

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

3

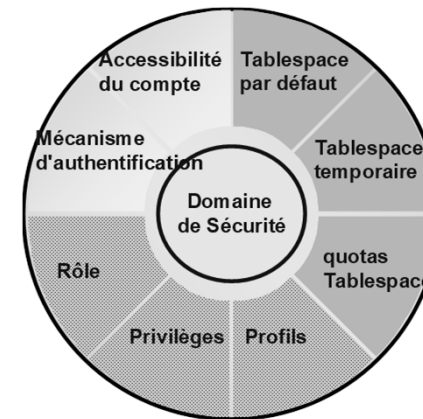


CONTRÔLE DES ACCÈS MÉCANISMES DE BASE

47

Bases de données - © Christine Bonnet

UTILISATEURS ET SÉCURITÉ



48

Bases de données - © Christine Bonnet



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

49

Bases de données - © Christine Bonnet

OBJETS LIÉS À L'UTILISATEUR SCHÉMA DE BASE DE DONNÉES

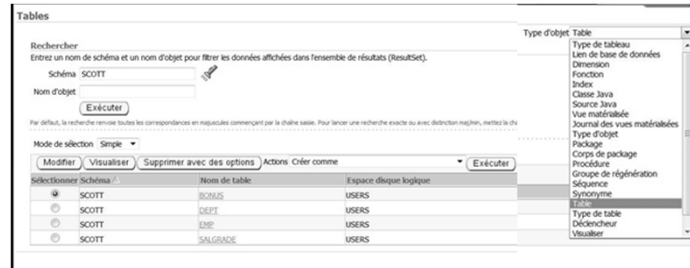
Tables
- Déclencheurs
- Contraintes
Index
Vues
Séquences
Procédures stockées
Synonymes
Types Explicites
Liens Base de Données

- 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

50

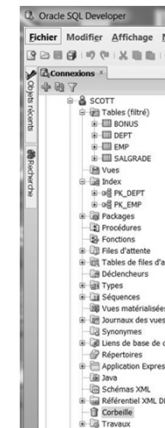
Bases de données - © Christine Bonnet

EXEMPLE – LE SCHÉMA SCOTT



51

Bases de données - © Christine Bonnet



52

Bases de données - © Christine Bonnet

PROPRIÉTÉS D'UN UTILISATEUR

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

53

Bases de données - © Christine Bonnet



CHANGER VOTRE MOT DE PASSE

ALTER USER nomUtilisateur
IDENTIFIED BY nouveauPassword;

Exemple :
alter user p1303195 identified by oraclemdp;

54

Bases de données - © Christine Bonnet



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

ORACLE Enterprise Manager 11g
Database Control

Instance de base de données: orcl > Utilisateurs >
Visualiser Utilisateur : P1303195

Général

Nom	P1303195
Profil	DEFAULT
Authentication	Mot de passe
Espace disque logique par défaut	1A
Espace disque logique temporaire	TEMP1A
Statut	UNLOCK
Groupe de destinataires par défaut	Aucune



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

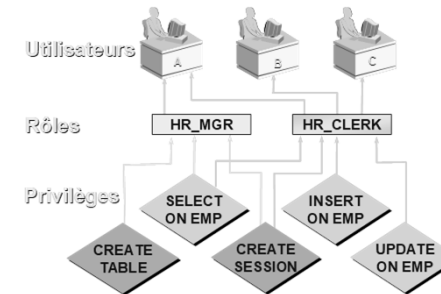
Deux types de privilèges

- **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*)

59

Bases de données - © Christine Bonnet

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

60

Bases de données - © Christine Bonnet

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

61

Bases de données - © Christine Bonnet

RÔLE CONNECT

ORACLE Enterprise Manager 11g
Database Control

Instance de base de données: orcl > Rôles >
Visualiser Rôle : CONNECT

Général

Nom: **CONNECT**

Authentification: **Aucune**

Rôles

Rôle: **Option d'administration**
Aucun élément trouvé

Privilèges système

Privilège système: **Option d'administration**
CREATE SESSION: **N**

Privilèges objet

Privilège objet: **Schéma Objet**
Aucun élément trouvé

Privilèges de groupe de consommateurs de ressources

Groupe de destinataires: **Aucun élément trouvé**

62

Bases de données - © Christine Bonnet

RÔLE RESOURCE

63

Bases de données - © Christine Bonnet

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;
```

64

Bases de données - © Christine Bonnet

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;
```

65

Bases de données - © Christine Bonnet

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

66

Bases de données - © Christine Bonnet

EXEMPLES

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

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

67

Bases de données - © Christine Bonnet

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;
```

68

Bases de données - © Christine Bonnet

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;
```

69

Bases de données - © Christine Bonnet

EXEMPLE UTILISATEUR p1303195

Rôles

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

Privilèges système

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

Privilèges système

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

70

Bases de données - © Christine Bonnet

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



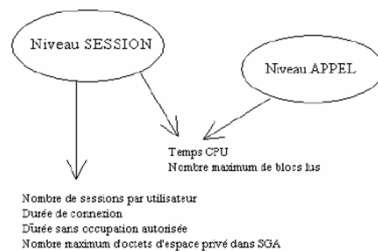
PROFIL

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

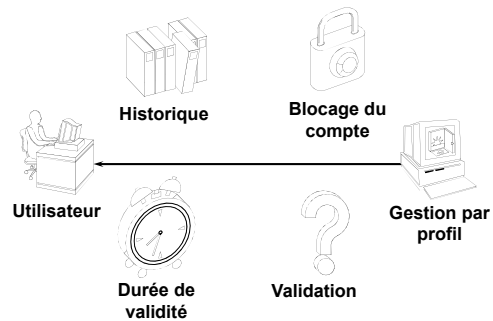
LIMITATION DES RESSOURCES

- 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



75

Bases de données - © Christine Bonnet

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

76

Bases de données - © Christine Bonnet

PROFIL DEFAULT

Instance de base de données: orcl > Profils > Visualiser Profil : DEFAULT	
Nom: DEFAULT	Mot de passe
Détails	Expiration dans (jours): UNLIMITED
UC/session (s/100): UNLIMITED	Verrouillage dans (jours après l'expiration): 7
UC/appel (s/100): UNLIMITED	Historique
Temps de connexion (minutes): UNLIMITED	Nombre de mots de passe à conserver: UNLIMITED
Temps d'inactivité (minutes): UNLIMITED	Nombre de jours de conservation: UNLIMITED
Services de base de données	Complexité
Sessions simultanées (par utilisateur): UNLIMITED	Fonction de complexité: NULL
Lectures/session (blocs): UNLIMITED	Echec de connexion
Lectures/appel (blocs): UNLIMITED	Nombre d'échecs de connexion déclenchant le verrouillage: 10
Mémoire SGA privée (Ko): UNLIMITED	Durée de verrouillage, en nombre de jours: 1
Limite composite (unités de service): UNLIMITED	

77

Bases de données - © Christine Bonnet

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`

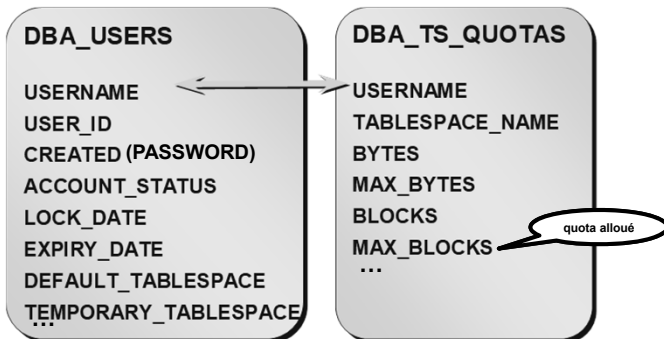
78

Bases de données - © Christine Bonnet



SURVEILLANCE DES UTILISATEURS

Vues du dictionnaire



79

Bases de données - © Christine Bonnet

AFFICHAGE DES PRIVILÈGES SYSTÈME

Vues du dictionnaire

Niveau base de données

DBA_SYS_PRIVS

- GRANTEE
- PRIVILEGE
- ADMIN OPTION

Niveau session

SESSION_PRIVS

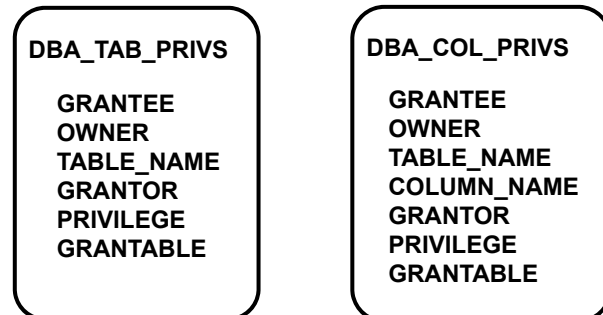
- PRIVILEGE

80

Bases de données - © Christine Bonnet

AFFICHAGE DES PRIVILÈGES OBJET

Vues du dictionnaire



81

Bases de données - © Christine Bonnet

INFORMATIONS SUR LES RÔLES

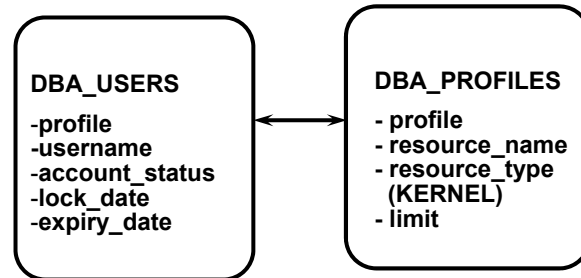
Vues du dictionnaire

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

82

Bases de données - © Christine Bonnet

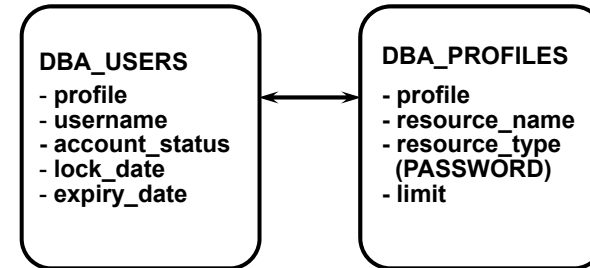
INFORMATIONS SUR LES LIMITES DE RESSOURCES



83

Bases de données - © Christine Bonnet

INFORMATIONS SUR LES MOTS DE PASSE



84

Bases de données - © Christine Bonnet



Exercices

85

Bases de données - © Christine Bonnet