Administration système: cours 7 (PP)

- AD: gestion des groupes
- AD: délégation de contrôle, consoles MMC
- AD avancé: forêt, arborescences, relations d'approbation, maîtres d'opérations, serveur de catalogue global
- AD: stratégies de groupe
- AD: Les domaines windows 2000
- Sauvegardes: présentation générale, ntbackup
- SMTP

Groupes: présentation

- Un groupe est un ensemble d'utilisateurs
- Les membres d'un groupe bénéficient des droits attribués au groupe
- Un utilisateur peut être dans plusieurs groupes
- Les groupes peuvent contenir d'autres groupes
- Les groupes simplifient l'administration
- Jusqu'à 5000 membres
- Groupes de distribution et groupes de sécurité

Groupes: étendue de groupes

- Groupes locaux sur un ordinateur autonome
- Groupes locaux de domaine
- Groupes globaux
- Groupes universels
- Restriction dans un domaine en mode mixte

Groupes locaux de domaine (LD)

- Peut contenir
  - des utilisateurs, des groupes globaux et des groupes universels de tous les domaines de la forêt;
  - des groupes de domaine locaux de son domaine
- Utilisable seulement dans son domaine;
- Peut être membre de DL de son domaine;
- On peut l'utiliser pour affecter droits et permissions
- Membres non copiés dans le catalogue global.

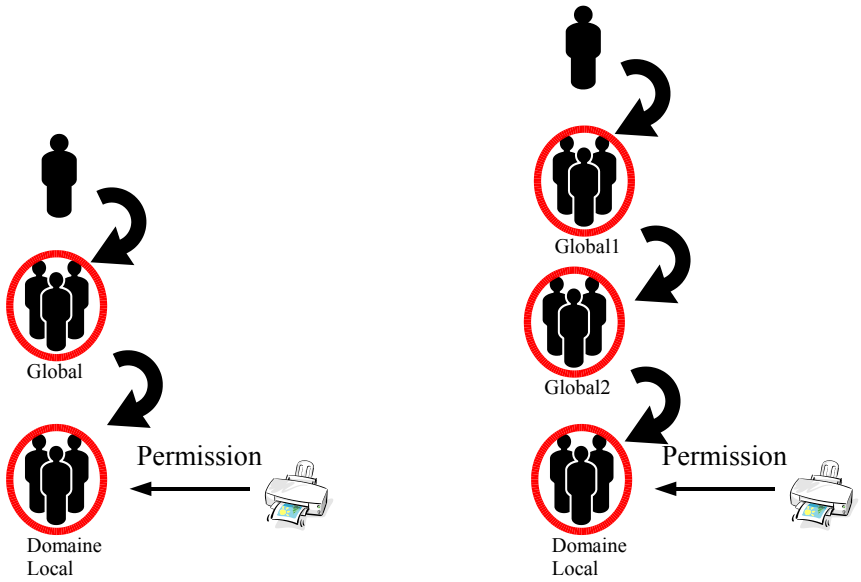
Groupes globaux

- Peut contenir des utilisateurs, des groupes globaux du **même** domaine;
- Peut être membre de groupes (DL, G, U) de tout domaine de la forêt
- On **ne** peut **pas** l'utiliser pour affecter droits et permissions
- Membres non copiés dans le catalogue global.

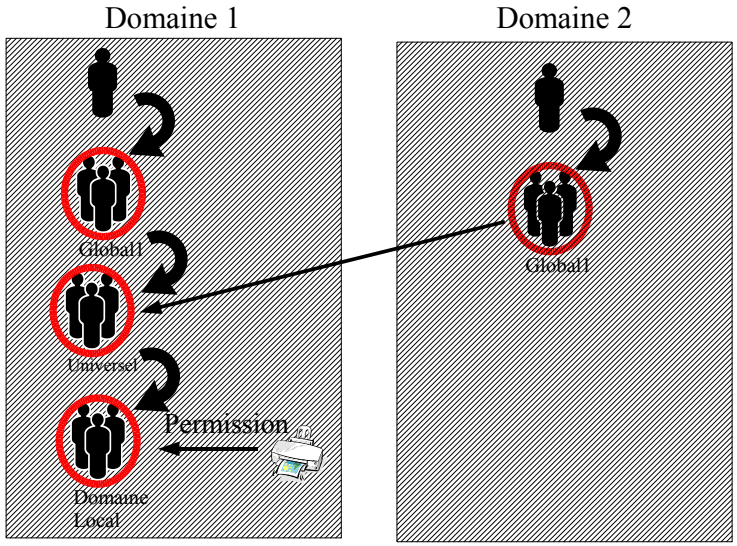
Groupes universels

- Peut contenir des utilisateurs, des groupes globaux et des groupes universels de **tous** les domaines de la forêt;
- Peut être membre de DL de tout domaine et de groupes universels
- On peut l'utiliser pour affecter droits et permissions
- Ses membres copiés dans le catalogue global.

Planification des groupes



Planification des groupes (2)



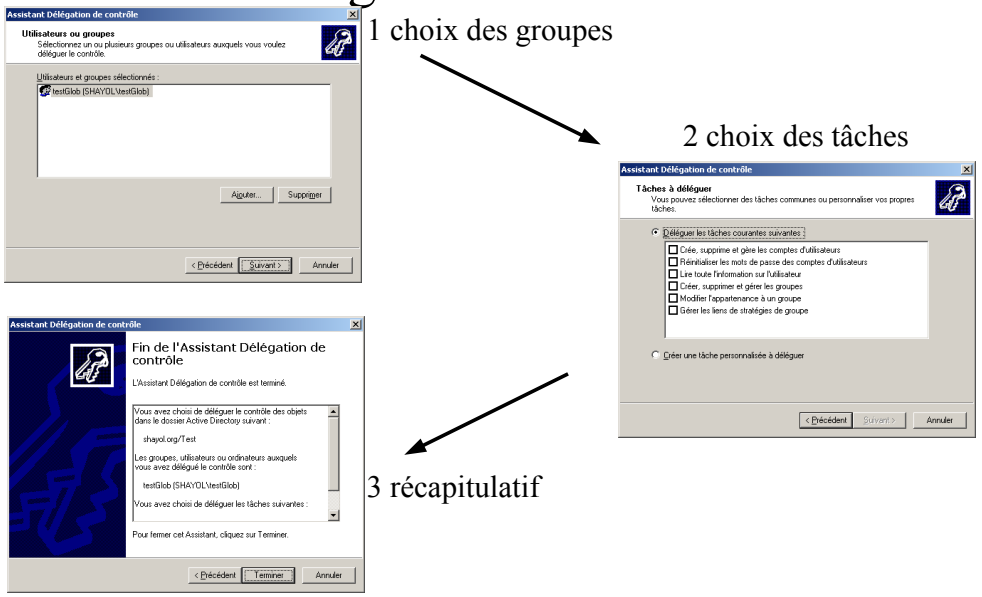
AD-DEMO: gestion des groupes dans un domaine

- Création d'un groupe Gtest sur le domaine (groupe local de domaine)
- Ajout de l'utilisateur test1 à Gtest
- Sur une station de travail, créer un dossier RepTest et donner le droit CT à Gtest et lecture au groupe « Tout le monde » sur RepTest
- Vérifier les accès
- Utiliser Gtest pour sélectionner les utilisateurs qui peuvent changer l'heure des stations de travail

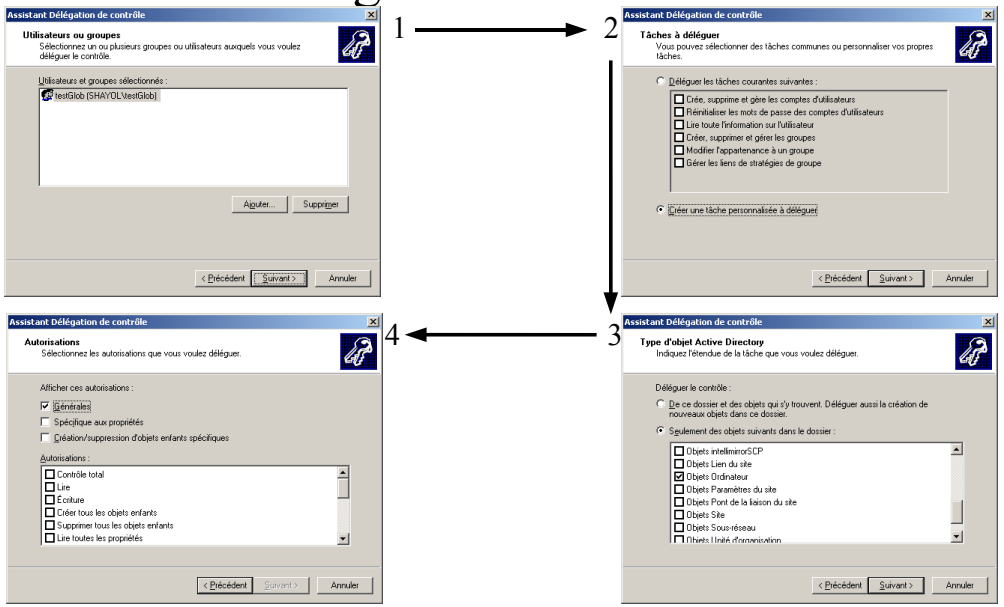
Délégation de tâche

- Délégation de contrôle sur le domaine ou sur une unité d'organisation : déléguer une partie des tâches d'administration sur certains objets à certaines personnes
- Création de console MMC personnalisées,
- Administration à distance

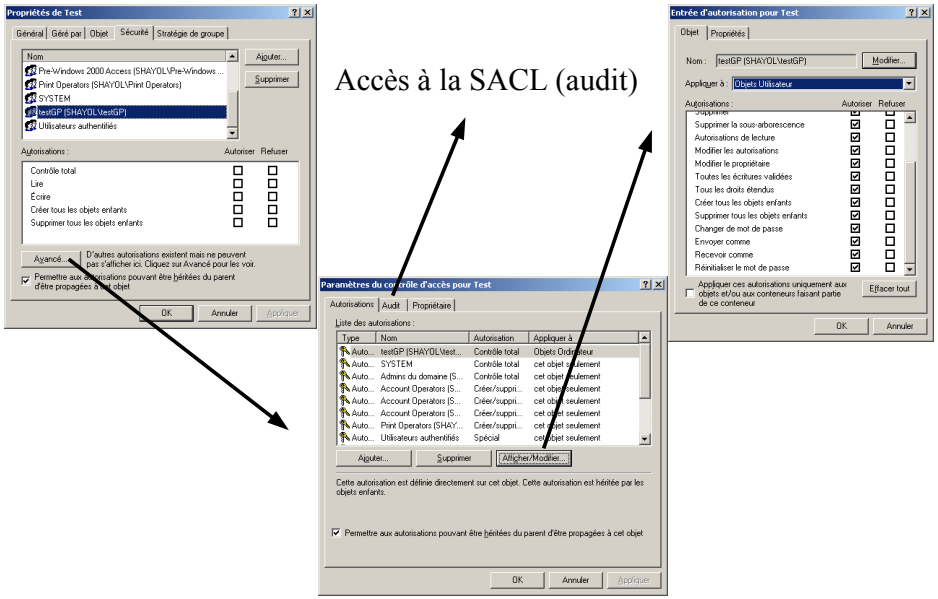
Délégation de contrôle



Délégation de contrôle



Modification de délégation, Audit



AD-DEMO: delegation de contrôle

- Création d'une unité d'organisation UOtest
- On y met les utilisateurs test2, test3
- On délègue la remise à zéro des mots de passe de l'UO à l'utilisateur test1
- Remarque: travailler avec un groupe plutôt qu'avec un utilisateur test1.

Création d'une console personnalisée

- L'administration W2K: des consoles MMC pré-créées;
- En standard, un jeu plus riche sur un contrôleur de domaine mais installable sur tout ordinateur W2K (adminpak)
- Administration à distance
- Possibilité de créer des consoles personnalisées

Création d'une console personnalisée

- Utilisation de mmc.exe
- Ajout de composants enfichables, extensions
- Mode auteurs, mode utilisateur

Structure logique

- Forêts
- Arborescences
- Domaines
- Unités d'organisation

Domaine

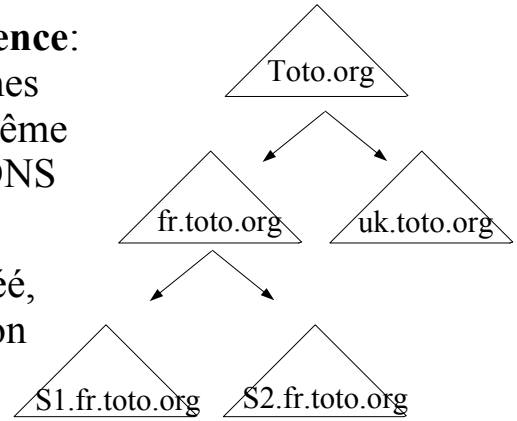
- Limite de sécurité
- Unité d'administration
- Unité de réplication
- Mode d'un domaine: mixte ou natif (dépend de l'OS des contrôleurs de domaine)

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

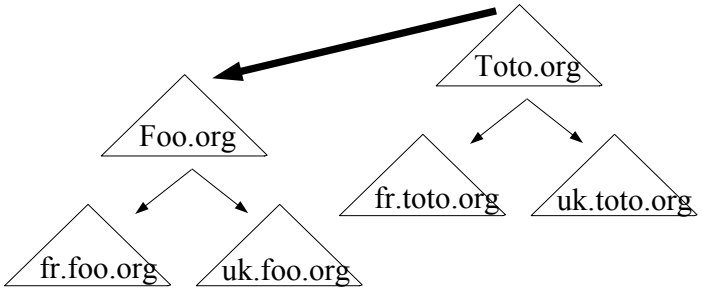
Arborescences

- **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**



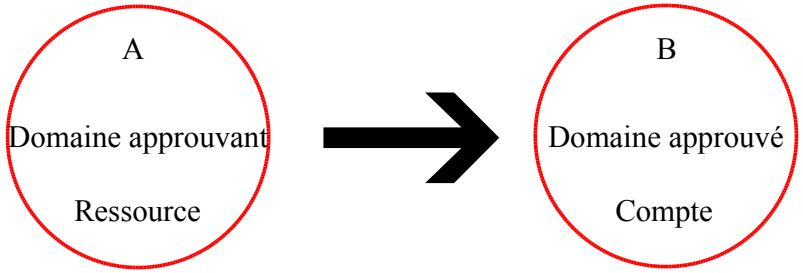
Forêts

- **Forêt**: ensemble d'arborescences



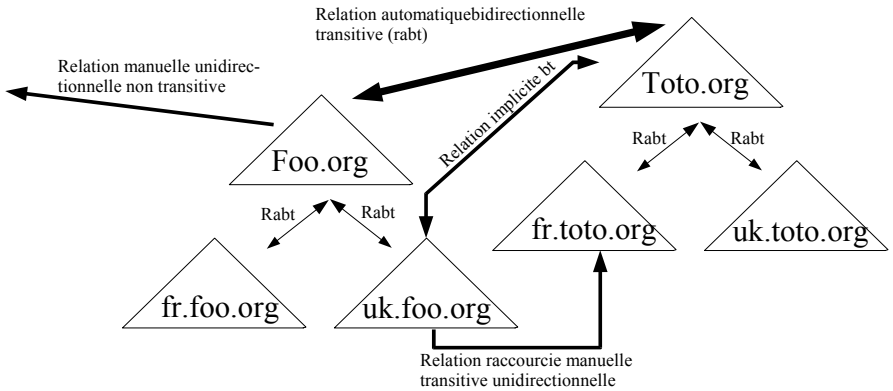
Relations d'approbation

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



Relation d'approbation sous W2K

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



Structure physique

- Sites
- Contrôleurs de domaines

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

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

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

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)

Placement des rôles de maître d'opération

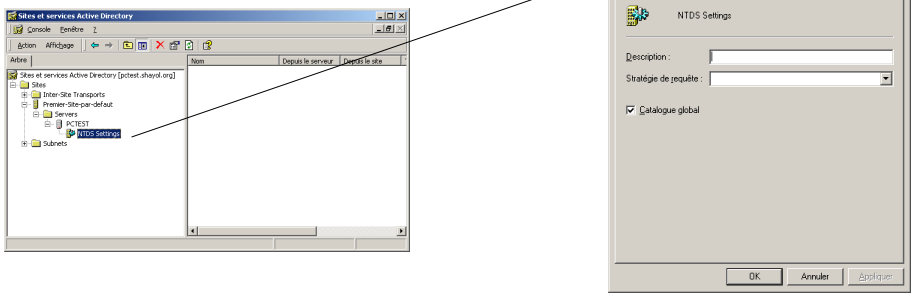
- 3 soucis :
  - Contrôler la charge réseau
  - Augmenter les performances et la fiabilité
  - Permettre un remplacement rapide en cas de défaillance
- Transfert de rôle:
  - Ntdsutil: pour transférer un rôle en ligne de commande
  - Repadmin: diagnostique de la réplication (vérification de la mise à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

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

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.



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

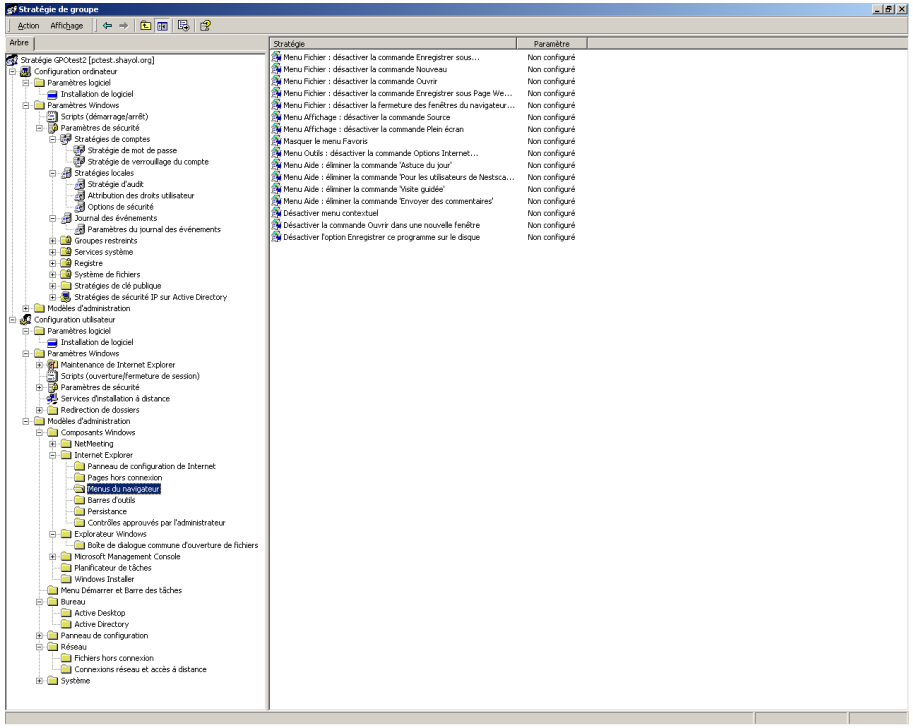
- Permet d'imposer à des ordinateurs ou à des utilisateurs des configurations, des paramètres
- 2 types de stratégies:
  - Stratégies locales : propre à un ordinateur
  - Stratégies non locales: s'appuient sur Active Directory

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

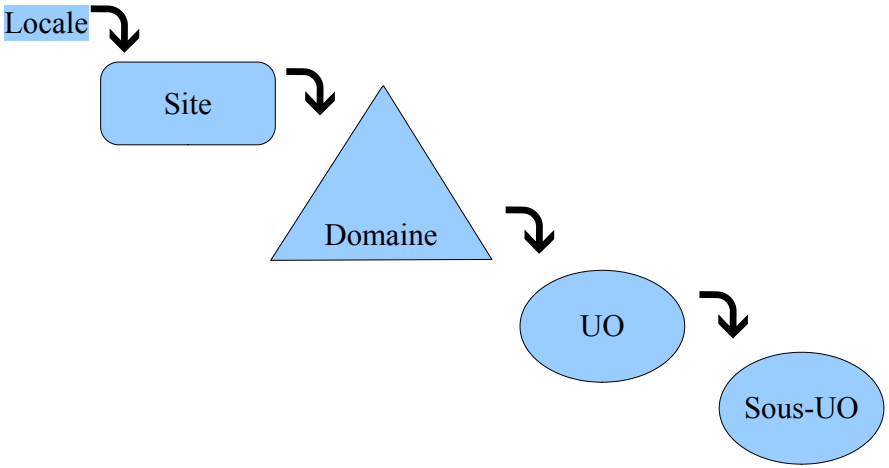
Objets stratégie de groupe (GPO)

- 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

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

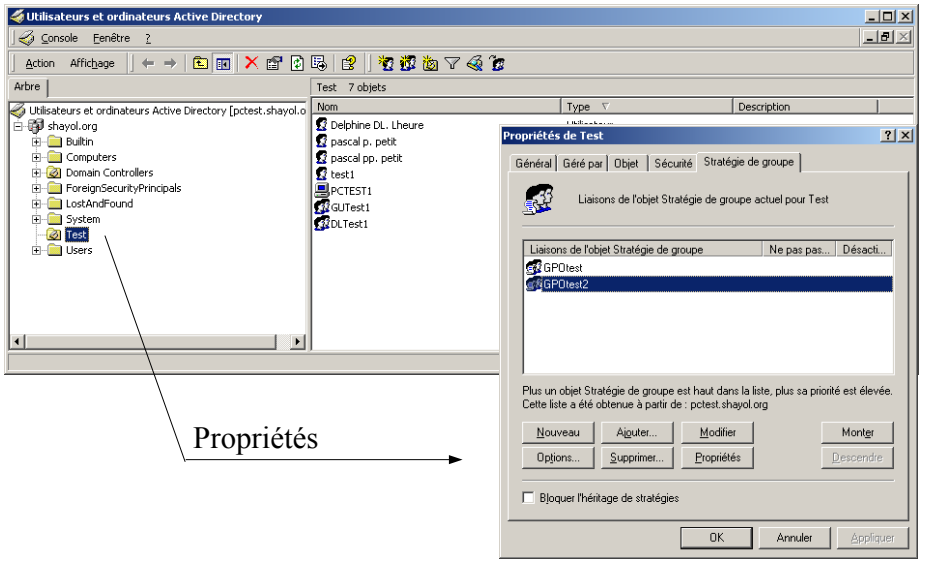
Demo2:

- 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: scedit /refreshpolicy ...

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

Sauvegarde

- Sauvegarde / archivage
- Sauvegarde des données / du système
- on sauvegarde certaines données pour se protéger de certains risques
  - faire la liste des risques dont il faut se protéger
  - adapter le cahier des charges des sauvegardes et des autres mesures en fonction des ces risques
  - les sauvegardes ne sont qu'un des éléments permettant de garantir la continuité du service à côté d'autres : disques raid, redondance des serveurs, ...

Solutions qui ont prouvé leur inefficacité

- Faire faire les sauvegardes par les utilisateurs : pour dégager sa responsabilité mais aucune garantie qu'elles seront faites
- Sauvegardes sur des supports peu fiables (disquettes, DAT, ...)
- Sauvegarde en écriture seule : il faut valider sauvegarde et procédures de restauration
- Sauvegarde d'un système en cours d'exécution
- Un seul support de sauvegarde
- Sauver sur une partition du même disque
- Pas de sauvegarde hors site (incendie, ...)

Sauvegardes : procédure/planification

- Planifier les sauvegardes, tester leur réalisation
  - il faut avoir l'assurance que les sauvegarde prévues ont eu lieu
  - les procédures de sauvegardes doit être écrites
  - procédures testées
  - procédures et planification validées par les utilisateurs/propriétaires des données

Sauvegardes : planification

- choix des données à sauvegarder :
  - données des utilisateurs (y compris : boîtes aux lettres, profil, ...), fichiers de configuration, ..;
    - retrouver un système en état suppose de réinstaller le système puis de restaurer les données
    - volumétrie plus faible
  - Système entier avec procédure de redémarrage:
    - restauration directe et rapide d'un système opérationnel
    - volumétrie plus importante
- périodicité, choix des données ont un impact fort sur la volumétrie et donc sur le coût =>compromis

Problèmes liés à la volumétrie:

- Coût
- Charge réseau
- Durée des sauvegardes
- Indisponibilité des serveurs/applications dans le cas où le logiciel de sauvegarde impose l'arrêt des logiciels.

Restauration

- procédures de restauration
  - écrites
  - au résultat validé par les propriétaires des données (pour ne pas en oublier
  - **testées régulièrement en grandeur réelle** de façon à garantir :
    - que toutes les données pertinentes ont été sauvegardées
    - d'être capable de tout restaurer correctement

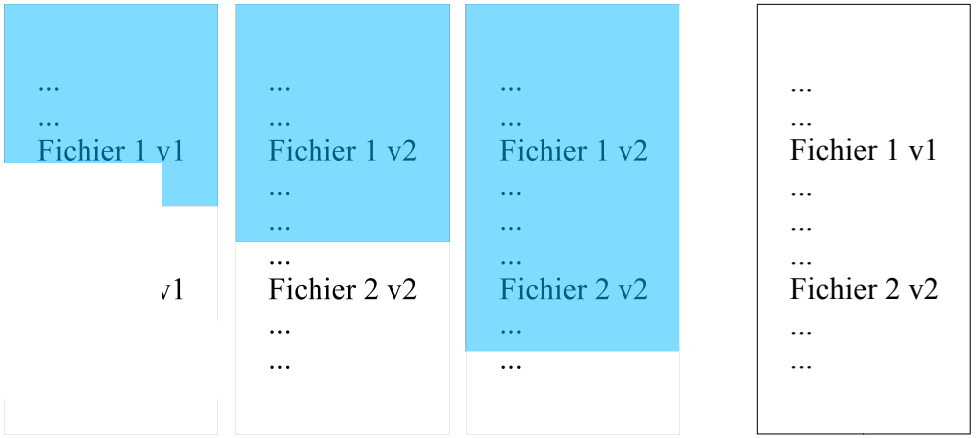
Fiablisation

- utiliser des média fiables
  - éviter disquettes, CD RW, DAT, ..et leur préférer CD R,DLT, ...
  - varier les marques de media pour palier un défaut de fabrication, ...)
- gérer le vieillissement des média de sauvegarde (reprise sur des média récents, ...)

Fiabilisation (2)

- fiabiliser l'environnement des media de sauvegarde:
  - inondation, incendie, vol (coffre ignifugé, ...)
  - sauvegarde hors site (penser à la confidentialité des données, au risque de vol, à l'interception des données, ...)
- indexer les données pour s'y retrouver dans le volume total des jeux de sauvegardes
  - indexer les données
  - étiqueter les media

Sauvegarde live: problématique



Si l'application modifie plusieurs fichiers durant la sauvegarde, les versions sauvées peuvent ne pas être cohérentes.

Sauvegarde live: solutions

- Arrêt de l'application pendant la sauvegarde:
  - garantit de plus qu'aucun verrou n'empêchera l'accès à un fichier
- Snapshot: image des blocs du sgf, en cas d'effacement de fichier, les blocs ne sont pas réalloués tant que la sauvegarde n'est pas finie
  - Suppose un support dans le sgf
  - Proposé par les NAS, par afs, LVM, FreeBSD, ...
  - Application supplémentaire : proposer aux utilisateurs une image des états antérieurs de leur compte à moindre coût.

Sauvegarde live: snapshot

- Là, on mettra une illustration du fonctionnement des snapshot
- Fait en live au tableau.

Sauvegardes incrémentales/différentielles

- Sauvegarde incrémentales : fichiers créés ou modifiés depuis la sauvegarde précédente
  - Diminue le volume à sauver
  - Restauration nécessite toutes les sauvegardes, restaure toutes les versions d'un même fichier
  - Peu adapté si la totalité des fichiers changent
- Sauvegarde différentielle : fichiers créés/modifiés depuis la dernière sauvegarde de référence
  - Diminue le volume à sauver
  - Plus de volume qu'en incrémental
  - Restauration nécessite la sauvegarde de référence et la dernière sauvegarde différentielle

Exemple:

- Comparer la taille des sauvegardes et les procédures de restauration dans les cas suivants : (ST: sauvegarde totale, I: sauvegarde incrémentale, D: sauvegarde Différentielle)
- Cas 1) ST, I1, I2, I3, I4, I5, I5
- Cas 2) ST, D1, D2, D3, D4, D5
- Cas 3) ST, I1, I2, I3, D1, I4, I5

Dump: un outil de sauvegarde sous unix

- Dump est un outil unix
- Il est efficace (travail directement au niveau du sgf)
- Sauvegarde non portable d'un unix à un autre (lié au sgf)
- Niveau (0 à 9) permettant un gestion très souples des sauvegarde incrémentales/differentielles:
  - Une sauvegarde niveau *n* sauvegarde tous les fichiers modifiés depuis la dernière sauvegarde de niveau *n-1*

Ntbackup: un outil de sauvegarde sous windows

- Un outil apparu avec windows 2000
- Pratique et polyvalent
- Supporte les sauvegarde incrémentales et différentielles
- Permet de sauver les données (au choix) et/ou les fichiers systèmes
- Utile pour des sauvegardes « artisanales »
- Pour des sauvegardes lourdes, la pratique est d'utiliser des logiciels dédiés (cf cours sauvegarde AF) qui géreront les verrous sur les fichiers, les sauvegardes live de certaines applications, ...

Ntbackup

- La restauration nécessite que w2k soit installé
- NT Backup est installé par défaut sous windows 2000/XP pro et serveur.
- Ntbackup est fourni avec windows Xp home (cf VALUEADD\MSFT\NTBACKUP)

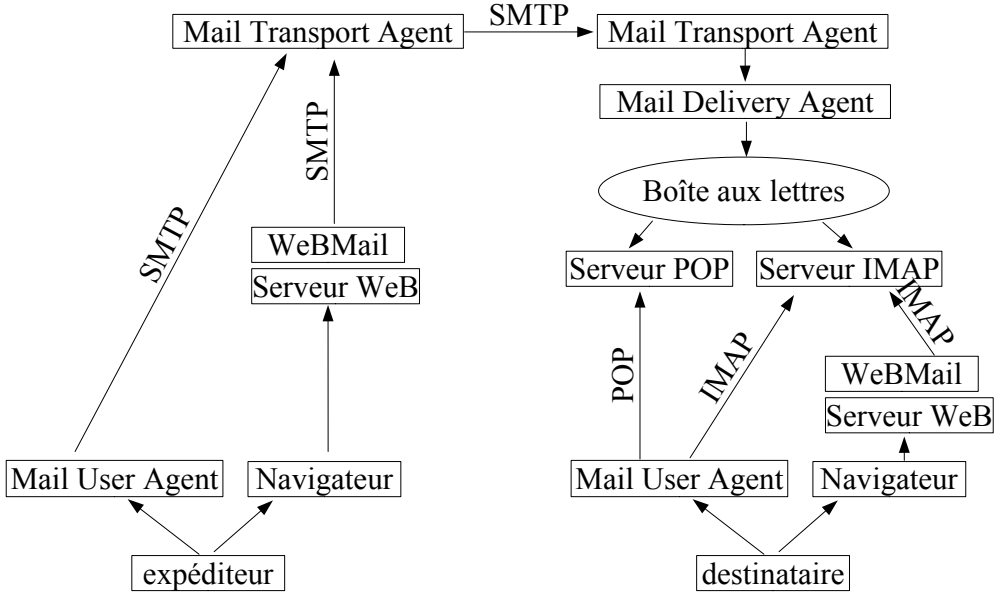
Windows: droit requis pour les sauvegardes

- Dans la prochaine version de ce document

SMTP: notions de base

- L'envoi et la réception d'un courrier mettent en jeu de nombreux outils et protocoles. Notamment :
  - MUA: Mail User Agent ou agent utilisateur (mail, mutt, thunderbird (mozilla), eudora, voire même Outlook express si n'a peur de rien),
  - MTA: Mail Transport Agent ou agent de transport (serveur smtp: sendmail, postfix, qmail, exim, voire exchange),
  - MDA: Mail Delivery Agent ou agent de délivrance du courrier, chargé par le MTA de déposer le courrier dans la boîte aux lettre de l'utilisateur (exemple: procmail, ...)

SMPT: architecture



SMTP:

- Rfc821 puis 2821: protocole SMTP
- Rfc822 puis 2822: format des courriers
- D'autres documents concernent le courrier: POP3, IMAP, ETRN, MIME, ...

SMTP: commandes

- Contrôle de session
  - HELO/EHLO
  - RSET/QUIT
  - NOOP
- Traitement des courriers
  - MAIL From:<adresse>
  - RCPT To:<adresse>
  - DATA
  - VRFY/EXPN

SMTP: DEMO (1)

- On se connecte sur le port 25 d'un serveur existant et on tape quelques commandes pour jouer
- On commente les capacités annoncées par le MTA
- On commente les codes d'acquittement (il est de bon ton de faire quelques fautes de frappe pour générer des erreurs)

SMTP: DEMO (2)

- On se connecte sur le port 25 d'un serveur existant et on envoie un courrier:
  - Un courrier raisonnable
  - Un courrier avec un expéditeur bidon et des entêtes bidon
- On commente encore les codes d'acquittement
- On montre un refus de relais

SMTP: acquittement (rfc 2821)

- un code normalisé suivi par du texte (non normalisé)
- Codes:
  - 1xy: acquittement positif préliminaire
  - 2xy: acquittement positif
  - 3xy: acquittement positif intermédiare : commande acceptée mais attente de données pour compléter (ex: DATA)
  - 4xy: acquittement négatif provisoire
  - 5xy: acquitement négatif définitif

SMTP: acquittement

- Codes: signification du deuxième caractère
  - x0z: erreur de syntaxeThe second digit encodes responses in specific categories:
  - x1z: Information: statut ou aide
  - x2z Connecxions: réponse ayant trait au canal de communication
  - x5z Système de courrier : réponses indiquant l'état du système de courrier suite à la commande
- Codes: 3e caractères: précise le deuxième

SMTP: exemples d'acquittements

500 Syntax error, command unrecognized

501 Syntax error in parameters or arguments

502 Command not implemented

214 Help message

220 <domain> Service ready

250 Requested mail action okay, completed

450 Requested mail action not taken: mailbox unavailable (e.g., mailbox busy)

550 Requested action not taken: mailbox unavailable (e.g., mailbox not found, no access, or command rejected for policy reasons)

452 Requested action not taken: insufficient system storage

552 Requested mail action aborted: exceeded storage allocation

SMTP: demo (3)

- Un serveur mal configuré qui retourne un code en 4xy en cas d'utilisateur inexistant
- Conséquence: pas de courrier d'erreur pour l'expéditeur dans que son MTA n'a pas fini d'essayer d'envoyer le courrier

Message: entête et corps

- une ligne vide sépare le corps des entêtes
- une entête logique peut se poursuivre sur plusieurs lignes :
  - les lignes de continuation commencent par un espace (espace, tabulation, ...)
- les entêtes comprennent des entêtes placées par le MUA et des entêtes de traçage placées par le MTA
- Enveloppe: information échangées entre MUA et MTA ou entre MTA, pas dans le message

Entête des messages (rfc 2822)

- Notion d'enveloppe
- Champs de traçage
  - Return-path
  - Received
- Adresses et champs utilisateur
  - From:,Sender,Reply-To:
  - To:, CC:, BCC:
- Champs informationnels souvent optionnels
  - Date, Subject, X-...
  - Message-ID
  - In-Reply-To:, References:

format des adresses (RFC 819)

```
<mailbox> ::= <local-part> "@" <domain>

<local-part> ::= <string> | <quoted-string>

<string> ::= <char> | <char> <string>

<quoted-string> ::=  """ <qtext> """

<qtext> ::=  "\" <x> | "\" <x> <qtext> | <q> | <q>
  <qtext>

<char> ::= <c> | "\" <x>

<a> ::= any one of the 52 alphabetic characters A
  through Z in upper    case and a through z in
  lower case

<c> ::= any one of the 128 ASCII characters except
  <s> or <SP>
```

format des adresses (2)

```
<d> ::= any one of the ten digits 0 through 9

<q> ::= any one of the 128 ASCII characters except
  CR, LF, quote ("),   or backslash (\)

<x> ::= any one of the 128 ASCII characters (no
  exceptions)

<s> ::= "<", ">", "(", ")", "[", "]", "\", ".",
  ",", ";", ":", "@",""", and the control
  characters (ASCII codes 0 through 31 inclusive
  and 127)

Le nom de domaine peut être écrit en majuscules ou
  minuscules mais il n'est pas sensible à la casse
  (ShayoL.org et shayol.org sont le même domaine).

La « local-part » peut être sensible à la casse
  mais c'est déconseillé.
```

format des adresses (3): exemples

- Exemples corrects:
  - pascal.petit@shayol.org
  - pascal.petit@ShaYol.org
  - Pascal.Petit@shayol.org
  - petit+adieve@shayol.org
  - "Pascal Petit"@foo.fr
  - Pascal\,Petit@shayol.org
  - petit@[81.56.171.187]
- Exemples incorrects:
  - Pascal Petit@foo.fr
  - petit@toto$.fr
  - Cécile@toto.fr

SMTP: DEMO

- On prend les courriers envoyés dans la première demo.
- On met en évidence les champs de traçage (Received) et les informations récupérées de l'enveloppe (Return-path)
- On commente les autres champs et notamment le fait que le champ From n'a rien à voir avec MAIL FROM:, et le champ To: avec le RCPT TO:

MIME (RFC2045 à 2049)

- Multipurpose Internet Mail Extension
- permet de transporter des données de types variés dans des courriels
- Principe:
  - l'entête contient une description du type de données
  - les champs d'entête peuvent utiliser un codage indépendant de cette description (car rien ne garantit qu'elle sera lue avant)

MIME champs d'entête

- MIME-Version: numéro de version (2.0)
- Content-Type: indique le type d'informations sous la forme : *type/subalterne; attribut=chaîne [; attribut=chaîne]*
- Exemples de types:
  - text/plain; text/html; text/enriched
  - image
  - multipart: le courrier composé de plusieurs partie avec son champ Content-Type et, éventuellement, Content-Transfert-encoding. ex: multipart/alternative.
  - application/pdf; application/postscript;

MIME: champ d'entête (2)

- les données sont codées (image, texte avec des caractères accentués, ...) pour palier les limitations des passerelles
- champ Content-Transfert-Encoding: précise le codage utilisé (rfc 2045):
  - 7bit
  - 8bit
  - binary (site supportant 8BITMIME)
  - quoted-printable
  - base64

MIME

- codage des entêtes
- RFC 1524: problème posé par MIME aux MUA
- RFC3030: répartition des attachements sur plusieurs courriers

MIME: demo

- on analyse les entêtes de divers courriers contenant des attachements, en multipart/alternative, ...

Accusé de réception

- par défaut: accusé de non réception (temporaire, définitif)
- accusés de réceptions supportés par les MUA : impose que le MUA du destinataire le supporte
- DSN (RFC 3461), type MIME correspondant (RFC 3462), format (RFC3464)

Configuration de base d'un MTA: postfix

- Les questions auxquelles répondre :
  - domaine indiqué sur les courriers sortant
  - domaines gérés par le MTA (les courriers adressés à ces domaines sont gérés localement)
  - pour quels clients accepte-t-on de relayer le courrier ?
  - de quelles destinations relayer le courrier ?
  - méthode de livraison du courrier: directe ou indirecte ?

Domaines gérés par le MTA: courrier entrant

- paramètre *mydestination* de postfix
- mydestination=$myhostname localhost.$mydomain exemple1.com exemple2.com
- liste des domaines dont le courrier reçu sera délivré dans les boîtes aux lettres locales
- toto@exemple1.com et toto@exemple2.com auront la même boîte aux lettres

Domaines virtuels

- voir http://x.guimard.free.fr/postfix/index.php?page=V (VIRTUAL README)

de quels clients relayer le courrier ?

- paramètres *mynetwork* et m*ynetworkstyle* (ignoré si mynetwork est défini)
- mynetwork=127.0.0.0/8 192.168.196.0/24 81.56.171.187/32
- mynetworkstyle=host|subnet|class : autorise les machines: machine locale, machine du même sous-réseau, machine de la même classe réseau
- mynetwork= liste de réseaux dont les machines seront autorisées

De quelles destinations relayer le courrier

- paramètre *relay_domains* de postfix
- par défaut: mydestination
- sert pour définir les domaines dont on est MX de secours

Méthode de livraison du courrier: directe ou indirecte

- paramètre *relayhost* de postfix
- indique la machine à laquelle envoyer le courrier sortant
- s'il est vide, le serveur de courrier gère lui-même l'envoi à la destination (détermination des MX puis envoi à l'un des MX)

Bibliographie

- Unix Administration, Jean-Michel Moreno, Dunod
- BSD, Emmanuel Dreyfus, Eyrolles
- TCP/IP Administration de réseau, Craig hunt, O'Reilly
- Documentation de postfix en vf: http://x.guimard.free.fr/postfix/