Sécurité et protection des objets externes

Service attendu

- Service attendu sur la conservation des données
  - *Retrouver les données dans l'état*
  - *Permettre d'avoir un rôle de "propriétaire"*
- Altération due à une mauvaise utilisation des opérations
  - protection = méthodes qui spécifient les *règles d'utilisation* des opérations
- Altération due à une défaillance du matériel ou du logiciel
  - sécurité = méthodes qui assurent que les opérations se déroulent conformément à leur *spécification*

La protection

- Définir les règles d'utilisation des opérations
- Par droit d'accès
  - liste de contrôle d'accès indique `qui` est autorisé à faire `quoi`
- Par mot de passe
  - accès autorisé à ceux qui connaissent le mot de passe

Protection par droit d'accès (1)

- Unix
  - les droits
    - r droit de lire
    - w droit d'écrire
    - x droit d'exécuter un programme ou de rechercher dans un répertoire
  - regroupement des utilisateurs
    - objet externe => un propriétaire et un groupe d'usagers
  - liste de contrôle d'accès en 3 catégories
    - le propriétaire de l'objet
    - ceux appartenant au groupe
    - les autres

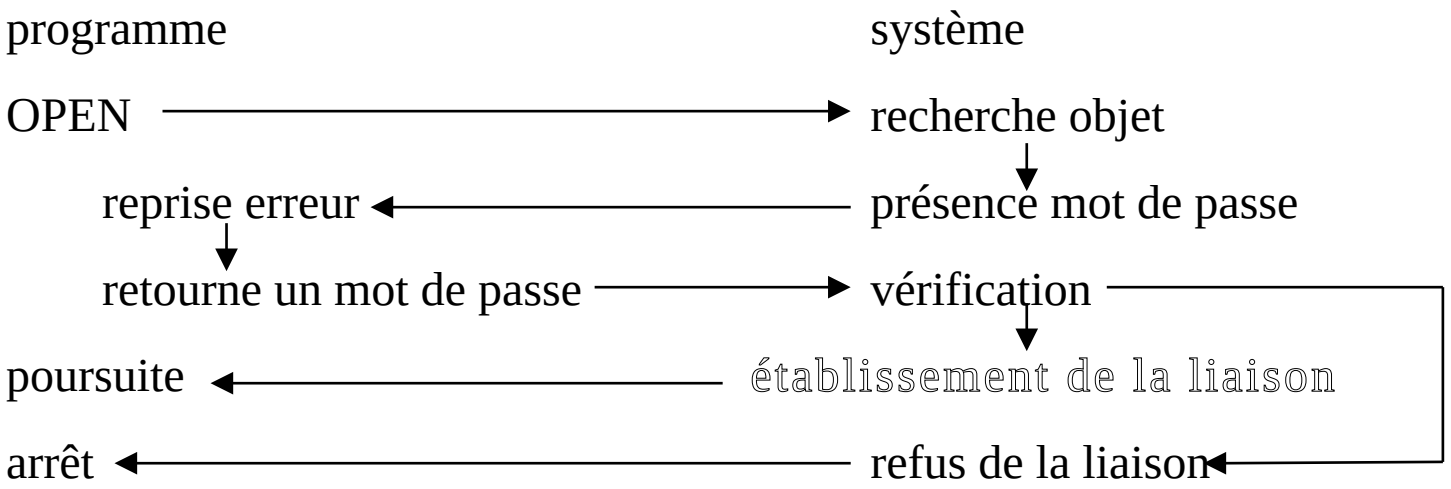
  ➪ 9 bits par objet, dans le descripteur de l'objet

Protection par droit d'accès (2)

- Multics
  - droits r, w x, regroupement par projets
  - à chaque objet => liste de droits d'accès
  - <r, COMPTABLE.*>, <rw, COMPTABLE.Jean, *.Paul>
- Windows NT
  - droits plus étendus: certains prédéfinis, d'autre définis par l'utilisateur
  - regroupement des utilisateurs
  - à chaque objet => liste de droits d'accès, positifs ou négatifs
  - <~r, Pierre>, <r, COMPTABLE>, <rw, Paul>
- Autres => utilisateurs attachés à un numéro de compte
  - liste des numéros autorisés à lire (par défaut tous)
  - liste des numéros autorisés à écrire (par défaut celui du créateur)

Protection par mot de passe

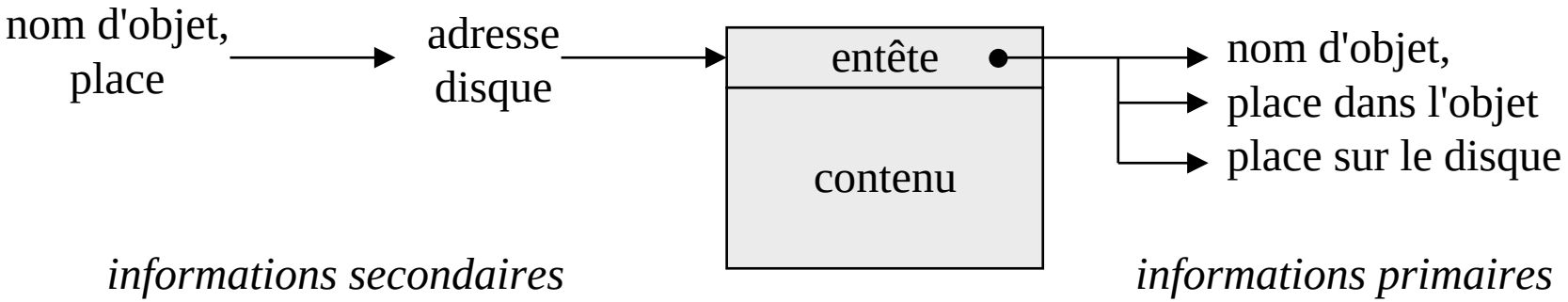
- À l'établissement de la liaison



- Efficacité
  - ♦ non divulgation
  - ♦ très difficile à trouver
  - ♦ changés souvent

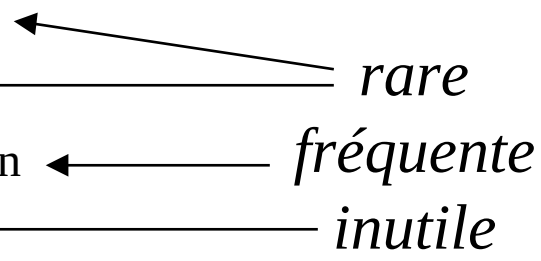
La sécurité

- Palier les défaillances du matériel ou du logiciel
- Mécanismes: redondance des informations (interne/externe)
- Redondance interne
  - Information primaire = information de base
  - Information secondaire = accélération des accès
  - lors de chaque accès, vérification des informations primaires
  - perte des informations secondaires ➞ reconstruction depuis primaires



Redondance externe (1)

- Par sauvegarde périodique
- Sauvegarde complète => photographie instantanée de tout
  - 35 minutes, 7 bandes pour 1 Go à 500 Ko/s
  - 50 heures, 700 bandes pour 100 Go
- Sauvegarde de reprise => photographie partielle (volume)
  - partitionnement des disques pour réduire la taille
  - arborescence unique cache le partitionnement
  - volumes dédiés suivant les besoins de sauvegarde
    - utilitaires standards, exécutables stables
    - documentation stable
    - fichiers sources en cours de modification
    - fichiers temporaires



Redondance externe (2)

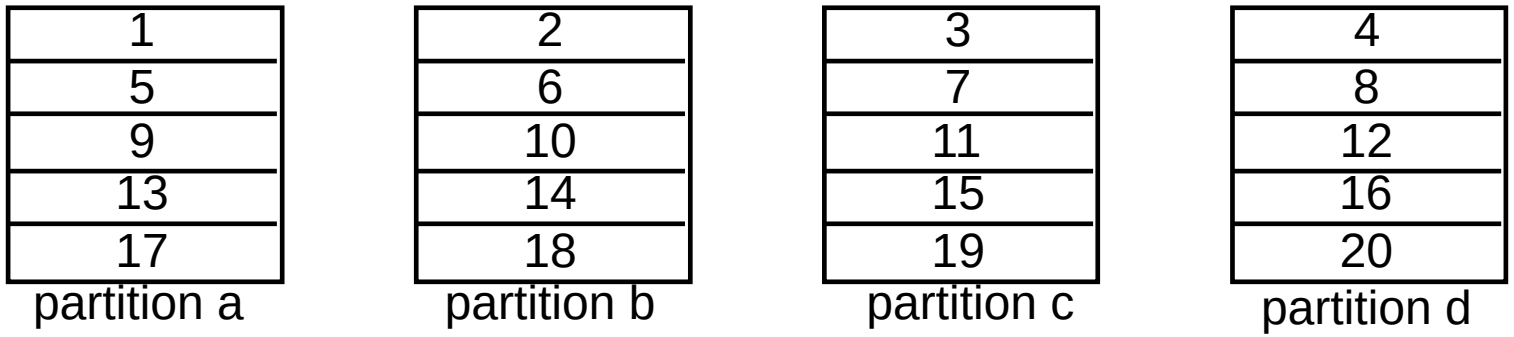
- Sauvegarde incrémentale => photographie des modifications
  - par objet, suivant leur date de dernière modification
  - parcours périodique de toute l'arborescence
  - uniquement s'ils ne sont pas ouverts en écriture (cohérence)
- Restauration
  - objet
    - remonter les sauvegardes incrémentales,
    - jusqu'à dernière sauvegarde de reprise du volume
  - volume
    - reprendre la dernière sauvegarde de reprise
    - appliquer les modifications des sauvegardes incrémentales
- Accès facile aux sauvegardes incrémentales => disque dédié

Redondance externe (3)

nature	période	conservation	nombre	taille	durée
incrémentale	8 heures	15 jours	45	20	en ligne
reprise	7 jours	3 mois	13	130	volume 50’
complète	1 mois	1 an	12	120	tout 6h.

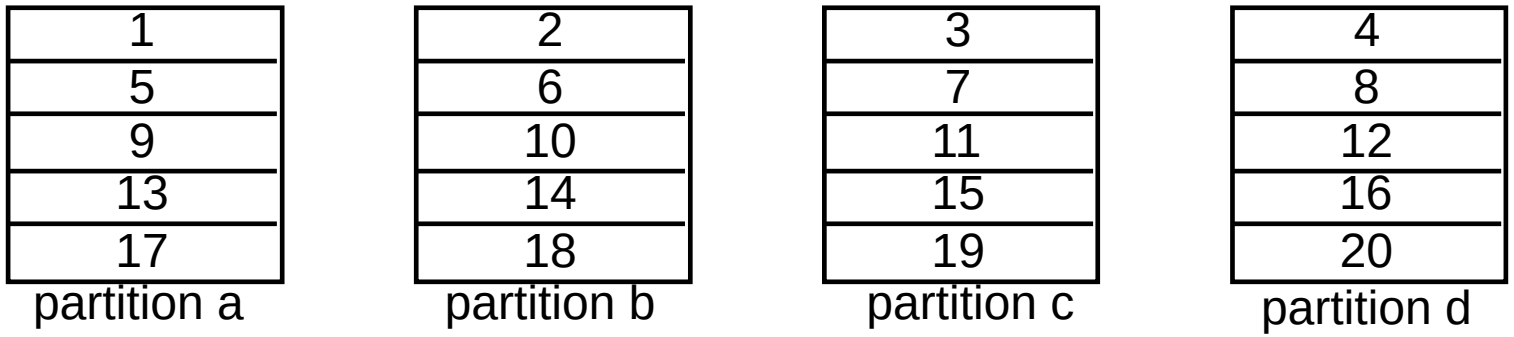
- Pour 10 Go, avec 5% de modifications pour 8 heures
  - coût machine: sans doute 5% (pour une utilisation 24h/24)
  - bandes: 2000
  - disques: 500 Mo (dernière sauvegarde incrémentale)
- Service: retrouver l'état d'un objet à une date donnée
  - < 15 jours, à 8 heures près
  - < 3 mois, à 7 jours près
  - < 1 an => à 1 mois près
- Insuffisant pour SGBD => fichier journal (~incrémentale)

R. A. I. D. (1)



- Redundancy Array Inexpensive Disc
- Volume réparti sur plusieurs partitions (disques distincts)
- RAID-1 ou disques miroirs
  - duplication sur plusieurs partitions => 2 partitions nécessaires, a et b
  - écriture sur les deux, contenu (a) = contenu (b)
  - accès soit sur a soit sur b
  - une des deux en panne les données encore accessibles sur l'autre
  - 50% espace pour la redondance

R. A. I. D. (2)



- RAID-5 ou disque avec parité
  - sur chaque ligne horizontale, une des bandes est combinaison des autres

    b4 = b1 **`xor`** b2 **`xor`** b3
  - écriture de b1 => calcul b4 = b4' **`xor`** b1' **`xor`** b1
  - le rôle de combinaison tourne sur les partitions (b5, b10, b15, b20,…)
  - en cas de panne de a, on recalcule b1 = b4 **`xor`** b2 **`xor`** b3
  - 25% espace pour la redondance (plus généralement 1/n pour n partitions)
  - peut être implanté dans le système ou dans le contrôleur disque

Conclusions

- Altération des données
  - mauvaise utilisation des opérations => protection
    - droits d'accès <qui, quoi>
    - mot de passe (avoir la clé)
  - défaillance du matériel ou du logiciel => sécurité
    - redondance interne, plusieurs informations de structure
    - redondance externe, sauvegardes périodiques
    - disques à redondance (RAID)