# Formation Stratégies GPO & AD - sr 26 - Cours

Michel Cabaré / www.cabare.net / michel@cabare.net

Stratégies GPO et Active Directory - sr 26 - Cours V3-3 – Septembre 2022



https://WWW.CABARE.NET ©



Microsoft Partner

# TABLE DES MATIÈRES

| STRATEGIES LOCALES WINDOWS 10-7   | 4                            |
|---|------------------------------|
| Types de strategie :  | 4                            |
| Stratégies locales ( cf microsoft GPO hors AD):                           | 4                            |
| Stratégies de Groupe GPO (cf microsoft GPO dans AD):                      | 5                            |
| CONFIGURER DES STRATEGIES LOCALEMENT – PARAMETRES GPO STRATEGIES LOCALES: | 5                            |
| CONFIGURER UNE STRATEGIE LOCALEMENT – PICTOGRAMME:                        | 7                            |
| CONTENU DES PARAMETRES LOCAUX DE SECURITE :                               | 9                            |
| Imprimer lister les strategies :  | 12                           |
| STRATEGIES LOCALES MULTIPLES MLGPO  | 13                           |
| STRATEGIES LOCALES MULTIPLES DITES MLGPO                                  | 13                           |
| DEFINIR UNE MLGPO   | 13                           |
| ENREGISTRER LA MMC EDITEUR DE STRATEGIE MLGPO                             | 15                           |
| SUPPRIMER LES MLGPO   | 16                           |
| DESACTIVATION DES MLGPO   | 17                           |
| WINDOWS 10 SCT SECUDITY COMPLIANCE TOOL VIT LODO                          | 10                           |
| WINDOWS 10 - SCI SECURITY COMPLIANCE TOOLKIT, LITHUTADE L GPO             | 10 10                        |
| FYDORT INDORT AVECIGEO  | 10                           |
| EAFORT - IMPORT AVEC LOT O.EAE  | 10                           |
| WINDOWS 7 – SCM SECURITY COMPLIANCE MANAGER - LPT                         | 20                           |
| WINDOWS 7 - SCM SECURITY COMPLIANCE MANAGER - LPT:                        | 20                           |
| EXTRAIRE LOCAL POLICY TOOL DEPUIS SCM:                                    | 21                           |
| LANCER LE SCRIPT EN LIGNE DE COMMANDE LOCALGPO.WSF:                       | 22                           |
| EXPORTER UNE LGPO SEVEN AVEC LPT:   | 22                           |
| IMPORTER UNE LGPO SEVEN AVEC LPT:   | 23                           |
| KESTAURER UNE LGPO PAR DEFAUT AVEC LP1:                                   | 23                           |
| STRATEGIES DE DOMAINE   | 24                           |
| STRATEGIES DE DOMAINE :   | 24                           |
| GESTION DES STRATEGIES DE GROUPE - GPMC.MSC:                              | 24                           |
| MODIFIER LA STRATEGIE DE DOMAINE :  | 26                           |
| STRATEGIE ORDINATEUR, UTILISATEUR:  | 26                           |
| PROPAGATION STRATEGIES DE DOMAINE :                                       | 26                           |
| L'UTILITAIRE EN LIGNE GPUPDATE ( DEPUIS SEVEN -2003)                      | 28                           |
| GESTION PROPAGATION DES STRATEGIES DE DOMAINE :                           | 29                           |
| EXEMPLE : ATTRIBUTION DROITS UTILISATEUR MODIFIER L'HEURE SYSTEME :       |                              |
| STRATEGIES CONTROLEUR DOMAINE   | 33                           |
| STRATEGIES DE CONTROLEUR DE DOMAINE :                                     | 33                           |
| MODIFIER LA STRATEGIE DES CONTROLEUR DE DOMAINE :                         | 34                           |
| EXEMPLE : ATTRIBUTION DROITS UTILISATEUR MODIFIER L'HEURE DC :            | 34                           |
| BEST PRACTICE GPO DOMAINE ET CD   | 36                           |
| NE PAS MODIFIER LES GPO PAR DEFAUT:                                       | 36                           |
| 1 GPO = 1 ACTION :  | 36                           |
| LIAISON - PORTEE :  | 36                           |
| PROPAGATION ET TEST :   | 37                           |
| CESTION ET SAUVECARDE DES CPO   | 38                           |
| "VISUAL ISATION" EN DIRECT DE LA STRATEGIE ·                              | 38                           |
| FICHIER DE "VISUALISATION" DE LA STRATEGIE :                              |                              |
| SAUVEGARDER UNE OU TOUTES LES STRATEGIES :                                |                              |
| Restaurer les strategies :  | 41                           |
| COPIER UNE STRATEGIE :  | 42                           |
| SAUVGARDE DES STRATEGIES PAR DEFAUT :                                     | 42                           |
| STDATECIES ET DDEEEDENCES   | 12                           |
| I ES DEFERENCES DEDING 2008 ·   | <b>43</b><br>//2             |
| CLEAT SIDE EXTENSION POUR XP SP2-Sp3 & VISTA+                             | <del>4</del> 3<br><u>1</u> 1 |
| PRINCIPALES PREFERENCES ORDINATEUR  | <br>44                       |
| PRINCIPALES PREFERENCES UTILISATEUR :                                     | 44                           |
| Options Communes des Preferences :  | 46                           |
| CIBLAGE DES PREFERENCES :   | 47                           |



| GPO D'UNITE ORGANISATIONELLE                                  |    |
|---|----|
| TYPES ET NIVEAUX DE STRATEGIE :                               |    |
| NIVEAU DE MODIFICATION DANS LA BASE DE REGISTRE               |    |
| CREER UNE STRATEGIE DE GROUPE:                                | 50 |
| LIER UNE STRATEGIE DE GROUPE SUR UNE U.O :                    | 51 |
| VERIFICATION DES ELEMENTS DE L'UO:                            |    |
| GPRESULT.EXE /R /H DEPUIS 7                                   | 53 |
| RSOP JEU DE STRATEGIE RESULTANT                               | 55 |
| RSOP.MSC RESULTANT SET OF POLICY (LOCAL)                      | 55 |
| RSOP.MSC AUTRE UTILISATEUR - ORDINATEUR                       | 56 |
| MMC JEU DE STRATEGIE RESULTANT                                |    |
| ERREUR RPC – CHANGEMENT D'ORDINATEUR                          | 58 |
| RSOP DANS LA CONSOLE GESTION DE STRATEGIE DE GROUPE           | 59 |
| HIERARCHIE DES STRATEGIES                                     | 61 |
| ORDRE FINAL D'APPLICATION DES STRATEGIES :                    | 61 |
| Clients Hors Domaine  | 61 |
| Clients du Domaine Hors Contrôleurs de Domaine                | 61 |
| Contrôleurs de Domaine  | 61 |
| LIAISONS MULTIPLES - PRIORITE - HERITAGE -GPO                 | 62 |
| LIAISON DE GPO :  |    |
| PRIORITE DE GPO :   | 62 |
| HERITAGE – BLOQUE :   | 63 |
| HERITAGE - APPLIQUE:  | 65 |
| PRIORITE DE GPO ORDRE ET HERITAGE :                           | 66 |
| GPO - MODELES D'ADMINISTRATION                                |    |
| Les Modeles presents  |    |
| RAPPELS METHODOLOGIE DE MISE EN ŒUVRE                         | 68 |
| STOCKAGE DES MODELES DE GPO – SUR CHAQUE DC                   | 69 |
| MAGASIN CENTRAL – CENTRALISATION DES MODELES DE GPO           | 70 |
| Trouver le DC ayant le rôle PDC                               |    |
| Création du dossier PolicyDefinitions                         |    |
| Copier les modèles de GPO                                     |    |
| AJOUT SUPPRESSION DES MODELES DE GPO                          |    |
| TROUVER DES MODELES DE GPO – TECHNET WIKI                     |    |
| 1 Selection - Technet WIKI                                    |    |
| <i>I LISTE EXHAUSTIVE - GETAAMX.COM</i>                       |    |
| TELECHARGER ET INSTALLER UN MODELES DE GPO – OFFICE 2013      |    |
| TELECHARGER ET INSTALLER UN MODELES DE GLO – WINDOWS 10 V1809 |    |
|   |    |
| FILTRES WMI   |    |
| OBJECTIFS DES FILTRES WMI SUR LES GPO                         | 81 |
| CREATION DU FILTRE WITH                                       |    |
|   |    |
| CIDEAGE DE FREFERENCE   |    |
| GPEDIT.MSC  |    |
| SECPOL.MSC - KAPPEL STRATEGIES LOCALES ET GPO DE DOMAINE      |    |
| GPEDIT.MSC - EDITEUR DE STRATEGIE DE DOMAINE "LOCALE" !:      | 84 |
| OBJECTIF BOUCLE DE RAPPEL                                     | 85 |
| GPO - NORMALES  |    |
| GPO – LOOPBACK PROCESSING                                     | 85 |
| GPO STARTER   |    |
| OBJETS GPO STARTER  |    |



# **STRATEGIES LOCALES WINDOWS 10-7**

#### Types de stratégie :

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

il existe essentiellement 2 méthodes pour implémenter des stratégies sur des postes Windows 10 (et depuis 7), les **stratégie système locale** appliquée sur un ordinateur unique, ou les **stratégies de groupe** appliquée dans un domaine et déployée sur plusieurs ordinateurs...

## Stratégies locales (cf microsoft GPO hors AD):

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



- Depuis Windows 7 (et Windows -XP 2000) (qu'il soit membre d'un domaine ou non)
- Sur les Serveurs 2022, 2019 2016 2012R2 même Contrôleur de Domaine et sur les Serveur 2008R2-2003 (s'ils ne sont pas Contrôleur de Domaine).

On demande soit

Menu démarrer / Outils d'administration / Stratégies de sécurités locales,

|   | <u>A</u> |
|---|----------|
| হ | ٣.       |

Soit d'exécuter la commande control.exe



puis Outils d'administration / Stratégies de

#### sécurités locales

Soit on effectue une recherche avec Outils d'administration

| Meilleur résultat   |  |
|---|--|
| Outils d'administration<br>Panneau de configuration   |  |
| Image: Stratégie de sécurité locale         Fichier       Action       Affichage       ?         Image: Imag |  |
| <ul> <li>Paramètres de sécurité</li> <li>Stratégies de comptes</li> <li>Stratégie de mot de passe</li> <li>Stratégie de verrouillage du compte</li> <li>Stratégies locales</li> <li>Stratégie d'audit</li> <li>Attribution des droits utilisateur</li> <li>Options de sécurité</li> <li>Pare-feu Windows avec fonctions avancées de sécuri</li> <li>Pare-feu Windows avec fonctions avancées de sé</li> <li>Stratégies du gestionnaire de listes de réseaux</li> <li>Stratégies de clé publique</li> <li>Stratégies de contrôle de l'application</li> <li>Stratégies de sécurité IP sur Ordinateur local</li> <li>Configuration avancée de la stratégie d'audit</li> </ul>  | Nom<br>Stratégies de comptes<br>Stratégies locales<br>Pare-feu Windows avec fonctions avancé<br>Stratégies du gestionnaire de listes de rés<br>Stratégies de clé publique<br>Stratégies de clé publique<br>Stratégies de restriction logicielle<br>Stratégies de contrôle de l'application<br>Stratégies de sécurité IP sur Ordinateur lo<br>Configuration avancée de la stratégie d'a |



Par exemple sur un Serveur 2019 2016 on aura en plus par rapport à un client Windows 10 dans les stratégies locales une entrée dans les Stratégies de comptes - Stratégie Kerberos

| <ul> <li>Stratégies locales</li> <li>Pare-feu Windows avec fonctions avancées</li> <li>Tolérance maximale pour la synchronisation de l'horloge de 5 minutes</li> </ul> | Stratégie de mot de passe     Stratégie de verrouillage du compte     Stratégie Kerberos | ée de vie maximale du ticket de service<br>ée de vie maximale du ticket utilisateur<br>ée de vie maximale pour le renouvellement du ticket utili | 600 minutes<br>10 minutes<br>7 minutes |
|--|--|--|--|
|--|--|--|--|

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

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

#### Configurer des stratégies localement – paramètres GPO stratégies locales:

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

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



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

Stratégies de compte (~gestion compte utilisateur)

Passées via le Panneau de configuration



Passées via domaine par GPO





Stratégies locales (~ouverture session locale et prérogatives associées)

#### Passées via le Panneau de configuration



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

Passées via Panneau de configuration

#### Passées via domaine par GPO

Passées via domaine par GPO

| 🚡 Stratégie de sécurité locale                           | Éditeur de gestion des stratégies de groupe                         |
|--|---|
| Fichier Action Affichage ?                               | Fichier Action Affichage ?  |
| 🗢 🔿   🚈 📰   🛛 🖬  | 🗢 🔿   🖄 📰   🛛 🖬   |
| 🚡 Paramètres de sécurité                                 | Stratégie Nouvel objet de stratégie de groupe [SRVDC1-FORM16.FORM ^ |
| Stratégies de comptes                                    | 🗸 👰 Configuration ordinateur  |
| > A Stratégies locales                                   | ✓ <sup>™</sup> Stratégies   |
| → V Pare-feu Windows avec fonctions avancées de sécurité | > 📋 Paramètres du logiciel  |
| ✓ ● Pare-feu Windows avec fonctions avancées de sécuri   | 🗸 🚞 Paramètres Windows  |
| 🧱 Règles de trafic entrant                               | > iii Stratégie de résolution de noms                               |
| 🎇 Règles de trafic sortant                               | 😫 Scripts (démarrage/arrêt)   |
| 🌆 Règles de sécurité de connexion                        | > 💼 Imprimantes déployées   |
|  | 🗸 🚡 Paramètres de sécurité  |
|  | > 📑 Stratégies de comptes   |
|  | > 📓 Stratégies locales  |
|  | > ቭ Journal des événements  |
|  | > 📴 Groupes restreints  |
|  | > 强 Services système  |
|  | > 🔂 Registre  |
|  | > 📴 Système de fichiers   |
|  | > Stratégies de réseau filaire (IEEE 802.3)                         |
|  | Pare-feu Windows avec fonctions avancées de sécu                    |
|  | ✓ Pare-feu Windows avec fonctions avancées de s                     |
|  | 🧱 Règles de trafic entrant  |
|  | 🥂 Règles de trafic sortant  |
|  | Negles de sécurité de connexion                                     |



#### Stratégies de clé publique (agent de récupération EFS)

Passées via Panneau de configuration



Passées via domaine par GPO

Et aussi

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

#### Configurer une stratégie localement – Pictogramme:

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



HOID றுற indiquera qu'elle est gérée localement.



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

| ur une machine en <b>Workgroup</b>  |  |   |
|---|--|---|
| 🔒 Stratégie de sécurité locale  |  | _   |
| Fichier Action Affichage ?  |  |   |
|   |  |   |
| Paramètres de sécurité  | Stratégie  | Paramètre de sécurité   |
| <ul> <li>Gastratégies de comptes</li> <li>Gastratégie de mot de passe</li> <li>Gastratégies de verrouillage du compte</li> <li>Gastratégies locales</li> <li>Pare-feu Windows avec fonctions avancées de sécurité</li> <li>Stratégies du gestionnaire de listes de réseaux</li> <li>Stratégies de clé publique</li> </ul>   | Conserver l'historique des mots de passe     Durée de vie maximale du mot de passe     Durée de vie minimale du mot de passe     Enregistrer les mots de passe en utilisant un chiffrement     Le mot de passe doit respecter des exigences de complex     Longueur minimale du mot de passe | 0 mots de passe mémori.<br>42 jours<br>0 jours<br>rév Désactivé<br>xité Désactivé<br>0 caractère(s) |
| On la « main »  |  |   |
| Propriétés de : Longueur minimale du mot de pa  | sse ? X  |   |
| Paramètre de sécurité locale Expliquer  |  |   |
| Aucun mot de passe n'est nécessaire.  |  |   |
| Stratégie de sécurité locale  |  |   |
| Fichier Action Affichage ?  |  |   |
| 🗢 🔿 🚾 📰 🗙 🗟 🛛 🖬 🔪   |  |   |
| 🚡 Paramètres de sécurité 💙 Stratégie  | ^ Pi   | aramètre de sécurité  |
| ✓ Gastratégies de comptes ☐ Stratégies de met d | r l'historique des mots de passe 24  | 4 mots de passe mémo  |
| Stratégie de verrouillage du comp   | vie maximale du mot de passe 42  | 2 jours   |
| > 🛃 Stratégies locales  | vie minimale du mot de passe 1   | jours<br>(  |
| > 🧰 Pare-feu Windows avec fonctions ava   | er les mots de passe en utilisant un chiffrement rev D   | esactive  |
| <ul> <li>Stratégies du gestionnaire de listes de<br/>Stratégies de clé publique</li> <li>Longueur</li> </ul>  | r minimale du mot de passe 7   | caractère(s)  |
| On n'a pas la « main »  |  |   |
| Propriétés de : Longueur minimale du mot de pa  | isse ? X   |   |
| Paramètre de sécurité locale Expliquer  |  |   |
| Longueur minimale du mot de passe   |  |   |





#### Contenu des Paramètres locaux de sécurité :

N.B : il faut bien évidemment faire très attention au fait que <u>toutes les stratégies ne</u> <u>sont pas disponibles à l'identiques sur toutes les machines</u>, en fonctions des systèmes Windows 10 (selon les branches), Seven, voir des modules complémentaires spécifiques, les noms des stratégies peuvent varier, parfois considérablement.

#### Stratégies de comptes



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





#### Attribution des droits utilisateurs

| Strategie A   | Stratégie ^  |
|---|--|
| Céder à cet ordinateur depuis le réseau   |  |
| Agir en tant que partie du système d'exploitation   | Acceder a cet ordinateur a partir du reseau                      |
| 👸 Ajouter des stations de travail au domaine  | Accèder au gestionnaire d'informations d'identification en       |
| المعالم Arrêter le système المعالم الم  | 📓 Agir en tant que partie du système d'exploitation              |
| iii) Augmenter la priorité de planification   | 📓 Ajouter des stations de travail au domaine                     |
| المراجع | Ajuster les quotas de mémoire pour un processus                  |
| Autoriser que l'on fasse confiance aux comptes ordinal  | 📓 Arrêter le système   |
| iiii)Charger et décharger des pilotes de périphériques  | Augmenter la priorité de planification                           |
| ing Creer des objets partages permanents  | Augmenter une plage de travail de processus                      |
| ing Creer un fichier d'échange  | Autoriser l'ouverture de session nar les services Bureau à di    |
| ing Créer un objet-jeton  | Changer le fureau beraire  |
| nicipeboguer des programmes   | Changer le fuseau noralle  |
| ning Forcer l'arret a partir d'un système distant   | Charger et decharger les pilotes de peripheriques                |
| ing Generer des audits de securite  | Contourner la vérification de parcours                           |
| ing Gerer le journal d'audit et de securite   | 📖 Créer des liens symboliques                                    |
| Modifier les valeurs d'env. de microprogrammation   | 🔯 Créer des objets globaux                                       |
| ing Modifier Theure systeme   | 📓 Créer des objets partagés permanents                           |
| Optimiser les performances système  | 📓 Créer un fichier d'échange                                     |
| Departmenter un processus unique  | Créer un obiet-ieton   |
|   | Déboquer les programmes  |
| Cuvrir une session en tant que service  | Effectuer les tâches de maintenance de volume                    |
| Curvir une session en calc que cache  | Emprunter l'identité d'un client ancès l'authentification        |
|   |  |
| Ť   | References a partir d'un systeme distant                         |
|   | Generer des audits de securite                                   |
|   | 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                     |
| Exemple de difference de libelle  | Interdire l'ouverture de session en tant que service             |
| N   | Interdire l'ouverture de session en tant que tâche               |
|   | 🔯 Interdire l'ouverture de session par les services Bureau à di  |
| $\backslash$  | Modifier l'heure système   |
| $\backslash$  | Modifier les valeurs de l'environnement du micronrogram          |
| $\backslash$  | Modifier up nom d'objet  |
| $\langle \rangle$   |  |
| $\backslash$  | Obtenir un jeton d'emprunt d'identité pour un autre utilis       |
|   | Ouvrir une session en tant que service                           |
| $\langle \rangle$   | 📖 Ouvrir une session en tant que tâche                           |
| $\backslash$  | 📓 Performance système du profil                                  |
|   | 🔪 📓 Permettre à l'ordinateur et aux comptes d'utilisateurs d'êtr |
|   | Permettre l'ouverture d'une session locale                       |
|   | Prendre possession de fichiers ou d'autres objets                |
|   | Processus unique du profil                                       |
|   | Remplacer un jeton de niveau processus                           |
|   |  |
|   | we restaurer les fichiers et les répertoires                     |

#### Options de sécurité

Ouvertures de sessions interactives : nombre d'ouvertures d... 10 Ouvertures de session
Ouverture de session interactive : seuil de verrouillage du co... Non défini
Ouverture de session interactive : limite d'inactivité de l'ordi... Non défini
Ouverture de session interactive : Windows Hello Entreprise ... Désactivé
Ouverture de session interactive : titre du message pour les ...
Ouverture de session interactive : prévenir l'utilisateur qu'il d... 5 jours
Ouverture de session interactive : ne pas demander la combi... Non défini
Ouverture de session interactive : ne pas afficher le nom du ... Désactivé
Ouverture de session interactive : ne pas afficher le nom de l... Non défini
Ouverture de session interactive : ne pas afficher le nom de l... Non défini
Ouverture de session interactive : contenu du message pour...



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

~

#### Stratégie

|             | Stategie  |
|-------------|---|
|             | 💐 Accès réseau : chemins et sous-chemins de Registre accessibles à distance   |
|             | 📓 Accès réseau : les autorisations spécifiques des utilisateurs appartenant au groupe Tout le monde s'ap  |
|             | 📖 Accès réseau : les canaux nommés qui sont accessibles de manière anonyme  |
|             | 🙀 Accès réseau : les chemins de Registre accessibles à distance   |
|             | 📖 Accès réseau : les partages qui sont accessibles de manière anonyme   |
|             | 📖 Accès réseau : modèle de partage et de sécurité pour les comptes locaux   |
|             | 📖 Accès réseau : ne pas autoriser l'énumération anonyme des comptes et partages SAM   |
|             | 📖 Accès réseau : ne pas autoriser l'énumération anonyme des comptes SAM   |
|             | 📖 Accès réseau : Permet la traduction de noms/SID anonymes  |
|             | Accès réseau : restreindre l'accès anonyme aux canaux nommés et aux partages  |
|             | 📓 Accès réseau : ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'   |
|             | 🖗 Accès réseau : restreindre les clients autorisés à effectuer des appels distants vers SAM   |
|             | 🙀 Arrêt : effacer le fichier d'échange de mémoire virtuelle   |
|             | Arrêt : permet au système d'être arrêté sans avoir à se connecter   |
|             | arrêter immédiatement le système s'il n'est pas possible de se connecter aux audits de sécurité   |
| >           | Audit : auditer l'accès des obiets système globaux  |
|             | Audit : auditer l'utilisation des privilèges de sauvegarde et de restauration   |
|             | a Audit : force les paramètres de sous-catégorie de stratégie d'audit (Windows Vista ou version ultérieu  |
|             |   |
|             | Chiffrement systeme : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la   |
| <b>&gt;</b> | Client reseau Microsoft : communications signees numeriquement (lorsque le serveur l'accepte)   |
| F           | in Client reseau Microsoft : communications signees numeriquement (toujours)  |
|             | in Client réseau Microsoft : envoyer un mot de passe non chiffré aux serveurs SMB tierce partie   |
|             | Comptes : renommer le compte administrateur   |
|             | Comptes : renommer le compte invité   |
|             | Comptes : restreindre l'utilisation de mots de passe vides par le compte local à l'ouverture de session   |
|             | 📖 Comptes : statut du compte Administrateur   |
|             | 📖 Comptes : statut du compte Invité   |
|             | 🔤 Comptes : bloquer les comptes Microsoft   |
|             | i Connexion interactive : afficher les informations relatives à l'utilisateur lorsque la session est verrouillée  |
|             | i console de récupération : autoriser l'ouverture de session d'administration automatique   |
|             | Console de récupération : autoriser la copie de disquettes et l'accès à tous les lecteurs et dossiers   |
|             | Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur i  |
|             | Contröle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation   |
| >           | Contröle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans utili  |
|             | Contröle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en   |
|             | a Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard  |
|             | a Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation  |
|             | Contrôle de compte d'utilisateur : élever uniquement les applications UIAccess installées à des empla   |
|             | الله Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés   |
|             | 📖 Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'a   |
|             | i virtualiser les échecs d'écritures de fichiers et de Registre dans des  |
|             | 📖 Contrôleur de domaine : conditions requises pour la signature de serveur LDAP   |
|             | 📖 Contrôleur de domaine : permettre aux opérateurs du serveur de planifier des tâches   |
|             | الله Contrôleur de domaine : refuser les modifications de mot de passe du compte ordinateur   |
|             | 📖 Cryptographie système : force une protection forte des clés utilisateur enregistrées sur l'ordinateur   |
|             | in DCOM : Restrictions d'accès à un ordinateur au format du langage SDDL (Security Descriptor Definiti  |
|             | 📖 DCOM : Restrictions de démarrage d'ordinateur au format du langage SDDL (Security Descriptor Defi   |
|             | Membre de domaine : ancienneté maximale du mot de passe du compte ordinateur  |
|             | Converture de session interactive : comportement largque la carte à puce est retirée  |
|             | Ouverture de session interactive : comportement ionsque la carte à puce est retiree   |
|             | () Ouverture de session interactive : concent du message pour les utilisateurs essayant de se connecter   |
|             | Converture de session interactive : ne pas amener le combinaison de touches Ctrl. Alt. Super  |
| <b>&gt;</b> | Ouverture de session interactive : né pas demander la complinaison de toucries Ctil+Ait+Suppr. Ouverture de session interactive : nécessite l'authentification par la contrôleur de demaire : nouvel a dé |
| r r         | w ouverture de session interactive : necessite radurentification par le controleur de domaine pour le de  |
|             | w ouverture de session interactive : prevenir i dunsateur qu'il doit changer son mot de passe avant qu'il   |
|             | a ouverture de session interactive : une du message pour les duisateurs essayant de se connecter  |
|             | Constructione de session interactive : annue à mactivite de l'ordinateur  |
|             | au construire de session initeractive : seuli de venouinage du compte d'ordinateur  |





#### Imprimer lister les stratégies :

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

#### Exporter la liste...



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

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

#### Ou le travailler (fichier texte délimité par des tabulations)

|   | A   | В                         |
|---|---|---------------------------|
| 1 | Conserver l'historique des mots de passe  | O 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   | O Caractères              |
| 6 | Stocker le mot de passe en utilisant le cryptage réversible pour tous les utilisateurs du domaine | Désactivé                 |
| 7 | Stratégie   | Paramètre de sécurité     |



# STRATEGIES LOCALES MULTIPLES MLGPO

#### Stratégies locales multiples dites MLGPO

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

• tous les utilisateurs....

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

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

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

Depuis **Windows Seven, et donc avec 10** il est possible maintenant de définir des stratégies multiples locales **MLGPO Multiples Local Group Policies Objects** dont la portée peut être plus fine...

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

#### Définir une MLGPO

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



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

mais plutôt Parcourir





| Assistant Stratégie de groupe |   |
|-------------------------------|---|
|                               | Les objets de stratégie de groupe locale sont stockés sur<br>l'ordinateur local.<br>Utilisez le bouton Parcourir pour sélectionner un objet de<br>stratégie de groupe.                                  |
|                               | Objet de stratégie de groupe :<br>Ordinateur local  |
|                               | Parcourir   |
|                               | Autoriser la modification du composant logiciel<br>enfichable de stratégie de groupe lors de l'exécution à<br>partir de la ligne de commande. Ceci ne s'applique que<br>si vous enregistrez la console. |
|                               | <pre>&lt; Précédent Teminer Annuler</pre>   |

#### Et on choisit l'onglet Utilisateur

| Rechercher un objet Stratégie de groupe            | ? <mark>×</mark>                   |
|--|------------------------------------|
| Ordinateurs Utilisateurs                           |                                    |
| Utilisateurs et groupes locaux compatibles avec la | stratégie de groupe locale :       |
| Nom  | Il existe des objets de str        |
| Administrateur                                     | Non                                |
|  | Non                                |
| Administrateurs                                    | Non                                |
| Annual accurs                                      | Non                                |
|  | OK Annuler                         |
| On retrouve ici les choix annoncés                 |                                    |
| <ul> <li>l'ordinateur, -il aurait</li> </ul>       | fallut faire terminer (*)          |
| <ul> <li>tous les utilisateurs</li> </ul>          | il aurait fallut faire terminer(*) |
| <ul> <li>Tous les administrate</li> </ul>          | urs (locaux)                       |
| <ul> <li>Tous les non-adminis</li> </ul>           | trateurs (locaux)                  |

- Un utilisateur local du poste

**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 <u>la portée</u> de cette stratégie locale...

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

On obtient







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

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

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

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

#### Enregistrer la MMC editeur de strategie MLGPO

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





Ce qui permettrais ensuite de la 🕌 Microsoft Office Administrateur Outils d'administration retrouver via 🔊 Analyseur de performances Documents Configuration du système Diagnostic de mémoire Windows Images 🔚 Gestion de l'impression 🜆 Gestion de l'ordinateur Ordinateur 🍭 Initiateur iSCSI a Igpo-administrateur.msc Panneau de configuration 🛃 Observateur d'événements 😽 Pare-feu Windows avec fonctions avanc Périphériques et imprimantes Planificateur de tâches les Services de composants Programmes par défaut Services Sources de données (ODBC) Aide et support 🚡 Stratégie de sécurité locale 💹 Windows PowerShell Modules Exécuter... Précédent ۰. Rechercher les programmes et fichiers Ø Arrêter 🕨

#### Supprimer les MLGPO

Les MLGPO sont stockées dans System32\GroupPolicy et \GroupPolicyUsers



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

| Rechercher un objet Stratégie de groupe                      | ? ×                         |
|--|-----------------------------|
| Ordinateurs Utilisateurs                                     |                             |
| Utilisateurs et groupes locaux compatibles avec la stratégie | e de groupe locale :        |
| Nom  | Il existe des objets de str |
| Se Administrateur  | Non                         |
| 🏽 🖉 util   | Non                         |
| Administrateurs  | Oui                         |
| A Non-administrateurs  | Oui                         |
|  |                             |

le clic droit souris permet de les Supprimer

| Rechercher un objet Stra     | tégie de groupe                                      | ? × |
|------------------------------|--|-----|
| Ordinateurs Utilisateurs     |  |     |
| Utilisateurs et groupes loca | aux compatibles avec la stratégie de groupe locale : |     |
| Nom                          | Il existe des objets de str                          |     |
| 🌉 admin                      | Non  |     |
| Administrateur               | Non  |     |
| 🅭 bob                        | Oui  |     |
| 🌉 toto                       | Non  |     |
| Administrateurs              | Oui  |     |
| Non-administrateurs          | Oui ,  |     |
|                              | Supprimer l'objet de stratégie de groupe             |     |
|                              | Actualiser   |     |
|                              | Propriétés   |     |



#### Désactivation des MLGPO

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

Dans Ordinateur \ modèles d'administration \ système \stratégies de groupe \ Desactiver le traitement des objets de stratégie de groupe locaux



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



## WINDOWS 10 - SCT SECURITY COMPLIANCE TOOLKIT LGPO

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

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

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

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

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

Microsoft Security Compliance Toolkit 1.0



This set of tools allows enterprise security administrators to download, analyze, test, edit and store Microsoft-recommended security configuration baselines for Windows and other Microsoft products, while comparing them against other security configurations.

### Details

Note: There are multiple files available for this download. Once you click on the "Download" button, you will be prompted to select the files you need.

| Version:<br>1.0   | Date Published:<br>6/13/2017 |
|---|------------------------------|
| File Name:  | File Size:                   |
| LGPO.zip  | 797 KB                       |
| PolicyAnalyzer.zip  | 1.5 MB                       |
| Windows 10 Version 1507 Security Baseline.zip                         | 904 KB                       |
| Windows 10 Version 1511 Security Baseline.zip                         | 902 KB                       |
| Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip | 1.5 MB                       |

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

#### Export – import avec LGPO.exe :

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





On peut exporter notre GPO locale avec la commande suivante :

#### LGPO.exe /b C:\GPO

Donc dans l'exemple



Ce qui crée une GPO dans le dossier de destination

| 🛩 🏪 os-systeme (C:)                   | ^ | Nom                                   |
|---------------------------------------|---|---------------------------------------|
| > SRecycle.Bin                        |   | GB53DA03-884A-4FF9-9FA0-B94A27968C21} |
| 🗸 📙 backup-gpo                        |   |                                       |
| > 📙 {CB53DA03-884A-4FF9-9FA0-B94A2796 |   |                                       |

On peut importer les paramètres GPO avec la commande suivante :

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

LGPO.exe /g: c:\GPO\

sans spécifier, prend tous le dossier

Toutes les stratégies seront restaurées,

| Audit policy directory exists   |
|---|
| Copied c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GP0\Machine\microsoft\windows nt\Audit\audit.cs            |
| v   |
| to C:\Windows\system32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv   |
| Clearing existing audit policy  |
| Apply Audit policy from c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GPO\Machine\microsoft\windows             |
| nt\Audit\audit.csv  |
| Apply security template: c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GP0\Machine\microsoft\windows            |
| nt\SecEdit\GptTmpl.inf  |
| <pre>Import Machine settings from registry.pol: c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GP0\Machine</pre> |
| \registry.pol   |
| <pre>Import User settings from registry.pol: c:\backup-gpo\{CB53DA03-884A-4FF9-9FA0-B94A27968C21}\DomainSysvol\GPO\User\regis</pre> |
| try.pol   |
|   |
|   |

Il ne faut pas oublier de redémarrer le poste !





## WINDOWS 7 – SCM SECURITY COMPLIANCE MANAGER - LPT

#### Windows 7 - SCM Security Compliance Manager - LPT:

Il faut télécharger les LPT au sein d'un package technet plus complet nommé Security\_Compliance\_Manager\_Setup

Security\_Compliance\_Manager\_Setup.exe 08/10/2014 14:20 Application 27 595 Ko

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

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

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

### Programmes et fonctionnalités





#### **Extraire Local Policy Tool depuis SCM:**

# Microsoft Security Compliance Manager Setup Welcome to the Microsoft Security Compliance Manager Setup Wizard This wizard guides you through the process of installing the Microsoft Security Compliance Manager as well as Microsoft® SQL Server® Express Edition. If you have not previously downloaded Microsoft SQL Server Express Edition, you need an Internet connection to download therequired installation files. To start the installation process, click Next. I Check for updates automatically at startup. Microsoft Solution Accelerators Read the online privacy statement Accelerators Read the online privacy statement Accelerators Read the online privacy statement

Après avoir installer SCM Security\_Compliance\_Manager\_Setup

Qui se stockeront dans

| <u> </u>  | Microsoft Security Compliance Manager Se                                       | etup   | × |  |  |
|---|--|--------|---|--|--|
| Installation Folder<br>Specify the installation folder for the Microsoft Security Compliance Manager. |  |        |   |  |  |
|   | Installation folder:<br>C:\Program Files\Microsoft Security Compliance Manager | Browse |   |  |  |

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

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



Onchoisit un dossier d'installation





#### Lancer le script en ligne de commande LocalGPO.wsf:

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

|   | ▶ Utilitaires ▶ localgpo                      |
|---|---|
| Utilisateurs  | ^ Nom   |
| <ul> <li>Utilitaires</li> <li>bginfo</li> <li>cccleaner</li> <li>kms-activation-office-windows</li> </ul> | SCE Update Security Templates Accelerator.xml |
| Jocalgpo     Microsoft-toolkit  | Command-line here.cmd                         |

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

#### Exporter une LGPO Seven avec LPT:

La syntaxe pourrait être

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

avec

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

Par exemple

```
C:\Utilitaires\localgpo>cscript LocalGPO.wsf /Path:C:\utilitaares\stock-gpo /export
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. Tous droits réservés.
Exporting Local Policy... this process can take a few moments.
Local Policy Exported to C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}
```





#### Importer une LGPO Seven avec LPT:

La syntaxe pourrait être

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

avec

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

Par exemple

| C:\Utilitaires\localgpo>cscript LocalGPO.wsf /Path:C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}<br>Microsoft (R) Windows Script Host Version 5.8<br>Copyright (C) Microsoft Corporation. Tous droits réservés.  |  |
|--|--|
| Modifying Local Policy this process can take a few moments.  |  |
| Applied valid INF from C:\utilitaires\stock-gpo\{07A72B66-F38C-4BBB-8848-CF4136498337}<br>Applied valid Machine POL from C:\utilitaires\stock-gpo\(07A72B66-F38C-4BBB-8848-CF4136498337}<br>Applied valid User POL from C:\utilitaires\stock-gpo\(07A72B66-F38C-4BBB-8848-CF4136498337)<br>Applied valid Audit Policy CSV from C:\utilitaires\stock-gpo\(07A72B66-F38C-4BBB-8848-CF4136498337) |  |
| Local Policy Modified!   |  |
| Please restart the computer to refresh the Local Policy  |  |
|  |  |

#### Restaurer une LGPO par défaut avec LPT:

La syntaxe pourrait être

#### cscript LocalGPO.wsf /restore

```
C:\Utilitaires\localgpo>cscript LocalGPO.wsf /restore
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. Tous droits réservés.
Modifying Local Policy... this process can take a few moments.
Restoring Security Settings...
```



#### Stratégies de Domaine :

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

#### • les contrôleurs de domaine en font partie

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

### Gestion des stratégies de groupe - gpmc.msc:

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



| Proprie | étés de : G                                       | estion des stratégies de groupe  |   |
|---------|---|--|---|
| Général | Raccourci   | Compatibilité Sécurité Détails Versions précédentes  | ĺ   |
|         | Gesti   | on des stratégies de groupe  |   |
| Type de | e cible :   | Application  |   |
| Emplac  | ement :   | system32   |   |
| Cible : |   | \mmc.exe %SystemRoot%\system32\gpmc.msc  |   |
|         | Propri<br>Général<br>Type de<br>Emplac<br>Cible : | Propriétés de : G<br>Général Raccourci<br>Gesti<br>Type de cible :<br>Emplacement :<br>Cible : | Propriétés de : Gestion des stratégies de groupe         Général       Raccourci       Compatibilité       Sécurité       Détails       Versions précédentes         Gestion des stratégies de groupe |



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

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

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





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

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

| Gestion de stratégie de gro | upe   | formation.edu                 |  |
|-----------------------------|---|-------------------------------|--|
| 🖃 🔬 Forët : formation.edu   |   | Objeta da atratágia da arguna |  |
| 🖃 📑 Domaines                |   | Objets de strategie de groupe |  |
| 🖃 🏥 formation.edu           |   | Ordre des liens 🔺             |  |
| 🛒 Default Do                | Créer un objet GPO dan  | s ce domaine, et le lier ici  |  |
| 🕀 📑 Domain Co               | Lier un objet de stratégie de groupe existant<br>Bloquer l'héritage |                               |  |
| 🕀 🖬 service-inf             |   |                               |  |
| 🕀 📑 Objets de               |   |                               |  |
| 🕀 📑 Filtres WM              | Assistant Modélisation d  | e stratégie de groupe         |  |
| 🕀 🛅 Objets GP               | Nouvelle unité d'organisa   | ation                         |  |
|                             | -   |                               |  |

Plaçons nous sur la stratégie Default Domain Controller



🖃 📗 sysvol

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

Dans lequel on y trouvera nos stratégies



Il existe 2 GUID connus :

# Default Domain Policy : {31B2F340-016D-11D2-945F-00C04FB984F9}. Default Domain Controllers Policy: {6AC1786C-016F-11D2-945F-00C04fB984F9}.



#### Modifier la Stratégie de Domaine :

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



On demande Modifier... la Default Domain policy



#### Stratégie Ordinateur, Utilisateur:

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

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



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

#### Propagation Stratégies de Domaine :

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

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

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





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

#### Depuis Windows Seven - XP

#### Gpupdate /force



#### Par exemple

Effectivement, dans le journal on peut observer

| Gestionnaire de serveur (DC)                    | Système Nombre d'événements : 1 403 (!) Nouveaux événements disponibles |                              |                           |                           |
|---|---|------------------------------|---------------------------|---------------------------|
|   | Niveau  | Date et heure                | Source                    | ID de l'évé               |
| <ul> <li>Gestion des stratégies de g</li> </ul> | (i) Information   | 02/06/2013 09:36:01          | Service Control M         | lanager 7036              |
| Diagnostics                                     | <ol> <li>Information</li> </ol>   | 02/06/2013 09:36:00          | GroupPolicy               | 1502                      |
| 🖃 🛃 Observateur d'événements                    | 1 Information   | 02/06/2013 00:34:23          | Service Control N         | lananer 7036              |
| 🛨 📑 Affichages personnalisé                     | 👔 🔡 Propriétés de   | e l'événement - Événeme      | ent 1502, GroupPolicy     |                           |
| 🖃 📫 Journaux Windows                            |   | . 1                          | N                         |                           |
| Application                                     | General Déta  | ils                          |                           |                           |
| 😭 Sécurité                                      | <u> </u>  |                              |                           |                           |
| Installation                                    | 👔 Les paramètr  | es de stratégie de groupe    | pour l'ordinateur ont été | é traités. De nouveaux pa |
| 😭 Système                                       | provenant de  | e 2 objets de stratégie de g | roupe ont été détectés e  | et appliqués.             |
| Evénements transfi                              | 1   |                              |                           |                           |
| Journaux des applicatio                         | Ā   |                              |                           |                           |
| Abonnements                                     | $\overline{1}$  |                              |                           |                           |
| OPerformance                                    | 1 I   |                              |                           |                           |
| Gestionnaire de peripheriqu                     | Õ   |                              |                           |                           |
|   | Journal :   | Système                      |                           |                           |
|   | Source :  | GroupPolicy                  | Connecté : 02             | 2/06/2013 09:36:00        |
|   | Événement :   | 1502                         | Catégorie : A             | ucun                      |

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



Pour mémoire sous Windows 2000 :

#### Secedit /refreshpolicy machine\_policy



Et / OU Secedit /refreshpolicy user\_policy



https://www.cabare.net Page 27 - Michel Cabaré -

#### L'utilitaire en ligne Gpupdate (Depuis Seven -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...

Avant sous 2000 on avait secedit

#### gpupdate /?

C:\Users\Administrateur>gpupdate /? Description : met à jour plusieurs paramètres de stratégie de groupe. Syntaxe : Gpupdate [/Target:{Computer | User}] [/Force] [/Wait:<valeur>] [/Logoff] [/Boot] [/Sync]

#### notamment

| /target:<br>{computer user} | Spécifie que seuls les paramètres de stratégie de l'ordinateur ou de l'utilisateur sont mis à jour. Par défaut, les<br>paramètres de stratégie de l'utilisateur et de l'ordinateur sont mis à jour.   |
|-----------------------------|---|
| /Force                      | Réapplique tous les paramètres de stratégie. Par défaut, seuls les paramètres de stratégie modifiés sont<br>appliqués.  |
| /logoff                     | Provoque une déconnexion après la mise à jour des paramètres de stratégie de groupe. Cela est requis pour les<br>extensions côté client stratégie de groupe qui ne traitent pas la stratégie sur un cycle de mise à jour en arrière-<br>plan, mais qui traitent la stratégie quand un utilisateur ouvre une session. Par exemple, l'installation de logiciels<br>ciblés par l'utilisateur et la redirection de dossiers. Cette option n'a aucun effet si aucune extension nommée ne<br>nécessite de fermeture de session. |
| /boot                       | Entraîne le redémarrage de l'ordinateur après l'application des paramètres de stratégie de groupe. Cela est<br>requis pour les extensions côté client stratégie de groupe qui ne traitent pas la stratégie sur un cycle de mise à<br>jour en arrière-plan, mais qui traitent la stratégie au démarrage de l'ordinateur. Par exemple, l'installation de<br>logiciels ciblés sur l'ordinateur. Cette option n'a aucun effet si aucune extension appelée ne nécessite un<br>redémarrage.                                     |
| Et encore                   |   |

/Wait <VALUE> Définit le nombre de secondes à attendre que le traitement de la stratégie se termine avant de revenir à l'invite de commandes. Lorsque la limite de temps est dépassée, l'invite de commandes s'affiche, mais le traitement de la stratégie se poursuit. La valeur par défaut est 600 secondes. La valeur 0 signifie qu'il n'est pas attendu. La valeur -1 signifie qu'elle est indéfinie.

Dans un script, en utilisant cette commande avec une limite de temps spécifiée, vous pouvez exécuter **gpupdate** et continuer avec les commandes qui ne dépendent pas de l'achèvement de **gpupdate**. Vous pouvez également utiliser cette commande sans limite de temps spécifiée pour laisser l'exécution de l'option **gpupdate** avant l'exécution d'autres commandes qui dépendent de celle-ci.



#### Gestion Propagation des Stratégies de Domaine :

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

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



on trouve

#### 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

#### Donnant

| Intervalle d'actualisation de la stratégie de groupe pour les ordinateurs  |  |  |  |  |
|--|--|--|--|--|
| Thtervalle d'actualisation de la stratégie de g  | groupe pour les ordinateurs  |  |  |  |
| Paramètre précédent Paramètre suivant  |  |  |  |  |
| Non configuré Commentaire :     Activé     Désactivé     Pris en charge sur : Au   | minimum Windows 2000   |  |  |  |
| Options :  | Aide :   |  |  |  |
| Ce paramètre vous permet de personnaliser la<br>fréquence d'application de la stratégie de group<br>aux ordinateurs. L'étendue est comprise entre 0<br>64 800 minutes (45 jours).<br>Minutes : 90  | Pe       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'intervalle<br>d'actualisation pour éviter<br>que tous les clients effectuent des requêtes de<br>stratégie de groupe en<br>même temps. L'étendue est comprise entre 0 et<br>440 minutes (24 heures)<br>Minutes : 30 | <ul> <li>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.</li> <li>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</li> </ul> |  |  |  |

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<br>d'administratio | /<br>n / S | Stratégies                  | 1        | Modèles        | 🗆 👰 Configura<br>🖃 🧰 Strat | ation ordinateur<br>régies            |    |
|-------------------------------|------------|-----------------------------|----------|----------------|----------------------------|---------------------------------------|----|
| u auninistratio               | ,, 0       | ysteme                      |          |                | 🕀 📔 P                      | aramètres du logiciel                 |    |
|                               |            |                             |          |                | 🕀 📔 P                      | aramètres Windows                     |    |
|                               |            |                             |          |                | 🖃 🧮 N                      | 1odèles d'administration : définitior | n. |
|                               |            |                             |          |                | ÷ [                        | Composants Windows                    |    |
|                               |            |                             |          |                |                            | Imprimantes                           |    |
| Mais là on trouv              | o to       | it un naquet                | doc      | tratágias ·    | + 🧧                        | Panneau de configuration              |    |
|                               | 6 100      | n un paquei                 | ue s     | nuiegies.      | + 🧧                        | 🖥 Réseau                              |    |
| 🗈 Autoriser la strat          | égie utili | sateur et les profils itiné | rants en | tre les forêts | = [                        | 📔 Système                             |    |
| 📰 Traitement de la            | stratégie  | d'installation de logiciel  | l .      |                |                            |                                       |    |
| 📰 Traitement de la            | stratégie  | de quota de disque          |          |                |                            |                                       |    |
| 📰 Traitement de la            | stratégie  | de récupération EFS         |          |                |                            |                                       |    |
| 🗄 Traitement de la            | stratégie  | de redirection de dossi     | er       |                |                            |                                       |    |
| 🗄 Traitement de la            | stratégie  | de maintenance Intern       | et Explo | rer            |                            |                                       |    |

- Traitement de la stratégie de sécurité IP
- 🗄 Traitement de la stratégie du Registre
- 🗈 Traitement de la stratégie de scripts
- 🗈 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"

k

| 🔙 Traitement de la   | stratégie de sécurité  |            |  |
|--|--|------------|--|
| Traitement de la   | stratégie de sécurité  |            | Paramètre précédent Paramètre suivant  |
| C Non configuré  | Commentaire :  |            | <u> </u>   |
| Activé   |  |            |  |
| O Désactivé  | <b>D</b> · · · ·   |            | ×  |
|  | Pris en charge sur :   | Au minimun | n Windows 2000   |
| Options :  |  |            | Aide :   |
| Ne pas appliquer<br>arrière-plan régu ✓ Traiter même si le<br>groupe n'ont pas | · lors d'un traitement en<br>lier<br>es objets de stratégie de<br>s été modifiés | Δ.         | <ul> <li>Si vous activez ce paramètre, vous pouvez utiliser les cases à cocher proposées pour modifier les options. Si vous désactivez ce paramètre ou ne le configurez pas, il n'a aucun effet sur le système.</li> <li>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.</li> <li>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. 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 après sa modification par un utilisateur.</li> </ul> |
|  |  |            | OK Annuler Appliquer   |

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





#### Exemple : Attribution droits Utilisateur Modifier l'heure système :

Depuis les <u>clients Windows 10-7 du domaine</u>, la **stratégie locale** ne montre qu'une seule colonne, (le **service local** remplace les **utilisateurs avec pouvoir**...)

| 🚡 Stratégie de sécurité locale   |  |  |   |
|--|--|--|---|
| Fichier     Action     Affichage       Image: State of the state |  |  |   |
| <ul> <li>Paramètres de sécurité</li> <li>Stratégies de comptes</li> <li>Stratégies locales</li> <li>Stratégie d'audit</li> </ul>   | Stratégie<br>Interdire l'ouverture de session en tant que tâche<br>Interdire l'ouverture de session par les services | Paramètre de sécurité                    | ^ |
| Attribution des droits utilisateur     G Options de sécurité   | Interdire l'ouverture d'une session locale     Modifier l'heure système  | Invité<br>SERVICE LOCAL, Administrateurs |   |

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

| Paramètres de sécurité  | ^ | Stratégie A   | Paramètre de sécurité                        |
|---|---|---|--|
| E Gratégies de comptes  |   | BOModifier les valeurs d'env. de microprogrammation | Administrateurs                              |
| <ul> <li>Stratégies locales</li> <li>Stratégie d'audit</li> </ul> |   | B 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 un <u>client 2000 du domaine</u>, voila l'aspect de la **stratégie locale** concernant qui peut mettre à l'heure la machine.... (on voyait mieux quel niveau disait... quoi...)

| Paramètre de stratégie de sécurité locale |                             |                          |                                    |  |  |  |  |  |
|---|-----------------------------|--------------------------|------------------------------------|--|--|--|--|--|
| F   | Modifier l'heure systèm     | e                        |                                    |  |  |  |  |  |
| Attribué à                                | Paramèt                     | Local<br>re de stratégie | Effectif<br>Paramètre de stratégie |  |  |  |  |  |
| Administ<br>Utilisateu                    | rateurs<br>urs avec pouvoir | N                        | V                                  |  |  |  |  |  |

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.EI 🔺 | Stratégie 🔺   | Paramètres de stra |  |  |  |  |
| 🖃 👰 Configuration ordinateur                               | 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         |  |  |  |  |
| El Stratégie de résolution de noms                         | 🔯 Interdire l'accès à cet ordinateur à partir du réseau               | Non défini         |  |  |  |  |
| Scripts (démarrage/arrêt)                                  | 🔯 Interdire l'ouverture d'une session locale                          | Non défini         |  |  |  |  |
| Parametres de securite                                     | 🔯 Interdire l'ouverture de session en tant que service                | Non défini         |  |  |  |  |
| Strategies de comptes                                      | 📖 Interdire l'ouverture de session en tant que tâche                  | Non défini         |  |  |  |  |
| E Stratégies locales                                       | 🔯 Interdire l'ouverture de session par les services Bureau à distance | Non défini         |  |  |  |  |
| Attribution des droits utilisateur                         | Modifier l'heure système  | FORMATION\bob      |  |  |  |  |
| Options de sécurité  | Modifier les valeurs de l'environnement du microprogramme             | Non défini         |  |  |  |  |



https://www.cabare.net Page 31 - Michel Cabaré - Sur le <u>client Windows 10 du domaine</u>, la **stratégie locale** ne montre qu'une seule colonne, (le service local est maintenu !) et bob <u>est ajouté</u>...



| 📴 Paramètres de sécurité                  | Stratégie 🛆                            | Paramètre de sécurité   |
|---|--|-------------------------|
| E Image: Englishing Stratégies de comptes | BB Modifier les valeurs d'env. de micr | Administrateurs         |
|   | 🕼 Modifier l'heure système             | MANUEL\bob              |
| + III Stratėgie d'audit                   | Optimiser les performances système     | Administrateurs         |
| Attribution des droits utilisateur        | 20 Ontimiser un processus unique       | Administrateurs I Itili |

Sur le client 2000 du domaine on avait les deux informations

| Arbre                                | Stratégie 🛆                               | Paramètre local                            | Paramètre en cours   |
|--------------------------------------|---|--|----------------------|
| Paramètres de sécurité               | 🕮 Gérer le journal d'audit et de sécurité | Administrateurs                            | Administrateurs      |
| 🔄 📴 Stratégies de comptes            | Modifier les valeurs d'env. de micr       | Administrateurs                            | Administrateurs      |
| 🖻 📴 Stratégies locales               | Modifier l'heure système                  | Utilisateurs avec pouvoir, Administrateurs | MANUEL\bob           |
| 🗄 🔟 Stratégie d'audit                | Optimiser les performances système        | Administrateurs                            | Administrateurs      |
| 💼 Attribution des droits utilisateur | Coptimiser un processus unique            | Utilisateurs avec pouvoir, Administrateurs | Utilisateurs avec po |

Avec bob uniquement

|                              |       | Paramètre de strat                                   | égie de sécurité locale         | ? >                                | <                    |      |
|------------------------------|-------|--|---------------------------------|------------------------------------|----------------------|------|
|                              |       | Modifier   | l'heure système                 |                                    |                      |      |
| Pas changement<br>localement | de    | Attribué à   | Local<br>Paramètre de stratégie | Effectif<br>Paramètre de stratégie | Mais ici             | on a |
|                              | [<br> | MANUEL\bob<br>Administrateurs<br>Utilisateurs avec p | ouvoir 🗹                        |                                    | stratégie<br>domaine | de   |

Et sur le Contrôleur de Domaine ???



# STRATEGIES CONTROLEUR DOMAINE

#### Stratégies de Contrôleur de Domaine :

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

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

| 📔 Utilisateurs et ordinateurs Active | e Directory   |            |                | _                |
|--------------------------------------|---------------|------------|----------------|------------------|
| Fichier Action Affichage ?           |               |            |                |                  |
| 🗢 🔿  📊 🔏 📋 🗙 🛙                       | 🗐 🧟 🗟 🛛 🖬 🖉 📾 | 1 🝸 🗾 🐍    |                |                  |
| Utilisateurs et ordinateurs Active   | Nom           | Туре       | Type de contrô | Site             |
| > i Requêtes enregistrées            | NVDC1-FORM16  | Ordinateur | GC             | Default-First-Si |
| > 📔 Builtin                          |               |            |                |                  |
| Computers                            |               |            |                |                  |
| Domain Controllers                   |               |            |                |                  |
| > ForeignSecurityPrincipal:          |               |            |                |                  |

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         |   |   |  |
|--|---|---|--|
| Fichier Action Affichage ?             |   |   |  |
| 🗢 🔿 🙍 🖬 🗙 🖬 🛃 🗖                        |   |   |  |
| haramètres de sécurité                 | Stratégie 🔺   | Paramètre de sécurité                                 |  |
| 🕀 📴 Stratégies de comptes              | 💹 Interdire l'ouverture de session en tant que service                |   |  |
| E 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 utilisateur | Modifier l'heure système  | SERVICE LOCAL, Administrateurs, Opérateurs de serveur |  |
| Options de sécurité                    | Modifier les valeurs de l'environnement du microprogramme             | Administrateurs                                       |  |

#### En fait la Default Domain Controller policy est active...

| Fichier Action Affichage ?                                |   |  |             |
|---|---|--|-------------|
|   |   |  |             |
| 🗐 Stratégie Default Domain Controllers Policy [SRV-2008.F | Stratégie 🔺   | Paramètres de stratégie                  |             |
| 🖃 👰 Configuration ordinateur                              | B Forcer l'arrêt à partir d'un système distant  | Administrateurs, Opérateurs de serveur   |             |
| 🖃 🧮 Stratégies  | Générer des audits de sécurité  | SERVICE LOCAL, SERVICE RÉSEAU            |             |
| 🕀 🚞 Paramètres du logiciel                                | Gérer le journal d'audit et de sécurité   | Administrateurs                          |             |
| 🖃 🚞 Paramètres Windows                                    | Interdire l'accès à cet ordinateur à partir du réseau   | Non défini                               |             |
| El Estratégie de résolution de noms                       | Interdire l'ouverture d'une session locale  | Non défini                               |             |
| 🔄 Scripts (démarrage/arrêt)                               | Interdire l'ouverture de session en tant que service  | Non défini                               |             |
| Paramètres de sécurité                                    | N Interdire l'ouverture de session en tant que tâche  | Non défini                               | 7           |
| Stratégies de comptes                                     | Interdire l'ouverture de session par les services Bureau à distance   | Non défini                               |             |
| E J Strategies locales                                    | Modifier l'heure système  | SERVICE LOCAL, Administrateurs, Opérateu | ırs de serv |
|   | B Modifier les valeurs de l'environnement du microprogramme   | Administrateurs                          |             |
| Ontions de ségurité                                       | 💹 Modifier un nom d'objet   | Non défini                               |             |
|   | Look Andread An |  |             |



#### 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 :



**Stratégies GPO & AD 2019-2016** - sr 26- Cours - ver 3.3 - https://www.cabare.net Pa - Michel Cabaré - Sur le serveur les stratégies locales montrent bien



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





# **BEST PRACTICE GPO DOMAINE ET CD**

#### Ne pas modifier les GPO par défaut:

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

- Default Domain Controllers Policy
- 🗐 Default Domain Policy

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

#### 1 GPO = 1 action :

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



#### explicite

on se crée une "bibliothèque...



#### liaison - portée :

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

| Gestion de stratégie de groupe |   | formation.edu              |  |
|--------------------------------|---|----------------------------|--|
| Forêt : formation.edu          |   | Objete de statésie de su   |  |
| 🖃 🙀 Domaines                   |   | Objets de strategie de gro |  |
| 🖃 🏥 formation.edu              |   | Ordre des liens            |  |
| 🛒 affichage-n                  | O Créer un objet GPO dans ce domaine, et le lier ici. |                            |  |
| 🛒 affiche-mes                  | Lier un objet de stratégie de                         | groupe existant.           |  |
| 🛒 Default Dor                  | Bloquer l'héritage                                    | 5                          |  |
| 🛨 🖬 Domain Cor                 |   |                            |  |
| 🕀 🛅 service-info               | Assistant Modélisation de str                         | atégie de groupe           |  |


Pour le-les Contrôleur de Domaine

| Gestion de stratégie de groupe |                        | Doma          | in Controllers         |
|--------------------------------|------------------------|---------------|------------------------|
| E 🚠 Forët : formation.edu      |                        | Objets        | de stratégie de groupe |
|                                |                        |               |                        |
| 🖃 🎬 formation.edu              |                        |               | Ordre des liens 🔺      |
| affichage-message-             | test                   | $\Rightarrow$ | 1                      |
| 🛒 affiche-message-bet          | ta                     |               |                        |
| 🛒 Default Domain Polic         | у                      | $\sim$        |                        |
| 🖃 🖬 Domain Controllers         |                        |               |                        |
| 🛒 Default Domair               | Créer un objet GPO d   | lans ce do    | omaine, et le lier ici |
| 🕀 🖬 service-info               | Lier un objet de strat | égie de g     | roupe existant         |
| 🖃 📑 Objets de stratégi         | Bloquer l'héritage     |               | 6                      |
| -2 (0.1                        |                        |               |                        |

### Propagation et Test :

Une fois la GPO propagée...

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

on la teste

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

en cas de problème on pense à :

Des problèmes de « propagation »

- vérification **DNS**
- outils gpresult

Des problèmes de « sécurité »

• vérification Droits

Des problèmes de « logique » dans la hiérarchie des GPO

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

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





# **GESTION ET SAUVEGARDE DES GPO**

### "Visualisation" en direct de la stratégie :

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

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

| Gestion de stratégie de groupe   | Default Domain Policy                           |                 |
|--|---|-----------------|
|  | Étendue Détails Paramètres Délégation           |                 |
| Figure 1 Default Domain Policy   | Default Domain Policy                           |                 |
| Domain Controllers   | Données recueillies le : 02/06/2013<br>11:34:46 | afficher tout   |
|  | Configuration ordinateur (activée)              | masquer         |
| Default Domain Controllers Policy  | Stratégies                                      | masquer         |
| Default Domain Policy  | Paramètres Windows                              | masquer         |
| If the swift | Paramètres de sécurité                          | <u>afficher</u> |
| Image: Sites<br>Image: Modélisation de stratégie de groupe                                 | Configuration utilisateur (activée)             | masquer         |
| Résultats de stratégie de groupe   | Aucun paramètre n'est défini.                   |                 |
|  |   |                 |

un jeu d'affichage assez intuitif est disponible



### fichier de "Visualisation" de la stratégie :

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

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

| 🟥 formation.edu                              |                         |
|--|-------------------------|
| 🚮 Default Domain Policy                      |                         |
| 🛨 📔 Domain Controllers                       | Modifier                |
| <ul> <li>Image: Image: production</li> </ul> | ✓ Appliqué              |
| 🖃 🛅 test                                     | ✓ Lien activé           |
| 🛒 Nouvel objet de s                          | Enregistrer le rapport. |
| 🚐 stratégie de grou                          | <u>,</u> ,              |

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

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





|   | Default Domain Controllers Policy.htm | 01/12/2009 09:32 | Document HTML |
|---|---------------------------------------|------------------|---------------|
|   | Default Domain Policy 2.htm           | 29/12/2009 12:37 | Document HTML |
|   | Default Domain Policy.html            | 01/12/2009 09:33 | Document HTML |
| 1 | / 📄 fermeture de session.htm          | 28/12/2009 13:03 | Document HTML |
| / | mot de passe simple.htm               | 29/12/2009 12:49 | Document HTML |

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

| <u> </u>       | D:\rapports-gpo\Default  | Domain Policy.htm            |                    | 🔄 🗠 🔁 🔼                                | ing  |   |
|----------------|--|------------------------------|--------------------|--|--|---|
| - Favoris      | 🚖 🔁 Sites suggérés 👻 🕻   | 🔋 Galerie de composants W    | I <del>-</del>     |  |  |   |
| -<br>실 Default | Domain Policy  |                              |                    | 🛅 • 🔊 -                                | 🖃 🖶 🔹 Page 🗸 Sécurité 🕶 Outils 🕶             | ( |
| Pour vou       | ıs aider à protéger votre ordinat<br>dinateur. Cliquez ici pour afficher | eur, Internet Explorer a res | treint l'exécutior | n des scripts ou des contrôles Active) | ( de cette page Web qui pourraient accéder à |   |
| Default        | Domain Policy  |                              |                    |  |  | _ |
| Données re     | cueillies le : 02/06/2013 11:34:4  | 6                            |                    |  |  |   |
| iénéral        |  |                              |                    |  |  |   |
| Détails        |  |                              |                    |  |  |   |
|                | Domaine  |                              |                    | formation.edu                          |  |   |
|                | Propriétaire   |                              |                    | FORMATION\Admins du dom                | aine   |   |
|                | Créé le  |                              |                    | 01/06/2013 10:29:54                    |  |   |
|                | Modifié le   |                              |                    | 02/06/2013 11:29:02                    |  |   |
|                | Révisions utilisateur  |                              |                    | 1 (AD), 1 (sysvol)                     |  |   |
|                | Révisions ordinateur   |                              | N                  | 6 (AD), 6 (sysvol)                     |  |   |
|                | ID unique  |                              | 13                 | {31B2F340-016D-11D2-945F-              | 00C04FB984F9}                                |   |
|                | État GPO   |                              |                    | Activé                                 |  |   |
| Liaisons       | ;  |                              |                    |  |  |   |
|                | Emplacement  | Appliqué                     |                    | État du lien                           | Chemin d'accès                               |   |
|                |  |                              |                    |  |  |   |

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

| mot de passe simple                                  |                           |  |
|--|---------------------------|--|
| Données recueillies le : 29/12/2009 12:49:28         | afficher tout             |  |
| Général  | masquer                   |  |
| Détails  | afficher                  |  |
| Liaisons   | afficher                  |  |
| Filtrage de sécurité                                 | afficher                  |  |
| Délégation   | afficher                  |  |
| Configuration ordinateur (activée)                   | masquer                   |  |
| Stratégies   | masquer                   |  |
| Paramètres Windows                                   | masquer                   |  |
| Paramètres de sécurité                               | masquer                   |  |
| Stratégies de comptes/Stratégie de mot de passe      | masquer                   |  |
| Stratégie  | Paramètre                 |  |
| Antériorité maximale du mot de passe                 | 30 jours                  |  |
| Antériorité minimale du mot de passe                 | 0 jours                   |  |
| Appliquer l'historique des mots de passe             | 0 mots de passe mémorisés |  |
| Le mot de passe doit respecter des exigences de comp | Désactivé                 |  |
| Longueur minimale du mot de passe                    | 0 caractères              |  |
| Configuration utilisateur (activée)                  | masquer                   |  |
| Aucun paramètre n'est défini.                        |                           |  |

### Sauvegarder une ou toutes les stratégies :

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





https://www.cabare.net Page 39 - Michel Cabaré - Sur la stratégie que l'on souhaite sauvegarder, et demander Sauvegarder...



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

et demander Sauvegarder tout...

| 🖃 📑 Objets de stratégie de groupe | 📕 🧾 🎩 strat - ordi - mo                |
|-----------------------------------|--|
| Default Domain Controllers        | Nouveau                                |
| Default Domain Policy             | Sauvegarder tout                       |
| 🧾 Nouvel objet beta de stra       | Gérer les sauvegardes                  |
| 🧾 Nouvel objet de stratégie (     | Ouvrir l'éditeur de table de migration |
| - · ·                             |  |

Il faut indiquer un emplacement

|                         | 🛃 Sauvegarde de l'objet GPO  | X       |          |            |        |
|-------------------------|--|---------|----------|------------|--------|
|                         | Entrez le nom du dossier où placer les sauvegardes de cet objet GPO. Vous<br>pouvez sauvegarder plusieurs objets GPO dans le même dossier.   | 3       |          |            |        |
|                         | Remarque : les paramètres qui sont externes à l'objet de stratégie de groupe<br>tels que les filtres WMI et les stratégies IPSec sont des objets indépendants<br>dans Active Directory et ne seront pas sauvegardés. | es,     |          |            |        |
|                         | Pour éviter toute modification non autorisée des objets GPO sauvegardés,<br>veillez à sécuriser ce dossier pour que seuls les administrateurs autorisés<br>puissent écrire à cet emplacement.                        |         |          |            |        |
|                         | Emplacement :  |         |          |            |        |
|                         | F:\partage\exercices   | •       |          |            |        |
|                         | Parcourir  |         |          |            |        |
|                         | Description :  |         |          |            |        |
|                         | backup stratégies formation  |         |          |            |        |
|                         | n.   |         |          |            |        |
|                         | Sauvegarder Annuler  | r       | on a u   | ne confirn | nation |
| 📕 Sauve                 | garder   |         | ×        |            |        |
| État de la              | sauvegarde :   |         |          |            |        |
|                         |  |         |          |            |        |
| État :                  |  |         |          |            |        |
| Objet de :              | stratégie de groupe :Nouvel objet de stratégie de groupeOpération réussie  |         | <b>_</b> |            |        |
| Objet de :              | stratégie de groupe :pref - ordi - gestion users locauxOpération réussie   |         |          |            |        |
| Objet de :              | stratégie de groupe :pref - ordi - crer dossier et ciblage os- systemeOpération  | réussie | •        |            |        |
| Objet de :              | stratégie de groupe :pref - util - mappage sur domaineOpération réussie  |         |          |            |        |
| Objet de :              | stratégie de groupe :strat - ordi - mise a l heure - horodatageOpération réussie   | •       |          |            |        |
| Objet de :              | stratégie de groupe :strat - ordi - mot de passe simpleOpération réussie   |         |          |            |        |
| Objet de :              | stratégie de groupe :stratégie de groupe 1Opération réussie  |         |          |            |        |
| Objet de :              | stratégie de groupe :stratégie de groupe 2Opération réussie  |         |          |            |        |
| 11 objets<br>0 objets 0 | GPO ont été sauvegardés.<br>GPO n'ont pas été sauvegardés.   |         |          | et voila   |        |
|                         |  |         |          |            | •      |



| 🗄 🍌 exercices                              | ▲ Nom ↑       |
|--|---------------|
| 🖪 📙 {0FFF3CE2-A27D-4891-A52A-0A2267639AE4} | DomainSyraual |
| 🕀 퉬 {4A946EF4-E66D-48E5-8A0A-B38BDEED6254} | DomainSysvor  |
| 🗄 퉬 {4AAC1A8F-2C81-4C49-9F9F-2F2CEE6E1EC7} | Backup.xml    |
|  | bkupInfo.xml  |
| H 48160AB5C-8438-4F01-B0CD-64771CAC11D7    | gpreport.xml  |
| H 49836843F-A92D-4282-B871-67C0CE5DF8CC    |               |
|  |               |
|  |               |
| 🗄 📗 {E08E6F76-B50E-49F7-ABC5-EC91D7A0B378} |               |

### **Restaurer les stratégies :**



On sélectionne la stratégie à restaurer, puis on demande Restaurer







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

### Copier une stratégie :

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

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



Alors on réponds

| 🔜 Copier l'objet GPO  | × |  |
|---|---|--|
| Spécifier les autorisations pour le nouvel objet GPO :              |   |  |
| Utiliser les autorisations par défaut pour les nouveaux objets GPO. |   |  |
| O Conserver les autorisations existantes.                           |   |  |
| OK Annuler  |   |  |

On a confirmation, et voila...

## Sauvgarde des Stratégies par défaut :

Bien penser à effectuer une sauvegarde au minimum de

- defaults domain policy et •
- default domain controller policy...





## STRATEGIES ET PREFERENCES

### Les Préférences depuis 2008 :

Les préférences sont une nouveauté disponible depuis 2008 et uniquement à destination des clients 10 . En fait depuis Seven (natif) ou Vista - Xp dotés des... **Clients Side Extensions**.

| 🛐 Stratégie essais preferences [SRV-2008.FORMATION.EDU |
|--|
| 🖃 👰 Configuration ordinateur                           |
| 🕀 📔 Stratégies   |
| 🕀 🚞 Préférences  |
| 🖃 🐔 Configuration utilisateur                          |
| 🕀 📔 Stratégies   |
| 🕀 🚞 Préférences  |

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

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

| Préféren | ces |
|----------|-----|
|          |     |

🛨 🚞 Paramètres Windows

🛨 🗟 Paramètres du Panneau de configuration

• Donnés via les **stratégie**s, ces paramètres ne sont pas modifiables par l'utilisateur...

• Donnés via les **préférences**, ces paramètres sont modifiables par l'utilisateur...





### Client Side Extension pour XP SP2-Sp3 & Vista:

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

### XP Sp2-Sp3

| Détails rapides   |                              |
|---|------------------------------|
| Nom du fichier:   | Windows-KB943729-x86-FRA.exe |
| Version:  | 943729                       |
| Articles de la base de<br>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<br>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.

### Option des dossiers

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

### Utilisateurs et groupes locaux

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





### Imprimantes

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

### menu Démarrer

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

### Services

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

### **Options Communes des Préférences :**

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



### Les principales étant

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

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

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

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

### Appliquer une fois et ne plus réappliquer :

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









https://www.cabare.net Page 47 - Michel Cabaré -

### 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 de créer des UO directement depuis la **gestion des stratégies de groupe,** mais cela n'est pas une bonne habitude...

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



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





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

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

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 <u>ajouts notables</u> dans les **stratégies de groupe pour les utilisateurs** sont:

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



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





### Niveau de modification dans la base de registre

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

### HKEY\_LOCAL\_MACHINE Et HKEY\_CURRENT\_USER

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

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

### Créer une Stratégie de Groupe:

Cela repose sur 3-4 étapes

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

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



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

| <b>strat</b> = stratégie  | Nouvel objet GPO  |
|---|---|
| <b>pref</b> = préférence  | Nom :   |
| <b>o</b> = ordinateur   |   |
| $\mathbf{u}$ = utilisateur  | (aucun)   |
| et on la modifie clic – droit / <b>Modifier</b>                     | <ul> <li>Objets de stratégie de groupe</li> <li>Default Domain Controllers Policy</li> <li>Default Domain Policy</li> <li>Nouvel objet de stratégie de groupe</li> <li>pref - ordi - gestion users locaux</li> </ul>                    |
| <b>N.B</b> : les tp suivant porteront sur "contenu" d'une stratégie | pref - util - mappage sur domaine     if pref - util - mise a l heure - horodatage     if strat - ordi - mise a l heure - horodatage     if strat - ordi - mot de passe simple     if pref - ordi - crer dossier et ciblage os- systeme |





https://www.cabare.net Page 50 - Michel Cabaré -

### 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 Fasily formation and                                   |               |
|--|---------------|
| A Poret : formation.edu                                  | Objets c      |
| 🖃 📑 Domaines   |               |
| 🖃 🏥 formation.edu  | IΓ            |
| Default Domain Policy                                    | $\Rightarrow$ |
| 🕀 🖬 Domain Controllers                                   |               |
| 🖬 test   | $\sim$        |
| 🖃 📑 Obj 🛛 Créer un objet GPO dans ce domaine, et le lier | ici           |
| Lier un objet de stratégie de groupe existant            | · .           |
| Bloquer l'héritage                                       | 3             |

Tous les objets apparaissent

| jets ( | de stratégie de groupe :   |  |
|--------|--|--|
| _      |  |  |
|        | Nom 🔺  |  |
| 1      | Default Domain Controllers Policy  |  |
|        |  |  |
| 1      | Default Domain Policy  |  |
|        | Default Domain Policy<br>Nouvel objet de stratégie de groupe                                       |  |
|        | Default Domain Policy<br>Nouvel objet de stratégie de groupe                                       |  |
|        | Default Domain Policy<br>Nouvel objet de stratégie de groupe<br>pref - ordi - gestion users locaux |  |
|        | Default Domain Policy<br>Nouvel objet de stratégie de groupe<br>pref - ordi - gestion users locaux |  |

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 <u>sa nature</u> (stratégie, préférence... ordinateur, utilisateur...), <u>et son objectif</u> (son action...)





| Pour supprimer la stratégie (et non pas le lien) il suffit de la sélectionner la stratégie et demander  | Modifier<br>État GPO  |
|---|---|
| Supprimer<br>E ist<br>Nouvel objet de stratégie de groupe<br>stratégie de groupe 1<br>stratégie de groupe 2<br>Objets de stratégie de groupe<br>Default Domain Controllers Policy<br>Default Domain Policy<br>Nouvel objet de stratégie de groupe | Sauvegarder<br>Restaurer à partir d'une sauvegarde<br>Importer des paramètres<br>Enregistrer le rapport<br>Nouvelle fenêtre à partir d'îci<br>Copier<br>Supprimer<br>Renommer<br>Actualiser |
| 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   |   |

(par défaut NON)

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

### Vérification des éléments de l'UO:

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

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



Et de même un compte ordinateur...



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



### **Gpresult.exe /R /H depuis 7**

Il existe un utilitaire Disponible depuis 7 permettant d'avoir un compte rendu sur une machine des GPO sui se sont appliquées. Un appel par la ligne de commande **gpresult.exe /R** 



gpresult /R suffira au quotidien



L'option /V est très complète...

gpresult /H permet de générer un fichier HTML exploitable



| d-os-s | ystem | e (C:) >        |   |
|--------|-------|-----------------|---|
|        | ^     | Nom             | ~ |
|        |       | 💽 resultat.html |   |



|             |                              |  | Résultats de str                       | atégie de groupe                  |                         |                             |                            |         |
|-------------|------------------------------|--|--|-----------------------------------|-------------------------|-----------------------------|----------------------------|---------|
| <b>BPAR</b> | E-1\Administrateu            | ir sur CABARE-INTF                           | RA\SPARE-1                             |                                   |                         |                             |                            |         |
| Donnée      | s recueillies le : 11/01/202 | 22 13:28:33<br>des présédentes stratégie d'a | rdinateur actualizer le 11/01/2022 13  | 1-15-20                           |                         | afficher tout               |                            | masquer |
|             | Aucous                       | Annual annual disertie                       | rumateur actualiser le 11/01/2022 15   | .13.27                            |                         |                             |                            |         |
|             | ~                            | Aucune erreur detectee                       | testis Direction                       |                                   |                         |                             |                            |         |
|             | <b>†</b>                     | Une maison rapide a ete det                  | ebiete CDO non emilionée liée en deu   | un de enhane inter net/e neutre   |                         |                             |                            |         |
|             | <b>†</b>                     | L neritage bioque tous les c                 | objets OF O non appliques les au-dess  | sus de cabare-initia.net/2-postes |                         |                             |                            |         |
|             | <b>^</b>                     | Les objets de strategre de g                 | roupe survants ont des alertes special |                                   |                         |                             |                            |         |
|             |                              | Nom d'objet de stratég                       | gie de groupe                          | Alerte                            |                         |                             |                            |         |
|             |                              | Default Domain Policy                        |  | Applique                          |                         |                             |                            |         |
|             |                              |  |  |                                   |                         |                             |                            |         |
|             | Au cours                     | des précédentes stratégie d'u                | tilisateur actualiser le 11/01/2022 09 | :49:24                            |                         |                             |                            |         |
|             | Ø                            | Aucune erreur détectée                       |  |                                   |                         |                             |                            |         |
|             | <u>^</u>                     | Une liaison rapide a été dét                 | tectée Plus d'informations             |                                   |                         |                             |                            |         |
|             |                              |  |  |                                   |                         |                             |                            |         |
| Détails d   | le l'ordinateur              |  |  |                                   |                         |                             |                            | masquer |
| Généra      | 1                            |  |  |                                   |                         |                             |                            |         |
|             |                              |  |  |                                   |                         |                             |                            | masquer |
|             | Nom de l'ordinateur          |  |  |                                   | CABARE-INTRA/SP         | AKE-1                       |                            |         |
|             | Domaine                      |  |  |                                   | cabare-intra.net        |                             |                            |         |
|             | Site                         |  | Ν                                      |                                   | Premier-Site-par-defa   | ut .                        |                            |         |
|             | Unité d'organisation         |  | 145                                    |                                   | cabare-intra.net/z-post | tes/salle-cours-2-srv-spare |                            |         |
|             | Bloquer l'héritage           |  |  |                                   | cabare-intra.net/z-post | ites                        |                            |         |
|             | Adhesion au groupe o         | de securite                                  |  |                                   | atticher                |                             |                            |         |
| État du     | composant                    |  |  |                                   |                         |                             |                            |         |
|             | New designers                |  | Status                                 | Wenne ob etc                      |                         | Wenne das desertes anno     | المستعمل المستعمل المستعمل | masquer |
|             | nom de composant             |  | Statut                                 | rieure photo                      | 145                     | meure au aernier processus  | Journal des evenements     |         |
|             | intrastructure de strate     | gie de groupe                                | Operation reussie                      | i seconde(s) 40 millise           | conde(s)                | 11/01/2022 15:15:29         | Amcher le journal          |         |

#### Avec

| Paramètres  | masquer         |
|---|-----------------|
| Stratégies  | masquer         |
| Paramètre: Windows  |                 |
| Script  | - Of shore      |
| Paramètres de sécurité  | antener         |
| Modèles d'administration  | amener          |
| Prifireases   | <u>afficher</u> |
| Paramètres Windows  | masquer         |
| Fibin   | masquer         |
| · anno  | afficher        |
|   | afficher        |
| Argaine   | <u>afficher</u> |
| Paramètres du Panneau de configuration  | masquer         |
| Utilitateura et groupes locaux  | afficher        |
| Services  | afficher        |
| Objet: de stratégie de groupe   | masquer         |
| Objets GPO appliqués  | masquer         |
| Default Domain Policy [(31B27340-016D-11D2-948F-00C04FB984F9)] Log  | afficher        |
| pref-ordi-copie-batch-programdata-startup-mappage-lecteur-R-commun [[A3590841-592.A-4C04-B560-085EB9687AEB]]                | afficher        |
| pref-ordi-ok-ajout-utiliisteur-domaine-compte-local-poste [[DSFSSB1A-91B2-474D-AD20-S9BDD0AF1AE6)]                          | afficher        |
| pref-ordi-ok-dezactiva-demarrage-rapide-via-registre [[4EE08096-4DAC-4AAD-B4AB-F90EF7830F89]]                               | afficher        |
| pref-ordi-ok-interface-avatar-l-creation-donier [[ED6072E6-2A11-4569-9E40-B9A49DB04C94]]                                    | affichar        |
| pref-ordi-ok-interface-avatar-2-copie-contenu-dossier-avatar-depuis-lan [[1056BB97-5761-4F34-933E-CF7C9B77BDF4]]            | afficher        |
| pref-ordi-ok-interface-avatar-3-copie-contenu-dossier-avatar-dans-account-pictures [[FD442C3E-E903-4B31-BA90-0A536E94D6BF]] | amener          |
| pref-ordi-ok-interface-avatar-4-strategie-avatar-compte-par-defaut [[413F1F4E-ED22-4963-876C-7D2EF51C7F2B}]                 | antener         |

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



# **RSOP JEU DE STRATEGIE RESULTANT**

### RSop.msc resultant set of policy (local)

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

#### rsop.msc

Il permet de donner la situation, par défaut,

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

| Le jeu de stratégies résultant est en co   | ours de traitement   |
|--|--|
| Cette console MMC contient le composa<br>À partir de Microsoft Windows Vi<br>résultant pour l'ordinateur (RSOP<br>groupe Microsoft. Si vous voulez<br>groupe Microsoft appliqués pour<br>commande coresult.<br>Veuillez patienter pendant le traitement. | nt logiciel enfichable RSoP défini ci-dessous.<br>ista Service Pack 1 (SP1), le rapport du jeu de stratégies<br>) ne montre pas tous les paramètres de stratégie de<br>z afficher le jeu complet des paramètres de stratégie de<br>un ordinateur ou un utilisateur, utilisez l'outil de ligne de |
| Sélection<br>Mode<br>Nom d'utilisateur<br>Afficher les paramètres de stratégie<br>Nom de l'ordinateur<br>Afficher les paramètres de stratégie  | Paramètres<br>Enregistrement<br>WIN10-171\Administrateur<br>Oui<br>FORM1\WIN10-171<br>Oui  |
| État d'avancement :  |  |

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

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









Entrez le nom d'un programme, Windows l'ouvrira pour vous.

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



### RSop.msc autre utilisateur - ordinateur

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

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





https://www.cabare.net Page 56 - Michel Cabaré - On peut changer cela, en fonction des droits avec lesquels on est connecté, en demandant Modifier la requête...



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

| istant Jeu de stratégie résultant   |  |
|---|--|
| Aperçu des sélections<br>La liste contient les sélections effect  | tuées dans cet Assistant.  |
|   |  |
| Pour modifier vos sélections, cliquez su<br>cliquez sur Suivant.<br>Sélection   | r Précédent. Pour recueillir les paramètres de stratégie,<br>Paramètres  |
| Pour modifier vos sélections, cliquez su<br>cliquez sur Suivant.<br>Sélection<br>Mode   | r Précédent. Pour recueillir les paramètres de stratégie,<br>Paramètres<br>Enregistrement  |
| Pour modifier vos sélections, cliquez su<br>cliquez sur Suivant.<br>Sélection<br>Mode<br>Nom d'utilisateur  | r Précédent. Pour recueillir les paramètres de stratégie,<br>Paramètres<br>Enregistrement<br>WIN10-171 \andré                          |
| Pour modifier vos sélections, cliquez su<br>cliquez sur Suivant.<br>Sélection<br>Mode<br>Nom d'utilisateur<br>Afficher les paramètres de stratégie                        | r Précédent. Pour recueillir les paramètres de stratégie,<br>Paramètres<br>Enregistrement<br>WIN10-171\andré<br>Oui                    |
| Pour modifier vos sélections, cliquez su<br>cliquez sur Suivant.<br>Sélection<br>Mode<br>Nom d'utilisateur<br>Afficher les paramètres de stratégie<br>Nom de l'ordinateur | r Précédent. Pour recueillir les paramètres de stratégie,<br>Paramètres<br>Enregistrement<br>WIN10-171\andré<br>Oui<br>FORM1\WIN10-171 |





https://www.cabare.net - Michel Cabaré -

### Mmc Jeu de stratégie résultant

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

Et dans lequel on demande Generer les donnees RSUP...

🚟 Console1 - [Racine de la console\Jeu de stratégie résultant]

| 🚟 Fichier Action Affichage   | Favoris Fenêtre ?            |
|------------------------------|------------------------------|
| 🗢 🔿 🙍 🖬                      |                              |
| 📔 Racine de la console       | 🧉 Jeu de stratégie résultant |
| 🧾 Jeu de stratégie résultant |                              |
|                              | Générer les données RSoP     |
|                              | Generer les données Nobr     |

### En Mode Journalisation

| Sélection du mode<br>Vous pouvez afficher les paramètres de stratégie appliqués à un ordinateur ou un<br>utilisateur sélectionné, ou simuler une implémentation de stratégie.<br>Quel mode voulez-vous utiliser ? | ×  |
|---|--|
| Quel mode voulez-vous utiliser ?  | le stratégie appliqués à un ordinateur ou un<br>implémentation de stratégie. |
| Mode de la umalication  |  |
| C Mode de journaisation   |  |
| Vérifier les paramètres de stratégie appliqués à un ordinateur ou un<br>utilisateur spécifique.   | e appliqués à un ordinateur ou un  |

### **Erreur RPC – changement d'ordinateur**

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

| Erreur d        | le stratégie de groupe   | ×      |
|-----------------|--|--------|
| <u> </u>        | Le composant logiciel enfichable RSoP n'a pas pu<br>générer les données RSoP en raison de l'erreur<br>indiquée ci-dessous. | Fermer |
| Détail<br>Le se | s :<br>rveur RPC n'est pas disponible.   |        |

Il faut penser à ouvrir dans le  $\ensuremath{\text{Pare-feu}}$  les accès administration distante et  $\ensuremath{\text{WMI}}$ 





### Rsop dans la console Gestion de stratégie de groupe

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

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



| Assistant Résultats de stra   | atégie de groupe  | ×        |                  |          |
|---|---|----------|------------------|----------|
|   | Assistant Résultats de stratégie<br>de groupe<br>Cet Assistant vous aide à vérifier les paramètres de stratégies<br>d'un utilisateur ou d'un ordinateur. L'Assistant interroge<br>l'ordinateur de l'utilisateur et génère un rapport à partir du jeu<br>de stratégies résultant actuellement déployé. |          |                  |          |
| On peut indiquer n'in   | nporte quel ordinateur du Domaine   |          |                  |          |
| Assistant Résultats de stra   | atégie de groupe  | $\times$ |                  |          |
| Sélection des ordinal<br>Vous pouvez affiche<br>ordinateur sur ce rés | t <b>eurs</b><br>r les paramètres de stratégie pour cet ordinateur ou pour un autre<br>eau.   |          | roupe            |          |
| Sélectionnez l'ordinateur   | pour lequel vous voulez afficher les paramètres de la stratégie.  |          | Ordinateur       | Date     |
| ◯ Cet ordinateur  |   |          |                  |          |
| O Un autre ordinateur :   |   |          |                  |          |
|   | Parcourir   |          |                  |          |
|   | Sélectionnez un ordinateur  |          |                  | $\times$ |
| Ne pas afficher dans<br>(afficher uniquement                          | Sélectionnez le type de cet objet :   |          |                  |          |
|   | un ordinateur   |          | Types d'objets.  |          |
|   | À partir de cet emplacement :   |          |                  |          |
|   | form1.edu   |          | Emplacements.    |          |
|   | Entrez le nom de l'objet à sélectionner ( <u>exemples</u> ) :   |          |                  |          |
|   | win10-171   |          | Vérifier les nom | 3        |



https://www.cabare.net - Michel Cabaré -

### Et un utilisateur souhaité

| Assistant Résultats de stratégie de groupe   | × |
|--|---|
| Sélection de l'utilisateur<br>Vous pouvez afficher les paramètres de stratégie pour les utilisateurs de l'ordinateur<br>sélectionné.   |   |
| Afficher les paramètres de la stratégie de :   |   |
| Utilisateur actuel   |   |
| Sélectionner un utilisateur spécifique :   |   |
| FORM1\Administrateur<br>WIN10-171\Administrateur<br>WIN10-171\andré<br>WIN10-171\Bruno   |   |
| Cette liste affiche uniquement les utilisateurs qui se sont connectés à l'ordinateur ou<br>pour lesquels vous avez l'autorisation de lire les données des résultats de stratégie<br>de groupe. |   |
| O Ne pas afficher les paramètres de stratégie utilisateur (uniquement les paramètres ordinateur)   |   |

On peut donc se construire un ensemble de test...

- Résultats de stratégie de groupe
   Administrateur sur SRVDC1-FORM16
   andré sur WIN10-171
   Bruno sur WIN10-171
- Et la lecture pour chacun est détaillée

| 📓 Gestion de stratégie de groupe  |   |                       |
|---|---|-----------------------|
| Fichier Action Affichage Fenêtre ?                                      |   | _ 5                   |
| 🗢 🔿   🙋 🔲   |   |                       |
| Gestion de stratégie de groupe<br>✓ ▲ Forêt : form1.edu<br>✓ ▲ Domaines | Administrateur sur SRVDC1-FORM16<br>Résumé Détails Événements de stratégie                            |                       |
| > 🏥 form1.edu   | Paramètres  | masquer               |
| > 🙀 Sites   | Stratégies  | masquer               |
| Modélisation de stratégie de groupe                                     | Paramètres Windows  | masquer               |
| Administrateur sur SRVDC1-FORM16  | Paramètres de sécurité  | masquer               |
| andré sur WIN10-171   | Stratégies de comptes/Stratégie de mot de passe   | masquer               |
| 🖆 Bruno sur WIN10-171   | Stratégie Paramètre   | OSG gagnant           |
|   | Antériorité maximale du mot de passe 42 jours   | Default Domain Policy |
|   | Antériorité minimale du mot de passe 1 jours  | Default Domain Policy |
|   | Appliquer l'historique des mots de 24 mots de passe mémorisés<br>passe                                | Default Domain Policy |
|   | Enregistrer les mots de passe en Désactivé<br>utilisant un chiffrement réversible                     | Default Domain Policy |
|   | Le mot de passe doit respecter des Activé<br>exigences de complexité                                  | Default Domain Policy |
|   | Longueur minimale du mot de passe 7 caractères  | Default Domain Policy |
|   | Stratégies de comptes/Stratégie de verrouillage du compte   | afficher              |
|   | Stratégies de comptes/Stratégie Kerberos  | afficher              |
|   | Stratégies locales/Attribution des droits utilisateur   | afficher              |
|   | Stratégies locales/Options de sécurité  | afficher              |
|   | Stratégies de clé publique/Client des services de certificats - Paramètr<br>d'inscription automatique | es<br>afficher        |
|   | Stratégies de clé publique/Système de fichiers de chiffrement   | afficher              |



# **HIERARCHIE DES STRATEGIES**

### Ordre final d'application des stratégies :

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

## **Clients Hors Domaine**

Pour des clients 11, 10 SEVEN XP(PRO) ou serveur 2022-2019-à-2008R2
 stratégies locales - & MLGPO

## Clients du Domaine Hors Contrôleurs de Domaine

• Pour des client 10 SEVEN XP(PRO) ou les serveurs 2022-2019 à -2008R2 membres:

## stratégies locales / stratégies de domaine

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

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

et si la notion de site est activée

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

## Contrôleurs de Domaine

• Pour des serveurs 2022 2019 à -2008R2

## stratégies locales / stratégies de domaine / stratégies de CD

et si la notion de site est utilisée

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

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

## stratégies de domaine / stratégies de CD

et si la notion de site est utilisée

stratégies de site /stratégies de domaine / stratégies de CD

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



## LIAISONS MULTIPLES - PRIORITE -HERITAGE-GPO

### Liaison de GPO :

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

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

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



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

## Priorité de GPO :

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

stratégie de groupe 1 stratégie de groupe 2



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

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

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





### dans l'exemple ci-dessous

| forma         | tion.edu               |                                 |           |             |          |            |            |
|---------------|------------------------|---------------------------------|-----------|-------------|----------|------------|------------|
| Objets        | de stratégie de groupe | liés Héritage de stratégie de g | roupe Dél | égation     |          |            |            |
|               |                        |                                 |           |             |          |            |            |
|               | Ordre des liens 🔺      | Objet de stratégie de groupe    | Appliqué  | Lien activé | État GPO | Filtre WMI | Modifié le |
| $\Rightarrow$ | 1                      | 🛒 Default Domain Policy         | Non       | Oui         | Activé   | Aucun(e)   | 02/06/     |
|               | 2                      | 🗐 affichage-message-test        | Non       | Oui         | Activé   | Aucun(e)   | 02/06/     |
| $\sim$        | 3                      | 🗊 affiche-message-beta          | Non       | Oui         | Activé   | Aucun(e)   | 02/06/     |

- les machines affichent le message "TEST" car la défaut policy elle , ne fait rien afficher..
- pour que les machines affichent le message "BETA" il faut élever l'ordre du lien de la GPO beta, comme ci-dessous

| forma         | tion.edu                 |                                |             |             |          |            |            |
|---------------|--------------------------|--------------------------------|-------------|-------------|----------|------------|------------|
| Objets        | de stratégie de groupe l | iés Héritage de stratégie de g | roupe   Dél | égation     |          |            |            |
|               | Ordre des liens 🔺        | Objet de stratégie de groupe   | Appliqué    | Lien activé | État GPO | Filtre WMI | Modifié le |
| $\Rightarrow$ | 1                        | 🗊 Default Domain Policy        | Non         | Oui         | Activé   | Aucun(e)   | 02/06/     |
|               | 2                        | 🗊 affiche-message-beta         | Non         | Oui         | Activé   | Aucun(e)   | 02/06/     |
|               | 3                        | 🗊 affichage-message-test       | Non         | Oui         | Activé   | Aucun(e)   | 02/06/     |

### héritage – bloqué :

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

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

| - | Ê. | 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 Gestion de stratégie de groupe test A Forêt : formation.edu Objets de stratégie de groupe liés Héritage de stratégie de groupe Délégation 🗆 📑 Domaines Cette liste n'inclut aucun objet de stratégie de groupe lié à des sites. Pour obtenir plus d'informations 🖃 🏥 formation.edu Default Domain Policy
 Domain Controllers Priorité Objet de stratégie de groupe + 🗊 production 1 stratégie de groupe 1 🖃 📋 test 🛒 Nouvel objet de stratégie de groupe 2 Nouvel objet de stratégie de groupe H. 🛒 stratégie de groupe 1 J. 3 stratégie de groupe 2 4 T Default Domain Policy 🛒 stratégie de groupe 2 표 📑 Objets de stratégie de groupe Et ainsi de suite

| El dinsi de sulle  |  |                                     |
|--|--|-------------------------------------|
| A Forêt : formation.edu<br>□  B Domaines<br>□  B formation.edu<br>B Default Domain Policy<br>□  Domain Controllers                                 | Objets de stratégie de groupe liés Héritage de st<br>Cette liste n'inclut aucun objet de stratégie de grou                                   | ratégie de <u>c</u><br>upe lié à de |
|  | Priorité  Objet de stratégie de groupe I Nouvel objet beta de stratégie e  | de aroupe                           |
| <ul> <li>test</li> <li>Nouvel objet de stratégie de groupe</li> <li>stratégie de groupe 1</li> <li>stratégie de groupe 2</li> <li>ineta</li> </ul> | 2     stratégie de groupe 1       3     Nouvel objet de stratégie de gro       4     stratégie de groupe 2       5     Default Domain Policy | upe                                 |
| Nouvel objet beta de stratégie de groupe   |  |                                     |



https://www.cabare.net Page 63 - Michel Cabaré -

Emplacement

formation.edu

s sites. Pour obtenir plus d'informations

Emplacement beta test test test formation.edu

test

test

test

roupe Délégation

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

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



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

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



par exemple sur l'UO test

Cela se traduit par un Point d'exclamation !



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





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

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





### héritage - appliqué:

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

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



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



Cela se traduit par un Cadenas!



On se place dessus et on demande clic-droit Appliqué

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



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 ot

 Priorité
 Objet de stratégie de groupe

 I (appliqué)
 Default Domain Policy

 2 (appliqué)
 stratégie de groupe 2

 3
 Nouvel objet beta de stratégie de groupe



### Priorité de GPO Ordre et héritage :

L'ordre d'application des GPO c'est de bas en haut pour que les GPO de priorité les plus fortes, soient appliquées en dernier !







## **GPO - MODELES D'ADMINISTRATION**

### Les Modèles présents

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

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

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

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

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



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





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

| électionnez le type de paramà  | tras da stratágia à affichar  |   |          |
|--|---|---|----------|
| Géré :   | Configuré :   | Commentés :   |          |
| Oui 🗸  | Oui ~   | Nîmporte leqi $ \smallsetminus $                                      |          |
| Activer les filtres par mots d   | és  |   |          |
| Filtrer par le ou les  |   | Nîmporte la   | q. ~     |
| mores '  |   |   |          |
| Dans : Titre param   | . de stratégie 🗸 Texte d'aid  | e 🗸 Commentai   | re       |
| Dans ; Titre param   | . de stratégie 🛛 Texte d'aid  | e 🗹 Commentai   | re       |
| Dans : Titre param   | n. de stratégie ⊡ Texte d'aid   | e 🗹 Commentai   | re       |
| Dans : Titre param   | I. de stratégie   | e 🗹 Commentai   | re       |
| Dans : Titre param<br>Activer les filtres de conditio<br>Sélectionnez le ou les filtres d<br>Induez les paramètres qui co  | <ul> <li>de stratégie  Texte d'aid</li> <li>ns</li> <li>l'application et de plateforme soul</li> <li>porrespondent à l'une quelconque of</li> </ul>   | e ✓ Commentai<br>naités :<br>les plz ✓ Sélectionner t                 | put      |
| Dans :<br>Activer les filtres de conditio<br>Sélectionnez le ou les filtres d<br>Induez les paramètres qui co  | a. de stratégie<br>Texte d'aid<br>ns<br>l'application et de plateforme soul<br>prrespondent à l'une quelconque d<br>provindows XP   | e Commentai   | put      |
| Activer les filtres de conditio<br>Sélectionnez le ou les filtres d<br>Induez les paramètres qui co  | <ul> <li>de stratégie  Texte d'aid</li> <li>ns</li> <li>l'application et de plateforme soul<br/>prrespondent à l'une quelconque on<br/>Windows XP<br/>on Windows 10</li> </ul>  | e Commentai<br>haités :<br>les pla ~<br>Sélectionner t<br>Effacer tou | out      |
| Dans : ☐ Titre param<br>Activer les filtres de conditio<br>Sélectionnez le ou les filtres d<br>Induez les paramètres qui co<br>  | I. de stratégie<br>Texte d'aid<br>Ins<br>l'application et de plateforme soul<br>prrespondent à l'une quelconque o<br>on Windows XP<br>on Windows 10<br>RT   | e Commentai<br>haités :<br>les pla ~<br>Sélectionner t<br>Effacer tou | out      |
| Dans : ☐ Titre param<br>Activer les filtres de conditio<br>Sélectionnez le ou les filtres de<br>Induez les paramètres qui co<br>   | I. de stratégie Texte d'aid Ins I'application et de plateforme soul prrespondent à l'une quelconque o privindows XP privindows 10 privindows 10 RT privindows 10 Server   | e Commentai<br>naités :<br>les pla V<br>Sélectionner t<br>Effacer tou | out      |
| Dans : Titre param<br>Activer les filtres de conditio<br>Sélectionnez le ou les filtres d<br>Induez les paramètres qui co<br>Systèmes d'exploitatio<br>Systèmes d'exploitatio<br>Windows 10<br>Systèmes d'exploitatio<br>Systèmes d'exploitatio<br>Windows Installer ver | I. de stratégie Texte d'aid Ins I'application et de plateforme soul prrespondent à l'une quelconque o privespondent à l' | e Commentai   | out<br>t |
| Dans : Titre param<br>Activer les filtres de conditio<br>Sélectionnez le ou les filtres de<br>Induez les paramètres qui co<br>   | I. de stratégie Texte d'aid Ins I'application et de plateforme soul orrespondent à l'une quelconque o on Windows XP on Windows 10 on Windows 10 RT on Windows 10 Server sion 2 sion 3   | e Commentai   | out<br>t |

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





### Stockage des Modèles de GPO – sur chaque DC

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

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



Default Domain Controllers Policy Default Domain Policy

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

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

N.B: On peut se rendre compte lorsque l'on modifie dans une GPO un réglage en provenance d'un modèle d'administration, par l'apparition de la mention « définition de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local » Stratégie Nouvel objet de stratégie de groupe [SRVDC1-FORM16.FORM1.EDU]



Pourquoi cela peut poser probleme :

Soit 2 DC dans un Domaine, DC1 et DC2

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





### Magasin Central - centralisation des Modèles de GPO

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

## Trouver le DC ayant le rôle PDC

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



Et on regarde qui est CDP Controlleur de domaine Principal

| Maître d'opérations ?   |     |                |  |  |  |  |  |
|---|-----|----------------|--|--|--|--|--|
| RID   | CDP | Infrastructure |  |  |  |  |  |
| Le maître d'opérations émule les fonctions d'un contrôleur de domaine<br>principal pour les clients antérieurs à Windows 2000. Seul un serveur du<br>domaine joue ce rôle.<br>Maître d'opérations : |     |                |  |  |  |  |  |
| srvdc1form16.form1.edu  |     |                |  |  |  |  |  |
| Pour transférer le rôle de maître d'opérations à l'ordinateur Modifier  |     |                |  |  |  |  |  |

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

| Gestionnaire du pool RID srvdc1-form16.form1.edu<br>Maître d'infrastructure srvdc1-form16.form1.edu<br>L'opération s'est bien déroulée. | C:\Windows\system32>netdom query fsmo<br>Contrôleur de schéma srvdc1-form16.form1.e<br>Maître des noms de domaine srvdc1-form16.form1.e<br>Contrôleur domaine princip. srvdc1-form16.form1.e<br>Gestionnaire du pool RID srvdc1-form16.form1.e<br>Maître d'infrastructure srvdc1-form16.form1.e<br>L'opération s'est bien déroulée. | edu<br>edu<br>edu<br>edu<br>edu |
|---|---|---------------------------------|
|---|---|---------------------------------|

## Création du dossier PolicyDefinitions

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





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

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



## Copier les modèles de GPO

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

Au lieu de tous les modèles (anciennement)



On a maintenant 0 modèles, dans le Magasin Central...

Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à partir du magasin central.
Tous les paramètres

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





### Ajout suppression des Modèles de GPO

- Pour les nouveaux Modèles a base de fichier ADMX il faut copier les fichiers dans le dossier de stockage, donc soit
  - o le dossier local de la machine
  - o le magasin central dans sysvol
- Pour les anciens Modèle a base de fichier ADM, on pouvait demander via un clic droit sur la console, Modèle D'administration / Ajout Suppression de modèles...

| <ul> <li>Stratégie Nouvel objet de stratégie de groupe [Si</li> <li>Marcia Configuration ordinateur</li> <li>Stratégies</li> </ul> |           | G Modèles d'administration : définitions de stratégies (fichiers ADMX |                     |           |  |
|--|-----------|---|---------------------|-----------|--|
|  |           | Sélectionnez un élément pour obtenir<br>une description.              |                     | Paramètre |  |
| > Paramètres du logiciel > Paramètres Windows  |           |   | Ious les parametres |           |  |
| <ul> <li>Modèles d'administration : définit</li> </ul>   | io Ajout/ | Ajout/Suppression de modèles X Modèles de stratégie actuels :         |                     |           |  |
| 🖺 Tous les paramètres  |           |   |                     |           |  |
| > Préférences  | Modèl     |   |                     |           |  |
| <ul> <li>Konfiguration utilisateur</li> <li>Stratégies</li> <li>Préférences</li> </ul>   | Nom       | Nom   |                     | Modifié   |  |
|  |           |   |                     |           |  |

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

### Trouver des Modèles de GPO – technet WIKI

On peut trouver des modèles un peu... partout

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

## **1 Sélection - Technet WIKI**

Faire une recherche sur google avec le titre du WIKI



Selected Content Relating to Group Policy Administrative Templates (ADM and ADMX)


#### Avec un choix sélectif, mais vaste !

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

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

ADM and ADMX Downloads for MS Internet Explorer

Administrative Templates for Internet Explorer 11 🗹

This page provides the Group Policy Administrative Template files for Internet Explorer 11. Administrative Templates for Windows Internet Explorer 10 12

This page provides the Group Policy Administrative Template files for Windows Internet Explorer 10.

\*\* Warning: IE10 deprecates/removes the IEM methods.

Refer: AskIEBlog Z

Administrative Templates for Windows Internet Explorer 9 🗹

This page provides the Group Policy Administrative Template files for Windows Internet Explorer 9 Administrative Templates for Internet Explorer 7 for Windows 🗹

This page provides the Group Policy Administrative Template file for Internet Explorer 7 for Windows.

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

ADM and ADMX Downloads for MS Office

Office 2016 Administrative Template files (ADMX/ADML) and Office Customization Tool

This download includes Group Policy Administrative Template (ADMX/ADML) and Office Customization Tool (OPAX/OPAL) files for Microsoft Office 2016.

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

This download includes Group Policy Administrative Template (ADMX/ADML) and Office Customization Tool (OPAX/OPAL) files for Microsoft Office 2013.

Office 2013 Help Files: Office Fluent User Interface Control Identifiers Id

This download details the ControlIDs needed for OFF2013, if you want to disable specific UI controls, buttons, menu items, via a registry policy.





# 1 Liste exhaustive - https://admx.help/

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



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



#### Télécharger et installer un Modèles de GPO – office 2013

Essayons de télécharger et installer un templates pour office 2013







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

| Language: | English | Download |
|-----------|---------|----------|

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

Choose the download you want

| File Name                              | Size    |  |
|--|---------|--|
| admintemplates_x64_4869-1000_en-us.exe | 11.6 MB | Download Summary:<br>1. admintemplates_x86_4869-1000_en-us.exe |
| admintemplates_x86_4869-1000_en-us.exe | 11.4 MB |  |

# Il faut le désarchiver, et l'executant

| Nom                                      | Modifié le       | Туре        | Taille    |
|--|------------------|-------------|-----------|
| 🝘 admintemplates_x86_4869-1000_en-us.exe | 16/06/2017 18:45 | Application | 11 661 Ko |

#### Pour obtenir

| Nom  | Modifié le       | Туре                | Taille    |
|--|------------------|---------------------|-----------|
| i office2013grouppolicyandoctsettings.xlsx | 22/09/2016 20:27 | Feuille de calcul   | 565 Ko    |
| 鐞 admintemplates_x86_4869-1000_en-us.exe   | 16/06/2017 18:46 | Application         | 11 661 Ko |
| 📊 admx                                     | 16/06/2017 18:47 | Dossier de fichiers |           |
| 📊 admin                                    | 16/06/2017 18:47 | Dossier de fichiers |           |

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

| access15.admx | 22/09/2016 20:27 | Fichier ADMX | 116 Ko   |
|---------------|------------------|--------------|----------|
| excel15.admx  | 22/09/2016 20:27 | Fichier ADMX | 264 Ko   |
| inf15.admx    | 22/09/2016 20:27 | Fichier ADMX | 110 Ko   |
| lync15.admx   | 22/09/2016 20:27 | Fichier ADMX | 35 Ko    |
| office15.admx | 22/09/2016 20:27 | Fichier ADMX | 1 367 Ko |
| onent15.admx  | 22/09/2016 20:27 | Fichier ADMX | 119 Ko   |
| outlk15.admx  | 22/09/2016 20:27 | Fichier ADMX | 598 Ko   |
| ppt15.admx    | 22/09/2016 20:27 | Fichier ADMX | 199 Ko   |
| proj15.admx   | 22/09/2016 20:27 | Fichier ADMX | 279 Ko   |
| pub15.admx    | 22/09/2016 20:27 | Fichier ADMX | 59 Ko    |
| spd15.admx    | 22/09/2016 20:27 | Fichier ADMX | 37 Ko    |
| visio15.admx  | 22/09/2016 20:27 | Fichier ADMX | 144 Ko   |
| word15.admx   | 22/09/2016 20:27 | Fichier ADMX | 432 Ko   |

# dossiers de langue fr-fr et en-us

| Nom   | <u>n</u> | Modifié le       | Туре                | Taille |
|-------|----------|------------------|---------------------|--------|
| de-de |          | 16/06/2017 18:47 | Dossier de fichiers |        |
| en-us |          | 16/06/2017 18:47 | Dossier de fichiers |        |
| es-es |          | 16/06/2017 18:47 | Dossier de fichiers |        |
| fr-fr |          | 16/06/2017 18:47 | Dossier de fichiers |        |

Il faut copier tout cela dans notre Magasin Central

# Du coup on aura désormais



- Stratégie Nouvel objet de stratégie de groupe [SRVDC1-FORM16.FORM1.EDU]
- 🗸 👰 Configuration ordinateur
  - ✓ <sup>™</sup> Stratégies
    - 🔉 🧮 Paramètres du logiciel
    - > 🧮 Paramètres Windows
    - Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à p
      - > Composants Windows
        - Imprimantes
        - Menu Démarrer et barre des tâches
      - > Microsoft InfoPath 2013 (ordinateur)
      - > Microsoft Lync 2013
      - > Microsoft Office 2013 (ordinateur)
      - > Microsoft PowerPoint 2013 (ordinateur)
      - > Panneau de configuration
      - > 📔 Réseau
      - 📔 Serveur
      - > 📔 Système
        - 📲 Tous les paramètres

#### Εt

- 🐔 Configuration utilisateur
- 🗸 📔 Stratégies
  - 🔉 🚞 Paramètres du logiciel
  - > 🣔 Paramètres Windows
  - Modèles d'administration : définitions de stratégies (fichiers ADMX) récupérées à p
    - > 🚞 Bureau
    - > 📔 Composants Windows
      - 📔 Dossiers partagés
    - 🔉 🧮 Menu Démarrer et barre des tâches
    - > Microsoft Access 2013
    - > Microsoft Excel 2013
    - > Intervention Microsoft InfoPath 2013
    - > 📔 Microsoft Lync 2013
    - > Microsoft Office 2013
    - > Intervention Microsoft OneNote 2013
    - > Interest of the second se
    - > Microsoft PowerPoint 2013
    - > Interpretention of the second se
    - > Microsoft Publisher 2013
    - > Microsoft SharePoint Designer 2013
    - > i Microsoft Visio 2013
    - > 🎽 Microsoft Word 2013
    - 🔉 🚞 Panneau de configuration
    - > 🚞 Réseau
    - > 📔 Système
      - 📲 Tous les paramètres

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



### Télécharger et installer un Modèles de GPO – Windows 10 v1803

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

| 😽 Administrative     | Templates (.admx) for  | Windows 10 April 2018 U                          | lpdate.msi                                   | 17/05/2    | 018 09:05       | Package Windows | 14 322 Ko |
|----------------------|--|--|--|------------|-----------------|-----------------|-----------|
| Pour obtenir         |  |  |  |            |                 |                 |           |
| 波 Admi               | nistrative Templates (.admx)   | for Windows 10 April 2018                        |  | ×          |                 |                 |           |
| Welc<br>for W        | ome to the Adminis<br>indows 10 April 20                             | strative Templates (<br>18 Update Setup V        | .admx)<br>Vizard                             |            |                 |                 |           |
| The insta<br>Windows | aller will guide you through the s<br>s 10 April 2018 Update on your | teps required to install Administra<br>computer. | tive Templates (.a                           | dmx) for   |                 |                 |           |
| G                    |  |  |  |            |                 |                 |           |
| WARNIN               | IG: This computer program is p                                       | rotected by copyright law and inte               | ernational treaties.<br>It may result in sev | vere civil |                 |                 |           |
| or crimina           | al penalties, and will be prosecu                                    | ited to the maximum extent possil                | ble under the law.                           | ere civil  |                 |                 |           |
|                      |  |  |  |            |                 |                 |           |
|                      |  | Cancel < Ba                                      | ick Ni                                       | ext >      |                 |                 |           |
|                      | _  |  |  |            |                 |                 |           |
|                      | en-US  |  | 17/05/2018                                   | 09:26      | Dossier de fich | niers           |           |
|                      | es-ES  |  | 17/05/2018                                   | 09:26      | Dossier de fich | niers           |           |
|                      | fi-Fl  |  | 17/05/2018                                   | 09:26      | Dossier de fich | niers           |           |
|                      | fr-FR  |  | 17/05/2018                                   | 09:26      | Dossier de fich | liers           |           |
|                      | hu-HU  | N  | 17/05/2018                                   | 09:26      | Dossier de fich | ners            |           |
|                      | l it-ll  |  | 1//05/2018                                   | 09:26      | Dossier de fich | ners            |           |
|                      | ActiveXInstallServ   | ice.admx   | 03/05/2018                                   | 14:56      | Fichier ADMX    |                 |           |
|                      | AddRemoveProgr   | ams.admx   | 03/05/2018                                   | 14:56      | Fichier ADMX    |                 |           |
|                      |  | v.admx   | 03/05/2018                                   | 14:50      | Fichier ADMX    |                 |           |
|                      | AppCompat.adm  | C  | 03/05/2018                                   | 14:50      | Fichier ADMX    |                 |           |
|                      |  |  | 03/05/2018                                   | 14:00      | Fichier ADMX    |                 |           |
|                      | AppPrivacy.admx  |  | 03/05/2018                                   | 14:50      | Fichier ADMX    |                 |           |
|                      | appv.admx  |  | 03/05/2018                                   | 14:50      | Fichier ADMX    |                 |           |

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

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

| ➤ modeles-gpo-ajoutes                                 | ^ | Nom                        | Modifié le               |
|---|---|----------------------------|--------------------------|
| <ul> <li>PolicyDefinitions-windows-10-1803</li> </ul> |   | en-US                      | 17/05/2018 09:41         |
| en-US   |   | fr-FR                      | 17/05/2018 09:41         |
| fr-FR   |   | ActiveXInstallService.admx | 03/05/2018 14:56         |
| v windows-update-10-1803                              |   | AddRemovePrograms.admx     | 03/05/2018 14:56         |
| fr-FR   |   | AllowBuildPreview.admx     | 03/05/2018 14:56         |
| windows-undate-origine-sry-2016                       |   | AppCompat.admx             | 03/05/2018 14:56         |
|   |   | AppHVSI.admx               | 03/05/2018 14:56         |
| II-FK   |   | A                          | 00/0E/0010 1 <i>4.EE</i> |



https://www.cabare.net Page 77 - Michel Cabaré - L'idée est que par rapport à un ebsemble de mises à jour disponibles, comme ici à la sortie d'une nouvelle version de l'OS windows 10 v1803, on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx...

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

| ✓ → windows-update-10-1803      | fr-FR              | 17/05/2018 09:52 |
|---------------------------------|--------------------|------------------|
| 📊 fr-FR                         | WindowsUpdate.admx | 03/05/2018 14:56 |
| Du coup on aura désormais       |                    |                  |
| windows-update-origine-srv-2016 | fr-FR              | 17/05/2018 09:56 |
| fr-FR                           | WindowsUpdate.admx | 12/07/2017 04:49 |
|                                 |                    |                  |

# Télécharger et installer un Modèles de GPO – Windows 10 v1809

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

Administrative Templates (.admx) for Windows 10 October 2018 Update (1809)

| Im                | portant! Selecting a la                     | nguage below will d                       | dynamically change the complete                  | page content              | to that language |                  |  |
|-------------------|---|---|--|---------------------------|------------------|------------------|--|
| Lai               | nguage:                                     | English                                   |  |                           | Downloa          | d                |  |
| This pa<br>10 Oct | age provides th<br>tober 2018 Upc           | ne complete :<br>date (1809)              | set of Administrative                            | Templates                 | (.admx) fo       | r Windows        |  |
| ) D               | etails                                      |   |  |                           |                  |                  |  |
|                   | Version:<br>1.0                             |   |  | Date Publis<br>11/13/2018 | hed:             |                  |  |
|                   | File Name:<br>Administrative Templa<br>.msi | ates (.admx) for Wir                      | ndows 10 October 2018 Update                     | File Size:<br>13.8 MB     |                  |                  |  |
|                   |   |   |  |                           |                  |                  |  |
| On téle           | écharge le fic                              | chier                                     |  |                           |                  |                  |  |
|                   | Ouverture de Admin                          | nistrative Template                       | s (.admx) for Windows 10 Octo                    | ber ×                     |                  |                  |  |
|                   | Vous avez choisi d'<br><sub> </sub>         | 'ouvrir :<br>es (.admx) for Wir           | ndows 10 October 2018 Updat                      | e.msi                     |                  |                  |  |
|                   | qui est un fic<br>à partir de :             | :hier de type : Win<br>https://download.r | dows Installer Package (13,8 Mo<br>nicrosoft.com | )                         |                  |                  |  |
|                   | Voulez-vous enreg                           | istrer ce fichier ?                       |  |                           |                  |                  |  |
|                   |   |   | Enregistrer le fichier An                        | nuler                     |                  |                  |  |
| Nom               |   |   |  | Туре                      |                  | Modifié le       |  |
| 🖶 Admir           | nistrative Templates (.a                    | dmx) for Windows                          | 10 October 2018 Update.msi                       | Pack                      | age Windows      | 26/11/2018 13:28 |  |



https://www.cabare.net Page 78 - Michel Cabaré -

### Et on l'installe



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

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



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



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

| 📙 recup-totale-admx-PolicyDefinitions-windows-10-1809         | ^ | Nom                |
|---|---|--------------------|
| en-US   |   | fr-FR              |
| 📙 fr-FR   |   | OOBE.admx          |
| 📙 remplacement-et-ajout-depuis-les-recup-dans-magasin-central |   | WindowsUpdate.admx |
| fr-FR   |   |                    |





#### **Objectifs des Filtres WMI sur les GPO**

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

La procédure se fait en 2 temps :

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

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

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

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

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

# Création du filtre WMI

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

| 😹 Gestion de stratégie de groupe\Forêt : form1.edu\Domaines\form1.edu \Filtres WMI |               |        |                            |             |                                  |
|--|---------------|--------|----------------------------|-------------|----------------------------------|
| 🔜 Gestion de stratégie de groupe   |               | Filtre | Filtres WMI dans form1.edu |             |                                  |
| 🗸 🔬 Forêt : form1.edu  |               | Conte  | nu Déléc                   | nation      |                                  |
| 🗸 🙀 Domaines   |               |        | -                          | gotion      | 1                                |
| ∨ 🟥 form1.edu  | ✓ i form1.edu |        | ı Û                        | Description | Objet de stratégie de groupe lié |
| Default Domain Policy  |               |        |                            |             |                                  |
| 🛒 mot de passe simplifié   |               |        |                            |             |                                  |
| > 📔 Domain Controllers   |               |        |                            |             |                                  |
| > 📑 Objets de stratégie de groupe  |               |        |                            |             |                                  |
| > 📑 Filtres WM   | I             |        |                            |             |                                  |
| > 🛅 Objets GP(   | Nouveau       |        |                            |             |                                  |
| > 📑 Sites  | Importer      |        |                            |             |                                  |



| Dans la boite de dialogue, il faut  | Nouveau filtre WMI X  |  |  |  |
|---|---|--|--|--|
|   | Nom :   |  |  |  |
|   | selection Windows 10  |  |  |  |
| nommer le script,   | Description :   |  |  |  |
|   | que Windows 10  |  |  |  |
| et surtout écrire la  | Requêtes :  |  |  |  |
| requête qui   | Espace de noms Requête Ajouter  |  |  |  |
| correspondra a notre<br>recherche   | Requête WMI ×   |  |  |  |
| \   | Espace de noms :  |  |  |  |
|   | root\CIMv2 Parcourir  |  |  |  |
|   | Requête :   |  |  |  |
|   | select Version from Win32_OperatingSystem WHERE Version like "10.<br>%" AND ProductType="1" |  |  |  |
| select Version from<br>Win32 OperatingSystem WHERE Version like "10.%" AND ProductType=1" |   |  |  |  |

### Lier la GPO et le filtre WMI

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

| 😹 Gestion de stratégie de groupe\Forêt : form1.edu\Domaine  | s\form1.edu \Objets de stratégie de groupe\Nouvel objet de stratégie de groupe                  |
|---|---|
| Gestion de stratégie de groupe                              | Nouvel objet de stratégie de groupe   |
| ✓ ▲ Forêt : form1.edu                                       | Étendue Détails Paramètres Délégation État  |
| ✓ I Domaines  |   |
| ✓ jii form1.edu   |   |
| Default Domain Policy                                       | fom 1.edu   |
| mot de passe simplifié                                      | Les sites, domaines et unités d'organisation suivants sont liés à cet objet GPO :               |
| Domain Controllers  | Emplacement Appliqué Lien activé Chemin d'av  |
| Objets de strategie de groupe                               |   |
| Default Domain Controllers Policy     Pofault Domain Policy |   |
| mot de parce simplifié                                      |   |
| Nouvel objet de stratégie de groupe                         |   |
| Filtres WMI   | Filtrage de sécurité  |
| > 🛅 Objets GPO Starter                                      | Les paramètres de cet obiet GPO ne s'appliquent qu'à ces groupes, utilisateurs et ordinateurs : |
| > 📑 Sites   |   |
| 👸 Modélisation de stratégie de groupe                       | Nom   |
| > 📴 Résultats de stratégie de groupe                        | Chilisateurs authentifiés   |
|   |   |
|   | Ajouter Supprimer Propriétés  |
|   | Filtrage WMI  |
|   | Cet objet de stratégie de groupe est lié au filtre WMI suivant :                                |
|   | <aucun> V Ouvrir</aucun>  |
|   | k   |
|   | Filtrage WMI  |
|   | Cet objet de stratégie de groupe est lié au filtre WMI suivant :                                |
|   | selection Windows 10  |
|   | <aucun></aucun>   |
|   | selection Windows 10  |

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

Autrement dit on ne peut pas selon les liens GPO-UO choisir en plus le filtre  $\mathsf{W}\mathsf{M}\mathsf{I}$ 



#### Ciblage de préférence

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

Cela permet de choisir le filtre à appliquer parmis ceux disponibles



Par exemple

| 🍸 Éditeur cible   |  |   |                          |                 | ×   |  |
|---|--|---|--------------------------|-----------------|-----|--|
| Nouvel élément 👻  | Ajouter une collection Options de l'él   | ément 🗕 📥 🗮 👗   | <b>b B</b> •             | -               | **  |  |
| 😻 le système d  | 🐲 le système d'exploitation est Windows 10 (édition Professional)                      |   |                          |                 |     |  |
|   |  | $\searrow$  |                          |                 |     |  |
|   |  |   |                          |                 |     |  |
|   |  |   |                          |                 |     |  |
|   |  |   |                          |                 |     |  |
|   |  |   |                          |                 |     |  |
| Produit   | Windows 10   | $\sim$  |                          |                 | ^   |  |
| Edition   | Professional   | $\sim$  |                          |                 |     |  |
| Version   | N'importe lequel   | ~   |                          |                 |     |  |
| Rôle d'ordinateur   | N'importe lequel   | ~   |                          |                 |     |  |
| Un élément cible Système d'exploitation permet l'application d'un élément de préférence aux |  |   |                          |                 |     |  |
| de l'ordinateur de t  | utilisateurs uniquement si le nom, la ver<br>raitement ou le rôle d'ordinateur corresr | sion, l'édition du systèm<br>condent à ceux snécifiés | e d'exploi<br>dans l'élé | tation<br>ément | ~   |  |
|   |  |   | ОК                       | Annu            | ler |  |



https://www.cabare.net Page 83 - Michel Cabaré -

#### Secpol.msc - Rappel stratégies locales et GPo de domaine

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

ce qui donne ensuite accès aux paramètres suivants :

| Paramètres de sécurité locaux   |  |                           |                    |
|---|--|---------------------------|--------------------|
| $   \underline{A}ction  Affichage    \Leftarrow \Rightarrow   \textcircled{E}   \overrightarrow{R}   \times \textcircled{B}   $ | Ê  |                           |                    |
| 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 |
| E III Stratégies de comptes   | BDurée de vie maximale du mot de passe                         | 42 Jours                  | 42 Jours           |
| 🗄 🕮 Stratégie de mot de passe   | BDurée de vie minimale du mot de passe                         | 0 Jours                   | 0 Jours            |
| 🛨 👜 Stratégie de verrouillage du compte   | BELes 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   | BS 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 **GPO** ou **stratégies de domaine/réseaux** elles sont en général utilisées à travers le réseau (pour tout le domaine ou une partie à travers les UO...)

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

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

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

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



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





# **OBJECTIF BOUCLE DE RAPPEL**

# Gpo – « normales »

Une stratégie de groupe ou GPO, se découpe en deux parties distinctes,

- la partie **« Configuration Ordinateur »** qui elle contient les paramètres appliqués aux objets de type Ordinateur.
- la partie **« Configuration Utilisateur »**, contenant les paramètres appliqués aux objets Active Directory de type Utilisateurs

lorsque un utilisateur ouvre une session sur une machine, le résultat de la configuration appliquée est le cumul des parametres **« Configuration Ordinateur »** appliqués à la machine utilisée et des parametres **« Configuration Utilisateur »** appliqués à l'utilisateur utilisé pour l'ouverture de session.

Ceci est vrai en règle générale, **sauf** ! En cas d'activation du **Loopback Processing** au sein de la GPO concernée.

#### **Gpo – loopback processing**

Partons du principe que nous avons 2 OU distinctes qui ont chacune une GPO de liée (nous avons donc 2 GPOs).

Une de ces OU contient un objet de type Ordinateur

l'autre OU contient un objet de type Utilisateur habilité à ouvrir une session sur l'Ordinateur présent dans la première OU.

z-uo-loopback-processing
 uo-ordi
 loopback-ordi
 uo-util
 loopback-utilis

Lors de l'activation de cette option (Loopback Processing) sur la GPO s'appliquant à l'ordinateur, donc dans l'exemple *loopback-ordi* 

# Ordinateur/Stratégies/Modeles d'administration/Système/Stratégie de groupe







https://www.cabare.net Page 85 - Michel Cabaré -

| Configurer le mo                           | ode de traitement par l | oouclage de la stratégie de groupe utilisateur 🛛 🗌   | ×      |
|--|-------------------------|--|--------|
| Configurer le mo                           | ode de traitement par   | bouclage de la stratégie de groupe utilisateur   |        |
| Paramètre précéde                          | nt Paramètre sui        | vant   |        |
| 🔿 Non configuré                            | Commentaire :           |  | ^      |
| Activé                                     |                         |  |        |
| O Désactivé                                |                         |  | × .    |
|  | Pris en charge sur :    | Au minimum Windows 2000  | $\sim$ |
|  |                         |  | ~      |
| Options :                                  |                         | Aide :   |        |
| Mode : Remplacer<br>Fusionner<br>Remplacer |                         | Ce paramètre de stratégie demande au système d'appliquer le<br>jeu d'objets de stratégie de groupe à l'ordinateur pour tout<br>utilisateur qui ouvre une session sur un ordinateur affecté par ce<br>paramètre. Il est conçu pour des ordinateurs à usage particulier,<br>comme ceux dans les lieux publics. les laboratoires et les écoles. | ^      |

le processus d'application des paramètres se fera de la façon suivante :

Lors du démarrage de la machine, les paramètres **Configuration Ordinateur** de la **GPO liée à l'OU contenant l'Ordinateur** seront appliqués à la machine comme d'habiture

Donc on applique les "param ordi" de



MAIS lors de l'ouverture de session d'un objet **Utilisateur** qui lui **n'est normalement pas visé par cette dernière GPO**, ce sont les paramètres de **Configuration Utilisateur** contenus dans la GPO appliquée à l'objet de type Ordinateur qui seront appliqués d'abords (et non la « Configuration Utilisateur » de la GPO liée à l'Utilisateur). Donc pour nous les <u>paramètres utilisateurs</u> de la GPO !!!

📋 uo-ordi 🛒 loopback-ordi

Ensuite, suivant l'option choisie lors de l'activation du Loopback Processing, les paramètres de **Configuration Utilisateur** provenant de la GPO liée au

compte Utilisateur, (a priori légitimes) donc pour nous 🗟 loopback-utilis seront traités ainsi :

- Si l'option fusion est choisie, les paramètres de « Configuration Utilisateur » appliqués à la session Utilisateur seront un <u>cumul</u> de ceux présent dans la partie « Configuration Utilisateur » de la GPO appliquée à l'Ordinateur et de ceux présents dans la partie « Configuration Utilisateur » de la GPO appliquée à l'Ordinateur et appliquée l'Utilisateur. <u>En cas de conflits sur un paramètre, ce sera le paramètre appliqué à l'objet Ordinateur qui sera effectivement appliqué.</u>
- Si l'option remplacer est choisie, dans ce cas les paramètres de « Configuration Utilisateur » appliqués seront uniquement ceux définis dans partie « Configuration Utilisateur » de la GPO appliquée à l'objet Ordinateur.



# **GPO STARTER**

# **Objets GPO starter**

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

#### **GPO Starter**

#### GPO complète



Permet la création de GPO à partir de ces templates facilement

| Objets de stratégie de groupe Default Domain Controllers Policy  | Nouvel objet GPO  |
|--|---|
| Default Domain Policy Filtres WMI  | Nom :   |
| 🖃 🛅 Objets GPO Starter   | Nouvel objet de stratégie de groupe   |
| Ordinateur EC Windows Vista Ordinateur EC Windows XP SP2 Ordinateur SSLF Windows Vista Ordinateur SSLF Windows XP SP2 Utilisateur EC Windows Vista Utilisateur EC Windows XP SP2 Utilisateur EC Windows XP SP2 | Objet Starter GPO source :<br>(aucun) (aucun) (aucun) essais Ordinateur EC Wil Lows Vista |

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

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

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



