Présentations

- Pascal PETIT
- 01 69 47 80 47 (tel prof.)
- Email: donnée en cours
- http://www.lami.univ-evry.fr/~petit/
- Administration w2k:
  - Gestion d'une station de travail
  - Serveur: création et administration d'un domaine
  - Réseau: dns, dhcp, ...

Administration W2k cours 1:

- Démarrage d'un système windows 2000
- 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
- Partages, gestion des accès aux partages

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

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

NTLDR:
·Passe le processeur mode 32 bits
·Démarre le système de fichier ad hoc
·Lit le boot.ini
·Permet la sélection du système d'exploitation
·Ràf

Boot.ini

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

On peut montrer que le délai et le choix de l'os peuvent être réglés soit via Systeme dans le panneau de conf, soit via la modif directe du boot.ini et que la modif de l'un se voit sur l'autre.

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

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

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
- Charge les pilotes de périphériques dont Start vaut 0x0
- Le noyau puis les pilotes de périphériques sont initialisés
- Les pilotes dont Start = 0x1 sont chargés et initialisés

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

Résolution des problèmes de démarrage

- Utiliser ntdetect.chk du reskit : version de débogage de ntdetect
- Commutateur /mem ou /sos de boot.ini
- Mode sans échec
- Console de récupération
- Disquette de réparation d'urgence
- Démarrer sur le CD d'installation et choisir « réparation automatique »

Fichiers nécessaire au démarrage

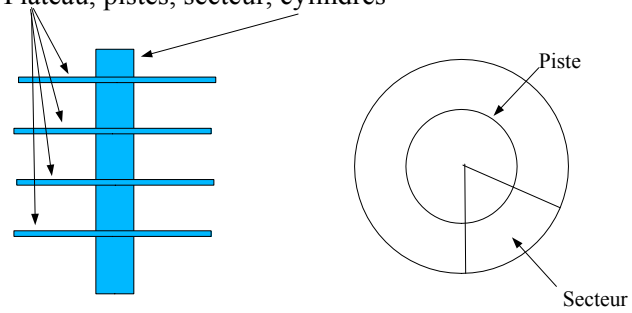
Fichier	Emplacement
NTLDR	Partition active
Boot.ini	Partition active
Bootsect.dos (si autre OS que w2k)	Partition active
Ntdetect.com	Partition active
Ntbootdd.sys (scsi sans bios)	Partition active
Ntoskrnl.exe	%Systemroot\System32
Hall.dll	%Systemroot\System32
Clef System	%Systemroot\System32\Config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

Démarrage: démonstration

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

Gestion des disques: rappels sur le matériel

- Plateau, pistes, secteur, cylindres



Vue de face

Un plateau vu de dessus

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 performance de Raid.

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.

Les premiers systèmes d'exploitation utilisaient directement les partitions.
Les systèmes de fichiers ont permis d'avoir une représentation interne indépendante du disque.
Les gestionnaires de volume logique représentent une abstraction supplémentaire permettant de s'abstraire des partitions.

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)

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)

Disques de base/Dynamiques

- Disque de base: disque physique contenant des partitions principales ou étendues. Ne peut contenir de volumes 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).

Les disques de base contiennent des partitions principales ou étendues visibles par toutes les versions de windows. Ces partitions ne peuvent pas être étendues . Un disque de base contient des volumes de base (partitions du disque).
Les disques dynamiques contiennent des volumes dynamiques mais plus de partitions. Ils ne sont accessibles que depuis windows 2000. Un volume dynamique peut être : simple, fractionné, agrégé par bande (RAID0), miroir et Raid 5. Ils ne sont pas supportés sur les ordinateurs portables ni sur les medias amovibles.
Les informations concernant les volumes d'un disques dynamique sont stockées à la fin du disque (et donc pas dans la table de partition).
Un volume dynamique qui a été créé à l'origine en tant que volume dynamique peut être étendu (mais on ne peut revenir en arrière sans supprimer l'intégralité du volume).
Un volume dynamique qui a été obtenu par conversion d'un volume de base ne peut être étendu.
Par défaut, windows 2000 initialise les disques comme disques de base. Un disque de base peut être transformé en disque de base. La transformation inverse est possible à l'aide d'utilitaires non microsoft (ràf: exemple).
Les volumes à tolérances de panne ne peuvent être créés que sur des disques dynamiques.

Gestion des disque: démonstration

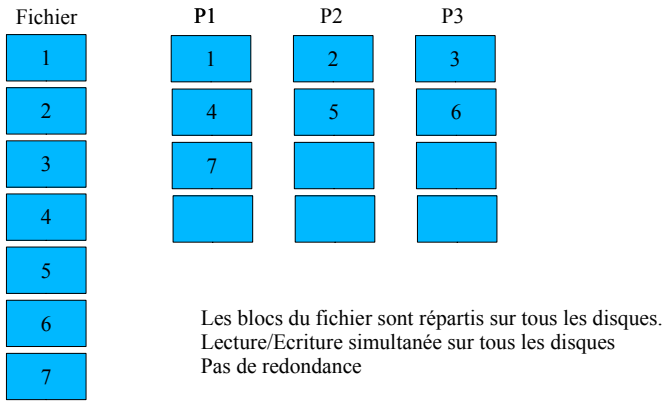
- Machine avec 3 disques (1 système, 2 disques de 500Mo non initialisés)
- Utilisation du gestionnnaire de disques
- Création d'un volume dynamique de 300Mo sur le disque 2
- Extension de ce volume en y ajoutant 400Mo pris sur le disque 3

La Tolérance de pannes

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

Le logiciel de tolérance de panne permet trois types d'options:
Jeux de disques en miroir RAID niveau 1.
Agrégats par bande avec parité RAID niveau 5.
Neutralisation des secteurs défectueux.
Systèmes RAID
6 niveaux
0- Exploitation de disques par bandes.
1- Exploitation de jeux de disques en miroir.
2- Agrégats par bandes avec codes de correction d'erreur ECC (Obsolète).
3- Agrégats par bandes avec codes ECC stocké comme parité (Obsolète).
4- Agrégats par bandes à grands blocs; parité sur un lecteur (Obsolète).
5- Agrégats par bandes à grands blocs; parité sur plusieurs lecteurs.
Mise en œuvre au niveau hardware
Elle est réalisée par certains fournisseurs.
Plus efficace mais souvent plus couteuse (+ Disques Hot Plug).

Raid 0: agrégat par bande



Disques agrégés par bandes (RAID 0) :

supporté par W2K pro et serveur

Deux disques au minimum. Les blocs sont de 64 Ko sous W2K.

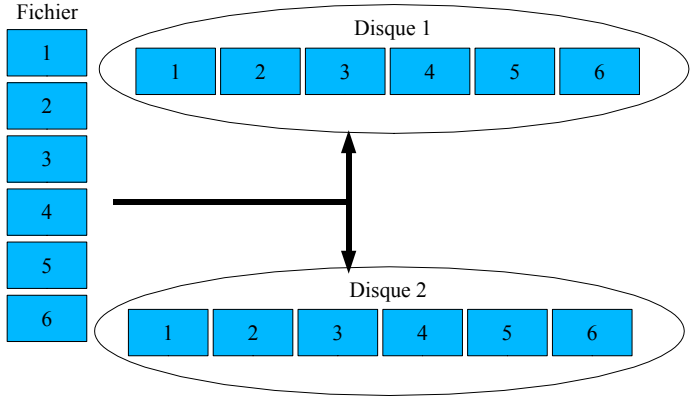
Si une partition tombe les données sont perdues.

La taille nécessaire est celle des données.

En théorie, le débit brut est la somme des débits des disques mais le temps d'accès n'est pas amélioré.

La présence de plusieurs contrôleurs de disque favorise la performance en permettant un réel traitement en parallèle des requètes sur les disques sans goulot d'étranglement dû à la liaison contrôleur-disques.

Raid 1: Disques mirroirs



Disques en miroir (RAID 1)

Duplication d'une partition (données) sur un ou plusieurs autres disques.

Quelles sont les partitions duplicables ? Toutes y compris celle d'amorçage.

Disque en duplex.

L'espace disque nécessaire est au moins le double de celui des données qui y sont stockées.

Si un disque tombe en panne, les données sont disponibles sur l'autre.

Idem avec plusieurs contrôleurs de disque.

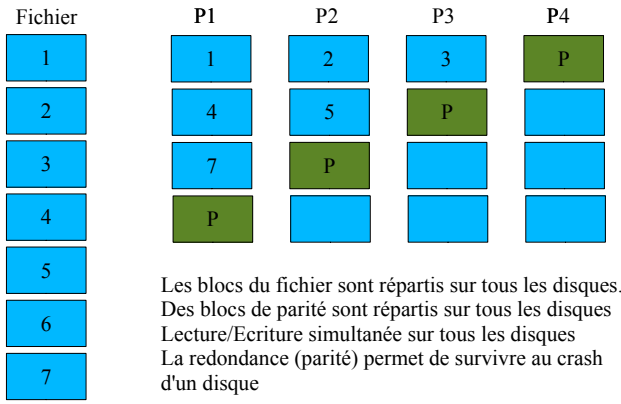
Moins d'activité sur le canal = plus de performances

Solution Hardware : Le disque entier est miroré et non une ou plusieurs partitions.

Les performances en écriture sont dégradées (on doit écrire les données sur chaque disque).

En lecture, les performances dépendent de la politique choisie par le logiciel RAID: windows 2000 répartit les lectures sur les disques du mirroir (à la RAID0). Les performances en lecture sont donc proches de celles de RAID0.

Raid 5:agrégat par bande avec parité



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

Agrégats par bandes avec parité

C'est la méthode la plus employée en tolérance de panne.

Les informations de parité sont écrites à travers tous les disques (contraitement à RAID4 qui réservait un disque pour les informations de parité).

Les données et les informations de parité sont toujours sur des disques différents.

Si un disque tombe en panne, les informations de parité réparties sur tous les disques restants permettront la reconstruction des données manquantes.

La partition d'amorçage ne peut être en RAID5..

En temps normal le temps de lecture est amélioré, en cas de panne il se dégrade car il est obligatoire de parcourir les informations de parité pour récupérer les données.

La totalité des opérations d'écriture normales ont besoin d'au moins trois fois plus de mémoire (chargement des blocs pour le calcul de parité). Le fait de devoir charger les blocs pour le calcul de parité diminue les performances en écriture dans certains cas. En pratique, les données nécessaires au calcul de parité ont de grandes chances d'être dans les caches (lues précédemment ou bien faisant partie des données écrites). La perte de performance est limitée dans les cas de figure courants.

La reconstruction d'un disque est une opération lourde car il faut lire l'intégralité des autres données pour reconstituer les données ou parités manquantes.

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

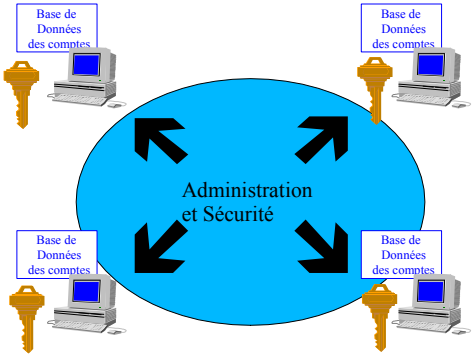
Tolérance de panne

Quel que soit le choix, un disque en spare est souvent une excellente solution, le RAID5 matériel également.

Bibliographie

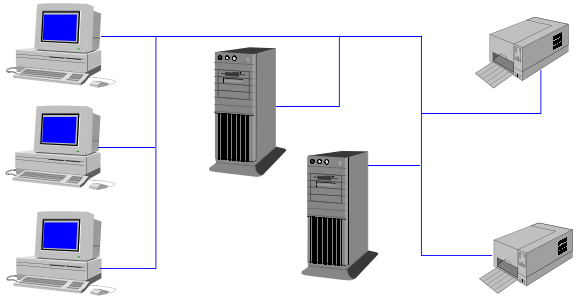
- « Unix Administration » de J.-M. Moreno, Dunod
- Kit de ressource technique windows 2000, tome 2 :administration des serveurs
- « softupdates et filesystèmes journalisés », Thomas Pornin, ràf: URL
- Raid:

Modèle groupe de travail

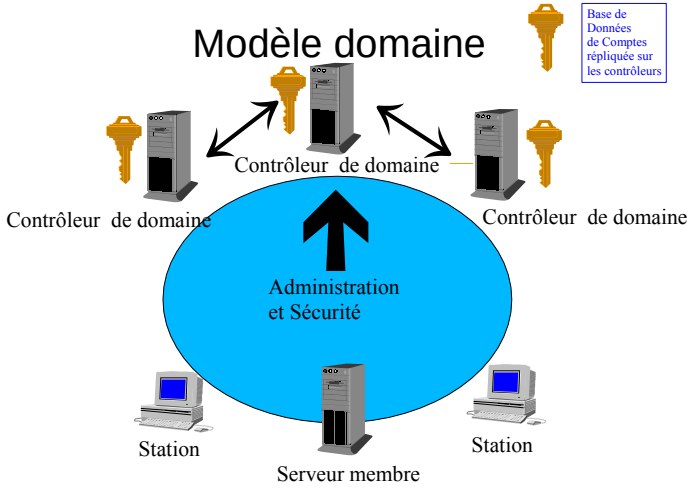


Les Domaines

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



Modèle domaine



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 2000 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.

Quelques notions qui seront développées par la suite :
Autorisations basées sur l'utilisateur: un programme a les droits de l'utilisateur qui l'exécute.
Accès discrétionnaire aux objets sécurisables:Le propriétaire d'un objet peut contrôler qui peut l'utiliser et avec quel genre d'accès. Windows 2000 permet de plus de gérer l'accès à des propriétés précises de l'objet ou à l'objet entier.
Héritage des permissions: Les permissions placées sur un conteneur (répertoire par exemple) sont héritées par les nouveaux objets (comme sous NT) mais aussi par les objets existants (nouveauté W2K).
Privilèges administratifs: Il est possible de gérer l'accès d'utilisateurs ou de groupe à certaines fonctions d'administration. Les stratégies de groupe W2K permettent une gestion centralisée des privilèges administratifs sur tous les ordinateurs du domaine.
Audit: il est possible de détecter les échecs ou les réussites de toute action ayant trait à la sécurité (de l'ouverture de session à l'utilisation de privilèges en passant par les accès aux fichiers ou répertoires)

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.

Les autorisations W2K sont basées sur l'utilisateur : toute application démarre dans le **contexte de sécurité** de l'utilisateur et ne peut faire que ce que l'utilisateur a le droit de faire. Cette notion est valable pour les **principaux de sécurité** (utilisateurs, groupes, ordinateurs ou service) qui sont les entités qui doivent avoir des comptes.

Le **compte utilisateur** : Toute personne faisant partie d'un domaine doit avoir un compte utilisateur

Le compte contient les informations sur l'utilisateur, ses appartenances aux groupes et les informations concernant la politique de sécurité.

Un **SID** (**identifiant de sécurité**) est attribué automatiquement par W2K au nouveau compte lors de sa création ou lors de son déplacement.

Jeton d'accès : Il est créé à l'ouverture de session de l'utilisateur.

Il comprend un ID de sécurité pour l'utilisateur, un pour les groupes auxquels il appartient et des informations nom de l'utilisateur etc..

Chaque processus possédera une copie du jeton d'accès, de même W2K se référera aux ID de sécurité en cas de tentative d'accès à un objet.

Il sont comparés à la liste de permission de l'objet pour validation des droits d'accès à celui-ci.

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.

Le programme exécuté par un utilisateur ne doit pas avoir plus de droits d'accès aux objets que ceux que possède l'utilisateur.

SUJET :

Il est la combinaison du jeton d'accès de l'utilisateur et du programme exécuté.

Il est employé par W2K pour suivre et gérer les droits des programmes.

Le programme s'exécute donc dans le contexte de sécurité de l'utilisateur.

Le contexte de sécurité contrôle les droits d'accès aux objets que possède le sujet .

Emprunt d'identité: Un processus peut utiliser les attributs de sécurité d'un autre. Ainsi, un processus serveur emprunte l'identité d'un processus client pour compléter une tâche impliquant des objets auxquels il n'a normalement pas droit.

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)

Les informations de sécurité des objets

Un objet pouvant contenir d'autres objets est appelé un **conteneur**. Un dossier est un exemple de conteneur. Les objets contenus dans un conteneur sont appelés les **enfants** du conteneur tandis que le conteneur est le **parent** de ces objets.

Tous les objets nommés et certains anonymes peuvent être sécurisés.

Le **descripteur de sécurité** détaille les attributs de sécurité d'un objet.

Il comporte 4 parties :

ID de sécurité du propriétaire

Indique l'utilisateur ou le groupe processeur de l'objet.

Il peut changer les permissions d'accès à l'objet.

ID de sécurité du groupe

Employé uniquement par POSIX

Liste de contrôle discrétionnaire (DACL)

Identifie les droits d'accès des utilisateurs et des groupes, les ACL sont contrôlés par le propriétaire.

ACL système (SACL)

Contrôle les messages d'audits générés par le système, ils sont contrôlés par les administrateurs de sécurité.

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.

Un programme est un processus comportant des des threads d'exécution. Lors que l'utilisateur tente d'accéder à un objet, il le fait grâce à un thread d'un programme. Pour accèder à un objet, un thread doit s'identifier auprès du sous-système de sécurité. N'ayant pas d'identifiant de sécurité, le thread va devoir en emprunter un à un principal de sécurité : l'utilisateur qui a lancé le programme dans notre cas. Le thread a une copie du jeton d'accès de l'utilisateur qui l'exécute qui lui permettra de s'identifier comme appartenant à l'utilisateur qui l'a lancé. Le jeton d'accès contient des informations permettant d'identifier l'utilisateur et tous les groupes auxquels il appartient.
Ce jeton va être comparé avec la DACL du descripteur de sécurité de l'objet. Si le sous-système de sécurité ne peut conclure lors de cette comparaison, il refuse l'accès à l'objet.

Héritage

- Conteneur, parents, enfants
- Héritage des permissions

Un objet pouvant contenir d'autres objets est appelé un **conteneur**. Un dossier est un exemple de conteneur. Les objets peuvent hériter des permissions de leur parent.

Quand on annule l'héritage, on se voit proposer deux choix pour les permissions héritées :

- supprimer les permissions correspondantes des ACL
- laisser les choses en l'état en recopiant les permissions correspondantes comme si elles avaient été définies localement .

Les second choix rend ce permissions indépendantes de celle du parent (ce qui peut être une bonne ou une mauvaise chose suivant le contexte) et permet de les modifier localement.

L'héritage est un mécanisme puissant qui permet de changer finement les permissions sur toute une arborescence en modifiant simplement celles de sommet de l'arborescence.

Droits

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

Un **droit** est l'autorisation d'effectuer une opération. Le seul droit inhérent est celui qu'à le **propriétaire** d'un objet de contrôler l'accès à cet objet. Le propriétaire a donc ce droit même s'il n'apparaît pas dans la DACL.Les autres droits doivent être explicitement attribués. Le **propriétaire initial** d'un objet est son créateur. Un autre utilisateur peut **s'approprier un objet** si le propriétaire l'y a autorisé. Les administrateurs peuvent s'approprier un objet sans l'accord de son propriétaire.
On distingue deux types de droits :
• Les **permissions** : autorisation d'accès à un objet précis
•Les **droits utilisateurs**: autorisation d'effectuer une opération qui affecte tout l'ordinateur plutôt qu'un objet précis. On en distingue deux sortes:

- Les **droits de procédures de connexion** : contrôle de l'accès à un ordinateur
- Les **privilèges**.: contrôle de la manipulation des ressources système.

Les droits d'utilisateurs sont affectés à travers la stratégie de sécurité (locale, du contrôleur de domaine, du domaine, ...). Nous développerons cela quand nous parlerons de stratégies de groupes.
En cas de conflit entre permission et privilège, le privilège l'emporte (exemple: accès aux fichiers et opérateur de sauvegarde qui aura le droit d'accéder au fichiers pour réaliser des sauvegardes mais pas pour l'ouvrir dans d'autres programmes si l'accès lui est interdit).

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 le fichiers et dossiers: démonstration (1)

- Sur une station windows 2000 pro
- Création d'un dossier et visualisation des ACL par défaut
- Notion d'ACE
- autorisation/refus

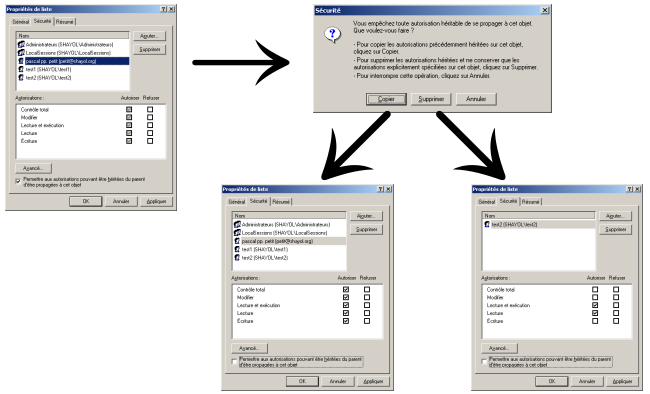
Permissions par défaut

- 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

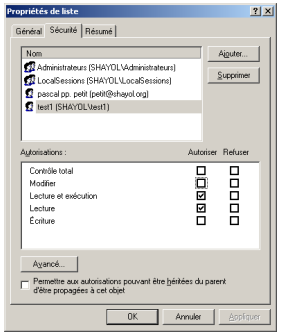


Permissions sur le fichiers et dossiers: démonstration (2)

- 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



Lecture:

- Lire le contenu du fichier ;;
- Voir les attributs (lecture seule, caché, ...) du fichier
- Voir les permissions et le propriétaire du fichier

écriture:

- Sauvegarder/écraser le fichier;
- Changer les attributs du fichierr
- Voir les permissions et le propriétaire du fichier

Lire et exécuter

- Exécuter des logiciels
- Implique “lecture”

Modifier

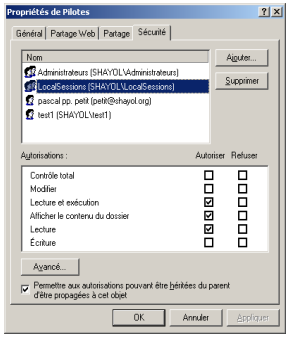
- Modifier ou supprimer le fichier
- Implique “lire et exécuter” et “écriture”

Contrôle Total (CT)

- Changer les permissions, devenir propriétaire
- Implique l'ensemble des autres permissions

Permissions sur les dossiers

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



Lecture:

- voir les fichiers et les sous-dossiers présents dans ce dossier;
- Voir les attributs (lecture seule, caché, ...) du dossier

•Voir les permissions et le propriétaire du dossier

écriture:

- Créer des fichiers et des dossiers dans ce dossier
- Changer les attributs du dossier
- Voir les permissions et le propriétaire du dossier

afficher le contenu du dossier:

- Voir les noms des fichiers et dossiers contenus dans le dossier

Lire et exécuter

- Traverser le dossier
- Implique “lecture” et “afficher le contenu du dossier”

Modifier

- Supprimer le dossier
- Implique “lire et exécuter” et “écriture”

Contrôle Total (CT)

- Changer les permissions, devenir propriétaire
- Détruire des fichiers et des sous-dossiers
- Implique l'ensemble des autres permissions

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

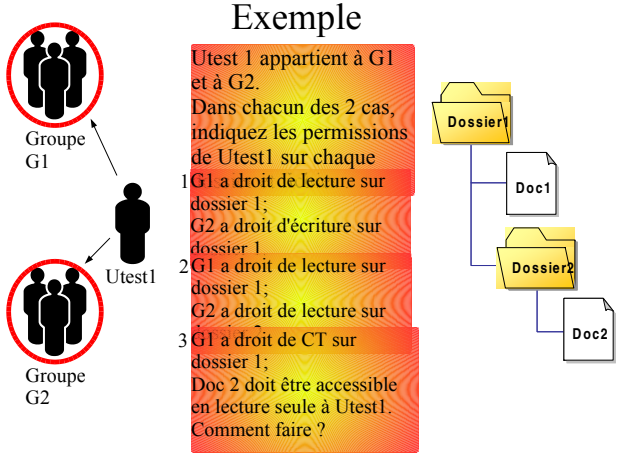
Algorithme déterminant l'accès à un objet

- 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



Cas 1: Utest1 cumule les permissions obtenues sur chaque groupe. Il a dont les permissions de lecture et écriture sur **Dossier1**. Si l'héritage n'a pas été désactivé(ce qui nous supposerons par la suite), il a ces permissions sur **Dossier2, Doc1** et **Doc2**.
Cas 2: Utest1 a droit de lecture sur **Dossier1** et **Doc1**. Il a droit de lecture/écriture sur **Dossier2** et **Doc2**.
Cas 3: Pour avoir des permissions plus restrictives sur Dossier2 ou sur Doc2, 3 solutions:

- On place des interdictions dans l'ACE Utest1 de Doc2. Ce n'est pas une bonne idée car il faudra le faire à la main pour chaque fichier et pour chaque utilisateur.
- On désactive l'héritage sur Doc2 et on enlève Utest1 et tous les groupes auxquel il appartient des ACL de Doc2. Le fait d'être obligé de le faire pour tous les groupes peut avoir des effets sur d'autres utilisateurs. Le fait d'agir au niveau de Doc2 imposera de faire de même pour les autres fichiers dans le même cas.
- Dans une administration cohérente, on travaillerait 1) au niveau d'un groupe plutôt que d'un utilisateur seul et 2) au niveau d'un dossier plutôt que d'un fichier. La solution la plus cohérente serait de désactiver l'héritage sur **Dossier2** et de donner la permission lire au groupe **G2** ou de créer un groupe ad hoc si le groupe **G2** ne convient pas.

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.

Lors d'une copie de fichiers ou répertoires, les permissions d'origine ne sont pas affectées à la version copiée :

- Les permissions de la version copiée sont celles du répertoire parent (héritage)
- Le propriétaire de la version copiée est l'utilisateur qui a réalisé la copie

Pour préserver les permissions, il est possible d'utiliser l'utilitaire robocopy fournit avec le kit de ressources techniques de windows 2000. L'utilitaire scopy (NT res. Kit) n'existe plus et est remplacé par robocopy.

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

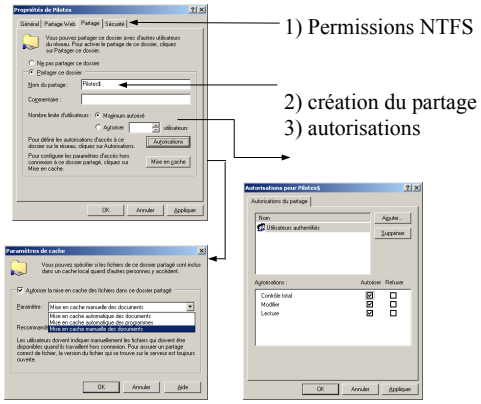
Partages: notation UNC

- 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 spéciaux

Un partage spécial est un partage créé automatiquement par le système. Les partages spéciaux dépendent des fonctionnalités prises en charge par l'ordinateur Un contrôleur de domaine aura ainsi des partages spéciaux que n'auront pas les autres ordinateurs. Voici une liste des partages spéciaux (extrait de l'aide en ligne deW2K server) :

[lettre de lecteur]$ Partage qui permet au personnel administratif de se connecter au répertoire racine d'un périphérique de stockage. Les partages spéciaux ont des noms de la forme A$, B$, C$, D$ et ainsi de suite. Par exemple, D$ est un nom de partage permettant à un administrateur d'accéder par le réseau au lecteur D.

Pour un ordinateur Windows 2000 Professionnel, seuls les membres des groupes Administrateurs et Opérateurs de sauvegarde peuvent se connecter à ces partages. Pour un ordinateur Windows 2000 Server, les membres du groupe Opérateurs de serveur peuvent également se connecter à ces partages.

ADMIN$ Ressource utilisée par le système pendant l'administration à distance d'un ordinateur. Le chemin d'accès de cette ressource est toujours celui de la racine système de Windows 2000 (répertoire dans lequel Windows 2000 est installé : par exemple, C:\Winnt).

IPC$ Ressource assurant le partage des canaux nommés, qui jouent un rôle essentiel dans la communication entre les programmes. Elle est utilisée pendant l'administration à distance d'un ordinateur et l'examen de ses ressources partagées.

PRINT$ Ressource utilisée lors de l'administration à distance des imprimantes.

NETLOGON Ressource utilisée par le service Accès réseau d'un ordinateur Windows 2000 Server pendant le traitement des demandes d'ouverture de session sur un domaine.

Cette ressource est disponible uniquement pour les ordinateurs Windows 2000 Server. Elle n'est pas fournie pour les ordinateurs Windows 2000 Professionnel.

FAX$ Disponible sur un serveur, ce partage est utilisé par des clients de télécopie lors de l'envoi de télécopies. Ce partage sert à placer temporairement des fichiers dans un cache et à accéder à des pages de garde stockées sur le serveur.

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