Principes d'utilisation des systèmes de gestion de bases de données

Confidentialité

L3 Informatique

Emmanuel Waller, LRI, Orsay

Rappel : les deux parties du cours

- création et gestion de la base
  - les problèmes BD
    - liés à la construction de la base :

      modèle, conception, indépendance des niveaux, contraintes, confidentialité, mise à jour, persistance
    - liés à la dynamique de la base (HP) :

      reprise sur panne, contrôle de concurrence
    - liés à l'interrogation de la base (HP) :

      interrogation, grandes quantités (optimisation)
  - les traitements bas niveau en mode programme : PL/SQL
- accès à la base depuis un programme généraliste
  - pbs MP étudiés à travers (outre PL/SQL) : PHP (BD2Miage : Java)

Rappel du problème

- La situation :
  - Un client veut modifier
    - L'horaire d'un train
    - Les réservation d'autres clients
- Il faut :
  - Un client ne doit pas pouvoir, mais un employé si
  - Cas général :
    - N'importe qui
    - Ne doit pas pouvoir faire n'importe quoi
    - Sur n'importe quelles données

Exemple : analyse du problème

- Personne toto
- Cas 1 : toto non déclaré dans l'application SNCF
  - Veut y accéder
  - Problème : cela ne respecte pas le cahier des charges (clients et employés doivent être connus)

- Cas 2 : toto déclaré dans l'application SNCF
  - toto exécute :

    update train

    set nom = 'toto'

    where nom = 'titi' and dest = 'St Trop'
  - Problème :
    - Ce triplet (utilisateur, action, objet)
    - Contredit le cahier des charges de la SNCF

principe

- protéger entrée dans système :
  - Notion d'utilisateur : connexion que si déclaré
- une fois dedans, limiter les accès :
  - Notion d'autorisation : accès objet que si autorisé

définition

- Un *utilisateur* est défini par un nom (et mot de passe) lui permettant de se connecter au SGBD
- une *autorisation* est un triplet (utilisateur, action, objet)
- le *langage de gestion de la confidentialité* est le sous-ensemble de SQL (ordres BD) qui permet :
  - À l'administrateur de : créer/détruire un utilisateur
  - À chaque utilisateur de : donner/retirer une autorisation sur les objets qu'il possède

Outils fournis par le SGBD

- Langage gestion confidentialité :
  - En particulier : pour chaque application, chaque utilisateur (dont programmeur) définit qui a le droit de faire quoi sur ses propres objets
- Comportement SGBD :
  - maintient liste toutes autorisations
  - Tout ce qui n'est pas autorisé est interdit
  - Détection automatique mises à jour violant autorisations déclarées
  - Refus de ces mises à jour (non effectuées)
  - attention : transaction en cours pas annulée

Objets et leurs actions, utilisateurs

- Table : insert, update, delete, select, alter, index (all)
- Séquence : utiliser
- Procédure : exécuter
- Autres objets et autres actions (hors programme)
- Vocabulaire : action appelée *privilège*
- Utilisateurs : utilisateurs SGBD (public)

exemple

- Le problème ci-dessus est géré comme suit
- le programmeur de l'application, tutu, utilisateur SGBD, propriétaire des tables, tape ordres SQL :
  - Donner l'autorisation (toto, select, train) :

```
grant select
on train
to toto    -- client
```

  - Donner les autorisations (tata, select, réservation) et (tata, update, réservation) :

```
grant select, update
on réservation
to tata    -- employé
```

- Retirer l'autorisation (tata, update, réservation)

  revoke update

  on réservation

  from tata

Ordres SQL

- grant privilège(s)

  on objet

  to utilisateur(s)
- revoke
- Accéder objet de riton autorisé : riton.t
  - Ex : select * from riton.t

Autorisations explicites et implicites

- Une autorisation peut être accordée :
  - Par un ordre explicite de confidentialité : grant/revoke
  - Automatiquement (implicitement) pour chaque utilisateur : sur propres tables
- Autorisation implicites :
  - Tous ordres SQL de mise à jour (dont création) sur ses propres tables
- Autorisations sur les tables des autres :
  - selon autorisations explicites

remarque

- limitations :
  - propriété (admise, TD) : il existe des « autorisations » qu'il est impossible de définir avec SQL
- les pallier ?
  - énoncer l'autorisation en français en commentaire (TD)
  - programmation : vu bientôt

motivation

- Les objets sont tous les objets du SGBD (en gros)
- Les actions sont tous les ordres SQL (en gros), chacun portant sur l'objet correspondant
- Comparaison avec les fichiers Unix (rwx) : comparable

Compétences à acquérir

- Analyse : savoir dire ce que fait une séquence d'ordres SQL dans un contexte d'autorisations donné
- Construction : accorder les droits adéquats à une situation donnée

démonstration

- 2 comptes
- exemples
- anomalies (ex)