Active Directory: plan

- Présentation générale
- Gestion des utilisateurs dans un domaine
- Planification des groupes
- Délégation de tâches, console mmc

Active Directory

- Gère un domaine windows
- Service d'annuaire
- Base d'annuaire distribuée des ressources réseau : comptes utilisateurs, groupes, ordinateurs, imprimantes, dossiers partagés, ...
- Administration centralisée
- Tolérance de panne
- Protocoles standard => interopérabilité (clients)
- Produit propriétaire => pas de serveur AD non microsoft

Active Directory

- Gère un domaine windows
- Service d'annuaire
- Base d'annuaire distribuée des ressources réseau : comptes utilisateurs, groupes, ordinateurs, imprimantes, dossiers partagés, ...
- Administration centralisée
- Tolérance de panne
- Protocoles standard => interopérabilité (clients)
- Produit propriétaire => pas de serveur AD non microsoft

Structure logique

- Nom de domaine AD => nom de doma ine DNS
- Domaines
- Arborescences: domaines de noms hiérarchiquement liés
- Forêts: ensemble d'arborescences
- Unités d'organisation : organisation logique à l'intérieur d'un domaine

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

AD-DEMO: installation d'Active Directory

- Installation d'Active Directory sur une machine virtuelle windows 2000 server :
  - Domaine suzdal.shayol.org
  - Pas de dns présent => à installer
  - Premier domaine de l'entreprise (nouveau domaine dans une nouvelle arborescence dans une nouvelle forêt)
  - Pas de contrôleur NT => Mode natif

Les objets Active Directory

- Instances d'une classe définie dans le Schéma :
  - Comptes utilisateurs,
  - ordinateurs,
  - imprimantes,
  - groupes,
  - dossiers partagés publiés
- Objets conteneur, objet feuille

Nom des objets

CN= « Pascal PP Petit », OU=test, DC=shayol, DC=org

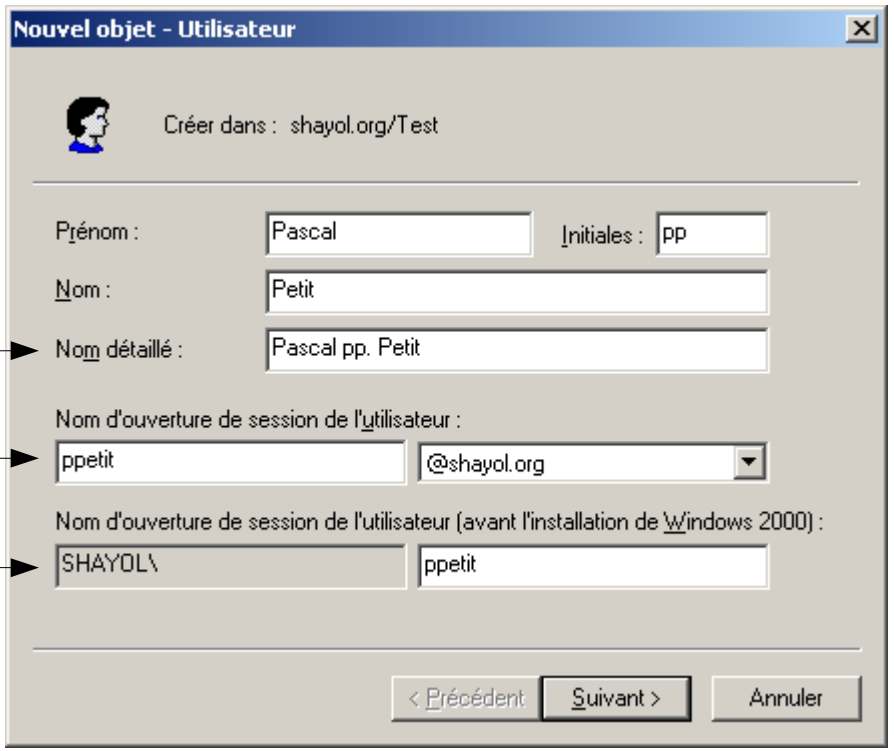
- Nom unique
- Nom unique relatif
- Identificateur global (GUID)
- Format des noms active directory
- Nom principal d'utilisateur
- Identifiant de sécurité :SID = RID + ID domaine

Nom des objets (2)

Nom unique relatif (RDN)

Nom principal d'utilisateur

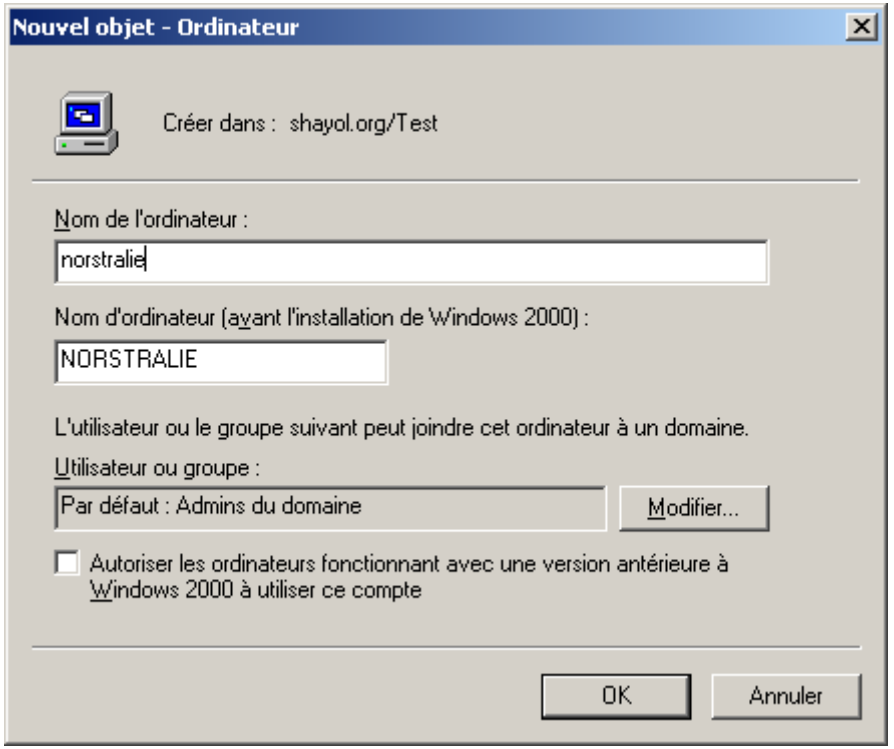
Nom SAM



Compte d'ordinateur

- Nécessaire pour ordinateur WinNT ou W2K
- Création depuis l'ordinateur lors de l'inclusion dans le domaine

- Création à l'avance
  - Création du compte dans AD à l'avance
  - Inclusion de l'ordinateur par un utilisateur déclaré à la création du compte



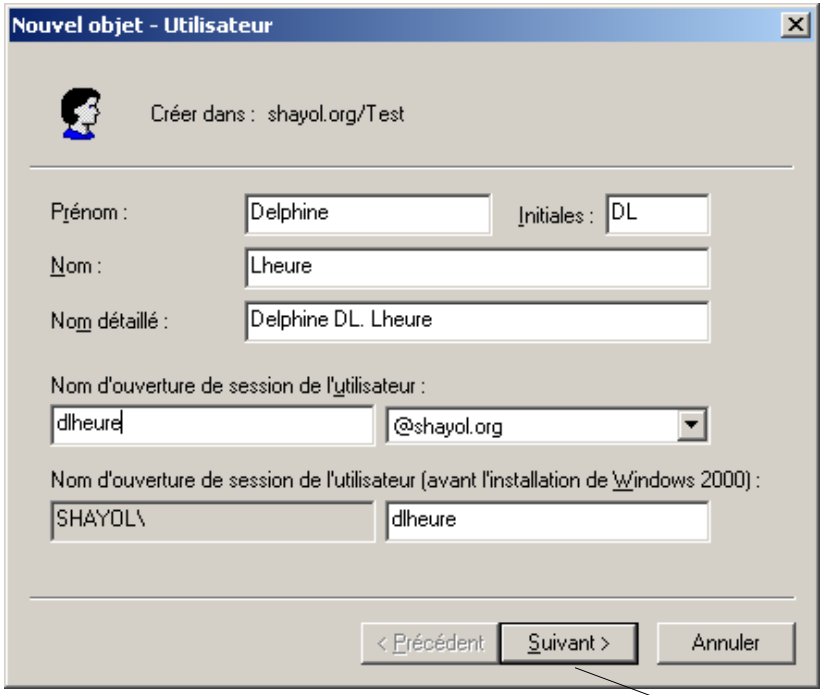
Compte utilisateur

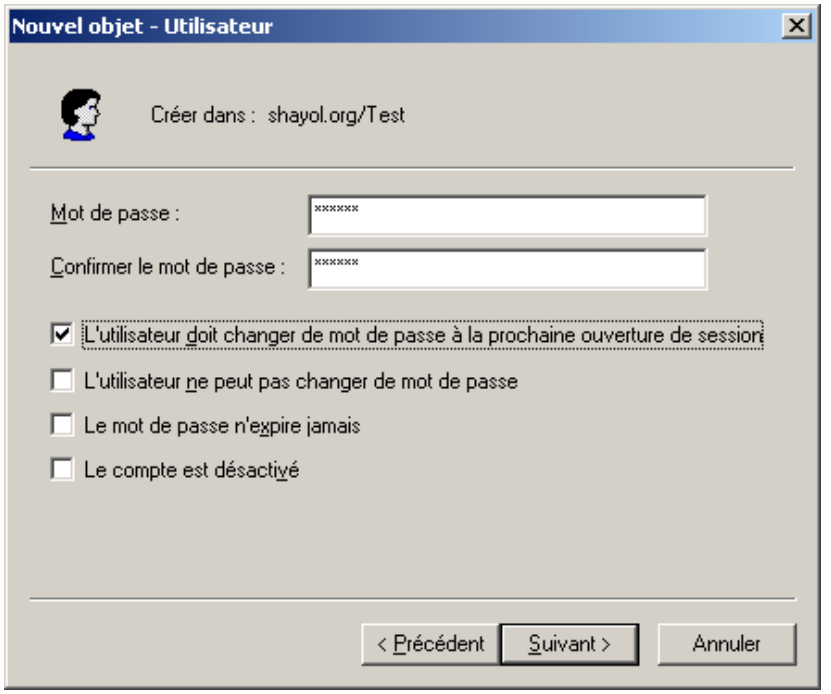
- Compte d'utilisateur local :
  - Stocké dans la base SAM de l'ordinateur
  - Donne accès aux ressources locales
  - Permet l'ouverture de session sur l'ordinateur
- Compte d'utilisateur du domaine :
  - Stocké au niveau du domaine dans Active Directory
  - Donne accès aux ressources réseau
  - Permet d'ouvrir des sessions sur les ordinateurs du domaine

Comptes prédéfinis dans un domaine

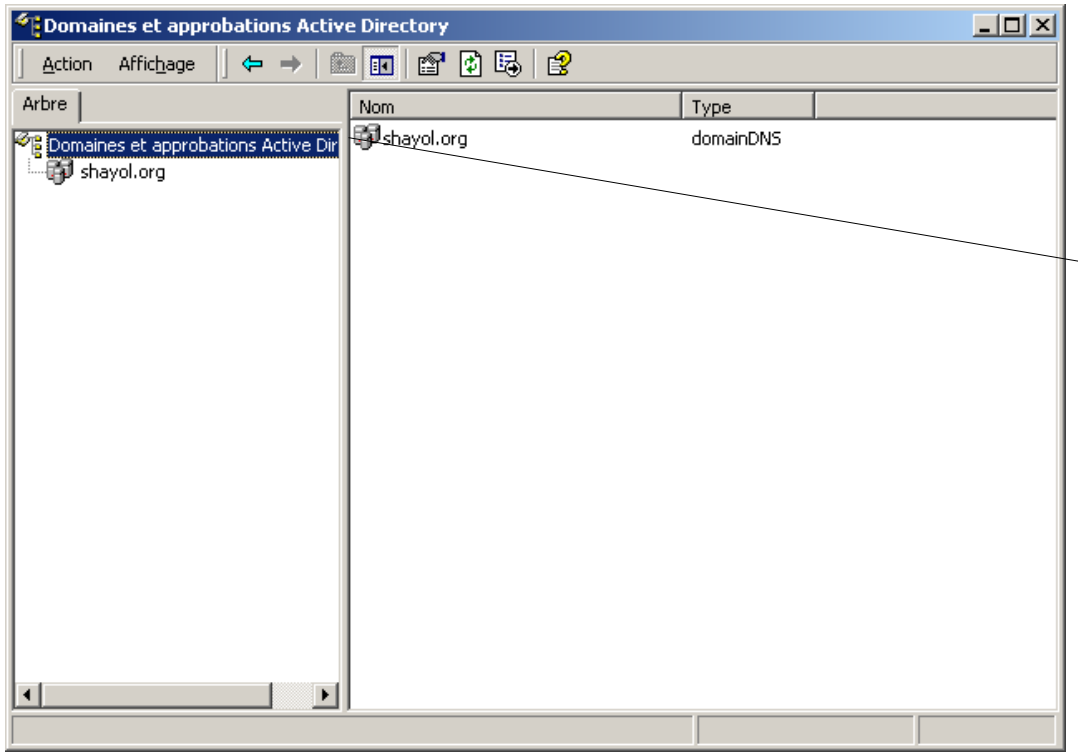
- Computers
- Users
- Comptes:
  - Administrateur
  - Invité
  - IUSR_NomOrdinateur et IWAM_NomOrdinateur

Création des comptes sur un domaine

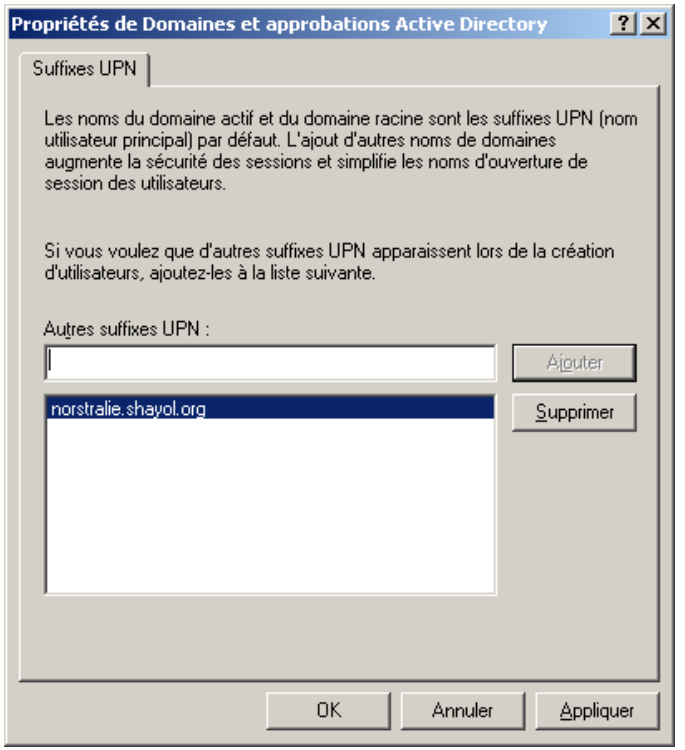




Création d'un suffixe UPN



Propriétés



Propriétés des comptes d'utilisateurs

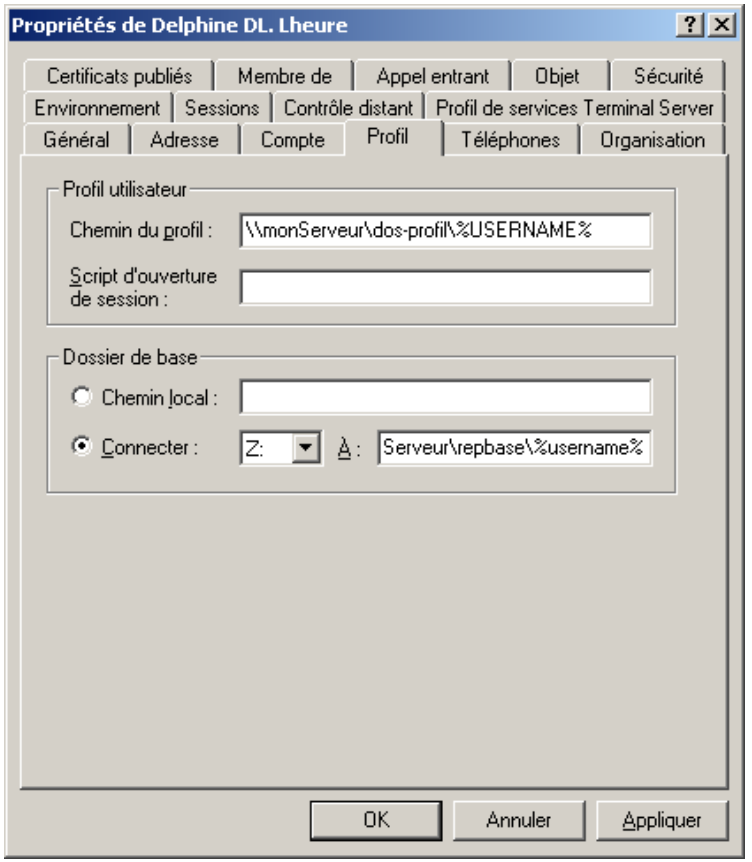
- Options de mot de passe
- Délégation: interdire la délégation, autoriser la délégation des tâches à d'autres utilisateurs
- Chiffrement de mot de passe: réversible, pas de pré authentification kherberos, chiffrement DES
- Expiration de compte
- Restrictions horaires
- Restriction d'accès (se connecter à)

AD-DEMO

- Intégration de deux stations de travail dans le domaine
- Création de compes utilisateur sur le domaine,L'utilisateur travaille sur sa station de travail (pas de répertoire de base réseau, pas de profil itinérant)
- Deux stations de travail : tout ce qui est fait sur l'une n'est pas automatiquement accessible depuis l'autre.
- Ouverture de session en utilisant le nom principal d'utilisateur

Profils utilisateurs, répertoire de base

- Profils locaux
- Profils itinérants
- Profils itinérant obligatoire
- Répertoire de base



AD-DEMO: profil itinérant

- Mettre le répertoire de base sur le serveur et constater qu'il est accessible depuis les deux stations mais que le profil reste propre à chaque station (fond d'écran par ex.)
- Définir un profil itinérant et constater que le profil est bien le même sur les deux stations et que les changements sont pris en compte sur les deux stations

Création de masse

- Par copie d'un compte désactivé
- Via addusers, csvde, ldifde
- Net account
- Net users
- Net group
- Net localgroup

Gestion des comptes

- Réinitialiation du mot de passe
- Désactivation
- Suppression
- déverouillage
- déplacement

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.

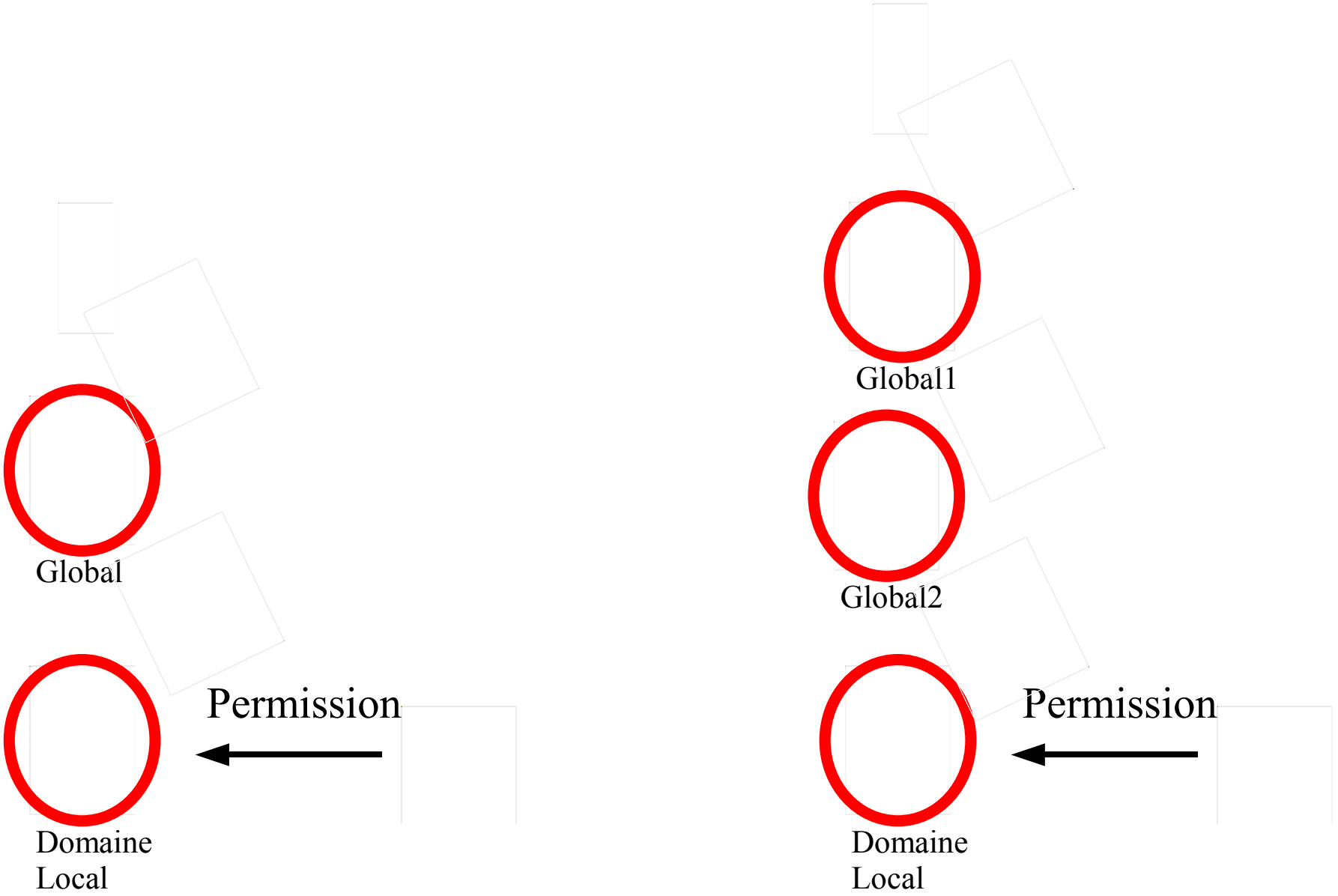
Groupes globaux

- 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.

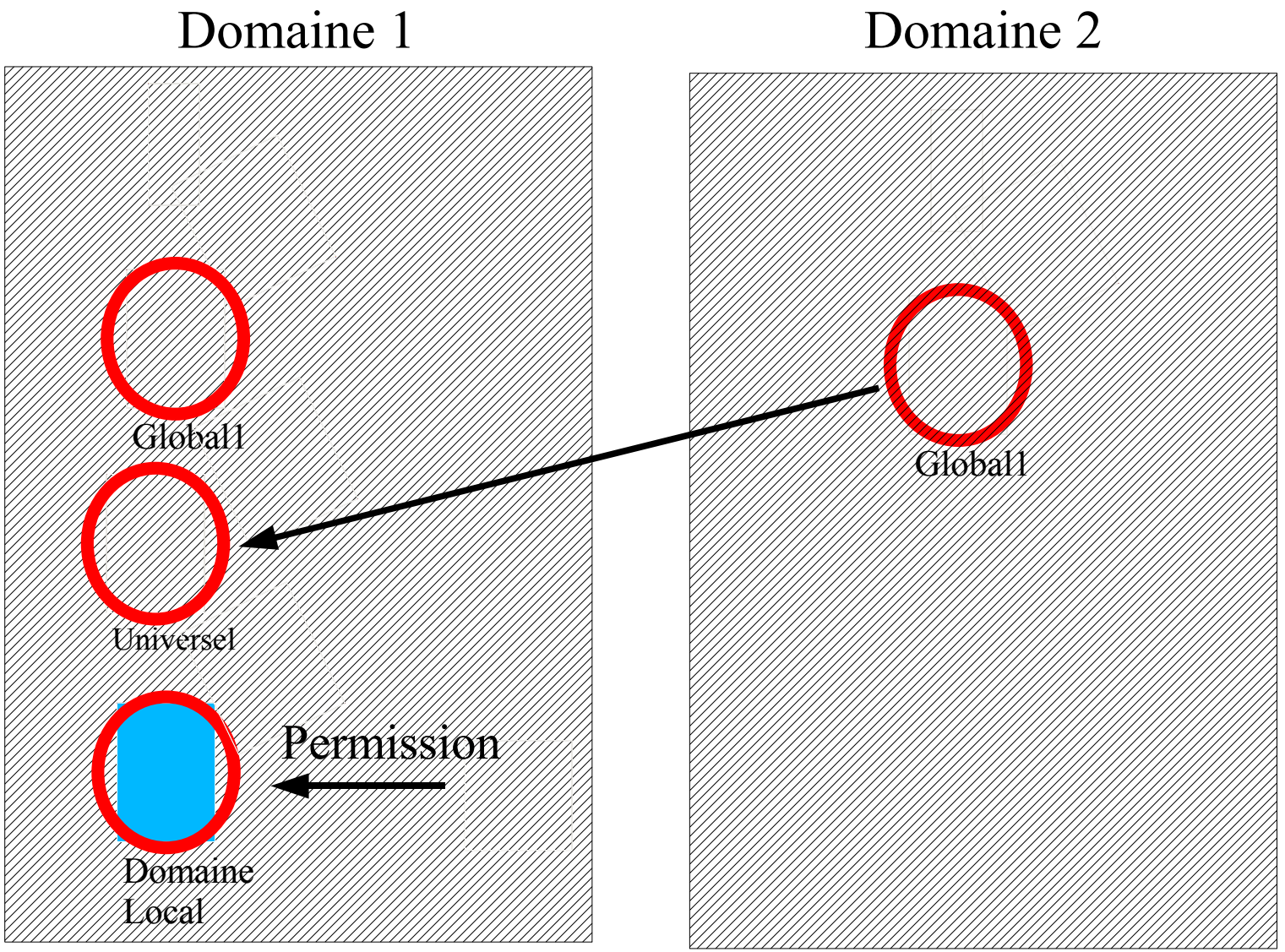
Groupes universels

- 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

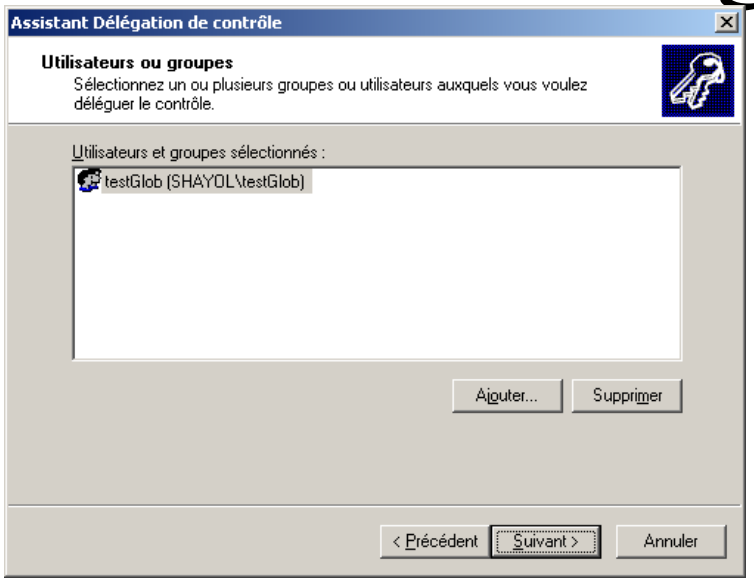
- Création d'un groupe Gtest sur le domaine (groupe local de domaine)
- Ajout de l'utilisateur test1 à Gtest
- Sur une station de travail, créer un dossier RepTest et donner le droit CT à Gtest et lecture au groupe « Tout le monde » sur RepTest
- Vérifier les accès
- Utiliser Gtest pour sélectionner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

Délégation de tâche

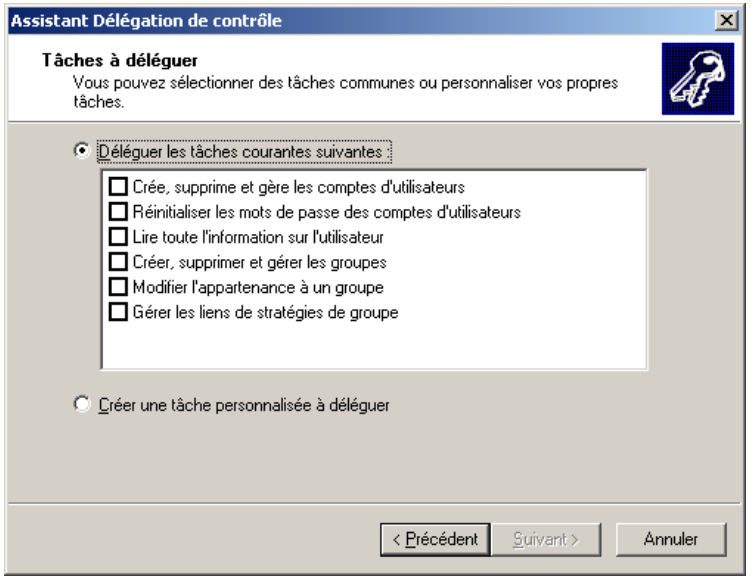
- Délégation de contrôle sur le domaine ou sur une unité d'organisation : déléguer une partie des tâches d'administration sur certains objets à certaines personnes
- Création de console MMC personnalisées,
- Administration à distance

Délégation de contrôle

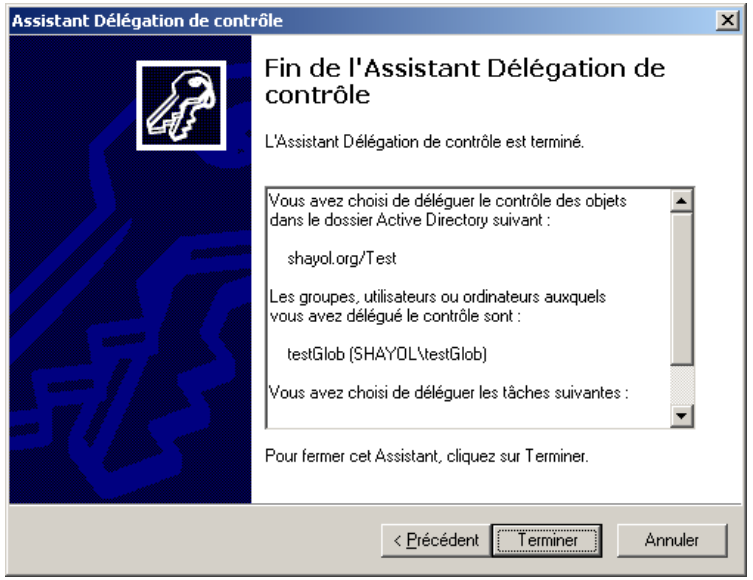
1 choix des groupes



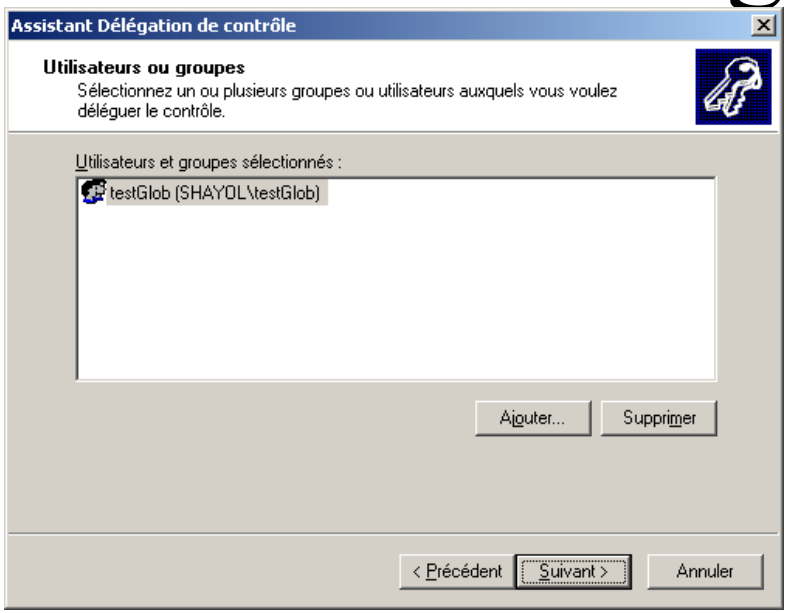
2 choix des tâches



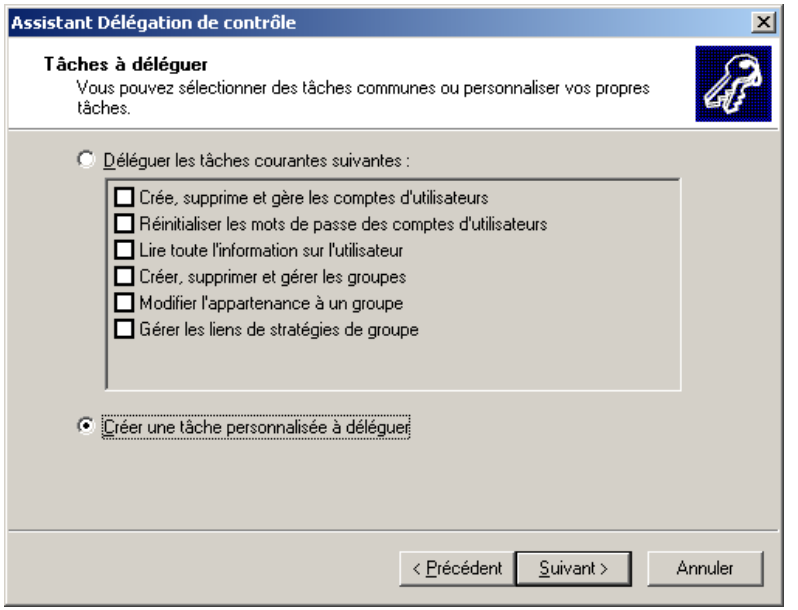
3 récapitulatif



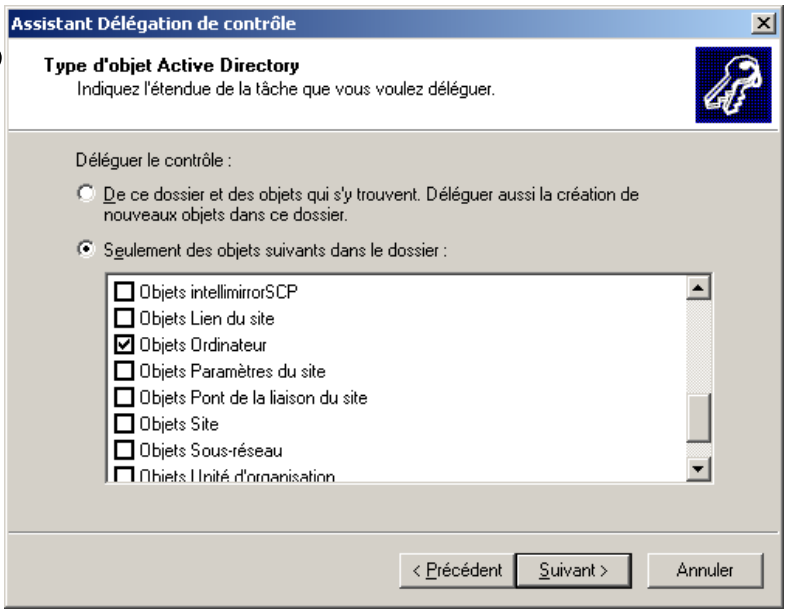
Délégation de contrôle



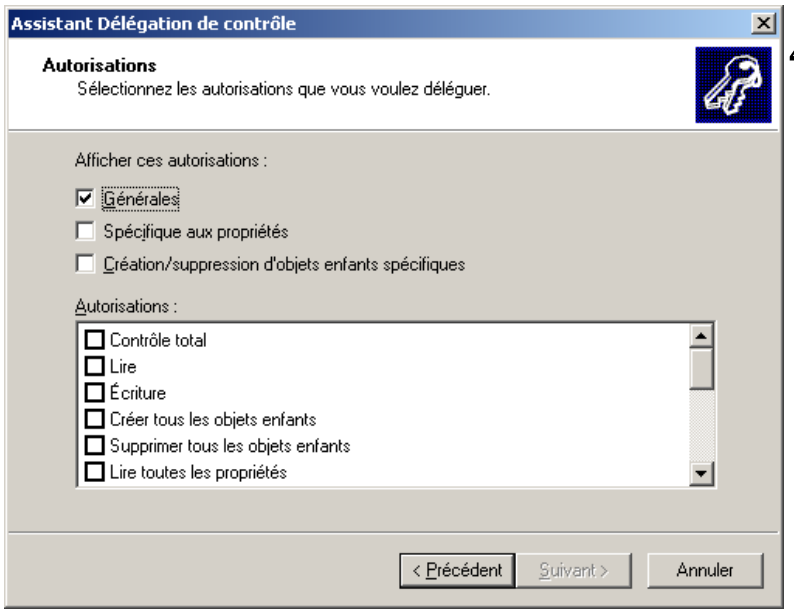
1 → 2



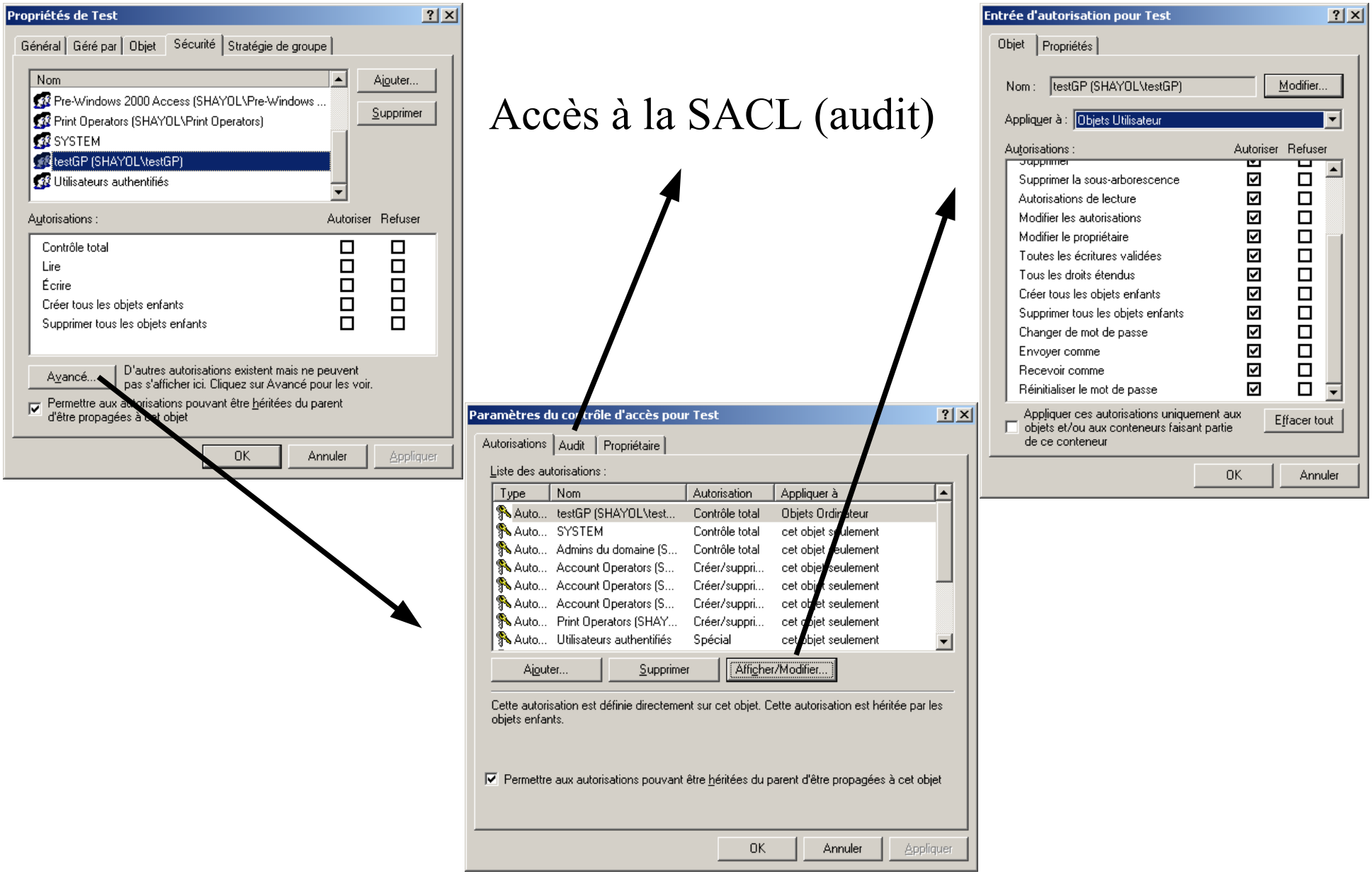
2 → 3



3 → 4



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.