USTHB – Faculté d'Electronique et Informatique
Département Informatique

Architecture de S.G.B.D. relationnels
TP Oracle (2) : Privilèges d'accès à la base de données

Oracle permet à plusieurs utilisateurs de travailler sur la même base de données en toute sécurité.
*Deux commandes sont particulièrement importantes : **GRANT** et **REVOKE** et permettent de définir les droits de chaque utilisateur sur les objets de la base.*
Tout utilisateur accède à la base à l'aide de son nom utilisateur et de son mot de passe. C'est le nom utilisateur qui permet de déterminer les droits d'accès aux objets de la base de données.
Au cours des TP précédents vous avez travaillé seul dans un schéma de nom égal à votre nom d'utilisateur. Nous allons vérifier que le SGBD gère la concurrence d'accès à des objets de la base entre plusieurs utilisateurs différents. Tout utilisateur qui crée des objets est propriétaire de ces objets. Le créateur d'un objet peut décider de donner (ou de supprimer) certains droits d'accès à tout autre utilisateur de sa connaissance.

GRANT privilège [ON table/vue] TO utilisateur [WITH GRANT OPTION]
Cet ordre permet de donner le privilège concerné sur la table ou la vue à l'utilisateur.

Un utilisateur ayant accordé un privilège peut le reprendre à tout moment à l'aide de l'ordre RE-VOKE :
REVOKE privilège ON [table/vue] FROM utilisateur

Les privilèges qui peuvent être donnés sont les suivants :
***SELECT** droit de lecture, **INSERT** droit d'insertion de lignes, **UPDATE** droit de mise-à-jour de lignes, **DELETE** droit de suppression de lignes,*
***ALTER** droit de modification de la définition de la table, **INDEX** droit de création d'index , **ALL** tous les droits ci-dessus.*
Un utilisateur ayant reçu un privilège avec la mention facultative WITH GRANT OPTION peut les transmettre à son tour à un autre utilisateur (User3).

Questions :

1. Connectez-vous avec l'utilisateur **DBAGYMNASE.**
2. Créez un autre utilisateur : **ADMINGYM** qui possède les mêmes tablespaces.
3. Connectez-vous à l'aide de cet utilisateur. Que remarquez-vous ?
4. Donnez le droit de création d'une session pour cet utilisateur (Create Session) et reconnectez-vous.
5. Donnez les privilèges suivants à **ADMINGYM**: créer des tables, des vues et des utilisateurs. Vérifiez.
6. Exécutez la requête Q1 suivante : **Select * from GYMNASES;** Que remarquez-vous ?
7. Donnez le droit de lecture à cet utilisateur pour la table **GYMNASES**. Exécutez la requête Q1 maintenant.
8. On veut supprimer toutes les gymnases qui n'organisent pas de séances. Que faut-il faire ? Que remarquez-vous ?
9. Donner le droit de suppression à cet utilisateur pour la table **GYMNASES** et réessayez de refaire la suppression.
10. Créez un index LIBELLE_IX sur l'attribut LIBELLE de la table **SPORTS**. Que remarquez-vous ?
11. Donnez le droit de création d'index à **ADMINGYM** pour la table **SPORTS**, ensuite réessayez de créer l'index. Que se passe-t-il ?
12. Enlevez les privilèges précédemment accordés.
13. Vérifiez que les privilèges ont bien été supprimés.
14. Créez un profil « **Gymnase_Profil** » qui est caractérisé par : (4 sessions simultanés autorises, Un appel système ne peut pas consommer plus de 30 secondes de CPU, Chaque session ne peut excéder 70 minutes, Un appel système ne peut lire plus de 1300 blocs de donnes en mémoire et sur le disque, Chaque session ne peut allouer plus de 30 ko de mémoire en SGA, Pour chaque session, 20 minutes d'inactivité maximum sont autorisés, 3 tentatives de connexion avant blocage du compte, Le mot de passe est valable pendant 60 jours et il faudra attendre 40 jours avant qu'il puisse être utilisé à nouveau, 1 seul jour d'interdiction d'accès après que les 3 tentatives de connexion ont été atteintes, La période de grâce qui prolonge l'utilisation du mot de passe avant son changement est de 7 jours).
15. Affectez ce profil à l'utilisateur **ADMINGYM**. Vérifiez.
16. Créez le rôle : « **GESTIONNAIRE_DES_GYMNASES** » qui peut voir les tables **SPORTIFS**, **SPORTS**, **GYMNASES** et peut modifier les tables **ARBITRER, ENTRAINER, JOUER et SEANCES.**
17. Assignez ce rôle à **ADMINGYM**. Vérifier que les autorisations assignées au rôle **GESTIONNAIRE_DES_ GYMNASES**, ont été bien transférées sur l'utilisateur à **ADMINGYM**.

La syntaxe SQL de création d'un utilisateur

CREATE USER utilisateur
IDENTIFIED {BY motdePasse | EXTERNALLY | GLOBALLY AS 'nomExterne' }
[DEFAULT TABLESPACE nomTablespace [QUOTA {entier [K | M] | UNLIMITED} ON nomTablespace]]
[TEMPORARY TABLESPACE nomTablespace] [PROFILE nomProfil] [PASSWORD EXPIRE] [ACCOUNT {LOCK |UNLOCK}] ;

- **IDENTIFIED BY mot de Passe** permet d'affecter un mot de passe à un utilisateur local (cas le plus courant et le plus simple).
- **IDENTIFIED BY EXTERNALLY** permet de se servir de l'authenticité du système d'exploitation pour s'identifier Oracle (cas des compte OPS$ pour Unix).
- **IDENTIFIED BY GLOBALLY** permet de se servir de l'authenticité d'un système d'annuaire.
- **DEFAULT TABLESPACE** nomTablespaceassocie un espace disque de travail (appelétablespace) à l'utilisateur.
- **TEMPORARY TABLESPACE** nomTablespaceassocie un espace disque temporaire (dans lequel certaines opérations se dérouleront) à l'utilisateur.
- **QUOTA** permet de limiter ou pas chaque espace alloué.
- **PROFILE** nomProfil affecte un profil (caractéristiques système relatives au CPU et aux connexions) à l'utilisateur.
- **PASSWORD EXPIRE** pour obliger l'utilisateur à changer son mot de passe à la première connexion (par défaut il est libre). Le DBA peut aussi changer ce mot de passe.
- **ACCOUNT** pour verrouiller ou libérer l'accès à la base (par défaut UNLOCK).

La syntaxe SQL de Création d'un Profil

CREATE PROFILE nomProfil
LIMIT { Paramètre Ressource | Paramètre Mot de Passe } [Paramètre Ressource | Paramètre Mot de Passe];

Paramètre Ressource : {{SESSIONS_PER_USER|CPU_PER_SESSION|CPU_PER_CALL|CONNECT_TIME|
IDLE_TIME|LOGICAL_READS_PER_SESSION|LOGICAL_READS_PER_CALL | COMPOSITE_LIMIT}{entier | UNLIMITED | DEFAULT } |
PRIVATE_SGA {entier[K|M] | UNLIMITED | DEFAULT}}
Paramètre Mot de Passe : { FAILED_LOGIN_ATTEMPTS | PASSWORD_LIFE_TIME | PASSWORD_REUSE_TIME | PASSWORD_REUSE_MAX | PASSWORD_LOCK_TIME | PASSWORD_GRACE_TIME } { expression | UNLIMITED | DEFAULT } }

Les options principales sont les suivantes :

- SESSIONS_PER_USER : nombre de sessions concurrentes autorisées.
- CPU_PER_SESSION : temps CPU maximal pour une session en centièmes de secondes.
- CPU_PER_CALL : temps CPU autorisé pour un appel noyau en centièmes de secondes.
- CONNECT_TIME : temps total autorisé pour une session en minutes (pratique pour les examens de TP minutés).
- LOGICAL_READS_PER_SESSION : définir le nombre maximal de bloc lus durant une session. On parlera ici des blocs lus sur le disque et dans la mémoire.
- LOGICAL_READS_PER_CALL : définir le nombre maximal de bloc lus durant un "appel serveur". On parlera ici des blocs lus sur le disque et dans la mémoire
- IDLE_TIME : temps d'inactivité autorisé, en minutes, au sein d'une même session (pour les étudiants qui ne clôturent jamais leurs sessions).
- PRIVATE_SGA : espace mémoire privé alloué dans la SGA (System Global Area).
- FAILED_LOGIN_ATTEMPTS : nombre de tentatives de connexion avant de bloquer l'utilisateur.
- PASSWORD_LIFE_TIME : nombre de jours de validité du mot de passe (il expire sil n'est pas changé au cours de cette période).
- PASSWORD_REUSE_TIME : nombre de jours avant que le mot de passe puisse être utilisé à nouveau. Si ce paramètre est initialisé à un entier, le paramètre PASSWORD_REUSE_MAX doit être passé à UNLIMITED.
- PASSWORD_REUSE_MAX : nombre de modifications de mot de passe avant de pouvoir réutiliser le mot de passe courant. Si ce paramètre est initialisé un entier, le paramètre PASSWORD_REUSE_TIME doit être passé à UNLIMITED.
- PASSWORD_LOCK_TIME : nombre de jours d'interdiction d'accès à un compte après que le nombre de tentatives de connexions a été atteint.
- PASSWORD_GRACE_TIME : nombre de jours d'une période de grâce qui prolonge l'utilisation du mot de passe avant son changement (un message d'avertissement s'affiche lors des connexions). Après cette période le mot de passe expire.

Syntaxe de Création d'un rôle

CREATE ROLE nomRle [NOT IDENTIFIED | IDENTIFIED
{BY motdePasse | USING [sechma.]paquetage | EXTERNALLY | GLOBALLY }]