Administration système windows

- 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
- Les diapositives marquées d'une étoile (*) ne sont pas au programme de l'examen écrit

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

Boot.ini

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

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 dotn 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

Fichiers nécessaire au démarrage (*)

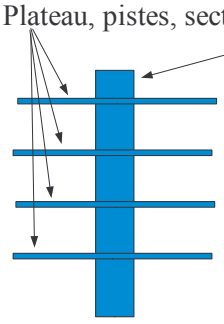
Fichier	Emplacement
NTLDR	Partition active
Boot.ini	Partition active
Bootsect.dos (si autre OS que w2k)	Partition active
Ntdetect.com	Partition active
Ntbootdd.sys (scsi sans bios)	Partition active
Ntoskrnl.exe	%Systemroot\System32
Hall.dll	%Systemroot\System32
Clef System	%Systemroot\System32\Config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

Démarrage: démonstration (*)

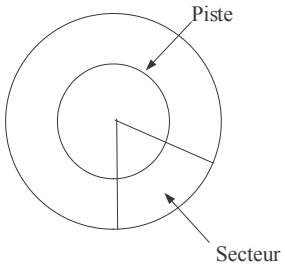
- Modification du boot.ini en direct ou via panneau de configuration/Système
- Démarrage d'un système windows avec l'option / SOS

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.

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).

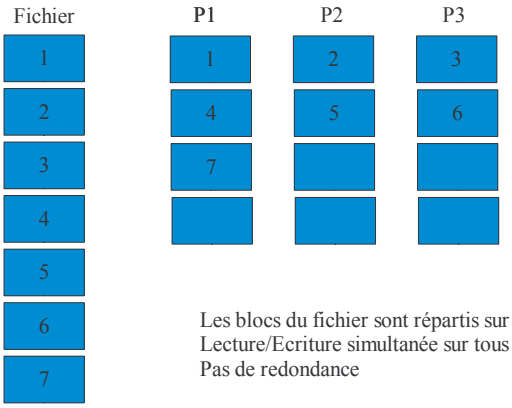
Gestion des disque: démonstration

- 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

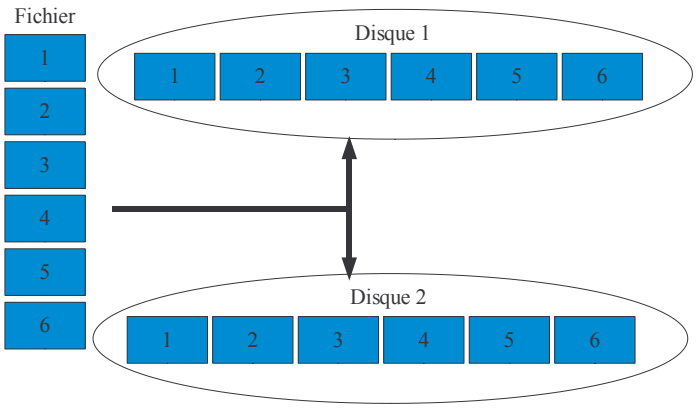
- Généralités
- Systèmes Raid (Redundant Arrays of Inexpensive Disks)
- Miroring Raid 1
- Agrégats par bande avec parité Raid 5

Raid 0: agrégat par bande

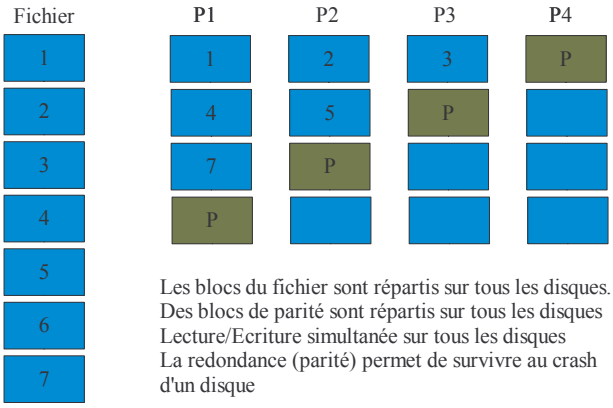


Les blocs du fichier sont répartis sur tous les disques.
Lecture/Ecriture simultanée sur tous les disques
Pas de redondance

Raid 1: Disques mirroirs



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

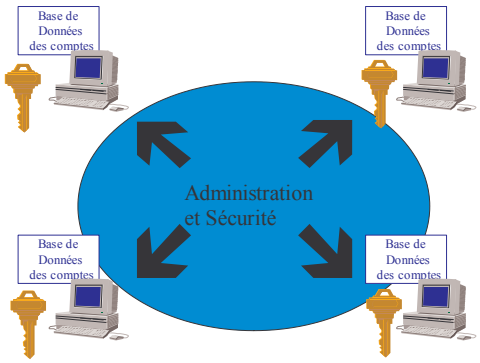
Comparaison Raid 1 et Raid 5

- 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

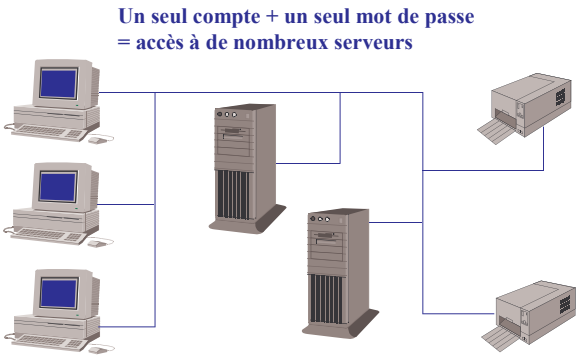
Bibliographie

- « 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:

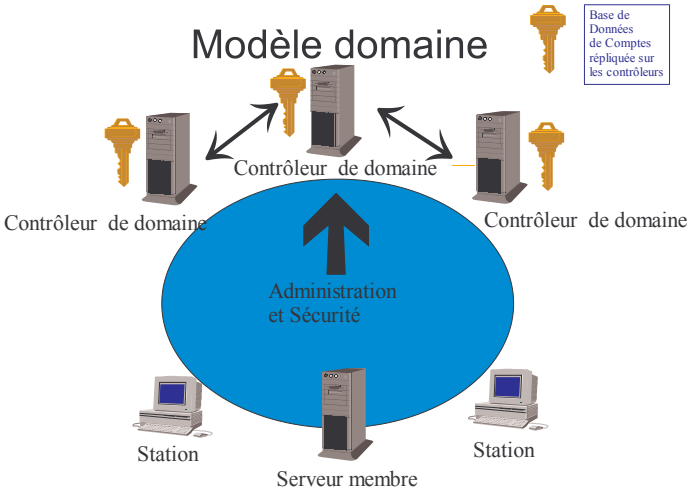
Modèle groupe de travail



Les Domaines



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.

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 :
  - 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

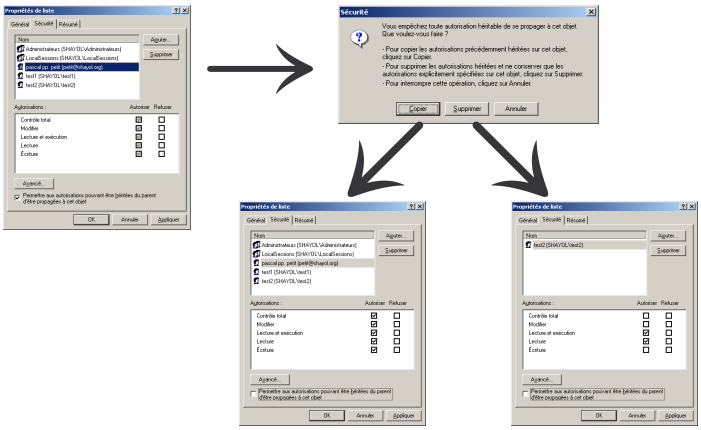
Permissions par défaut

- 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

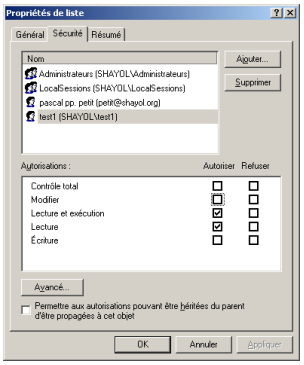


Permissions sur le fichiers et dossiers: démonstration (2)

- 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

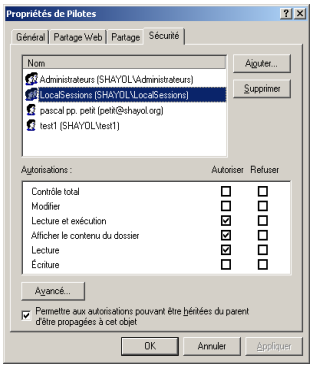
Permissions sur les fichiers

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



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

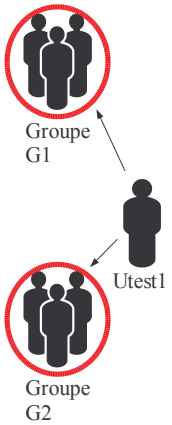
Algorithme déterminant l'accès à un objet

- 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)

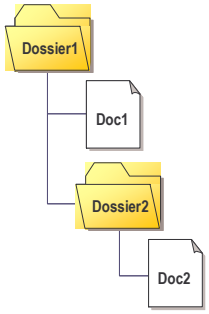
- Suite de la démonstration précédente
- On illustre la priorité des refus
- Exemple classique: refus pour tout le monde, CT pour test1 => refus pour test1

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
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)