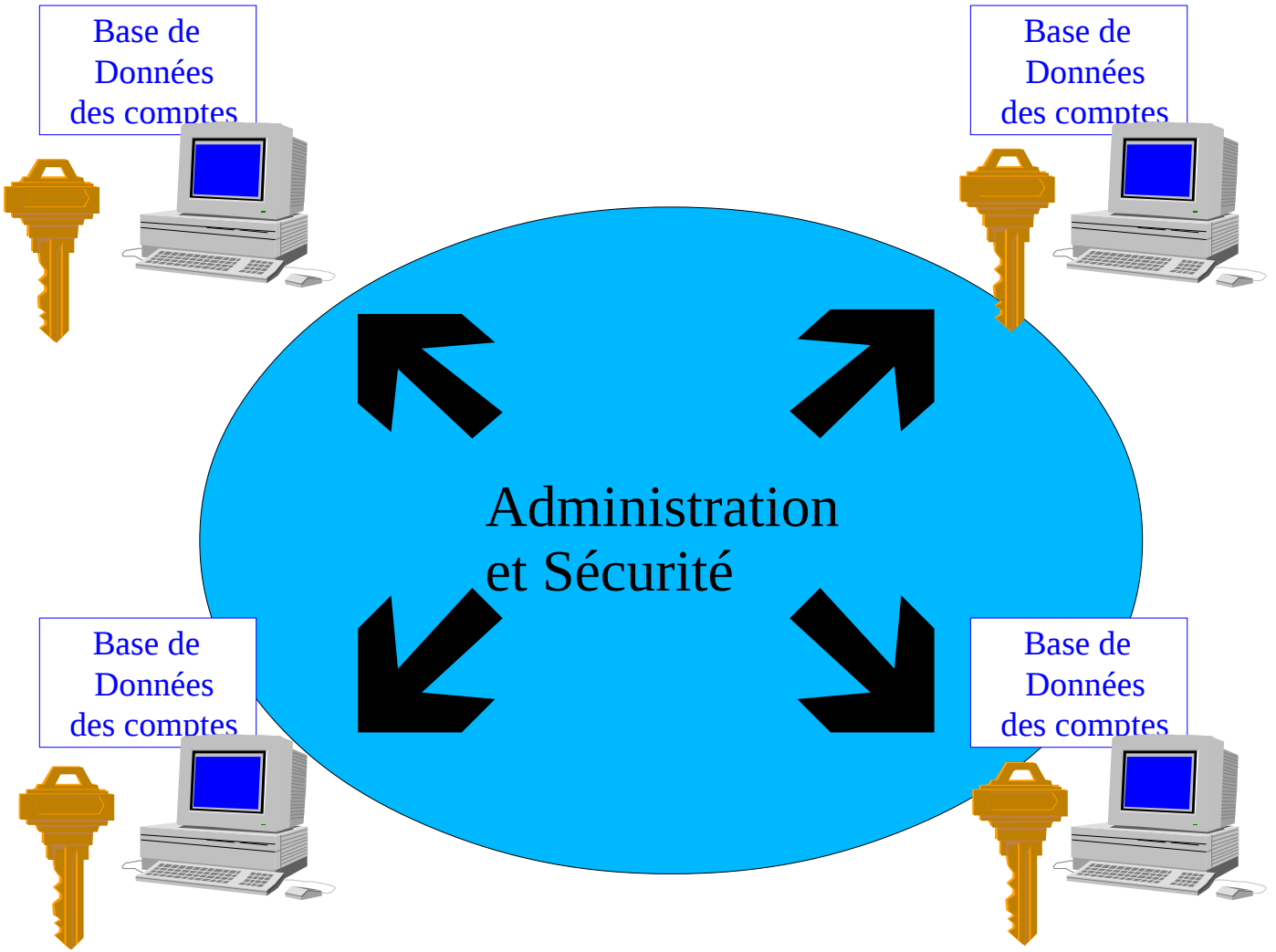
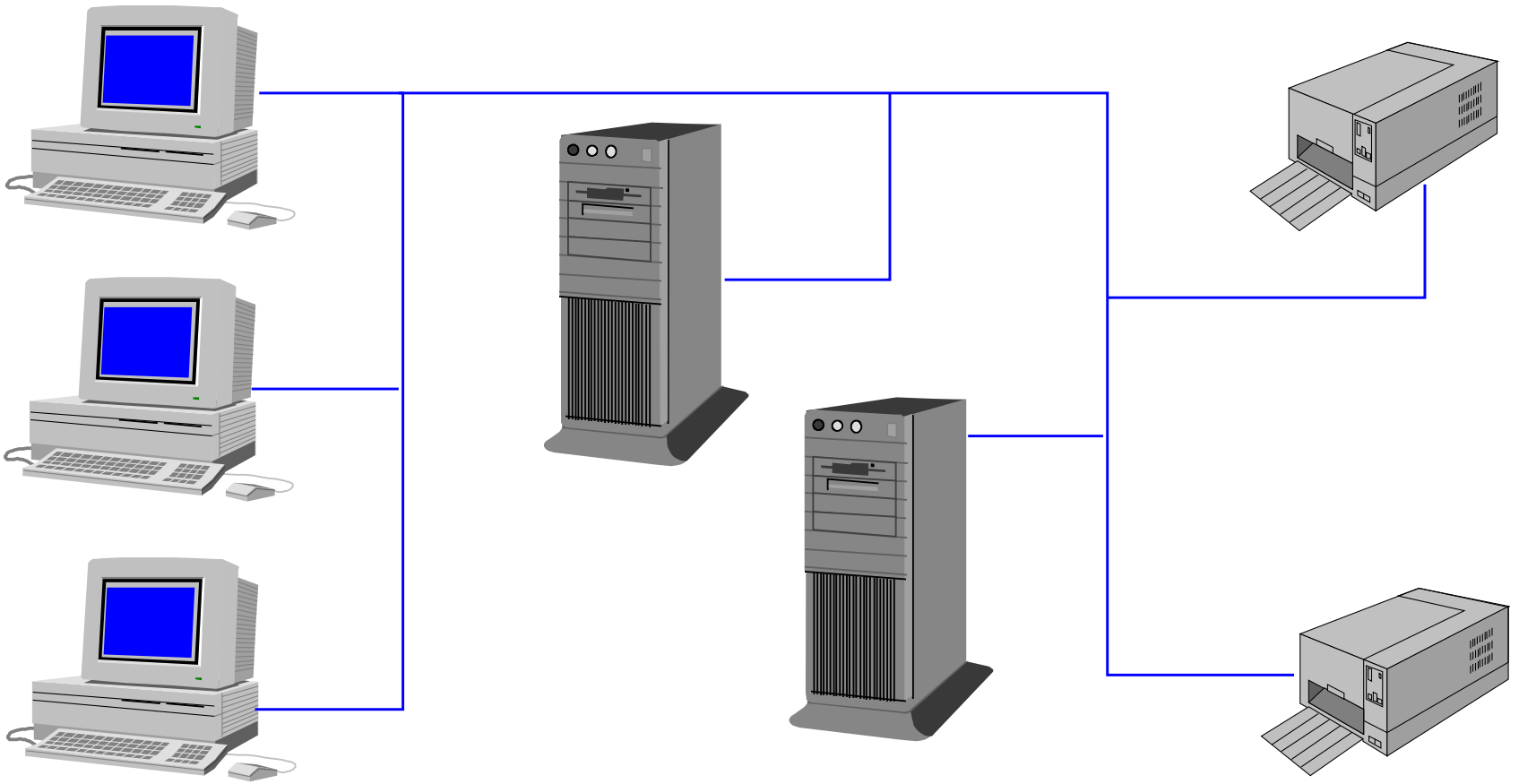
# Modèle groupe de travail



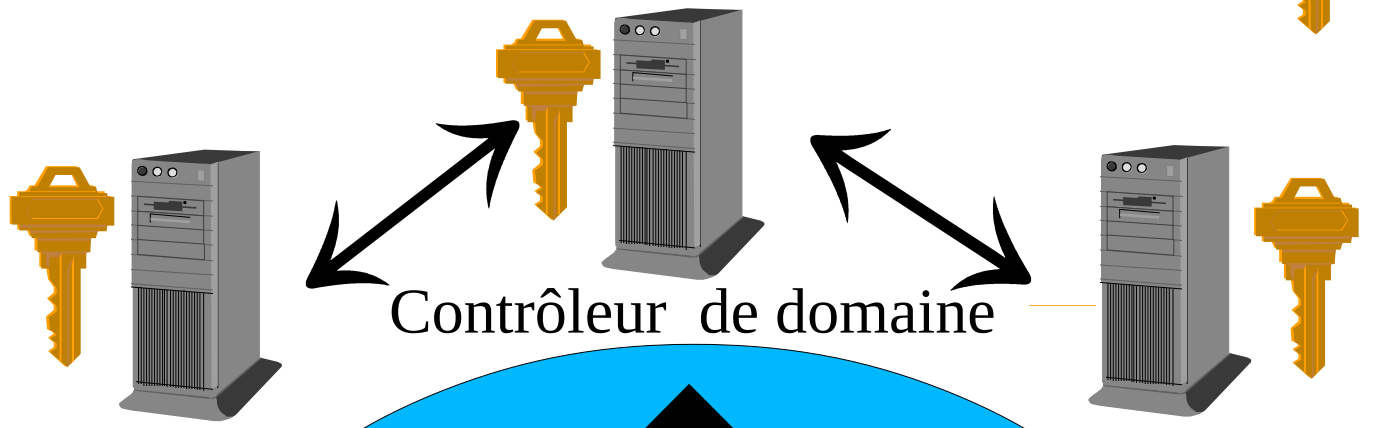
# Les Domaines

**Un seul compte + un seul mot de passe**
**= accès à de nombreux serveurs**



# Modèle domaine

Base de Données de Comptes répliquée sur les contrôleurs

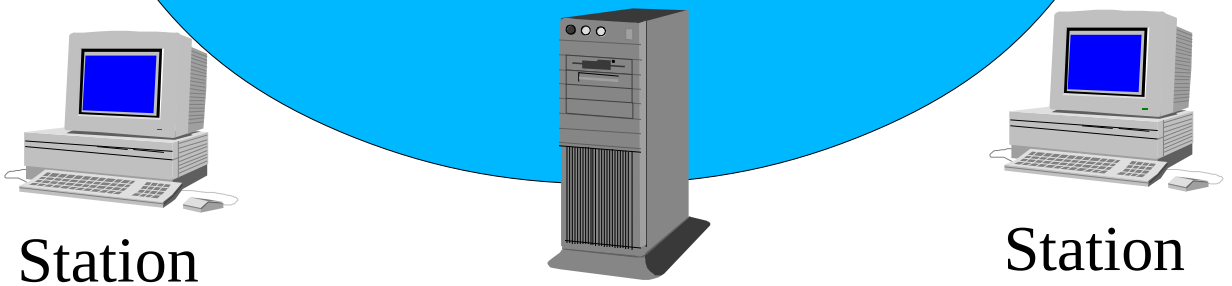


Contrôleur de domaine

Contrôleur de domaine

Contrôleur de domaine

Administration et Sécurité



Station

Serveur membre

Station

# Domaine/Groupe de travail

- L'intégration à un domaine suppose :
  - Un nom de domaine
  - Un compte d'ordinateur dans le domaine
  - Un contrôleur de domaine et un serveur DNS disponibles.
- L'intégration dans un groupe de travail suppose :
  - Un nom de groupe de travail (existant ou nouveau)

# Utilisateurs et groupes sous windows : Démonstration

- Sur une station de travail windows Xp pro
- Deux outils pour gérer les utilisateurs (préférer la console de gestion)
- Création d'utilisateurs (mot de passe mis par l'admin mais l'utilisateur doit le changer à la première ouverture de session)
- Ajout dans le groupe administrateurs

# Modèle de contrôle d'accès W2K+

- Autorisations basées sur l'utilisateur
- Accès discrétionnaire aux objets sécurisables
- Héritage des permissions
- Privilèges administratifs
- Audit des événements du système.

# Limiter les accès

- Principal de sécurité : utilisateur, groupe, ordinateur ou service :
  - Ont des comptes
  - Sont identifiés par Identifiant de sécurité (SID) créé lors de la création du compte
  - Jeton d’accès :
    - Créé lors de l’ouverture de session ou de la connexion d’un principal
    - Fournit un contexte de sécurité
    - Jeton créé à l'ouverture de session : les modifications sur les groupes d'utilisateurs ne seront pris en compte qu'à la prochaine ouverture de session.

# Sujet

- Sujet : processus s’exécutant dans le contexte de sécurité d’un principal authentifié
- Prise d’identité: possibilité pour un processus de s’exécuter dans un contexte de sécurité différent de celui de son processus père. Utile pour les pour les applications client/serveur.

# Objets

- Objets sécurisables,  informations de sécurité (Permissions)
- Listes de contrôle d’accès (ACL)
  - DACl: liste de contrôle d'accès discrétionnaire: permissions
  - SACL: liste de contrôle d'accès Système  (Audit)

# Contrôle d’accès

- Principe de base :

**Les sujets agissent sur les objets**

- Comparaison du jeton d’accès du principal associé au sujet et du descripteur de sécurité de l’objet.

# Héritage

- Conteneur, parents, enfants
- Héritage des permissions

# Droits

- Droit du propriétaire
- Propriétaire initial
- Changement de propriétaire
- Permissions
- Droits utilisateurs
  - Droits de procédure de connexion
  - Privilèges

# NTFS: permissions sur les dossiers et sur les fichiers

- Uniquement dans les partitions NTFS
- Liste de contrôle d'accès (ACL) contenant des entrées (ACE)
- ACE: un couple (utilisateur ou groupe, permission ou interdiction)
- Modification des ACL par :
  - le propriétaire de l'objet;
  - les utilisateurs ayant Contrôle Total sur l'objet.

# Permissions sur le fichiers et dossiers: démonstration (1)

- Sur une station windows Xp pro
- Création d'un dossier et visualisation des ACL par défaut
- Notion d'ACE
- autorisation/refus

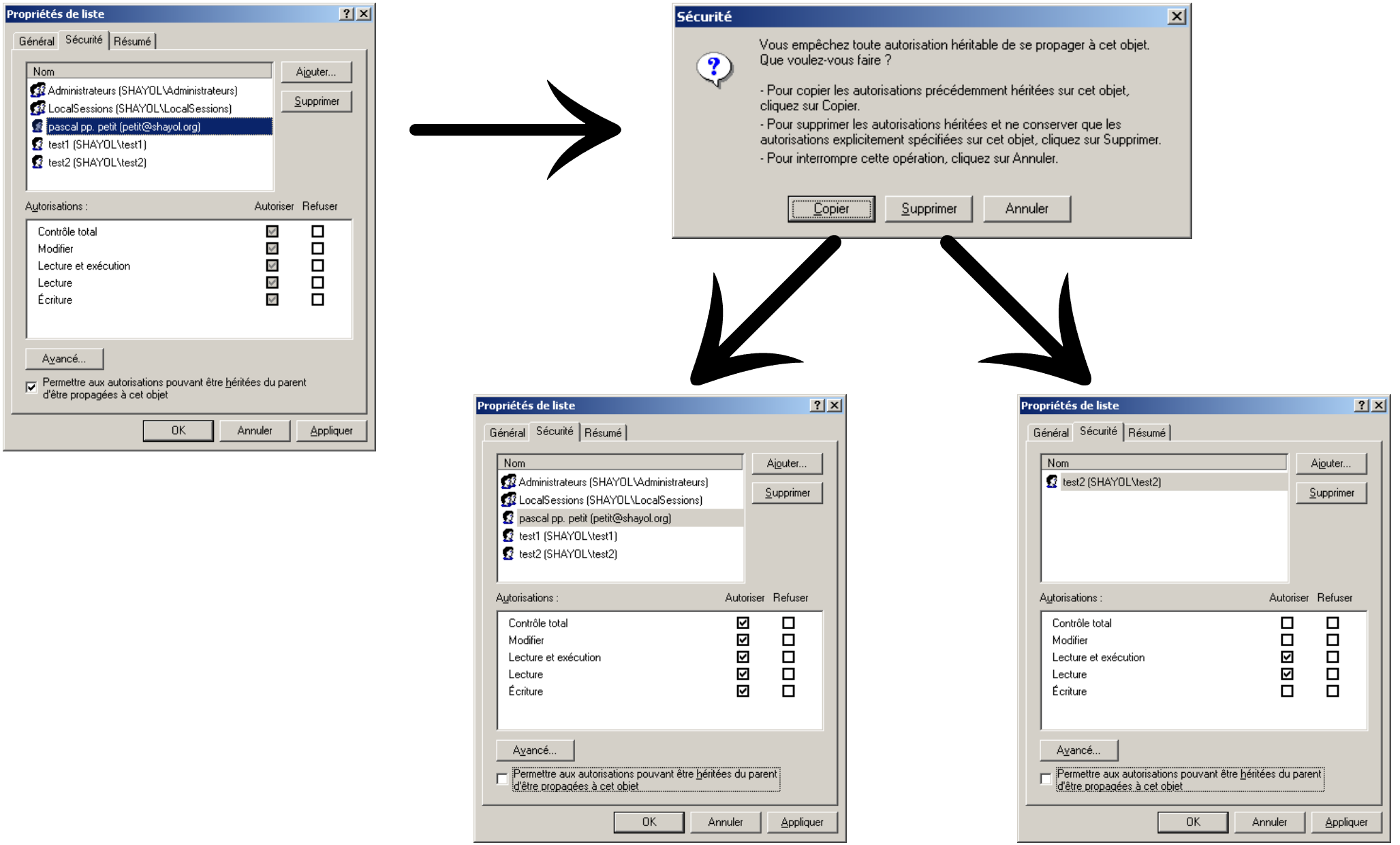
# Permissions par défaut

- Au formatage NTFS: CT à « tout le monde »
- A la création d'un fichier ou d'un dossier: hérité des permissions de son dossier père
- Ajout d'une ACE à l'ACL d'un dossier ou d'un fichier: droit « lecture et exécution » par défaut

# Héritage des permissions

- Par défaut, les permissions d'un dossier s'appliquent aux sous dossiers et aux fichiers qu'il contient
- 3 valeurs possibles pour les cases à cocher d'une ACE: non coché, coché grisé (hérité) , coché
- Il est possible de refuser l'héritage des ACL du père

# Suppression de l'héritage

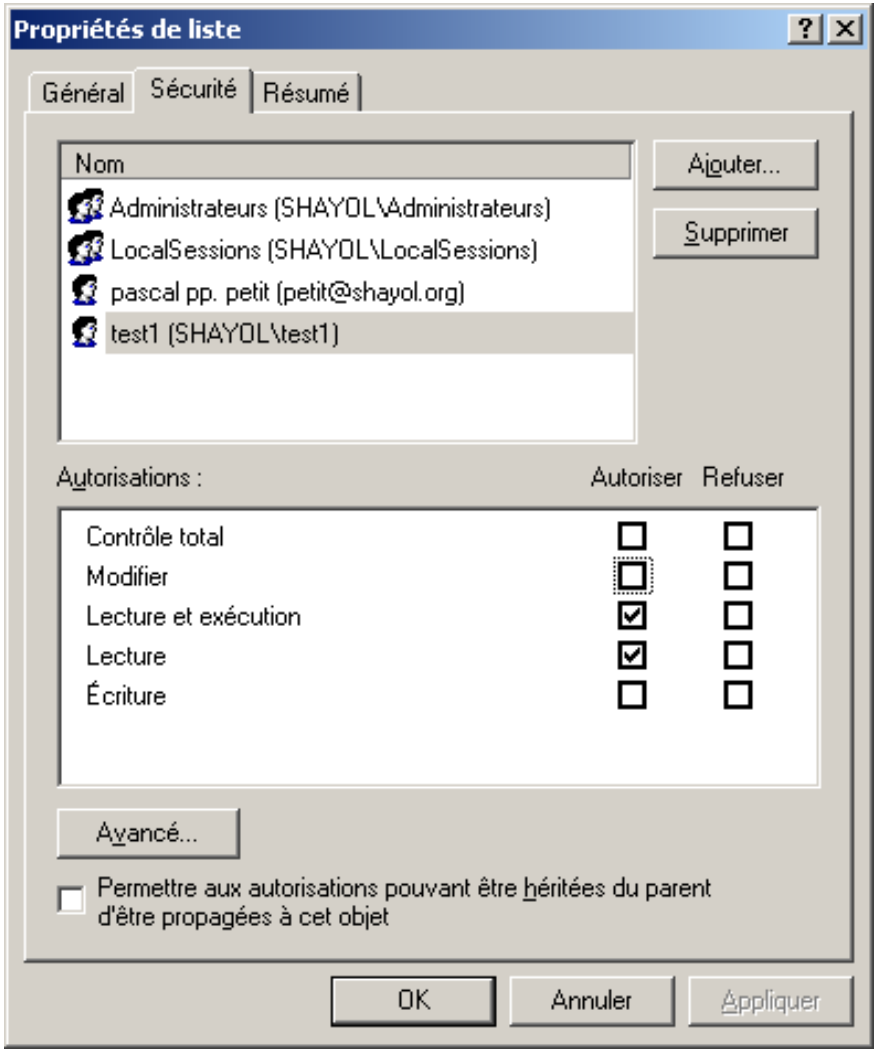


# Permissions sur le fichiers et dossiers: démonstration (2)

- Sur une station windows 2000 pro
- On reprend le dossier précédent que l'on complète éventuellement avec d'autres sous dossiers
- Suppression de l'héritage
- Création de 3 utilisateurs test1, test2 et test3, d'un groupe Gtest auquel test1 appartient
- Variations sur l'aspect cumulatif des permissions
- Droit du propriétaire, appropriation
- Particularité de l'administrateur

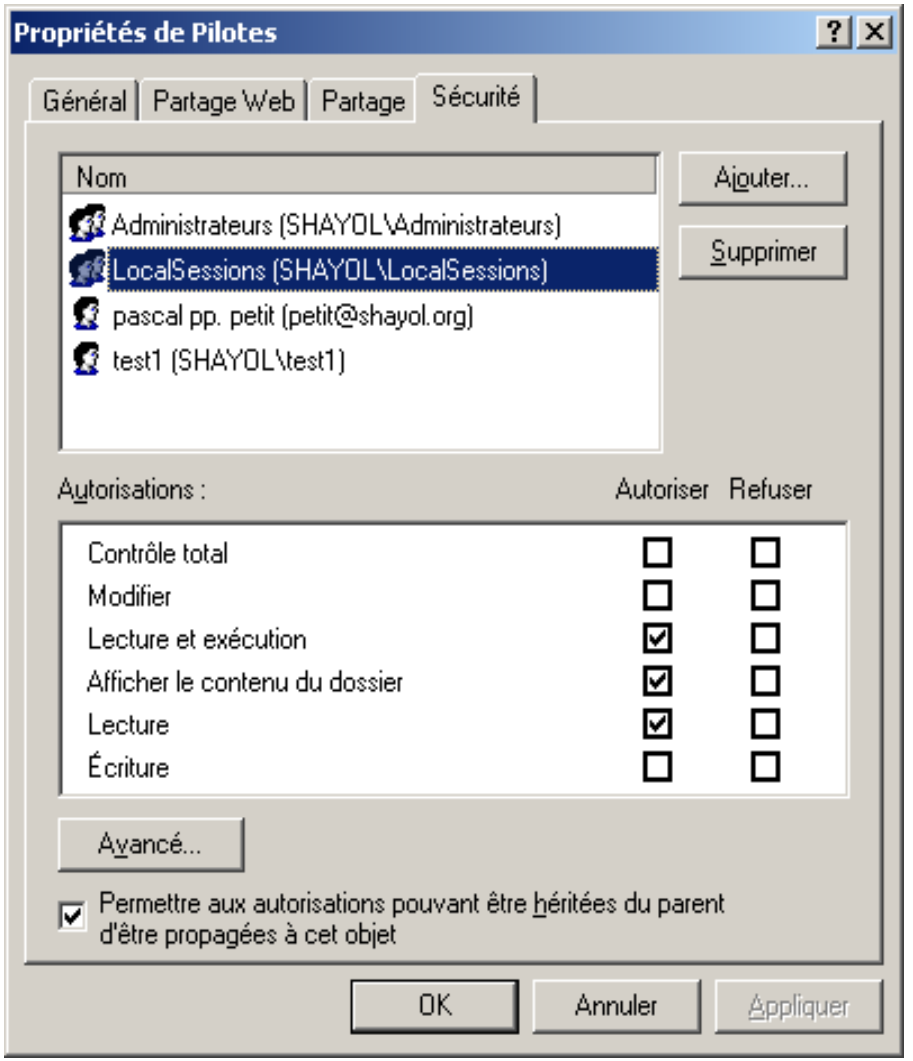
# Permissions sur les fichiers

- Modifier
- Lecture et exécution
- Lecture
- Écriture
- CT



# Permissions sur les dossiers

- Modifier
- Lecture et exécution
- Afficher le contenu
- Lecture
- Écriture
- CT



# Mode de fonctionnement des permissions

- Les permissions sont cumulatives
- Les interdictions ont priorité sur les permissions
- Les permissions sur les fichiers l'emportent sur les permissions sur les répertoires
- Pas de permission = pas d'accès

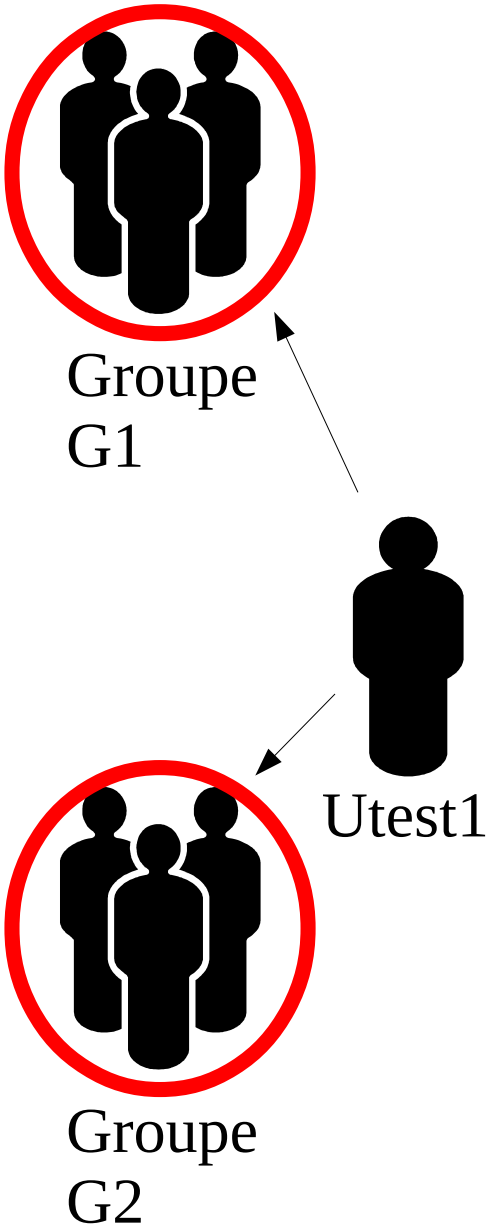
# Algorithme déterminant l'accès à un objet

- S'il y a une interdiction pour l'utilisateur ou l'un des groupes auquel il appartient: Accès refusé
- S'il y a une autorisation pour l'utilisateur ou l'un des groupes auquel il appartient: accès autorisé
- Sinon l'accès est refusé

# Permissions sur le fichiers et dossiers: démonstration (3)

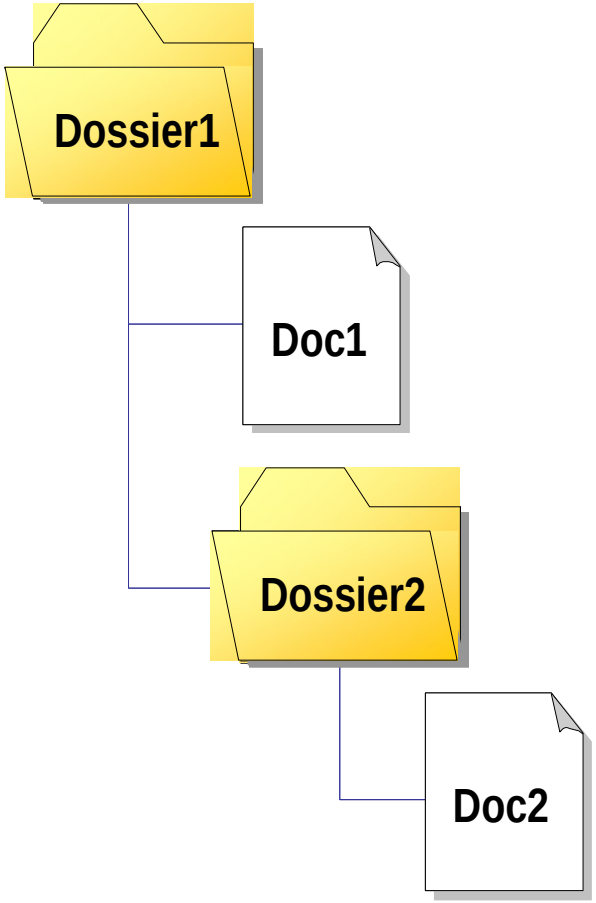
- Suite de la démonstration précédente
- On illustre la priorité des refus
- Exemple classique: refus pour tout le monde, CT pour test1 => refus pour test1

# Exemple




Utest 1 appartient à G1 et à G2.
Dans chacun des 2 cas, indiquez les permissions de Utest1 sur chaque

1. G1 a droit de lecture sur dossier 1;
   G2 a droit d'écriture sur dossier 1.
2. G1 a droit de lecture sur dossier 1;
   G2 a droit de lecture sur dossier 2
3. G1 a droit de CT sur dossier 1;
   Doc 2 doit être accessible en lecture seule à Utest1.
   Comment faire ?



# Conseils méthodologiques

- Donner des permissions à des groupes plutôt qu'à des utilisateurs
- Placer les permissions sur les répertoires plutôt que sur les fichiers
- Utiliser l'héritage pour simplifier la gestion des permissions
- Eviter d'utiliser les interdictions
- Lors de la suppression de l'héritage, utilisez « Copier » plutôt que « Supprimer ».

# Permissions et copie de fichiers

- Un fichier ou un dossier copié a les permissions du répertoire de destination
- FAT 16/32: pas de permissions sur la copie
- Pour préserver les permissions lors de la copie: robocopy (kit de ressources techniques)
- La copie appartient à l'utilisateur qui a réalisé la copie
- Pour réaliser la copie: lecture sur la source, écriture sur le dossier destination.

# Permissions et déplacement de fichier

- Déplacement **sur la même partition**: permissions d'origine conservées
- Déplacement **vers une autre partition**: permissions du répertoire de destination
- Pour réaliser le déplacement: modification sur la source et écriture sur le dossier destination.

# Outils en ligne de commande

- En cours de rédaction
- Cacls
- Robocopy (reskit, remplace scopy)

# Partages: Présentations

- W2K+ ne partage que des dossiers (pas des fichiers individuels)
- Un partage est identifié par un nom de partage (pas forcément identique au nom du dossier)
- Un dossier peut avoir plusieurs partages
- Partage caché: le nom finit par $
- Partage de dossiers NTFS ou FAT 16/32

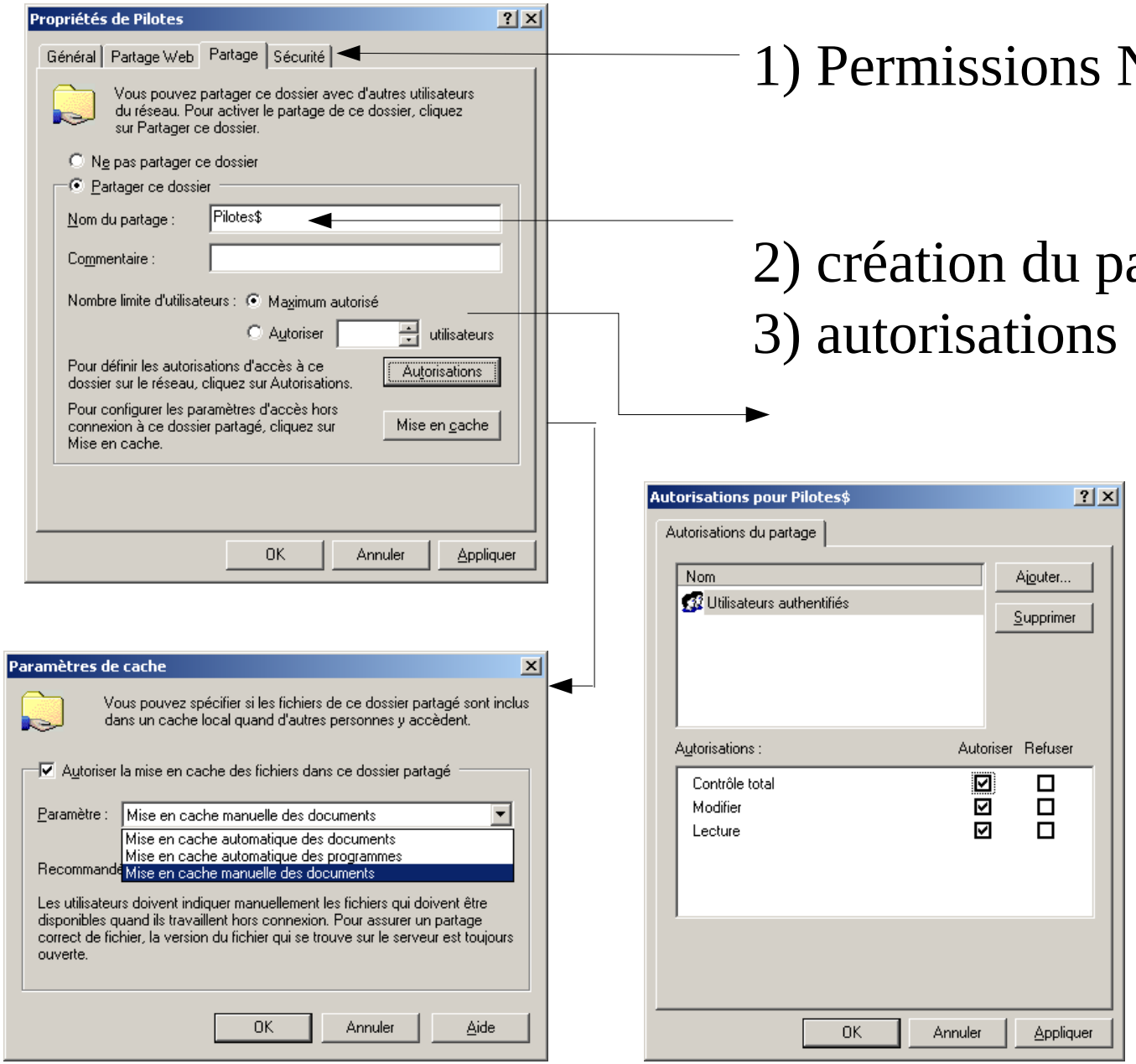
# Partages: notation UNC

- Notation unc (Universal Naming Convention): **\\serveur\partage**\chemin\fichier
- Net use z:\\serveur\partage :  associe un partage à une unité:
- Net use z: /d : annule
- Net view : liste des ordinateurs du domaine
- Net view \\serveur : liste des partages publics du serveur

# Dossiers partagés: création

- À distance avec la MMC « gestion de l'ordinateur »
- Windows 2000 Professionnel
  - Administrateurs
  - utilisateurs avec pouvoir
- Windows 2000 Server:
  - idem
  - Opérateurs de serveur

# Dossiers partagés: création (2)



# Partages spéciaux

- Créés automatiquement par le système
- Dépendent des fonctionnalités prises en charge par l'ordinateur
- Quelques partages spéciaux:
  - C$, D$, ... (un partage par lettre de lecteur);
  - ADMIN$: répertoire système (c:\winnt)
  - IPC$: partage des canaux nommés;
  - NETLOGON
  - PRINT$

# Partages: autorisations

- Pour accèder à un partage, il faut passer 2 filtres :
  - Les autorisations du partage
  - Les permissions du système de fichier NTFS
- Conseils:
  - Mettre les restrictions sur les permissions NTFS
  - CT aux utilisateurs authentifiés  comme autorisation

# autorisations partage vs permissions NTFS