LE LCD (Langage de contrôle des données)

1. Notion d'utilisateur de rôle et de privilège

Chaque utilisateur d'une base de données (comme Oracle ou PostgreSQL par exemple) dispose d'un nom et d'un mot de passe, et possède également des tables, des vues et d'autres ressources qu'il a créées. Dans Oracle, un rôle représente un ensemble de privilèges. Vous pouvez assigner des privilèges spécifiques à des rôles, puis assigner ces rôles aux utilisateurs appropriés. Un utilisateur peut aussi attribuer des privilèges à d'autres utilisateurs s'il a été accrédité pour.

Deux types de privilèges :

 Privilège au niveau système : qui donne le droit d'exécuter une action particulière sur n'importe quel objet. Le privilège CREATE TABLE, par exemple, permet de créer des tables. Le privilège GRANT ANY PRIVILEGE permet d'accorder des privilèges à d'autres utilisateurs.

 Privilège au niveau objet : qui donne le droit d'exécuter une action donnée sur un objet spécifique. Le privilège SELECT, par exemple, permet d'exécuter une opération SELECT sur une table, une vue, une séquence (ou un snapshot sous Oracle).
La norme SQL2 propose trois fonctions pour connaître l'utilisateur connecté : SYSTEM_USER (nom de l'utilisateur connecté), SESSION_USER (nom d'utilisateur qui a ouvert la session), CURRENT_USER (nom de l'utilisateur courant). On utilise ces fonctions avec une commande SELECT.

Créer un utilisateur

```
CREATE USER <utilisateur> IDENTIFIED BY <mot_de_passe> | EXTERNALLY
```

Le paramètre EXTERNALLY permet de ne pas définir de mot de passe si le mot de passe du système d'exploitation de l'ordinateur vous suffit pour identifier l'utilisateur. Stratégie dangereuse tout de même, car il vaut mieux avoir un autre filtre sur la base de donnée qui offre un second niveau de sécurité.
On peut également fixer pour cet utilisateur un espace disque spécifique (TABLESPACE) et une limitation de son utilisation des ressources (QUOTAS).

Modifier le mot de passe des utilisateurs

```
ALTER USER <utilisateur> IDENTIFIED BY <nouveau_mot_de_passe>
```

On peut gérer la « vie » des mots de passe grâce à la création de profils (CREATE PROFILE) qui permettent au DBA de fixer des conditions d'accès :

- durée de vie d'un mot de passe ;
- période de grâce qui suit l'expiration d'un mot de passe et pendant laquelle il peut être changé ;
- nombre d'échecs de connexion répétés autorisés avant de verrouiller le compte ;
- durée (en jours) de verrouillage d'un compte ;
- nombre de jours qui doivent s'écouler avant de pouvoir changer un mot de passe ;
- nombre de changements de mot de passe qui doivent avoir lieu avant de réutiliser un mot de passe.

Supprimer un utilisateur

```
DROP USER <utilisateur> [CASCADE]
```

2. Les rôles standards

Les rôles ont été implémentés dans le langage SQL à partir de 1999. Seules les bases de données solides comme Oracle ont implémenté ces ordres. Les rôles peuvent être apparentés à des groupes, ou des profils qui permettent de définir un ensemble de privilèges à attribuer à des utilisateurs de la base de données.

Il existe trois rôle par défaut dans Oracle :

 CONNECT : Pour les utilisateurs occasionnels qui n'ont normalement pas besoin de créer des tables (même s'ils pourront le faire). Ce rôle autorise simplement d'utiliser Oracle : il permet de créer des tables, des vues, des séquences, des clusters, des synonymes, des sessions et des liens vers d'autres bases de données.
 RESOURCE : Pour les utilisateurs réguliers. Accorde des droits supplémentaires pour la création de tables, de séquences, de procédures, de déclencheurs, d'index et de clusters.
 DBA : Regroupe tous les privilèges de niveau système avec des quotas d'espace illimités et la
possibilité d'accorder n'importe quel privilège à un autre utilisateur. Le compte système est employé par un utilisateur disposant d'un rôle DBA.

3. Les privilèges

GRANT <privilège_système> | <rôle> [,<privilège_système> | <rôle>, ...] TO <utilisateur> | <rôle> [,<utilisateur> | <rôle>, ...] [WITH ADMIN OPTION]

La commande GRANT permet d'accorder n'importe quel privilège système ou rôle à un utilisateur, à un rôle, ou au groupe d'utilisateurs PUBLIC. Si la clause WITH ADMIN OPTION est spécifiée, le bénéficiaire peut à son tour assigner le privilège ou le rôle qu'il a reçu à d'autres utilisateurs ou rôles.

Celui qui attribut un privilège à un rôle peut aussi le révoquer :

REVOKE <privilège_système> | <rôle> [,<privilège_système> | <rôle>, ...] TO <utilisateur> | <rôle> [,<utilisateur> | <rôle>, ...] ...

Un utilisateur qui dispose du rôle de DBA peut révoquer les privilèges CONNECT, RESSOURCE, DBA ou tout autre privilège ou rôle accordés à un autre utilisateur ou administrateur de base de données. Cette commande est donc très dangereuse, c'est pourquoi les privilèges DBA doivent être accordés uniquement aux personnes dont la fonction l'exige.

Nota : Révoquer tous les privilèges d'un utilisateur ne supprime ni son compte ni les objets qu'il possède. Cela l'empêche simplement d'y accéder. Les autres utilisateurs disposant d'un accès aux objets de cet utilisateur peuvent continuer à y accéder comme si de rien n'était.

Pour supprimer l'utilisateur et tous les objets qu'il possède (CASCADE) :

DROP USER <utilisateur> [CASCADE];

Un utilisateur peut accorder des privilèges d'accès à tout objet qu'il possède, alors que l'administrateur de la base peut octroyer n'importe quel privilège système, car le rôle DBA inclut les privilèges GRANT ANY et GRANT ANY ROLE.

L'utilisateur peut accorder les privilèges suivants :
 Sur les tables, vues et snapshot qu'il possède : INSERT, UPDATE, DELETE, SELECT.
 Sur les tables qu'il possède : ALTER, REFERENCES, INDEX, ALL (tous les privilèges évoqués).
 Sur les procédures, fonctions, packages, types de données abstraits qu'il possède : EXECUTE.
 Sur les séquences qu'il possède : SELECT, ALTER.

Administration paramétrée

1. Création de rôles

On peut ajouter à la liste des rôles par défaut d'Oracle (CONNECT, RESOURCE, DBA) des rôles comprenant des privilèges de niveau système ou objet, ou une combinaison des deux.
Pour pouvoir créer des rôles il faut avoir le privilège système CREATE ROLE.

L'instruction suivante permet de créer un rôle :

```
CREATE ROLE <nom_rôle> [NOT IDENTIFIED | IDENTIFIED [BY <mot_de_passe | EXTERNALLY]];
```

Lorsqu'ils viennent d'être créés, les rôles ne sont associés à aucun privilège.

2. Activer ou désactiver des rôles

```
ALTER USER <utilisateur> DEFAULT ROLE [<rôle1>, <rôle2>] [ALL | ALL EXECPT <rôle1>, <rôle2>] [NONE]

ALTER ROLE <nom_rôle>
```

3. Pour désactiver un rôle

```
DROP ROLE <nom_rôle>;
```

Activer ou désactiver un rôle :

```
SET ROLE <nom_rôle>;
SET ROLE NONE;
```

4. Révoquer les privilèges d'un rôle

```
REVOKE <rôle> FROM <nom_rôle>;
```

Exemple : REVOKE SELECT ON PRODUIT FROM CLERK;

5. Suppression d'un rôle

```
DROP ROLE <nom_rôle>;
```