

Administration Des Bases de Données

TP1 : Gestion des utilisateurs

Annexe : Notions Théoriques

A. Gestion des utilisateurs

Un **utilisateur** d'une base de données Oracle (User) :

- Est identifié par un **login** avec lequel il se connecte au système
- Possède un ensemble de **droits** ou de **privileges** associés à son login
- Dispose d'un espace de stockage par défaut (**tablespace**) dans lequel sont stockés les objets qu'il crée.

1. Ordre Sql de création d'un nouvel utilisateur

```
CREATE USER login IDENTIFIED [by motDePasse|EXTERNALLY|GLOBALLY AS nomExterne]
[DEFAULT TABLESPACE nomTablespace]
[TEMPORARY TABLESPACE nomTablespaceTemporaire]
[QUOTA [int [K|M] | UNLIMITED ] ON nomTablespace]
[QUOTA [int [K|M] | UNLIMITED] ON nomTablespace2]]
[PASSWORD EXPIRE]
[ACCOUNT[LOCK|UNLOCK]]
[PROFILE nomPro_1] ;
```

Le tableau suivant explique le rôle des différentes options dans la création d'un user

Option	Description
IDENTIFIED	Mode d'identification du user
DEFAULT TABLESPACE nomTablespace	<ul style="list-style-type: none"> - Tablespace par défaut où seront stockés les objets créés par l'utilisateur - si pas mentionné alors les données du user seront stockés sous le tablespace system

TEMPORARY TABLESPACE nomTablespaceTemporaire	<ul style="list-style-type: none">- Tablespace temporaire des requêtes exécutées par l'utilisateur,- Si pas mentionné, alors le tablespace Temp sera utilisé
QUOTA	Espace maximal que l'utilisateur peut utiliser dans les tablespaces
PASSWORD EXPIRE	Indique si l'utilisateur doit changer son mot de passe à la première connexion
ACCOUNT	Verrouillage du compte
PROFILE	Profil

Exemples :

» Créer un utilisateur ayant le login user1 et le mot de passe « pass1 »

Create user **user1** identified by **pass1**;

» Créer un utilisateur ayant le login user2, le mot de passe « pass2 », utilisant comme tablespace par défaut « tbs1 » ayant comme quota maximal 5M.

Create user **user2** identified by **pass2**
Default tablespace tbs1
Quota 5M on tbs1;

2. Modification et suppression des utilisateurs

Modification du mot de passe

```
ALTER USER user1 IDENTIFIED BY new_password ;
```

Modification des quotas

```
ALTER USER user2 QUOTA 15M ON tbs1 ;
```

Modification des tablespaces par défaut

```
ALTER USER user1 DEFAULT TABLESPACE tbs2 TEMPORARY TABLESPACE tmp2;
```

Verrouillage

```
ALTER USER user1 ACCOUNT LOCK
```

Déverrouillage

```
ALTER USER user1 ACCOUNT UNLOCK
```

Suppression d'un utilisateur (ajouter l'option cascade pour supprimer son schéma s'il n'est pas vide)

```
DROP USER user1 [CASCADE]
```

3. Attribution des privilèges pour un utilisateur :

Après sa création, un utilisateur n'a aucun privilège ou droit de connexion, création ou de manipulation des données.

Les **privilèges** déterminent quelles actions l'utilisateur est autorisé à effectuer sur la base. Ils sont regroupés en deux catégories :

a) Privilèges au niveau système

- Droit d'exécuter une action sur n'importe quel objet d'un type particulier. Par exemple : **CREATE/DROP/ALTER TABLESPACE, USER, SESSION, TABLE, VIEW, etc.**
- Mot réservé **ANY** : droit d'exécuter un ordre dans n'importe quel schéma

Tableau 1 : Exemples de Privilèges Systèmes

Catégorie	Exemple
TABLE	CREATE [ANY] TABLE ALTER [ANY] TABLE DROP [ANY] TABLE SELECT [ANY] TABLE UPDATE [ANY] TABLE DELETE [ANY] TABLE
INDEX	CREATE [ANY] INDEX ALTER [ANY] INDEX DROP [ANY] INDEX
SESSION	CREATE SESSION ALTER SESSION RESTRICTED SESSION
TABLESPACE	CREATE TABLESPACE ALTER TABLESPACE DROP TABLESPACE

Syntaxe : pour attribuer un privilège système

```
GRANT [nomPrivilege | ALL PRIVILEGES] TO [nomUtilisateur|nomRole|PUBLIC]
[WITH ADMIN OPTION]
```

- » **ALL PRIVILEGES** : tous les privilèges système sont accordés à l'utilisateur
- » **PUBLIC** : le privilège est attribué à tous les utilisateurs
- » **WITH ADMIN OPTION** : donne à l'utilisateur le droit d'attribuer et de retirer le privilège reçu à d'autres utilisateurs.

Exemples :

- » Attribuer le privilège de création de table et de tablespace au user « user1 »

GRANT CREATE TABLE, CREATE TABLESPACE TO user1;

- » Attribuer le privilège de création de session (afin de pouvoir se connecter) pour tous les utilisateurs

GRANT CREATE SESSION TO PUBLIC

Syntaxe : pour retirer un privilège système

```
REVOKE [nomPrivilege | ALL PRIVILEGES | nomRole1] FROM  
[nomUtilisateur|nomRole2|PUBLIC]
```

Exemples :

- » Retirer le privilège « alter tablespace » du user isticuser

REVOKE ALTER TABLESPACE FROM isticuser

- » Retirer le privilège create session de tous les utilisateurs

REVOKE CREATE SESSION FROM PUBLIC

b) Privilège au niveau objet

- Droit d'exécuter une action sur un objet spécifique. Ex. SELECT, UPDATE, INSERT, etc.

Syntaxe pour attribuer un privilège objet :

```
GRANT [nomPrivilege | ALL PRIVILEGES] ON login:nomTable[(nomColonne)] TO  
[nomUtilisateur|nomRole|PUBLIC][WITH GRANT OPTION]
```

- » **WITH GRANT OPTION** : donne à l'utilisateur le droit d'attribuer et de retirer le privilège reçu

Exemples

- » Attribuer tous les privilèges objets sur la table etudiant du user isticuser à l'utilisateur scolarite

GRANT ALL PRIVILEGES ON isticuser.etudiant TO scolarite

- » Attribuer le privilège objets « select » sur la table etudiant du user isticuser à l'utilisateur guichet

GRANT SELECT ON isticuser.etudiant TO guichet

Syntaxe pour retirer un privilège objet :

```
REVOKE [nomPrivilege | ALL PRIVILEGES | nomRole1] ON  
login:nomTable[(nomColonne)] FROM [nomUtilisateur|nomRole2|PUBLIC]
```

Exemple : REVOKE select ON isticuser.etudiant FROM guichet

Notez que seul l'utilisateur ayant attribué un privilège objet peut le révoquer

B. Gestion des Rôles

Un Rôle est

- Ensemble nommé de privilèges
- Peut être affecté soit à un utilisateur soit à un autre rôle
- Oracle fournit un ensemble de rôles pré-définis (CONNECT, RESSOURCE, DBA, MGMT_USER, etc..). La vue [DBA_ROLES](#) fournit l'ensemble des rôles définis

Opérations de base sur les rôles

Création

```
CREATE ROLE nomRole [NOT IDENTIFIED | IDENTIFIED BY motDePasse]
```

Attribution et révocation de privilèges système à un rôle (même syntaxe que pour un utilisateur)

```
GRANT...[WITH ADMIN OPTION]
```

```
REVOKE...
```

Attribution et révocation de privilèges objet à un rôle (même syntaxe que pour un utilisateur, mais pas de clause [WITH GRANT OPTION])

```
GRANT...
```

```
REVOKE...
```

Suppression

```
DROP ROLE nomRole
```

Attribution d'un rôle à un utilisateur

```
GRANT nomRole TO nomUser [WITH ADMIN OPTION]
```

Révocation d'un rôle

```
REVOKE nomRole FROM nomUser
```