NTFS: permissions sur les dossiers et sur les fichiers

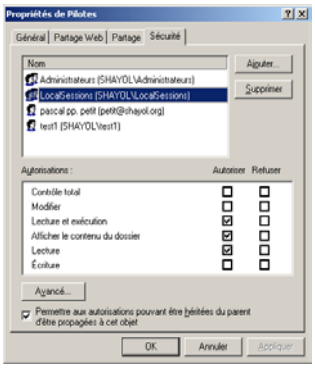
- Uniquement dans les partitions NTFS
- Liste de contrôle d'accès (ACL) contenant des entrées (ACE)
- ACE: un couple (utilisateur ou groupe, permission ou interdiction)
- Modification des ACL par :
  - Les membres du groupe administrateur;
  - le propriétaire de l'objet;
  - les utilisateurs ayant Contrôle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

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 (1)

- 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

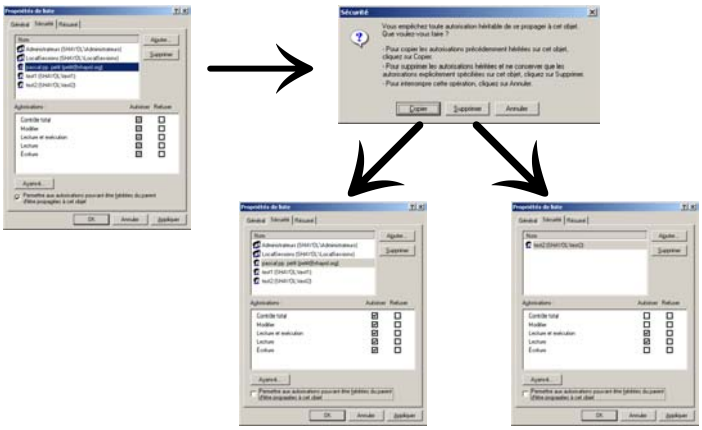
Algorithme déterminant l'accès à un objet

- 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

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

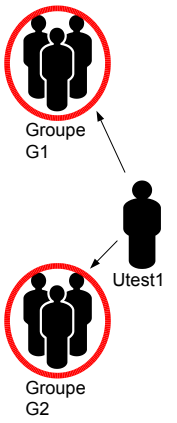
Suppression de l'héritage



Permissions par défaut

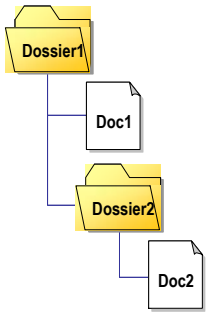
- Au formatage NTFS: CT à « tout le monde »
- A la création d'un fichier ou d'un dossier: hérité des permissions de son dossier père
- Ajout d'une ACE à l'ACL d'un dossier ou d'un fichier: droit « lecture et exécution » par défaut

Exemple



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

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.

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

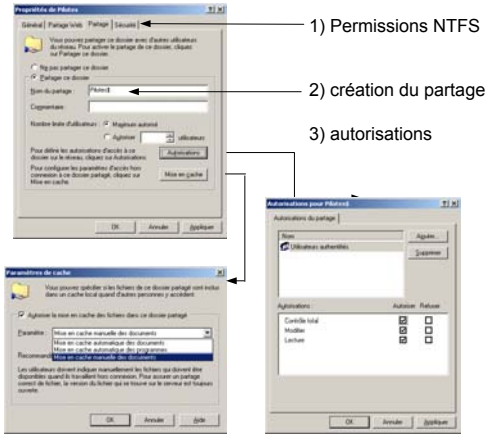
Partages: notation UNC

- 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)



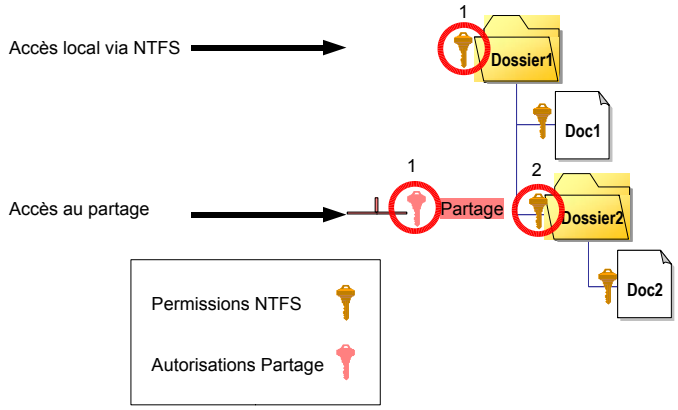
Partages spéciaux

- 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



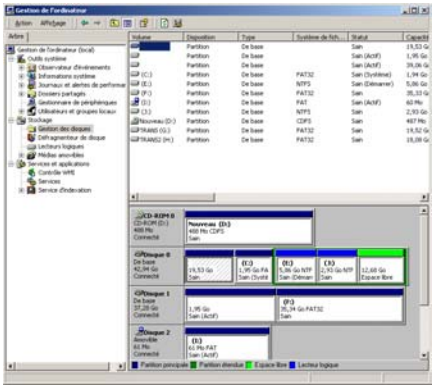
Dossiers hors connexion

- ràf

Audit

- Là, on parle de la surveillance de l'accès à un fichier ou à un répertoire

Gestion de l'ordinateur (1)

- MMC (microsoft management console) permettant de gérer des ordinateurs locaux ou distants
- Disponible par défaut sous Windows 2000, peut être installée sur les autres versions de windows
- Gère partages, périphériques, utilisateurs, groupes, services, …

Gestion de l'ordinateur (2)