Ch8:Sécurisation d'une Base de Données

I. Les piliers de la sécurité des BD :

- **Authentification**

Elle consiste à s'assurer de l'identité d'un utilisateur avant de lui donner l'accès à une base de données (Mot de passe, login, certification, …) ;

- **Confidentialité**

L'administrateur de la BD donne un certain nombre de droits et de ressources en fonction d'un profil (rôles) bien maintenu à l'ensemble des utilisateurs ;

- **Disponibilité**

Des mécanismes de sauvegarde variés doivent être mis en place pour assurer la disponibilité (mécanismes de journalisation, de reprise et restauration, …) ;

- **Intégrité**

Il s'agit de satisfaire les contraintes d'intégrité à fin de respecter la cohérence des données dans une BD répartie ou non répartie ;

- **Traçabilité**

En cas de problème, on doit recourir à une analyse de traces ou de journaux concernant l'aspect système, les caractéristiques réseaux, l'accès aux données, …

II. Les mécanismes de mis en œuvre de la sécurité:

Les SGBD offre un certain nombre de mécanismes pour satisfaire la sécurité de la BD.

- **L'authentification**

Est le processus qui contrôle l'identité de l'utilisateur grâce à un mot de passe, un login, un nom utilisateur, une adresse IP,… ;

- **Les droits et privilèges**

C'est la gestion des droits accordés à un individu ou à un groupe d'individus ;

- **Les LOGs ou traces**

Les traces permettent d'enregistrer périodiquement tout ou partie des informations selon le droit d'accès attribué;

- **Tolérance aux pannes**

Il s'agit de supporter partiellement ou complètement des différents types de pannes (au niveau client, serveur, réseau) à l'aide de l'utilisation d'un certain matériels et de logiciels ;

- **Sauvegarde et restauration**

Il s'agit de sauvegarder les données sur des supports de stockage externes dont le but de restaurer le système en cas de panne, de fausse manipulation.

- **Mécanismes transactionnels**

Il s'agit de créer une image à la BD avant toute modification à fin de maintenir la cohérence des données.

II. Gestion des droits d'accès:

- **Définir un mot de passe pour une base mono utilisateur (Marche à suivre)**
  1) Le menu Fichier =>Ouvrir=>Ouvrir en exclusif
  2) Le menu Outil=>Sécurité=>Définir le mot de passe de la base de données
  3) Choisir un mot de passe (page 213)
- **Sécuriser les accès à une Base de Données (Marche à suivre)**
  1) ouvrir la Base de Donnée
  2) Le menu Outil=>Sécurité=>Autorisations d'accès
  3) Fixer les droits d'accès à votre base (page 214)

IV. Cryptage d'une base de données:

Crypter la base de données permet de rendre le déchiffrement par un éditeur de texte totalement impossible.(Marche à suivre)

1) ouvrir la Base de données
2) Le menu Outil=>Sécurité=>Coder /Décoder une base de données (page 215)

V. Gestion des utilisateurs:

Il s'agit de créer des groupes de travail pour contrôler les droits d'accès aux données et les modifications de structure de la base.

- **Via l'assistant (marche à suivre)**

1) ouvrir la Base de données
2) Le menu Outil=>Sécurité=>assistant sécurité au niveau utilisateur
3) créer un nouveau fichier de groupe de travail
4) suivre les fenêtres (page 218-219-220)

- **Manuellement (marche à suivre)**

1) ouvrir la Base de données
2) Pour créer un fichier de groupe de travail (Outil=>Sécurité=>administrateur de groupe de travail)
3) Outil=>Sécurité=>gestion des utilisateurs et des groupes
4) Outil=>Sécurité=>Autorisation d'accès

VI. Intégrité des données:

L'intégrité des données se répartit entre les catégories suivantes :

- **L'intégrité d'entité (clé primaire)**
- **L'intégrité de domaine (**les valeurs de colonnes doivent être valides)
- **L'intégrité référentielle (**les relations définies entre les tables)
- **Intégrité définie par l'utilisateur**

VII. Sauvegarde et restauration de bases de données:

- **Sauvegarde :** Une copie de données qui peut être utilisée pour restaurer et récupérer des données =>Archivage est une solution pour restaurer la BD en cas de problèmes matériels ou logiciels.

VIII. Contrôle données dans le langage SQL:

1. Création des utilisateurs

```
CREATE USER nom_utilisateur
IDENTIFIEDY BY  mot_de _passe
```

Exp : 1. créer l'utilisateur PROF avec le mot de passe : "info"

```
CREATE USER ELEVE
IDENTIFIEDY BY  4sibd
```

2. créer l'utilisateur ELEVE avec le mot de passe : "4sibd"

……

……

2. Attribution des droits :

Les privilèges sont :

SELECT	Droit de lecture
INSERT	Droit d'insertion de lignes
UPDATE	Droit de modification de lignes
UPDATE (Attr1, Attr2, …)	Droit de modification de lignes limité à certains attributs
DELETE	Droit de suppression de lignes
ALTER	Droit de modification de la structure de la table
INDEX	Droit de création d'index
ALL	Tous les droits

Application :

a. Les droits globaux ou droits systèmes

Attribuer des droits sur l'accès et l'utilisation de toute la BD :

```
GRANT  ALL/droit1, droit2,…droit N
TO  public / utilisateur1, utilisateur2, …, utilisateurp
[WITH ADMIN OPTION]
```

Rque :

- **ALL** => désigne tous les droits
- **PUBLIC** => désigne tous les utilisateurs
- **WITH ADMIN OPTION :** autorise le nouvel utilisateur à accorder les droits reçus à d'autres utilisateurs.

Exp : 1. attribuer tous les droits à l'utilisateur Prof avec l'option d'administration

GRANT ALL
TO prof
WITH ADMIN OPTION

2. accorder les droits de recherche et d'insertion à l'utilisateur ELEVE

……

……

3. accorder le droit de recherche à tout le monde

……

……

3. Les droits d'objets :

Attribuer des droits sur l'accès et l'utilisation d'une table ou d'une vue de la BD :

GRANT ALL /droit1, droit2,…droit N
ON objet
TO public / utilisateur1, utilisateur2, …, utilisateurp
[WITH GRANT OPTION];

Rques :

- **WITH GRANT OPTION** autorise le nouvel utilisateur à accorder les droits reçus à d'autres utilisateurs.

Exp : 1. attribuer tous les droits à l'utilisateur Prof sur la table client avec l'option d'administration

GRANT ALL
On client
TO prof
WITH GRANT OPTION

2. accorder les droits de recherche et de mise à jour à l'utilisateur ELEVE sur la table facture

……

……

3. accorder les droits de recherche à tous les utilisateurs sur la table facture

……

……

3. Suppression des droits :

Permet de retirer un ou plusieurs droits accordés sur la base ou sur un objet

REVOKE ALL/droit1, droit2, … droitn
[ON objet**]**
FROM Public/utilisateur1, utilisateur2, …, utilisateurn ;

Exp :

1. retirer le droit suppression de l'utilisateur Prof sur la table client

REVOKE delete
On client
From prof

2. supprimer les droits de recherche et de mise à jour de l'utilisateur ELEVE sur la table facture

……

……

……

3. retirer tous les droits de tous les utilisateurs de la base

……

……