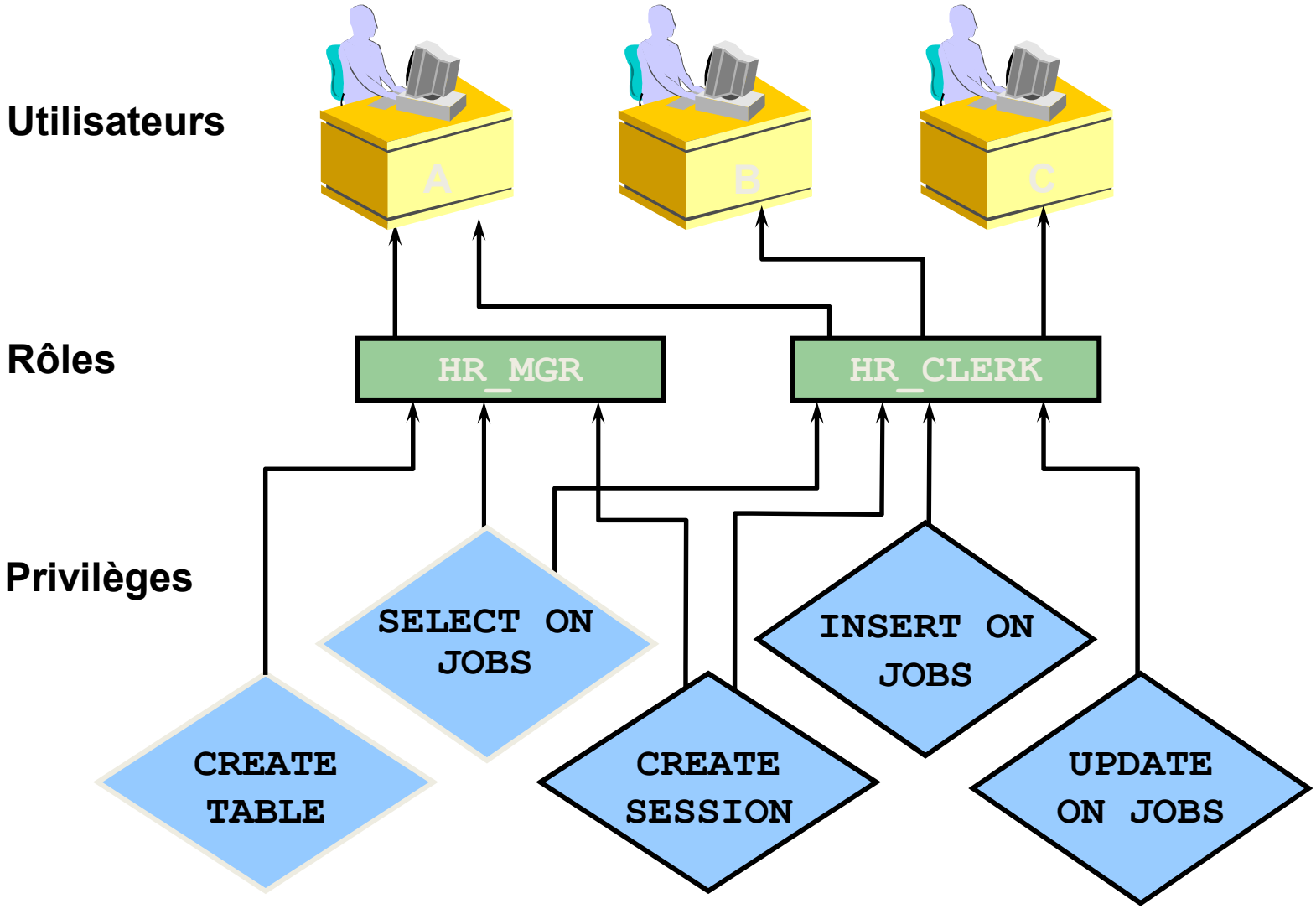
Gérer les rôles

Objectifs

- A la fin de ce chapitre, vous pourrez :
  - créer et modifier des rôles
  - gérer la disponibilité des rôles
  - supprimer des rôles
  - utiliser des rôles prédéfinis
  - afficher des informations sur les rôles à partir du dictionnaire de données

Rôles


Utilisateurs
Rôles
Privilèges
A
B
C
HR_MGR
HR_CLERK
SELECT ON JOBS
INSERT ON JOBS
CREATE TABLE
CREATE SESSION
UPDATE ON JOBS

Rôles

- sont accordés et révoqués.
- peuvent être accordés à tout utilisateur ou rôle. En revanche, un rôle ne peut pas être accordé à lui-même ou de façon circulaire.
- peuvent être constitués de privilèges système et de privilèges objet.
- peuvent être activés ou désactivés pour chaque utilisateur auquel ils ont été accordés.
- peuvent nécessiter un mot de passe pour être activés.
- doivent posséder un nom unique différent des noms utilisateur et des noms de rôle existants.
- n'ont pas de propriétaire et ne se trouvent dans aucun schéma.
- sont décrits dans le dictionnaire de données.

Avantages des rôles

- Gestion simplifiée des privilèges
- Gestion dynamique des privilèges
- Disponibilité sélective des privilèges
- Octroi possible via le système d'exploitation

•

Créer des rôles

- Si vous disposez du privilège système `CREATE ROLE`, vous pouvez créer des rôles à l'aide de l'instruction `CREATE ROLE`.
- Rôles avec l'option `ADMIN` :
  - Non identifié :

```
CREATE ROLE oe_clerk;
```

  - Identifié par mot de passe :

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

  - Identifié de manière externe :

```
CREATE ROLE hr_manager
IDENTIFIED EXTERNALLY;
```

Rôles prédéfinis

Rôles	Description
`CONNECT, RESOURCE, DBA`	Fournis pour garantir une compatibilité descendante
`EXP_FULL_DATABASE`	Privilèges d'export de la base de données
`IMP_FULL_DATABASE`	Privilèges d'import de la base de données
`DELETE_CATALOG_ROLE`	Privilèges `DELETE` sur les tables du dictionnaire de données
`EXECUTE_CATALOG_ROLE`	Privilège `EXECUTE` sur les packages du dictionnaire de données
`SELECT_CATALOG_ROLE`	Privilège `SELECT` sur les tables du dictionnaire de données

Modifier des rôles

- **Utilisez `ALTER ROLE` pour modifier la méthode d'authentification.**
- **Cette commande requiert l'option `ADMIN` ou le privilège `ALTER ANY ROLE`.**

```
ALTER ROLE oe_clerk
IDENTIFIED BY order;
```

```
ALTER ROLE hr_clerk
IDENTIFIED EXTERNALLY;
```

```
ALTER ROLE hr_manager
NOT IDENTIFIED;
```

Accorder des rôles

Pour accorder un rôle, utilisez la commande `GRANT` :

```
GRANT oe_clerk TO scott;
```

```
GRANT hr_clerk TO hr_manager;
```

```
GRANT hr_manager TO scott WITH ADMIN OPTION;
```

RQ:

`GRANT ANY ROLE, WITH ADMIN OPTION` : permet au bénéficiaire d'accorder le rôle à d'autres utilisateurs ou le révoquer, le modifier ou le supprimer

Etablir des rôles par défaut

- **Un utilisateur peut se voir accorder un grand nombre de rôles.**
- **Un utilisateur peut se voir accorder un rôle par défaut.**
- **Vous pouvez limiter le nombre de rôles par défaut d'un utilisateur.**

```
ALTER USER scott
      DEFAULT ROLE hr_clerk, oe_clerk;
```

```
ALTER USER scott DEFAULT ROLE ALL;
```

```
ALTER USER scott DEFAULT ROLE ALL EXCEPT
      hr_clerk;
```

```
ALTER USER scott DEFAULT ROLE NONE;
```

Rôles d'application

- Seuls les packages PL/SQL autorisés peuvent activer des rôles d'application
- La clause de package `USING` permet de créer un rôle d'application

```
CREATE ROLE admin_role
IDENTIFIED USING hr.employee;
```

Activer et désactiver les rôles

- Désactivez un rôle accordé à un utilisateur pour le révoquer temporairement
- Activez un rôle pour l'accorder temporairement
- La commande `SET ROLE` permet d'activer et de désactiver les rôles
- Les rôles par défaut d'un utilisateur sont activés à la connexion
- Un mot de passe peut être requis pour activer un rôle

Activer et désactiver les rôles

- `SET ROLE hr_clerk;`

```
SET ROLE oe_clerk IDENTIFIED BY order;
```

```
SET ROLE ALL EXCEPT oe_clerk;
```

```
SET ROLE {role [ IDENTIFIED BY password ]
          [, role [ IDENTIFIED BY password ]]...
            | ALL [ EXCEPT role [, role ] ...]
                        | NONE }
```

Révoquer des rôles accordés à des utilisateurs

- **La révocation d'un rôle accordé à un utilisateur requiert l'option `ADMIN OPTION` ou le privilège `GRANT ANY ROLE`.**
- **Pour révoquer un rôle, utilisez la syntaxe suivante :**

```
REVOKE oe_clerk FROM scott;
```

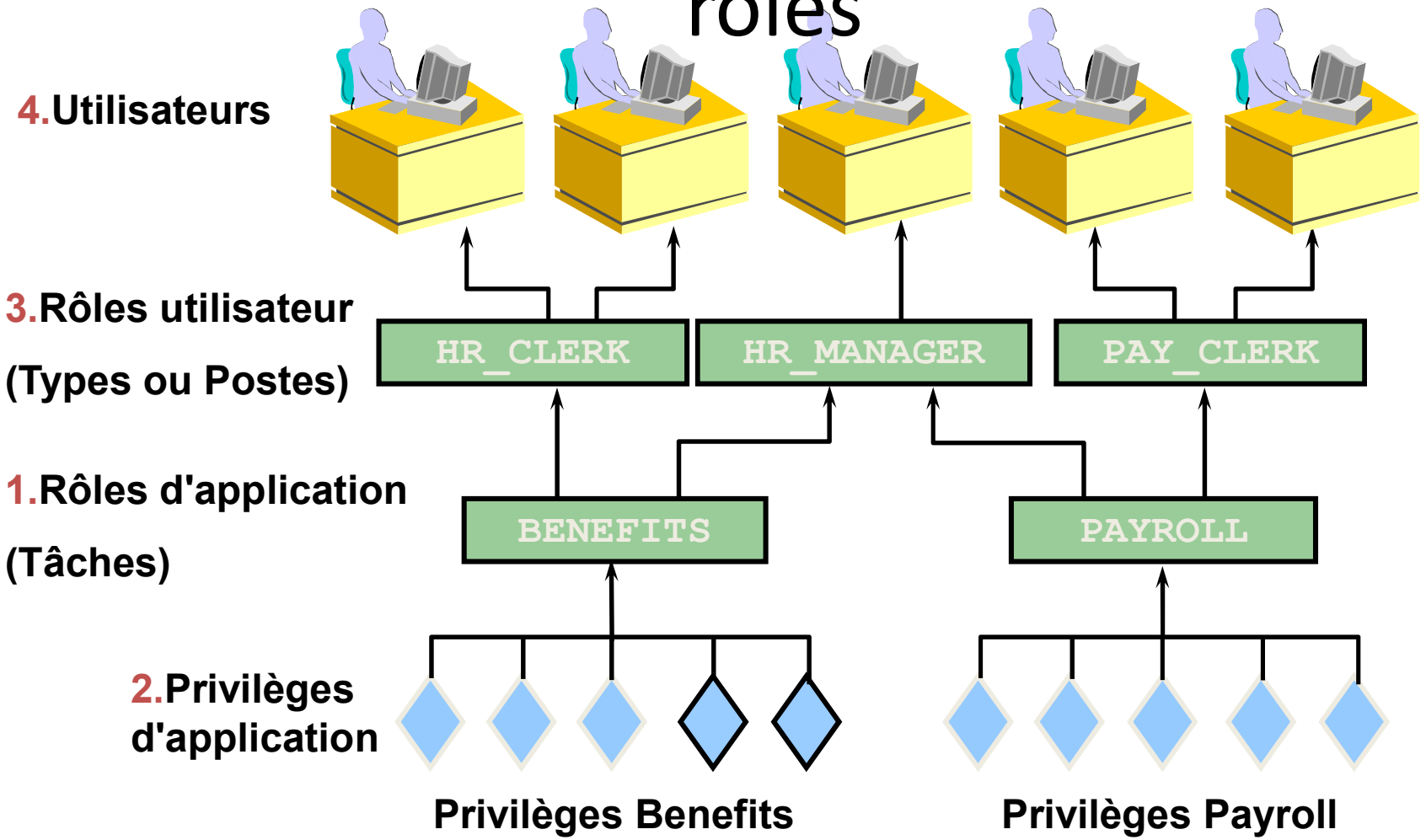
```
REVOKE hr_manager FROM PUBLIC;
```

Supprimer des rôles

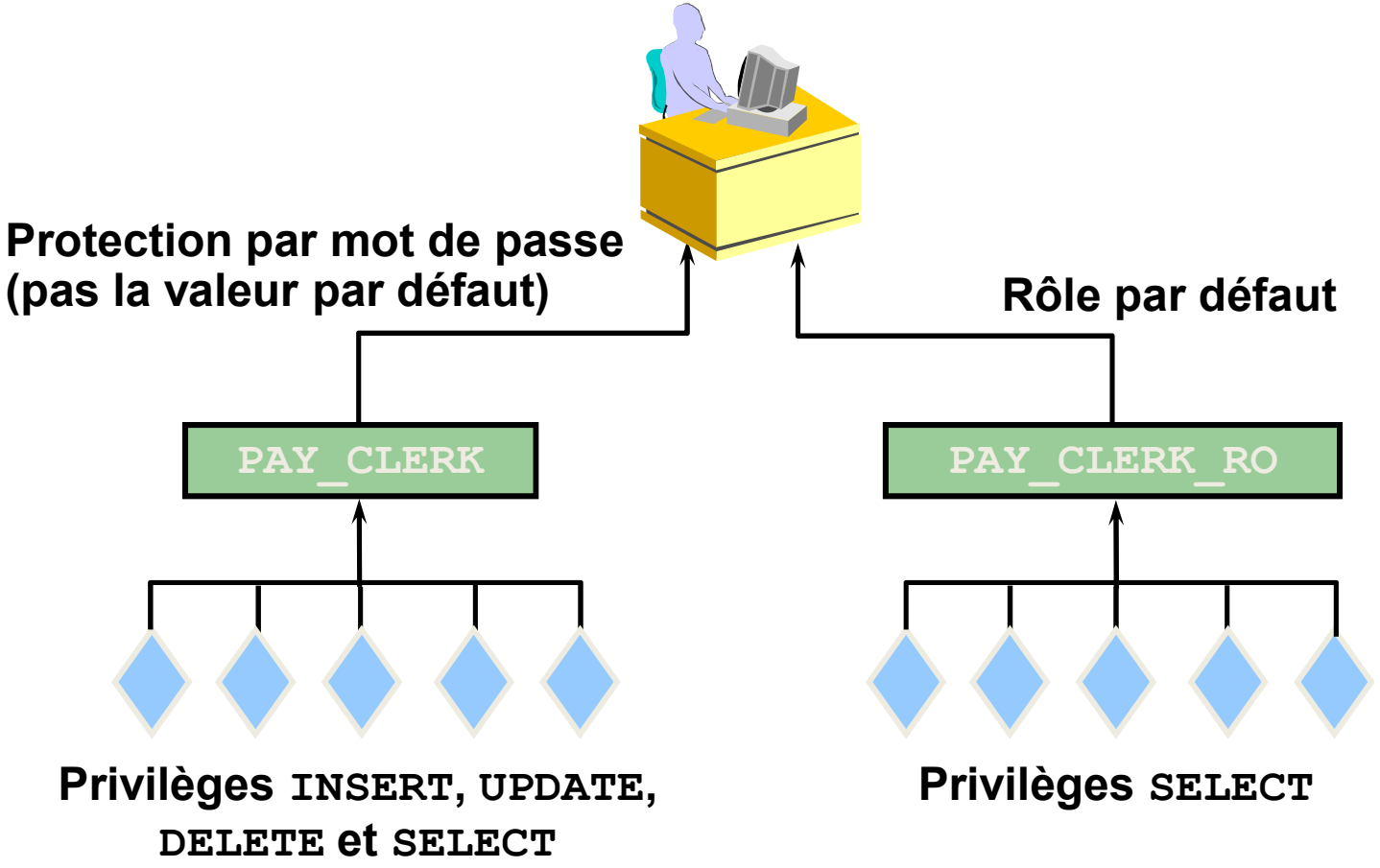
- Lorsque vous supprimez un rôle :
  - il est retiré à tous les utilisateurs et rôles auxquels il était accordé,
  - il est supprimé de la base de données.
- La suppression d'un rôle requiert l'option `ADMIN OPTION` ou le privilège `DROP ANY ROLE`.
- Pour supprimer un rôle, utilisez la syntaxe suivante :

```
DROP ROLE hr_manager;
```

Instructions relatives à la création de rôles



Règles d'utilisation des mots de passe et des rôles par défaut



Obtenir des informations sur les rôles

Pour obtenir des informations sur les rôles, interrogez les vues suivantes du dictionnaire de données :

- **`DBA_ROLES` : Tous les rôles qui existent dans la base de données**
- **`DBA_ROLE_PRIVS` : Rôles accordés à des utilisateurs et à des rôles**
- **`ROLE_ROLE_PRIVS` : Rôles accordés à des rôles**
- **`DBA_SYS_PRIVS` : Privilèges système accordés à des utilisateurs et à des rôles**
- **`ROLE_SYS_PRIVS` : Privilèges système accordés à des rôles**
- **`ROLE_TAB_PRIVS` : Privilèges objet accordés à des rôles**
- **`SESSION_ROLES` : Rôles activés par l'utilisateur**

Synthèse

- Ce chapitre vous a permis d'apprendre à :
  - créer des rôles
  - accorder des privilèges à des rôles
  - accorder des rôles à des utilisateurs ou à des rôles
  - établir des rôles par défaut