Sécurisation d'une base de données

I. Introduction :

La manipulation des données personnelles est devenue l'une des opérations courante d'une base de données, ce qui menace les droits des personnes et touche leur vie privée. D'où l'apparition d'un ensemble de mécanismes assurant un niveau de sécurité.

II. Les concepts de base de la sécurité des BD :

1. Authentification :

Avant d'accéder à une base de données l'utilisateur doit identifier, tout en tapant un mot de passe, login…

2. Confidentialité :

Chaque personne connectée à une base de données à un ensemble de ressources et de droits propre à lui définies par un administrateur.

3. Disponibilité :

Des mécanismes de sauvegarde variés doivent être mis en place pour éviter la perte d'information et pour quelle soit toujours disponible.

4. Intégrité :

Les informations d'une base de données doivent êtres cohérentes et doivent satisfaire les contraintes d'intégrités, tant qu'il y a des accès concurrents d'utilisateurs, notamment lors de mises à jour.

5. Traçabilité :

En cas de problème important au niveau de système, on peut recourir à l'analyse de traces ou de journaux.

III. Les mécanismes mise en œuvre pour la sécurité :

1. Authentification :

C'est un processus qui contrôle l'identité de l'utilisateur. Dans certain cas l'authentification peut être implicite ou reconnue automatiquement (adresse IP de l'utilisateur sur le réseau par exemple).

2. les privilèges :

Tout objet possède un créateur. Ce créateur possède tous les privilèges sur cet objet.
Un privilège est le droit d'exécuter un type d'instruction spécifique. Un rôle est un regroupement de privilèges, pour simplifier la gestion des utilisateurs.

3. les logs ou trace :

Permettent d'enregistrer tout ou partie des informations concernant les accès.

4. Tolérance aux pannes :

Permet grâce à des logiciels et matériels de supporter différents types de pannes à un certain coût.

5. Mécanismes transactionnels :

Avant modification l'information est stockées plusieurs fois dans ou hors la BD. Les mécanismes transactionnels permettent de faire d'éventuels retours arrière pour retrouver le dernier état cohérent, ou de s'assurer que la BD n'a pas eu d'opérations incomplètes.

IV. Gestion des droits d'accès :

1. Définir un mot de passe pour une base mono-utilisateur :

Si la base est mono-utilisateur, il est conseillé de définir un mot de passe sur cette base. Si la base est multiutilisateur, il faut créer un mot de passe pour chaque utilisateur.

Activité1 :

1) Charger la base de données existante sur votre poste puis définir un mot de passe.

Démarche à suivre :

1- Ouvrir la base de données en mode exclusif (menu fichier/ouvrir/cliquer sur la flèche à droite).
2- Dérouler le menu outils/sécurité puis définir le mot de passe de la base de données.

Remarque :

Pour le choix d'un mot de passe il faut suivre les règles suivantes :

- Entre 1 et 20 caractères (au minimum 8 caractère)
- Un mot de passe doit contenir des minuscules, majuscule, des chiffres et des symboles.
- Ne peut pas commencer par un espace et ne peut pas contenir les symboles suivante:\ **[] :|<> + = ; , . ?***

2. Définir les droits d'accès à une base de données :

Activité 2 :

Définir les droits d'accès correspondant à votre base de données

Démarche à suivre :

1- ouvrir la base de données
2- Activer le menu outils, /sécurité/autorisations d'accès
3- Fixer les droits d'accès à votre base.
4- valider

3. Cryptage d'une base de données :

Même si on définie un mot de passe pour la base de données c'est possible qu'une personne non autorisée puisse l'ouvrir avec un éditeur de texte. Le cryptage permet de rendre le déchiffrement d'une base de données par un éditeur de texte impossible.

Activité 3 :

1) Crypter la base de données courante.

Démarche à suivre :

1) Ouvrir la base de données
2) Activer le menu outils, /sécurité
3) Sélectionner l'option coder/décoder une base de données
4) valider

4. Gestion des utilisateurs :

Dans une Entreprise la base de données est multiutilisateur. Chaque utilisateur appartient à un service (Ex : Commercial, clientèle…), pour ce la il faut mettre en place des groupes de travail pour contrôler les droits d'accès aux données puis créer des utilisateurs et de les affecter à un ou plusieurs de ces groupes.

a. via l'assistant :

Activité 4 :

1) à l'aide de l'assistant créer des groupes de travail.
2) Créer des utilisateurs et assigner les à un ou plusieurs des groupes déjà définis.

Démarche à suivre :

Pour créer des groupes de données :

1) Ouvrir la base de données
2) Activer le menu outils, /sécurité/assistant sécurité au niveau utilisateur
3) Sélectionner l'option créer un nouveau fichier de groupe de travail (porte l'extension .mdw).
4) Choisir le nom du fichier et son identifiant unique(WID).
5) Choisir les objets sur lesquels vont s'appliquer les stratégies définies dans l'étape précédente.

6) Choisir les groupes de travail prédéfinis. tous les utilisateurs sont membre de groupe utilisateur, par défaut l'assistant n'attribut aucune autorisation au groupe vous pouvez décider de lui attribuer.
7) Créer les utilisateurs un par un on leur donnant un mot de passe et un identifiant unique(PID).
8) Accorder à chaque utilisateur un groupe de travail
9) Donner un chemin d'accès à la copie non sécurisée de la base, en cas où la nouvelle base créer ne vous conviendra pas.
10) Imprimer et stocker de manière sécurisée le rapport assistant sécurité (il contient : les emplacements des BD, des groupes de travail, les utilisateurs avec leurs mots de passe et les permissions accorder aux utilisateurs.

b. manuellement :

Démarche à suivre :

1- Pour créer un fichier de groupe de travail, dérouler le menu Outils/sécurité/administrateur de groupe de travail.
2- Pour créer un groupe de travail, pour affecter un utilisateur à un groupe de travail, pour changer le mot de passe d'un utilisateur dérouler le menu outils/sécurité/gestion des utilisateurs et des groupes.
3- Pour modifier les permissions accorder à un groupe, dérouler le menu Outils/sécurité/autorisations d'accès.

5. Intégrité des données :

Lors de la création des tables il faut passer de deux étapes importantes d'une part identifier les valeurs valides pour une colonne et d'autre part décider de la façon d'appliquer l'intégrité des données dans cette colonne. On trouve plusieurs catégories d'intégrité :

- **Intégrité d'entité :** définit une ligne comme étant une entité unique pour une table particulière.
- **Intégrité de colonne :** fait référence à l'intervalle des entrées valide pour une colonne spécifique.
- **Intégrité référentielle :** préserve les relations définies entre les tables lors de l'insertion ou de la suppression de lignes.
- **Intégrité définie par l'utilisateur :** permet de définir des règles propres à l'entreprise, qui n'appartiennent à aucune des autres catégories

Remarque :

Toutes les catégories d'intégrité acceptent l'intégrité définie par l'utilisateur.

6. Sauvegarde et restauration de base de données :

Les sauvegardes d'une base de données permettent de restaurer les données et d'effectuer des récupérations après de nombreux types d'échecs :

- erreur utilisateur (suppression d'une table)
- défaillances matérielles …

7. Contrôle de données dans le langage SQL :

a- création d'utilisateurs :

L'administrateur d'une base de données peut créer un nouvel utilisateur à l'aide de la commande :

Create user nom_utilisateur
Identified by mot_de_ passe **;**

Jusqu'à maintenant l'utilisateur ne possède aucun droit.il ne peut même pas se connecter.

b- attribution des droits :

Il existe deux types de droits ou (privilèges) :

- **Des droits globaux** sur la base appelés **droits système :**

Permettent à l'utilisateur d'effectuer des opérations globales sur la base de données, Ex : connexion, la sauvegarde de la base de données à l'aide de la commande :

```
Grant droit1, droit2…
To utilisateur1, utilisateur2…
[With Admin option] ;
```

Remarque :

- On peut utiliser Public pour désigner tous les utilisateurs
- **With Admin option** autorise à l'utilisateur à accorder les droits reçus à d'autres utilisateurs.

- **Des droits** sur des objets de la base appelés **droits objet :**

Permettent à l'utilisateur d'effectuer des opérations sur les objets la base de données, tel que les tables, les vues… à l'aide de la commande :

```
Grant droit1, droit2…
On objet
To utilisateur1, utilisateur2…
[With Grant option] ;
```

Remarque :

- On peut utiliser **Public** pour désigner tous les utilisateurs.
- On peut utiliser **ALL** pour désigner tous les droits.
- **With Grant option** autorise à l'utilisateur à accorder les droits reçus à d'autres utilisateurs.

Exemple de droit à accorder : insert, delete, update…

Voir exemple page 224.

c- retrait des droits :

Permet de supprimer un ou plusieurs droits sur un objet :

```
Revoke droit1, droit2…
[On objet]
From utilisateur1, utilisateur2… ;
```

Remarque :

- cette commande valable pour le retrait de droits système ou objet.
- la commande **On objet** utiliser seulement si on veut retirer les droits sur objet
- On peut utiliser **Public** pour désigner tous les utilisateurs.
- On peut utiliser **ALL** pour désigner tous les droits.

Exemple :

```
Revoke All
  On comande
    from Public ;
```