



Institut catholique des arts et métiers
Université catholique d'Afrique centrale - Université Loyola du Congo

Systèmes de gestion de bases de données *Contrôle d'accès*

MCED_SGBD_12

Christina KHNAISSER (christina.khnaisser@usherbrooke.ca)

Luc LAVOIE (luc.lavoie@usherbrooke.ca)

(les auteurs sont cités en ordre alphabétique nominal)

CoFELI/Scriptorium/SGBD_12-Contrôle-d'accès, version 1.0.0.a, en date du 2025-05-05

Document de travail

Plan

Introduction	3
1. SŽcuritŽ des bases de donnŽes	4
2. Contr TM le dŃacc•s.	14
Conclusion	33

Introduction

Le présent module traite de la définition et de la mise en oeuvre d'une politique de contrôle des accès au sein d'un SGBD.

1. S curit  des bases de donn es

La s curit  des bases de donn es est un vaste domaine qui aborde de nombreuses questions, dont les suivantes:

-   Les r gles juridiques et  thiques concernant l'acc s et la diffusion de l'information et des donn es.
-   La politique de s curit  de l'information et des donn es  tablie par l'organisation.
-   La cat gorisation en regard de cette politique des utilisateurs, des donn es et des informations d tenues, transitant ou accessible au sein ou depuis l'organisation.
-   La localisation des utilisateurs, des donn es et des moyens d'acc s aux donn es et aux informations au sein de l'organisation.
-   Le recensement des menaces anticip es.

¥ Les dispositions ^ prendre, ^ maintenir, ^ vřrifier et ^ valider afin de faire respecter la politique en fonction de la catřgorisation et de la localisation des utilisateurs, des moyens d'acc•s, des donnřes tout en prenant en compte le recensement des menaces identifiřes.

1.1. Portée

La portée du présent document est présentement limitée à la présentation d'un cadre général permettant de définir les dispositifs applicables aux bases de données.

1.2. Menaces

Perte de l'intégrité

La perte de l'intégrité découle essentiellement de modifications inappropriées. La modification comprend la création, l'insertion, la suppression et la mise à jour de données. L'intégrité est perdue si des modifications non autorisées sont apportées aux données par des actions intentionnelles ou accidentelles. Les données corrompues peuvent entraîner des inexactitudes, des fraudes ou des décisions erronées.

Perte de disponibilité

La perte de disponibilité fait référence à l'incapacité d'accéder aux données auxquelles un agent a un droit d'accès légitime.

Perte de confidentialit 

La perte de confidentialit  fait r f rence   la divulgation non autoris e, non anticip e ou non intentionnelle des donn es. Cela peut entra ner une perte de confiance du public ou une action en justice contre l'organisation.

1.3. Définitions

Pour protéger les bases de données contre les menaces, il est nécessaire de mettre en oeuvre quatre types de mesures de contrôle:

- ¥ le contrôle d'accès,
- ¥ le contrôle d'intégrité,
- ¥ le contrôle de flux et
- ¥ le chiffrement.

Les agents ayant accès au SGBD ont différents privilèges qui leur donnent des habiletés à consulter et à modifier la structure et les données.

Le SGBD fournit un mécanisme de privilèges permettant à certains agents ou groupes d'agents d'accéder à des parties sélectionnées d'une base de données sans avoir accès au reste de la base de données.

Agent

Utilisateur (*user*), groupe d'utilisateurs (*user group*).

Objet

Entité contributive ^ une base de données!

¥ relation, voire une partie de celle-ci (tuple, attribut)!

¥ type, voire une partie de celui-ci (contrainte)!

¥ routine!

¥ agent, voire des regroupements ou des classes d'agents!

¥ É

Action

Opération définie sur une classe d'objets.

Accéder

Effectuer une action sur un objet.

Privilege

Droit exclusif accordé à un agent d'accéder à objet.

Compte

Ensemble des paramètres permettant à un agent-utilisateur d'établir une connexion avec un service (ici un SGBD).

Gérer les droits d'accès

Spécifier la capacité d'un agent à exécuter une action sur un objet.

Contrôler les droits d'accès

Procéder la vérification du respect de la spécification lors de l'exécution d'une action sur un objet par un agent.

2. Contrôle d'accès

Les responsabilités du DBA (*database administrator*) comprennent

- ¥ la classification des données conformément à la politique de sécurité;
- ¥ la classification des agents conformément à la politique de sécurité;
- ¥ l'octroi de privilèges aux agents qui utilisent le système

Le DBA dispose d'un compte d'administration (utilisateur du système, superutilisateur) qui offre tous les privilèges.

Par exemple:

- ¥ la création/suppression d'agents,
- ¥ la création/suppression de bases de données,
- ¥ l'octroi de privilèges,
- ¥ la révocation de privilèges,
- ¥ É

Le SGBD permet d'accorder des privilèges à un agent spécifique pour effectuer des actions sur des objets spécifiques de la base de données.

Ainsi, le fait d'avoir un compte ne donne pas nécessairement droit à toutes les fonctionnalités fournies par le SGBD.

2.1. Intermédiaires du contrôle d'accès

2.1.1. Agents: Utilisateurs (USER) et Groupes (GROUP)

USER

Un agent ayant la capacité de s'authentifier et la possibilité d'établir une connexion avec le SGBD.

GROUP

Un ensemble d'agents défini en énumérant les USER et les GROUP qui le composent.

2.1.2. RTMles (ROLE)

Un rTMle est l'ensemble des privilèges nécessaires à la réalisation d'un ensemble de tâches connexes pouvant être confiées à un agent. C'est l'instrument de découplage entre les agents et les privilèges. Les rTMles peuvent être organisés selon une structure hiérarchique d'inclusion..

Commandes requises

- ¥ Définir les privilèges d'un rTMle.
- ¥ Assigner un rTMle à un utilisateur.

L'agent se voit octroyer tous les privilèges de tous les rTMles qui lui ont été assignés.

RTMle owner

Pour contrTMler l'octroi et la rTMvocation des privil•ges sur un objet, chaque objet d'une base de donnŽes se voit attribuer un rTMle de propriŽtaire correspondant initialement \wedge l'agent l'ayant crŽŽ.

Le propriŽtaire dispose de tous les privil•ges sur l'objet.

Le propriŽtaire peut transmettre les privil•ges \wedge d'autres agents en octroyant le rTMle appropriŽ (donc les privil•ges associŽs).

2.2. Actions du contrôle d'accès

¥ Création

¥ Mise à jour

¥ Suppression

¥ Recherche

¥ Exécution

2.3. Objets du contrôle d'accès

2.3.1. Données

¥ Table

¥ Vues

¥ Tuple(t)

¥ Attribut

Contrainte d'accès sur des tuples d'une relation

Le propriétaire A de la table R souhaite qu'un autre agent B ne puisse récupérer que certains tuples de R. A doit créer une vue V de R avec une restriction pour sélectionner les tuples concernés, puis accorder à B l'autorisation SELECT sur V.

Contrainte d'accès sur un attribut d'une relation

Le propriétaire A de la table R souhaite qu'un autre agent B ne puisse récupérer que certains attributs de R. A doit créer une vue V de R qui ne comprend que ces attributs, puis accorder à B l'autorisation SELECT sur V.

2.3.2. Routines

¥ Fonctions

¥ ProcŽdures

¥ Automatismes

2.3.3. Types

¥ Types

¥ Domaines

¥ *Large objects*

2.3.4. Structures

¥ Base de donnŽes

¥ SchŽmas de donnŽes

2.4. Propagation des privilèges

Un agent peut avoir un droit de propager les privilèges qu'il possède.

Par exemple, l'agent A1 octroie le droit de recherche sur une relation R à A2 avec le droit de propagation. A2 peut à son tour octroyer les droits de recherche à A3. Si A1 révoque le droit de recherche sur la relation R à A2, le SGBD révoque automatiquement le droit à A3.

2.5. Droits d'accès

2.5.1. PostgreSQL

droit-access ::=

Ê SELECT

Ê | INSERT

Ê | UPDATE

Ê | DELETE

Ê | TRUNCATE

Ê | REFERENCES

Ê | TRIGGER

Ê | CREATE

Ê | CONNECT

Ê | TEMPORARY

Ê | EXECUTE

Ê | USAGE
Ê | SET
Ê | ALTER SYSTEM
Ê | ...

type-object ::=

Ê TABLE
Ê | TYPE
Ê | ROUTINE
Ê | ...

2.5.2. Exemple

Soit un SGBD avec 4 agents-utilisateur: A1, A2, A3 et A4.

A1 doit pouvoir créer des relations.

Le DBA octroie le privilège suivant:

```
grant create table to A1;
```

Si A1 peut créer des relations, mais seulement dans un schéma spécifique 'S1'.

A1 octroie le privilège suivant:

```
grant create table to A1 on schema 'S1';
```

ou

```
create schema 'S1' authorization A1;
```

A1 crée deux relations R1 et R2. A1 possède tous les privilèges sur R1 et R2. A1 veut permettre à A2 d'insérer ou de supprimer des tuples dans R1 sans propagation.

Le A1 octroie le privilège suivant:

```
grant insert, delete on R1 to A2
```

A1 veut permettre à A3 de chercher des informations dans R1 et R2 avec propagation.

Le A1 octroie le privilège suivant:

```
grant select on R1, R2 to A3 with grant option;
```

A3 veut permettre à A4 de chercher des informations dans R1.

A3 octroie le privilège suivant:

```
grant select on R1 to A4;
```

A1 veut empêcher A3 de chercher de l'information dans R1.

Le A1 révoque le privilège suivant:

```
revoke select on R1 to A3;
```

Le SGBD doit automatiquement révoquer ce privilège à A4.

A1 veut permettre à A3 d'avoir un accès sur certains attributs (a et b) et certains tuples (attribut a > 60) de la relation R1 avec propagation.

Le A1 doit exécuter les instructions suivantes:

```
create view A3_R1
  Ê select a, b
  Ê from R1
  Ê where a > 60;
```

```
grant select on A3_R1 to A3 with grant option;
```

Quiz

Un problème va se produire. Lequel? Pourquoi?

Conclusion

La sécurité des bases de données est un grand sujet qui mérite d'être étudié en profondeur.

Un SGBD offre des mécanismes de protection sur l'ensemble ou une portion des données.

Utilisez-les adéquatement selon la politique d'accès mise en place par l'organisation.

!

Produit le 2025-05-06 11:53:37 UTC



Institut catholique des arts et métiers
Université catholique d'Afrique centrale - Université Loyola du Congo