Administration W2K: cours 3

- AD avancé: forêt, arborescences, relations d'approbation, maîtres d'opérations, serveur de catalogue global
- AD: stratégies de groupe
- AD: Les domaines windows 2000

Structure logique

- Forêts
- Arborescences
- Domaines
- Unités d'organisation

Il est important de planifier la structure avant de l'implanter. La structure logique: décomposition de l'entreprise en domaines, arborescences, unités d'organisation. Cette décomposition pourra être guidée par la structure de l'entreprise et, surtout, par les besoins d'administrations :

- Limites de sécurité (qui est responsable de quoi) : domaines
- Possibilité de délégation d'administration : unités d'organisation
- Autorisation d'accès aux ressources
- Contraintes ou configurations des comptes et des sessions des utilisateurs
- ...

Nous allons détailler les outils qui sont à la dispositions de l'architecte du réseau pour créer sa structure logique. Plus tard, nous parlerons de éléments qui l'inciteront à adopter une structure plutôt qu'une autre: délégation de tout ou partie de l'administration de tout ou partie d'un ensemble d'utilisateurs et, dans un autre chapitre, les stratégies de groupes (imposer des configurations aux utilisateurs et aux ordinateurs).

Domaine

- Limite de sécurité
- Unité d'administration
- Unité de réplication
- Mode d'un domaine: mixte ou natif (dépend de l'OS des contrôleurs de domaine)

Limite de sécurité: chaque domaine dispose de ses propres stratégies de sécurité.

Unité d'administration: L'administrateur du domaine gère l'ensemble de la sécurité sur son domaine. Il est le seul à pouvoir accorder des permissions sur les objets de son domaine. Sauf autorisation accordée explicitement, il ne gère rien en dehors de son domaine.

Unité de réplication: les données actives directory sont répliquées sur tous les contrôleurs de domaine toutes les 5 mn.

Mode d'un domaine: **mode mixte**: s'il reste des contrôleur de domaine NT4. Certaines fonctionnalités ne sont pas disponibles. **Mode natif**: si tous les contrôleurs de domaine sont en W2K. L'OS des ordinateurs non contrôleur du domaine n'influe pas sur le mode.

Il est possible de passer du mode mixte au mode natif mais pas l'inverse.

Unités d'organisations

- Organisation logique à l'intérieur d'un domaine
- Contient des objet active directory
- Permet
  - De déléguer des pouvoirs
  - De simplifier la sécurité
  - D'appliquer une stratégie à des ordinateurs ou utilisateurs
- Rend obsolète la construction usuelle domaine de compte/domaine de ressources NT4
- Une UO ne peut être créée que dans le domaine ou une autre UO

Une **unité d'organisation** (UO) est un « container » pouvant contenir des utilisateurs, des ordinateurs, des groupes, ... et d'autres unités d'organisation.

Une unité d'organisation doit être utilisée quand on souhaite déléguer des pouvoirs ou appliquer une stratégie particulière à un sous-ensembles des objets du domaine.

Il est possible de donner tout ou partie des droits d'administration sur les objets d'une UO à certains utilisateurs.

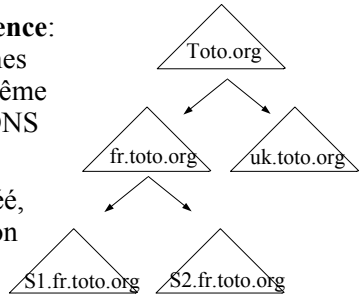
En créant une unité d'organisation regroupant les ordinateurs du domaine, on peut déléguer leur gestion à un utilisateur qui n'aura pas de droit sur les comptes utilisateurs. On évite de mettre en place deux domaines ressources/comptes comme sous NT4.

Sans UO, les utilisateurs sont dans le container *Users* (qui n'est pas une UO) et les ordinateurs dans un container *Computers* qui n'est pas une UO.

Un petit piège: une UO ne peut être créée que dans le domaine ou dans une autre UO. « users » n'est pas une UO et on ne peut donc pas créer d'UO (« unité d'organisation » n'apparait alors pas dans le menu « Nouveau ».

Arborescences

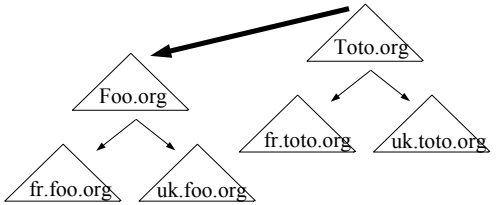
- **Arbre ou arborescence**: ensemble de domaines appartenant à une même hiérarchie de nom DNS
- **Domaine racine**: premier domaine créé, non renommable, non supprimable
- **Domaine enfant**



L'ajout d'un nouveau domaine se fait en créant un domaine enfant à un domaine existant de l'arborescence. Le nom complet (DNS) du nouveau domaine est obtenu en concaténant son nom au nom du domaine parent. Ainsi, le nom de S1 est S1.fr.toto.org.

Forêts

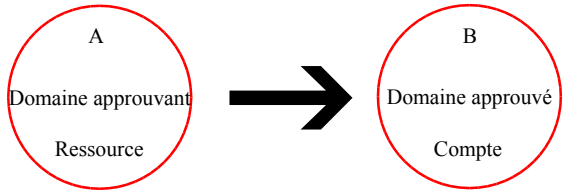
- **Forêt**: ensemble d'arborescences



Une **forêt** est un ensemble d'arborescences ayant des noms appartenant à des espaces non contigus. Les arborescences d'une forêt partagent une configuration, un schéma et un catalogue global communs. Le nom de la forêt est le nom de l'arborescence racine (première arborescence créée dans la forêt).
Une forêt peut ne contenir qu'une seule arborescence.

Relations d'approbation

- Déléguer l'authentification
- Permettre d'autoriser des utilisateurs d'un autre domaine à utiliser des ressources de son domaine



Une relation d'approbation permet à l'administrateur d'un domaine A de déléguer l'authentification de certains utilisateurs à un autre domaine B.

L'administrateur du domaine A peut accorder l'accès à certaines ressources (ouvrir une session, accès à des ressources, ...) aux utilisateurs validés par le domaine B. Cet accès doit être explicitement donné par l'admin de A qui reste donc maître chez lui.

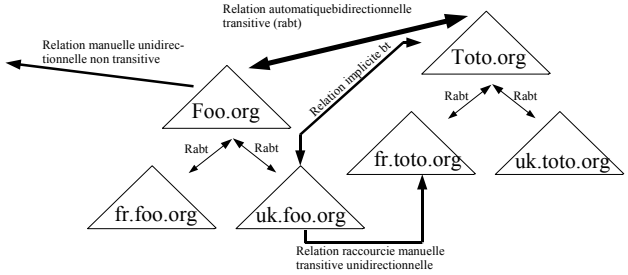
Parallèle avec la vie courante : une médiathèque départementale peut accepter les cartes délivrées par les bibliothèques municipales pour identifier certains de ses lecteurs. Dans ce cas, la médiathèque joue le rôle du domaine approuvant et les bibliothèques municipales jouent le rôle du domaine approuvé.

La médiathèque est libre de décider l'accès à ses ressources qu'elle laisse aux membres des bibliothèques municipales tout comme l'administrateur du domaine A est libre de décider l'accès qu'il laisse aux membres du domaines B (en général, l'accès est donné aux membres d'un groupe de B, pas à des utilisateurs individuels).

Une carte de bibliothèque locale permet à la médiathèque de vous authentifier (elle sait qui vous êtes) mais son règlement intérieur peut ensuite vous refuser l'accès (vous n'êtes pas autorisé).

Relation d'approbation sous W2K

- Relation bidirectionnelles/unidirectionnelles, transitives, implicites, manuelles/automatiques, raccourcies



Une relation entre un domaine A et un domaine B est **bidirectionnelle** si A approuve B et si B approuve A.

Une relation est **transitive** si A approuve B, B approuve C alors A approuve C même s'il n' y a pas de relation d'approbation explicite entre A et C.

Au sein d'un forêt, des relations d'approbations bidirectionnelles transitives entre domaine parent et domaines enfantset entre arborescences et racine sont automatiquement mises en place lors de la création des arborescences et des domaines.

Il est possible de créer manuellement des **relations raccourcies** qui évitent le parcours complet du chemin entre deux domaines. De telles relations sont unidirectionnelles et transitives.

Les **relations d'approbations externes** peuvent être créées manuellement entre deux domaines de deux forêts différentes ou entre un domaine W2K et un domaine non W2K. Ces relations externes sont unidirectionnelles et non transitives.

Structure physique

- Sites
- Contrôleurs de domaines

La structure physique d'active directory est distincte de sa structure logique. La structure physique vous permet de gérer et d'optimiser le trafic de votre réseau. Elle se compose de deux éléments: les contrôleurs de domaine et les sites:

Un **site** est un ensemble de plusieurs sous réseaux IP reliés entre eux par des liaisons à haut débit. Les liaisons entre sites peuvent être plus lentes ou plus coûteuses.

Définir des sites, c'est donner des informations à windows 2000 qui lui permettront d'optimiser le trafic lié à la duplication entre contrôleurs de domaines et la vitesse de la liaison entre les utilisateurs et leur contrôleur de domaine.

La notion de site est indépendante de la notion de domaine: un domaine peut contenir plusieurs sites e un site peut contenir plusieurs domaines.

Un **contrôleur de domaine** est un ordinateur sous windows 2000 server qui stocke et gère une copie de la base d'active directory. Il duplique les modifications de l'annuaire vers les autres contrôleurs. Le processus d'ouverture de session des 'utilisateurs met forcément en jeux au moins un contrôleur de domaine. Il est donc important que tout utilisateur puisse avoir une liaison rapide et fiable avec au moins un contrôleur de domaine.

Pour concevoir une structure physique cohérente, il faut maîtriser le fonctionnement de la réplication entre contrôleurs de domaine et les rôles des maîtres d'opérations.

Exécution multimaîtres (W2K) vs maître unique (NT 4)

- Sous NT4: un contrôleur principal (original en lecture/écriture) et des contrôleurs secondaires (copie en lecture)
- Sous W2K: des contrôleurs de domaines identiques, une base en lecture/écriture sur chaque contrôleur
- W2K: Opérations en maîtres unique : maitres d'opérations

Sous windows NT4, un contrôleur de domaine particulier appelé le **contrôleur principal** du domaine hébergeait les informations du domaine (sécurité, ...) et y avait un accès en lecture/écriture. Les **contrôleurs secondaire** avaient une copie de ces informations. Un contrôleur secondaire pouvait servir à consulter les informations mais pas à les modifier. Les modifications devaient avoir forcément lieu sur le contrôleur principal (changement de mot de passe, création d'utilisateurs, ...)

Sous W2K, les contrôleurs de domaines sont globalement tous équivalents et hébergent une copie des informations de la base d'annuaire accessible en lecture/écriture. La base d'annuaire est dupliquée et distribuée sur chaque contrôleur de domaine (**réplication multimaîtres)**. Les opérations usuelles (créations de comptes, changement de mot de passe, ...) peuvent être réalisées sur n'importe quel contrôleur du domaine. Dans certains cas, si des modifications incompatibles sont réalisées sur des contrôleurs à un moment où ils sont coupés du réseau, seule l'une de ces modification sera prise en compte. W2K a été conçu pour limiter au maximum ce type de problèmes.

Certaines opérations critiques sont prises en charges par un seul contrôleur de domaine. Pour ces quelques opérations, on retrouve un fonctionnement en maître unique (mais une copie en lecture est accessible sur tout ou partie des autres contrôleurs). Les ordinateurs réalisant ces opérations critiques sont appelés des **maîtres d'opérations** (ou **FSMO** : Flexible Single Master Operation).

Partition d'annuaire

- Partition d'annuaire : portion de l'espace de noms de l'annuaire
- Sert à répartir les données de l'annuaire
- Sous arbres :
  - Configuration
  - Schema
  - Domaine

Consultez le tome 6 du kit de ressources techniques pour plus d'information sur la parition d'annuaire: reskit tome 6 page 99 et suivantes

Voir cours3-AF pour une présentation de LDAP.

Maîtres d'opérations

- Maître de schéma
- Maître d'attribution de noms de domaine
- Le maître émulateur CPD
- Le maître de RID (identifiants relatifs)
- Le maître d 'infrastructure

Maître de schéma: modification sur le schéma d'annuaire. Un par forêt.

Maître d'attribution de nouveau noms de domaine:permet d'ajouter/retirer un domaine de la forêt et les objets de référence croissée avec les annuaires externes. Un par forêt. S'il est indisponible, les fonctions qu'il assure ne sont plus assurée. Le rôle peut être transféré définitivement à un autre contrôleur.

Maître émulateur CPD: sert de contrôleur principal de domaine aux ordinateurs w9x ou NT membres du domaines sur lesquels le client Active Directory n'a pas été installé. Il y en a un par domaine. S'il est indisponible, les changements de mot de passe depuis des ordinateurs w9x et NT sans client active directory seront impossibles. Certaines ouvertures de sessions seront perturbées (cf reskit chap. 7).

Maître des identificateurs relatifs : distribue des paquets d'identificateurs relatifs aux contrôleurs de domaine. Les contrôleurs de domaines peuvent ainsi utiliser ces identifiants relatifs lors de la création des principaux de sécurité (utilisateurs, groupes ou ordinateurs). Quand un contrôleur de domaine a épuisé son stock d'identifiants relatifs, il doit contacter le maître RID pour en obtenir de nouveaux. Si le maître RID est indisponible, il ne sera plus possible de créer de nouveaux principaux sur ce contrôleur. Il y a un maître RID par domaine. Le maître RID sert aussi lors du transferts de principaux d'un domaine dans un autre à l'aide de l'utilitaire movetree. L'utilitaire DCDIAG permet d'afficher l'allocation des paquets (option /v, test RidManager, cf reskit tome 6, chapitre 10 et dcdiag /?) -> cf diapo suivante pour la suite.

Exemple

- Arborescence de domaines : toto.fr, s1.toto.fr et s2.toto.fr
- Indiquez les rôles de maître d'opération de cette forêt (11 rôles)

Maître d'infrastructure:Quand un utilisateur et un groupe sont dans deux domaines différents, le changement de nom de l'utilisateur n'est pas pris en compte tout de suite au niveau du groupe. le maître d'infrastructure est responsable de la référence transdomaine groupe-à-utilisateur de façon à mettre à jour le nom de l'utilisateurs là où il est utilisé dans les autres domaine. Il y a un maître d'infrastructure par domaine.

Le maître d'infrastructure compare ses données à celles du serveur de catalogue global. Les deux rôles ne doivent pas être assurés par le même ordinateur.

En cas d'indisponibilité du maître d'infrastructure, les mises à jour seront retardées.

Réponse de l'exemple: au niveau de la forêt toto.fr: 1 maître de schéma et un maître d'appellation de domaines. Au niveau de chaque domaine : un émulateur CPD, un maître d'infrastructure et un maître des RID (soit 3*3=9 rôles).

Placement des rôles de maître d'opération

- 3 soucis :
  - Contrôler la charge réseau
  - Augmenter les performances et la fiabilité
  - Permettre un remplacement rapide en cas de défaillance
- Transfert de rôle:
  - Ntdsutil: pour transférer un rôle en ligne de commande
  - Repadmin: diagnostique de la réplication (vérification de la mise à jour)

En cas de défaillance d'un rôle, il est possible de transférer le rôle à un contrôleur existant. Pour éviter les pertes d'informations, il est utile de repérer les contrôleurs de domaines qui sont partenaires de réplication de chaque maître d'opération. En tant que partenaire direct, ces ordinateurs auront la base de données la plus à jour possible et sont des remplaçants idéaux.

Le placement par défaut des rôles convient bien aux domaines de petite taille. Pour les domaines de grande taille, on peut planifier le placement des rôles :

La planification prendra en compte la topologie du réseau et les actions à mener en cas de défaillance.

Pour plus d'information, consultez le kit de ressources techniques, tome 6 pages 400 et suivantes.

Serveurs du catalogue global

- Mémorise une copie partielle des données Active Directory de tous les domaines de la forêt
- Utile pour l'ouverture de session des utilisateurs :
  - Appartenance aux groupes universels
  - Domaine d'un nom principal d'utilisateur
- Localisation d'objets dans la forêt
- Un contrôleur de domaine peut devenir serveur de catalogue global (action manuelle)
- Conseil: au moins un serveur de catalogue global par site et par domaine

Un **serveur de catalogue global** est un contrôleur de domaine possédant une copie en lecture seule des attributs les plus utilisés de **tous** les objets de la forêt.

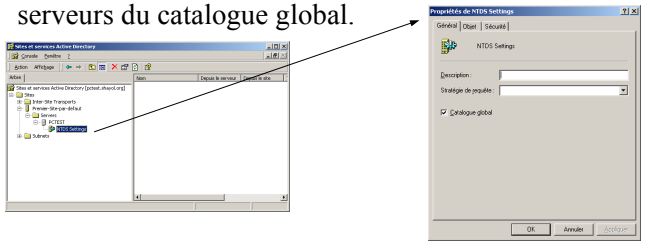
Le premier contrôleur de la forêt est serveur de catalogue global. Les administrateurs de domaines peuvent transformer n'importe quel contrôleur de domaine en serveur de catalogue global. Le serveur de catalogue global va être utilisé pour des recherches à l'échelle de la forêt. Il est conseillé d'avoir un serveur de catalogue global par site pour éviter l'utilisation de liaison lentes et d'avoir un serveur de catalogue global par domaine. Sans serveur de catalogue global, les recherches s'effectuent sur chaque contrôleur de domaine de la forêt.

Le serveur de catalogue global est consulté pendant l'ouverture de session des utilisateurs. Il fournit les informations sur l'appartenance de l'utilisateur à des groupes universels nécessaires à la création du jeton de sécurité de l'utilisateur. Si l'utilisateur a fourni un nom principal (petit@ueve.world) pour l'ouverture de session au lieu du couple identifiant/domaine ou nom SAM (UEVE\petit), c'est le serveur de catalogue global qui fournit le nom de domaine (UEVE) associé au nom principal.

Le serveur de catalogue global est consulté en cas d'ajout d'un utilisateur ou d'un groupe d'un domaine différent à un groupe du domaine.

Serveurs du catalogue global

- Sites et services Active Directory pour passer un contrôleur de domaine serveur de catalogue global
- Ouverture de session en cas d'indisponibilité des serveurs du catalogue global.



Pour passer serveur de catalogue global un contrôleur de domaine, il faut utiliser **Sites et Services Active Directory** et cocher l'option ad hoc dans les propriétés de **NTDS Settings**.

En cas d'indisponibilité de tous les serveurs de catalogue global :

- Un membre du groupe administrateurs du domaine peut ouvrir une session
- Pour les autres utilisateurs, la connexion s'appuie sur les informations mises en cache : si l'utilisateur s'est déjà connecté sur le domaine, il peut ouvrir une session. S'il ne s'est jamais connecté sur le domaine, il ne peut y ouvrir de session. Il peut néanmoins ouvrir une session sur l'ordinateur local.

Bibliographie

- Structure logique AD: reskit tome 6 chap. 1
- Maîtres d'opération, catalogue global : reskit tome 6, chapitre 1, chapitre 7
- Les RFC concernant LDAP : cf http://www.rfc-editor.org/ pour le texte des RFCs et l'annexe B du tome 6 du reskit pour la liste des RFCs concernées.

Bibliographie (2)

- Sécurité: reskit tome 6 chap. 12
- Sécurité: "Modèle de sécurité windows », Joel Marchand (hsc), MISC No 2

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

Les stratégies de groupes permettent d'imposer des paramètres de configuration (menus, paramètres des programmes (proxy, ...), paramètres de sécurité, limitations (pas de chgt de mot de passe, pas d'ouverture de session sur le cotrôleur de domaine, ...) à des utilisateurs ou à des ordinateurs. C'est un outil extrèmement utile qui permet de tout gérer au niveau du domaine (stratégies non locales).
Stratégie locale:
gérée par l'outil « stratégie de sécurité locale »
Stockée dans *%systemRoot%\System32\GroupPolicy*
la stratégie locale est écrasée par les stratégies non locales.
Stratégies non locales:
s'appuie sur active directory.
Une stratégie non locale consiste à définit un objet de stratégie de groupe et à le lier à un ou plusieurs conteneur (site, domaine, unité d'organisation.
On peut ainsi appliquer des paramètres identiques à plusieurs conteneurs. On peut désactiver l'application de paramètres à un conteneur en détruisant le lien sans détruire l'objet GPO. On peut les réactiver en recréant le lien. Ainsi, on ne perd tout le travail de configuration réalisé sur l'objet GPO.

- **Un objet GPO peut être lié à plusieurs conteneurs**
- **Un conteneur peut être lié à plusieurs objets GPO**

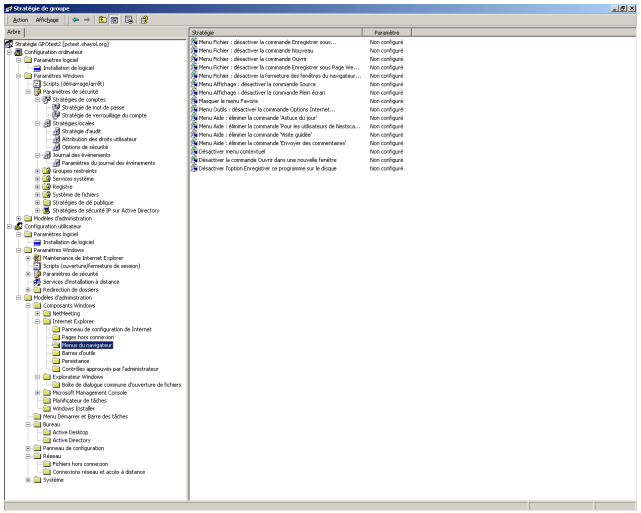
Paramètres contrôlés

- Modèle d'administration: paramètres basé sur le registre
- 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: paramètres s'appuyant sur le registre configurant les paramètres d'application (proxy internet explorer par exemple), la présentation des sessions utilisateurs, le comportement des services système.
Sécurité: configuration des options de sécurité locale, de domaine, de site. Par exemple: stratégie de sécurité des contrôleurs de domaine pour autoriser un utilisateur à ouvrir une session sur un contrôleur de domaine
installation des logiciels:gestion centralisée de la mise à jour des logiciels
Scrips:scrips exécutés à l'ouverture ou à la fermeture de session utilisateur, scripts exécuté au démarrage ou à l'arrêt de l'ordinateur
Redirection de dossiers: rediriger les dossiers de l'utilisateurs (Mes Documents, ...) sur le réseau. Permet à un utilisateur de voir ses dossiers quelque soit la machine sur laquelle il travaille.

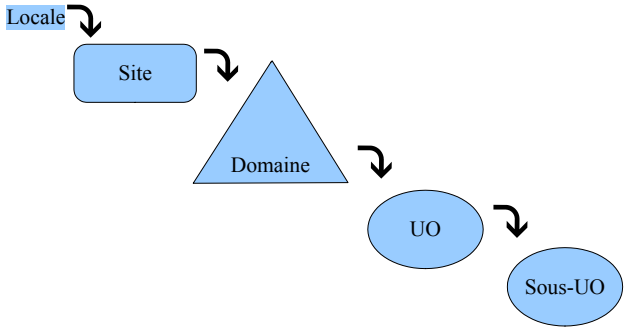
Objets stratégie de groupe (GPO)

- 2 parties :
  - Conteneur de stratégie de groupe (Group Policy Container) : objet AD
  - Modèle de stratégie de groupe (Group Policy Template GPT) : dossier
- Peut-être lié à plusieurs conteneurs
- Un conteneur peut être lié à plusieurs GPOs
- La stratégie s'applique aux objets du conteneur



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

Puis +sieurs diapo avec des exemples (cf ENI par 310ss)

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 LicProGSI, 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 LicProGSI et LicAutre
- Une GPO imposant la photo d'un prof barbu en fond d'écran liée à l'UO LicProGSI
- Qu'est-ce qui s'applique réellement à LicProGSI ?

Les GPO vont s'appliquer dans l'ordre suivant :

- GPO de site: fond d'écran chambord
- GPO de domaine : pas d'Exécuter dans « Démarrer »
- GPO d'UO: pas de changement de mot de passe et fond d'écran barbu

Quand un paramètre est redéfini, c'est le dernier appliqué qui l'emporte.

On obtient donc :

- pas d'Exécuter dans « Démarrer »
- pas de changement de mot de passe
- fond d'écran barbu

Demo2:

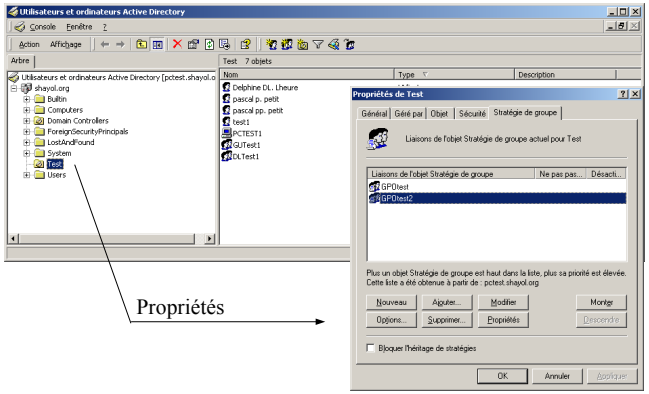
- On applique l'exemple
- On force la propagation des stratégies de groupe avec un « secedit /refreshpolicy machine_policy » et « secedit /refreshpolicy user_policy ». Souswindows XP, on utilisera gpupdate à la place de secedit.
- On le vérifie
  - soit avec le compte étu1 sur le contrôleur de domaine,
  - 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)
- Actualisation toutes les 5 mn sur les contrôleurs de domaine
- Forcer l'actualisation:
- secedit /refreshpolicy user_policy| machine_policy

Pour forcer la mise à jour :
Scedit /refreshpolicy machine_policy ou Scedit /refreshpolicy user_policy
Sous windows Xp: utiliser la commande gpupdate

Création d'un objet stratégie de groupe



Bibliographie

- Kit de ressource technique tome 6
- « Active Directory, les services d'annuaires windows 2000 » de V. Cottin, édition ENI