Faculté des Sciences de Gabès

Cours Administration BD

Chapitre 4 : Administrer la sécurité utilisateur

Gestion des privilèges et des rôles

(Partie 2)

Faîçal Felhi

felhi_fayssal@yahoo.fr

Privilèges système et objet

- **Lorsqu'un utilisateur est créé avec l'instruction CREATE USER, il ne dispose encore d'aucun droit car aucun privilège ne lui a encore été assigné .**
- **Il ne peut même pas se connecter à la base !**

Utilisateur Oracle

Nom Utilisateur

Mot de passe

Ensembles de *privilèges* ≡ *Droits* des utilisateurs

Profil

Privilège

Privilège Système → **Le droit d'exécuter un ordre SQL (Ex : créer une table)**

Privilège Objet → **Le droit d'accéder à un objet d'un autre utilisateur (Ex : Mettre à jour les données De la table CLIENT)**

3

Gestion des privilèges

- Gestion des privilèges **au niveau system**
  - Attribution des privilèges systèmes
  - Suppression des privilèges systèmes
  - Listes de quelques privilèges systèmes
- Gestion des privilèges **au niveau objet**
  - Attribution des privilèges objets
  - Suppression de privilèges
  - Listes des privilèges objets

Gérer les droits:
A. Privilège système

Définition

- Est le droit d'exécuter un ordre SQL
- Chaque ordre SQL a au moins un privilège système associé qui porte le même nom que l'ordre SQL
- Par exemple l'ordre CREATE TABLE possède un privilège système associé CREATE TABLE qui donne le droit de créer une table dans son propre schéma

Attribution d'un privilège système : Syntaxe (1)

GRANT **{**<privilège_système> | <rôle>**}**
[,{<privilège_système> | <rôle>}, …] **TO**
{<nom_utilisateur> | <rôle> | **PUBLIC** **}**
[,{<nom_utilisateur> | <rôle> | **PUBLIC**, }]…
[**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

Faîçal Felhi - felhi_fayssal@yahoo.fr
6

Attribution d'un privilège système : Syntaxe (2)

GRANT **{**<privilège_système> | <rôle>**}**
[,{<privilège_système> | <rôle>}, …] **TO**
{<nom_utilisateur> | <rôle> | **PUBLIC** **}**
[,{<nom_utilisateur> | <rôle> | **PUBLIC**, }]…
[**WITH ADMIN OPTION**] ;

PUBLIC permet d'affecter le **privilège** ou le **rôle** à tous les utilisateurs

Faîçal Felhi - felhi_fayssal@yahoo.fr
7

Attribution d'un privilège système : Syntaxe (3)

GRANT **{**<privilège_système> | <rôle>**}**
[,{<privilège_système> | <rôle>}, …] **TO**
{<nom_utilisateur> | <rôle> | **PUBLIC** **}**
[,{<nom_utilisateur> | <rôle> | **PUBLIC**, }]…
[**WITH ADMIN OPTION**] ;

WITH ADMIN OPTION **autorise** celui qui a reçu le **privilège** ou le **rôle** à le **transmettre** à un **autre utilisateur** ou un **autre rôle**

Faîçal Felhi - felhi_fayssal@yahoo.fr
8

Exemple

```
GRANT
  CREATE TABLE,
  CREATE VIEW,
  TO nom_utilisateur ;
```


Faîçal Felhi - felhi_fayssal@yahoo.fr

9

Suppression d'un privilège système : Syntaxe

REVOKE { <privilège_système> | <rôle> }
[, { <privilège_système> | <rôle> }]…
FROM { <utilisateur> | <rôle> | **PUBLIC** }
[, { <utilisateur> | <rôle> | **PUBLIC** }] ;

REVOKE permet **d'enlever** un **privilège** ou un **rôle** à un **utilisateur** ou un **rôle**

Faîçal Felhi - felhi_fayssal@yahoo.fr
10

Gérer les droits:
B. Privilège objet

Définition

- Est le droit d'accéder à un objet d'un autre utilisateur
  - Par exemple mettre à jour les données de la table CLIENT
- Par défaut, seul le propriétaire d'un objet a le droit d'y accéder
- Pour qu'un autre utilisateur puisse accéder à l'objet, le propriétaire de l'objet doit lui donner un privilège objet
- Les principaux privilèges objets sont les suivants :

Privilège	Table	Vue	programme
SELECT	X	X	
INSERT	X	X	
UPDATE	X	X	
DELETE	X	X	
EXECUTE			X

Attribution d’un privilège objet à un utilisateur

Syntaxe:

GRANT {nom_privilège [(liste de colonnes)] [,…] | ALL PRIVILEGES}

ON[nom_schema.] objet

TO {nom_utilisateur | PUBLIC} [,…]

[WITH GRANT OPTION]

Exemple

```
GRANT
   SELECT
  ,INSERT
  ,UPDATE
  ,DELETE
  ON SCOTT.EMP
  TO nom_utilisateur ;
```

Pour pouvoir mettre à jour ou supprimer des lignes d'une table, les privilèges UPDATE ET DELETE ne suffisent pas. Le privilège SELECT est nécessaire

Révocation d'un privilège objet à un utilisateur

Syntaxe:

REVOKE {nom_privilège [(liste de colonnes)] [,…] | ALL PRIVILEGES}

ON[nom_schema.] objet

FROM {nom_utilisateur | PUBLIC} [,…]

Gérer les droits:
C. Rôle

Définition

- Est un regroupement nommé de privilèges (système ou objet) qui peut être attribué à un utilisateur
- Les principales caractéristique sont:
  - Un rôle peut être attribué à un rôle
  - Un utilisateur peut avoir plusieurs rôles
- La mise en œuvre s'effectue en trois étapes:
  - Création du rôle
  - Attribution des privilèges
  - Attribution de rôle aux utilisateurs

Création d'un rôle

Syntaxe:

CREATE ROLE nom [IDENTIFIED { BY mdp | EXTERNALLY | NOT IDENTIFIED }

IDENTIFIED BY mdp: indique qu'un mdp est nécessaire pour activer le rôle

IDENTIFIED EXTERNALLY indique qu'une identification externe est nécessaire pour activer le rôle

Attribution d’un privilège à un rôle

- Syntaxe pour les privilèges système:

GRANT {nom_privilège [,…]

TO nom_rôle [,…]

[WITH ADMIN OPTION]

- Syntaxe pour les privilèges objet:

GRANT {nom_privilège [(liste de colonnes)] [,…] | ALL PRIVILEGES}

ON[nom_schema.] objet
TO nom_rôle [,…]
[WITH ADMIN OPTION]

Révocation d’un privilège à un rôle

- Syntaxe pour les privilèges système:

REVOKE nom_privilège   [,…]

FROM nom_rôle [,…]

- Syntaxe pour les privilèges objet:

REVOKE {nom_privilège [(liste de colonnes)] [,…] | ALL PRIVILEGES}

ON[nom_schema.] objet

FROM nom_rôle [,…]

Attribution d’un rôle à un utilisateur ou à un rôle

Syntaxe:

GRANT nom_rôle [,…]

TO {nom_utilisateur | PUBLIC | nom_rôle} [,…]

[WITH ADMIN OPTION]

Révocation d'un rôle à un utilisateur ou à un rôle

Syntaxe

REVOKE nom_rôle [,…]

FROM {nom_utilisateur |PUBLIC | nom_rôle} [,…]

Suppression d'un rôle

Syntaxe

DROP ROLE nom_rôle

Activation ou désactivation d'un rôle (1)

- Un rôle attribué à un utilisateur est par défaut automatiquement activé lors de la connexion de l'utilisateur
- Si l'utilisateur est connecté au moment de l'attribution du rôle, l'activation immédiate n'est pas automatique
  - L'utilisateur peut activer le rôle grâce à l'ordre SQL SET ROLE
- L'ordre ALTER USER permet de définir les rôles par défaut d'un utilisateur

Activation ou désactivation d'un rôle (2)

Syntaxe

ALTER USER nom_utilisateur DEFAULT ROLE

{nom_rôle [,..] | ALL EXCEPT nom_rôle [,..]] | NONE};

- ALL tous les rôles attribués à l'utilisateur sont activés par défaut. EXCEPT permet d'en enlever certains
- NONE aucun des rôles attribués à l'utilisateur n'est activé par défaut

- Cet ordre annule et remplace la situation actuelle des rôles par défaut, elle n'enlève pas les rôles à la liste actuelle
- L'ordre SET ROLE permet d'activer ou désactiver un rôle

Rôles Standards

- Il existe trois **rôles** 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, etc.
  - **RESOURCE :** Pour les **utilisateurs réguliers**. Accorde des droits supplémentaires pour la création de tables, de séquences, de procédures, de déclencheurs, d'index, etc.
  - **DBA :** Regroupe **tous les privilèges de niveau système** et la **possibilité d'accorder n'importe quel privilège à un autre utilisateur**.

Trouver les informations sur les droits (1)

Privilège système

- Plusieurs vues du dictionnaire de données permettent d'obtenir des informations sur les privilèges système
  - DBA_SYS_PRIVS : Privilèges systèmes attribuées aux utilisateurs ou aux rôles
  - SESSION_PRIVS : Privilège système actuellement actifs dans la session
  - SYSTEM_PRIVILEGE_MAP liste de tous les Privilège système

Trouver les informations sur les droits (2)

Privilège objet

- Plusieurs vues du dictionnaire de données permettent d'obtenir des informations sur les privilèges objet
  - DBA_TAB_PRIVS : Privilèges objet attribuées aux utilisateurs ou aux rôles sur la totalité de l'objet
  - DBA_COL_PRIVS : Privilèges objet attribuées aux utilisateurs ou aux rôles sur certaines colonnes de l'objet
  - TABLE_PRIVILEGE_MAP liste de tous les Privilège objet

Trouver les informations sur les droits (3)

Rôle

- Plusieurs vues du dictionnaire de données permettent d'obtenir des informations sur les rôle
  - DBA_ROLE : listes des rôles existant dans la BD
  - DBA_SYS_PRIVS : Privilèges système attribuées aux utilisateurs ou aux rôles sur la totalité de l'objet
  - DBA_COL_PRIVS : Privilèges objet attribuées aux utilisateurs ou aux rôles sur certaines colonnes de l'objet
  - DBA_ROLE_PRIVS : rôles attribués au utilisateurs ou au rôles
  - SESSION_ROLE: rôles actuellement actifs dans la session

Quelques exemples

```
CREATE ROLE comp;
GRANT SELECT, INSERT, UPDATE, DELETE ON CPT.FACTURE TO comp;
GRANT SELECT, INSERT, UPDATE, DELETE ON CPT.LIG_FAC TO comp ;
GRANT SELECT, INSERT, UPDATE, DELETE ON CPT.JOURNAL TO comp ;
```

Une fois le rôle créé, il peut être assigné à un utilisateur ou à un autre rôle

```
GRANT comp TO nom_utilisateur ;
```

Superviser les utilisateurs

La V$SESSION permet d'identifier les utilisateurs actuellement connectés

SELECT sid, serial#,username,osuser,status FROM V$SESSION