



Chapitre 3:

Gestion des utilisateurs et de leurs droits

Chapitre 3



Gestion des utilisateurs



Gestion des droits d'accès



Gestion des rôles



Gestion des profils



Gestion des utilisateurs

L'utilisateur SYS (administrateur)



- 🗄 Créé par la commande **CREATE DATABASE**
- 🗄 Le **rôle DBA** et le **privilège SYSDBA** sont **attribués par défaut** à l'utilisateur **SYS**
- 🗄 Le **mot de passe** est défini dans la commande CREATE DATABASE.
- 🗄 Lors de la connexion avec **SYS**, **vous devez fournir les mots clés 'AS SYSDBA'**.

```
SQL> connect sys as sysdba
```

NB. Donc il est préférable de ne pas utiliser **SYS** pour des tâches administratives quotidiennes.

L'utilisateur SYSTEM (administrateur)




- 🗄 **Créé** par la commande **CREATE DATABASE**
- 🗄 Le **rôle DBA** est **attribué par défaut** à **SYSTEM**
- 🗄 Le **mot de passe** est défini dans la commande CREATE DATABASE.


NB. SYSTEM: utilisateur administratif standard que l'on préférera pour *créer les objets de schéma* tels que les utilisateurs, les tables, les vues, etc.



 **SYSDBA** est un privilège administratif spécial.

 **SYSDBA** contient le privilège de **démarrer** et **d'arrêter** la BD.

 La particularité de **SYSDBA** est que vous devez spécifier explicitement "**AS SYSDBA**" dans la chaîne de connexion pour que le privilège soit actif pendant la session.

 Après une connexion en « **userID AS SYSDBA** », vous utiliserez le **schéma SYS** (même si le nom d'utilisateur est différent de SYS, par exemple, "User1").

→ Cela signifie que si vous créez une table avec "CREATE TABLE X...", le nom complet de la table sera SYS.X.



Les **Privilèges SYSDBA**:

- Privilège CREATE DATABASE
- Privilèges de **démarrage** et **d'arrêt** de la **BD**
- **Monter** ou **ouvrir** une **BD**
- **Sauvegarder** la **BD**
- Lancer l'archivage des journaux de restauration
- Récupération de la **BD**
- Modification de la **BD** en mode **RESTRICTED SESSION**



- Un **rôle** est une **collection de privilèges**
- Oracle fournit plusieurs rôles prédéfinis pour notre commodité.
 - Un de ces rôles est le rôle «**DBA**».
- Il contient tous les privilèges au niveau système (par exemple, CREATE TABLE, CREATE USER) avec des droits d'administrateur.

NB. Mais, avec le rôle **DBA** **sans se connecter avec le privilège SYSDBA**, l'utilisateur **ne peut pas** démarrer ou arrêter la BD.



🗄️ L'**administrateur** de la BD définit:

- ✓ le nom des utilisateurs autorisés à accéder à la BD,
- ✓ un **domaine de sécurité** qui s'applique à l'utilisateur.

🗄️ Le **domaine de sécurité** contient un ensemble de paramètres:

- ✓ **Mécanisme d'authentification**
- ✓ **Quotas de tablespace :**
 - Les **quotas** de tablespace contrôle la quantité d'espace physique de stockage alloué à un utilisateur dans les tablespaces de la BD.

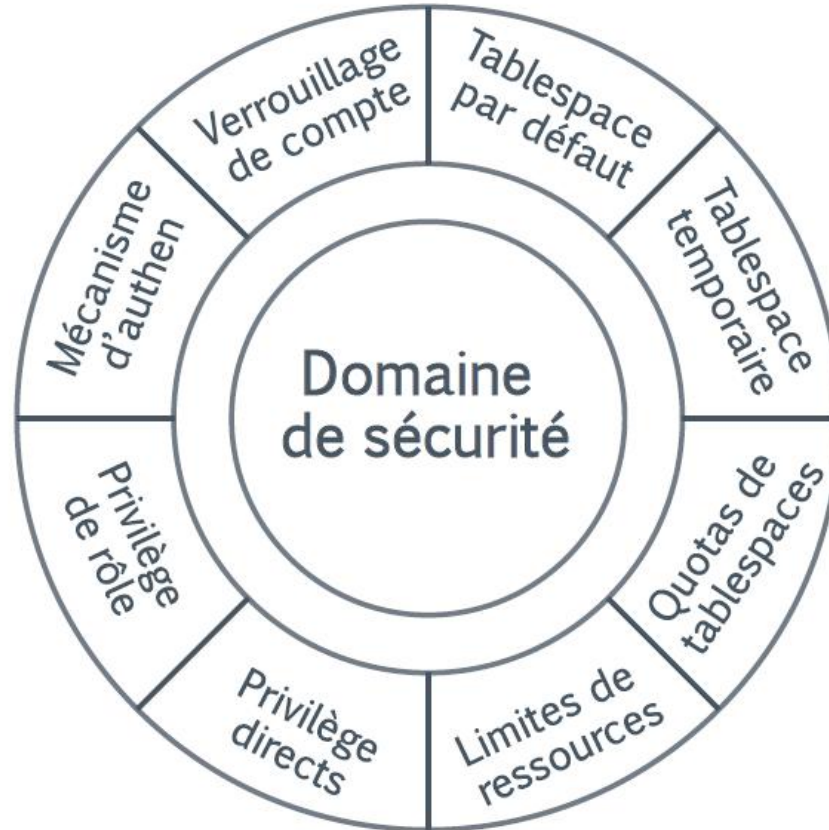


Tablespace par défaut :

– Le tablespace par défaut définit l'emplacement de stockage des **objets (segments)** créés par un utilisateurs, si celui ci **n'indique pas explicitement un tablespace** lors de la création des objets.

Tablespace temporaire :

– Définit l'emplacement d'allocation des extends (ensembles de blocs contigus) par le serveur lorsque l'utilisateur **exécute une opération** dans laquelle les données sont écrites sur disque.





 Les **utilisateurs** sont gérés dans Oracle comme tous les objets de la base :

- Action de création (**CREATE**)
- Action de modification (**ALTER**)
- Action de suppression (**DROP**)

 Chaque utilisateur peut avoir des **rôles**, **profils**, des **tablespaces** **par défaut**, etc.



- Un **compte utilisateur** est requis pour se connecter à la **BD**.
- La commande **CREATE USER** permet de créer un compte utilisateur :

```
CREATE USER nom_utilisateur  
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] ;
```



- **nom_utilisateur**: Le nom d'utilisateur est conforme aux conventions de dénomination standard d'Oracle: *1 à 30 caractères alphanumériques, le premier caractère doit être alphabétique*. Les caractères spéciaux *_*, *\$* et *#* sont autorisés.
- **IDENTIFIED BY mot_de_passe**: permet d'affecter un mot de passe à un utilisateur.
- **IDENTIFIED EXTERNALLY** : permet de créer un utilisateur qui a le même nom et le même mot de passe qu'un utilisateur défini au niveau SE .
 - ➔ Évite la saisie du mot de passe lors des connexions à Oracle (connexion avec /).
- **DEFAULT TABLESPACE** : spécifie le tablespace à utiliser pour les objets créés par cet utilisateur lorsque aucun tablespace spécifique n'est spécifié pour l'objet.



- **TEMPORARY TABLESPACE** : attribue un tablespace temporaire par défaut à l'utilisateur
 - ➔ emplacement dans lequel l'utilisateur peut créer des objets temporaires tels que les tris et les tables temporaires
- **QUOTA** { **valeur [K | M]** | **UNLIMITED** } **on nom_Tablespace** : permet de limiter (**valeur** en KO ou MO) ou non (**UNLIMITED**) l'espace attribué à l'utilisateur sur un tablespace précis.
- **PROFILE** : affecte un profil à l'utilisateur qui contrôle les ressources et les fonctions de mot de passe utilisées par cet utilisateur.
- **PASSWORD EXPIRE** : permet de forcer une modification du mot de passe lors de la première connexion ➔ inutile, si l'utilisateur est identifié par le système d'exploitation
- **ACCOUNT** : pour verrouiller (**LOCK**) ou autoriser (**UNLOCK**) l'accès à la base
 - ➔ par défaut, c'est **UNLOCK**

Création d'un utilisateur - Exemple




```
Create user User1  
IDENTIFIED BY "1234"  
DEFAULT TABLESPACE USERS  
TEMPORARY TABLESPACE TEMP  
QUOTA 46k on USERS  
PASSWORD EXPIRE;
```

Mot de passe initial

User USER1 créé(e).



 La commande ALTER USER peut être utilisée pour modifier les attributs d'un utilisateur :

```
ALTER USER nom_utilisateur  
IDENTIFIED {BY mot_de_passe| EXTERNALLY}  
[DEFAULT TABLESPACE nom_tablespace]  
[TEMPORARY TABLESPACE nom_tablespace]  
[QUOTA {valeur[K |M] | UNLIMITED} ON nom_tablespace ...]  
[DEFAULT ROLE {rôle [, rôle,... ] | ALL [ ALL EXCEPT rôle [, rôle,... ] | NONE}]  
[PROFILE profile_name]  
[PASSWORD EXPIRE]  
[ACCOUNT LOCK | UNLOCK] ;
```

Modification d'un utilisateur - Exemples



```
Alter user User1  
DEFAULT TABLESPACE USERS  
QUOTA UNLIMITED on USERS;
```

```
Alter user system  
IDENTIFIED BY "IIT"  
DEFAULT TABLESPACE USERS  
QUOTA UNLIMITED on USERS  
;
```

Suppression d'un utilisateur



- La commande **DROP USER** permet de supprimer un utilisateur Oracle de la base de données.
- L'entrée de l'utilisateur est supprimée de la vue Dictionnaire de données **DBA_USERS**, supprimant toute trace de l'existence de l'utilisateur Oracle.
- Il faut soit **s'assurer de supprimer chacun des objets avant de supprimer l'utilisateur**, soit utiliser l'option **CASCADE** (suppression automatiquement tous les objets de l'utilisateur).

```
DROP USER nom_utilisateur [CASCADE];
```

NB. Un utilisateur connecté ne peut pas être supprimé.



Gestion des droits d'accès




 On distingue deux types de privilèges :

- ❑ **Privilège système** : Le droit d'exécuter un ordre SQL
 - ❑ Par défaut, droit réservé uniquement au DBA

- ❑ **Privilège objet** : Le droit d'accéder à un objet **d'un autre utilisateur**
 - ❑ Par défaut, un utilisateur qui crée un nouvel objet a tous les droits sur lui, les autres aucun (sauf DBA)



 Le privilège **CREATE TABLE** donne le droit à l'utilisateur de créer une table dans son propre schéma.

 Le privilège **CREATE ANY TABLE** donne le droit de créer une table dans n'importe quel schéma de la BD.



Attribution d'un privilège système à un utilisateur

```
GRANT nom_privilège1 [,nom_privilège2,...] / ALL PRIVILEGES  
TO {nom_utilisateur1, ...| PUBLIC} [,nom_utilisateur2, ...]  
[WITH ADMIN OPTION] ;
```

- **nom_privilège** : nom du privilège système
 - **ALL PRIVILEGES** : accorder tous les privilèges système sauf SELECT ANY DICTIONARY
 - **nom_utilisateur** : le nom de l'utilisateur qui va bénéficier des privilèges
 - **PUBLIC** : attribuer les privilèges à tous les utilisateurs
 - **WITH ADMIN OPTION** : **permettre à l'utilisateur de transférer ses privilèges aux utilisateurs de son choix**
- NB.** sans WITH ADMIN OPTION, seul DBA peut accorder des privilèges système

Retrait de privilège système

```
REVOKE nom_privilège1 [,nom_privilège2,...]  
FROM {nom_utilisateur1, ...| PUBLIC} [,nom_utilisateur2, ...];
```



PROFILS	
CREATE PROFILE	Création de profils
ALTER PROFILE	Modification de profils
DROP PROFILE	Suppression de profils
ROLES	
CREATE ROLE	Création de rôles
ALTER ANY ROLE	Modification de n'importe quel rôle
DROP ANY ROLE	Suppression de n'importe quel rôle
GRANT ANY ROLE	Assignment de n'importe quel rôle
ROLLBACK SEGMENTS	
CREATE ROLLBACK SEGMENT	Création de segments de rollback
ALTER ROLLBACK SEGMENT	Modification de segments de rollback
DROP ROLLBACK SEGMENT	Suppression de segments de rollback
SEQUENCES	
CREATE SEQUENCE	Création de séquences dans le schéma
CREATE ANY SEQUENCE	Création de séquences dans n'importe quel schéma
ALTER ANY SEQUENCE	Modification de n'importe quelle séquence
DROP ANY SEQUENCE	Suppression de séquences dans n'importe quel schéma
SELECT ANY SEQUENCE	Interrogation de séquences dans n'importe quel schéma



SESSIONS	
CREATE SESSION	Connexion à la base
ALTER RESOURCE COST	Application de coûts pour les ressources de la session
ALTER SESSION	Permet l'instruction ALTER SESSION
RESTRICTED SESSION	Connexion restreinte à l'instance
SYNONYMS	
CREATE SYNONYM	Création de synonymes dans le schéma
CREATE ANY SYNONYM	Création de synonymes dans n'importe quel schéma
CREATE PUBLIC SYNONYM	Création de synonymes publics
DROP ANY SYNONYM	Suppression de synonymes dans le schéma
DROP PUBLIC SYNONYM	Suppression de synonymes publics
TABLES	
CREATE TABLE	Création de tables dans le schéma
CREATE ANY TABLE	Création de tables dans n'importe quel schéma
ALTER ANY TABLE	Modification de tables ou vues dans n'importe quel schéma
BACKUP ANY TABLE	Autorise l'utilisation de l'outil Export
DELETE ANY TABLE	Suppression de lignes des tables de n'importe quel schéma
DROP ANY TABLE	Suppression ou troncature de tables dans n'importe quel schéma
INSERT ANY TABLE	Insertion de lignes dans les tables de n'importe quel schéma
LOCK ANY TABLE	Vérouillage des tables ou vues de n'importe quel schéma
SELECT ANY TABLE	Interrogation des tables, vues ou vues matérialisées de n'importe quel schéma
FLASHBACK ANY TABLE	Autorise les requêtes FlashBack sur n'importe quelle table de n'importe quel schéma
UPDATE ANY TABLE	Mise à jour de lignes dans les tables de n'importe quel schéma



VIEWS	
CREATE VIEW	Création de vues dans le schéma
CREATE ANY VIEW	Création de vues dans n'importe quel schéma
DROP ANY VIEW	Suppression de vues dans n'importe quel schéma
UNDER ANY VIEW	Création de sous-vues sous n'importe quelle vue objet
Autres	
ANALYZE ANY	Analyse de tables, clusters et index dans n'importe quel schéma
AUDIT ANY	Audit de n'importe quel objet de n'importe quel schéma
COMMENT ANY TABLE	Pose de commentaires sur les tables et vues de n'importe quel schéma
FORCE ANY TRANSACTION	Force le commit ou rollback de n'importe quelle transaction distribuée douteuse
FORCE TRANSACTION	Force le commit ou rollback de n'importe quelle transaction distribuée douteuse
GRANT ANY OBJECT PRIVILEGE	Assigne n'importe quel privilège objet
GRANT ANY PRIVILEGE	Assigne n'importe quel privilège système
RESUMABLE	Active l'allocation d'espace pour les instructions résumables
SELECT ANY DICTIONARY	Interrogation de n'importe quel objet dans le dictionnaire du schéma SYS
SYSDBA	Autorise les opérations STARTUP et SHUTDOWN ALTER DATABASE: open, mount, back up, ou changement du jeu de caractères CREATE DATABASE ARCHIVELOG et RECOVERY CREATE SPFILE Inclue le privilège RESTRICTED SESSION
SYSOPER	Autorise les opérations STARTUP et SHUTDOWN ALTER DATABASE OPEN MOUNT BACKUP ARCHIVELOG et RECOVERY CREATE SPFILE Inclue le privilège RESTRICTED SESSION



TABLESPACES	
CREATE TABLESPACE	Création de tablespace
ALTER TABLESPACE	Modification de tablespace
DROP TABLESPACE	Suppression de tablespace
MANAGE TABLESPACE	Autorise la mise en ligne/hors ligne des tablespace
UNLIMITED TABLESPACE	Quota illimité sur le tablespace

DATABASE	
ALTER DATABASE	Modification de la base
ALTER SYSTEM	Autorise l'instruction ALTER SYSTEM
AUDIT SYSTEM	Autorise les instructions AUDIT sql_statements
DATABASE LINKS:	
CREATE DATABASE LINK	Création de liens de base de données dans le schéma
CREATE PUBLIC DATABASE LINK	Création de liens de base de données pour le groupe PUBLIC
DROP PUBLIC DATABASE LINK	Suppression de liens de base de données pour le groupe PUBLIC



- Créer l'utilisateur « Zied » identifié par « IIT », ayant :
 - Une tablespace par défaut « Tab1 », quota 10M
 - Une tablespace temporaire par défaut « Tab2 »
 - le mot de passe doit changer dès la première connexion

-- Créer l'utilisateur Zied avec le mot de passe IIT

CREATE USER Zied IDENTIFIED BY IIT;

-- Définir la tablespace par défaut Tab1 avec un quota de 10M

ALTER USER Zied DEFAULT TABLESPACE Tab1 QUOTA 10M;

-- Définir la tablespace temporaire par défaut Tab2

ALTER USER Zied TEMPORARY TABLESPACE Tab2;

-- Demander à l'utilisateur de changer son mot de passe à la première connexion

ALTER USER Zied PASSWORD EXPIRE;



- Changer le mot de passe de « Zied » par « IIT2024 » et lui attribuer le rôle par défaut « DBA »

-- Changer le mot de passe de l'utilisateur Zied en "IIT2024"

ALTER USER Zied IDENTIFIED BY IIT2024;

-- Attribuer le rôle par défaut DBA à l'utilisateur Zied

ALTER USER Zied DEFAULT ROLE DBA;

eq

-- une seule requête

**ALTER USER Zied
IDENTIFIED BY IIT2024
DEFAULT ROLE DBA;**

- Supprimer l'utilisateur « Zied »

DROP USER Zied CASCADE;



🗄 Donne le droit d'**exécuter une action particulière sur un objet** (Table, Vue, Procédure, Séquence, ...)

🗄 Les principaux privilèges objets sont :

- **ALTER** : modification de la structure d'un objet (table, séquence)
- **DELETE** : suppression des lignes d'un objet (table, vue)
- **INDEX** : création d'un index sur un objet (table)
- **INSERT** : insertion de lignes dans un objet (table, vue)
- **REFERENCES** : création de contraintes d'intégrité (table, vue)
- **SELECT [(col₁, ..., col_n)]** : consultation (table, vue, séquence)
- **UPDATE [(col₁, ..., col_n)]** : mise à jour des lignes (table, vue)
- **EXECUTE** : exécuter un programme (procédure, fonction)



Attribution de privilèges objet à un utilisateur

```
GRANT privilège_objet1 [(col1, ..., coln)] [,privilège_objet2, ...] | [ALL [PRIVILEGES]]  
ON [nom_schéma.] nom_objet]  
TO {nom_utilisateur1 [, nom_utilisateur2, ...] | PUBLIC}  
[WITH GRANT OPTION];
```

- **WITH GRANT OPTION** : donne au bénéficiaire le droit de transmettre le(s) privilège(s) à d'autres utilisateurs

NB. Les privilèges peuvent être attribués à plusieurs utilisateurs en un seul ordre.
L'attribution de privilèges se fait objet par objet.

Exemples :

- **GRANT SELECT, INSERT, UPDATE** (nom, adresse) **ON** Client **TO** Ali ;
- **GRANT ALL ON** Client **TO** Salah ;



Retrait de privilèges objet d'un utilisateur

```
REVOKE privilège_objet1 [(col1, ..., coln)] [,privilège_objet2, ...] | [ALL [PRIVILEGES]]  
ON [nom_schéma.] nom_objet]  
TO {nom_utilisateur1 [, nom_utilisateur2, ...] | PUBLIC}  
[CASCADE CONSTRAINT];
```

- **CASCADE CONSTRAINTS** : permet de retirer des privilèges REFERENCES

NB. Pour pouvoir enlever un privilège objet, il faut :

- Etre **propriétaire de l'objet**.
- Avoir reçu le **privilège objet** avec l'option **WITH GRANT OPTION** ou avoir reçu le **privilège système ANY OBJECT PRIVILEGE**.



Gestion des rôles



Définition

- ✓ Un rôle est un **regroupement nommé de privilèges (système et objet)** qui peut être attribué à un utilisateur
 - ➔ tous les privilèges regroupés dans le rôle sont alors simultanément attribués à l'utilisateur

Caractéristiques d'un rôle

- ✓ Un rôle peut être attribué à un autre rôle
- ✓ Un utilisateur peut avoir plusieurs rôles
- ✓ Un rôle n'appartient à personne

Mise en oeuvre d'un rôle

1. Création du rôle
2. Attribution des privilèges (système, objet) au rôle
3. Attribution du rôle à l'utilisateur



Création de rôle

```
CREATE ROLE nom_role  
[IDENTIFIED BY mot_de_passe |  
IDENTIFIED EXTERNALLY |  
IDENTIFIED USING nom_package |  
IDENTIFIED GLOBALLY |  
NOT IDENTIFIED ];
```

- IDENTIFIED BY *mot_de_passe* → un mot de passe est nécessaire pour activer le rôle
- IDENTIFIED EXTERNALLY → une identification externe est nécessaire pour activer le rôle
- IDENTIFIED USING *nom_package* → un package va être utilisé pour activer le rôle
- IDENTIFIED GLOBALLY → une identification d'un utilisateur GLOBAL est nécessaire pour activer le rôle
- NOT IDENTIFIED → aucune identification n'est nécessaire pour activer le rôle



Modification d'un rôle

```
ALTER ROLE nom_role  
[IDENTIFIED BY mot_de_passe |  
IDENTIFIED EXTERNALLY |  
IDENTIFIED USING nom_package |  
NOT IDENTIFIED ];
```

NB. La modification d'un rôle **ne concerne que son mot de passe**



Attribution de privilège système à un rôle

```
GRANT nom_privilège1 [,nom_privilège2,...]
TO {nom_rôle1, ... [,nom_rôle2, ...]
[WITH ADMIN OPTION] ;
```

Attribution de privilège objet à un rôle

```
GRANT privilège_objet1 [(col1, ..., coln)] [,privilège_objet2, ...] | [ALL [PRIVILEGES]]
ON [nom_schéma.] nom_objet
TO nom_rôle1 [, nom_rôle2,, ...] ;
```



Révocation de privilèges système à un rôle

```
REVOKE nom_privilège1 [,nom_privilège2,...]
FROM nom_rôle1, ... [,nom_rôle2, ...];
```

Révocation de privilèges objet à un rôle

```
REVOKE privilège_objet1 [(col1, ..., coln)] [,privilège_objet2, ...] | [ALL [PRIVILEGES]]
ON [nom_schéma.] nom_objet]
FROM nom_rôle1 [, nom_rôle2,, ...] ;
```



Attribution de rôle à un utilisateur ou à un rôle

```
GRANT nom_rôle1 [,nom_rôle2,...]
TO { nom_utilisateur | PUBLIC | nom_rôle } [, ...]
[WITH ADMIN OPTION] ;
```

➔ **Remarque** : « WITH ADMIN OPTION » donne aussi le droit de **modifier** et de **supprimer** le rôle

Révocation de rôle à un utilisateur ou à un rôle

```
REVOKE nom_rôle1 [,nom_rôle2, ...]
FROM {nom_utilisateur | PUBLIC | nom_rôle}[, ...];
```



Un rôle attribué à un utilisateur est **par défaut automatiquement** activé lors de la connexion de l'utilisateur.

Si l'utilisateur est connecté au moment de l'attribution du rôle, l'**activation** immédiate n'est pas automatique

→ L'**utilisateur** peut activer le rôle grâce à l'ordre SQL : **SET ROLE**

SET ROLE

```
{ nom_rôle1 [IDENTIFIED BY mot_de_passe],  
  nom_rôle2 [IDENTIFIED BY mot_de_passe],...}  
| ALL | [ALL EXCEPT rôle [,rôle] ...] | NONE ;
```

→ **SET ROLE** permet d'**activer** ou de **désactiver** un ou plusieurs rôles préalablement affectés à l'utilisateur par une commande **GRANT** pour la session courante.

→ Un rôle qui ne figure pas dans la liste est considéré comme **désactivé**.



🗄 L'ordre **ALTER USER** permet de définir les rôles par défaut d'un utilisateur

```
ALTER USER nom_utilisateur  
[ DEFAULT ROLE { rôle [,rôle,...]  
| ALL | [ALL EXCEPT rôle [,rôle] ...] | NONE} ] ;
```

- **DEFAULT ROLE ALL** : signifie que tous les rôles attribués à l'utilisateur sont activés par défaut.
- **DEFAULT ROLE ALL EXCEPT ...** : signifie que tous les rôles attribués à l'utilisateur sont activés par défaut sauf certains.
- **DEFAULT ROLE NONE** : signifie qu'aucun des rôles attribués à l'utilisateur n'est activé par défaut.



```
DROP ROLE nom_rôle;
```

- Pour supprimer un rôle, il faut avoir reçu ce rôle avec la clause « **WITH ADMIN OPTION** » ou avoir le privilège système **DROP ANY ROLE**.
- La suppression d'un rôle entraîne la révocation immédiate de ce rôle des utilisateurs bénéficiaires.



 Trois rôles prédéfinis : **CONNECT**, **RESOURCE**, **DBA**

CONNECT

Privilèges associés : CREATE VIEW, CREATE TABLE, ALTER SESSION, CREATE CLUSTER, CREATE SESSION, CREATE SYNONYM, CREATE SEQUENCE, CREATE DATABASE LINK

➔ `Select * from DBA_SYS_PRIVS where grantee = 'CONNECT' ;`

RESOURCE

Privilèges associés : CREATE TYPE, CREATE TABLE, CREATE CLUSTER, CREATE TRIGGER, CREATE OPERATOR, CREATE SEQUENCE, CREATE INDEXTYPE, CREATE PROCEDURE

DBA

Privilèges associés : Tous les privilèges



- ❑ Salah possède la table EMPLOYE. Il veut créer le rôle « R1 » identifié par le mot de passe « MPR1 » et lui attribuer le privilège de création de vues ainsi que tous les privilèges permettant de manipuler la table EMPLOYE.

-- Création du rôle R1 identifié par le mot de passe MPR1

CREATE ROLE R1 IDENTIFIED BY MPR1;

-- Attribution du privilège de création de vues au rôle R1

GRANT CREATE VIEW TO R1;

-- Attribution de tous les privilèges permettant de manipuler la table EMPLOYE au rôle R1

GRANT SELECT, INSERT, UPDATE, DELETE ON EMPLOYE TO R1;

- ❑ Salah veut attribuer le rôle R1 à Ali qui est actuellement connecté. Que doit faire Salah et que doit faire Ali ? (Voir diapo 40)

-- Salah (administrateur) doit accorder le rôle R1 à Ali

GRANT R1 TO Ali;

-- Ali doit **activer le rôle R1** où bien se déconnecter et se connecter de nouveau

SET ROLE R1 IDENTIFIED BY MPR1;



Gestion des profils



Notion de profil

Un profil est un **ensemble** nommé de **limitations de ressources** qui peut être attribué à un **utilisateur**

☐ Les ressources suivantes peuvent être limitées :

- Nombre de sessions ouvertes simultanément par un utilisateur
- Temps CPU par appel et/ou par session
- Temps d'inactivité par session
- Nombre de lectures logiques par appel et/ou par session
- Durée totale de la session
- Nombre de tentatives de connexion



Le profil DEFAULT

- Le profil nommé **DEFAULT** est automatiquement créé lors de la création de la BD
- Ce profil est attribué par défaut aux utilisateurs
- Par défaut, ce profil n'impose aucune limitation pour les ressources.
 - ➔ Par contre, depuis la version 11 de Oracle, ce profil comporte des limites pour les mots de passe

Actions sur les profils

- Création d'un profil
- Modification de profil
- Suppression de profil
- Attribution d'un profil à un utilisateur



```
CREATE PROFILE nom_profile LIMIT  
[SESSIONS_PER_USER {valeur | UNLIMITED | DEFAULT}]  
[CPU_PER_SESSION {valeur | UNLIMITED | DEFAULT}]  
[CPU_PER_CALL {valeur | UNLIMITED | DEFAULT}]  
[CONNECT_TIME {valeur | UNLIMITED | DEFAULT}]  
[IDLE_TIME {valeur | UNLIMITED | DEFAULT}]  
[LOGICAL_READS_PER_SESSION {valeur | UNLIMITED | DEFAULT}]  
[LOGICAL_READS_PER_CALL {valeur | UNLIMITED | DEFAULT}]  
[COMPOSITE_LIMIT {valeur | UNLIMITED | DEFAULT}]  
[PRIVATE_SGA {valeur [K|M] | UNLIMITED | DEFAULT}]  
[FAILED_LOGIN_ATTEMPTS {valeur | UNLIMITED | DEFAULT}]  
[PASSWORD_LIFE_TIME {valeur | UNLIMITED | DEFAULT}]  
[PASSWORD_REUSE_TIME {valeur | UNLIMITED | DEFAULT}]  
[PASSWORD_REUSE_MAX {valeur | UNLIMITED | DEFAULT}]  
[PASSWORD_LOCK_TIME {valeur | UNLIMITED | DEFAULT}]  
[PASSWORD_GRACE_TIME {valeur | UNLIMITED | DEFAULT}]  
[PASSWORD_VERIFY_FUNCTION {fonction | NULL | DEFAULT}];
```




Option	Description
SESSIONS_PER_USER	Nombre de session max qu'un utilisateur peut ouvrir simultanément
CPU_PER_SESSION	Temps de processeur max (en centième de seconde) qu'une session peut utiliser
CPU_PER_CALL	Temps de processeur max (en centième de seconde) qu'un « appel serveur » peut utiliser
CONNECT_TIME	Temps en minutes pour la durée de connexion maximale d'une session. A la fin de ce temps, la session est automatiquement déconnectée
IDLE_TIME	Temps en minutes pour la durée d'inactivité maximale d'une session. A la fin de ce temps, la session est automatiquement déconnectée
LOGICAL_READS_PER_SESSION	Nombre maximal de blocs lus pendant une session
LOGICAL_READS_PER_CALL	Nombre maximal de blocs lus pendant un appel serveur



Option	Description
COMPOSITE_LIMIT	Coût total des limitations autorisées pour une session. Il s'agit de la somme pondérée de CPU_PER_SESSION, CONNECT_TIME, LOGICAL_READS_PER_SESSION et PRIVATE_SGA.
PRIVATE_SGA	Quantité de la mémoire privée dans la SGA (par session)



Option	Description
FAILED_LOGIN_ATTEMPTS	Nombre d'échecs de tentative de connexion , avant verrouillage du compte.
PASSWORD_LIFE_TIME	Durée de vie du mot de passe (en jours), <u>180 dans le profil DEFAULT</u>
PASSWORD_REUSE_TIME	Nombre de jours pendant lequel un mot de passe ne peut pas être réutilisé
PASSWORD_REUSE_MAX	Nombre de changements de mot de passe avant qu'un mot de passe puisse être réutilisé
PASSWORD_LOCK_TIME	Durée du verrouillage (en jours), <u>1 dans le profil DEFAULT</u>
PASSWORD_GRACE_TIME	Période de grâce après expiration du mot de passe (en jours), <u>7 dans le profil DEFAULT</u>
PASSWORD_VERIFY_FUNCTION	Fonction de vérification de la complexité du mot de passe



ALTER PROFILE nom_profil **LIMIT**

[**SESSIONS_PER_USER** {valeur | **UNLIMITED** | **DEFAULT**}]

[**CPU_PER_SESSION** {valeur | **UNLIMITED** | **DEFAULT**}]

[**CPU_PER_CALL** {valeur | **UNLIMITED** | **DEFAULT**}]

[**CONNECT_TIME** {valeur | **UNLIMITED** | **DEFAULT**}]

[**IDLE_TIME** {valeur | **UNLIMITED** | **DEFAULT**}]

[**LOGICAL_READS_PER_SESSION** {valeur | **UNLIMITED** | **DEFAULT**}]

[**LOGICAL_READS_PER_CALL** {valeur | **UNLIMITED** | **DEFAULT**}]

[**COMPOSITE_LIMIT** {valeur | **UNLIMITED** | **DEFAULT**}]

[**PRIVATE_SGA** {valeur [K|M] | **UNLIMITED** | **DEFAULT**}]

[**FAILED_LOGIN_ATTEMPTS** {valeur | **UNLIMITED** | **DEFAULT**}]

[**PASSWORD_LIFE_TIME** {valeur | **UNLIMITED** | **DEFAULT**}]

[**PASSWORD_REUSE_TIME** {valeur | **UNLIMITED** | **DEFAULT**}]

[**PASSWORD_REUSE_MAX** {valeur | **UNLIMITED** | **DEFAULT**}]

[**PASSWORD_LOCK_TIME** {valeur | **UNLIMITED** | **DEFAULT**}]

[**PASSWORD_GRACE_TIME** {valeur | **UNLIMITED** | **DEFAULT**}]

[**PASSWORD_VERIFY_FUNCTION** {fonction | **NULL** | **DEFAULT**}];



```
DROP PROFILE nom_profil [CASCADE];
```

- Pour pouvoir supprimer un profil, il faut disposer du privilège **DROP PROFILE**.
- Si le **profil** à supprimer **n'a été attribué à aucun utilisateur**, l'option CASCADE est inutile.
- Si le **profil** à supprimer a été **attribué à des utilisateurs**, il faut utiliser l'option **CASCADE**.



❑ Un profil peut être attribué à un utilisateur :

- lors de la création de l'utilisateur (CREATE USER)
- lors d'une modification de l'utilisateur (ALTER USER)

➔ L'**affectation d'un nouveau profil** à des utilisateurs ne prend effet qu'à leur **prochaine connexion**.

➔ **Par défaut**, un utilisateur est créé avec le profil DEFAULT.

➔ **Par défaut**, le contrôle de la limitation des ressources n'est pas actif.



❑ Créer un profile « PROFIL_ADMIN » ayant comme limitations de ressources :

- Max 50 sessions autorisées simultanément
- CPU max par session active est de 30 secondes
- Chaque session ne peut excéder 1 heure
- Durée max d'inactivité de session courante est de 30 minutes
- Nombre maximal de blocs transférés est 100000 blocs
- Mot de passe valable pendant 90 jours et il faut attendre 30 jours avant qu'il puisse être utilisé
- 5 tentatives de connexion sont possibles avant le blocage du compte

Gestion des profils - Exemple - Correction



CREATE PROFILE PROFIL_ADMIN LIMIT

SESSIONS_PER_USER 50 -- L'utilisateur peut ouvrir simultanément au maximum 50 sessions

CPU_PER_SESSION 30000000 -- Temps de processeur max=30 secondes qu'une session peut utiliser

CONNECT_TIME 60 -- 1 heure = durée de connexion maximale de session

IDLE_TIME 30 -- 30 minutes = durée d'inactivité maximale de session courante

LOGICAL_READS_PER_SESSION 100000 -- Nombre maximal de blocs lus pendant une session

PASSWORD_LIFE_TIME 90 -- Durée de vie du mot de passe=90 jours, 180 dans le profil DEFAULT

PASSWORD_REUSE_TIME 30 -- 30 jours pendant lequel un mot de passe ne peut pas être réutilisé

PASSWORD_LOCK_TIME 30 -- 30 jours du verrouillage, 1 jour dans le profil DEFAULT

PASSWORD_GRACE_TIME 5 -- Période de grâce après expiration du mot de passe = 5 jours), 7 dans le profil DEFAULT

FAILED_LOGIN_ATTEMPTS 5; -- 5 échecs de tentative de connexion , avant verrouillage du compte