## Gamme windows Xp

- Windows XP Edition Familiale
- Windows XP Pro
- Windows XP Media center
- Windows XP 64 bits
- Windows XP pro 64 bits

## Présentations

- Pascal PETIT
- 01 60 87 39 03 (tel prof.)
- Email: pascal.petit@info.univ-evry.fr
- http://www.ibisc.univ-evry.fr/~petit
- Administration w2k3-XP:
  - Installation
  - Gestion d'une station de travail
  - Serveur: création et administration d'un domaine

## Processus de démarrage de windows 2000

- Démarrage pc (post, chargement piste boot)
- Chargeur d'amorçage (NTLDR)
- Sélection système d'exploitation
- Détection matériel (NtDectet)
- Sélection configuration
- Chargement et init. Noyau (Ntoskrnl.exe)
- Ouverture d'une session

## Administration W2k3

- Gamme W2K3 et Xp
- Démarrage d'un système windows W2K3
- Notions générales sur la gestion des disques
- Notion générale sur les systèmes de fichiers
- Windows: gestion des utilisateurs et groupes locaux
- Windows: modèle de sécurité
- NTFS: généralités, ACL

## Chargeur d'amorçage (NTLDR)

- Permet le choix du système d'exploitation (boot.ini)
- Charge les fichiers du système d'exploitation
- Détecte les périphériques nécessaires au noyau

## Gamme windows 2003 server

- WeB
- Standard
- Entreprise
- DataCenter

## Noyau, pilotes de périphériques

- NTLDR charge le noyau, la couche d'abstraction matériel (HAL) mais ne les lance pas
- Charge la clef Config/System
- Sélectionne une configuration matérielle
- Sélectionne le jeu de contrôle (controlSet: jeux de pilotes)
  - plusieurs jeux de pilotes sont disponibles
  - il y a au moins le jeux courant et la « dernière bonne configuration connue »

## Boot.ini

- Utilisé par NTLDR pour spécifier les systèmes d'exploitations présents
- Peut-être modifié directement ou via Systeme dans le panneau de configuration

## Noyau, pilotes de périphériques

- Le noyau puis les pilotes de périphériques sont initialisés
- Les pilotes dont Start = 0x1 sont chargés et initialisés

## Boot.ini: quelques commutateurs

- /basevideo: démarrage en vga
- /maxmem:n : limite la taille mémoire utilisée
- numproc=x : limite le nombre de processeurs utilisé dans un ordinateur multiprocesseur
- /fastdetect=[Comx|Comx,y,z...}
- /SOS:  affiche les noms de pilotes au fur et à mesure de leur chargement

## Ouverture de session

- winlogon.exe est lancé
- Winlogon lance lsass.exe (administration de la sécurité locale)
- La mire de login apparaît
- À l'ouverture de session, le contrôleur de services lance les services dont start=0x2
- => le démarrage du système n'est complet qu'après une première ouverture de session ADM

## Détection du matériel (NT Detect)

- NTDetect détecte : type d'ordinateur, d'adaptateur, adaptateurs scsi, video, clavier, port de com., port parallèle, disquette, souris, coprocesseur mathématique

## Fichiers nécessaire au démarrage

| Fichier | Emplacement |
|---|---|
| NTLDR | Partition active |
| Boot.ini | Partition active |
| Bootsect.dos (si autre OS que w2k) | Partition active |
| Ntdetect.com | Partition active |
| Ntbootdd.sys (scsi sans bios) | Partition active |
| Ntoskrnl.exe | %Systemroot\System32 |
| Hall.dll | %Systemroot\System32 |
| Clef System | %Systemroot\System32\Config |
| Pilotes de périph. | %Systemroot\System32\Drivers |

## Résolution des problèmes de démarrage

- utiliser votre connaissance du processus de démarrage pour déterminer à quel stade se situe le problème
- consulter les journaux
- « informations système » pour détecter les conflits de ressources et « gestionnaire de périphériques » pour les régler
- « dernière bonne configuration » via menu d'option avancées du démarrage

## Créer une disquette de boot:

- formater une disquette sur une machine windows 2003 server : formatage simple, pas de boot msdos
- copier les fichiers Ntldr et Ntdetect.com à la racine de la disquette
- créer un fichier boot.ini à la racine de la disquette (ou copier celui de votre installation w2k3srv)

## Résolution des problèmes de démarrage

- démarrage en mode VGA en cas de problème avec un pilote graphique
- « mode sans échec » via F8 au boot
  - charge le minimum de pilotes
  - permet de désinstaller le pilote fautif
  - fichier \Windows\Ntbtlog.txt : liste les périphériques et services correctement chargés et ceux en erreur
- Utiliser ntdetect.chk du reskit : version de débogage de ntdetect
- Commutateur /mem ou /sos de boot.ini

## Démarrage: démonstration

- Modification du boot.ini en direct ou via panneau de configuration/Système
- Démarrage d'un système windows avec l'option /SOS

## Résolution des problèmes de démarrage

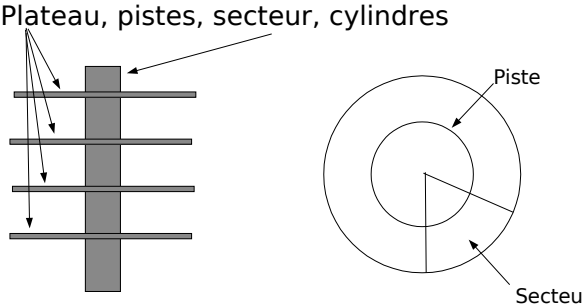
- Console de récupération
  - chkdsk
  - fixmbr
  - restauration de fichier à partir de copie locales
  - ...
- Démarrer sur le CD d'installation et choisir « réparation automatique »
- idem et « installation en mode réparation »: nécessite de réinstaller applications et données

## Choix d'un système de fichier :

- Critères de choix :
  - Fonctionnalités (dossiers, ACL, ...)
  - Vitesse
  - Fiabilité
  - Remise en service rapide en cas de crash
- Metadonnées: informations servant au stockage des données (info du sgf, info. Sur les dossiers, ...)
- La perte de metadonnées peut entrainer la perte de nombreuses données (ex. perte de l'entrée d'un dossier qui entraine la perte de son contenu)

## Gestion des disques: rappels sur le matériel

- Plateau, pistes, secteur, cylindres




Vue de face

Un plateau vu de dessus

## Choix d'un système de fichier : monde windows

- FAT16/FAT32:
  - En cas de multi-boot win9x/windows 2000
  - Pas de sécurité au niveau des fichiers
- NTFS (seule solution viable en entreprise)
  - Sécurité au niveau des fichiers
  - Quotas, Chiffrement, Compression de fichiers ou de répertoires
  - Plus fiable en cas de crash (garantie sur la cohérence des métadonnées)
  - imposé pour AD/domaine

## Gestion des disques: rappels sur le matériel (2)

- Interfaces, caches mémoires, bus, ...
- À ajouter: un dessin illustrant le transit des données du processeur vers les disques en passant par le cache de l'OS, le bus pci, le contrôleur disque, son éventuel cache mémoire, la nappe, l'électronique du disque, son cache en lecture/écrire et pour finir la mécanique du disque.
- Cette présentation aura une application pratique quand on parlera de

## Disques de base/Dynamiques

- Disque de base:
  - disque physique contenant des partitions principales ou étendues.
  - ne peut contenir de volumes dynamiques;
  - ses partitions doivent être associées à des lettres de lecteurs (C:, D:, ..., Z:)
  - l'installateur de w2k3 ne gère que les disques de base;
  - un disque de base peut être converti en disque dynamique.

## Partitions, gestionnaire de volumes logiques,systèmes de fichier

- Partition: partie du disque (morceau inerte de disque)
- Volume logique: une ou plusieurs partitions d'un ou plusieurs disques
- Système de fichier: une partition ou un volume logique dans lequel le système d'exploitation a placé la structure nécessaire au stockage des fichiers.

# La Tolérance de pannes

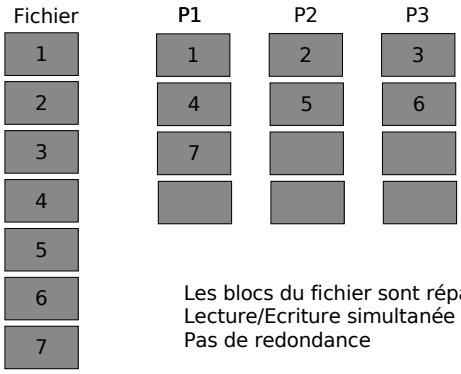
- Généralités
- Systèmes Raid (Redundant Arrays of Inexpensive Disks)
- Miroring Raid 1
- Agrégats par bande avec parité Raid 5



# Disques de base/Dynamiques

- Disque dynamique:
  - contient des volumes dynamiques mais pas de volumes de base;
  - Un volume dynamique peut être simple, fractionné, agrégé, en miroir ou en raid5;
  - Un volume dynamique depuis sa création peut être étendu (mais pas réduit).
  - configuration du disque stockée sur tous les disques dynamique (tolérance de panne)
  - un volume dynamique :
    - peut être associé à une lettre d'unité (D:\, ..., Z:\ )

# Raid 0: agrégat par bande

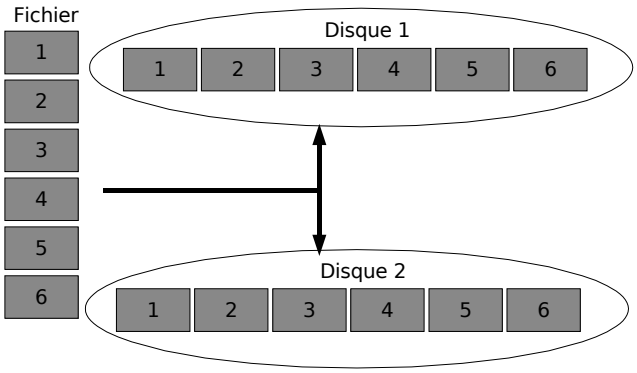



Les blocs du fichier sont répartis sur tous les d
Lecture/Ecriture simultanée sur tous les disque
Pas de redondance

# Disques de base/Dynamiques : vocabulaire

| windows NT | Windows 2k/2k3 | |
|---|---|---|
| disque de base | disque de base | disque dynamique |
| partition | partition | volume simple |
| partition principale | partition principale | volume simple |
| partition étendue | partition étendue | - |
| lecteur logique | lecteur logique | volume simple |
| raid 1 | - | volume raid1 (en mirroir) |
| raid 0 | - | volume raid 0 (agrégat par bande) |
| raid 5 | - | volume raid 5 |
| jeux de volumes | - | volume fractionné |

# Raid 1: Disques mirroirs



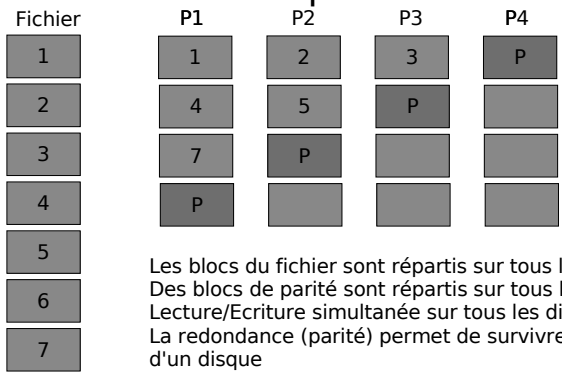

# Gestion des disque: démonstration

- Machine avec 3 disques (1 système, 2 disques de 500Mo non initialisés)
- Utilisation du gestionnnaire de disques
- Création d'un volume dynamique de 300Mo sur le disque 2 (clic droit sur le volume puis nouveau nom)
- Extension de ce volume en y ajoutant 400Mo pris sur le disque 3
- destruction de l'ensemble puis création et association à un dossier vide de l'arborescence

# Bibliographie

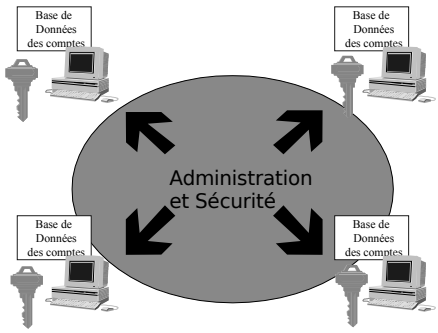

- « Unix Administration » de J.-M. Moreno, Dunod
- Kit de ressource technique windows 2000, tome 2 :administration des serveurs
- kit d'administration de w2k3 server vol. 1
- « softupdates et filesystèmes journalisés », Thomas Pornin, http://www.diablotins.org/medias/downloads/fsj.pdf


# Raid 5:agrégat par bande avec parité




Les blocs du fichier sont répartis sur tous les disqu
Des blocs de parité sont répartis sur tous les disqu
Lecture/Ecriture simultanée sur tous les disques
La redondance (parité) permet de survivre au cras d'un disque

# Modèle groupe de travail



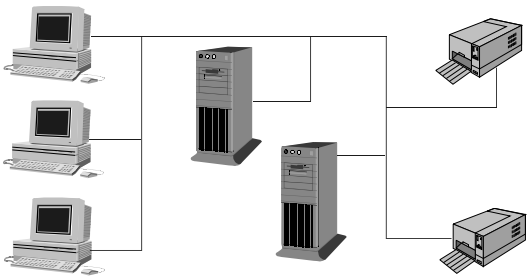

# Comparaison Raid 1 et Raid 5

- Disques en miroir
  - Compatible FAT, HPFS, NTFS
  - Partition système ou d'amorçage
  - Deux disques durs obligatoires
  - Coût au méga-octet supérieur (utilisation à 50%)
  - performances en écriture correctes
  - Excellentes performances en lecture (similaire RAID 0)
  - Utilisent moins de mémoire système
- Agrégats par bandes avec parité
  - Compatible FAT, HPFS, NTFS
  - Sans partition système ou d'amorçage
  - An moins trois disques durs obligatoires
  - Coût au méga-octet inférieur
  - Performance moyenne en écriture
  - Excellentes performances en lecture
  - Requièrent plus de mémoire système
  - Englobent jusqu'à 32 disques durs



# Les Domaines

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



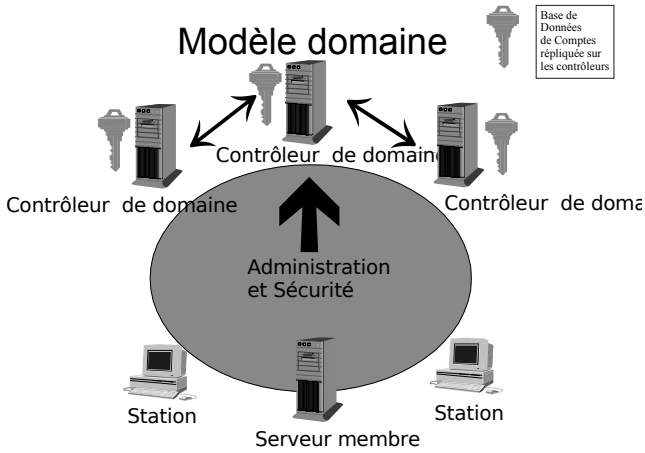
# RAID: problèmes liés à la taille des données

- crash pendant la reconstruction => Aie !
- reconstruction : durée dépend de la taille
- gros disques courants de nos jours
- la probabilité de crash pendant la reconstruction est non nulle. Solutions:
  - limiter la taille des grappes raid
  - systèmes RAID pouvant survivre au crash de plus d'un disque (RAID 0+1 ou 1+0, raid 6, ...)
  - laisser des disques « spare » qui permette à la reconstruction de démarrer sans intervention humaine

## 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.

## Modèle domaine




## 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.

## 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)

## 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.

## 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

## Droits

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

## 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)

## 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 :
  - Les membres du groupe administrateur;
  - le propriétaire de l'objet;
  - les utilisateurs ayant Contrôle Total sur l'objet.

## 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.

## 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

## Héritage

- Conteneur, parents, enfants
- Héritage des permissions

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

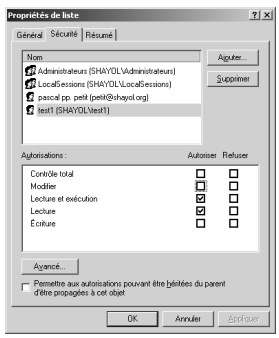
- Sur une station windows 2000 pro
- On reprend le dossier précédent que l'on complète éventuellement avec d'autres sous dossiers
- Suppression de l'héritage
- Création de 3 utilisateurs test1, test2 et test3, d'un groupe Gtest auquel test1 appartient
- Variations sur l'aspect cumulatif des permissions

## 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

## Permissions sur les fichiers

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

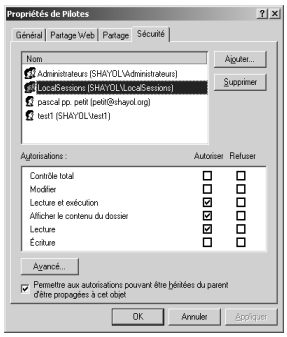



## Héritage des permissions

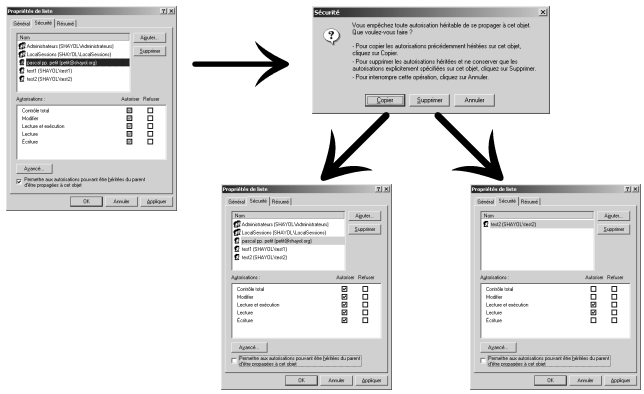
- Par défaut, les permissions d'un dossier s'appliquent aux sous dossiers et aux fichiers qu'il contient
- 3 valeurs possibles pour les cases à cocher d'une ACE: non coché, coché grisé (hérité) , coché
- Il est possible de refuser l'héritage des ACL du père

## Permissions sur les dossiers

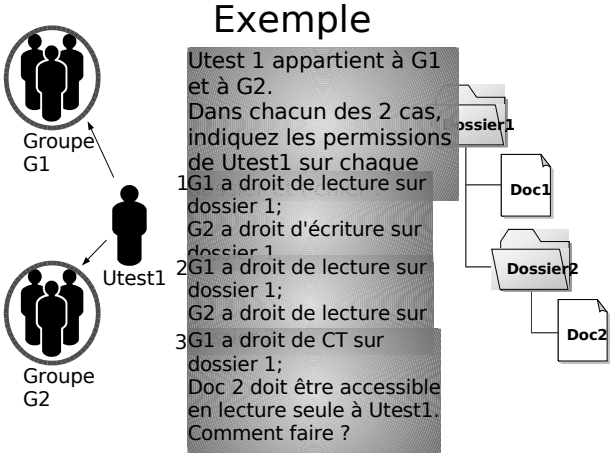
- Modifier
- Lecture et exécution
- Afficher le contenu
- Lecture
- Écriture
- CT




## Suppression de l'héritage



## Exemple




## 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

## 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 ».

## 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 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 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

## 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

## 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.

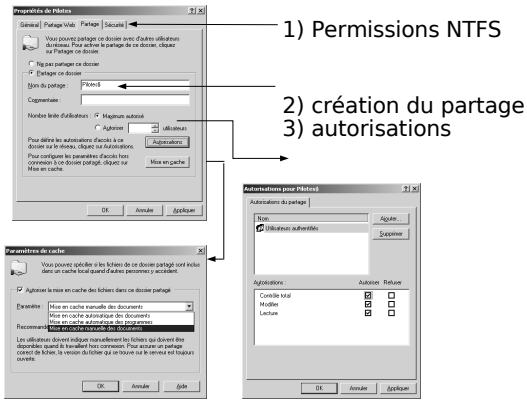
## Dossiers partagés: création

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

## Outils en ligne de commande

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

## Dossiers partagés: création (2)




## 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 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