de l'audit	27/11/2009	17:34:59	Microsoft Wi	463
Application	1	🔍 Succès de l'audit	27/11/2009	17:33:37	Microsoft Wi	467
Sécurité		🔍 Succès de l'audit	27/11/2009	17:33:37	Microsoft Wi	462
Setup	Ouv	rir le journal enregistré	aut.	8.37	Microsoft Wi	464
Système Evénem ↓ 2ournaux de	Crée Imp	er une vue personnalisé orter une vue personna	ie ilisée	curity auditir	ng.	
Abonneme	Effa	cer le journal				
Dossiers partag	Filtre	er le journal actuel				
Fiabilité et perf	Prop	oriétés	B			

Dans lequel on peut indiquer dans notre cas

ittrer XML	
Connecté :	À tout moment
Niveau d'événement :	Critique Avertissement Commentaire
	Erreur Information
Par journal	Journaux d'événements : Sécurité
December 2	C
Par source	Sources d evenements :
Inclut/exclut des ID séparant par des vii Par exemple 1,3,5-9	Sources à evenements :) d'événements : entrez les numéros ou les plages d'identificateurs en rgules. Pour exclure des critères, faites-les précéder du signe « moins 99,-76
Inclut/exclut des ID séparant par des vii Par exemple 1,3,5-9	Sources a evenements :) d'événements : entrez les numéros ou les plages d'identificateurs el rgules. Pour exclure des critères, faites-les précéder du signe « moins 39,-76 <tous d'événements="" id="" les=""></tous>
Inclut/exclut des ID séparant par des vir Par exemple 1,3,5-5 Catégorie de la tâche :	Sources à evenements :) d'événements : entrez les numéros ou les plages d'identificateurs en rgules. Pour exclure des critères, faites-les précéder du signe « moins 99,-76 <tous d'événements="" id="" les=""></tous>
Inclut/exclut des IE séparant par des vi. Par exemple 1,3,5-9 Catégorie de la tâche : Mots clés :	Sources à evenements :) d'événements : entrez les numéros ou les plages d'identificateurs en rgules. Pour exclure des critères, faites-les précéder du signe « moins 39,-76 <tous d'événements="" id="" les=""> Échec de l'audit</tous>

Ce qui donne uniquement

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





http://www.cabare.net Page 17 - Michel Cabaré -

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 (en plus de la sécurité d'accès éventuellement posée

Audit ressource sur un dossier

ll faut

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

Exemple :

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

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



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







3. puis que l'on pose un audit dessus

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

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



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

1:39 1:39 1:01 1:01 1:01 1:01	Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi	4656 4656 4672 4624 4624 4624	Système de fie Système de fie Ouverture de Ouvrir la sessi Ouvrir la sessi
1:39 1:01 1:01 1:01 1:01	Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi	4656 4672 4624 4624 4648	Système de fi Ouverture de Ouvrir la sessi Ouvrir la sessi
1:01 1:01 1:01 1:01	Microsoft Wi Microsoft Wi Microsoft Wi Microsoft Wi	4672 4624 4624	Ouverture de Ouvrir la sessi Ouvrir la sessi
1:01 1:01 1:01	Microsoft Wi Microsoft Wi Microsoft Wi	4624 4624	Ouvrir la sessi Ouvrir la sessi
1:01 1:01	Microsoft Wi Microsoft Wi	4624	Ouvrir la sessi
L:01	Microsoft Wi	4649	Our intersection
		4040	Ouvrir la sessi
<u>1·50 </u>	Microsoft Wi	4647	Fermer la sess
ecurity auditir	ng.		×
e	m curity auditir	III ecurity auditing,	m ecurity auditing.

Un hand	lle vers un objet a été den	iandé.			
	ID de sécurité :	PC-de-util\u	til		
	Nom du compte :	util	1		
	ID d'ouverture de session	n: 0x2	de-util 0189e		
Objet :					
	Serveur de l'objet :	Sec	unty		
o <mark>urn</mark> al :	Sécurité				
Source :	Microsoft Wi	ndows security	Connecté :	27/11/2009 18:11:39	
véneme	nt: 4656		Catégorie :	Système de fichiers	





- SYS 26- Cours - ver 2.0 -

http://www.cabare.net Page 19 - Michel Cabaré -

Audit ressource sur une imprimante

On veut savoir qui utilise l'imprimante réellement :

ll faut

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

General	Partage	Ports	Avancé
Gestion des couleurs	Sécurité	Paramètres	du périphérique
iroupes ou noms d'utilis	ateurs :		
🍇 Tout le monde		ar and	
& CREATEUR PROP	RIETAIRE	20	
🔏 Administrateur (PC-	de-util\Administrateur)		
용 Administrateurs (PC	-de-util\Administrateurs)	
		Ajouter	Supprimer
utorisations pour Tout I	e monde	Autoris	er Refuser
Imprimer			
Gestion d'imprimantes			
Gestion des documen	its		
Autoriantiana anáciala	5		
Autorisations speciale			

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

Autorisations	Audit	Propriétaire	Autorisations effectives			
Pour officia	. ou mad	ifier les détails	d'une entrée d'audit, sélections	nez l'entrée, puis clique	z eur Modifier	
Four aniche	ou mou	iller les details	u une chilee u duuit, selectioni	not remote, puis cilque	z aur mountor.	
Four aniche	ou mou	inel les details		nez i entree, pale enque		
Entrées d'au	dit :	nier ies details		ine formou, pais orque		



Et il faut indiquer ce que l'on veut auditer

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

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





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

Planificateur de tâches	Mots clés	Date et heure		Source	ID de l'événe	Catégorie de
Observateur d'événeme	Succès de l'	udit 27/11/2009 18:29	:07	Microsoft Wi	4656	Autres évén
Affichages personna	🔍 Succès de l'a	audit 27/11/2009 18:29	:07	Microsoft Wi	4658	Autres évén
Journaux Windows	🔍 Succès de l'a	audit 27/11/2009 18:26	:17	Microsoft Wi	4656	Autres évén
Application	🔍 Succès de l'a	audit 27/11/2009 18:26	:17	Microsoft Wi	4658	Autres évén
Securice	🔍 Succès de l'a	audit 27/11/2009 18:26	:17	Microsoft Wi	4656	Autres évén 🔻
Secup	4		m			- F
Événements trar Journaux des applica Abonnements	Événement 465 Général Dét	δ, Microsoft Windows s ails	curity auditing.			×
 Bossiers partagés Willisateurs et groupes I Fiabilité et performance Gestionnaire de périphé Stockage 	ID No Do ID	de sécurité : om du compte ; maine du compte : d'ouverture de session :	PC-de-util\Adr Administrateur PC-de 0x23d	ministrateur r e-util l6c8		E
Gestion des disques	Objet : Se Ty	rveur de l'objet : pe d'objet :	Spool Printer	ler	de la	





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 2008-2003 ou 2000 en font partie

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

La gestion des stratégies de groupe :

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



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



Les Objets de stratégie de groupe représentent l'endroit logique de stockage de

toutes I	es	🗐 Éditeur de gestion des stratégie	es de groupe
groupe,	de	Fichier Action Affichage ?	Propriétés de : Stratégie Default Domain Controllers Policy [S ? X
Si on demand Modifier Propriété, on vo alors le GUID de stratégie	de / oit la	 Stratégie Default Domain Controlle Configuration ordinateur Stratégies Préférences Configuration utilisateur Stratégies Préférences Préférences 	Default Domain Controllers Policy [SRV-2008.FORMATION.EDU] Résumé Créé le : 25/11/2009 13:00:32 Modifié le : 28/11/2009 13:27:28 Révisions : 67 (Ordinateur), 0 (Utilisateur) Domaine : FORMATION.EDU Nom unique : {6AC1786C-016F-11D2-945F-00C04FB984F9}
Correspondant		-	

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



http://www.cabare.net Page 22 - Michel Cabaré - Dans lequel on y trouvera nos stratégies

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

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

Correspondant à

Default Domain Controllers Policy
Default Domain Policy



Il existe 2 GUID connus :

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

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

Modifier la Stratégie de Domaine :

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



On demande Modifier... la Default Domain policy

Éditeur de gestion des stratégies de groupe	
Fichier Action Affichage ?	
 Stratégie Default Domain Policy [SRV-2008.FORMATION.EDU] Configuration ordinateur Stratégies Paramètres du logiciel Paramètres Windows Modèles d'administration : définitions de stratégies Modèles d'administration Stratégies Stratégies Paramètres du logiciel Préférences Stratégies Paramètres du logiciel Paramètres du logiciel Préférences Modèles d'administration : définitions de stratégies Paramètres du logiciel Paramètres Windows Paramètres Windows Préférences 	Sélectionnez un élément pour obtenir une description.

Stratégie Ordinateur, Utilisateur:

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

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

🖃 👰 Configuration ordinateur
🕀 🚞 Stratégies
🕀 🚞 Préférences
🖃 🕵 Configuration utilisateur
🕀 🚞 Stratégies





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

Propagation Stratégies de Domaine :

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

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

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

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

Sous Windows Seven - XP

Gpupdate /force

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

Par exemple

effectivement, dans le journal on peut observer

F	ropriétés de	e Événement			? ×
	Événement				
	Date : Heure : Type : Utilisateur : Ordinateur	16/12/2002 21:20 Informations N/A : CLIENT1R1	Source : Catégorie : ID événement :	SceCli Aucun 1704	 ↑ ↓ □ □
	Description La stratégi correcteme	i : le de sécurité da ent.	ans les objets Stra	tégie de groupe	est appliquée

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

Sous Windows 2000 :

Secedit /refreshpolicy machine_policy



Et / ou



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

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

Gpupdate



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

Syntaxe

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

/target:{ordinateur|utilisateur}

Permet de traiter uniquement les paramètres de l'ordinateur ou les paramètres de l'utilisateur courant. Par défaut, sont traités à la fois les paramètres de l'ordinateur et de l'utilisateur.

/force

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

/logoff

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

/boot

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

L'utilitaire en ligne Secedit (2000)

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



Actualiser les paramètres de sécurité

secedit /refreshpolicy

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

Syntaxe

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

Parameters

stratégie_ordinateur

Actualise les paramètres de sécurité pour l'ordinateur local.

stratégie_utilisateur

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

/enforce

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

Gestion Propagation des Stratégies de Domaine :

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

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



Stratégie de groupe : Intervalle d'actualisation...



Intervalle d'actualisation de la stratégie de groupe pour les ordinateurs Intervalle d'actualisation de la stratégie de groupe pour les contrôleurs de domaine

Non erreur doc:

machine policy

Non erreur doc:

user_policy

Donnant





Intervalle d'actualisation de la stra	tégie de grou égie de group	upe pour les ordinateurs
Paramètre précédent Paramètre :	suivant	
 Non configuré Commentaire : Activé Désactivé Pris en charge sur 	· Au minin	num Windows 2000
Options :	1	Aide :
Ce paramètre vous permet de personnal fréquence d'application de la stratégie o aux ordinateurs. L'étendue est comprise 64 800 minutes (45 jours). Minutes : 90	iser la le groupe entre 0 et	Spécifie la fréquence de mise à jour de la stratégie de groupe pour les ordinateurs pendant que l'ordinateur est en cours d'utilisation (en tâche de fond). Ce paramètre spécifie une fréquence de mise à jour en tâche de fond uniquement pour les stratégies de groupe du dossier Configuration ordinateur. En plus des mises à jour en tâche de fond, la stratégie de groupe pour l'ordinateur est toujours mise à jour au démarrage du système.
Cette durée aléatoire est ajoutée à l'inter d'actualisation pour éviter que tous les clients effectuent des requé stratégie de groupe en même temps. L'étendue est comprise er 440 minutes (24 heures) Minutes : 30	valle ites de itre 0 et 1	Par défaut, la stratégie de groupe de l'ordinateur est mise à niveau en tâche de fond toutes les 90 minutes avec un décalage aléatoire compris entre 0 et 30 minutes. Vous pouvez spécifier une fréquence de mise à jour comprise entre 0 et 64 800 minutes (45 jours). Si vous sélectionnez 0 minute, l'ordinateur tente de mettre à jour la stratégie de groupe toutes les 7 secondes. Cependant, des intervalles de mise à jour trop courts ne sont pas recommandés pour la plupart des installations car les mises à jour peuvent interférer sur le travail de l'utilisateur et

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

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

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

Ordinateur / Stratégies / Modèles d'administration /	🖃 👰 Configuration ordinateur
Svetème	🖃 🧮 Stratégies
Oysteme	표 🚞 Paramètres du logiciel
	🛨 🚞 Paramètres Windows
	🖃 🚞 Modèles d'administration : déf
	🕀 🚞 Composants Windows
	📔 Imprimantes
Mais là an trauva taut un naquat de stratégies :	🕀 🚞 Panneau de configuration
Mais la officione tout off paquet de situlegies.	🕀 🧰 Réseau
🗄 Autoriser la stratégie utilisateur et les profils itinérants entre les forêts	🖃 🚞 Système
Traitement de la stratégie d'installation de logiciel	
Traitement de la stratégie de quota de disque	
Traitement de la stratégie de récupération EFS	
Traitement de la stratégie de redirection de dossier	
📰 Traitement de la stratégie de maintenance Internet Explorer	
Traitement de la stratégie de sécurité IP	
🧾 Traitement de la stratégie du Registre	
📰 Traitement de la stratégie de scripts	
E Traitement de la stratégie de sécurité	
📰 Traitement de stratégie de réseau câblé 🛛 🎋	
📰 Traitement de la stratégie sans fil	

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



définition

Traitement de l	a stratégie de sécurité		Paramètre précédent Paramètre suivant
			Palanetic precedent
🔿 Non configuré	Commentaire :		2
Activé		L	
Désactivé			2
	Pris en charge sur :	Au minimu	um Windows 2000 🔄
		1	
ptions :			Aide :
Traiter même si groupe n'ont pa	les objets de stratégie d Is été modifiés	e	cocher proposées pour modifier les options. Si vous désactivez ce paramètre ou ne le configurez pas, il n'a aucun effet sur le système. L'option « Ne pas appliquer lors d'un traitement en arrière-plan régulier » empêche l'ordinateur de mettre à jour les stratégies concernées lorsqu'il est sollicité. Lorsque les mises à jour en tâche de fond sont désactivées, les changements de stratégie ne sont appliqués que lors de la prochaine ouverture de session ou du prochain redémarrage du système.
		R	pas été modifiés » met à jour et applique à nouveau les stratégies même si celles-ci n'ont pas été modifiées. De nombreuses implémentations de stratégie spécifient qu'elles sont mises à jours uniquement lorsqu'elles ont été modifiées. Vous pourriez toutefois souhaiter mettre à jour des stratégies inchangées, comme par exemple appliquer à nouveau un paramètre souhaité

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

Exemple : Attribution droits Utilisateur Modifier l'heure système :

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

Fichier Action Affichage ?	The second s		
🧼 🧼 🖄 📰 🗶 🖻 🔒 🔟 🗊			
🔒 Paramètres de sécurité	Stratégie	Paramètre de sécurité	^
 Kratégies de comptes Stratégies locales Stratégie d'audit 	Interdire l'ouverture de session en tant que tâche Interdire l'ouverture de session par les services	1	
🔀 Attribution des droits utilisateur	Interdire l'ouverture d'une session locale	Invite	- 1
Options de sécurité	Modifier l'heure système	SERVICE LOCAL, Administrateurs	

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

🔁 Paramètres de sécurité 📃 🔺	Stratégie 🛆	Paramètre de sécurité
	BMOdifier les valeurs d'env. de microprogrammation	Administrateurs
E- B Stratégies locales	Modifier l'heure système	Administrateurs, Utilisateurs avec pouvoir
	😼 Optimiser les performances système	Administrateurs
Attribution des droits utilisateur	Contimiser un processus unique	Administrateurs. I Itilisateurs avec nouvoir

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







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



On modifie donc la Default Domain Policy



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

🗊 Éditeur de gestion des stratégies de groupe		
Fichier Action Affichage ?		
🗢 🔿 🖄 🔜 💥 🗐 🌛 🛛 🖬		
🧾 Stratégie Default Domain Policy [SRV-2008.FORMATION.EL	Stratégie 🔺	Paramètres de stra
🖃 👰 Configuration ordinateur	B Emprunter l'identité d'un client après l'authentification	Non défini
🖃 🚞 Stratégies	B Forcer l'arrêt à partir d'un système distant	Non défini
🕀 🚞 Paramètres du logiciel	💹 Générer des audits de sécurité	Non défini
🖃 🚞 Paramètres Windows	Gérer le journal d'audit et de sécurité	Non défini
	Interdire l'accès à cet ordinateur à partir du réseau	Non défini
Scripts (démarrage/arrêt)	Interdire l'ouverture d'une session locale	Non défini
🖃 🚡 Paramètres de sécurité		Non défini
E Stratégies de comptes	Interdire l'ouverture de session en tant que tâche	Non défini
🖃 📺 Stratégies locales	Interdire l'ouverture de session par les services Bureau à distance	Non défini
표 📺 Stratégie d'audit	Modifier l'houre quetème	FORMATIONIbab
Attribution des droits utilisateur		
① Options de sécurité	Modifier les valeurs de l'environnement du microprogramme	Non defini

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

🚡 Stratégie de sécurité locale			
Fichier Action Affichage Image: State of the state			
🚡 Paramètres de sécurité	Stratégie	Paramètre de sécurité	*
 La Stratégies de comptes Stratégies locales Stratégie d'audit 	Interdire l'ouverture de session	T-1024.2	
强 Attribution des droits utilisateur	Modifier l'heure système	SERVICE LOCAL FORMATION bob	
 Detions de sécurité Pare-feu Windows avec fonctions avantes 	Modifier les valeurs de l'environ	Administrateurs	

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



http://www.cabare.net Page 29 - Michel Cabaré -

 Paramètres de sécurité Guis Stratégies de comptes Guis Stratégies locales Guis Stratégie d'audit Guis Attribution des droits utilisateur 	Stratégie Stratégie Modifier les valeurs d'env. de micr Modifier l'heure système Optimiser les performances système Montimiser un processus unique	Paramètre de sécurité Administrateurs MANUEL\bob Administrateurs Administrateurs			
Avec bob uniquement					
Propriétés de Modifier l'he	eure système 🛛 ?	×			
Paramètre de sécurité locale					
Modifier l'heure systè	ème				
MANUEL\bob					
		📃 en grisé			

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

Arbre	e		Stratégie 🔺		Paramètre local		Paramètre	en cours
🔁 Pa	, aramètres	de sécurité	Gérer le journal d'a	audit et de sécurité	Administrateurs		Administrat	eurs
÷	🙆 Stratégi	ies de comptes	Modifier les valeur	s d'env. de micr	Administrateurs		Administrat	eurs
ė	📴 Stratégi	ies locales	Modifier l'heure sy	stème	Utilisateurs avec pouvo	oir,Administrateurs	MANUEL\bo	ob
Ē	🗄 🛄 Stra	atégie d'audit	Optimiser les perfo	ormances système	Administrateurs		Administrat	eurs
	🔤 Attr	ibution des droits utilisateur	Dptimiser un proce	essus unique	Utilisateurs avec pouvo	oir, Administrateurs	Utilisateurs	avec po
Ave	ec bo Pat	b uniquement ramètre de stratégie de Modifier l'heure s	sécurité locale ystème		? ×			
Pas de changement localement	, _^	attribué à Par MANUEL\bob Administrateurs Utilisateurs avec pouvoir	Local ramètre de stratégie 2 2 2	Effectif Paramètre de strat	égie	Mais ici récupéré stratégie domaine	on	a la de



E

STRATEGIES CONTROLEUR DE DOMAINE

Stratégies de Contrôleur de Domaine :

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

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



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

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

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

🖥 Stratégie de sécurité locale <u>_ | ×</u> Fichier Action Affichage ? 🗢 🔿 | 🚈 🖬 🖌 📰 😹 🛛 🗾 📁 🚡 Paramètres de sécurité Paramètre de sécurité Stratégie 4 🕀 📑 Stratégies de comptes 💹 Interdire l'ouverture de session en tant que service 🖃 📆 Stratégies locales 🛞 Interdire l'ouverture de session en tant que tâche 🗄 📴 Stratégie d'audit 📖 Interdire l'ouverture de session par les services Bureau à distance Attribution des droits u + SERVICE LOCAL, Administrateurs, Opérateurs de serveur Modifier l'heure système options de sécurité Modifier les valeurs de l'environnement du microprogramme Administrateurs

En fait la Défault Domain Controller policy est active...

Stratégies - GPO 2008

- SYS 26- Cours - ver 2.0 -

Éditeur de gestion des stratégies de groupe			
Fichier Action Affichage ?			
Stratégie Default Domain Controllers Policy [SRV-2008.F	Stratégie 🔺	Paramètres de stratégie	
Configuration ordinateur Stratégies Stratégies Paramètres du logiciel Paramètres Windows Stratégie de résolution de noms Stratégie de résolution de noms Stratégies de sécurité Stratégies de comptes	Forcer l'arrêt à partir d'un système distant Générer des audits de sécurité Gérer le journal d'audit et de sécurité Interdire l'accès à cet ordinateur à partir du réseau Interdire l'ouverture d'une session locale Interdire l'ouverture de session en tant que service Interdire l'ouverture de session en tant que tâche Interdire l'ouverture de session en tant que tâche	Administrateurs,Opérateurs de serveur SERVICE LOCAL,SERVICE RÉSEAU Administrateurs Non défini Non défini Non défini Non défini	
① ① Stratégie d'audit ① ② Stratégie d'audit ① ③ Attribution des droits utilisateur ③ ④ Options de sécurité	Modifier I heure système Modifier les valeurs de l'environnement du microprogramme Modifier un nom d'objet	SERVICE LOCAL, Administrateurs, Opérateurs Administrateurs Non défini	de serveur



Modifier la Stratégie des Contrôleur de Domaine :

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



On demande Modifier... la Default Domain Controllers policy

Exemple : Attribution droits Utilisateur Modifier l'heure DC :

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

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

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



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



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





Vérification :

Sur le serveur de Domaine 2008 les stratégies locales montrent bien

🚪 Stratégie de sécurité locale		
Fichier Action Affichage ?		
🗢 🔿 🔁 🔐 💥 🗎 🗟 🔽 🖬		
🖥 Paramètres de sécurité	Stratégie 🔺	Paramètre de sécurité
🗉 📴 Stratégies de comptes	🖾 Interdire l'ouverture de session en tant que tâche	
🖃 📴 Stratégies locales	💹 Interdire l'ouverture de session par les services Bureau à distance	
🕀 📑 Stratégie d'audit	Modifier l'heure système	SERVICE LOCAL, marie, Administrateurs, Opérateurs de serveur
Attribution des droits utilisateur	🚰 Modifier les valeurs de l'environnement du microprogramme	Administrateurs
Options de sécurité	🔯 Modifier un nom d'objet	
🖽 🧮 Pare-feu Windows avec fonctions avancé	and thomas at thomas object	
Stratégies du gestionnaire de listes de réc	Ouvrir une session en tant que service	NT SERVICE VALL SERVICES
Stratégies de dé publique	Ouvrir une session en tant que tâche	Administrateurs,Opérateurs de sauvegarde,Utilisateurs du jou
Stratégies de restriction logicielle	Performance système du profil	Administrateurs
Stratégies de contrôle de l'application	Permettre à l'ordinateur et aux comptes d'utilisateurs d'être appr	Administrateurs
F R Stratégies de sécurité IP sur Ordinateur le	Permettre l'ouverture d'une session locale	marie, Administrateurs, Opérateurs de compte, Opérateurs de s
Configuration avancée de la stratégie d'a	📰 Prendre possession de 🕅 hiers ou d'autres objets	Administrateurs
	🚰 Processus unique du profil	Administrateurs

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

🚡 Paramètres de sécurité du contrôleur de domaine par défaut				
Eichier Action Affichage ?				
📄 Paramètres Windows 🔺	Stratégie 🛆	Paramètres de stratégie		
🗐 Scripts (démarrage/arrêt)	Modifier les valeurs d'env. de microprogram	Administrateurs		
🖃 😳 Paramètres de sécurité	BU Modifier l'heure système	Administrateurs, MANUEL\marie, Opérateurs de se		
Stratégies de comptes	Optimiser les performances système	Administrateurs		
🖻 🚽 🛃 Stratégies locales	Optimiser un processus unique	Administrateurs		
⊡ 🛃 Stratégie 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 sécurité	Ouvrir une session en tant que tâche			
⊡ grounes restreints	Permettre l'ouverture d'une session locale	Administrateurs, MANUEL\marie, Opérateurs de co 🗲		

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

Paramètre de stratégie de sécurité locale ? 🔀					
Modifier l'	heure système				
Attribué à	Local Paramètre de stratégie	Effectif Paramètre de stratégie			
Opérateurs de serve DOMAINE1\marie Administrateurs Utilisateurs avec po	eur 🔲				





Pa	Paramètre de stratégie de sécurité locale					
	<u>e</u>	rir une session loca	lement			
	Attribué à	L Paramètre	.ocal e de stratégie	Effectif Paramètre de stra	atégie	
	Opérateurs d'in	npression		~		
	Opérateurs de	serveur		\checkmark		
	Opérateurs de	compte		\checkmark		
	IUSR_SERVE	UR		\checkmark		
	DOMAINE1\m	arie		~		
	DOMAINE1\IU	JSR_SERVEUR	\checkmark			

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





STRATEGIES ET PREFERENCES

Les préférences 2008 Serveur :

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



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

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

□ Préférences
 ① Paramètres Windows
 ① Paramètres du Panneau de configuration

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

Les préférences sont nombreuses



Stratégies - GPO 2008

- SYS 26- Cours - ver 2.0 -



Client Side Extension pour XP SP2 & Vista:

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

XP SP2

Détails rapides				
Nom du fichier:	Windows-KB943729-x86-FRA.exe			
Version:	943729			
Articles de la base de connaissances (KB) (en anglais) :	<u>KB943729</u>			
Date de publication :	10/11/2009			
Langue:	Français			
Taille du téléchargement:	690 Ko			
Durée de téléchargement estimée:	Accès distant (56 K) 💌 2 min			

Vista

Détails rapides	
Nom du fichier:	Windows6.0-KB943729-x86.msu
Version:	943729
Articles de la base de connaissances (KB) (en anglais) :	<u>KB943729</u>
Date de publication :	23/06/2009
Langue:	Français
Taille du téléchargement:	521 Ko
Durée de téléchargement estimée:	Accès distant (56 K) 💌 2 min

Principales Préférences Ordinateur :



Principales Préférences Utilisateur :




Mappages de lecteurs

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

Fichiers

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

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

Dossiers

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

Raccourcis

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

Périphériques

Possibilité d'activer ou désactiver des périphériques à distance soit au niveau ordinateur soit au niveau utilisateur. Vous pouvez agir soit au niveau d'une classe (ensemble d'objets) soit directement au niveau d'un objet. (pour couper l'accès au graveur de CD, désactiver les connexions sans fil.)

Option des dossiers

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

Utilisateurs et groupes locaux

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



Imprimantes

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

menu Démarrer

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

Services

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

Options Communes des Préférences :

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



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

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

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

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

Appliquer une fois et ne plus réappliquer :

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





préférences, celles-ci seront remodifiées par la stratégie. Pour éviter ce comportement, cochez cette case pour que la stratégie ne s'applique qu'une seule fois.

Ciblage au niveau de l'élément :

Ciblage au niveau de l'élément	Ciblage
--------------------------------	---------

Permet de construire une requête...



Avec pas mal de choix...





MODELE DE STRATEGIES

Les modèles de stratégie de sécurité:

N.B: La notion existe déjà sous NT4 avec les fichiers Ntconfig.pol, que l'on créait avec le poledit de NT, voire sous win95-98 avec les fichiers Config.pol que l'on créait avec le poledit de windows...
on peut continuer à s'en servir en placant ces fichiers dans

on peut continuer à s'en servir en plaçant ces fichiers dans **SYSVOL\Sysvol\domaine\Scripts**...(là où l'on met les scripts de connexion)

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

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

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



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

	×	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
庄 🔄 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
		🗟 hisecws.inf	18 Ko	Informations de configuration	16/12/1999 02:15
⊡ system32		🗟 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
		📓 setup security.inf	511 Ko	Informations de configuration	15/10/2001 17:45



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

💼 defltbase.inf		13/07/2	009 22:28	Informatio	ons de con	48 Ko
all defltdc.inf		13/07/2	009 22:28	Informatio	ons de con	82 Ko
💼 defltsv.inf		13/07/2	009 22:28	Informatio	ons de con	48 Ko
Fichier Ed Fichier Ed Copyr Secur Templ Templ Defau [Profil %SCEDef	se.inf-Bloc-notes tion Format Affichage ight (c) Microso ity Configuratio ate Name: ate Version: lt Security For e Description] ltSVProfileDescu	oft Corporation. on Template for Se DefltSV.INF 05.10.DS.0000 Windows VISTA Ser	All right curity Co ver.	ts reserved. onfiguration	Editor	
signatu revisio DriverV	"="\$CHICAGO\$" n=1 er=06/21/2006,6.	1.7600.16385				

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



Il va falloir :

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

Création d'un modèle:



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



		🚡 Console1 - [Racine de la	console\Modèles	de sécurité\E:\WIM	NT\Security\Templates]
Clic droit	sur le	🚰 Console Fenêtre <u>?</u>			
dossier	dans	Action Affichage Eavori	s] ⇐ ⇒ €		?
lequel	les	Arbre Favoris		Nom	Description
modèles	sont	Racine de la console		Basicdc	Paramètres de sécurité pa
stockés		Configuration et analyse	e de la sécurité	basicsv	Paramètres de sécurité pa
		🖻 📴 Modèles de sécurité		Dasicwk	Paramètres de sécurité pa
			Cuvrii		suppose que les fichiers e
puis			Nouvea	au modèle	te les paramètres
Nouveaum	 aláhor				
Nouveau II					
			E:\WINNT\Secu	irity\Templates	? ×
			Nom du modèle	:	
			test		
			Description :		
			essais formation	n	
	ete	on lui donne un nom		1	
On d	obtient alc	ors notre modèle de sé	curité	Modèles de s Modèles de s Modèles de s Siwinn Modèles de s Siwinn Siwinnn Siwinn Siwinn Siwinnn Siwinnn S	sécurité T\Security\Templates :sv :sv :wk batws :dc :ws :ss :ss :ss :ss :ss :ss :ss :ss :ss
Dan sécu locc	s lequel c urité que 11, (ainsi qu	on reconnaît les parai l'on modifiait aupar ie les autres) ———	mètres de avant en		lournal des événements Groupes restreints Gervices système Registre Système de fichiers

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 Non défini

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







Création d'une base locale de sécurité:

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

Configuration sécurité —	et analyse	de la ──►	Ajout d'un composant logiciel enfichab Composants logiciels enfichables disponible	ole autonome ? X
			Composant logiciel enfichable	Vendeur 🔺
			🗐 Certificats	Microsoft Corporation
			Configuration et analyse de la sécurité	Microsoft Corporation
			📸 Contrôle ActiveX	
			🍓 Contrôle WMI	Microsoft Corporation
			💕 Défragmenteur de disque	Executive Software Inte
			Dossier 📃	
			😡 Dossiers partagés	Microsoft Corporation
			🔊 Fax Service Management	Microsoft Corporation
Cette console	permet d'ou	vrir une	Description	
base de donn manipuler) ou	ée existante en crée une r	(pour la 10uvelle	Configuration et analyse de la sécurité es enfichable MMC qui permet la configurati les ordinateurs Windows qui utilisent les f	t un composant logiciel on et l'analyse de sécurité sur ichiers de modèle de sécurité.

à l'aide d'un modèle... Pour ouvrir une base de donnée

existante

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

Configuration et analyse de la sécurité Ouvrir

Ouvrir une base de données...

Analyser l'ordinateur maintenant...

Configurer l'ordinateur maintenant...

2

Nous avons besoin de la créer donc on va

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

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

Vérification modèle - poste:

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

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 ?					
<u>A</u> ction Affichage Eavoris $\Box \Leftrightarrow \Rightarrow$					
Arbre Favoris	Stratégie 🛆	Paramètre de base	Paramètre de l'ordin		
Racine de la console	Arrêter 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	Auditer 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 com	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		
Hard Groupes restreints	Contenu du message pour les utilisateurs essayant de	super,bravo !	+		
E Consistent	🕮 Créer un fichier d'échange de mémoire virtuelle lors de	Non défini	Désactivé		
En Custème de fichiers	BDésactiver la combinaison de touches Ctrl+Alt+Suppr	Non défini	Non défini		
Emiliar Systeme de fichiers		NILL 320:1:	4 m:		

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

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

Application du modèle sur le poste

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



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

Modification du modèle

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

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

Assistant 2008 et Modèles pré définis

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

	-
Vous pouvez créer une nouvelle stratégie de sécurité, modifier ou appliquer une stratégie de	
sécurité existante, ou annuler la dernière stratégie de sécurité appliquée.	
Sélectionnez l'action que vous voulez effectuer :	
• Créer une nouvelle stratégie de sécurité	
C Modifier une stratégie de sécurité existante	
O Appliquer une stratégie de sécurité existante	
O Annuler la dernière stratégie de sécurité appliquée	





http://www.cabare.net Page 44 - Michel Cabaré - Les modèles de sécurité prédéfinis sous 2003 SRV et client XP sont :

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

(Setup security.inf),

Les modèles de sécurité prédéfinis sous 2000 sont :

٠	Station de travail par défaut	(basicwk.inf)
٠	Serveur par défaut	(basicsv.inf)
٠	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)
		$(l_{1}, l_{2}, \ldots, l_{n}, l_{n}, l_{n}, l_{n})$

Contrôleur de domaine hautement sécurisé (hisecdc.inf)

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

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

Résumé

- On se: crée un modèle xxxxx.inf (rien ne se passe)
 - On ouvre/crée une base de donnée xxxx.sdb (rien ne se passe)
 - On importe un modèle (rien ne se passe)
 - On analyse différence entre base et registre (rien ne se passe)
 - On configure le poste (on modifie la base de registre)
- N.B: à partir du moment ou l'on a configuré le poste, la base contient des informations différentes du modèle utilisé, car elle est un résultat de (modèle+registre). Dans le doute, refaire une base avec une copie propre du modèle et recommencer. A la limite, appliquer le modèle de sécurité de base, puis ré appliquer le modèle spécifique
- N.B: Faire attention aux modèles dans lesquels on ne spécifie rien pour une clé, cela ne rétablira pas la clé dans sa valeur par défaut, mais cela la laissera en l'état
- N.B: Faire attention à appliquer des modèles construits sur un OS même 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

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



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

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

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

 Stratégie Nouvel objet de stratégie de groupe Me Configuration ordinateur 	📕 Stratégie Nouvel objet de strat	égie de groupe [SRV-2008.FORMATION.EDU]
	Sélectionnez un élément pour obtenir une	Nom
Configuration utilisateur	description.	Configuration ordinateur
🕀 🚞 Stratégies		So comgaradon daisateur

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



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

- les stratégies de groupe pour les ordinateurs s'exécutent avant que le message de bienvenue dans windows ne s'affiche.
- les stratégies de groupe pour les utilisateurs s'exécutent avant que l'interpréteur de commande du système ne soit activé et mis à la disposition de l'utilisateur.
- Les questions de propagations sont les mêmes que pour les stratégies de Domaine
 - **N.B:** Dans le cas ou l'on définirait des stratégies contradictoires, il faut savoir que normalement les stratégies ordinateurs prennent le pas sur les stratégies utilisateurs.

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

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



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

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



- N.B: les scripts qui sont gérés par les stratégies ne sont pas récupérés par les clients antérieurs à windows 2000
- N.B: Dans une stratégie on peut au niveau de ses propriétés invalider la catégorie que l'on ne pense pas utiliser (amélioration de la vitesse de connexion)

Désactivation
Pour améliorer les performances, utilisez ces options pour désactiver les composants inutilisés de l'objet Stratégie de groupe.
 Désactiver les paramètres de configuration de l'ordinateur Désactiver les paramètres de configuration de l'utilisateur





Niveau de modification dans la base de registre

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

HKEY_LOCAL_MACHINE Et HKEY_CURRENT_USER

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

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

Créer une Stratégie de Groupe:

Cela repose sur 3-4 étapes

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

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



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

strat = stratégie	Nouvel objet GPO
pref = préférence	Nom :
o = ordinateur	Nouvel objet de strategie de groupe
\mathbf{u} = utilisateur	Objet Starter GPO source : (aucun)
et on la modifie clic – droit / Modifier N.B : les tp suivant porteront sur l "contenu" d'une stratégie	C C C C C C C C C C C C C C C C C C C



Lier une Stratégie de Groupe sur une U.O :

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

A Forêt : formation.edu						
E i formation.edu						
Default Domain Policy						
🛨 🖬 Domain Controllers						
🖬 test						
🖃 📑 Obj 🛛 Créer un objet GPO dans ce domaine, et le lier i						
Lier un objet de stratégie de groupe existant						
Bloquer l'héritage						

Tous les objets apparaissent

Dbjets de stratégie de groupe : Nom ▲ Default Domain Controllers Policy Default Domain Policy Nouvel objet de stratégie de groupe Nouvel objet de stratégie de groupe	1	Concelling a de	
Dbjets de stratégie de groupe : Nom Default Domain Controllers Policy Default Domain Policy Nouvel objet de stratégie de groupe Rodin andie andie andie andie andie		formation.edu	_
Nom Default Domain Controllers Policy Default Domain Policy Nouvel objet de stratégie de groupe	Obiets	s de stratégie de groupe :	
Nom Default Domain Controllers Policy Default Domain Policy Nouvel objet de stratégie de groupe Stratégie de groupe		· · · · · · · · · · · · · · · · · · ·	
Default Domain Controllers Policy Default Domain Policy Nouvel objet de stratégie de groupe		Nom 🔺	
Default Domain Policy Nouvel objet de stratégie de groupe		Default Demain Controllere Deliny	
Nouvel objet de stratégie de groupe		Default Domain Controllers Policy	
and ant antian man harmy w		Default Domain Controllers Policy Default Domain Policy	
pret - ordi - gestion users locaux (1)		Default Domain Controller's Policy Default Domain Policy Nouvel objet de stratégie de groupe	
		Default Domain Controller's Policy Default Domain Policy Nouvel objet de stratégie de groupe pref - ordi - gestion users locaux pref - ordi - crer dossier et ciblage os-systeme	

Et un pointeur (indiquant un lien) se crée :



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





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

E	 test Nouvel objet de stratégie de groupe stratégie de groupe 1 stratégie de groupe 2 Objets de stratégie de groupe Default Domain Controllers Policy Default Domain Policy Nouvel objet de stratégie de groupe
Gestion	des stratégies de groupe
	Voulez-vous supprimer cet objet de stratégie de groupe et tous ces liens dans ce domaine ? Cela ne va pas supprimer les liens dans d'autres domaines. Oui Non

Modifier État GPO
Sauvegarder Restaurer à partir d'une sauvegarde Importer des paramètres Enregistrer le rapport
Nouvelle fenêtre à partir d'ici
Copier
Supprimer
Renommer 5
Actualiser

(par défaut NON)

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

Vérification des éléments de l'UO:

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

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



Et de même un compte ordinateur...



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



Vérification et utilitaire Gpresult.exe

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

Depuis Xp Sp3, (natif) et 2000 avec le Kit de ressource technique, appel par la ligne de commande **gpresult.exe**

🕅 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 comput	ter.			
usage: gpresult [/V] [/S] [/C /U] [/?]				
<pre>/V Verbose mode /S Super verbose mode /C Computer settings only /V User settings only</pre>				

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

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

C:\Users\Administrateur>gpresult /r
Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0 Copyright (C) Microsoft Corp. 1981-2001
Jeu créé le 05/01/2010 à 10:46:37
Données RSOP pour FORMATION\administrateur sur SRV-2008 : mode journalisation
Configuration du système d'exploitation : Contrôleur principal de domaine Version du système d'exploitation : 6.1.7600 Nom du site Profil itinérant : N/A Profil local N/A Connexion via une liaison lente ? : Non
Paramètre de l'ordinateur
CN=SRV-2008,OU=Domain Controllers,DC=formation,DC=edu Heure de la dernière application de la stratégie de groupe : 05/01/2010 à 10 :42:09 Stratégie de groupe appliquée depuis : srv-2008.formation.edu Seuil de liaison lente dans la stratégie de groupe : 500 kbps Nom du domaine : FORMATION Type de domaine : Windows 2000

L'option **/V** est très complète...

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





HIERARCHIE DES STRATEGIES

Ordre final d'application des stratégies :

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

- Pour des client SEVEN VISTA XP(PRO) serveur 2000-2003-2008 <u>Hors Domaine</u>: stratégies locales
- Pour des client SEVEN VISTA XP(PRO) <u>En Domaine</u> serveur 2000-2003 <u>membres</u>: stratégies locales / stratégies de domaine et si des GPO sont données sur des UO alors on a stratégies locales / stratégies de domaine / GPO d'UO et si la notion de site est activée stratégies locales / stratégies de site / stratégies de domaine / GPO d'UO
- Pour des serveurs 2000 et 2008 <u>Contrôleurs de Domaine</u>:

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 <u>Contrôleurs de Domaine</u>: (les stratégies locales sont dévalidées, pour les manipuler il faut passer par secpol.msc /s)

stratégies de domaine / stratégies de CD

et si la notion de site est activée

stratégies de site /stratégies de domaine / stratégies de CD

- N.B: toutes les stratégies définies par défaut dans la GPO de domaine, s'appliquent à la GPO des Contrôleurs de Domaine. SI ON VEUT QUES LES STRATEGIES DE DOMAINE NE S'APPLIQUENT PAS AUX CD IL FAUT BLOQUER L'HERITAGE
- N.B: Dans le cas ou l'on définirait des stratégies contradictoires, il faut savoir que normalement les stratégies ordinateurs prennent le pas sur les stratégies utilisateurs.



LIAISONS MULTIPLES - PRIORITE -HERITAGE – DES GPO

Liaison de GPO :

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

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

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



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

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



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



Si par exemple on souhaite que la stratégie de groupe 2 soit celle qui prenne le pas sur toutes les autres, alors il faut la passer en ordre 3...

test							
Objets de stratégie de groupe liés Héritage de stratégie de groupe Délégation							
[Ordre des liens 🔺	Objet de stratégie de groupe	Appliqué	Lien activé	État GPO		
会	1	🛒 stratégie de groupe 1	Non Non	Oui Oui	Activé Activé		
	2	📰 stratégie de groupe 2					
	3	🛒 Nouvel objet de stratégie de groupe	Non	Oui	Activé		
₹¢	éplacer le lien vers le ba	IS					

Pour obtenir

	Ordre des liens 🔺	Objet de stratégie de groupe	Appliqué	Lien activé	État GPO
\cong	1	🛒 stratégie de groupe 1	Non	Oui	Activé
	2	🛒 Nouvel objet de stratégie de groupe	Non	Oui	Activé
	3	🚮 stratégie de groupe 2	Non	Oui	Activé

héritage - bloqué :

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

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

-	1	formation.edu
		🛒 Default Domain Policy
	+	💼 Domain Controllers
	+	production
	-	💼 test
		🛒 Nouvel objet de stratégie de groupe
		🛒 stratégie de groupe 1
		🛒 stratégie de groupe 2
		_

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



Et ainsi de suite



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



http://www.cabare.net Page 54 - Michel Cabaré - Donc, lorsque l'on crée des **UO**, les **GPO** s'appliquent de manière hiérarchique.

Utilisateurs et ordinateurs Active Directo domaine2.edu 	ory Ur do	n él onc	ément plac ici :	:é d	ans l'UO vr	p re	∍çoit
⊡ ⊡ Computers ⊡ Ø Domain Controllers	\backslash	•	la GPO de	dor	naine par d	éfa	ut
ForeignSecurityPrincipals		•	La GPO existe)	de	Personnel	(si	elle
⊡		•	La GPO de exemple c	elle	o et celles li de comme	ées rcia	(par ux

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</u> <u>priment</u> ! mais cela doit être vérifié dans les explications des propriétés...

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



par exemple sur l'UO test

Cela se traduit par un Point d'exclamation !



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



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



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

héritage - appliqué:

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

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



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



Cela se traduit par un Cadenas!



Nouvel objet beta de stratégie de groupe

Appliqué

demande

On se place dessus et on

clic-droit

	in Nouver objet beta de strateg	le	ae g	roupe	
Et l''on voit bien que la stratégie				de nouveau	propagée
	 formation.edu Default Domain Policy Domain Controllers production test Nouvel objet de stratégie de groupe stratégie de groupe 1 stratégie de groupe 2 		Cette	liste n'inclut aucun ol nté ^ 1 (appliqué) 2	 Objet de stratégie de groupe lié à des sites. Pour obter Objet de stratégie de groupe stratégie de groupe 2 Nouvel objet beta de stratégie de groupe
	🗖 🚟 beta	11			

On peut procéder de même pour la Default Domain Policy...



Cette liste n'inclut aucun objet de stratégie de groupe lié à des sites. Pour ob

Priorité 🔺			Objet de stratégie de groupe
	-	1 (appliqué)	Default Domain Policy
	7	2 (appliqué)	stratégie de groupe 2
	T	3	Nouvel objet beta de stratégie de groupe



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

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

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

priétés de commerciaux	? ×	
âénéral Géré par Stratégie de	e groupe	
Liaisons de l'objet St commerciaux	Stratégie de groupe actuel pour	
Liaisons de l'objet Stratégie de	e groupe Ne pas passer outre Désactivé	
🕵 🖞 pour commerciaux	✓	
are pour commerciaux	· · · · · · · · · · · · · · · · · · ·	





GESTION ET SAUVEGARDE DES GPO

Résumé de la stratégie :

Il est possible d'avoir une idée (documentation) de ce que fait une stratégie. Cela se demande sur une **GPO** via le bouton droit : **Enregistrer le rapport...**

	formation.edu <mark>ﷺ Default Domain Policy ⊡ © Domain Controllers Modifier. ① © moduction </mark>			
	test Tratérie de grou	vé rer le rapport.		
	Et on indique ensuite un dos	sier et un nor	n de fichier (au format HTML)	
	Default Domain Controllers Policy.htm	01/12/2009 09:32	Document HTML	
	Default Domain Policy 2.htm	29/12/2009 12:37	Document HTML	
	Default Domain Policy.html	01/12/2009 09:33	Document HTML	
	fermeture de session.htm	28/12/2009 13:03	Document HTML	
	mot de passe simple.htm	29/12/2009 12:49	Document HTML	
	Ces fichiers sont ensuite fac	cilement visu	alisables (a condition d'autoriser	les
				1
	activex sur le navigateur	via sur la droi	te une fonction Afficher / Masque	er I
	activex sur le navigateur)	via sur la droi	te une fonction Afficher / Masque	er
	activex sur le navigateur) mot de passe simple Données recueilles le : 29/12/2009 12:49:28	via sur la droi	te une fonction Afficher / Masque	er afficher tout
	activex sur le navigateur) mot de passe simple Données recueillies le : 29/12/2009 12:49:28 Général	via sur la dro	te une fonction Afficher / Masque	er afficher tout masquer
	activex sur le navigateur) mot de passe simple Données recueillies le : 29/12/2009 12:49:28 Général Détails	via sur la droi	te une fonction Afficher / Masque	er afficher tout masquer afficher
	activex sur le navigateur) mot de passe simple Données recueilles le : 29/12/2009 12:49:28 Général Détails Liaisons	via sur la droi	te une fonction Afficher / Masque	er afficher tout masquer afficher afficher
	activex sur le navigateur) mot de passe simple Données recueilles le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité	via sur la droi	te une fonction Afficher / Masque	er afficher tout masquer afficher afficher afficher
	activex sur le navigateur) mot de passe simple Données recueillies le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation	via sur la dro	te une fonction Afficher / Masque	er afficher tout masquer afficher afficher afficher afficher afficher
	activex sur le navigateur) mot de passe simple Données recueillies le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée)	via sur la droi	te une fonction Afficher / Masque	er afficher tout masquer afficher afficher afficher afficher afficher masquer
,	activex sur le navigateur) mot de passe simple Données recueillies le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies	via sur la droi	te une fonction Afficher / Masque	er afficher tout masquer afficher afficher afficher afficher masquer masquer
	activex sur le navigateur) mot de passe simple Données recueillies le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres Windows	via sur la dro	te une fonction Afficher / Masque	er afficher tout masquer afficher afficher afficher afficher masquer masquer masquer
 ,	activex sur le navigateur) mot de passe simple Données recueilles le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres Windows Paramètres de sécurité	via sur la dro	te une fonction Afficher / Masque	er afficher tout masquer afficher afficher afficher masquer masquer masquer masquer masquer
,	activex sur le navigateur) mot de passe simple Dornées recueilles le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres Windows Paramètres de sécurité Stratégies de comptes/Stratégie de mot de passe	via sur la dro	te une fonction Afficher / Masque	er afficher tout masquer afficher afficher afficher masquer masquer masquer masquer masquer
	activex sur le navigateur) mot de passe simple Dornées recueilles le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres Windows Paramètres de sécurité Stratégie de mot de passe Stratégie	via sur la dro	Paramètre	er afficher tout masquer afficher afficher afficher masquer masquer masquer masquer masquer masquer masquer
	activex sur le navigateur) mot de passe simple Dornées recueilles le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres Windows Paramètres de sécurité Stratégies de comptes/Stratégie de mot de passe Stratégie Artériorité maximale du mot de passe Artériorité minimale du mot de passe	via sur la dro	Paramètre 30 jours 0 jours	er afficher tout masquer afficher afficher afficher masquer masquer masquer masquer masquer
	activex sur le navigateur) not de passe simple Données recueilles le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres de sécurité Stratégies de comptes/Stratégie de mot de passe Stratégie Artériorité maximale du mot de passe Artériorité minimale du mot de passe Appliquel Thistorique des mots de passe Appliquel Thistorique des mots de passe	via sur la dro	Paramètre 30 jours 0 jours 0 jours 0 mots de passe mémorisés	er afficher tout masquer afficher afficher afficher masquer masquer masquer masquer masquer
	activex sur le navigateur) mot de passe simple Dornées recueillies le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres Windows Paramètres de sécurité Stratégie Artériorité maximale du mot de passe Artériorité minale du mot de passe Apliquer l'historique des mots de passe Appliquer l'historique des mots de passe Le mot de passe doit respecter des exigences de compl	via sur la droi	Paramètre 30 jours 0 jours 0 mots de passe mémorisés Désactivé	er afficher tout masquer afficher afficher afficher masquer masquer masquer masquer masquer
	activex sur le navigateur) mot de passe simple Dornées recueillies le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres Windows Paramètres de sécurité Stratégies de comptes/Stratégie de mot de passe Stratégie Artériorité maximale du mot de passe Artériorité minimale du mot de passe Le mot de passe doit respecter des exigences de compl Longueur minimale du mot de passe	via sur la droi	Paramètre 30 jours 0 jours 0 mots de passe mémorisés Désactivé 0 caractères	er afficher tout masquer afficher afficher afficher masquer masquer masquer masquer
	activex sur le navigateur) mot de passe simple Dornées recueilles le : 29/12/2009 12:49:28 Général Détails Liaisons Filtrage de sécurité Délégation Configuration ordinateur (activée) Stratégies Paramètres Windows Paramètres de sécurité Stratégie Artériorité minimale du mot de passe Appliquer l'historique des mots de passe Le mot de passe doit respecter des exigences de compl Longueur minimale du mot de passe Configuration utilisateur (activée)	via sur la droi	Paramètre 30 jours 0 jours 0 mots de passe mémorisés Désactivé 0 caractères	er afficher tout masquer afficher afficher afficher masquer masquer masquer

Copier une stratégie :

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

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



🖃 📑 Objets de stratégie de groupe	
Default Domain Controllers Policy	
🧾 Default Domain Policy	
Nouvel objet beta de stratégie de groupe Nouvel objet de stratégie de groupe pref - ordi - gestion users locaux	1) il faut la sélectionner
pref - ordi - crer dossier et ciblage os- systeme pref - util - mappage sur domaine strat - ordi - mise a l heure - horodatage strat - ordi - mot de passe simple stratégie de groupe 1 stratégie de groupe 2	2) et la faire glisser dans Objets de stratégies de groupe

Alors on réponds

	🛃 Copier l'objet GPO	×
	Spécifier les autorisations pour le nouvel objet GPO :	
	O Utiliser les autorisations par défaut pour les nouveaux objets GPO.	
	C Conserver les autorisations existantes.	
	OK Annuler	
On a c	confirmation, et voila	

Sauvegarder les stratégies :

Le plus simple est de se placer sur le dossier Objets de stratégies de groupe

et demander Sauvegarder tout...



Il faut indiquer un emplacement

🧱 Sauvegarde de l'objet GPO	X
Entrez le nom du dossier où placer les sauvegardes de cet objet GPO. Vo pouvez sauvegarder plusieurs objets GPO dans le même dossier.	IS
Remarque : les paramètres qui sont externes à l'objet de stratégie de grou tels que les filtres WMI et les stratégies IPSec sont des objets indépendan dans Active Directory et ne seront pas sauvegardés.	es, s
Pour éviter toute modification non autorisée des objets GPO sauvegardés veillez à sécuriser ce dossier pour que seuls les administrateurs autorisés puissent écrire à cet emplacement.	
Emplacement :	
F:\partage\exercices	•
Parcou	ir
Description :	
backup stratégies formation	
Sauvegarder Annul	er







Restaurer les stratégies :

Dans la même logique sur le dossier Objets de stratégies de groupe

et demander Gérer les sauvegardes...





Objets GPO sauvega	rdes :	1	1
Domaine A	Nom	Date et heure	Description
formation.edu	Default Domain Controllers Policy	05/01/2010 11:2	backup stratég
formation.edu	Default Domain Policy	05/01/2010 11:2	backup stratég
formation.edu	Nouvel objet beta de stratégie de groupe	05/01/2010 11:2	backup stratég
formation.edu	Nouvel objet de stratégie de groupe	05/01/2010 11:2	backup stratég
🗐 formation.edu	pref - ordi - gestion users locaux	05/01/2010 11:2	backup stratég
🗐 formation.edu	pref - ordi - crer dossier et ciblage os- systeme	05/01/2010 11:2	backup stratég
🗐 formation.edu	pref - util - mappage sur domaine	05/01/2010 11:2	backup stratég
🗐 formation.edu	strat - ordi - mise a l heure - horodatage	05/01/2010 11:2	backup straté
🗐 formation.edu	strat - ordi - mot de passe simple	05/01/2010 11:2	backup stratég
🗐 formation.edu	stratégie de groupe 1	05/01/2010 11:2	backup stratég
🗐 formation.edu	stratégie de groupe 2	05/01/2010 11:2	backup stratég
✓ N'afficher que la €	demière version des objets GPO		

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

🛃 Restaurer	×	
État de la restauration :		
État :		
Nouvel objet de stratégie de groupeOpération réussie	<u> </u>	une confi

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





GPO - MODELES D'ADMINISTRATION

Les Modèles présents

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

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

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

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

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



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



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



Notamment pour cibler un système, et garder que les valeurs Configurées

Sélectionnez le de filtres globa	es options ci-dessous pour ac aux qui seront appliqués aux	ctiver et modifier ou dés : nœuds Modèles d'admi	activer les types histration.		Configuré Oui
Sélectionnez le type de p	paramètres de stratégie à af	fficher.			Oui Non
Géré : Oui	Configuré : Nîmporte le	commer	ntés : rte lequ		
Activer les filtres par	mots dés				
Filtrer par le ou les mots :			Nîmporte laqu	E	
Denc / R. Tite	e param, de stratégie 🔽	Texte d'aide	Commentaire		
Activer les filtres de	conditions	10/00 0 0 00			
Activer les filtres de Sélectionnez le ou les Induez les paramètre	conditions filtres d'application et de pla es qui correspondent à l'une i	teforme souhaités : quelconque des pla			
Activer les filtres de Sélectionnez le ou les Induez les paramètre Orremaille Window Orremaille Window	conditions filtres d'application et de pla es qui correspondent à l'une vs XP KP Service Pack 1	teforme souhaités : quelconque des pla 🔽	Sélectionner tout		
Activer les filtres de Sélectionnez le ou les Induez les paramètre	conditions filtres d'application et de pla es qui correspondent à l'une ws XP KP Service Pack 1 (P Service Pack 2 KP	teforme souhaités : quelconque des pla	Sélectionner tout		
Activer les filtres de Sélectionnez le ou les Induez les paramètre 	conditions filtres d'application et de pla es qui correspondent à l'une e ws XP (P Service Pack 1 (P Service Pack 2) (P err 3.0	teforme souhaités : quelconque des pla 🔽	Sélectionner tout		
Activer les filtres de Sélectionnez le ou les Induez les paramètre Order Famille Window Order Mindows Order Mindows Order Explo Order Mindows Order Order Mindows Order Mindows Ord	conditions filtres d'application et de pla es qui correspondent à l'une e ws XP KP Service Pack 1 KP Service Pack 2 KP rer 3.0 rer 4.0 wer 5.0	teforme souhaités : quelconque des pla 💌	Sélectionner tout		
Activer les filtres de Sélectionnez le ou les Induez les paramètre 	conditions filtres d'application et de pla es qui correspondent à l'une e ws XP (P Service Pack 1 (P Service Pack 2 (P ver 3.0 ver 4.0 ver 5.0 ver 6.0	teforme souhaités : quelconque des pla V	Sélectionner tout		
Activer les filtres de Sélectionnez le ou les Induez les paramètre 	conditions filtres d'application et de pla es qui correspondent à l'une e ws XP CP Service Pack 1 (P Service Pack 2) (P Service	teforme souhaités : quelconque des pla V	Sélectionner tout		

Rappels Méthodologie de mise en œuvre

Il est toujours conseillé de

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





GPO - SCRIPTS

Scripts de démarrage - arrêt - fin de session :

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

Créons nous une stratégie au nom parlant :

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

Stratégies - GPO 2008

- SYS 26- Cours - ver 2.0 -

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



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



http://www.cabare.net Page 64

- Michel Cabaré -

Pour avoir



une

deux

Copier le script dans la GPO : (Afficher...)

depuis la GPO, on demande le bouton Afficher les fichiers.

🕌 Logoff					
Formation.edu * Policies * {F2E5B8F5-DF30-4CB8-	9B80-6CCEA1B33DCB} User Scripts Logoff	•	Recher	cher dans : Logoff	<u> </u>
Organiser 🔻 Nouveau dossier			1		• 🔳 🔞
🗆 🚖 Favoris	Nom ^	Modifié	e le	Туре	Taille
Eureau Emplacements récents	Le d	ossier e	st vide.		

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

					concreter duris i cogori	
Organiser 🔹	 Inclure dans la bibliothèque 	Partager avec 🔻	Graver Nouveau dossier		= -	
	a formation.edu	_	Nom ^	Modifié le	Type Ta	ille
E	DO_NOT_REMOVE_NtFrs_PreIns Dolicies	stall_Directory	🚳 ferme.bat	09/01/2010 17:29	Fichier de command	
		4E42A59FBE2D}				
		00C04fB984F9}				
		C3EBAD5B7F24}				
	⊞ 퉬 {14E2F882-C05E-487E-9A56-6	331C9A2626A3}				
	⊞ 퉬 {31B2F340-016D-11D2-945F-0	00C04FB984F9}				
		49862215AC37}				
		B855E820E21D}				
	🕀 🌗 {567E744D-951F-4768-BF25-1	1C8D70D20344}				
\backslash	∃ {723FA4D5-2E90-4C63-BC2B-	BF7D4D319032}				
\backslash		5C8598C4D796}				
	Hereicking Band Band Band Band Band Band Band Band	54B031E1C5F4}				
	Hereit Big (B70738EA-307B-4C5D-BA35- BA35-	38F71158562F}	v v			
	⊞	6B051C8697E9}				
		E9EE5E8F18C3}				
	E {F2E5B8F5-DF30-4CB8-9B80-6	5CCEA1B33DCB}				
	Machine					
	🗆 🍈 User					
	Documents & Settings		1			
	E 👔 Scripts					
	Logoff					

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



http://www.cabare.net Page 65 - Michel Cabaré -

Utiliser le script dans la GPO (Ajouter...)

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

Propriétés de : Fermeture de session	? ×	
Scripts Scripts PowerShell		
Scripts « Fermeture de sessi	ion » pour « stra-util-script-fin-session »	
Nom Para	mètres	
	Monter	
	Descendre	
	Ajouter	
	Modifier	
	Supprimer	
Pour voir les fichiers de scripts stockés d sur le bouton ci-dessous.	lans cet objet de stratégie de groupe, cliquez	
Afficher les fichiers		
		¥
	Ajout d'u	in Script
	Nom du	script : Parcourir
	Paramèt	
		0K Annuler
		0K. Annuler
via Parcourir on prend	un script parmi ceux	
via Parcourir on prend tant dans la GPO (donc	un script parmi ceux parmi ceux précédemment c	opiés)
via Parcourir on prend tant dans la GPO (donc Parcourir	un script parmi ceux parmi ceux précédemment c	opiés)
via Parcourir on prend tant dans la GPO (donc Parcourir User + Scripts + Lo	un script parmi ceux parmi ceux précédemment c goff 🔹 🔛 Rechercher	Opiés)
via Parcourir on prend tant dans la GPO (donc Parcourir Organiser + Nouveau dossier	un script parmi ceux parmi ceux précédemment c goff • 😰 Rechercher	opiés)
via Parcourir on prend tant dans la GPO (donc Parcourir Organiser - Nouveau dossier Favoris	un script parmi ceux parmi ceux précédemment c goff Rechercher Nom -	Opiés)

Maintenant on a un script de déconnexion....

Propriétés de : l	Fermeture de session	? ×
Scripts Scripts	PowerShell	
Sc.	ripts « Fermeture de session » pour « stra-util-script-fin-session »	
Nom	Paramètres	
ferme.bat	Mont	er
	Descer	ndre



test et visualisation :

Sachant que

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

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

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



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







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

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

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

Image: The second	utilis	ateurs			
	Objet	s de stratégie de groupe lié	es Héritage de stratégie de groupe Dé	élégation	
🛒 stra-util-politique-globale-bureau	1	Ordre des liens 🔺	Objet de stratégie de groupe	Appliqué	Lien activé
stra-util-politique-globale-panneau-conf		1	🛒 stra-util-politique-globale-bureau	Non	Oui
stra-util-politique-globale-win-messenger	<u></u>	2	stra-util-politique-globale-panneau	Non	Oui
stra-util-redirection-dossier		3	stra-util-politique-globale-win-mess	Non	Oui
stra-util-script et ordi-script gestion ouv-ferm session		4	🗊 stra-util-redirection-dossier	Non	Oui
	- ₹	5	🛒 stra-util-script et ordi-script gestion	Non	Oui
 B Objets de stratégie de groupe 		6	🛒 stra-util-script fin-session	Non	Oui

Et dans le bon ordre...



Ľ

GPO - INSTALLATION DE LOGICIELS

Les 3 éléments Winstaller – GPO - AD

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

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

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

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

Windows installer et fichiers msi

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

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

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

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

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

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





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

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

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

Procédure d'installation et de maintenance logiciels

Il va falloir exécuter les étapes suivantes :

- 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.
- 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		侵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, mais cela peut être un emplacement réseau quelconque...

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

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



Attribution - Publication de logiciel

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

Déploiement du logiciel	×
Sélectionnez le type de déploieme	ent:
C Publié	
 Attribué 	
C Avancé	
Sélectionnez cette option pour as modification.	signer l'application sans
	OK Annuler

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			
🖉 <u>C</u> onsole <u>F</u> enêtre <u>?</u>			
Action Affichage ← → € 🖬 × 🖆 🛱 🛱 😰	12000	° 🗟 🐌	
Arbre	bidouilleur 1 objets		
Juliisateurs et ordinateurs Active Directory [serveur2.domaine2.edu]	Nom 🛆	Туре	Description
🗄 🗊 domaine2.edu	📕 client2kp7	Computer	
Ē			
Computers			
🗄 🧭 Domain Controllers			
🗄 📲 ForeignSecurityPrincipals			
🗄 🐼 nouveau			
🗄 🚳 Personnel			
Users			
- Bidouilleur			

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



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

🧾 Stratégie stra-ordi-deploie-office-200	3 [SRV-2008.FORMATION	.EDU]	Nom		Version	État du déploie	Source
🖃 👰 Configuration ordinateur					12	6 - 1 1 1	
🖃 🧮 Stratégies				Aucun e	lement a a	ifficher dans cet ape	rçu.
🖃 🚞 Paramètres du logiciel							
<u> I</u> nstallation de logiciel			L,				
🛨 📔 Paramètres Windows	Nouveau 🕨	Pac	kage				
🛨 🚞 Modèles d'administration :	Affichana N	ichier	7				
🕀 🚞 Préférences	Amenage •		_				

Pour laquelle on demande via un clic droit Nouveau / Package...

et on va

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

on nouveau / r ackage	
Déploiement du logiciel	×
Sélectionnez le type de déploiement :	
O Publié	
Attribué	
C Avancé	
Sélectionnez cette option pour assigner l'application sans modification.	

pour obtenir finalement

🚮 Stratégie de groupe							_ 8 ×
] <u>A</u> ction Affic <u>h</u> age] ⇐ ⇒ 🗗	1						
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							
- Paramètres 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 re-déploiement / désinstallation

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

Arbre		Type de mis	Mise à nive	eau	Paramètre	Source	Modifications
Stratégie msi-spywar 	re [serveur1.dc dinateur ogiciel Windows	Facultatif	Aucun	 Installation Attribuer Publier 	Ereoceic (automatique	\\Serveur1\instal	soft\sna
in modèles d'ad in marchine	ministration lisateur ogiciel		-	Toutes les t Actualiser	âches 🕨 🕨	Attribuer Publier	
Installati ⊕ (Paramètres \ R (Modèles d'ad	on de logiciel Windows		-	Propriétés	;	Supprimer Redéploiemer	nt des applications
et là on peut Suppression	ll choisir de logiciel		? ×	1		1	
Sélectionner	la méthode de supp	ression :					
 Désinstal des ordin 	ler immédiatement le ateurs	logiciel des utilisa	ateurs et				
C Autoriser mais inter	les utilisateurs à con dire de nouvelles ins	tinuer à utiliser le tallations	logiciel,				
)K An	nuler				
Stro	tégies - Cl	2008		http://	www.cab	ara nat D	ago 70


Propriétés de déploiement de logiciel



Donnant

_	Modifications	Sécurité
Général	Déploiement	Mises à niveau
ype de déploieme	ent	
C Publié		
Attribué		
)ptions de déploie	ment	
linstaller autor de fichier	natiquement cette application	en activant l'extension
Désinstaller ce l'étendue de l	ette application lorsqu'elle se t a gestion	trouve en dehors de
Ne pas affich de programme	er de package dans l'applicat es du Bappe at u de configuration	tion Ajout/Suppression
Installer cette	application lors de l'ouverture	en de ceccien





GPEDIT.MSC

Stratégie locale / réseau:

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

ce qui donne ensuite accès aux paramètres suivants :

🖥 Paramètres de sécurité locaux					
Action Affichage $4 \leftrightarrow \rightarrow 12$ 11 \times 12 22					
Arbre	Stratégie 🛆	Paramètre local	Paramètre en cours		
Paramètres de sécurité	Conserver l'historique des mots de passe	0 mots de passe mémorisés	0 mots de passe mé		
🔄 🕮 Stratégies de comptes	BDurée de vie maximale du mot de passe	42 Jours	42 Jours		
庄 💼 Stratégie de mot de passe	BDurée de vie minimale du mot de passe	0 Jours	0 Jours		
🗄 📑 Stratégie de verrouillage du compte	BCLes mots de passe doivent respecter des exigences de co	Désactivé	Désactivé		
🖻 🕮 Stratégies locales	🕮 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 de domaine "locale" :

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

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

📕 Éditeur de stratégie de groupe locale		
Fichier Action Affichage ?		
🗇 🔿 💼 🗎 📄 🖬		
Stratégie Ordinateur local	🧃 Stratégie Ordinateur local	
Paramètres du logiciel Paramètres du logiciel Paramètres Windows Modèles d'administration Modèles d'administration Panneau de configuration Panneau de configuration Réseau Système Système Tous les paramètres Configuration utilisateur Paramètres du logiciel Paramètres Windows Modèles d'administration	Sélectionnez un élément pour obtenir une description.	Nom

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

