



Collectif francophone pour l'enseignement libre de l'informatique

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/Scriptorum/SGBD_12-Controle-d-acces, version 1.0.0.a, en date du 2025-05-05

— document de travail —

Sommaire

Introduction aux stratégies de contrôle d'accès applicables aux systèmes de gestion de bases données.

Mise en garde

Le présent document est en cours d'élaboration ; en conséquence, il est incomplet et peut contenir des erreurs.

Historique

diffusion	resp.	description
2025-05-05	LL	Restructuration
2024-10-27	CK	Ébauche initiale à partir d'Elmasri 2016 chapitre 30.
2024-04-01	LL	Ébauche initiale selon les formats contenus dans CoLOED:AsciiDoc.

Table des matières

Introduction.....	4
1. Sécurité des bases de données.....	4
1.1. Portée.....	4
1.2. Menaces.....	4
1.3. Définitions	4
2. Contrôle d'accès	5
2.1. Intermédiaires du contrôle d'accès	6
2.2. Actions du contrôle d'accès	6
2.3. Objets du contrôle d'accès	6
2.4. Propagation des privilèges	7
2.5. Droits d'accès	7
Conclusion.....	10

Introduction

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

1. Sécurité des bases de données

La sécurité des bases de données est un vaste domaine qui aborde de nombreuses questions, dont les suivantes :

- Les règles juridiques et éthiques concernant l'accès et la diffusion de l'information et des données.
- La politique de sécurité de l'information et des données établie par l'organisation.
- La catégorisation en regard de cette politique des utilisateurs, des données et des informations détenues, transitant ou accessible au sein ou depuis l'organisation.
- La localisation des utilisateurs, des données et des moyens d'accès aux données et aux informations au sein de l'organisation.
- Le recensement des menaces anticipées.
- Les dispositions à prendre, à maintenir, à vérifier et à valider afin de faire respecter la politique en fonction de la catégorisation et de la localisation des utilisateurs, des moyens d'accès, des données tout en prenant en compte le recensement des menaces identifiées.

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

Parmi les principales menaces relatives aux bases de données qui peuvent entraîner la perte ou la dégradation de tout ou une partie des objectifs de sécurité, le présent document s'intéresse plus particulièrement aux suivantes.

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 confidentialité

La perte de confidentialité fait référence à la divulgation non autorisée, non anticipée ou non intentionnelle des données. Cela peut entraîner 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'inférence,
- le contrôle de flux et
- le chiffrement.

Le contrôle d'accès s'assure que toute donnée ou information n'est accédée que par un utilisateur en ayant le droit.

Le contrôle d'inférence concerne la protection des données issues d'un calcul statistique.

Le contrôle de flux concerne la régulation du flux de l'information entre les objets d'une base de données.

Le chiffrement est un procédé qui vise à rendre la compréhension d'une information (donnée, document) impossible à toute personne qui n'a pas la clé de 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 à 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;
- ...

Action

Opération définie sur une classe d'objets.

Accéder

Effectuer une action sur un objet.

Privilège

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,
- ...

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. Rôles (ROLE)

Un rôle 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 rôles peuvent être organisés selon une structure hiérarchique d'inclusion..

Commandes requises

- Définir les privilèges d'un rôle.
- Assigner un rôle à un utilisateur.

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

Rôle owner

Pour contrôler l'octroi et la révocation des privilèges sur un objet, chaque objet d'une base de données se voit attribuer un rôle de propriétaire correspondant initialement à l'agent l'ayant créé.

Le propriétaire dispose de tous les privilèges sur l'objet.

Le propriétaire peut transmettre les privilèges à d'autres agents en octroyant le rôle approprié (donc les privilèges associés).

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

Contrôle 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.

Contrôle 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
- Procédures
- Automatismes

2.3.3. Types

- Types
- Domaines
- *Large objects*

2.3.4. Structures

- Base de données
- Schémas de données

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-accès ::=  
    SELECT  
    | INSERT  
    | UPDATE  
    | DELETE
```

```
| TRUNCATE  
| REFERENCES  
| TRIGGER  
| CREATE  
| CONNECT  
| TEMPORARY  
| EXECUTE  
| USAGE  
| SET  
| ALTER SYSTEM  
| ...
```

```
type-d'objet ::=  
TABLE  
| TYPE  
| ROUTINE  
| ...
```

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 octroi 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 octroi 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
  select a, b
  from R1
  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 2025-11-13 06:05:14 -0500



Collectif francophone pour l'enseignement libre de l'informatique