# Gestion des utilisateurs et de leurs droits

Lors de la création d'un utilisateur, vous devez indiquer son nom, ses attributs, son profil, son *tablespace* par défaut, …

À la création de la base de données, l'utilisateur SYS reçoit tous les privilèges systèmes disponibles et tous les rôles existants.

Ayant le privilège *GRANT ANY PRIVILEGE****,*** il peut à son tour redistribuer tous les privilèges reçus.

Pour assurer la sécurité de la base de données, il faut supprimer les autorisations inutiles et ne donner que les droits nécessaires aux divers utilisateurs.

La gestion des utilisateurs implique :

La gestion des ressources par les profils.

La gestion des privilèges systèmes et des privilèges objetspar les rôles.

La gestion des quotas sur les *tablespaces.*

Dans le dictionnaire de données, plusieurs vues permettent de visualiser les privilèges et les rôles disponibles.

## Gestion d’un utilisateur

CREATE USER nom IDENTIFIED { BY mot\_de\_passe | EXTERNALLY}

[DEFAULT TABLESPACE nom\_tablespace]

[TEMPORARY TABLESPACE nom\_tablespace]

[QUOTA { valeur [K|M] | UNLIMITED } ON nom\_tablespace [,…] ]

[PROFILE nom\_profile]

[PASSWORD EXPIRE]

[ACCOUNT {LOCK | UNLOCK}];

###### CREATE USER nom IDENTIFIED { BY mot\_de\_passe | EXTERNALLY}

Le nom et le mot de passe doivent respecter les règles

###### [ DEFAULT TABLESPACE nom\_tablespace]

N’empêche pas l’utilisateur de créer des objets dans un autre tablespace

L’utilisateur doit avoir un quota pour utiliser un espace logique.

Si pas de «DEFAULT TABLESPACE», ce sera celui par défaut du système.

*ALTER DATABASE DEFAULT TABLESPACE nom;*

###### [TEMPORARY TABLESPACE nom\_tablespace]

Pour les gros tris trop gros pour être en totalité en mémoire PGA

Si pas de «TEMPORARY TABLESPACE», ce sera celui par défaut du système .

*ALTER DATABASE DEFAULT TEMPORARY TABLESPACE nom;*

###### [QUOTA { valeur [K|M] | UNLIMITED } ON nom\_tablespace [,…] ]

Quota dans un tablespace permanent en particulier (non temporaire…)

Sans quota, impossible d’ajouter des données dans les tables/index.

Par défaut les utilisateurs n’ont pas de quota

Possible de consulter les objets sans avoir de quota

###### [PROFILE nom\_profile]

Ensemble nommé de limitation de ressources (CPU, temps de connexion, password…)

###### [PASSWORD EXPIRE]

Force l’utilisateur à changer son mot de passe

###### [ACCOUNT {LOCK | UNLOCK}];

Pour verrouiller ou déverrouiller un utilisateur.

### Autres énoncés SQL

Modifier un utilisateur : ALTER USER nom….

Supprimer un utilisateur : DROP USER nom [CASCADE];

Essentiel de faire CASCADE si l’utilisateur possède des objets

S’il n’y a pas de CASCADE, alors une erreur sera affichée lors de la suppression de l’usager

## Les profils

Un profil est un mécanisme pour contrôler la quantité d'espace disque ou de bande passante d'E/S utilisé pour exécuter une requête utilisateur. Il est donc un ensemble nommé de limitations deressources. Un profil est attribuable à un utilisateur et un seul profil peut être donné à la fois à un utilisateur. Tous les utilisateurs doivent avoir un profil.

Un profil limite donc les ressources attribuées à un utilisateur. De plus, les profils facilitent la gestion des mots de passe des utilisateurs.

Le profil *DEFAULT* s'applique à tout nouvel utilisateur si aucun autre profil ne lui est assigné.

Par défaut, sur une nouvelle base de données, la gestion des profils est désactivée. Donc RESOURCE\_LIMIT est à FALSE.

Les limites de ressources seront appliquées si le paramètre *RESOURCE\_LIMIT* vaut *TRUE*

*ALTER SYSTEM SET RESOURCE\_LIMIT = TRUE SCOPE = BOTH;*

Le paramètre *RESOURCE\_LIMIT* n’a pas d’influence sur les limites des mots de passe.

### Le profil DEFAULT

* Ce profil est créé lors de la création de la base de données et ne peut être détruit.
* Le profil DEFAULT n’a aucune limite par défaut. Il est cependant possible de le modifier.

### Certaines valeurs permises lors de la création d’un profil

* Le mot clé UNLIMITED : aucun contrôle sur la ressource.
* Le mot clé DEFAULT : la valeur sera celle de la limite du profil DEFAULT
* Ne rien mettre : la valeur sera celle de la limite du profil DEFAULT

### Les ressources qui peuvent être limitées

Limite du nombre de sessions ouvertes en même temps par un utilisateur.

Limites de temps et d'activités

Pour le CPU, le temps par appel/session

Durée de la session

Temps d'inactivité par session

Les activités de lectures (LOGICAL\_READ)

Quantité de mémoire privée dans la SGA (si le serveur est en mode partagé)

### Limite sur les mots de passes

Nombre d’essais infructueux, temps de vie du mot de passe, nombre de réutilisation du mot de passe, blocage du mot de passe, fonction de vérification.

### Création d’un profil

CREATE PROFILE nom\_profil LIMIT

SESSIONS\_PER\_USER valeur | UNLIMITED | DEFAULT Nb de sessions simultanées

CPU\_PER\_SESSION valeur | UNLIMITED | DEFAULT Maximum CPU par session (1/100 s)

CPU\_PER\_CALL valeur | UNLIMITED | DEFAULT Maximum CPU total par appel (1/100 s)

CONNECT\_TIME valeur | UNLIMITED | DEFAULT Durée maximale de la connexion (en min.)

IDLE\_TIME valeur | UNLIMITED | DEFAULT Durée d’inactivité (en min.)

LOGICAL\_READS\_PER\_SESSION valeur | UNLIMITED | DEFAULT Nb maximum de blocs lus par session

LOGICAL\_READS\_PER\_CALL valeur | UNLIMITED | DEFAULT Nb maximum de blocs lus par appel

PRIVATE\_SGA valeur | UNLIMITED | DEFAULT Qté de mémoire privée max. dans SGA (bytes)

FAILED\_LOGIN\_ATTEMPTS valeur | UNLIMITED | DEFAULT Nb de connexions échouées avant

le verrouillage du compte

PASSWORD\_LOCK\_TIME valeur | UNLIMITED | DEFAULT Durée du verrouillage (en jour)

PASSWORD\_LIFE\_TIME valeur | UNLIMITED | DEFAULT Durée de vie du mot de passe (en jour)

PASSWORD\_REUSE\_TIME valeur | UNLIMITED | DEFAULT Nb de jours pendant lequel un mot de

passe ne peut pas être réutilisé

PASSWORD\_REUSE\_MAX valeur | UNLIMITED | DEFAULT Nb de changements de mots de passe

avant qu’un mot de passe puisse être

réutilisé

PASSWORD\_GRACE\_TIME valeur | UNLIMITED | DEFAULT Période de grâce après expiration du

mot de passe (en jour)

PASSWORD\_VERIFY\_FUNCTION nom | NULL | DEFAULT; Fonction qui vérifie la complexité du

mot de passe.

Il y a également la limitation COMPOSITE\_LOGIN, permettant de limiter selon la somme de :

CPU\_PER\_USER, CONNECT\_TIME, LOGICAL\_READS\_PER\_SESSION et PRIVATE\_SGA.

Exemple :

CREATE PROFILE profilUsager LIMIT

SESSIONS\_PER\_USER 5

FAILED\_LOGIN\_ATTEMPTS 3;

### Modification d’un profil

Une modification n'est effective que lors de la prochaine connexion de l'utilisateur.

Toute modification au profil DEFAULT affecte les valeurs par défaut des autres profils

ALTER PROFILE nom\_profil LIMIT….

### Suppression d’un profil

Si un profil est attribué à plusieurs utilisateurs on doit l'éliminer en *CASCADE*

Le profil DEFAULT sera alors attribué aux utilisateurs ayant perdu leur profil

DROP PROFILE nom [CASCADE];

### Assigner un profil à un usager

ALTER USER nom PROFILE nom\_profile;

### Dictionnaire de données

**DBA\_USERS**

Le profil attribué est spécifié dans la colonne PROFILE

**DBA\_PROFILES**

Permet d’avoir des informations sur les profils et leurs limites.

SELECT RESOURCE\_NAME, LIMIT FROM DBA\_PROFILES WHERE PROFILE = 'DEFAULT';

## Les privilèges système

Les privilèges système donnent le droit d’exécuter une opération (ex. SQL) sur la base de données. Les privilèges objet donnent le droit d’accéder à un objet (ex. table) d’un autre utilisateur par des instructions SELECT, INSERT, UPDATE et DELETE.

Exemple de privilège système : CREATE SESSION… (ça n'appartient à personne, c'est une opération)

Les privilèges systèmes représentent un droit d'exécuter des travaux *batch,* de modifier des paramètres systèmes, de créer des rôles, des créer des objets, etc.

Il existe plus de 200 privilèges système.

Ils sont énumérés dans la table SYSTEM\_PRIVILEGE\_MAP

Souvent, le privilège porte le nom de l’action (instruction SQL) permise:

Accorder le pouvoir de créer une table : CREATE TABLE

Accorder le pouvoir de créer un usager : CREATE USER

CREATE TABLE (7 droits d’un seul coup!)

Ce privilège donne les droits CREATE, ALTER et DROP ainsi que SELECT, INSERT, UPDATE et DELETE sur les tables dans le schéma de l'utilisateur.

Les privilèges qui permettent d’avoir accès aux objets de **tous les schémas** sont octroyés avec le modificateur *ANY*

Accorder le pouvoir de créer des tables dans tous les schémas : CREATE ANY TABLE

Ne s’applique pas si le privilège ne porte pas sur des objets : CREATE ANY USERS

CREATE ANY TABLE création des tables dans n’importe quel schéma.

ALTER ANY TABLE

DROP ANY TABLE

DELETE ANY TABLE détruire des rangées dans n’importe quelle table et schéma

INSERT ANY TABLE

SELECT ANY TABLE

UPDATE ANY TABLE

**Les privilèges les plus importants**

CREATE SESSION  Impossible de se connecter sans ce privilège. Erreur [ORA-01045](http://www.adp-gmbh.ch/ora/err/ora_01045.html).

CREATE TABLE

CREATE VIEW

CREATE PROCEDURE

**Liste de privilèges système**

Vue du dictionnaire de données : *SYSTEM\_PRIVILEGE\_MAP*

Références : <http://www.psoug.org/reference/system_privs.html>

**GRANT** nom\_priv [,…] TO {nom\_utilisateur | PUBLIC} [,…] [WITH ADMIN OPTION];

Un privilège reçu est effectif immédiatement.

Éviter de donner un privilège à tous les utilisateurs (PUBLIC)

L’option WITH ADMIN OPTION permet, à l’utilisateur qui a reçu le privilège
de redonner ce privilège à un autre usager.

GRANT CREATE TABLE TO Scott WITH ADMIN OPTION ;

L’utilisateur Scott pourra donner à d’autres utilisateurs le droit de créer des tables.

**REVOKE** nom\_priv [,…] FROM {nom\_utilisateur | PUBLIC} [,…];

### Dictionnaire de données

DBA\_SYS\_PRIVS Privilèges systèmes attribués aux utilisateurs

SESSION\_PRIVS Privilèges actifs pour la session actuelle.

SYSTEM\_PRIVILEGE\_MAP Liste de tous les privilèges

## Les privilèges objet

À la différence d'un privilège système, un privilège objet est le droit de réaliser un certain type d'action sur un objet précis de la base de données, tel qu'une table ou une séquence qui ne se trouve pas dans le propre schéma de l'utilisateur.

Un utilisateur possède automatiquement tous les privilèges sur les objets de son propre schéma et peut accorder tout privilège sur ses objets à n'importe quel utilisateur ou rôle.

Dans le cas de procédures, de fonctions ou de packages, seul le privilège EXECUTE est applicable. Une procédure invoquée avec les droits du créateur est exécutée comme s'il s'agissait du créateur avec tous ses privilèges actifs sur les objets référencés dans la procédure. Le créateur peut contrôler comment les autres utilisateurs accèdent aux objets.

Les types de privilèges objet accordés sur une table se répartissant en deux catégories :

Par défaut, seul le propriétaire d’un objet à le droit d’y accéder.

Un privilège objet accorde le droit d’accéder à un objet (ex. table) qui appartient à un autre utilisateur, par exemple le droit de mettre à jour le nom et prénom (colonne « nom et prenom ») de la table SCOTT.EMP qui appartient à SCOTT.

**GRANT** {nom\_privilège [(liste\_colonne)] [,…] | ALL [PRIVILEGES] }

ON [nom\_schéma].nom\_objet

TO {nom\_utilisateur | PUBLIC } [,…] [WITH GRANT OPTION];

L’option ALL PRIVILEGES permet d’attribuer tous les privilèges objets :

* INSERT, DELETE, INDEX, ALTER, UPDATE, SELECT (cette liste n’est pas complète)

Exemple : GRANT SELECT, INSERT(nom, prenom) ON SCOTT.EMP TO SCOTTY;

**REVOKE** {nom\_privilège [,…] | ALL [PRIVILEGES] }

ON [nom\_schéma].nom\_objet

FROM {nom\_utilisateur | PUBLIC } [,…];

### Dictionnaire de données

DBA\_TAB\_PRIVS Privilèges objet attribués aux utilisateurs sur la totalité de l’objet

DBA\_COL\_PRIVS Privilèges objet attribués aux utilisateurs sur certaines colonnes d’un objet

TABLE\_PRIVILEGE\_MAP Liste de tous les privilèges objets.

## Les rôles

Un rôle est un regroupement de privilèges au niveau système et/ou objet pour faciliter l'administration des privilèges en diminuant le nombre d'instructions GRANT à exécuter.

Tout changement aux privilèges octroyés à un groupe d'utilisateurs via un rôle sont immédiatement reportés au niveau des utilisateurs.

Par la suite un rôle peut être activé de manière sélective par l'utilisateur ou automatiquement lors de l'ouverture d'une nouvelle session.

Regroupement nommé de privilèges (système et objet) qui peuvent être attribué à un utilisateur ou à un autre rôle !

Un rôle peut être attribué à un utilisateur

Un rôle peut être attribué à un autre rôle

Un rôle n’appartient à aucun utilisateur ou schéma.

### Créer le rôle

CREATE ROLE nomRôle ;

Il faut avoir le privilège CREATE ROLE

Un rôle ne doit pas porter le même nom qu'un utilisateur/schéma

### Détruire un rôle

DROP ROLE nomRôle ;

### Attribuer des privilèges au rôle (semblable à un usager!)

GRANT privilege [,…] TO nomRôle [,..] [WITH ADMIN OPTION];

GRANT {nom\_privilège[(liste\_colonnes)] [,…] | ALL } ON [nom\_schéma.]nom\_objet TO nomRôle [,…];

### Révoquer un privilège à un rôle

REVOKE nom\_role FROM nom\_role;

### Attribuer un rôle à un utilisateur ou à un rôle!

GRANT nomRôle [,…] TO {nom\_utilisateur | PUBLIC | nomRôle } [,…] [WITH ADMIN OPTION];

### Révoquer un rôle à un utilisateur ou un rôle

REVOKE …FROM …;

### Les rôles pré-définis d’Oracle

Il est préférable de ne pas les utiliser. Il s'agit de CONNECT, DBA et RESSOURCE

Ces rôles permettent de se connecter et de créer les principaux objets d’un schéma (contiennent plusieurs privilèges!)

DBA : Tous les privilèges système avec l'option WITH ADMIN OPTION

MGMT\_USER : Permet d’utiliser le Database Contrôle (Enterprise Manager).

### Dictionnaire de données

DBA\_ROLES

Permet de voir la liste des rôles existants.

## Les quotas sur les espaces logiques

Permet de limiter l'espace utilisé par un utilisateur dans les tablespaces.

### Quota par défaut = 0

On ne peut ajouter de données à une table nous appartenant.

Pour assigner un quota spécifique à un utilisateur sur un tablespace

CREATE USER… ou ALTER USER… QUOTA 500K ON …

Exemple : ALTER USER SCOTT QUTOA 50M ON tablespaceNumero3;

### Quota illimité

Pour assigner un quota illimité à un utilisateur sur un tablespace:

CREATE USER… ou ALTER USER … QUOTA UNLIMITED ON …

Pour assigner un quota illimité sur tous les espaces logiques, il faut donner le privilège système UNLIMITED TABLESPACE

## Les synonymes

En utilisant un synonyme, un utilisateur n’a pas à préfixer un appel d’objet par son schéma.

CREATE [OR REPLACE] [PUBLIC] SYNONYM [schema.]synonym FOR [schema.]objet

Exemple :

CREATE SYNONYM inventaires FOR Test.inventaires;// accessible par l’usager ayant créé le synonyme

CREATE PUBLIC SYNONYM inventaires FOR Test.inventaires // synonyme accessible pour tous les usagers.

## Exemple complet

REM ------------------------------------------------

REM Création du profil

REM ------------------------------------------------

CREATE **PROFILE** PROFILE\_INTER LIMIT

IDLE\_TIME 15

SESSIONS\_PER\_USER 3;

REM ------------------------------------------------

REM Activation des profils (si nécessaire)

REM ------------------------------------------------

ALTER SYSTEM SET **RESOURCE\_LIMIT**=TRUE SCOPE=BOTH;

REM ------------------------------------------------

REM Création d’un role

REM ------------------------------------------------

CREATE **ROLE** **INTERROGATEUR**;

GRANT CREATE SESSION TO INTERROGATEUR;

GRANT SELECT ON SCOTT.EMP TO INTERROGATEUR;

GRANT SELECT ON SCOTT.DEPT TO INTERROGATEUR;

GRANT SELECT ON SCOTT.BONUS TO INTERROGATEUR;

REM ------------------------------------------------

REM Création d’un usager et assignation d’un rôle

REM ------------------------------------------------

CREATE USER **INTER** IDENTIFIED BY **INTER**

PROFILE PROFILE\_INTER

DEFAULT TABLESPACE USERS

TEMPORARY TABLESPACE USERSTMP;

REM Aucun quota, c'est un interrogateur.

GRANT INTERROGATEUR TO INTER;