TP 3 : Privilèges d'accès à la base de données

1. Connectez-vous en tant que SYSTEM à AGRICOLPDB.
2. Créer un tablespace agricolTBS et un tablespace temporaire agricolTempTBS.
3. Créer un utilisateur DBAGRICOL et lui associer les tablespaces précédents. Donner lui tous les privilèges.
4. Connectez-vous avec l'utilisateur **DBAGRICOL@AGRICOLPDB** :
    a. Créer les tables du TP1 et y insérer les données (exécuter le fichier TP1.SQL).
    b. Créez un autre utilisateur : **Admin en lui donnant les mêmes tablespace que DBAGRICOL**.
    c. Utiliser le dictionnaire de données pour vérifier la création des tablespaces, des utilisateurs et des tables.
5. Connectez-vous à l'aide de l'utilisateur **Admin**. Que remarquez-vous ?
6. Donnez le droit de création d'une session pour cet utilisateur (Create Session) et reconnectez-vous.
7. Donnez les privilèges suivants à **Admin**: créer des tables, des utilisateurs. Vérifier.
8. Exécutez la requête **Q1** suivante : **Select * from DBAGRICOL.AGRICULTEUR ;** Que remarquez-vous ?
9. Donnez le droit de lecture à cet utilisateur sur la table **AGRICULTEUR**. Exécutez la requête Q1 maintenant.
10. On veut créer une vue **AGRI_PROD** qui sauvegarde pour chaque agriculteur ses produits. Que faut-il faire ?
11. Créez un index **NAMEPROD_IX** sur l'attribut NOM de la table **PRODUIT**. Que remarquez-vous ?
12. Donnez le droit de création d'index à **Admin su**r la table **PRODUIT**, ensuite réessayez de créer l'index. Que se passe-t-il ?
13. Afficher tous les privilèges attribués à **Admin**.
14. Enlevez les privilèges précédemment accordés.
15. Vérifiez que les privilèges ont bien été supprimés.
16. Créez un profil « **AGRICOL_Profil** » qui est caractérisé par : (3 sessions simultanés autorisées, Un appel système ne peut pas consommer plus de 35 secondes de CPU, Chaque session ne peut excéder 90 minutes, Un appel système ne peut lire plus de 1200 blocs de donnes en mémoire et sur le disque, Chaque session ne peut allouer plus de 25 ko de mémoire en SGA, Pour chaque session, 30 minutes d'inactivité maximum sont autorisés, 5 tentatives de connexion avant blocage du compte, Le mot de passe est valable pendant 50 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 5 tentatives de connexion ont été atteintes, La période de grâce qui prolonge l'utilisation du mot de passe avant son changement est de 5 jours).
17. Affectez ce profil à l'utilisateur **Admin**.
18. Créez le rôle : « **MARCHE_MANAGER** » qui peut voir les tables **AGRICULTEUR**, **PRODUCTION** et peut modifier les lignes de la table **MARCHE**.
19. Assignez ce rôle à **Admin**. Vérifier que les autorisations assignées au rôle **MARCHE_MANAGER**, ont été bien transférées à l'utilisateur à **Admin**.

Syntaxe pour affecter et supprimer des privilèges

GRANT privilège [ON table/vue] TO utilisateur [WITH GRANT OPTION] → privilège sur un objet
GRANT privilège TO utilisateur [WITH ADMIN OPTION] → privilège système

REVOKE privilège ON [table/vue] FROM utilisateur → privilège sur un objet
REVOKE privilège FROM utilisateur → privilège système

Syntaxe 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** nomTablespace associe un espace disque de travail (appelé tablespace) à l'utilisateur.
- **TEMPORARY TABLESPACE** nomTablespace associe 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).

Syntaxe 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 s'il 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 }]