# Sécurisation des accès aux données : les privilèges

# Privilèges

- Les types d'objets
- Un privilège est un droit d'exécuter un type particulier de commande SQL, ou un droit d'accéder à un objet d'un autre utilisateur
- Un rôle est un ensemble de privilèges
- Privilèges systèmes : gérés par l'administrateur
- Privilèges vis à vis des objets : créés par les utilisateurs

# Privilèges systèmes

## Créer/modifier des objets essentiels de la base

```
GRANT {priv-syst | rôle}
   [, {priv-syst | rôle}]...

TO {utilisateur | rôle |PUBLIC}
   [, {utilisateur | rôle |PUBLIC}] ...

[WITH ADMIN OPTION] ;
```

WITH ADMIN OPTION permet au bénéficiaire de transmettre ses privilèges

# Rôle CONNECT

- se connecter à la base en appelant l'un des outils Oracle (SQL*Plus, par ex.)
- changer son mot de passe
- manipuler les objets (tables, vues) de la base si des droits (select, insert, ...) lui ont été accordés par les propriétaires des objets.
- transmettre des autorisations sur des objets s'il a obtenu le droit de retransmettre.
- créer des vues et des synonymes (nous en parlons d'ici peu) pour des objets autorisés.

# Rôle RESOURCE

- créer des tables, index
- donner des droits de manipulation (ou les reprendre...) sur ses propres objets à d'autres utilisateurs.

# Rôle DBA

- créer des utilisateurs
- donner (ou retirer) des privilèges aux utilisateurs
- accéder à tous les objets de la base
- créer des synonymes publics
- effectuer les opérations de maintenance de la base.

# Autres privilèges

- CREATE TABLE
- CREATE/DROP/ALTER USER
- CREATE VIEW
- ...

# Supprimer des privilèges

REVOKE {priv-syst | rôle} [, {priv-syst | rôle}]...

FROM {utilisateur | rôle | PUBLIC}
    [,{utilisateur | rôle | PUBLIC}]... ;

# Exemple

- Création (par un dba nécessairement) de l'utilisateur raffarin avec un mot de passe :

```
grant connect to raffarin
identified by ump ;
```

- L'utilisateur chirac a, en plus, la possibilité de définir des structures de tables (et des index,...) :

```
grant connect, ressource chirac
identified by mulot ;
```

# Exemples

- raffarin obtient les mêmes privilèges que chirac :

```
grant ressource to raffarin ;
```

- chirac reprend l'avantage :

```
grant dba to chirac ;
```

- Changement de mot de passe

```
grant connect to chirac identified
by elysee ;
```

# Privilèges sur les objets

GRANT {droit [, droit] ... | ALL } [(colonne [, colonne]...)]
ON [utilisateur.]objet
TO {utilisateur | rôle [, utilisateur | rôle]] ... | PUBLIC}
[ WITH GRANT OPTION ] ;

# Reprise de droits

REVOKE {droit [, droit ] ... | ALL}
ON [utilisateur.]objet
FROM {utilisateur | rôle [, utilisateur | rôle] ... |
PUBLIC} ;