Systèmes de Gestion de Bases de Données - 2e

Chapitre 6 - Confidentialité des données

Daniel Schreurs

14 février 2022

Haute École de Province de Liège

Table des matières du chapitre i

Introduction

Table des matières de la section : Introduction i

Introduction : Définition

La sécurité des données est un terme général contenant trois grands types de contrôle :

- Le contrôle d'accès au système par des utilisateurs non identifiés ;
- Le contrôle de l'accès illégal aux données ou confidentialité ;
- Le contrôle de la modification invalide des données ou intégrité.

Introduction : Définition

Le contrôle d'accès au système par des utilisateurs non identifiés ;
On suppose que l'**identification de l'utilisateur** est prise en charge par le système d'exploitation.

Introduction : Définition

Le contrôle de la modification invalide des données ou intégrité.
Le contrôle de l'intégrité est vaste. La gestion de la concurrence a été abordée au chapitre 5, l'intégrité sémantique le sera au chapitre 8 (contraintes d'intégrité et déclencheurs), la reprise après panne sort du cadre du cours.

Introduction : Définition

Le contrôle de l'accès illégal aux données ou confidentialité ;
Dans ce chapitre, nous allons donc nous attarder sur la confidentialité. Plus précisément, nous nous limiterons au contrôle des autorisations d'accès.

Introduction : Que signifie ”confidentialité” ?

4 grandes classes de techniques propres à assurer la confidentialité d’un système manipulant des données :

- Contrôle du flux des données,
- Contrôle d’intégrité
- Encryptage des données
- Contrôle des autorisations d’accès

Introduction : Que signifie ”confidentialité” ?

Les 3 premières (contrôle du flux des données, contrôle d’intégrité et chiffrement des données) sont impossibles à mettre en œuvre au moyen de SQL seul, ils font appel à des techniques particulières qui dépassent le cadre du cours. Nous étudierons en détail le contrôle des autorisations d’accès.

Mécanisme d’octroi et annulation de privilèges

Mécanisme d'octroi et annulation de privilèges : Deux types

Les privilèges sont de deux types :

- Les privilèges de niveau système
  - Permettent la création, modification, suppression de groupes d'objets. Exemple : `CREATE TABLE`, `CREATE VIEW`, `CREATE SEQUENCE`, permettent, à l'utilisateur qui les a reçus de créer des tables, des vues et des séquences.

  Les privilèges de niveau Objet
  - Permettent les manipulations sur des objets spécifiques. Exemple : les privilèges `SELECT`, `INSERT`, `UPDATE`, `DELETE` sur la table `INFOSOFT.employes` permettent à l'utilisateur qui les a reçus de sélectionner, ajouter, modifier et supprimer des lignes dans la table EMPLOYES appartenant à l'utilisateur INFOSOFT.

Mécanisme d’octroi et annulation de privilèges : Assigner des privilèges

Assigner des privilèges système à un utilisateur

- Lorsqu’un utilisateur est créé avec l’instruction CREATE USER, il ne dispose d’aucun droit. Il ne peut même pas se connecter à la base !
- Il doit pouvoir se connecter, créer des tables, des vues, des séquences. Pour lui assigner ces privilèges de niveau système, il faut utiliser l’instruction `GRANT`

Mécanisme d'octroi et annulation de privilèges : Assigner des privilèges

Assigner des privilèges système à un utilisateur

```
1 GRANT CREATE SESSION TO nom_utilisateur;
2 GRANT CREATE TABLE TO nom_utilisateur;
3 GRANT CREATE VIEW TO nom_utilisateur;
4 --OU
5 GRANT CREATE SESSION, CREATE TABLE,
6     CREATE VIEW
7     TO nom_utilisateur;
```

Mécanisme d’octroi et annulation de privilèges : Assigner des privilèges

La liste des privilèges système assignés à l’utilisateur au cours de sa session est visible via la vue `SESSION_PRIVS` Pour les voir, il suffit donc d’exécuter l’instruction : `SELECT * FROM SESSION_PRIVS;`

Mécanisme d’octroi et annulation de privilèges : Assigner des privilèges

Au centre des mécanismes d’octroi/annulation et de contrôle des autorisations se trouve le dictionnaire des données (ou méta-base) dans lequel sont enregistrées toutes les autorisations d’accès.
Pour SQL2, les privilèges sont enregistrés dans les tables `TABLE_PRIVILEGES`, `COLUMN_PRIVILEGE` et `USAGE_PRIVILEGES` (`all_tab_privs` en Oracle)

Mécanisme d'octroi et annulation de privilèges : Assigner des privilèges

Le contrôle des autorisations (niveau objet)
Le mécanisme d'octroi/annulation des privilèges permet à l'ADB ou à toute personne autorisée d'accorder ou de retirer les privilèges à des `sujets` sur des **objets.**

- **Sujets** : un utilisateur, un groupe d'utilisateur, tous les utilisateurs
- **Objets** : la base de données, les tables, les vues, les index, les procédures stockées, …
- **Privilèges** : varient d'un SGBD à l'autre, mais au minimum `SELECT`, `INSERT`, `DELETE`, `UPDATE`

Mécanisme d’octroi et annulation de privilèges : Assigner des privilèges

Le mécanisme de contrôle d’autorisation est le mécanisme qui vérifie qu’un sujet donné a le droit d’effectuer une requête précise (lecture, mise à jour d’une table, création d’une table, …) sur un objet. Ce contrôle est effectué en consultant les tables de la méta base.

Mécanisme d’octroi et annulation de privilèges : Assigner des privilèges

Principes généraux :

- Un utilisateur possède automatiquement tous les privilèges sur un objet qui lui appartient
- Un utilisateur ne peut pas donner plus de privilèges qu’il n’en a reçus
- S’il n’a pas reçu le privilège avec l’option `WITH GRANT OPTION`, un utilisateur ne peut pas donner à son tour ce privilège à un autre utilisateur

Mécanisme d'octroi et annulation de privilèges : Assigner des privilèges

Octroi de privilèges (niveau objet)

```
accorder_privilege ::=
 GRANT privilege ON objet TO utilisateur
 [ WITH GRANT OPTION];
```

- **privilege** `SELECT`, `INSERT`, `INSERT(x)`, `UPDATE`, `UPDATE(x)`, `DELETE`, `ALL` (= tous les privilèges que le donneur peut accorder sur l'objet)
- **objet** liste de tables, vues ou colonnes précédée de TABLE ou VIEW suivant qu'il s'agit d'une table ou d'une vueutilisateur liste d'utilisateurs ou `PUBLIC`
- `WITH GRANT OPTION` : permet au donneur d'indiquer que le receveur pourra transmettre les privilèges qu'il reçoit.

Mécanisme d'octroi et annulation de privilèges : Assigner des privilèges

Exemple : Le directeur possède tous les privilèges sur la table RESULTATS et peut les transmettre.

```
1 GRANT ALL ON TABLE resultats TO directeur WITH GRANT
      OPTION;
2 --Les deux secrétaires peuvent uniquement insérer dans
      la table  :
3 GRANT INSERT ON TABLE resultats TO srt_un, srt_deux;
4 --Les professeurs peuvent lire le contenu de la table et
       modifier le contenu de la colonne points :
5 GRANT SELECT, UPDATE (points) ON TABLE resultats TO
      prof_un, prof_deux, … , prof_n;
```

Mécanisme d’octroi et annulation de privilèges : Assigner des privilèges

Privilège objet et utilisateur ont la même signification que celle de la commande GRANT

```
retirer_privilege ::=
 REVOKE privilege ON objet FROM utilisateur;
```

```
REVOKE SELECT ON TABLE t FROM Obelix;
```

Complément SQL2

Complément SQL2 : Assigner des privilèges

Pour plus d'information, voir le livre de référence.

Les possibilités d’Oracle

Les possibilités d’Oracle : Assigner des privilèges

Pour plus d’information, voir le livre de référence.

Les possibilités d'Oracle : Assigner des privilèges

Pour plus d'informations, consulter le site : oracle.developpez.com