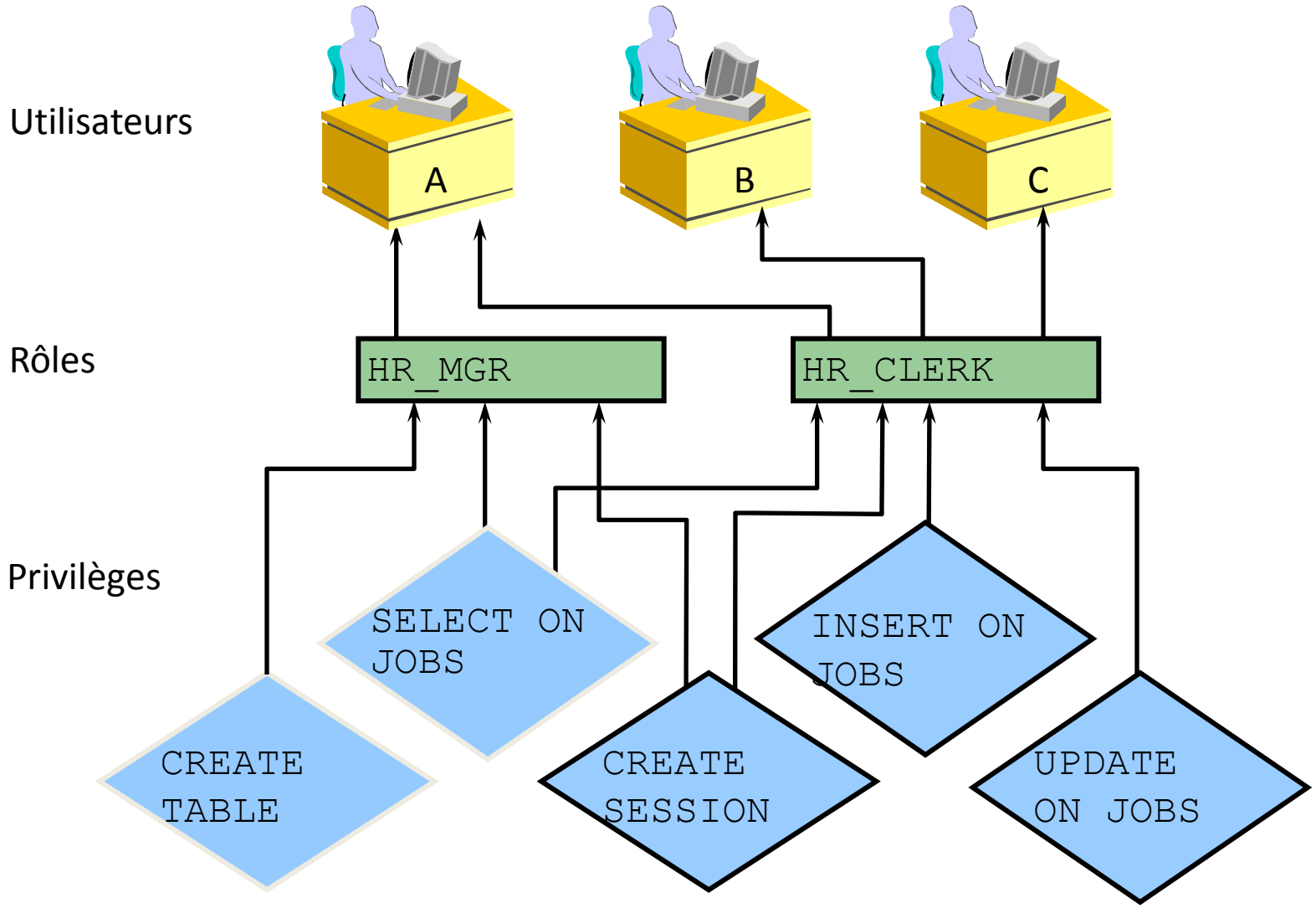
Gérer les rôles

Rôles


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

Rôles

- Les rôles sont des groupes nommés de privilèges associés qui sont accordés à des utilisateurs ou à d'autres rôles.
- Ils facilitent l'administration des privilèges dans une base de données.
- **Les rôles :**
  - sont accordés et révoqués à l'aide des commandes qui permettent d'accorder et de révoquer des privilèges système.
  - 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 :** au lieu d'accorder les mêmes privilèges à plusieurs utilisateurs, accorder les privilèges à un rôle et associer ce rôle à chaque utilisateur.
- **Gestion dynamique des privilèges :** En cas de modification des privilèges associés à un rôle, tous les utilisateurs auxquels ce rôle a été accordé bénéficient automatiquement et immédiatement des nouveaux privilèges.
- **Disponibilité sélective des privilèges :** activer et désactiver les rôles pour activer et désactiver temporairement les privilèges. L'activation d'un rôle permet également de vérifier qu'un utilisateur dispose de ce rôle.
- **Octroi possible via le système d'exploitation :** utiliser des commandes ou des utilitaires du système d'exploitation pour accorder des rôles aux utilisateurs dans la base de données.

Créer des rôles

- 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;
```

Créer des rôles

- Si vous disposez du privilège système `CREATE ROLE`, vous pouvez créer des rôles à l'aide de l'instruction `CREATE ROLE`.
- Lorsque vous créez un rôle défini comme `NOT IDENTIFIED`, `IDENTIFIED EXTERNALLY` ou `BY password`, Oracle l'accorde avec l'option `ADMIN`.
- Utilisez la commande suivante pour créer un rôle :

```
CREATE ROLE role [NOT IDENTIFIED |
  IDENTIFIED
  {BY password | EXTERNALLY | GLOBALLY
  | USING package}]
```

Créer des rôles

Où :

- `role` : correspond au nom du rôle.
- `NOT IDENTIFIED` : indique qu'aucune vérification n'est nécessaire lorsque le rôle est activé.
- `IDENTIFIED` : indique qu'une vérification est nécessaire lorsque le rôle est activé.
- `BY password` : fournit le mot de passe que l'utilisateur doit indiquer pour activer le rôle.
- `USING package` : crée un rôle d'application, qui ne peut être activé que par des applications utilisant un package autorisé.
- `EXTERNALLY` : indique que l'utilisateur doit avoir reçu une autorisation d'un service externe (tel que le système d'exploitation ou un service tiers) pour activer le rôle.
- `GLOBALLY` : indique que l'utilisateur doit être autorisé par le service de répertoire d'entreprise à utiliser le rôle pour l'activer à l'aide de l'instruction `SET ROLE` ou à la connexion.

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;
```

Modifier des rôles

- Vous ne pouvez modifier un rôle que pour changer sa méthode d'authentification. Pour cela, vous devez disposer du rôle approprié avec l'option `ADMIN` ou du privilège système `ALTER ANY ROLE`.
- Utilisez la commande suivante pour modifier un rôle :

```
ALTER ROLE role {NOT IDENTIFIED |
IDENTIFIED
 {BY password |USING package|
EXTERNALLY | GLOBALLY }};
```

Modifier des rôles

Où :

- `role` : correspond au nom du rôle.
- `NOT IDENTIFIED` : indique qu'aucune vérification n'est nécessaire lorsque le rôle est activé.
- `IDENTIFIED` : indique qu'une vérification est nécessaire lorsque le rôle est activé.
- `BY password` : fournit le mot de passe permettant d'activer le rôle.
- `EXTERNALLY` : indique que l'utilisateur doit avoir reçu une autorisation d'un service externe (tel que le système d'exploitation ou un service tiers) pour activer le rôle.
- `GLOBALLY` : indique que l'utilisateur doit être autorisé par le service de répertoire d'entreprise à utiliser le rôle pour l'activer à l'aide de l'instruction `SET ROLE` ou à la connexion.

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;
```

Accorder des rôles

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

```
GRANT role [, role ]...
   TO {user|role|PUBLIC}
    [, {user|role|PUBLIC} ]...
   [WITH ADMIN OPTION]
```

Où :

`role` : correspond à un ensemble de rôles à accorder.

`PUBLIC` : accorde le rôle à tous les utilisateurs.

`WITH ADMIN OPTION` : permet au bénéficiaire d'accorder le rôle à d'autres utilisateurs ou rôles. Si vous accordez un rôle avec cette option, le bénéficiaire peut l'accorder à d'autres utilisateurs ou le révoquer, le modifier ou le supprimer.

Accorder des rôles

L'utilisateur qui crée un rôle le reçoit de façon implicite avec l'option `ADMIN OPTION`. Un utilisateur qui n'a pas reçu de rôle avec cette option doit disposer du privilège système `GRANT ANY ROLE` pour accorder des rôles aux autres utilisateurs ou révoquer des rôles accordés.

Remarque : Le paramètre d'initialisation `MAX_ENABLED_ROLES` définit le nombre maximum de rôles de base de données que les utilisateurs peuvent activer.

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;
```

Etablir des rôles par défaut

- Un utilisateur peut disposer d'un grand nombre de rôles.
- Un rôle par défaut est un sous-ensemble de ces rôles activé automatiquement lorsque l'utilisateur se connecte. Par défaut, tous les rôles d'un utilisateur sont activés à la connexion sans indication de mot de passe.
- La commande `ALTER USER` permet de limiter les rôles par défaut d'un utilisateur.
- La clause `DEFAULT ROLE` s'applique uniquement aux rôles qui ont été accordés directement à l'utilisateur via une instruction `GRANT`. Elle ne permet pas d'activer :
    - les rôles qui n'ont pas été accordés à l'utilisateur,
    - les rôles qui ont été accordés par l'intermédiaire d'autres rôles,
    - les rôles gérés par un service externe (le système d'exploitation, par exemple).

Etablir des rôles par défaut

Syntaxe: `ALTER USER user DEFAULT ROLE {role [,role]... | ALL [EXCEPT role [,role]... ] | NONE}`

Où :

`user` : correspond au nom de l'utilisateur qui reçoit les rôles.

`role` : correspond au rôle par défaut de l'utilisateur.

`ALL` : transforme tous les rôles accordés à l'utilisateur en rôles par défaut, à l'exception de ceux figurant dans la clause `EXCEPT` (valeur par défaut).

`EXCEPT` : indique que les rôles qui suivent ne doivent pas être inclus dans les rôles par défaut.

`NONE` : ne convertit aucun des rôles accordés à l'utilisateur en rôle par défaut (lors de la connexion, l'utilisateur ne dispose que des privilèges qui lui ont été accordés directement).

Etant donné que les rôles doivent être accordés pour pouvoir être définis comme rôles par défaut, vous ne pouvez pas définir de rôles par défaut à l'aide de la commande `CREATE USER`.

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;
```

- Dans l'exemple, `admin_role` est un rôle d'application qui ne peut être activé que par les modules définis dans le package PL/SQL `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

- **Restrictions**
  - Vous ne pouvez pas activer un rôle à partir d'une procédure stockée, car cette action peut modifier le domaine de sécurité (ensemble de privilèges) qui a permis d'appeler la procédure.
  - Si une procédure stockée contient la commande `SET ROLE`, l'erreur suivante se produit à l'exécution :

```
ORA-06565: cannot execute SET ROLE
  from within stored procedure
```

Activer et désactiver les rôles

- La commande `SET ROLE` désactive tous les autres rôles accordés à l'utilisateur.

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

- Où :
  - `role` : correspond au nom du rôle.
  - `IDENTIFIED BY password` : fournit le mot de passe permettant d'activer le rôle.

Activer et désactiver les rôles

- Où :
  - `ALL` : active tous les rôles accordés à l'utilisateur en cours, à l'exception de ceux figurant dans la clause `EXCEPT` (vous ne pouvez pas utiliser cette option pour activer des rôles nécessitant des mots de passe).
  - `EXCEPT role` : n'active pas les rôles indiqués.
  - `NONE` : désactive tous les rôles de la session en cours (seuls les privilèges accordés directement à l'utilisateur sont actifs).
  - L'option `ALL` sans la clause `EXCEPT` ne fonctionne que lorsque les rôles activés ne nécessitent pas de mot de passe.

Activer et désactiver les rôles

- `SET ROLE hr_clerk;`

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

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

Révoquer des rôles accordés à des utilisateurs

- L'instruction SQL `REVOKE` permet de révoquer un rôle accordé à un utilisateur.
- Tout utilisateur possédant un rôle avec l'option `ADMIN` peut retirer ce rôle à un autre utilisateur ou rôle de la base de données.
- Les utilisateurs disposant du privilège `GRANT ANY ROLE` peuvent révoquer n'importe quel rôle.

Révoquer des rôles accordés à des utilisateurs

- Syntaxe

```
REVOKE role [, role ]
  FROM {user|role|PUBLIC}
    [, {user|role|PUBLIC} ]
```

- où :
  - role : correspond au rôle à révoquer ou au rôle à partir duquel des rôles doivent être révoqués.
  - user : définit l'utilisateur dont les privilèges système ou les rôles doivent être révoqués.
  - PUBLIC : révoque le privilège ou le rôle accordé à tous les utilisateurs.

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

- Syntaxe :

  `DROP ROLE role`
- 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`.

```
DROP ROLE hr_manager;
```

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