Cours : Systèmes de Gestion de Bases de Données
A/U : 2021/2022

Chapitre 4:
Administrer la sécurité utilisateur

PLAN

A. Les utilisateurs
   I. Création d'un utilisateur
   II. Modification d'un utilisateur
   III. Suppression d'un utilisateur
   IV. Informations sur les utilisateurs
B. Les privilèges
   I. Présentation
   II. Assigner des privilèges système à un user Les rôles
   III. Assigner des privilèges système à un user Les rôles
   IV. Principes généraux
   V. Retirer des privilèges système
C. Les rôles
   I. Présentation
   II. Création d'un rôle
   III. Assignation d'un rôle
   IV. Rôles standards sous Oracle
   V. Suppression d'un rôle
D. Les profils
   I. Présentation
   II. Les limitations de mot de passe
   III. Les limitations des ressources systèmes
   IV. Création d'un profil
   V. Modification d'un profil
   VI. Surpression d'un profil

A- Les utilisateurs

I- Création d'un utilisateur

Plusieurs étapes sont nécessaire pour la création d'un utilisateur

- Choisir un nom d'utilisateur
- Choisir une méthode d'authentification
- Choisir les TABLESPACEs que l'utilisateur pourra utiliser
- Définir les quotas sur chaque TABLESPACEs
- Définir les TABLESPACEs par défaut de l'utilisateur
- Créer l'utilisateur
- Assigner les rôles et privilèges à l'utilisateur

I- Création d'un utilisateur…

1. Définition :

- Un utilisateur de BD correspond à un login
- Il possède des privilèges.
- Il dispose d'un espace de stockage pour ses objets
- Les objets d'un utilisateur sont crées dans son schéma.

I- Création d'un utilisateur…

2. Choix du nom de l'utilisateur:

Créer un utilisateur consiste à lui définir un login :

- Taille maximale 30 caractères.
- Ne contient que des lettres se [a-z] et des chiffres [0-9]
- Les symboles #,$,_ sont acceptés.

Le login doit commencer par une lettre, pour créer des logins composés uniquement de chiffres, il faut l'encadrer par des " ".

Les guillemets rendent le login sensible à la casse.

" ALI" n'est pas identique à *ali*

I- Création d’un utilisateur…

3. Choix de la méthode d’identification :

Il existe 2 types d'authentification :

- Authentification par la base de données.
- Authentification par le système d'exploitation.

I- Création d'un utilisateur…

3.1 Authentification par la BD

- Ce mode, le plus courant, est le mode par défaut.
- l'utilisateur est authentifié avec le mot de passe stocké dans la base de données.

Syntaxe :

IDENTIFIED BY <password>

Exemple :

SQL>CREATE USER ali **IDENTIFIED BY** ali_ali;
SQL>CONNECT ali/ali_ali;

I- Création d'un utilisateur…

3.2 Authentification par l'OS

- Ce mode permettra à Oracle de se baser sur l'authentification de l'utilisateur par le système d'exploitation.

Syntaxe :

IDENTIFIED EXTERNALLY

I- Création d’un utilisateur…

4. Choix des TABLESPACEs :

- Pour des raisons de sécurité, on peut restreindre le champ d'action de l'utilisateur en choisissant les tablespaces que celui-ci sera en mesure d'utiliser.

- Il est très fortement déconseillé d'autoriser un utilisateur à utiliser le tablespace SYSTEM, qui doit impérativement rester dédié au dictionnaire de données.

I- Création d'un utilisateur…

5. Définir les QUOTAs du user :

- Une fois les tablespaces identifiés, l'étape suivante va consister à définir l'espace alloué à l'utilisateur sur chacun des tablespaces.

- Voici les différentes options disponibles pour les quotas :
  - Une taille en K (KiloBytes) ou en M (MegaBytes)
  - Unlimited

Exemple :

…
QUOTA 5M **ON** TBS_USERS
QUOTA UNLIMITED ON TMP_USERS
…
…

I- Création d'un utilisateur…

6. Choisir les TABLESPACEs par défaut de l'utilisateur :

- Cette étape va permettre de définir le *tablespace de parmenent* et le *tablespace temporaire* de l'utilisateur.
- Cette étape est indispensable pour éviter toute écriture dans le tablespace SYSTEM (qui est assigné si aucun tablespace par défaut n'est défini).

Syntaxe :

DEFAULT TABLESPACE nom_tablespace : pour le tablespace parmenent
TEMPORARY TABLESPACE nom_tablespace : pour le tablespace temporaire.

Exemple :

...
DEFAULT TABLESPACE tbs_user
TEMPORARY TABLESPACE tmp_user ... ...
...

I- Création d'un utilisateur…

7. Exemples :

```
CREATE USER salah IDENTIFIED
BY h_salah;
```

```
CREATE USER Aymen
IDENTIFIED BY L_aymen DEFAULT
TABLESPACE example QUOTA 10M on
example  TEMPORARY TABLESPACE
temp QUOTA  5M ON data
QUOTA  10M ON tools
PROFILE p_user
PASSWORD EXPIRE
ACCOUNT LOCK;
```

II- Modification d'un utilisateur…

Syntaxe :

SQL>ALTER USER < login user > …

Exemples :

1. **ALTER USER** aymen **IDENTIFIED BY** k_aymen
2. **ALTER USER** aymen **QUOTA** 15M **ON** example **QUOTA** 0M **ON** tools;
3. **ALTER USER** aymen **DEFAULT TABLESPACE** tbs_users2 **TEMPORARY TABLESPACE** tmp2;
4. **ALTER USER** aymen **ACCOUNT LOCK**;
5. **ALTER USER** aymen **ACCOUNT UNLOCK**;

III- Suppression d'un utilisateur…

un utilisateur connecté à la base ne pourra pas être supprimé.

Syntaxe :

- un utilisateur avec un schéma vide : **DROP USER** < login user >;

- un utilisateur avec son schéma : **DROP USER** < login user > **CASCADE**;
  - Oracle effacera tous les objets contenus dans le schéma de l'utilisateur.
  - Si le schéma contient des tables, Oracle effacera toutes les contraintes d'intégrités des tables et toutes les contraintes d'intégrités dans les schémas d'autres utilisateurs qui faisaient références aux contraintes UNIQUE et PRIMARY KEY du schéma qui est en cours de suppression.
  - Oracle supprimera aussi tous les index liés aux colonnes des tables, ainsi que tout les triggers, les types de données.
  - Oracle invalidera mais ne supprimera pas les objets contenus dans d'autres schéma mais qui faisaient références au schéma supprimé.
  - Par contre, Oracle ne supprimera pas les rôles créés par l'utilisateur.

Exemple : **DROP USER** aymen **CASCADE**;

IV- Information sur les utilisateurs

Les vues utiles pour obtenir des informations sur les utilisateurs :

- ***DBA_USERS***
- ***DBA_TS_QUOTAS***
- ***USER_USERS***
- ***USER_TS_QUOTAS***

DBA_USERS

Colonne	Type	Description
USERNAME	VARCHAR2(30) NOT NULL	Login de l'utilisateur
USER_ID	NUMBER NOT NULL	ID de l'utilisateur
PASSWORD	VARCHAR2(30)	Mot de passe encrypté
ACCOUNT_STATUS	VARCHAR2(32) NOT NULL	Statut du compte: OPEN : ouvert EXPIRED : Doit changer son mot de passe LOCKED(TIMED) : Vérouillé pour un certain temps LOCKED : Vérouillé de manière définitive EXPIRED(GRACE) & LOCKED(TIMED) EXPIRED & LOCKED
LOCK_DATE	DATE	Date à laquelle le compte a été vérouillé si le status est LOCKED
EXPIRY_DATE	DATE	Date du prochain changement de mot de passe
DEFAULT_TABLESPACE	VARCHAR2(30) NOT NULL	TABLESPACE par défaut pour les données
TEMPORARY_TABLESPACE	VARCHAR2(30) NOT NULL	TABLESPACE par défaut pour les données temporaires
CREATED	DATE NOT NULL	Date de création de l'utilisateur
PROFILE	VARCHAR2(30) NOT NULL	Nom du profil assigné à l'utilisateur
INITIAL_RSRC_CONSUMER_GROUP	VARCHAR2(30)	Nom du groupe de consomation des ressources
EXTERNAL_NAME	VARCHAR2(4000)	Nom exterieur (pour option IDENTIFIED GLOBALLY)

DBA_TS_QUOTAS

Colonne	Type	Description
TABLESPACE_NAME	VARCHAR2(30) NOT NULL	Nom du TABLESPACE
USERNAME	VARCHAR2(30) NOT NULL	Nom de l'utilisateur à qui ce quota est assigné
BYTES	NUMBER	Nombre de Bytes alloué actuellement à l'utilisateur sur le TABLESPACE
MAX_BYTES	NUMBER	Quota maximal en bytes de l'utilisateur sur ce TABLESPACE (contiendra -1 si il n'y a pas de limite)
BLOCKS	NUMBER NOT NULL	Nombre de blocs alloué actuellement à l'utilisateur sur le TABLESPACE
MAX_BLOCKS	NUMBER	Quota maximal en blocs de l'utilisateur sur ce TABLESPACE (contiendra -1 si il n'y a pas de limite)

B- Les Privilèges

I- Présentation

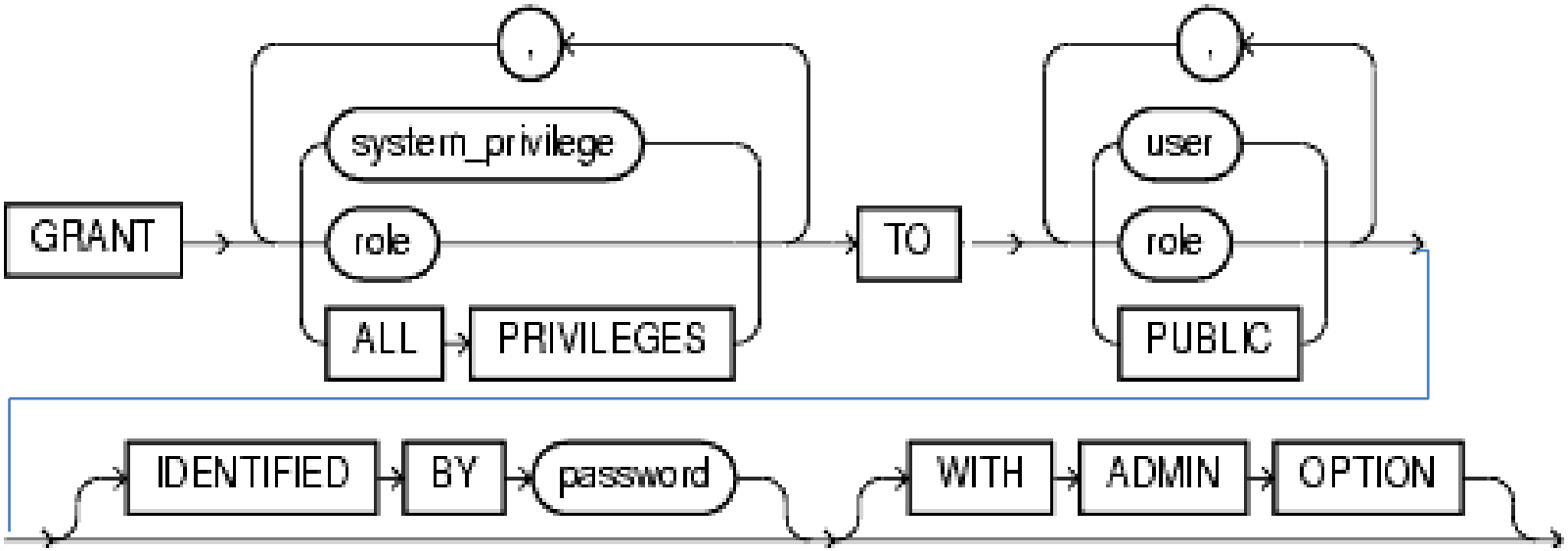
- Les privilèges sont définis pour sécuriser l'accès aux données de la BD.
- Les privilèges sont de deux types :
  - **Les privilèges de niveau système :** permettent la création, modification, suppression, exécution de groupes d'objets.

    Exemple : CREATE TABLE, CREATE VIEW, CREATE SEQUENCE
  - **Les privilèges de niveau objet :** permettent les manipulations sur des objets spécifiques .

    Exemple : SELECT, INSERT, UPDATE, DELETE

II- Assigner des privilèges système à un user :

Syntaxe :



II- Assigner des privilèges systèmes à un user…

Exemples:

1. **GRANT CREATE SESSION TO** aymen;
2. **GRANT CREATE TABLE TO** aymen;
3. **GRANT CREATE VIEW TO** aymen;
4. **GRANT CREATE SESSION ,CREATE TABLE, CREATE VIEW TO** aymen;
5. **GRANT ALTER TABLE** TO public;

III- Assigner des privilèges objets à un user :

Syntaxe :

GRANT Liste_de_permissions **ON** Liste_d_objets
TO Liste_d_utilisateurs [**WITH GRANT OPTION**];

Exemples:

1. **GRANT SELECT ,INSERT ,UPDATE ,DELETE**
   ON SCOTT.EMP **TO** aymen **WITH GRANT OPTION**;

2. **GRANT UPDATE** (JOB, MGR)
   ON SCOTT.EMP **TO** ali;

Pour la m-à-j et la suppression des lignes d'une table, les privilèges UPDATE et DELETE ne suffisent pas ➔ il faut avoir le privilège SELECT.

IV- Principes généraux

- Un utilisateur possède automatiquement tous les privilèges sur un objet qui lui appartient.
- Un utilisateur ne peut pas donner plus de privilèges qu'il n'en a reçu.
- S'il n'a pas reçu le privilège avec l'option WITH GRANT OPTION, un utilisateur ne peux pas assigner à son tour ce même privilège
- Un utilisateur non muni des droits DBA ne pourra pas accorder de privilèges sur un objet qui ne lui appartient pas
- GRANT permet d'assigner un ou plusieurs privilèges système ou objet. Cependant, lorsque la liste des privilèges est importante ➔ opération fastidieuse et répétitive

V- Retirer des privilèges

Syntaxe :

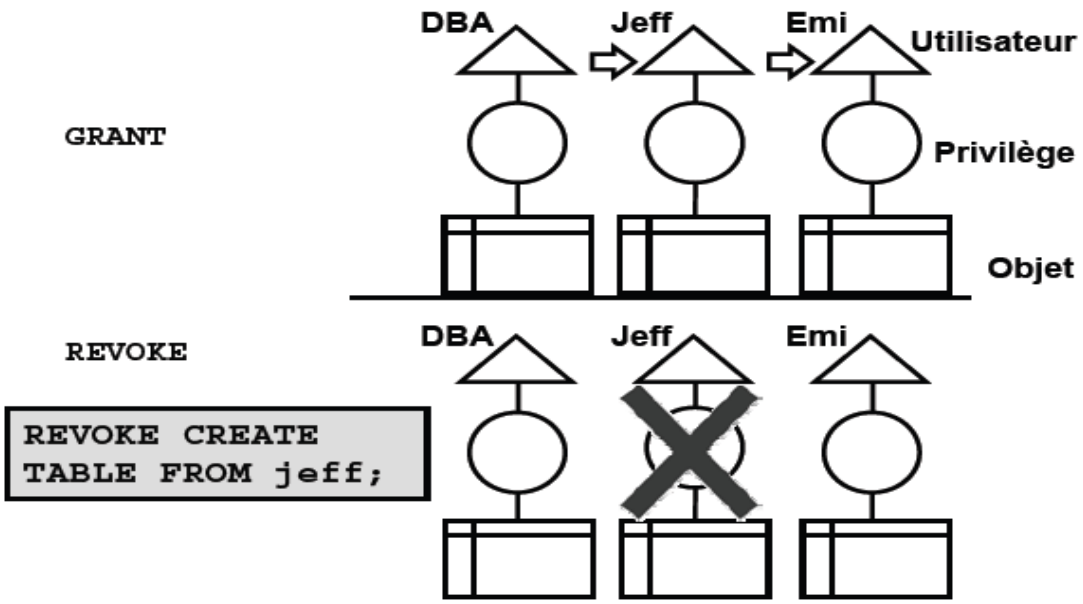
REVOKE privilège **FROM** nom_utilisateur ;

REVOKE privilège **ON** objets **FROM** nom_utilisateur ;

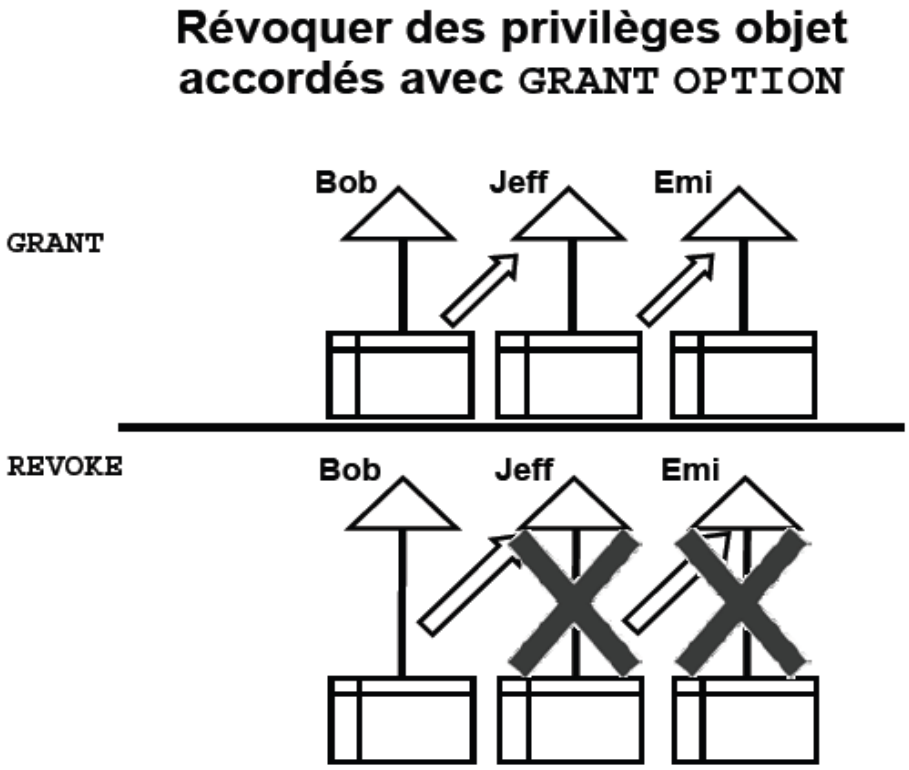
• Retirer des privilèges à un user ne supprime ni son schéma, ni les objets qu'il contient.

V- Retirer des privilèges

Révoquer des privilèges système accordés avec ADMIN OPTION



V- Retirer des privilèges



Quelques vues utiles

- DBA_TAB_PRIVS

Tous les droits sur toutes les colonnes des tables de la base

- TABLE_PRIVILEGES

Droits sur les objets de l'utilisateur en cours

- DBA_COL_PRIVS

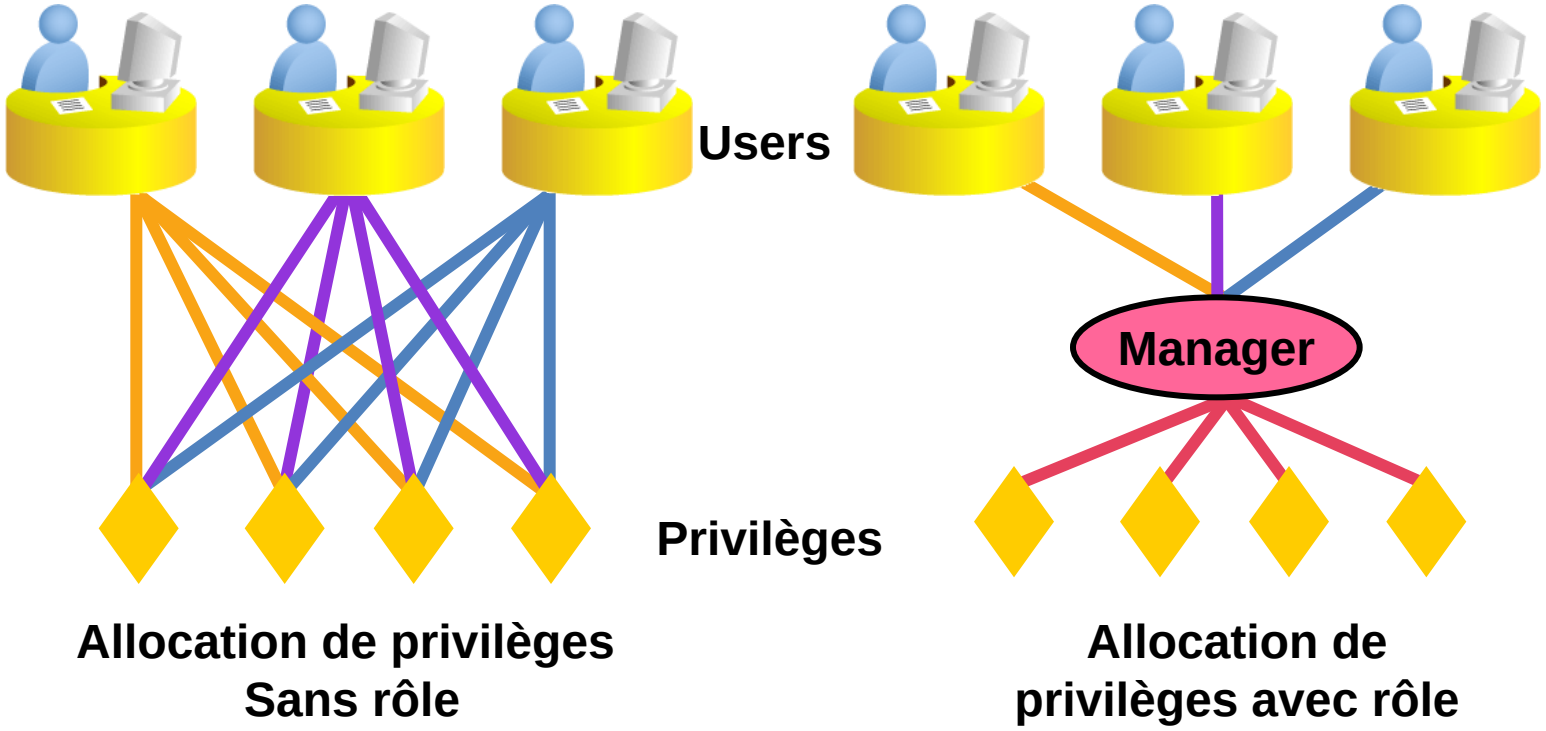
Tous les droites sur les colonnes de la base

- COLUMN_PRIVILEGES

Droits sur les colonnes de l'utilisateur en cours

C- Les rôles

I. Présentation



II- Création d'un rôle

Syntaxe :

CREATE ROLE nom_rôle [NOT IDENTIFIED/IDENTIFIED BY passwrd]

Exemples:

CREATE ROLE comptabilite ;

III- Assignation d'un rôle

1. **GRANT SELECT**, **INSERT**, **UPDATE**, **DELETE ON** FACTURE **TO** comptabilite ;
2. **GRANT SELECT**, **INSERT**, **UPDATE**, **DELETE ON** LIG_FAC **TO** comptabilite ;
3. **GRANT SELECT**, **INSERT**, **UPDATE**, **DELETE ON** JOURNAL **TO** comptabilite ;

4. **GRANT** comptabilite **TO** nom_utilisateur ;

IV- Rôles standards sous Oracle

CONNECT	CREATE SESSION
RESOURCE	CREATE CLUSTER, CREATE INDEXTYPE, CREATE PROCEDURE, CREATE OPERATOR, CREATE SEQUENCE, CREATE TABLE, CREATE TIGGER, CREATE TYPE
DBA	La plupart des privilèges systèmes et plusieurs autres rôles. Il est accordé seulement aux administrateurs

V- Suppression d’un rôle

Syntaxe :

DROP ROLE nom_rôle;

Quelques vues utiles

Vue	Description
DBA_ROLES	Affiche la liste des rôles
DBA_SYS_PRIVS	Liste l'ensemble des privilèges système
USER_SYS_PRIVS	Liste les privilèges système accordé à l'user courant
DBA_ROLE_PRIVS	Liste l'ensemble des rôles accordés aux users
USER_ROLE_PRIVS	Liste l'ensemble des rôles accordés à l'user courant
DBA_TAB_PRIVS	Liste tous les privilèges objets assignés dans la BD
ALL_TAB_PRIVS	Liste tous les privilèges objets dont l'user est bénéficiaire
USER_TAB_PRIVS	Liste les privilèges objet assignés à l'user courant
DBA_COL_PRIVS	Liste tous les privilèges sur les colonnes de la BD
ALL_COL_PRIVS	Liste tous les privilèges sur les colonnes dont l'user est bénéficiaire
USER_COL_PRIVS	Liste les privilèges sur les colonnes assignés à l'user courant
SESSION_ROLES	Liste les rôles assignés à l'user courant
SESSION_PRIVS	Liste les privilèges assignés à l'user courant

D- Les profils

I- Présentation

• Afin d'augmenter la sécurité de la base de données, il est intéressant de gérer en plus des mots de passe un certain nombre d'information comme le nombre maximal de tentatives de connexion à la base, le temps de verrouillage d'une compte, etc...

• Il peut parfois aussi être intéressant de limiter les ressources système allouées à un utilisateur afin d'éviter une surcharge inutile du serveur.

•Oracle nous propose une solution efficace et pratique pour mettre en place ce type d'action : les PROFILS.

I- Présentation …

- Un PROFIL est un ensemble de limitations système. Une fois qu'un PROFIL a été assigné à un utilisateur celui-ci ne pourra plus dépasser les limitations imposées.

- La première chose a vérifier et de savoir si vous disposez du privilège système CREATE PROFILE.

- Si c'est le cas il va falloir décider quelles limitations vous souhaitez mettre en place. Vous avez deux types de limitations:
    - Les limitations du mots de passe
    - Les limitations des ressources système

II- Les limitations du mot de passe

Option	Description
FAILED_LOGIN_ATTEMPTS	définit le nombre maximal de tentatives de connexion.
PASSWORD_LIFE_TIME	définit la durée (en jour) d'utilisation du même mot de passe. Une fois la date limite d'utilisation, Oracle demandera alors à user de changer son mot de passe.
PASSWORD_REUSE_TIME	définit le délai (en jour) entre deux utilisations du même mot de passe. Si vous donner une valeur numérique au paramètre PASSWORD_REUSE_TIME vous devrez alors donner la valeur UNLIMITED au paramètre PASSWORD_REUSE_MAX .
PASSWORD_REUSE_MAX	Ce paramètre permet de définir le nombre de réutilisation du même mot de passe (consécutive ou non). Si vous donner une valeur numérique au paramètre PASSWORD_REUSE_MAX vous devrez alors donner la valeur UNLIMITED au paramètre PASSWORD_REUSE_TIME.

II- Les limitations du mot de passe…

Option	Description
PASSWORD_LOCK_TIME	définir la durée(en jour) de verrouillage du compte utilisateur après avoir bloqué le compte avec le paramètre FAILED_LOGIN_ATTEMPTS. Le compte sera alors automatiquement déverrouillé lorsque le temps défini par ce paramètre sera atteint.
PASSWORD_GRACE_TIME	définit en jours le temps de grâce qui vous sera alloué pour changer votre mot de passe. donne un délai supplémentaire à l'utilisateur pour changer son mot de passe.
PASSWORD_VERIFY_FUNCTION	Ce paramètre devra contenir le nom d'une fonction PL/SQL qui servira à vérifier les mots de passe saisi. Si vous ne souhaitez pas utiliser de fonction de vérification utiliser la valeur NULL.

III- Les limitations des ressources systèmes

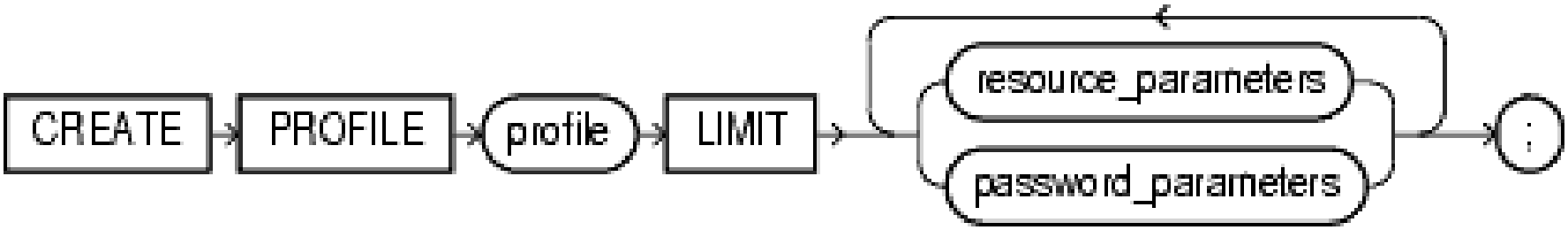
Option	Description
SESSIONS_PER_USER	définit le nombre de session maximum qu'un utilisateur pourra ouvrir.
CPU_PER_SESSION	définit le temps de processeur maximum en centièmes de secondes qu'une session pourra utiliser.
CPU_PER_CALL	définit le temps de processeur maximum en centièmes de secondes qu'un "appel serveur" pourra utiliser. On appelera "appel serveur" un parssage de requête, une execution de requête ou la recupération d'une requête (FETCH)
CONNECT_TIME	Ce paramètre va vous permettre de définir le temps en minutes pour la durée de connexion maximale d'une session. A la fin du temps imparti la session sera automatiquement déconnectée.

III- Les limitations des ressources systèmes…

Option	Description
IDLE_TIME	définit le temps en minutes pour la durée d'inactivité maximale d'une session. A la fin du temps imparti la session sera automatiquement déconnectée.
LOGICAL_READS_PER_SESSION	définit le nombre maximal de bloc lus durant une session. On parlera ici des blocs lus sur le disque et dans la mémoire.
LOGICAL_READS_PER_CALL	définit le nombre maximal de bloc lus durant un "appel serveur". On parle ici des blocs lus sur le disque et ds la émoire.
COMPOSITE LIMIT	définit le coût total des limitations autorisée pour une session. Oracle calcule le coût total de toute les ressources à partir du poids attribué aux paramètres CPU_PER_SESSION, CONNECT_TIME, LOGICAL_READS_PER_SESSION, et PRIVATE_SGA. Vous pourrez changer le poids associé à chaque limitations système avec la commande ALTER RESOURCE COST.
PRIVATE_SGA	définir la taille en (K ou M)Bytes que pourra utiliser une session.

IV- Création d'un profil

Syntaxe :



IV- Création d'un profil…

Exemple:

```
CREATE PROFILE app_user
LIMIT
SESSIONS_PER_USER UNLIMITED
CPU_PER_SESSION UNLIMITED
CPU_PER_CALL 3000
CONNECT_TIME 45
LOGICAL_READS_PER_SESSION DEFAULT
LOGICAL_READS_PER_CALL 1000
PRIVATE_SGA 15K
COMPOSITE_LIMIT 5000000;

ALTER USER scott PROFILE app_user;
```

V- Modification d’un profil

- Pour pouvoir modifier des limitations de ressources système, il faut disposer du privilège système ALTER PROFILE.
- Pour modifier des limitations de mot de passe, il faut disposer des privilèges ALTER PROFILE et ALTER USER.
- Si une limitation est modifiée les autres limitations en cours ne seront pas modifiées. Une fois la limitation modifiée seule les nouvelles sessions se verront assigner cette nouvelle limitation.

V- Modification d’un profil…

Exemple:

ALTER PROFILE app_user
LIMIT
FAILED_LOGIN_ATTEMPTS 5
PASSWORD_LOCK_TIME 1;

VI- Suppression d’un profil

- Pour supprimer un profil, il faut disposer du privilège DROP PROFIL.

- Si le profil à supprimer a été assigné à un utilisateur, on doit utiliser l'option CASCADE qui demandera à Oracle de supprimer le profil et d'assigner le profil DEFAULT à tout les utilisateurs qui possédaient le profil qui vient d'être supprimé.

  Exemple:

  DROP PROFILE app_user **CASCADE**;;

Rque: on peux pas supprimer le profile DEFAULT.

Quelques vues utiles

- **DBA_PROFILES**

Liste de tous les profils

- **USER_RESOURCE_LIMIT**

La valeur des limites pour les ressources de l'utilisateur courant