windows 2000 : GPO

Une **GPO** (Group Policy Object) ou **Stratégie de Groupe** est un ensemble de paramètres appliqués à un utilisateur ou à un groupe.
Les GPO sont gérés comme des objets de Active Directory.

"Policy" signifie politique (et pas police), dans le sens politique de la ville, ou politique de l'éducation, et on le traduit par "stratégie".

On peut attribuer une GPO :
- au niveau d'un site : utiliser Sites et services Active Directory
- au niveau d'un domaine ou d'une OU : utiliser Utilisateurs et ordinateurs Active Dir.

1. création d'une GPO :

- outils d'administration Utilisateurs et ordinateurs Active Dir
- clic droit sur le conteneur (par exemple une OU)
- clic Propriétés, puis onglet Stratégies de groupe
- clic Nouveau
- donner un nom clair (qui permet de se rappeler plus tard ce que fait la GPO)

2. ajout d'une GPO :

pour lier une GPO existante à un conteneur

- clic droit sur le conteneur
- clic Propriétés, puis onglet Stratégies de groupe
- clic Ajouter
- "Tous" permet de visualiser toutes les GPO existantes
- "Domaines, OU" permet de lister les GPO en fonction de leur lieu d'application
- "Sites" permet de lister les GPO qui sont appliqués par site
- sélectionner la GPO à appliquer au conteneur, puis OK

3. suppression d'une GPO :

la suppression peut

- ne supprimer que le lien entre conteneur et GPO, pas la GPO elle-même
- ou effacer la GPO

- sélectionner la GPO
- clic sur Supprimer
- choisir le mode de suppression et OK

4. paramètres des GPO :

une fois la GPO ajoutée, clic sur Modifier pour changer les paramètres

- la GPO peut concerner l'ordinateur ou l'utilisateur
- **Software settings** concerne le déploiement de logiciels
- **Modèles d'administration** concerne l'environnement de l'utilisateur (accès au panneau de configuration, au menu Démarrer, activer les dossiers hors connexion, quotas de disque...)
- **Scripts** concerne l'ouverture et la fermeture de session
- **Sécurité** concerne les droits des utilisateurs, les stratégies de compte et mots de passe...
- **Redirection de répertoire**

5. environnement utilisateur :

Quand un utilisateur ouvre une session, il consulte le dossier SYSVOL du contrôleur de domaine, recherche un fichier de stratégie nommé Regostry.pol
Il existe 2 fichiers Registry.pol pour chaque GPO : un pour l'ordinateur, un pour l'utilisateur.

Pour appliquer un paramètre dans une stratégie :
- sélectionner le paramètre, double clic
- choisir :
  - non configurée : le paramètre est ignoré
  - activée : le paramètre est appliqué et la valeur est ajoutée à Registry.pol
  - désactivée : le paramètre n'est pas appliqué et la valeur est ajoutée à Registry.pol

6. application des GPO :

Quand la machine démarre, on applique les paramètres GPO de la machine, puis les scripts.
Quand l'utilisateur ouvre une session, on applique les paramètres GPO de l'utilisateur.

Les stratégies sont rafraîchies toutes les 10 minutes.
S'il y a plusieurs stratégies pour un conteneur, elles sont lues dans la liste du bas vers le haut ! Celle du haut est appliquée en cas de conflit.

Les stratégies sont héritées des OU parents vers les OU enfants, sauf si on a bloqué l'héritage : voir Conteneur, Propriétés, Stratégies de groupe, case "bloquer l'héritage"

Pour qu'une stratégie s'applique aux utilisateurs, ils doivent avoir au moins des permissions Lire et Appliquer la stratégie de groupe (voir le fenêtre Stratégies de groupes, onglet Sécurité).

COMPTES UTILISATEURS :

un script est un enchaînement de commandes.
Ce peut être un fichier .BAT ou un fichier .VBX

Script d'ouverture de session :

les scripts s'exécutent dans l'ordre : site – domaine – OU – OU – user
à partir de n'importe quel partage de fichier, mais le répertoire standard est :

```
\winnt\system32\repl\import\script
```

exemple :

```
echo off
echo bienvenue sur le serveur Saturne
net use p: \\saturne\partage
net use q: \\saturne\applis
```

préférer les stratégies de groupes aux script individuels (plus longs à écrire)

Pour attribuer un script de stratégie de groupe :

- clic droit sur l'Objet conteneur ou groupe, puis Propriétés
- sélectionner stratégie de groupe
- clic (+) à côté de Configuration user et sur (+) à côté de Paramètres Windows pour développer l'arborescence
- sélectionner Scripts (ouverture-fermeture de session)
- double clic sur Ouverture de session, puis Ajouter
- régler les options
- dans la page Propriétés de Ouverture de session ou Déconnexion, indiquer les options :
  - ouverture de (indiquer l'ordre d'exécution des scripts disponibles)
  - ajouter
  - modifier
  - supprimer
  - afficher
- OK

Profils itinérants et obligatoires :

profil local : stocké sur la machine
profil itinérant : stocké sur le serveur
profil obligatoire :
aucun utilisateur ne peut y apporter des changements : tout doit rester générique et acceptable pour l'ensemble,
il faut renommer ntuser.dat en ntuser.man (par défaut dans \\serveur\netlogon)

clients 95/98 :
panneau de config – mots de passe – propriétés :
cocher "les utilisateurs peuvent personnaliser...
gérer un utilisateur de base pour les réseaux MS
configurer Win9x pour ouvrir une session sur le domaine

Procédure conseillée :

- mrim.fr (domaine)
  - OU eleves
  - OU profs
  - OU gpo
    - gpo1
    - gpo2
    - pgo3
      - ordinateur
        - logiciels
        - Windows (démarrage – arrêt de l'ordi)
        - administration
      - utilisateur
        - logiciels
        - Windows (ouverture – fermeture de session)
        - administration

créer une OU pour les GPO
créer des GPO selon les besoins
attribuer une ou plusieurs de ces GPO aux objets user ou groupes

une GPO ordinateur concerne la station sur laquelle un utilisateur travaille
une GPO utilisateur concerne l'utilisateur lui-même