Administration W2K3: Stratégies de groupe

Stratégie de groupes

- Permet d'imposer à des ordinateurs ou à des utilisateurs des configurations, des paramètres
- 2 types de stratégies:
  - Stratégies locales : propre à un ordinateur
  - Stratégies non locales: s'appuient sur Active Directory
    - => gestion centralisée
    - => souplesse (des stratégies différentes en fonction de l'UO d'appartenance)

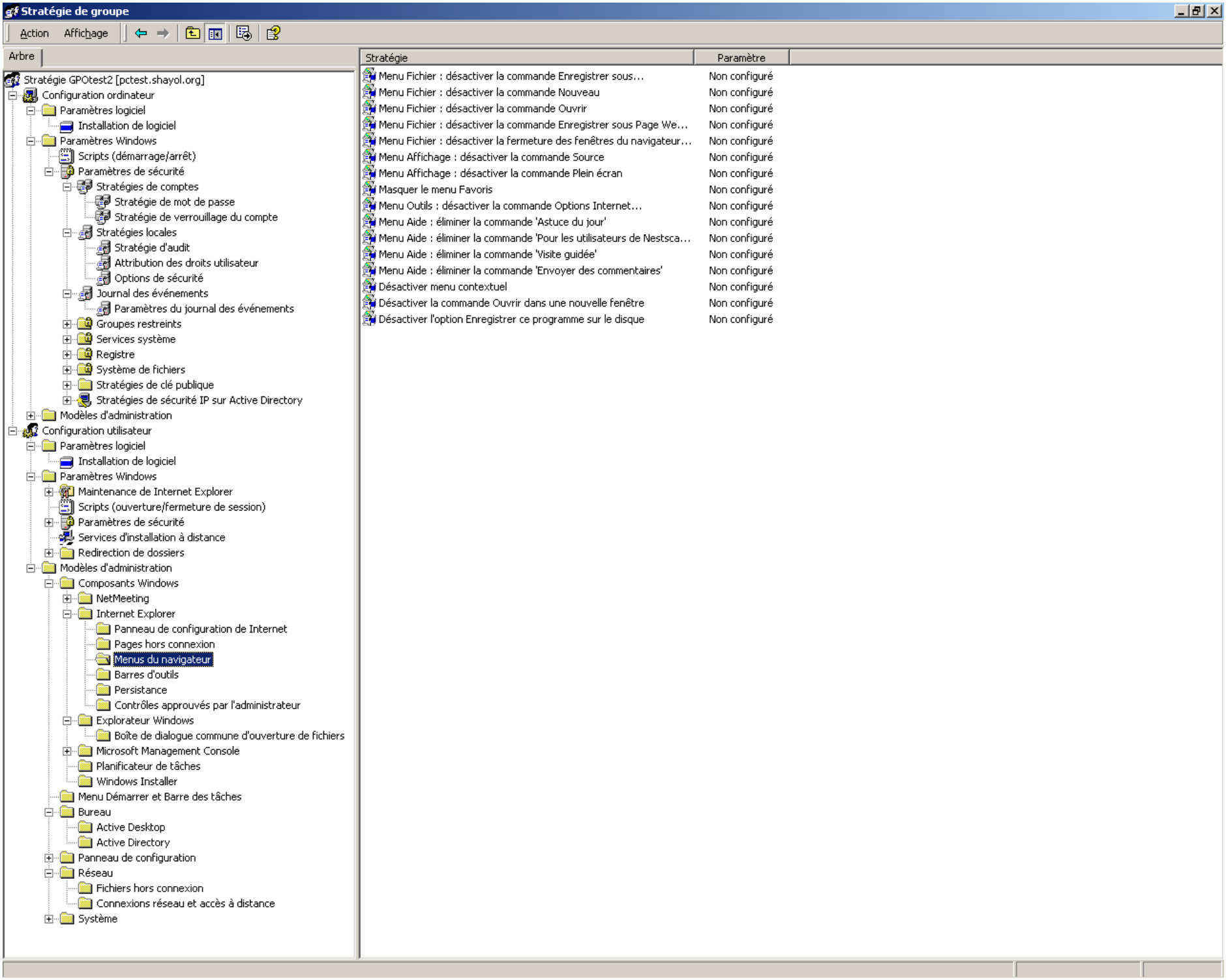
GPO: structure physique: 2 parties

- Conteneur de stratégie de groupe (Group Policy Container) : objet AD
- Modèle de stratégie de groupe (Group Policy Template GPT) : dossier situé dans SYSVOL

GPO: structure logique:

- configuration ordinateur: s'applique à tous les ordinateurs concernés par la stratégie de groupe
- configuration utilisateur: s'applique à tous les utilisateurs concernés par la stratégie de groupe

- Peut-être lié à plusieurs conteneurs
- Un conteneur peut être lié à plusieurs GPOs
- La stratégie s'applique aux objets du conteneur


Stratégie de groupe
Action
Affichage
Arbre
Stratégie GPOtest2 [pctest.shayol.org]
Configuration ordinateur
Paramètres logiciel
Installation de logiciel
Paramètres Windows
Scripts (démarrage/arrêt)
Paramètres de sécurité
Stratégies de comptes
Stratégie de mot de passe
Stratégie de verrouillage du compte
Stratégies locales
Stratégie d'audit
Attribution des droits utilisateur
Options de sécurité
Journal des événements
Paramètres du journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de clé publique
Stratégies de sécurité IP sur Active Directory
Modèles d'administration
Configuration utilisateur
Paramètres logiciel
Installation de logiciel
Paramètres Windows
Maintenance de Internet Explorer
Scripts (ouverture/fermeture de session)
Paramètres de sécurité
Services d'installation à distance
Redirection de dossiers
Modèles d'administration
Composants Windows
NetMeeting
Internet Explorer
Panneau de configuration de Internet
Pages hors connexion
Menus du navigateur
Barres d'outils
Persistance
Contrôles approuvés par l'administrateur
Explorateur Windows
Boîte de dialogue commune d'ouverture de fichiers
Microsoft Management Console
Planificateur de tâches
Windows Installer
Menu Démarrer et Barre des tâches
Bureau
Active Desktop
Active Directory
Panneau de configuration
Réseau
Fichiers hors connexion
Connexions réseau et accès à distance
Système
Stratégie
Paramètre
Menu Fichier : désactiver la commande Enregistrer sous... Non configuré
Menu Fichier : désactiver la commande Nouveau Non configuré
Menu Fichier : désactiver la commande Ouvrir Non configuré
Menu Fichier : désactiver la commande Enregistrer sous Page We... Non configuré
Menu Fichier : désactiver la fermeture des fenêtres du navigateur... Non configuré
Menu Affichage : désactiver la commande Source Non configuré
Menu Affichage : désactiver la commande Plein écran Non configuré
Masquer le menu Favoris Non configuré
Menu Outils : désactiver la commande Options Internet... Non configuré
Menu Aide : éliminer la commande 'Astuce du jour' Non configuré
Menu Aide : éliminer la commande 'Pour les utilisateurs de Nestsca... Non configuré
Menu Aide : éliminer la commande 'Visite guidée' Non configuré
Menu Aide : éliminer la commande 'Envoyer des commentaires' Non configuré
Désactiver menu contextuel Non configuré
Désactiver la commande Ouvrir dans une nouvelle fenêtre Non configuré
Désactiver l'option Enregistrer ce programme sur le disque Non configuré

Paramètres contrôlés

- Modèles d'administration: paramètres basé sur le registre concernant principalement la gestion de l'environnement des utilisateurs;
- Sécurité: paramètres de sécurité locale, de site, domaine ou UO
- Installation des logiciels
- Scripts: démarrage/arrêt d'ordinateur ou de session utilisateur
- Redirections de dossiers

Modèles d'administration

Type	description	configuration
panneau de configuration	pour cacher tout ou partie du panneau de configuration, de restreindre l'accès à certains composants (ajout/suppression de programmes, affichage, imprimantes et telecopieurs, options régionales et linguistiques	utilisateur
Bureau	apparence du bureau, (dés)activation d'Active Desktop, limiter les possibilités d'interrogation d'AD par l'utilisateur	utilisateur
Réseau	fichiers hors connexion, connexions réseau, clients DNS et SNMP	utilisateur et ordinateur
imprimantes	contrôler l'impression sur le WeB, la publication auto des imprimantes dans AD, ...	ordinateur
dossier partagés	autoriser la publication des dossiers partagés et des racines DFS (w2k3)	utilisateur
Menu Démarrer et barre de tâches	contrôler leur apparence et fonctionnalités	utilisateur
Système	ouverture/fermeture de sessions, quotas disque, suffixe dns, application stratégie de groupe, désactiver les outils de modif. du registre, l'exécution auto.,configurer les profils utilisateurs,la gestion de l'alimentation, ...	utilisateur et ordinateur
composants windows	contrôle des fonctionnalités d'IE; netmeeting, planificateur de tâches, explorer, ...	utilisateur et ordinateur

Sécurité

- stratégies de comptes:
  - stratégies de mot de passe, verrouillage de compte, ...
  - utilisables uniquement sur une GPO de domaine (sans effet sinon)
- stratégies locales: stratégies d'audit, droits utilisateurs, paramètres de sécurité du poste (par opposition au domaine)
- journal des évènements
- groupes restreints : pour forcer l'appartenance et l'inclusion de certains groupes
- services systèmes: paramètrer démarrer et sécurité des ordinateurs d'une UO ou d'un domaine

Sécurité

- registre: configurer les autorisations sur des sous-arborescences du registres pour tous les ordinateurs d'un domaine ou d'un UO
- système de fichiers: définir des autorisations NTFS cohérentes sur tous les postes d'un UO ou d'un domaine
- stratégie de réseau sans fil
- stratégie de clé publique
- stratégie de restriction logicielle: pour définir les logiciels autorisés à s'exécuter sur les ordinateurs
- stratégie de sécurité IP sur AD: configuration d'IPSec sur les postes d'un UO ou d'un domaine

Installation des logiciels

- dans une version future de ce document

Scripts

- pour automatiser l'exécution de scripts
  - scripts de démarrage: exécutés l'un après l'autre au démarrage du poste de travail
  - scripts d'arrêt: idem lorsqu'un système est arrêté normalement
  - scripts d'ouverture (fermeture) de session: exécutés en parallèle lorsqu'un utilisateur ouvre (ferme) une session

Redirections de dossiers

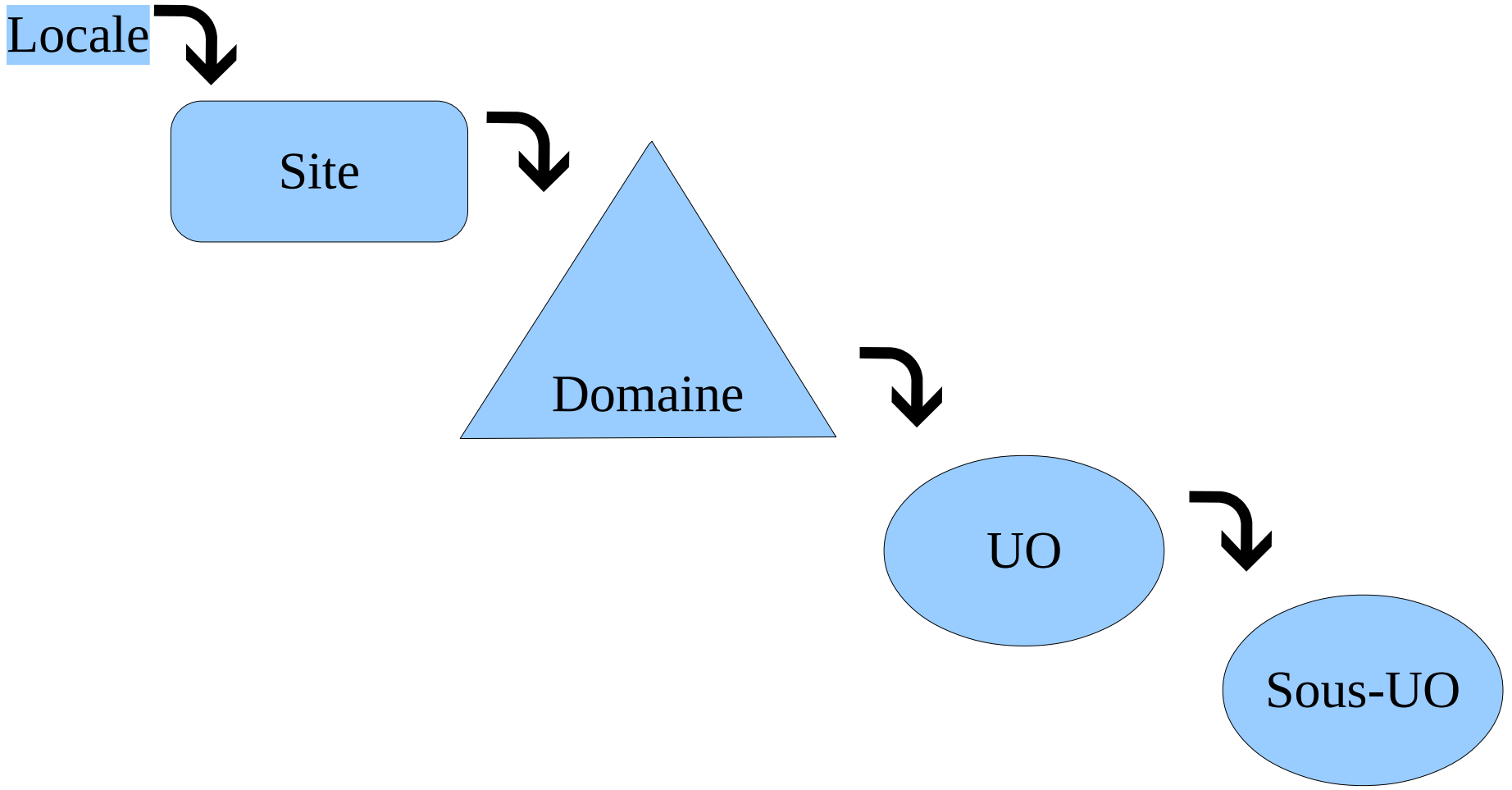
- rediriger certains dossiers vers un partage situé sur une serveur
- avantages:
  - ceux des profils itinérants (centralisation du profil, sauvegarde, ...)
  - pas de copie du profil en début de session

Redirections de dossiers

- sont concernés:
  - « Menu démarrer », Bureau: raccourcis et dossiers du menu démarrer et du bureau de l'utilisateur. Une redirection vers un emplacement en lecture seule permet d'avoir un environnement standardisé
  - « Application Data »: données spécifiques à l'utilisateur pour certaines applications. à rediriger si l'on souhaite que les données soient accessible depuis tout le parc
  - « Mes documents »: fichiers de travail de l'utilisateur. Idem.

Ordre d'applications des stratégies de groupes

- Héritage cumulatif des paramètres



Conflits entre GPOs

- Les paramètres de la dernière GPO sont appliqués :
  - Ordre d'application via l'héritage
  - Ordre d'application des GPOs liés à même conteneur.
- Dans un GPO, paramètres de l'ordinateur prioritaires sur ceux de l'utilisateur

Application des GPO

- Héritage: les sous-conteneurs héritent des GPO des conteneurs
- Blocage: on peut bloquer l'héritage. bloque **tous** les paramètres hérités
- Forçage: on peut forcer l'héritage aux conteneurs enfants
- Filtrage: on peut empecher certains objets d'un conteneur de se voir appliquer les paramètres des GPO. se fait via les autorisations de la GPO sur le conteneur

DEMO (1)

- On crée un utilisateur etu1 sur le contrôleur de domaine
- On vérifie qu'il est correctement authentifié mais qu'il n'a pas le droit d'ouvrir une session interactive sur le contrôleur de domaine
- On modifie la stratégie de sécurité du contrôleur de domaine pour qu'il ait le droit d'ouvrir une session dessus
- On vérifie que ça ne marche pas
- On attend 5 mn et on vérifie que ça marche.

Exemple

- Une UO LicProRS2I, une UO LicAutre toutes deux dans le domaine.
- Sur le site: GPO imposant un fond d'écran château de chambord
- Sur le domaine: GPO imposant de ne pas avoir d'item « Executer » dans le menu démarrer
- Une GPO empéchant le changement de mot de passe liée aux deux UO LicProRS2I et LicAutre
- Une GPO imposant la photo d'un prof barbu en fond d'écran liée à l'UO LicProRS2I
- Qu'est-ce qui s'applique réellement à LicProGSI ?

Demo2:

- On applique l'exemple
- On force la propagation des stratégies de groupe avec un « secedit /refreshpolicy machine_policy » et « secedit /refreshpolicy user_policy ». Souswindows XP, on utilisera gpupdate à la place de secedit.
- On le vérifie
  - soit avec le compte étu1 sur le contrôleur de domaine,
  - Soit avec le compte étu1 sur une des stations du domaine

Application des objets stratégie de groupe

- Paramètres utilisateurs: à l'ouverture de session
- Paramètre ordinateur: au démarrage de l'ordinateur
- Actualisation
  - toutes les 90 mn (+/- 30mn) (redirections de dossiers et installations de logiciels ne sont pas actualisées)
  - toutes les 5 mn sur les contrôleurs de domaine
- Forcer l'actualisation:
  - gpupdate (Wxp et w2k3)
  - secedit /refreshpolicy user_policy|machine_policy (W2k)

Planification de la stratégie de groupe

- stratégies de site:
  - appliquées à tous les ordinateurs et utilisateurs du site quelques soient leur domaine
  - utilisé pour limiter le trafic sur des liaisons Wan lentes
  - ex.: empecher les installations de logiciels de traverser les frontières des sites

Planification

- stratégies de domaine
  - s'applique à tous les objets du domaine
  - la stratégie définie dans un domaine ne s'applique pas aux domaines enfants
  - ne peut être configurer que par un administrateur du domaine
- stratégie d'UO
  - s'applique à tous les objets de l'UO
  - sa gestion est délégable à des utilisateurs non administrateur
  - héritage des stratégies des UO parentes
  - à préférer quand c'est possible

Planification

- plus il y a de GPO:
  - plus les ouvertures de session sont lentes
  - plus le trafic réseau associé est important
  - plus il est difficile de dépanner/détecter les éventuels conflits
- plus les GPO contiennent de paramètres:
  - moins leur nom sera lisible
  - elles ne pourront être appliquées qu'à un seul conteneut

Planification: 2 approches

- faire des GPO avec des noms lisibles, s'occupant de tâches élémentaires facilement identifiables
  - avantage: lisibilité, réutilisation
- faire de grosses GPO regroupant tous les paramètres devant s'appliquer à un conteneur
  - avantage: centralisation, trafic réseau modéré

Planification : conseils méthodologiques

- utiliser le forçage uniquement sur des conteneurs de haut niveau (domaine, UO de premier niveau), voire même pas du tout
- ne pas utiliser le filtrage de GPO (complexifie le débogage)
- désactiver la partie config. utilisateur ou ordinateur si elle ne sert pas : gain de vitesse
- toujours tester vos GPO (et surtout, depuis un autre poste en laissant votre session courante ouverte)

Stratégies de groupes: outils graphiques

- utilisateur et ordinateur active directory
  - créer/modifier/supprimer et lier des stratégies à des domaines et des OU
- sites et services active directory
  - idem pour des sites
- éditeur d'objet de stratégie de groupe:
  - modifier les paramètres de GPO existantes
- stratégie de sécurité locale, du domaine, du contrôleur de domaine
- jeux de stratégie résultant:
  - dans une version ultérieure de ce document

Stratégies de groupes: outils graphiques GPMC

- outil permettant de :
  - Visualiser rapidement la hiérarchisation des GPO
  - Créer ou modifier une GPO
  - Activer ou désactiver une GPO
  - Afficher via un rapport HTML les stratégies
  - Connaître les délégations des GPO
  - Sauvegarder ou restaurer une GPO
- installation:
  - sur www.microsoft.com puis rechercher gpmc
- La GPMC s'intègre complètement à w2k3

Tâches avec la GPMC

- Créer une GPO lié à un objet
  - Dans la console « utilisateurs et ordinateur AD » : Clic droit sur une OU ou un nom de domaine → créer et lier un objet GPO ici → spécifier le nom de l'objet
- Créer une GPO non liée
  - Sélectionner un domaine → clic droit « Objets stratégie de groupe » → nouveau → donner le nom
  - Ne pas oublier de lier l'objet GPO à un conteneur pour pouvoir l'utiliser

Tâches avec la GPMC

- Ouvrir un GPO
  - Clic droit sur un GPO → modifier
  - Ou clic droit sur une liaison de GPO
- Lier un GPO
  - Clic droit sur une UO ou un domaine → lier un objet stratégie de groupe existant → sélectionner l'objet à lier
- Afficher les liaisons d'un GPO
  - Sélectionner un GPO → étendue → spécifier un emplacement → Liaisons

Tâches avec la GPMC

- Modifier l'ordre de liaison des GPO
  - Sélectionner un conteneur → Objets stratégie de groupe liés → déplacer vers le haut ou vers le bas

Tâches avec la GPMC: déléguer une stratégie

- Créer des GPO : groupe GPCO (Group Policy Creators Owner)
- Autoriser la création des GPO à user1
  - Ajouter user1 à GPCO
  - Sélectionner Objet Stratégie de groupe → Délégation → ajouter → sélectioner user1 (ou un groupe)
- Déléguer une responsabilité limitée
  - Sélectionner l'objet GPO → Délégation → ajouter → sélectionner un utilisateur ou un groupe → spécifier les autorisations

Tâches avec la GPMC: sauvegarde/importation

- Avec la GPMC
- Avec les outils en ligne de commande RestoreGPO.wsf et RestoreAllGPO.wsf (outils installés avec la GPMC)