Windows Server

GPO

Méthode de création de GPO sous Windows Server 2008 R2

Définition de la structure Active Directory

UO : ENTREPRISE
- → Sous UO : LANNION
  - → Sous UO : Machines_lannion
  - → Sous UO : Machines_ouvertes
  - → Sous UO : Utilisateurs_lannion
- → Sous UO : RENNES
  - → Sous UO : Machines_rennes
  - → Sous UO : Utilisateurs_rennes

UO : GROUPE
- Création de deux groupes Manager & Employé (clic droit → nouveau groupe)

Comment créer des UO ?
Menu démarrer → Outils d'administration → Utilisateurs et ordinateurs active directory
Le nom de domaine (exemple.com) est disponible → clic droit → nouveau → unité d'organisation

Une fois nommée elle apparait en bas, faites la même manipulation que précédemment mais sur l'UO créée pour faire les sous unité d'organisation.

A quoi servent-elles ? Une unité d'organisation est l'étendue ou l'unité la plus petite à laquelle vous pouvez attribuer des paramètres de Stratégie de groupe ou déléguer une autorité administrative. Avec les unités d'organisation, vous pouvez créer des conteneurs à l'intérieur d'un domaine afin de représenter les structures hiérarchiques et logiques de votre organisation. Vous pouvez ensuite gérer la configuration et l'utilisation des comptes et des ressources en fonction de votre modèle d'organisation.

Créer un compte utilisateur et l'appliquer dans un groupe

Toujours au même endroit, mais cette fois-ci sur l'objet « USERS » → clic droit → nouveau → utilisateur

Une fois fait il apparait et on peut avec un clic droit sur ce dernier l'appliquer à un groupe « Ajouter à un groupe ».

On va se servir de cette architecture pour mettre en place des GPO (Group Ploicy Object), Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement *Active Directory*.

GPO

Création GPO

Menu démarrer → Outils d'administration → Gestion de stratégie de groupe

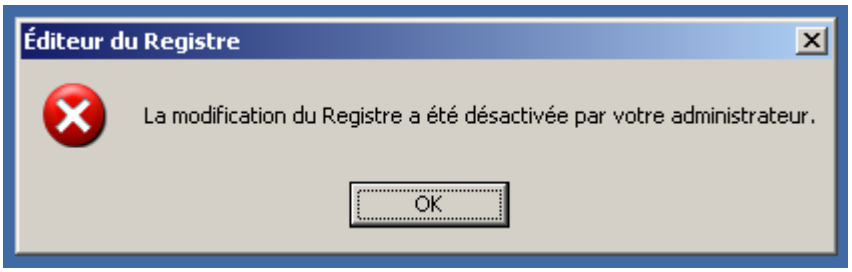
Dans la fenêtre qui s'ouvre on a notre domaine (exemple.com) → clic droit → créer un objet dans ce domaine et le lier ici → nommé votre GPO dans la fenêtre qui s'ouvre. Elle apparait dans une liste, en dessous « Default Domain Policy ». On remarquera donc que l'on changer l'ordre de priorité avec un petit menu de flèche au niveau de cette liste.

Un clic droit dessus et → modifier, cela nous permettra de l'éditer. Par exemple si on veut interdire l'accès à la base de registre on ferait comme ça :

Déployer configuration utilisateur → stratégies → modèles d'administration : définitions de stratégies… → Tous les paramètres → Empêche l'accès aux outils de modifications du registre

Un double clic ou sur la gauche « modifier le paramètre de stratégie » pour l'activer. Il faut l'appliquer à une UO, pour cela toujours dans notre console de gestion de stratégie de groupe, on a nos UO créées précédemment qui sont visible.

Un clic droit dessus (ex : Entreprise) puis → lier un objet de stratégie de groupe existant → dans la fenêtre qui suit, il suffit de choisir notre GPO créée. Si on se connecte avec un utilisateur dans notre domaine et qu'il tente d'afficher la console « regedit » il aura ce message :



Il faut savoir qu'il faut redémarrer la machine cliente pour appliquer les GPO ou via une commande CMD avec « gpupdate /force » (il demandera automatiquement si un redémarrage est nécessaire).

Blocage d'héritage

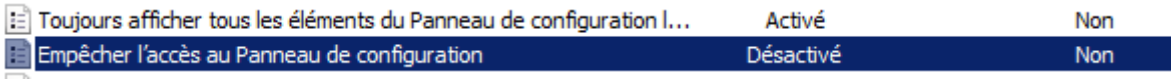
La gestion de stratégie de groupe permet aussi de bloquer l'héritage, par exemple on va créer une autre GPO qui elle interdira l'accès au panneau de configuration. Configuration utilisateur → stratégies → modèles d'administration : définitions de stratégies… → panneau de configuration → dans la liste il suffit de configurer les paramètres. On la lie évidemment elle aussi à notre UO Entreprise et a ses sous-uo. Sauf que l'on veut éviter que notre dernière GPO s'applique à une sous-uo en particulier. Un clic droit sur celle-ci → bloquer l'héritage.

Si dans cet UO il y a d'autres GPO elles seront bloquées. Un clic droit sur les GPO que l'on veut conserver active → appliqué. Cet effet a pour but de contourner le blocage d'héritage.

Filtrage GPO

Nous avons la possibilité de filtrer nos GPO, exemple si vous disposez d'une UO « Groupe » et des groupes définis avec le désir d'appliquer une GPO à seul groupe, et bien c'est possible.

Pour cela on va créer une GPO qui elle autorise l'accès au panneau de configuration : Configuration utilisateur → stratégies → modèles d'administration : définitions de stratégies… → panneau de configuration → il y a deux paramètres à modifier



Dans la gestion de stratégie de groupe, votre UO « groupe » est présente. Dedans toutes les GPO activées. Il y a évidemment une contradiction entre celle qui autorise et celle qui accepte les accès au panneau de configuration. Rappelez-vous on peut modifier l'ordre de priorité des GPO, on met donc notre GPO qui autorise en première. Il faut maintenant la filtrer pour qu'elle ne s'applique à un seul groupe. Dans la gestion de stratégie de groupe, déployer votre groupe et sélectionner la GPO à filtrer. Dans la fenêtre de droite, il y a l'onglet filtrage de sécurité, par défaut on a utilisateurs authentifiés. Supprimer le et ajoutez à la place votre groupe choisit.

Configuration de la base de registre

Exemple type de configuration, les utilisateurs ne peuvent pas déplacer la barre des tâches et modifier l'écran de veille. De plus la configuration avancée de TCP/IP et l'ajout et la suppression de composants Windows leurs seront interdits.

Barre de tâche :
configuration utilisateur → modèles d'administration … → menu démarrer et barre des tâches → empêcher les utilisateurs de déplacer…….de l'écran

Ecran de veille :
configuration utilisateur → modèles d'administration … → personnalisation →empêcher de modifier l'écran de veille

Configuration IP :
configuration utilisateur → modèles d'administration … → réseau → interdire la configuration avancée de TCP/IP

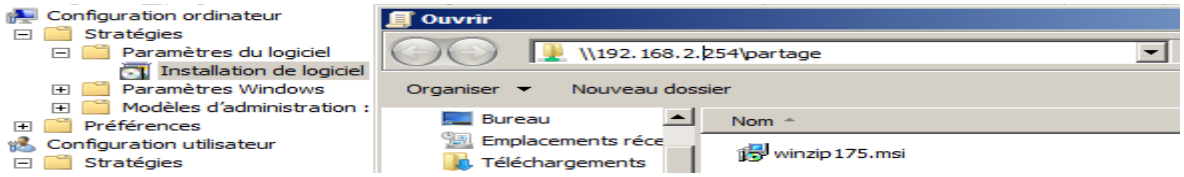
Ajout et suppression de composants Windows :
configuration utilisateur → modèles d'administration … → réseau → interdire l'ajout et la suppression…….ou réseau.

Déploiement d'applications, via MSI

Attention à la compatibilité du logiciel avec votre système d'exploitation, à tester avant.

Créer ou éditer une GPO → configuration ordinateur →stratégies → paramètres du logiciel → installation de logiciel → clic droit dessus → nouveau → package. Une fenêtre s'ouvre. Allez chercher votre paquet MSI dans un dossier que l'on va créer à la racine de « C : » et le partager avec tout le monde. Attention, afin qu'il soit installable il ne faut aller directement par « parcourir », mais en haut

dans la barre de recherche, vous devez indiquer le CHEMIN RÉSEAU, exemple : \\127.0.0.1\c:\partage\mon_logiciel.msi



Il faudra redémarrer le poste client.

Déploiement d'applications, à distance

Télécharger PsTools sur le serveur 2008 ainsi qu'un logiciel.exe de votre choix. Décompresser PsTools et placer PsExec.exe à la racine de C. Dans un CMD :

Psexec \\@ip_client c:\chemin de l'emplacement du logiciel.exe /SILENT

Redirection des dossiers

On va rediriger le bureau (desktop) de tous les utilisateurs. Nouvelle GPO ou on édite une autre :

Configuration utilisateurs → paramètres Windows → redirection de dossiers → bureau → clic droit → propriétés →paramètre de base… → chemin réseau du dossier cible (\\127.0.0.1\c:\bureau)

Traitement par boucle de rappel

On peut indiquer et appliquer une GPO ordinateur, qui prendra le dessus sur une GPO utilisateur. Par exemple, si on a configuré une GPO qui interdit aux utilisateurs d'un domaine d'accéder au Regedit, mais on veut l'autoriser sur une machine spécifique il existe le traitement par boucle.

Pour cela éditer la GPO concernée et activez cette options :

Configuration ordinateur → modèles d'administration… → système → stratégie de groupe → mode de traitement par boucle…….utilisateur → double clic puis activer

Filtrage de refus de GPO

A l'aide d'un filtre, on peut ignorer une GPO qui par configuration interdit un accès quelconque. Il faut configurer le filtrage (à droite lors de la sélection de la GPO Panneau Access), il y a délégation ce qui nous permettra d'affiner les droits.

Ajouter l'utilisateur ou le groupe qui ne doit pas être atteint par cette GPO. En bas à droite du panneau access, cliquez sur avancé et aller sur l'utilisateur qui vous intéresse. En bas de la liste il y « appliquer la stratégie de groupe », sélectionner REFUS. Ainsi la GPO ne lui sera pas appliquée.

Préférences ou Mappage réseau

Pour créer un lecteur réseau qui aura une lettre défini par nous-même, faire une nouvelle GPO puis configuration utilisateur → préférences → mappages de lecteurs → créer → mettre le chemin réseau (\\@ip\dossier partagé ou disque dur à partager) → mettre une lettre d'identification.