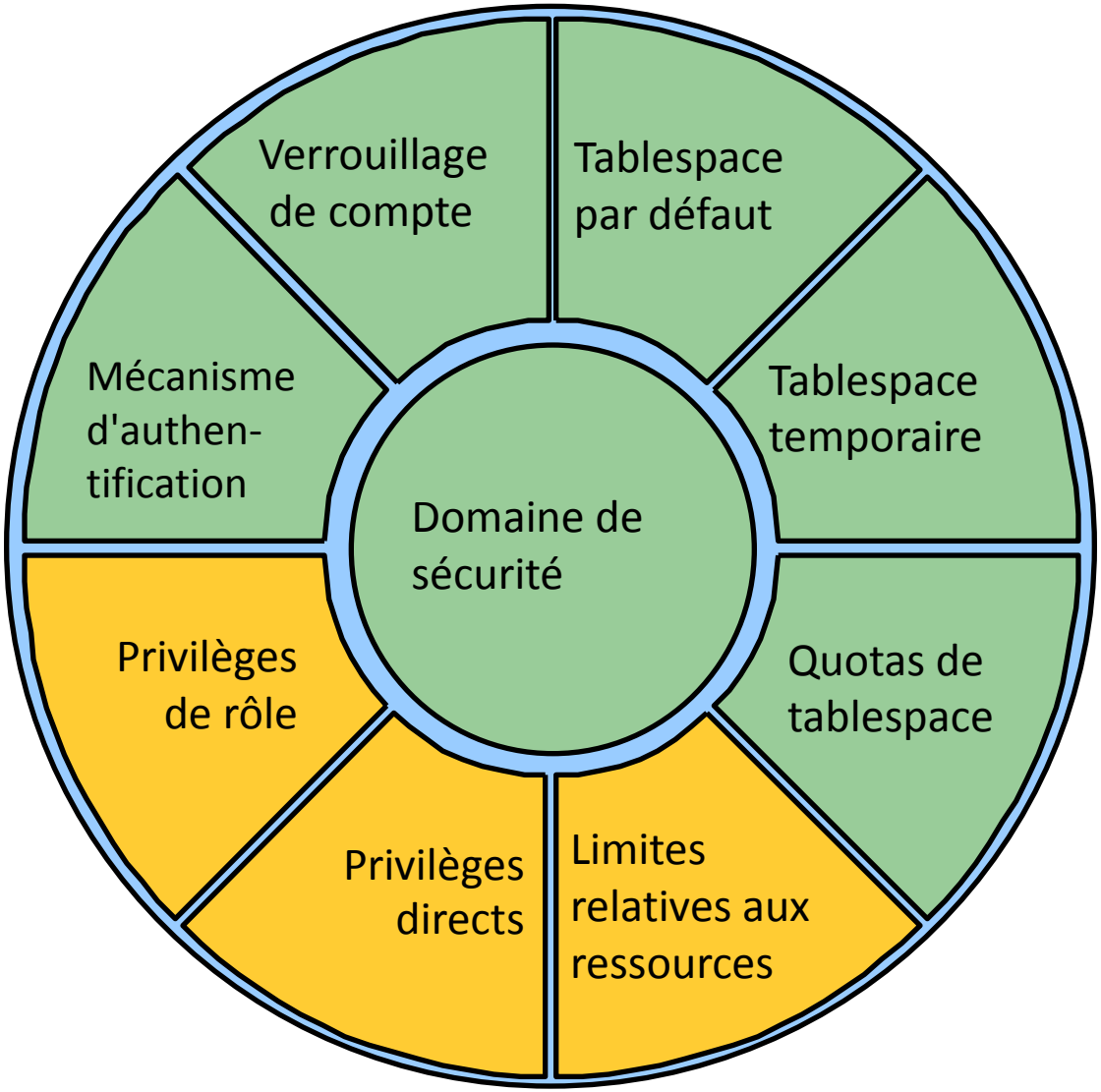
Gérer les utilisateurs

Utilisateurs et sécurité



Utilisateurs et sécurité

- Un schéma est un ensemble nommé d'objets.
- Lorsqu'un utilisateur est créé, un schéma correspondant est également créé.
- 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

Liste de contrôle pour la création d'utilisateurs

- Identifiez les tablespaces dans lesquels l'utilisateur a besoin de stocker des objets.
- Déterminez les quotas applicables pour chaque tablespace.
- Affectez un tablespace par défaut et un tablespace temporaire.
- Créez un utilisateur.
- Accordez des privilèges et des rôles à l'utilisateur.

Créer un utilisateur : authentification par la base de données

Syntaxe :

Utilisez la commande suivante pour créer un utilisateur :

```
CREATE USER user
IDENTIFIED {BY password | EXTERNALLY}
[ DEFAULT TABLESPACE tablespace ]
[ TEMPORARY TABLESPACE tablespace ]
[ QUOTA {integer [K | M ] | UNLIMITED } ON
tablespace
[ QUOTA {integer [K | M ] | UNLIMITED } ON
tablespace  ]...]
[ PASSWORD EXPIRE ]
[ ACCOUNT { LOCK | UNLOCK }]
[ PROFILE { profile | DEFAULT }]
```

Créer un utilisateur : authentification par la base de données

Où :

`BY password` indique que l'utilisateur est authentifié par la base de données et qu'il doit fournir un mot de passe pour se connecter.

`EXTERNALLY` indique que l'utilisateur est authentifié par le système d'exploitation.

`GLOBALLY AS` indique que l'utilisateur est authentifié de façon globale.

`DEFAULT TABLESPACE` ou `TEMPORARY TABLESPACE` désigne le tablespace par défaut ou le tablespace temporaire de l'utilisateur.

`QUOTA` définit l'espace maximum alloué aux objets détenus par l'utilisateur dans le tablespace.

Le mot-clé `UNLIMITED` permet d'indiquer que les objets détenus par l'utilisateur peuvent utiliser l'ensemble de l'espace disponible du tablespace.

Créer un utilisateur : authentification par la base de données

Où :

`PASSWORD EXPIRE` force l'utilisateur à réinitialiser le mot de passe lorsqu'il se connecte à la base de données à l'aide de SQL*Plus (cette option n'est valide que si l'utilisateur est authentifié par la base de données).

`ACCOUNT LOCK/UNLOCK` permet de verrouiller ou de déverrouiller explicitement le compte de l'utilisateur (la valeur par défaut est `UNLOCK`).

`PROFILE` permet de contrôler l'utilisation des ressources et de définir le mécanisme de contrôle par mot de passe à appliquer à l'utilisateur.

Créer un utilisateur : authentification par la base de données

- Définissez le mot de passe initial :

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

Créer un utilisateur : authentification par le système d'exploitation

- Le paramètre d'initialisation `OS_AUTHENT_PREFIX` indique le format des noms utilisateur.
- Sa valeur par défaut est `OPS$`.

```
CREATE USER aaron
IDENTIFIED EXTERNALLY
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE temp
QUOTA 15m ON data;
```

Modifier les quotas de tablespace d'un utilisateur

- Vous pouvez modifier les quotas de tablespace d'un utilisateur dans les cas suivants :
  - lorsque la taille des tables appartenant à l'utilisateur augmente de manière imprévue,
  - lorsqu'une application est étendue et nécessite des tables ou des index supplémentaires,
  - lorsque les objets sont réorganisés et placés dans des tablespaces différents.
- Procédez comme suit pour modifier le quota de tablespace d'un utilisateur :

```
ALTER USER aaron
QUOTA 0 ON USERS;
```

Modifier les quotas de tablespace d'un utilisateur

Syntaxe:

```
ALTER USER user
[ DEFAULT TABLESPACE tablespace]
[ TEMPORARY TABLESPACE tablespace]
[ QUOTA {integer [K | M] | UNLIMITED } ON
tablespace
[ QUOTA {integer [K | M] | UNLIMITED } ON
tablespace ]   ...]
```

- Si vous définissez un quota de 0, les objets de l'utilisateur sont conservés dans le tablespace révoqué, mais aucun nouvel espace ne peut leur être alloué.
- Les options non modifiées ne sont pas affectées.
- Le privilège `UNLIMITED TABLESPACE` est prioritaire sur les paramètres des quotas.

Supprimer un utilisateur

- Syntaxe
  - `DROP USER user [CASCADE]`
- Règles :
  - L'option `CASCADE` supprime tous les objets du schéma avant de supprimer l'utilisateur. Elle doit être définie si le schéma contient des objets.
  - Vous ne pouvez pas supprimer un utilisateur connecté au serveur Oracle.

```
DROP USER aaron CASCADE;
```

Obtenir des informations sur les utilisateurs

- Interrogez les vues suivantes pour obtenir des informations sur les utilisateurs :
  - DBA_USERS
  - DBA_TS_QUOTAS
- EXP : rechercher le tablespace par défaut de tous les utilisateurs
  - SQL> SELECT username, default_tablespace
    2 FROM dba_users;

```
USERNAME   DEFAULT_TABLESPACE
---------  ------------------
SYS        SYSTEM
SYSTEM     SYSTEM
OUTLN      SYSTEM
DBSNMP     SYSTEM
HR         SAMPLE
OE         SAMPLE
```

Gérer les privilèges

Gérer les privilèges

- Il existe deux types de privilèges utilisateur Oracle :
  - Système : permet aux utilisateurs de réaliser certaines actions dans la base de données
  - Objet : permet aux utilisateurs d'accéder à un objet donné et de le manipuler

Privilèges système

- 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.
- La commande `GRANT` permet d'accorder un privilège à un utilisateur ou un groupe d'utilisateurs.
- La commande `REVOKE` supprime les privilèges.

Privilèges système : exemples

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

Accorder des privilèges système

- Utilisez la commande `GRANT` pour accorder des privilèges système.
- Le bénéficiaire peut accorder le privilège système à d'autres utilisateurs grâce à l'option `ADMIN`.

```
GRANT CREATE SESSION TO emi;
```

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

Accorder des privilèges système

- Syntaxe:

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

- Où:
  - `system_privilege` : désigne le privilège système à accorder.
  - `role` : désigne le nom du rôle à accorder.
  - `PUBLIC` : accorde le privilège système à tous les utilisateurs.
  - `WITH ADMIN OPTION` : autorise le bénéficiaire à accorder son privilège ou son rôle à d'autres utilisateurs ou rôles.

Privilèges 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

Révoquer des privilèges système

- Utilisez la commande `REVOKE` pour révoquer un privilège système accordé à un utilisateur.
- Les utilisateurs qui disposent d'un privilège système avec l'option `ADMIN OPTION` peuvent révoquer des privilèges système.
- Seuls les privilèges accordés via la commande `GRANT` peuvent être révoqués.

```
REVOKE CREATE TABLE FROM emi;
```

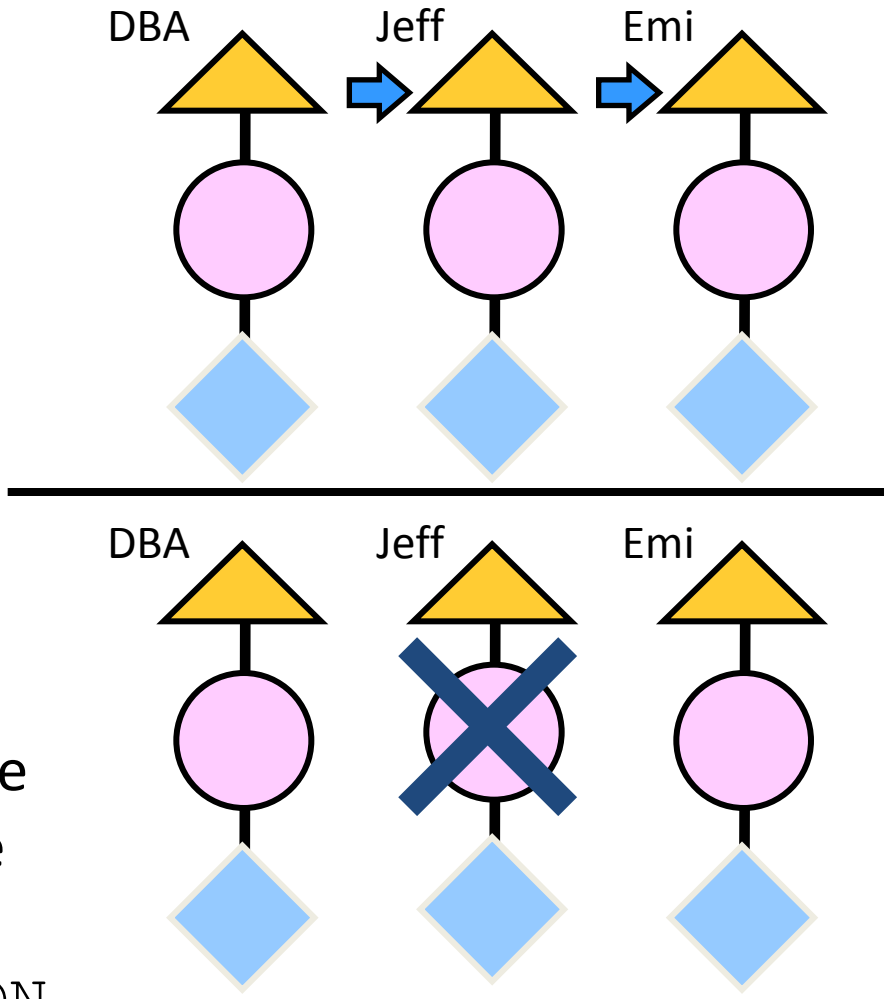
Révoquer des privilèges système

- Syntaxe

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

- **Remarque :**
  - La commande `REVOKE` permet uniquement la révocation des privilèges système accordés directement à l'aide de la commande `GRANT`.
  - La révocation de privilèges système peut avoir un impact sur certains objets dépendants. Par exemple, si vous accordez le privilège `SELECT ANY TABLE` à un utilisateur qui a créé des procédures ou des vues utilisant une table d'un autre schéma, la révocation de ce privilège invalide ces procédures ou vues.

Révoquer des privilèges système accordés avec l'option `ADMIN OPTION`



La révocation d'un privilège système n'entraîne aucun effet de cascade, que le privilège ait été accordé avec l'option `ADMIN OPTION` ou non.

Privilèges objet

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

Privilèges objet

- Un privilège objet est un privilège ou droit autorisant la réalisation d'une action donnée sur une table, une vue, une séquence, une procédure, une fonction ou un package spécifique.
- Chaque objet présente un ensemble propre de privilèges pouvant être accordés.
- Vous pouvez restreindre les privilèges `UPDATE`, `REFERENCES` et `INSERT` en précisant un sous-ensemble de colonnes pouvant être mises à jour.
- Vous pouvez limiter un droit de type `SELECT` en créant une vue présentant un sous-ensemble de colonnes et en accordant le privilège `SELECT` sur la vue.
- Un privilège accordé sur un synonyme octroie directement un droit sur la table de base référencée par ce synonyme.

Accorder des privilèges objet

- Utilisez la commande `GRANT` pour accorder des privilèges objet.
- L'objet doit se trouver dans votre schéma ou vous devez avoir reçu le privilège avec l'option `GRANT OPTION`.

```
GRANT EXECUTE ON dbms_output TO jeff;
```

```
GRANT UPDATE ON emi.customers TO jeff WITH
GRANT OPTION;
```

Accorder des privilèges objet

- Syntaxe

```
GRANT { object_privilege [(column_list)]
   [, object_privilege [(column_list)] ]...
   |ALL [PRIVILEGES]}
ON [schema.]object
TO {user|role|PUBLIC}[, {user|role|PUBLIC}
  ]...
  [WITH GRANT OPTION]
```

- Où :
  - `object_privilege` désigne le privilège objet à accorder.
  - `column_list` désigne une colonne de table ou de vue (cette valeur ne peut être définie que lors de l'octroi du privilège `INSERT`, `REFERENCES` ou `UPDATE`).
  - `ALL accorde tous les privilèges objet qui ont été accordés avec l'option WITH GRANT OPTION.`

Accorder des privilèges objet

- Où (suite):
  - `ON object` identifie l'objet sur lequel les privilèges doivent être accordés.
  - `WITH GRANT OPTION` autorise le bénéficiaire à accorder ses privilèges objet à d'autres utilisateurs ou rôles.
- Utilisez l'instruction `GRANT` pour accorder des privilèges objet.
  - Pour cela, l'objet doit se trouver dans votre schéma ou vous devez avoir reçu le privilège avec l'option `GRANT OPTION`.
  - Par défaut, si vous disposez d'un objet, tous les privilèges associés vous sont automatiquement accordés.
  - Par souci de sécurité, soyez prudent lorsque vous accordez à d'autres utilisateurs des privilèges sur vos objets.

Révoquer des privilèges objet

- Utilisez la commande `REVOKE` pour révoquer des privilèges objet.
- Seul l'utilisateur qui a accordé un privilège objet peut le révoquer.

```
REVOKE SELECT ON emi.orders FROM jeff;
```

Révoquer des privilèges objet

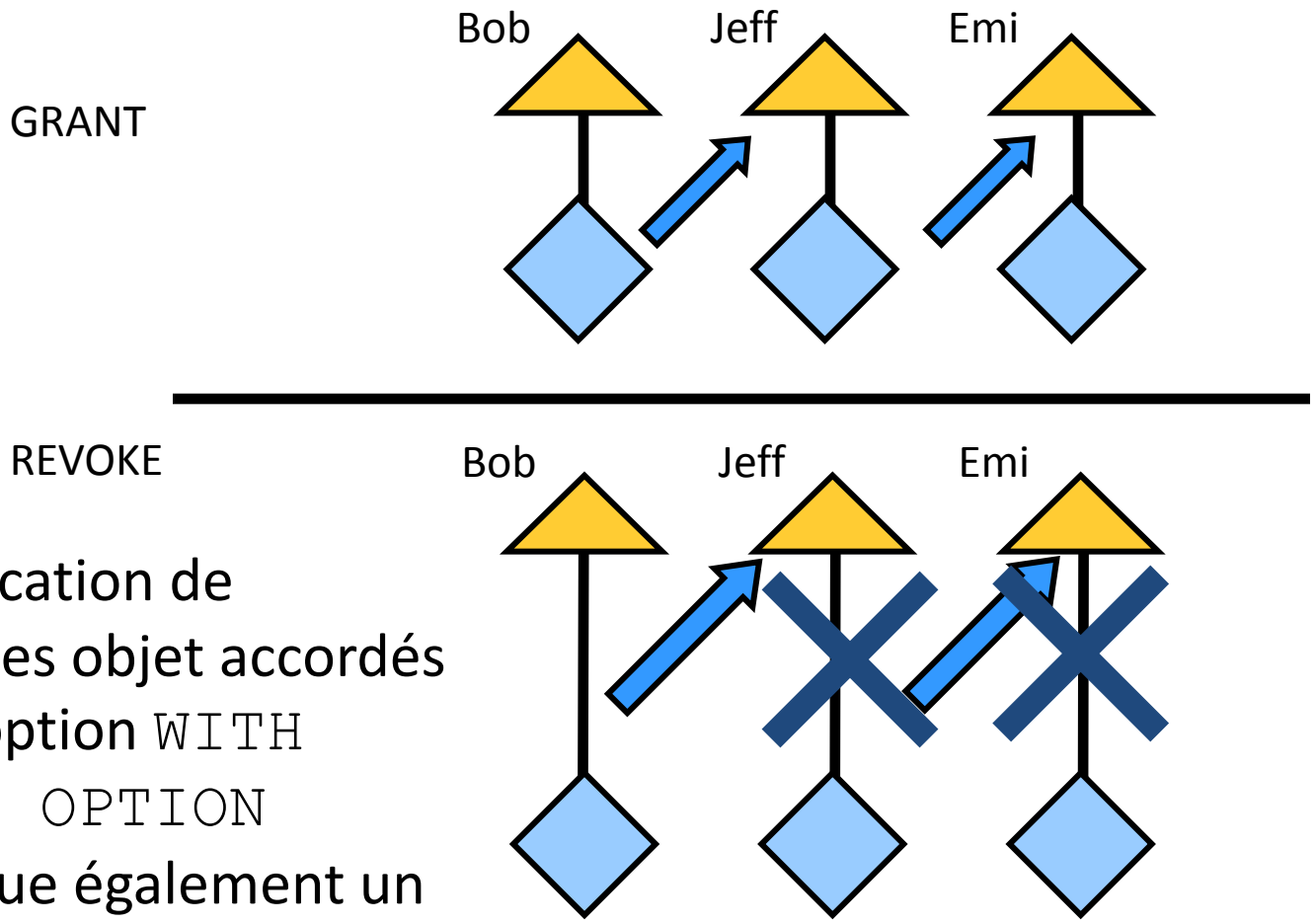
- Syntaxe

```
REVOKE { object_privilege
   [, object_privilege ]...
   | ALL [PRIVILEGES] }
ON[schema.]object
FROM {user|role|PUBLIC}
   [, {user|role|PUBLIC} ]...
   [CASCADE CONSTRAINTS]
```

Révoquer des privilèges objet

- Où :
  - `object_privilege` désigne le privilège objet à révoquer.
  - `ALL` révoque tous les privilèges objet accordés à l'utilisateur.
  - `ON` désigne l'objet sur lequel les privilèges objet doivent être révoqués.
  - `FROM` identifie les utilisateurs ou les rôles dont les privilèges objet sont révoqués.
  - `CASCADE CONSTRAINTS` supprime toutes les contraintes d'intégrité référentielle définies à l'aide du privilège `REFERENCES` ou `ALL`.
- **Restriction :**
  - Les utilisateurs qui accordent des privilèges objet peuvent les révoquer uniquement aux utilisateurs auxquels ils les ont accordés.

Révoquer les privilèges objet accordés avec l'option `WITH GRANT OPTION`



La révocation de privilèges objet accordés avec l'option `WITH GRANT OPTION` provoque également un effet de cascade.

Obtenir des informations sur les privilèges

- Interrogez les vues suivantes pour obtenir des informations sur les privilèges :
  - `DBA_SYS_PRIVS` affiche la liste des privilèges système accordés aux utilisateurs et aux rôles.
  - `SESSION_PRIVS` affiche la liste des privilèges auxquels l'utilisateur a accès.
  - `DBA_TAB_PRIVS` affiche la liste de tous les octrois de privilèges sur les objets de la base de données.
  - `DBA_COL_PRIVS` décrit tous les octrois de privilèges sur les colonnes de la base de données.