CHAP 01
Administrer la sécurité utilisateur

Schéma de base de données

- Un schéma est une collection d'objets qui appartiennent à 1 seul utilisateur.
- Lorsqu'un utilisateur est créé, un schéma correspondant est automatiquement créé.
- Le schéma porte le même nom que l'utilisateur
- Un utilisateur ne peut être associé qu'à un seul schéma.
- Le nom utilisateur et le nom de schéma sont souvent utilisés indifféremment

Objets de schéma

Tables

Déclencheurs

Contraintes

Index

Vues

Séquences

Programmes stockés

Synonymes

Types de données définis par l'utilisateur

Liens de base de données

Comptes utilisateur de la base de données

Chaque BD comporte deux types de comptes utilisateur :

- **Comptes prédéfinis:** ***SYS, SYSTEM, SYSAUX , …etc***

  Sont créés automatiquement avec la création de la BD

- **Comptes non prédéfinis:**

  Doivent être créés, explicitement, par un administrateur de BD selon les besoins.

Chaque compte utilisateur dispose des informations suivantes:

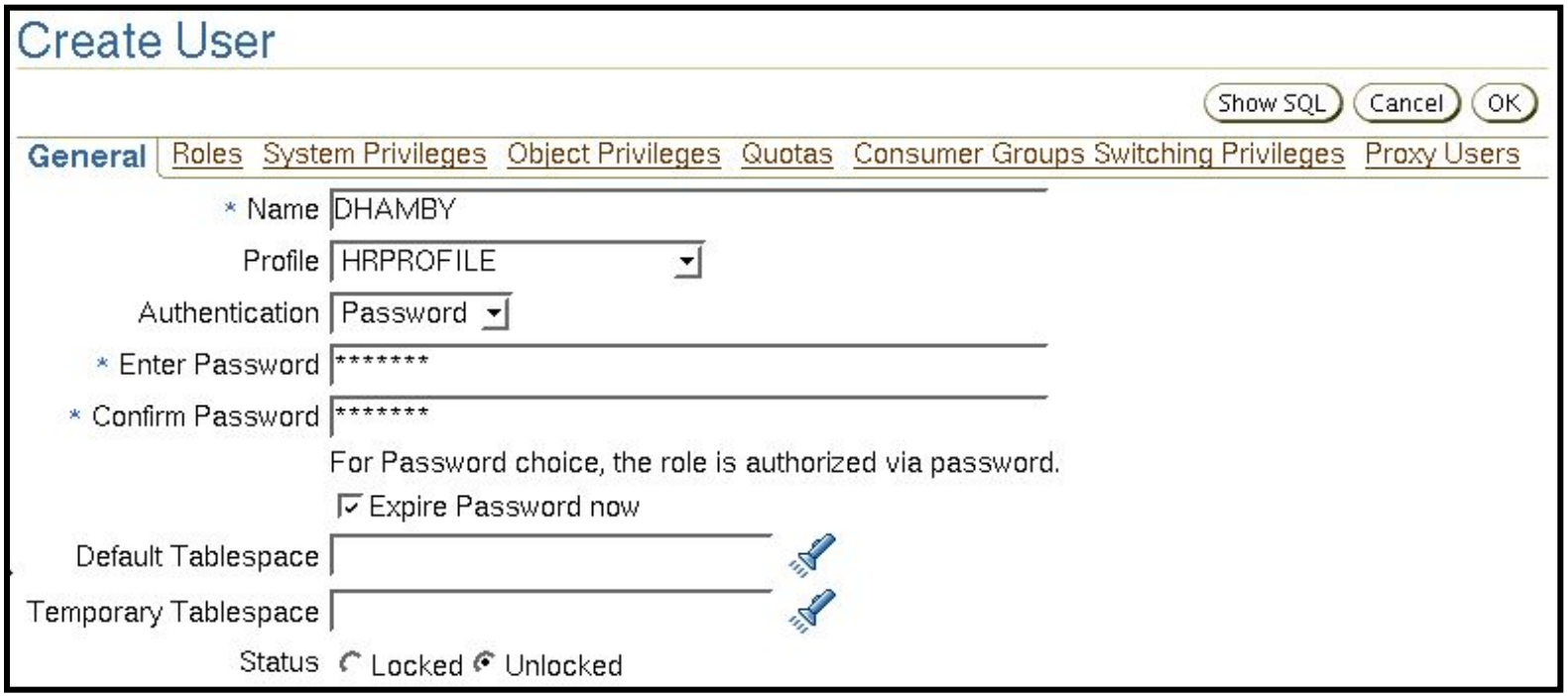
- ***Un nom utilisateur unique***
- ***Une méthode d'authentification (mot de pass, authentification OS, ..)***
- ***Un tablespace par défaut (Où sont créé les objets par défaut)***
- ***Un tablespace temporaire (Où sont éffectuées les opérations de tries)***
- ***Un profil utilisateur (Qui gère la sécurité des mots de passe et les resources)***
- ***Un groupe de consommateurs de ressources***
- ***Un statut de verrouillage (Compte blocké)***

Créer un utilisateur

Pour créer un utilisateur par ligne de commande:

```
CREATE USER aaron IDENTIFIED BY soccer
DEFAULT TABLESPACE data
DEFAULT TEMPORARY TABLESPACE temp
QUOTA 15M ON data
QUOTA 10M ON users
PROFILE DEFAULT
PASSWORD EXPIRE;
```

Pour créer un utilisateur par l'interface EM:



Modifier un compte utilisateur

- Modifier le mot de passe :

```
sql>ALTER USER aaron IDENTIFIED BY new_pass ;
```

- Modifier le tablesapce par défaut :

```
sql>ALTER USER aaron DEFAULT TABLESPACE users;
```

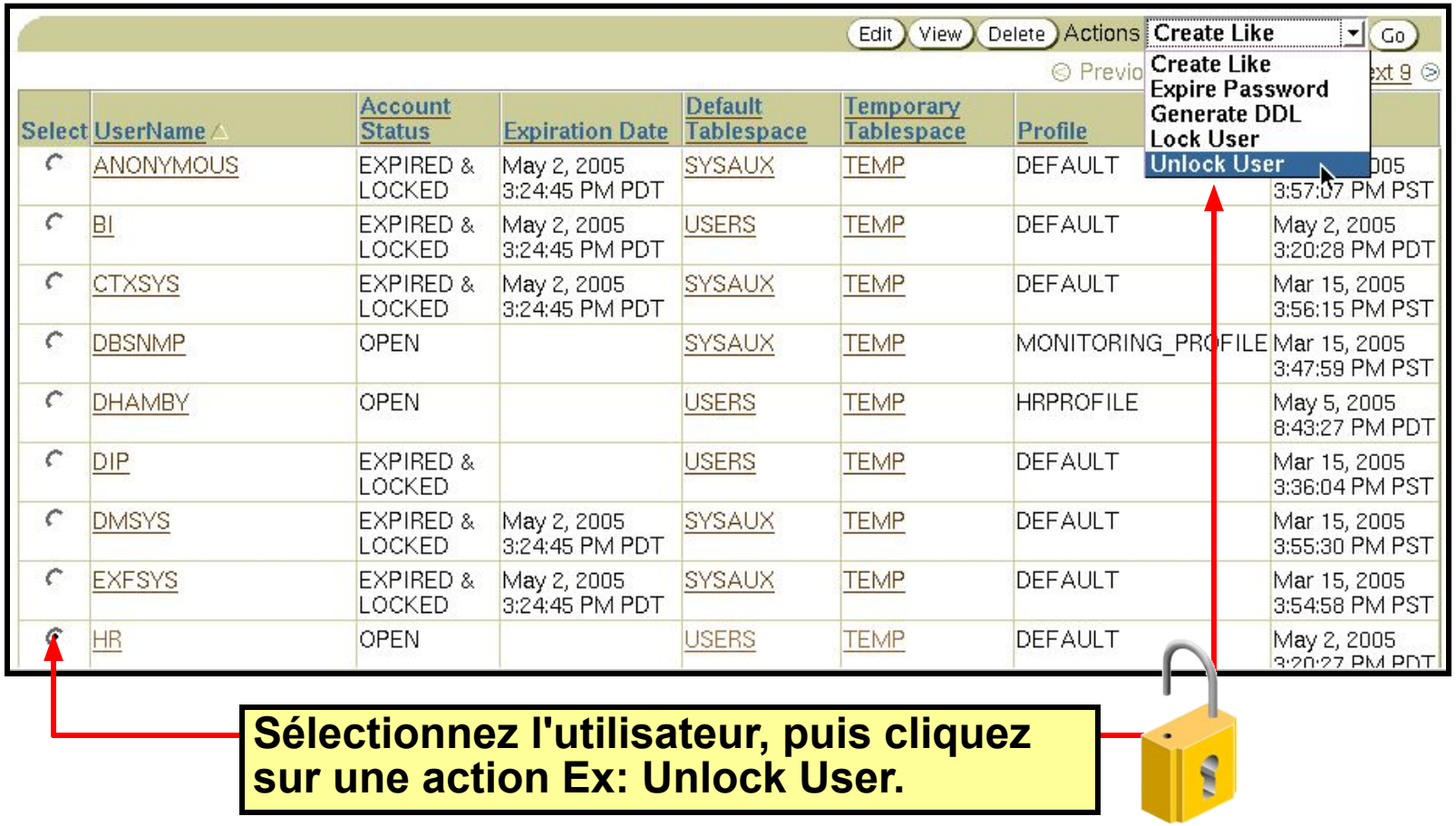
- Modifier le quota sur un tablesapce :

```
sql>ALTER USER aaron QUOTA 0M ON data;
```

- Verouiller un compte :

```
sql>ALTER USER aaron account lock;
```

Modifier un compte utilisateur



Les droits et privilèges utilisateurs

Par défaut un utilisateur nouvellement créé dispose des privilèges suivants:

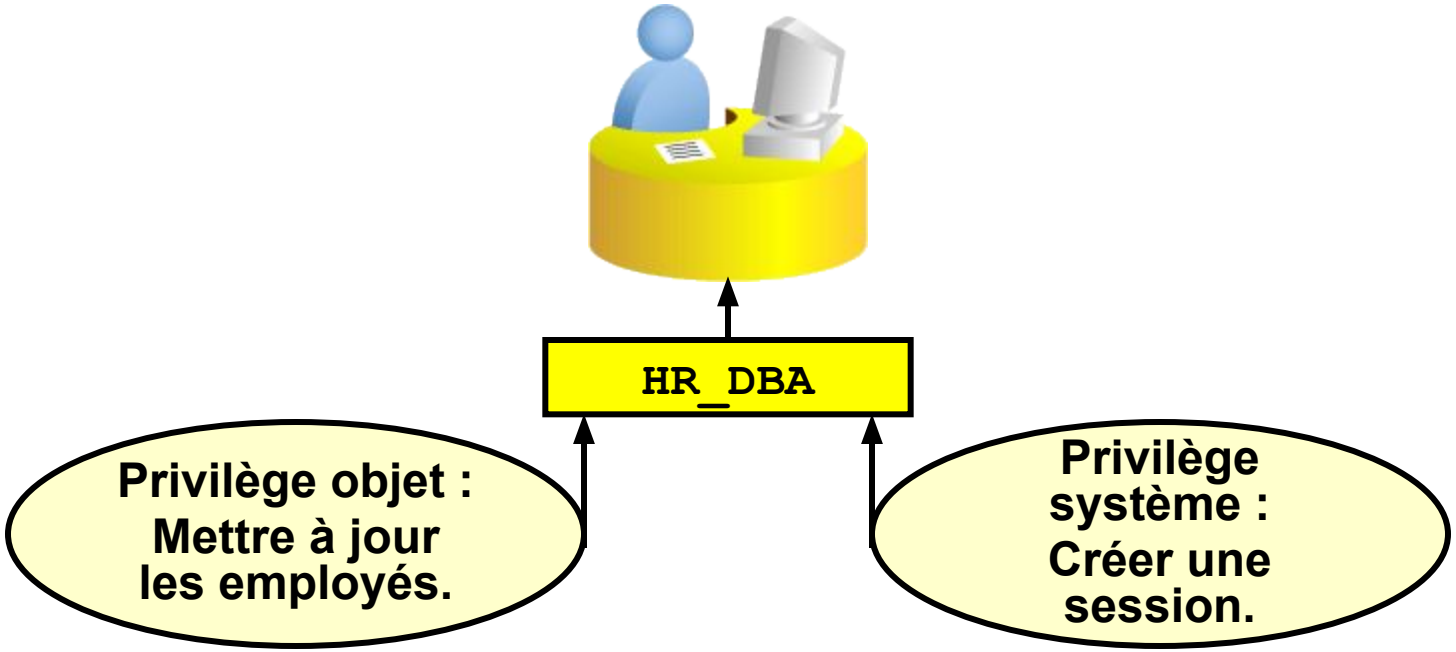
- **Si l'utilisateur est créé par une ligne de commande sql :**
  - **AUCUN PRIVILEGE**
  - **L'utilisateur ne peut même pas se connecter à la BD**

- **Si l'utilisateur est créé par l'interface EM :**
  - **OUVRIR UNE SESSION (par le biais du rôle *CONNECT*)**
  - **L'utilisateur ne peut effectuer aucune autre tâche**

Privilèges

Il existe deux types de privilège utilisateur :

- **Système : permet aux utilisateurs d'effectuer des actions particulières dans la base de données**
- **Objet : permet aux utilisateurs d'accéder à un objet spécifique et de le manipuler**



Privilèges système : exemples

- Il existe plus de 100 privilèges système différents.
- Le mot-clé `ANY` signifie que les utilisateurs disposent du privilège de gestion d'objets dans n'importe quel schéma.
- On accorde le privilège par la cmde

```
GRANT nom_privs TO
nom_user ou nom_role
[with admin option]
```

- On supprime le privilège par la cmde:

```
REVOKE nom_privs FROM
    nom_user ou nom_role
```

Catégorie	Exemples
INDEX	CREATE ANY INDEX ALTER ANY INDEX DROP ANY INDEX
TABLE	CREATE TABLE CREATE ANY TABLE ALTER ANY TABLE DROP ANY TABLE SELECT ANY TABLE UPDATE ANY TABLE DELETE ANY TABLE
SESSION	CREATE SESSION ALTER SESSION RESTRICTED SESSION
TABLESPACE	CREATE TABLESPACE ALTER TABLESPACE DROP TABLESPACE UNLIMITED TABLESPACE

Privilège SYSDBA et SYSOPER

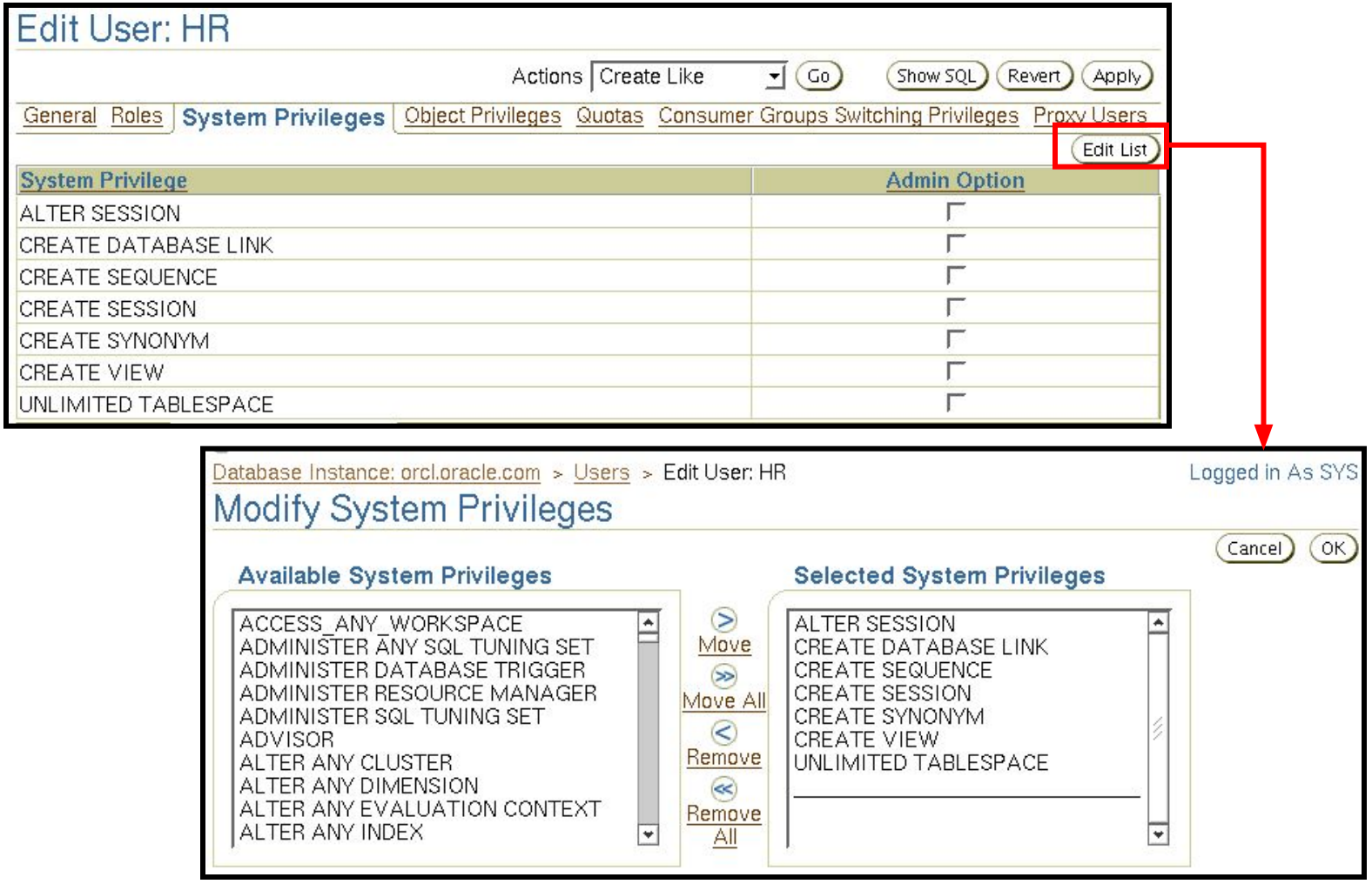
Catégorie	Exemples
SYSOPER	STARTUP SHUTDOWN ALTER DATABASE OPEN | MOUNT ALTER DATABASE BACKUP CONTROLFILE TO RECOVER DATABASE ALTER DATABASE ARCHIVELOG RESTRICTED SESSION
SYSDBA	SYSOPER PRIVILEGES WITH ADMIN OPTION CREATE DATABASE ALTER TABLESPACE BEGIN/END BACKUP RESTRICTED SESSION RECOVER DATABASE UNTIL

sql> connect emi/pwd as sysoper

Attribution de privilèges système

Qui peut attribuer des privilèges system?

- UN DBA
- Un utilisateur ayant acquis le même privilège avec l'option d'administration



Gestion des privilèges objet

Pour attribuer un privilège objet en ligne de commande :

GRANT nom_privs ON nom_objet TO nom_user ou nom_role
[with grant option]

with grant option : Option qui donne le droit au bénéficiaire d'accorder ce même privilège à un autre utilistaeur

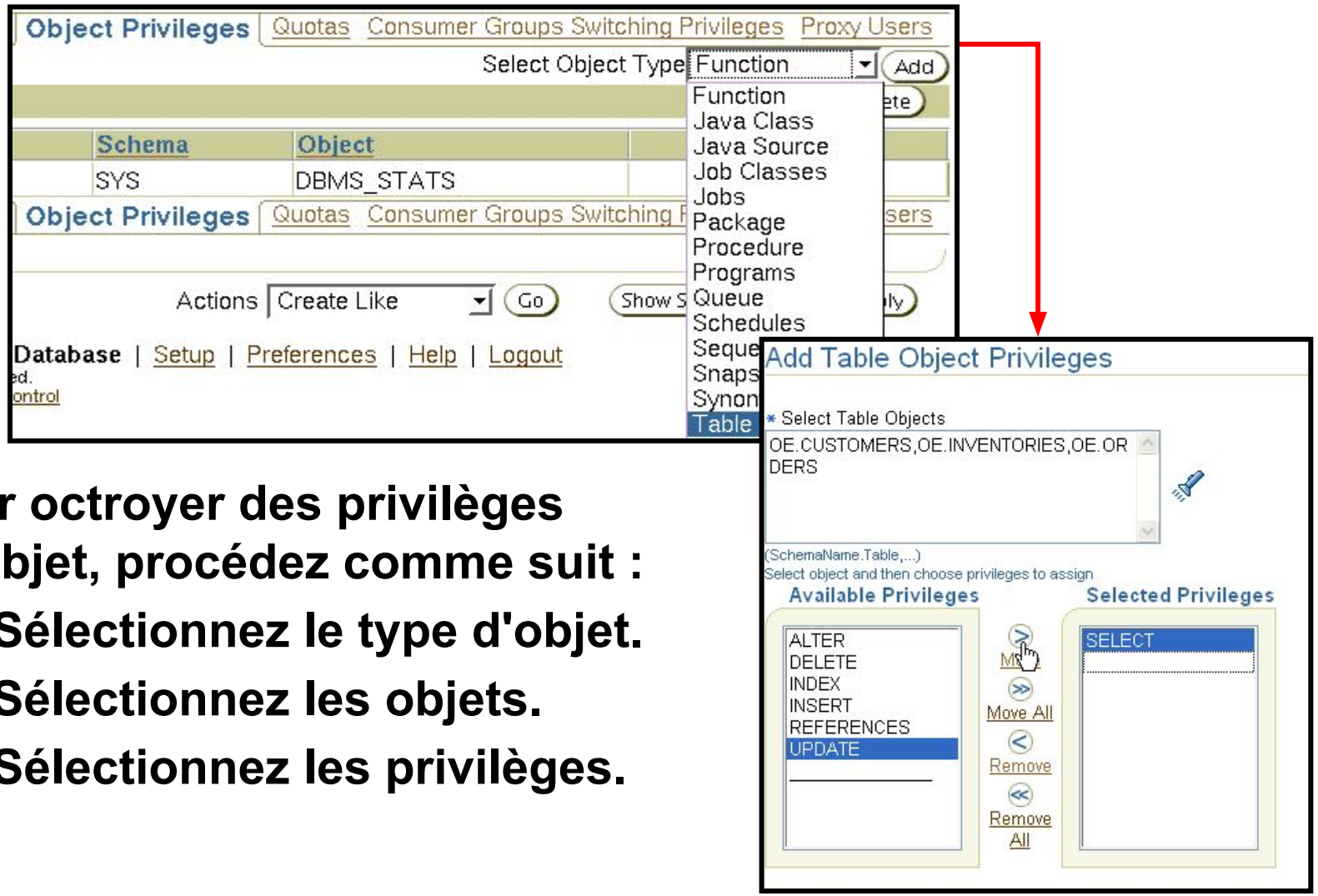
nom_privs

Priv. objet	Table	Vue	Séquence	Procédure
ALTER	√	√	√	√
DELETE	√	√		
EXECUTE				√
INDEX	√	√		
INSERT	√	√		
REFERENCES	√			
SELECT	√	√	√	
UPDATE	√	√		

Privilèges objet

Qui peut attribuer des privilèges Objet?

- Le propriètaire de l'objet
- Un utilisateur ayant acquis le même privilège avec l'option d'administration



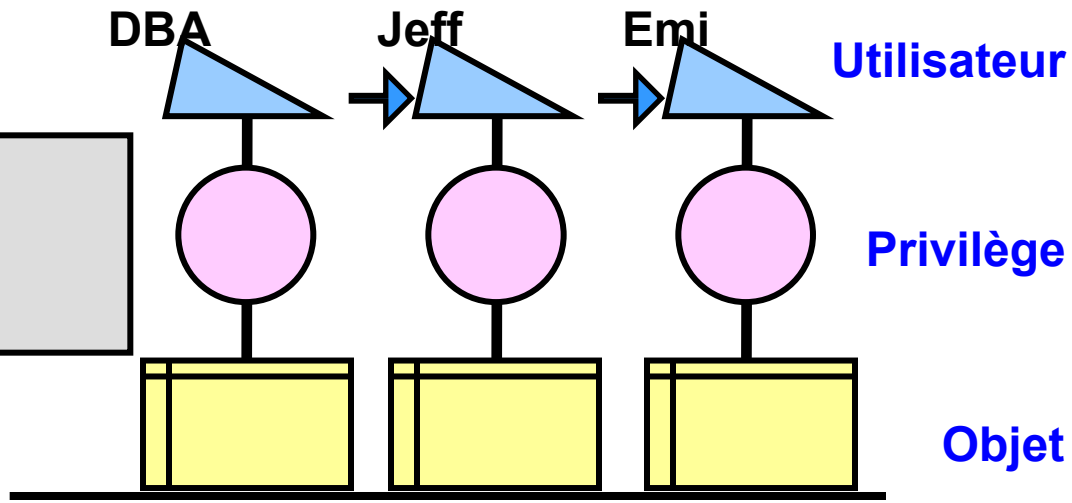
Pour octroyer des privilèges objet, procédez comme suit :

1. **Sélectionnez le type d'objet.**
2. **Sélectionnez les objets.**
3. **Sélectionnez les privilèges.**

Révoquer des privilèges système accordés avec ADMIN OPTION

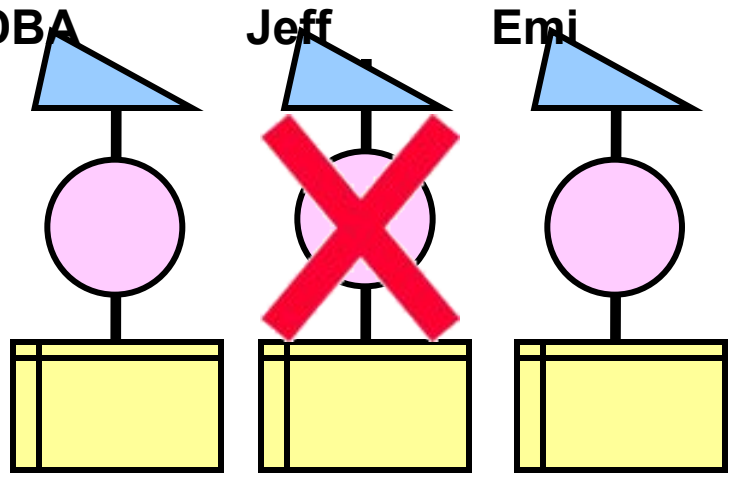
GRANT

```
GRANT CREATE TABLE
TO jeff
WITH ADMIN OPTION;
```

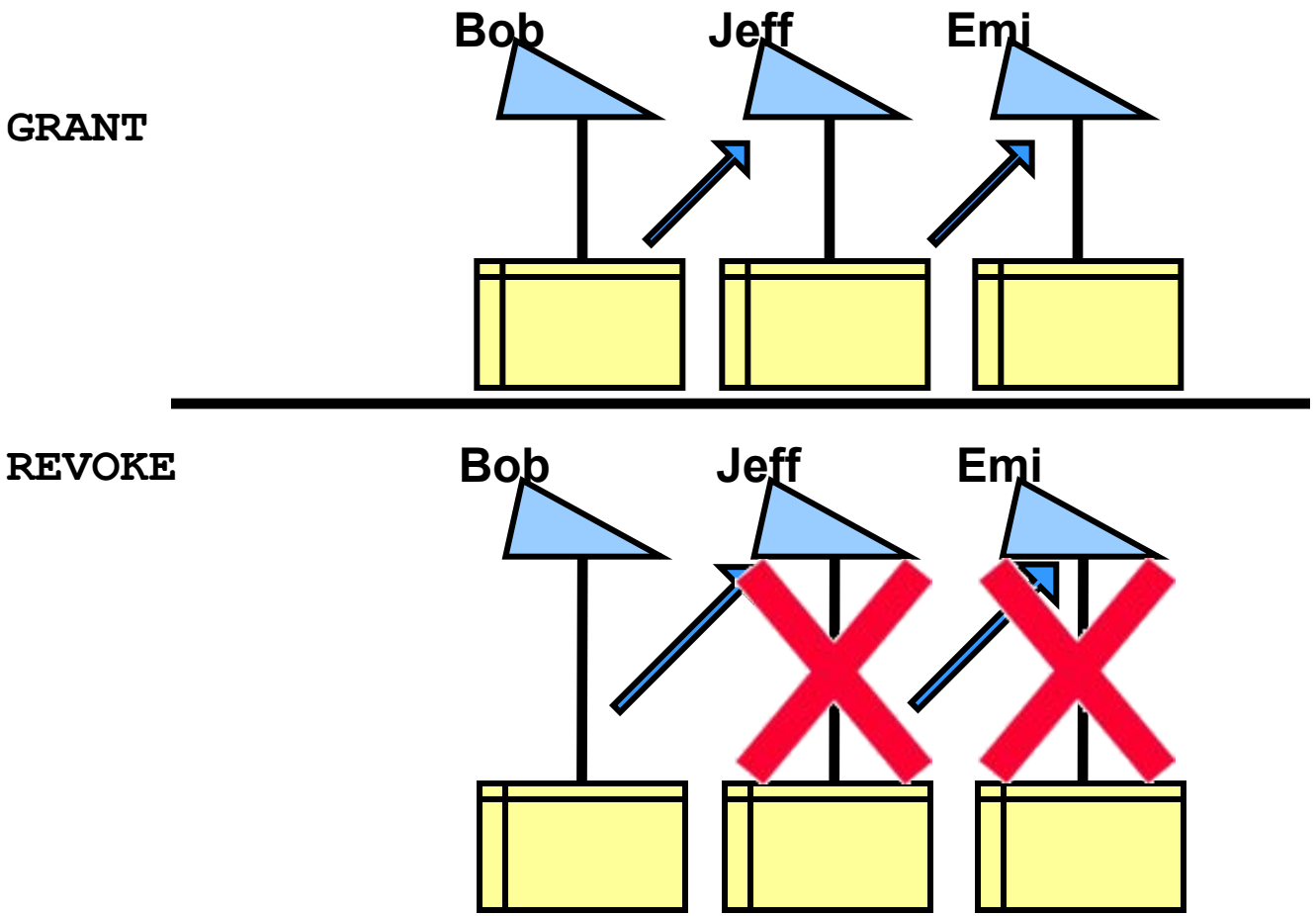


REVOKE

```
REVOKE CREATE TABLE
FROM jeff;
```



Révoquer des privilèges objet accordés avec GRANT OPTION



LES ROLES

Le rôle :

Est un groupement d'un ensemble de privilèges

Le contenu d'un rôle :

- Privilèges system
- Privilèges object
- Rôle

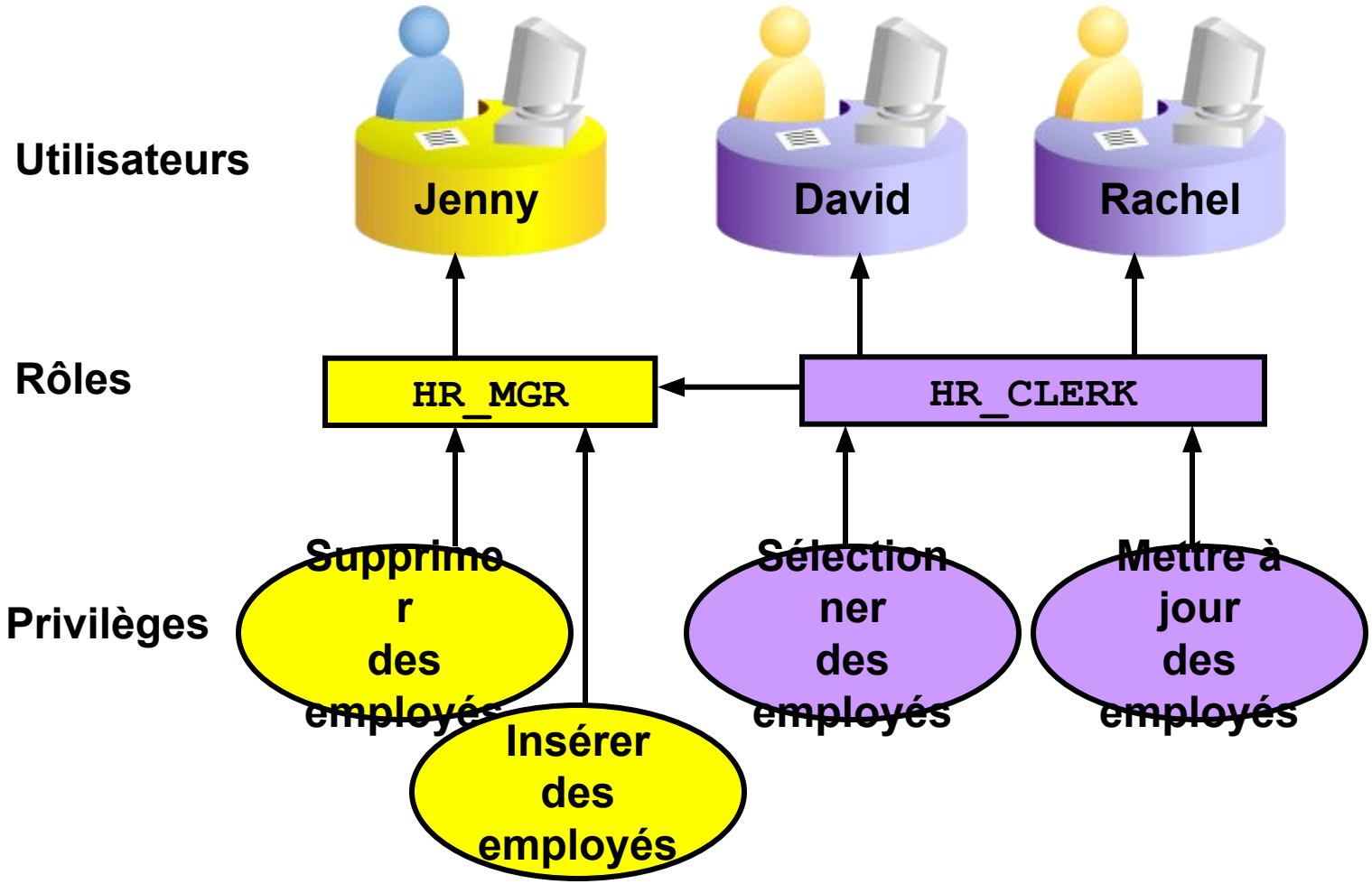
Types de rôles :

- Rôles prédefinis : Sont créés automatiquement par Oracle
- Rôle non prédefinis : Crées est gérés par le DBA

Avantages des rôles:

- Gestion plus facile des privilèges
- Gestion dynamique des privilèges
- Disponibilité sélective des privilèges

Affecter des privilèges à des rôles et des rôles à des utilisateurs

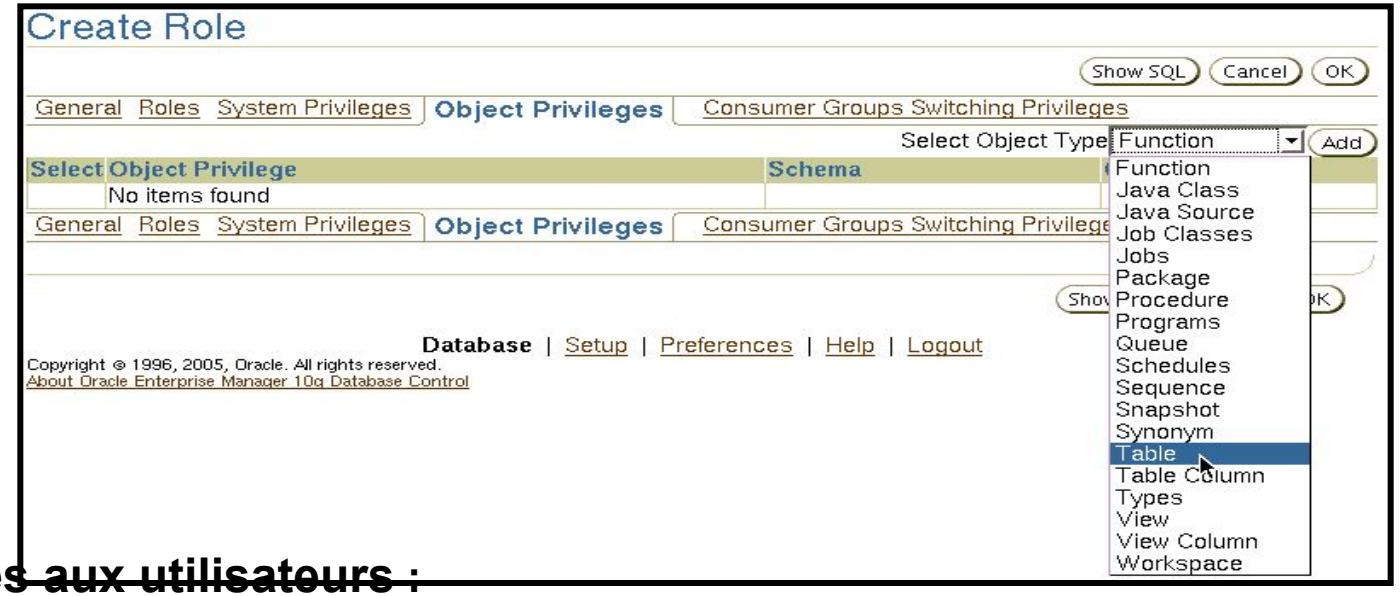


Rôles prédéfinis

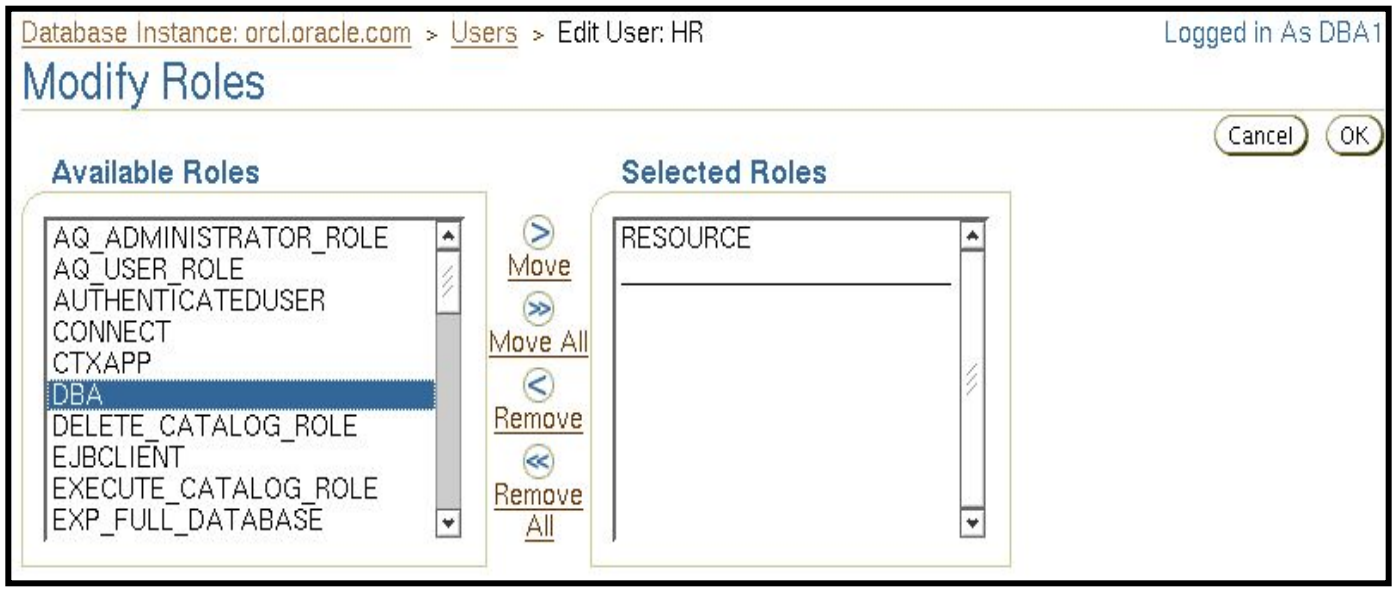
CONNECT	CREATE SESSION
RESOURCE	CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE
SCHEDULER_ ADMIN	CREATE ANY JOB, CREATE EXTERNAL JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER
DBA	La plupart des privilèges système et plusieurs autres rôles. Ce rôle ne doit pas être accordé aux utilisateurs qui ne sont pas administrateurs.
SELECT_ CATALOG_ ROLE	Aucun privilège système, mais le rôle HS_ADMIN_ROLE et plus de 1 700 privilèges objet sur le dictionnaire de données.

Gérer les rôles

- **Créer un rôle et affecter des privilèges au rôle :**

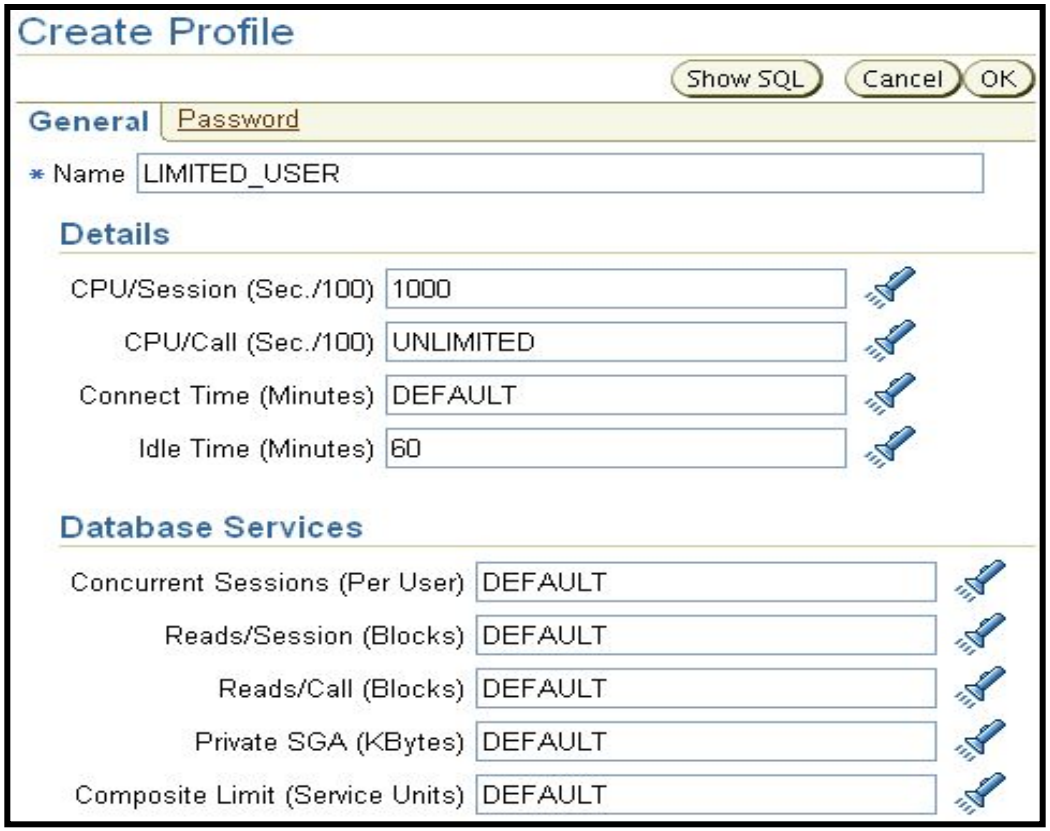


- **Affecter des rôles aux utilisateurs :**

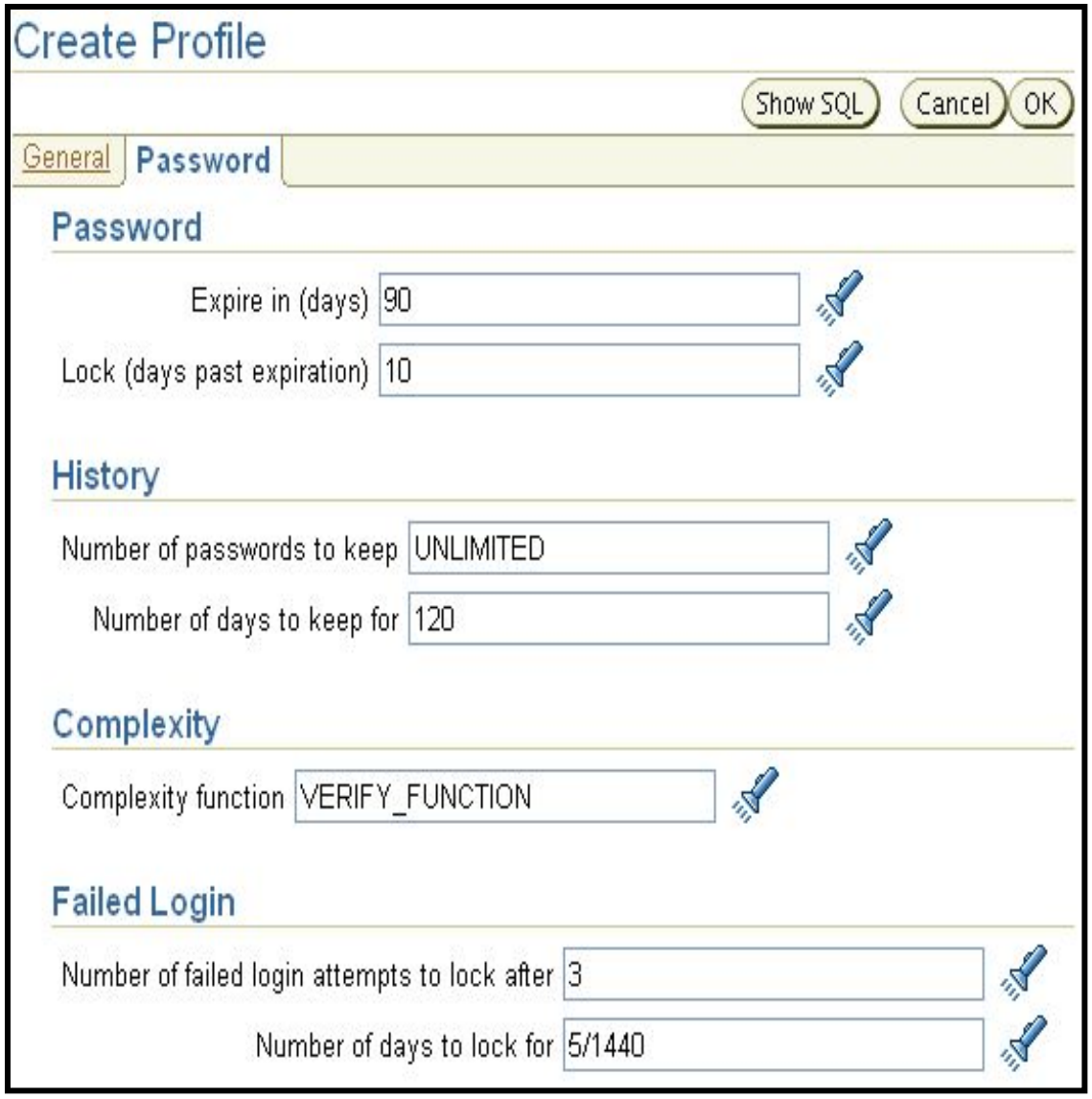


Les Profils

- Un profil est un ensemble nommé qui contrôle:
  - La sécurité des mots de passe
  - La consommation des ressources
- Chaque utilisateur doit être affecter à un profile
- Par défaut, un utilisateur est affecté au profil `DEFAULT`.
- Au moment de la création du profile, on lui affecte un nom et les limits relatives aux ressources et au mots de passe



Créer un profile de mot de passe



- Durée de vie, en jours, du mot de passe
- Période de grâce, en jours, pendant laquelle l'utilisateur peut changer de mot de passe une fois le mot de passe expiré
- Nombre maximum de réutilisations d'un mot de passe
- Période,en jours, pendant laquelle un mot de passe ne peut pas être réutilisé

- Fonction PLSQL qui vérifie la complexité du mot de passe

- Nombre d'échecs de connexion avant verrouillage du compte
- Durée, en jours, de verrouillage du compte après le nombre d'échecs de connexion défini

Fonction de vérification des mots

Cette fonction doit être créée dans le schéma `SYS` et respecter la spécification suivante :

```
function_name( userid_parameter IN VARCHAR2(30),
               password_parameter IN VARCHAR2(30),
           old_password_parameter IN VARCHAR2(30))
RETURN BOOLEAN
```

On peut utiliser la fonction "*VERIFY_FUNCTION* " fournie par oracle qui applique les restrictions suivantes :

- **La longueur minimale est de quatre caractères.**
- **Le mot de passe doit être différent du nom utilisateur.**
- **Le mot de passe doit comporter au moins un caractère alphabétique, un chiffre et un caractère spécial.**
- **Le mot de passe doit comporter au moins trois lettres différentes du précédent mot de passe.**