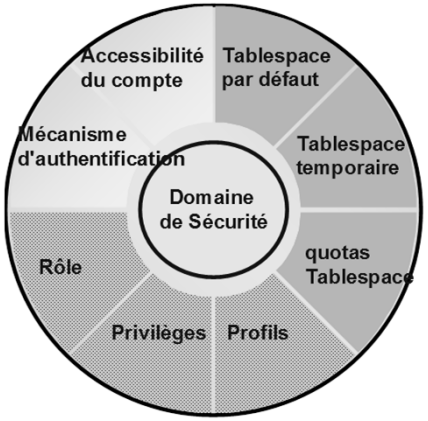
http://docs.oracle.com/database/121/index.htm#

3

CONTRÔLE DES ACCÈS MÉCANISMES DE BASE

UTILISATEURS ET SÉCURITÉ



UTILISATEUR

- Tout accès à la base de données s'effectue par l'intermédiaire de la notion d'utilisateur (compte Oracle)
- Créé par l'administrateur de la base de données

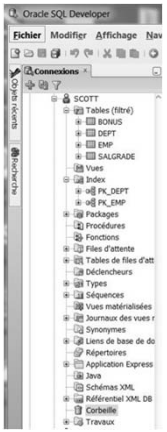
OBJETS LIÉS À L'UTILISATEUR SCHÉMA DE BASE DE DONNÉES

Tables
- Déclencheurs
- Contraintes

Index
Vues
Séquences
Procédures stockées
Synonymes
Types Explicites
Liens Base de Données

- Schéma: collection nommée d'objets (tables, vues, …) associée à un utilisateur particulier
- Quand un utilisateur est créé un schéma avec le même nom est créé pour cet utilisateur

EXEMPLE – LE SCHÉMA SCOTT



PROPRIÉTÉS D'UN UTILISATEUR

- **Nom et mot de passe**
- **Tablespace par défaut et tablespace temporaire**
- **Quota par tablespace**
- **Privilèges et rôles**
- **Profil**

CHANGER VOTRE MOT DE PASSE

ALTER USER nomUtilisateur
IDENTIFIED BY nouveauPassword;

Exemple :
alter user p1303195 identified by oraclemdp;

TABLESPACES PAR DÉFAUT ET TEMPORAIRE D'UN UTILISATEUR

- Tablespace (espace disque logique) : d'un point de vue logique, les données sont stockées par Oracle dans des tablespaces

- Tablespace par défaut : tablespace dans lequel les objets de l'utilisateur sont stockés (si aucun n'est désigné lors de la création de l'objet)
- Tablespace temporaire : pour les segments temporaires de l'utilisateur (utilisé pour toute opération de tri, tables/index temporaires, …)

QUOTA

- Un quota est une allocation d'espace dans un tablespace donné
- Un quota peut être :
  - Unlimited : l'utilisateur pourra employer tout l'espace disponible dans le tablespace
  - Une valeur spécifique en méga-octets ou en kilo-octets

EXEMPLE UTILISATEUR p1303195

PRIVILÈGE

- Droit attribué à un utilisateur d'exécuter un ensemble particulier d'ordres SQL ou d'accéder à certains objets de la base de données
- Accordé à un utilisateur ou à un rôle (ordre SQL *GRANT*). Le rôle sera ensuite attribué à un ou plusieurs utilisateurs
- L'ordre SQL *REVOKE* permet de supprimer des privilèges

PRIVILÈGE

Deux types de privilèges

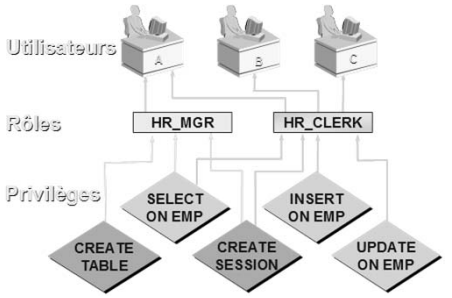
- **SYSTÈME : opérations que l'utilisateur peut exécuter soit sur ses objets (exemple: *create synonym*), soit sur un groupe d'objets (exemple: *select any table*) ET**

  les opérations portant sur l'administration de la base (exemple: *create tablespace*)

- **OBJET : autorisation d'accéder et de manipuler un objet spécifique (table, vue, séquence, procédure, fonction,…)**

  (exemples : *select on scott.emp*, *update (job,mgr) on scott.emp*

RÔLE



- **Regroupement de privilèges qui peut être attribué soit à un utilisateur, soit à un autre rôle**
- **Un rôle peut contenir à la fois des privilèges système et des privilèges objet**

RÔLES PRÉDÉFINIS

- **Plusieurs rôles sont prédéfinis à l'installation d'une base de données**

  Exemples :

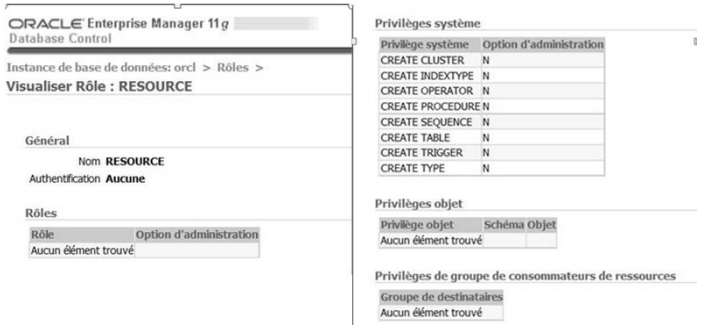
  - **CONNECT : possibilité de se connecter à la base de données (ce rôle n'a que le privilège système CREATE SESSION)**

    Rôle attribué automatiquement à la création d'un utilisateur

  - **RESOURCE : étend les privilèges d'un utilisateur ayant reçu le rôle CONNECT. Il inclut les privilèges CREATE TABLE, CREATE PROCEDURE, CREATE TRIGGER et d'autres privilèges système**

RÔLE CONNECT

RÔLE RESOURCE



CRÉATION D'UN RÔLE

Un rôle est créé sans caractéristique (vide). Il faut utiliser l'ordre *GRANT* pour lui affecter des privilèges ou des rôles

CREATE ROLE nom_rôle [identified by motDePasse];

```
CREATE ROLE sales_clerk;
```

```
CREATE ROLE hr_clerk
IDENTIFIED BY bonus;
```


ATTRIBUTION DE PRIVILÈGES OBJET

GRANT { object_priv [(column_list)]
[, object_priv [(column_list)]]...
| ALL [PRIVILEGES]}
ON [schema.]object
TO {user| rôle | PUBLIC}
[, {user | rôle | PUBLIC}]...
[WITH GRANT OPTION]

WITH GRANT OPTION : celui qui a reçu le droit pourra le transmettre à son tour

```
GRANT UPDATE(first_name, salary) ON
employee TO karen WITH GRANT OPTION;
```


ATTRIBUTION DE PRIVILÈGES SYSTÈME | DE RÔLES

Un privilège niveau système ou un rôle peut être attribué à un utilisateur ou à un rôle par :

GRANT {system_priv| rôle | ALL PRIVILEGES}
[, {system_priv| rôle | ALL PRIVILEGES}]...
TO {user| rôle | PUBLIC}
[, {user| rôle | PUBLIC}]...
[IDENTIFIED BY password]
[WITH ADMIN OPTION];

WITH ADMIN OPTION : autorise le bénéficiaire du privilège ou du rôle à le transmettre à un autre utilisateur ou rôle

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

EXEMPLES

```
GRANT CREATE SESSION, CREATE TABLE TO managers;
```

```
GRANT CREATE SESSION TO scott
WITH ADMIN OPTION;
```


RETIRER DES PRIVILÈGES OBJET

REVOKE { object_priv
[, object_priv]...
|ALL [PRIVILEGES] }
ON [schema.]object
FROM {user | rôle | PUBLIC}
[, {user | rôle | PUBLIC}]...

La commande REVOKE ne peut retirer que des privilèges attribués directement par l'ordre GRANT

```
REVOKE select, insert
ON departments
FROM scott;
```


RETIRER DES PRIVILÈGES SYSTÈME | DES RÔLES

Un privilège ou un rôle peut être retiré à un utilisateur ou à un rôle

REVOKE {system_priv| rôle |ALL PRIVILEGES}
[, {system_priv| rôle |ALL PRIVILEGES}]...
FROM {user| rôle | PUBLIC}
[, {user| rôle | PUBLIC}]...

La commande REVOKE ne peut retirer que des privilèges attribués directement par l'ordre GRANT

```
REVOKE CREATE TABLE FROM karen;
```


EXEMPLE UTILISATEUR p1303195

Rôles

Rôle	Option d'administration	Valeur par défaut
CONNECT	N	Y
RESOURCE	N	Y

Privilèges système

Précédent 1-10 sur 12 2 suivant(s)

Privilège système	Option d'administration
CREATE ANY DIRECTORY	N
CREATE PROCEDURE	N
CREATE PUBLIC SYNONYM	N
CREATE SEQUENCE	N
CREATE TRIGGER	N
CREATE TYPE	N
CREATE VIEW	N
DEBUG ANY PROCEDURE	N
DEBUG CONNECT SESSION	N
DROP PUBLIC SYNONYM	N

Précédent 1-10 sur 12 2 suivant(s)

Privilèges système

10 précédent(s) 11-12 sur 12 Suivant

Privilège système	Option d'administration
SELECT ANY DICTIONARY	N
UNLIMITED TABLESPACE	N

EXEMPLE UTILISATEUR p1303195

Privilèges objet

Privilège objet	Schéma	Objet	Option d'autorisation
Aucun élément trouvé			

Quotas

Espace disque logique	Quota	Valeur	Unité
1A (Default)	Valeur	5120	Kilo-octets

PROFIL

Permet de contrôler l'activité des utilisateurs en

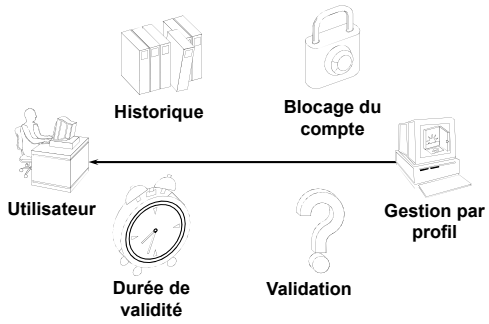
- **limitant les ressources auxquelles ils ont accès (nombre de sessions, durée de connexion, …)**
- **en gérant les mots de passe**

LIMITATION DES RESSOURCES

- **au niveau d'une session**
- **au niveau de chaque appel à la base de données (au cours de l'exécution d'un ordre SQL)**

- **Limite de ressources niveau appel atteinte**
  - **→ Oracle arrête l'opération en cours, annule la transaction et renvoie un code d'erreur**
- **Limite de ressources niveau session atteinte**
  - **→ Oracle envoie un message d'erreur (exemple : ORA-02391: exceeded simultaneous SESSIONS_PER_USER limit) et déconnecte l'utilisateur**

GESTION DES MOTS DE PASSE



PROFIL (suite)

- Plusieurs limites de ressources peuvent être regroupées sous un profil, identifié dans la base par un nom

- Un profil par défaut "DEFAULT" est créé à l'installation de la base de données (valeurs par défaut de la majorité des limites : UNLIMITED). Il est automatiquement attribué à un utilisateur à sa création

PROFIL DEFAULT

Instance de base de données: orcl > Profils >

Visualiser Profil : DEFAULT

Nom **DEFAULT**

Détails

UC/session (s/100)	**UNLIMITED**
UC/appel (s/100)	**UNLIMITED**
Temps de connexion (minutes)	**UNLIMITED**
Temps d'inactivité (minutes)	**UNLIMITED**

Services de base de données

Sessions simultanées (par utilisateur)	**UNLIMITED**
Lectures/session (blocs)	**UNLIMITED**
Lectures/appel (blocs)	**UNLIMITED**
Mémoire SGA privée (Ko)	**UNLIMITED**
Limite composite (unités de service)	**UNLIMITED**

Mot de passe

Expiration dans (jours)	**UNLIMITED**
Verrouillage dans (jours après l'expiration)	**7**

Historique

Nombre de mots de passe à conserver	**UNLIMITED**
Nombre de jours de conservation	**UNLIMITED**

Complexité

Fonction de complexité	**NULL**

Echec de connexion

Nombre d'échecs de connexion déclenchant le verrouillage	**10**
Durée de verrouillage, en nombre de jours	**1**

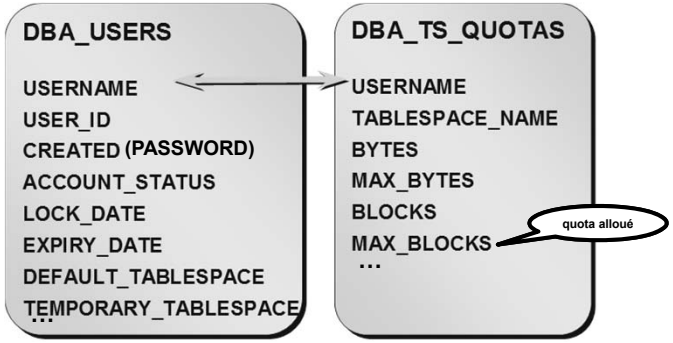
UTILISATEUR PUBLIC

Un utilisateur particulier PUBLIC, sans mot de passe, est créé à l'initialisation de la base de données

→ il permet à l'ensemble des utilisateurs d'avoir accès à certains objets de la base de données

Exemple : grant update(job) on scott.emp to public

SURVEILLANCE DES UTILISATEURS
Vues du dictionnaire



AFFICHAGE DES PRIVILÈGES SYSTÈME
Vues du dictionnaire

Niveau base de données

DBA_SYS_PRIVS
- GRANTEE
- PRIVILEGE
- ADMIN OPTION

Niveau session

SESSION_PRIVS
- PRIVILEGE

AFFICHAGE DES PRIVILÈGES OBJET
Vues du dictionnaire

DBA_TAB_PRIVS

GRANTEE
OWNER
TABLE_NAME
GRANTOR
PRIVILEGE
GRANTABLE

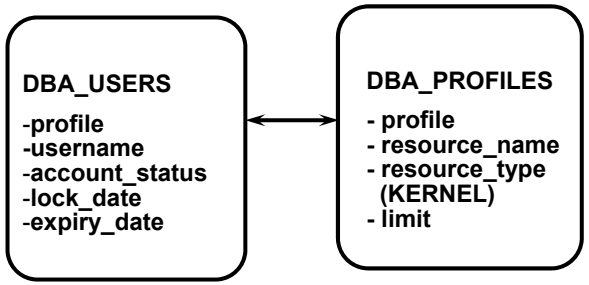
DBA_COL_PRIVS

GRANTEE
OWNER
TABLE_NAME
COLUMN_NAME
GRANTOR
PRIVILEGE
GRANTABLE

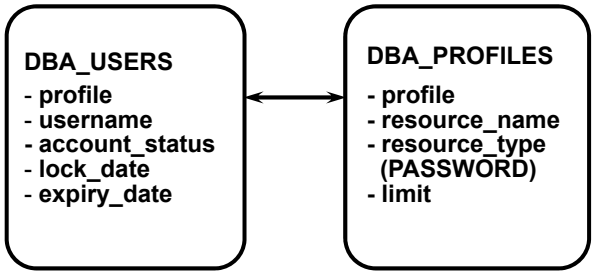
INFORMATIONS SUR LES RÔLES
Vues du dictionnaire

Vues	Description
DBA_ROLES	Tous les rôles
DBA_ROLE_PRIVS	Rôles affectés aux utilisateurs et rôles
ROLE_ROLE_PRIVS	Rôles affectés à des rôles
DBA_SYS_PRIVS	Privilèges système affectés aux utilisateurs et rôles
ROLE_SYS_PRIVS	Privilèges système affectés à des rôles
ROLE_TAB_PRIVS	Privilèges objet affectés à des rôles
SESSION_ROLES	Rôles attribués à l'utilisateur pour la session

INFORMATIONS SUR LES LIMITES DE RESSOURCES



INFORMATIONS SUR LES MOTS DE PASSE



Exercices