

---

**Administration Oracle 12\_19C**  
**Partie I, Chapitre 5.**  
**Gestion de la sécurité et des ressources**

**G. Mopolo-Moké**  
**prof. Associé UNSA**

# 5. Gestion de la sécurité et des ressources

---

## □ Plan

- 5.1 Généralités
- 5.2 Les Privilèges
  - Introduction
  - Les privilèges Systèmes
  - Les privilèges Objets
- 5.3 Les rôles
  - Intérêts des rôles
  - Création et suppression des rôles
  - Affectation des privilèges ou des rôles à un rôle
  - Sécurité des rôles
  - Les rôles du Système d'exploitation
  - Les rôles prédéfinis
- 5.4 Les profils
  - Intérêt des profils
  - Création , Suppression et Modification de profils
  - Utilisation des limites composites
  - Affectation d'un profil à un utilisateur

## 5. Gestion de la sécurité et des ressources

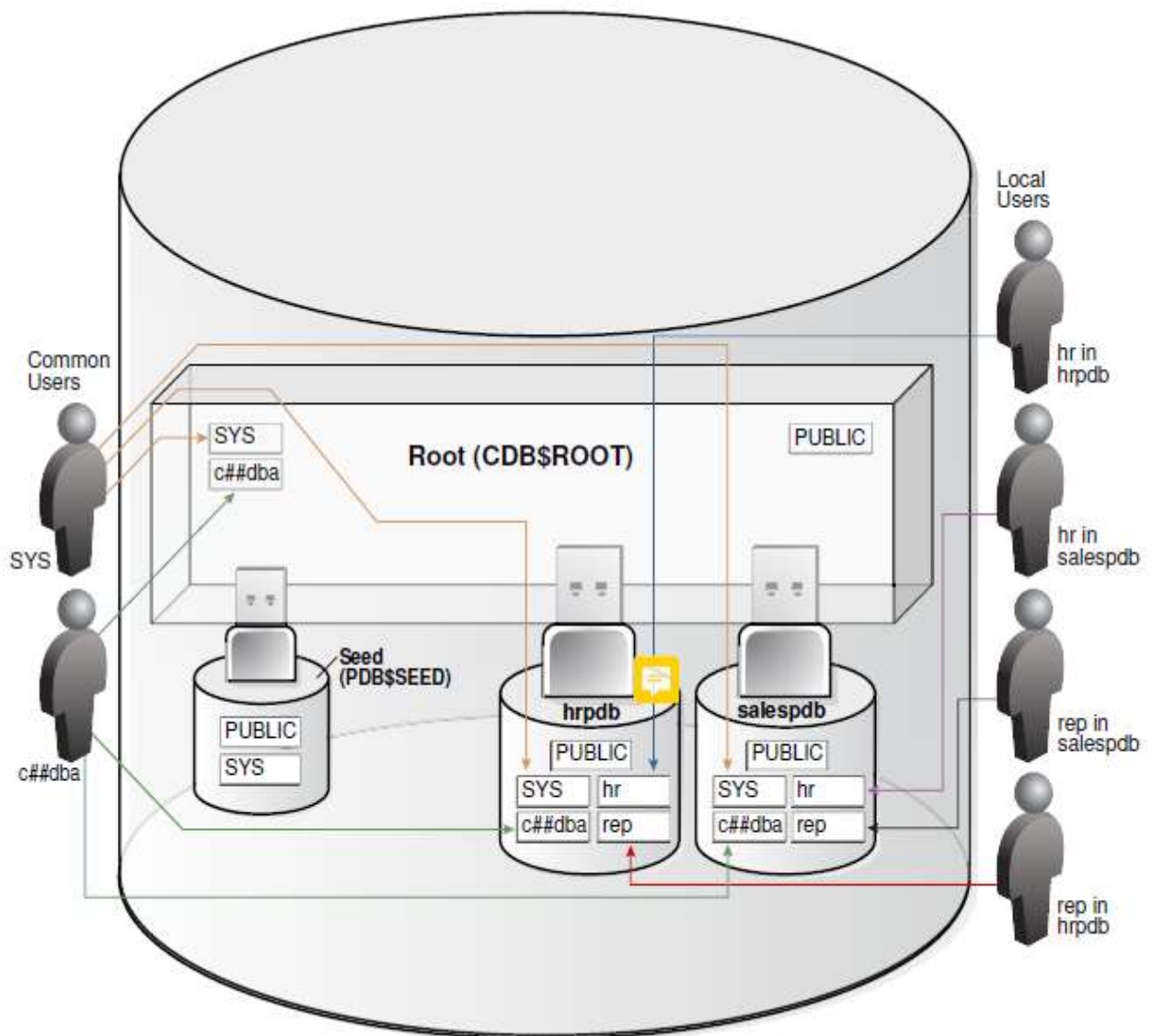
---

### □ PLAN

- 5.5 Les utilisateurs
  - La politique de licences d'Oracle
  - Les Utilisateurs prédéfinis
  - Les différents mode d'authentification
  - Création d'un Utilisateur
  - Modification d'un Utilisateur
  - Suppression d'un Utilisateur
  - Affectation des droits à un Utilisateur
- 5.6 L'audit traditionnel
  - Intérêt de l'audit
  - Types d'audit et modes d'activation
  - Audit Système
  - Audit objet
  - La table aud\$
- 5.7 L'audit unifié

## 5.1 Généralités

### □ Les utilisateurs et leurs schémas dans un CDB



1) Un **utilisateur créé au niveau CDB\$ROOT est visible** dans tous les PDBs. Par contre pour qu'il se connecte dans un PDB il faut lui donner les droits à ce niveau.

2) Un **utilisateur créé au niveau d'un PDB n'est visible que dans ce PDB.**

## 5.1 Généralités

---

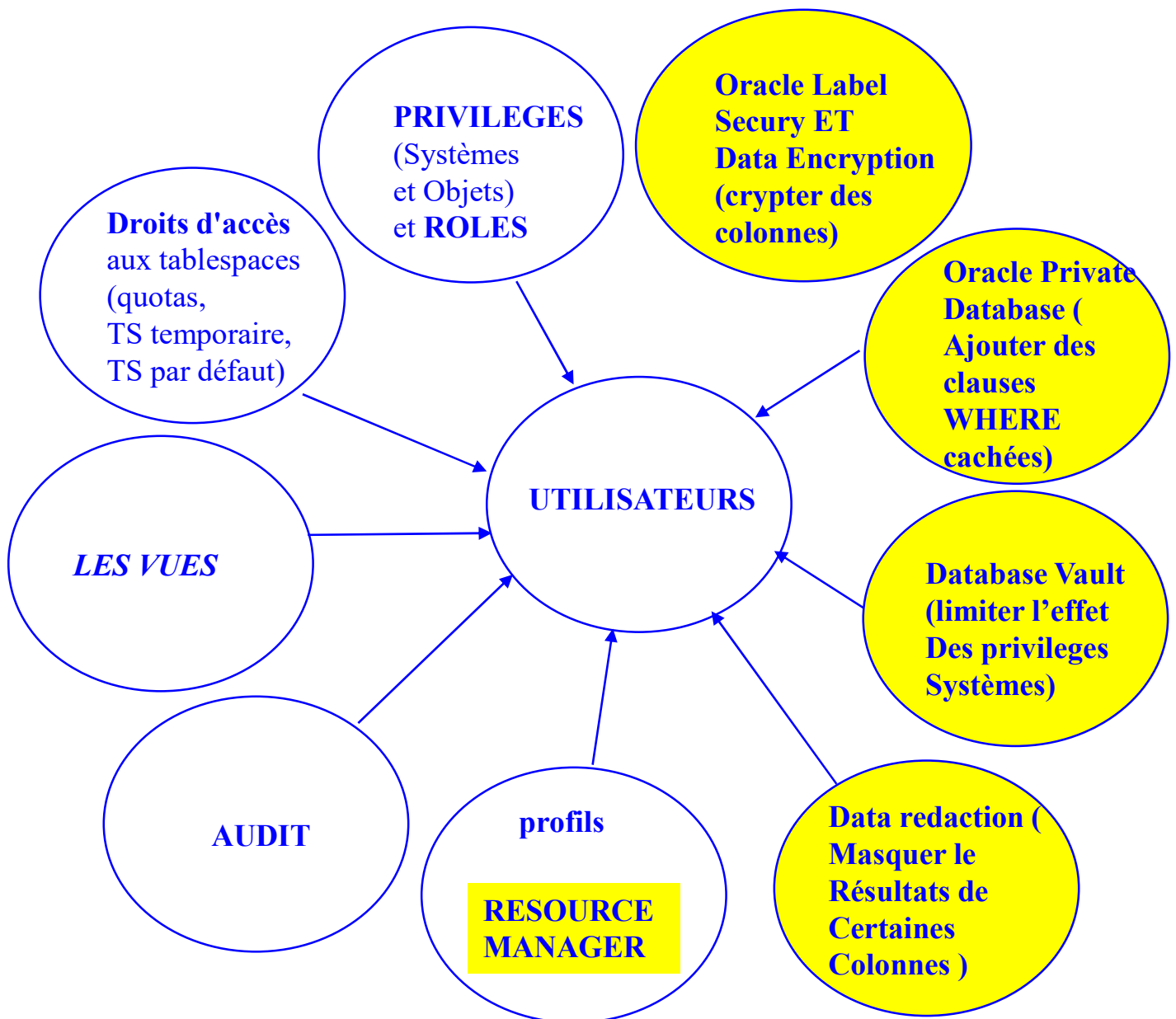
### □ Rôle de l'Administrateur de sécurité et des ressources

- Définir une politique de sécurité
- Faire les **choix du type de sécurité** : au niveau système, au niveau Oracle, au niveau Global (LDAP)
- Gérer les **utilisateurs**
- Gérer les ressources (**profils**)
- Assurer l'**affectation et le retrait** des droits
- **Affiner la politique** de sécurité par l'utilisation des rôles
- Effectuer les **audits**
- Gérer la sécurité avancée

## 5.1 Généralités

---

### □ Moyens pour la Gestion de la sécurité



NOTE : En jaune pas traité dans ce cours

## 5.1 Généralités

---

### □ Sécurité avancée (pas traité dans ce cours)

- **Data Redaction** : possibilité d'empêcher l'affichage des données de certaines colonnes, par exemple l'utilisateur ne verra que des 0 sur une colonne NUMBER sensible
- **Data Encryption** : Possibilité de créer des tables avec des colonnes cryptées (ENCRYPT)
- **Oracle Label Security** : catégorisation des objets et des accès
- **Oracle Database Vault** : Permet de limiter l'accès aux privilèges systèmes puissants tels que : Select any table, alter system, etc. aux données utilisateurs. Pour empêcher par exemple le DBA d'utiliser le Select Any Table pour consulter une table dans un schéma donné
- **Oracle private database** : permet d'ajouter à des requêtes SQL des clauses WHERE pour restreindre l'accès aux données

## 5.2 Les Privilèges

---

### □ Introduction

- Un privilège donne le droit d'exécuter certaines commandes SQL ou le droit d'accéder à certaines ressources
- Oracle possède deux types de privilèges :  
les *privilèges systèmes* et les *privilèges objets*.
- Un privilège peut être affecté (retiré) à un Utilisateur, un Rôle ou tous les utilisateurs (PUBLIC)



## 5.2 Les privilèges

---

### □ Les privilèges Systèmes

- *Plus de 237 privilèges en 12c, 220 en 11G, 160 en 10G* accordés au rôle DBA, la V6 en avait 3 : (*Connect, resource, dba*)
- Les privilèges Systèmes donnent le droit de réaliser des opérations systèmes tel que créer un tablespace, un utilisateur, ...

## 5.2 Les privilèges

---

### □ Les privilèges Systèmes

- Ces privilèges sont classés par catégories d'objets

ANALYTIC VIEWS	ANALYZE
AUDIT	CLUSTER
CONTEXT	DATA REDACTION
DATABASE	DATABASE LINK
DEBUGGING	DICTIONARIES
DIMENSION	DIRECTORIES
EDITIONS	Flashback data archivess
HIERARCHIES	INDEXES
INDEXTYPE	Job scheduler objects
KEY MANAGEMENT FRAMEWORK	LIBRARY
LOGMINER	MATERIALIZED VIEW
MINING MODELS	OLAP CUBES
Olap cube measure folders	OLAP CUBE Dimensions
Olap cube build processes	OPERATOR
OUTLINE	PDB LOCKDOWN profils
PLAN MANAGEMENT	PLUGGABLE DATABASES
PROCEDURE	profil
ROLES	ROLLBACK SEGMENTS
SEQUENCE	SESSION
SNAPSHOT	SQL TRANSACTION profils
SYNONYM	<b>TABLE</b>
TABLESPACE	TRANSACTION
TRIGGER	TYPE
USER	VIEW
SCHEDULE	<b>MISCELLANEOUS</b>

## 5.2 Les privilèges

---

### □ Les privilèges systèmes (suite)

- Exemple de privilèges systèmes de la catégorie **TABLE**:

CREATE TABLE	CREATE ANY TABLE
ALTER ANY TABLE	BACKUP ANY TABLE
DROP ANY TABLE	LOCK ANY TABLE
LOCK ANY TABLE	<i>SELECT ANY TABLE</i>
INSERT ANY TABLE	UPDATE ANY TABLE
<i>DELETE ANY TABLE</i>	COMMENT ANY TABLE
UNDER ANY TABLE	DEBUG ANY TABLE
FLASHBACK ANY TABLE	

- Exemple de privilèges systèmes **MISCELLANEOUS**

SYSBACKUP	SYSDB
SYSOPER	SYSDBA
SELECT ANY TRANSACTION	SELECT ANY Dictionary

**NOTE :** Voir le manuel SQL reference Manual (Ordre Grant) pour obtenir la liste complète des privilèges systèmes et objets

## 5.2 Les privilèges

---

### □ Les privilèges systèmes (suite)

- Affectation d'un privilège Système

```
GRANT { system_priv | role | ALL PRIVILEGES }  
      [CONTAINER={CURRENT | ALL}]  
      TO { user [IDENTIFIED BY password | role |  
      PUBLIC }, ...  
      [ WITH {ADMIN | DELEGATE} OPTION ]
```

**System\_priv** : nom d'un privilège système

**role** : Nom d'un rôle

**user, role ou PUBLIC** : droit affecté à un utilisateur, un rôle ou public

**With Admin Option** : le rôle pourra être redistribué par celui qui le reçoit

**ALL PRIVILEGES** : affectation de tous les privilèges system sauf *select any catalog*

**IDENTIFIED BY password** :

Si l'utilisateur n'existe pas, il sera créé avec le mot de passe indiqué. Les privilèges lui seront affectés

**With delegate option** : Celui qui reçoit le role peut le donner à un programme

**CONTAINER={CURRENT | ALL}** : donne les privileges au niveau du container courant ou de tous les containers.

## 5.2 Les privilèges

---

### □ Les privilèges systèmes (suite)

- Affectation des privilèges systèmes (suite)

- L'affectation d'un privilège avec l'option "WITH ADMIN OPTION" suit les règles suivantes :

- Celui qui reçoit le droit peut le redistribuer
    - **Son retrait** à un utilisateur qui lui-même l'a affecté à un autre **ne peut se faire en cascade**
    - ne peut être affecté à un ROLE

- **Exemple**

```
GRANT ALTER TABLESPACE TO scott ;
```

```
GRANT CREATE USER,  
      CREATE SESSION TO scott  
      WITH ADMIN OPTION ;
```

```
GRANT ALTER ANY TABLE TO PUBLIC ;
```

## 5.2 Les privilèges

---

### □ Les Privilèges Systèmes (suite)

- Révocation d'un privilège Système

#### Syntaxe

```
REVOKE { system_priv[,system_priv]... | role | ALL  
PRIVILEGES } [CONTAINER current | ALL]  
FROM { user | role | PUBLIC }
```

[cas cascade constraints | FORCE]

#### Exemple :

- ```
REVOKE ALTER ANY TABLE FROM PUBLIC ;  
REVOKE CREATE SESSION FROM SCOTT ;
```

**NOTE :** Supposant qu'un utilisateur U1 attribut un privilège P1 "WITH ADMIN OPTION" à un utilisateur U2 et que U2 l'attribut à son tour à U3. La révocation de P1 à U2 n'entraîne pas la révocation de P1 à U3.

## 5.2 Les privilèges

### □ Les Privilèges Systèmes (suite)

- Les vues du dictionnaire

set pagesize 2000

col grantee format A30

col privilege format A35

SELECT \* FROM DBA\_SYS\_PRIVS where  
grantee='DBA' ORDER BY grantee, privilege ;

| GRANTEE | PRIVILEGE                         | ADM | COM | INH |
|---------|-----------------------------------|-----|-----|-----|
| DBA     | ADMINISTER ANY SQL TUNING SET     | NO  | YES | NO  |
| DBA     | ADMINISTER DATABASE TRIGGER       | NO  | YES | NO  |
| DBA     | ADMINISTER RESOURCE MANAGER       | NO  | YES | NO  |
| DBA     | ADMINISTER SQL MANAGEMENT OBJECT  | NO  | YES | NO  |
| DBA     | ADMINISTER SQL TUNING SET         | NO  | YES | NO  |
| DBA     | ADVISOR                           | NO  | YES | NO  |
| DBA     | ALTER ANY ANALYTIC VIEW           | NO  | YES | NO  |
| DBA     | ALTER ANY ASSEMBLY                | NO  | YES | NO  |
| DBA     | ALTER ANY ATTRIBUTE DIMENSION     | NO  | YES | NO  |
| DBA     | ALTER ANY CLUSTER                 | NO  | YES | NO  |
| DBA     | ALTER ANY CUBE                    | NO  | YES | NO  |
| DBA     | ALTER ANY CUBE BUILD PROCESS      | NO  | YES | NO  |
| DBA     | ALTER ANY CUBE DIMENSION          | NO  | YES | NO  |
| DBA     | ALTER ANY DIMENSION               | NO  | YES | NO  |
| DBA     | ALTER ANY EDITION                 | NO  | YES | NO  |
| DBA     | ALTER ANY EVALUATION CONTEXT      | NO  | YES | NO  |
| DBA     | ALTER ANY HIERARCHY               | NO  | YES | NO  |
| DBA     | ALTER ANY INDEX                   | NO  | YES | NO  |
| DBA     | ALTER ANY INDEXTYPE               | NO  | YES | NO  |
| DBA     | ALTER ANY LIBRARY                 | NO  | YES | NO  |
| DBA     | ALTER ANY MATERIALIZED VIEW       | NO  | YES | NO  |
| DBA     | ALTER ANY MEASURE FOLDER          | NO  | YES | NO  |
| DBA     | ALTER ANY MINING MODEL            | NO  | YES | NO  |
| DBA     | ALTER ANY OPERATOR                | NO  | YES | NO  |
| DBA     | ALTER ANY OUTLINE                 | NO  | YES | NO  |
| DBA     | ALTER ANY PROCEDURE               | NO  | YES | NO  |
| DBA     | ALTER ANY ROLE                    | NO  | YES | NO  |
| DBA     | ALTER ANY RULE                    | NO  | YES | NO  |
| DBA     | ALTER ANY RULE SET                | NO  | YES | NO  |
| DBA     | ALTER ANY SEQUENCE                | NO  | YES | NO  |
| DBA     | ALTER ANY SQL PROFILE             | NO  | YES | NO  |
| DBA     | ALTER ANY SQL TRANSLATION PROFILE | NO  | YES | NO  |
| DBA     | ALTER ANY TABLE                   | NO  | YES | NO  |
| DBA     | ALTER ANY TRIGGER                 | NO  | YES | NO  |
| DBA     | ALTER ANY TYPE                    | NO  | YES | NO  |
| DBA     | ALTER DATABASE                    | NO  | YES | NO  |
| DBA     | ALTER LOCKDOWN PROFILE            | NO  | YES | NO  |
| DBA     | ALTER PROFILE                     | NO  | YES | NO  |
| DBA     | ALTER RESOURCE COST               | NO  | YES | NO  |
| DBA     | ALTER RESOURCE SEgment            | NO  | YES | NO  |

## 5.2 Les privilèges

---

### □ Les privilèges Objets

- Ces privilèges contrôlent l'accès aux objets des tables, vues, séquences, procédures, fonctions et packages, vue matérialisée (VM) ....
- La vue **v\$object\_privilege** contient la liste des privilèges objets , type et noms d'objets sur lesquels ils s'appliquent

- Voir le tableau page suivante

select

distinct PRIVILEGE\_NAME,

object\_type\_name

from **v\$object\_privilege**

order by PRIVILEGE\_NAME, object\_type\_name



## 5.2 Les privilèges

### □ Les privilèges Objets

- Classification selon les types d'objets

| Droit objet       | Libellé                                 | Objets concernés                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ALTER             | Droit de modifier                       | JOB RESOURCE, JSFW, MINING MODEL, MINING MODEL PARTITION, OLAP ANALYTIC VIEW, OLAP BUILD PROCESS, OLAP CUBE, OLAP CUBE DIMENSION, OLAP HIERARCHY, OLAP HIERARCHY DIMENSION, OLAP MEASURE FOLDER, RULE, RULE EVALUATION CONTEXT, RULESET, SCHEDULER CHAIN, SCHEDULER CREDENTIAL, SCHEDULER DESTINATION, SCHEDULER GROUP, SCHEDULER JOB, SCHEDULER PROGRAM, SCHEDULER SCHEDULE, SEQUENCE, SQL TRANSLATION PROFILE, TABLE |
| DEBUG             | Droit d'activer le mode debug           | ASSEMBLY, FUNCTION, JAVA CLASS, JAVA RESOURCE, JAVA SHARED DATA, JAVA SOURCE, LIBRARY, PACKAGE, PROCEDURE, TABLE, TYPE, VIEW                                                                                                                                                                                                                                                                                           |
| DELETE            | Droit de supprimer                      | OLAP CUBE DIMENSION, OLAP MEASURE FOLDER, TABLE, VIEW                                                                                                                                                                                                                                                                                                                                                                  |
| DEQUEUE           | Droit d'enlever de la queue             | QUEUE                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ENQUEUE           | Droit de mettre dans la queue           | QUEUE                                                                                                                                                                                                                                                                                                                                                                                                                  |
| EXECUTE           | Droit d'exécuter                        | ASSEMBLY, DIRECTORY, FUNCTION, INDEX, JAVA CLASS, JAVA RESOURCE, JAVA SHARED DATA, JAVA SOURCE, JSFW, LIBRARY, OPERATOR, PACKAGE, PROCEDURE, RESOURCE MANAGER CONSUMER GROUP, RULE, RULE EVALUATION CONTEXT, RULESET, SCHEDULER CHAIN, SCHEDULER CLASS, SCHEDULER CREDENTIAL, SCHEDULER PROGRAM, STREAMS FILE GROUP, TYPE                                                                                              |
| FLASHBACK         | Droit de reculer dans le passé          | TABLE, VIEW                                                                                                                                                                                                                                                                                                                                                                                                            |
| INDEX             | Droit de pauser un index                | TABLE                                                                                                                                                                                                                                                                                                                                                                                                                  |
| INSERT            | Droit d'insérer                         | OLAP CUBE DIMENSION, OLAP MEASURE FOLDER, TABLE, VIEW                                                                                                                                                                                                                                                                                                                                                                  |
| KEEP SEQUENCE     | Droit de conserver la valeur de nextval | SEQUENCE                                                                                                                                                                                                                                                                                                                                                                                                               |
| MERGE VIEW        | Droit d'effectuer un merge view         | VIEW                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ON COMMIT REFRESH | Droit de créer une vue matérialisée     | TABLE, VIEW                                                                                                                                                                                                                                                                                                                                                                                                            |
| QUERY REWRITE     | Droit de réécrire une requête           | TABLE, VIEW                                                                                                                                                                                                                                                                                                                                                                                                            |
| READ              | Droit de lire                           | DIRECTORY, OLAP ANALYTIC VIEW, OLAP HIERARCHY, OLAP HIERARCHY DIMENSION, STREAMS FILE GROUP, TABLE, VIEW                                                                                                                                                                                                                                                                                                               |
| REFERENCES        | Droit référencer (oreign key)           | TABLE, VIEW                                                                                                                                                                                                                                                                                                                                                                                                            |
| SELECT            | Droit de consulter                      | MINING MODEL, MINING MODEL PARTITION, OLAP ANALYTIC VIEW, OLAP BUILD PROCESS, OLAP CUBE, OLAP CUBE DIMENSION, OLAP HIERARCHY, OLAP HIERARCHY DIMENSION, OLAP MEASURE FOLDER, SCHEDULER GROUP, SEQUENCE, TABLE, VIEW                                                                                                                                                                                                    |
| UNDER             | Droit d'hériter                         | TABLE, TYPE, VIEW                                                                                                                                                                                                                                                                                                                                                                                                      |
| UPDATE            | Droit de mettre à jour                  | OLAP BUILD PROCESS, OLAP CUBE, OLAP CUBE DIMENSION, TABLE, VIEW                                                                                                                                                                                                                                                                                                                                                        |
| USE               | Droit d'utiliser un profil de requête   | EDITION, JOB RESOURCE, SQL TRANSLATION PROFILE                                                                                                                                                                                                                                                                                                                                                                         |
| WRITE             | Droit d'écrire                          | DIRECTORY                                                                                                                                                                                                                                                                                                                                                                                                              |

## 5.2 Les privilèges

---

### □ Les privilèges Objets (suite)

- Affectation de privilèges objets

#### Syntaxe

```
GRANT { object_priv | ALL [ PRIVILEGES ] } [( column [,column ] ... ) ]  
    [, { object_priv | ALL [ PRIVILEGES ] } [ ( column [,column] ... ) ] ]  
    ON {[ schema.] object | DIRECTORY directory_name |  
    EDITION edition_name |  
    MINING MODEL[schema.]mining_model_name |  
    JAVA {SOURCE | RESOURCE} [schema.]object |  
    SQL TRANSLATION PROFILE nomprofil}  
    TO { user [IDENTIFIED BY password] | role | PUBLIC }[,...]  
        [ WITH GRANT OPTION ]  
        [ WITH HIERARCHY OPTION]
```

#### Notes :

**ALL** : n'est pas un privilège mais signifie "tous les privilèges sur un objet"

**object\_priv**: Nom du privilège

**column** : Nom d'une colonne si object\_priv= *insert, update ou references*

**schema.objet** : Nom de l'objet concerné

**With Grant Option**: L'utilisateur qui reçoit le privilège peut le réaffecter

**Directory directoy\_name** : droit d'accès à une directory

**JAVA {SOURCE| RESOURCE} objet** : droit d'accès à une ressource java

**With grant hierarchy** :Les droits seront données à une hiérarchie d'objet

**EDITION** : name: droit de créer des versions

**MINING MODEL** :

## 5.2 Les privilèges

---

### □ Les privilèges Objets (suite)

- Affectation de privilèges objets

#### Exemple

```
sql> GRANT INSERT (ename, job) ON emp TO scott with grant option ;
```

```
sql> GRANT UPDATE (SAL), DELETE ON emp TO scott ;
```

```
sql> GRANT REFERENCES, UPDATE ON bonus TO dupont ;
```

```
sq>GRANT SELECT ON emp to dupond;
```

## 5.2 Les privilèges

---

### □ Les privilèges Objets (suite)

- Révocation de privilèges objets

#### Syntaxe

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

#### Notes

***CASCADE CONSTRAINTS*** : s'emploie avec le privilège REFERENCES, supprime les contraintes d'intégrité mises.

#### ***Retrait d'un privilège et WITH GRANT OPTION:***

Si un utilisateur U1 a affecté un privilège P1 à U2 et U2 l'a affecté à U3, le retrait à U2 entraîne le retrait à U3 : le retrait se fait en cascade.

#### Exemples

```
sql>REVOKE DELETE ON Bonus FROM scott ;  
sql>REVOKE UPDATE ON emp FROM public;  
sql>REVOKE REFERENCES ON scott.emp FROM dupont ;  
sql>REVOKE ALL ON bonus FROM PUBLIC ;
```

## 5.2 Les privilèges

---

### □ Les privilèges Objets (suite)

- Visualisation des privilèges objets

|                     |                     |
|---------------------|---------------------|
| DBA_TAB_PRIVS       | DBA_COL_PRIVS       |
| ALL_TAB_PRIVS       | ALL_COL_PRIVS       |
| USER_TAB_PRIVS      | USER_COL_PRIVS      |
| All_TAB_PRIVS_MADE  | DBA_COL_PRIVS       |
| USER_TAB_PRIVS_MADE | ALL_COL_PRIVS_MADE  |
| USER_TAB_PRIVS_MADE | USER_COL_PRIVS_MADE |
| ALL_TAB_PRIVS_RECD  | ALL_COL_PRIVS_RECD  |
| USER_TAB_PRIVS_RECD | ALL_COL_PRIVS_RECD  |
| TABLE_PRIVILEGES    | COLUMN_PRIVILEGES   |
| CDB_TAB_PRIVS       | CDB_COL_PRIVS       |

#### Principales Colonnes de vues ci-dessus

|             |                                          |
|-------------|------------------------------------------|
| GRANTEE     | : utilisateur ayant reçu le privilège    |
| OWNER       | : propriétaire de la table               |
| TABLE_NAME  | : nom de la table                        |
| COLUMN_NAME | : Nom de la colonne concerné             |
| GRANTOR     | : Utilisateur ayant affecté le privilège |
| PRIVILEGE   | : privilège affecté                      |
| GRANT       | : privilège reçu.                        |

## 5.2 Les privilèges

---

### □ Les privilèges Objets (suite)

- Visualisation des privilèges objets

Visualisation de tous les droits sur les objets de la base

Connect scott/tiger

GRANT alter, delete, index, insert, select, update, references ON  
Bonus TO dupont;

set linesize 200

col grantee format A10

col owner format A10

col table\_name format A10

col grantor format A10

col table\_name format A10

col privilege format A10

SELECT grantee, owner, table\_name, grantor, privilege

FROM sys.dba\_tab\_privs WHERE table\_name = 'BONUS' OR table\_name = 'EMP';

| GRANTEE | OWNER | TABLE_NAME | GRANTOR | PRIVILEGE  |
|---------|-------|------------|---------|------------|
| DUPONT  | SCOTT | BONUS      | SCOTT   | ALTER      |
| DUPONT  | SCOTT | BONUS      | SCOTT   | DELETE     |
| DUPONT  | SCOTT | BONUS      | SCOTT   | INDEX      |
| DUPONT  | SCOTT | BONUS      | SCOTT   | INSERT     |
| DUPONT  | SCOTT | BONUS      | SCOTT   | SELECT     |
| DUPONT  | SCOTT | BONUS      | SCOTT   | UPDATE     |
| DUPONT  | SCOTT | BONUS      | SCOTT   | REFERENCES |

7 lignes sélectionnées.

## 5.2 Les privilèges

---

### □ Les privilèges Objets (suite)

- Visualisation des privilèges objets

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

```
SELECT * FROM sys.dba_col_privs ;
```

## 5.3 Les rôles

---

### □ Plan

- Généralités
- Création d'un rôle
- Modification d'un rôle
- Suppression d'un rôle
- Affectation de privilèges à un rôle
- Affectation d'un rôle à un utilisateur
- Rôles prédéfinis
- Informations sur les rôles



## 5.3 Les rôles

---

### □ Généralités

- **Définition**

Un rôle est un concept Oracle qui permet de regrouper plusieurs privilèges et / ou rôles afin de les affecter ou retirer en bloc à un utilisateur et / ou un rôle.

- un rôle facilite la gestion des privilèges
- l'**affectation** d'un rôle à un utilisateur peut se faire sous Oracle ou **à travers l'OS**
- pour des raisons de sécurité, un **mot de passe** peut être assigné à un rôle
- Oracle fournit un certain nombre de **rôles par défaut** (connect, resource, dba, exp\_full\_database, imp\_full\_data\_base, select\_catalog\_role, delete\_catalog\_role / execute\_catalog\_role, ...)
- **pour créer un rôle**, il faut **avoir le privilège "CREATE ROLE"**

## 5.3 Les rôles

---

### □ Généralités

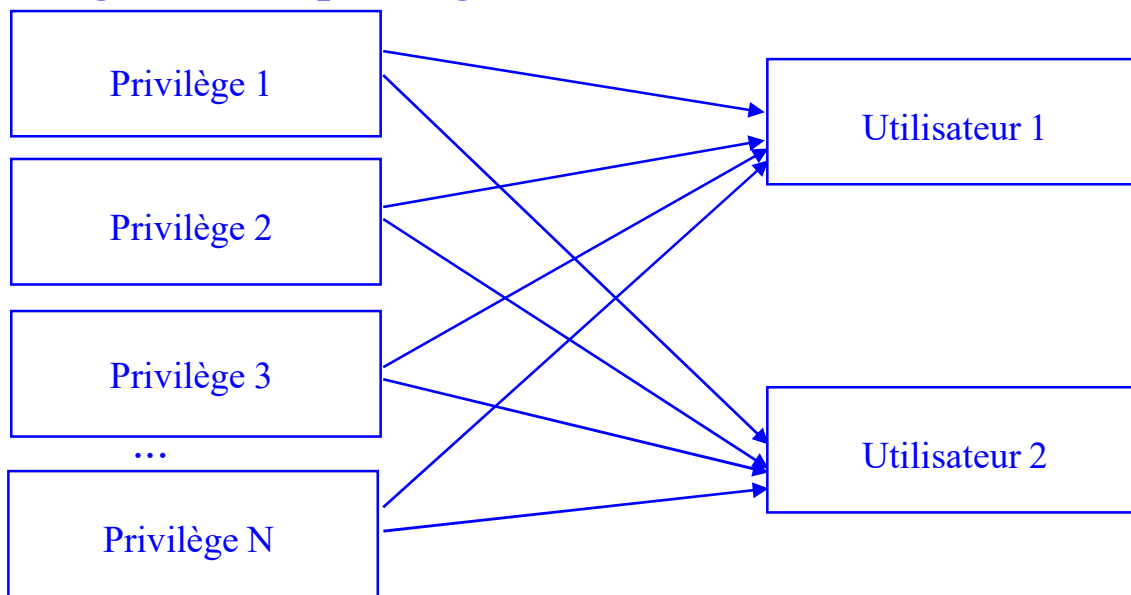
- **Nom de role**
  - **Au niveau de la cdb\$root**  
**Doit** commencer par le préfix affecté à  
COMMON\_USER\_PREFIX par défaut C## ou c##
  - **Au niveau d'une PDB**  
**NE DOIT PAS** commencer par le préfix affecté à  
COMMON\_USER\_PREFIX par défaut C## ou c##

## 5.3 Les rôles

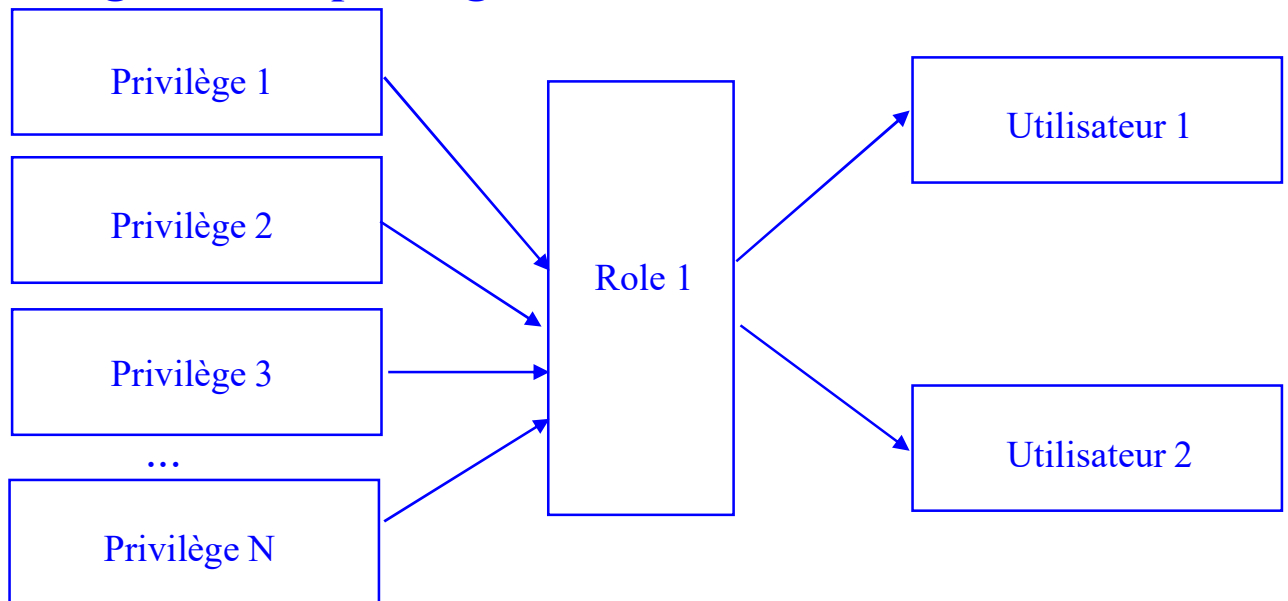
---

### □ Généralités (suite)

#### Assignation de privilèges aux utilisateurs : SANS ROLES



#### Assignation de privilèges aux utilisateurs : VIA UN ROLE



## 5.3 Les rôles

---

### □ Création d'un rôle

- A sa création, un rôle ne contient aucun privilège

#### Syntaxe

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

#### Mots clés et paramètres

|                |                                                      |
|----------------|------------------------------------------------------|
| role           | : nom du rôle à créer                                |
| NOT IDENTIFIED | : permet de créer un rôle sans mot de passe          |
| Password       | : mot de passe assigné au rôle                       |
| EXTERNALLY     | : mot de passe est contrôlé au niveau de l'OS        |
| GLOBALLY       | : Rôle autorisé au niveau de l'annuaire              |
| USING package  | : rôle applicatif                                    |
| CONTAINER      | Créer au rôle au niveau du container courant ou tous |

#### Exemple

```
sql> CREATE ROLE rl_etudiant ;
sql> CREATE ROLE rl_admin_backup;
sql> CREATE ROLE rl_admin_secu IDENTIFIED BY secu_pass ;
```

## 5.3 Les rôles

---

### □ Modification d'un rôle

- On peut modifier le *niveau de sécurité* d'un rôle
- privilège requis pour modifier un rôle ALTER ANY ROLE.

#### Syntaxe

```
ALTER ROLE role { NOT IDENTIFIED  
| IDENTIFIED { BY password | EXTERNALLY |  
Globally | USING package } } [CONTAINER={ALL | CURRENT}]
```

#### Mots clés et paramètres

|                |                                                   |
|----------------|---------------------------------------------------|
| role           | : nom du rôle à créer                             |
| NOT IDENTIFIED | : permet d'inhiber le mot de passe d'un rôle      |
| Password       | : nouveau mot de passe assigné au rôle            |
| EXTERNALLY     | : mot de passe contrôlé au niveau de l'OS         |
| GLOBALLY       | : Rôle autorisé au niveau de l'annuaire           |
| USING package  | : rôle applicatif                                 |
| CONTAINER      | : Modifier au niveau du container courant ou tous |

#### Exemple

```
sql> ALTER ROLE ROLE rl_etudiant IDENTIFIED EXTERNALLY ;  
sql> ALTER ROLE rl_admin_backup IDENTIFIED BY backup_pass;  
sql> ALTER ROLE rl_admin_secu NOT IDENTIFIED;
```

## 5.3 Les rôles

---

### □ Suppression d'un rôle

- Un rôle supprimé est retiré IMMEDIATEMENT du domaine de sécurité de l'utilisateur (connecté ou non) ou du rôle l'ayant reçu
- Le privilège DROP ANY ROLE et le fait d'avoir acquis un rôle avec WITH ADMIN OPTION permettent de le supprimer

- **Syntaxe**

DROP ROLE role ;

- **Exemple**

DROP ROLE rl\_admin\_secu ;

## 5.3 Les rôles

---

### □ Affectation de privilèges ou de rôles à un rôle

- Exemple

#### Création de deux rôles

# rôle rassemblant les privilèges pour se connecter  
CREATE ROLE rl\_connect ;

# rôle rassemblant les privilèges pour administrer la sécurité  
# ce rôle à un mot de passe.

CREATE ROLE rl\_admin\_secu **IDENTIFIED BY** pass;

#### Affectation des privilèges aux rôles

GRANT create session, alter session,  
Restricted session TO rl\_connect ;

GRANT create role, create user, create profile  
TO rl\_admin\_secu;

#### Affectation d'un Rôle à un autre Rôle

GRANT rl\_connect TO rl\_admin\_secu ;

## 5.3 Les rôles

---

### □ Affectation de privilèges à un rôle

- **Privilèges ne pouvant être affectés à un ROLE**

- **Privilège Système**

UNLIMITED TABLESPACE

Ce privilège inhibe tous les quotas et autorise l'utilisateur à créer des objets dans n'importe quel tablespace.

- **Privilèges Objets**

INDEX                    # droit de créer un index sur les tables d'autres utilisateurs

REFERENCES    # droit de référencer une table dans le schéma d'autres utilisateurs



## 5.3 Les rôles

---

### □ Affectation d'un rôle à un Utilisateur

- Elle peut se faire au niveau :
  - Oracle
  - du Système d'Exploitation (OS)
  - De l'annuaire de l'entreprise
- Affectation d'un Rôle au niveau Oracle

GRANT role to user [WITH ADMIN OPTION]

L'utilisateur ayant reçu le rôle avec WITH ADMIN OPTION peut le réaffecter, supprimer ou modifier.

```
sql> Grant role rl_admin_secu to scott;
```

## 5.3 Les rôles

---

### □ Affectation d'un rôle à un utilisateur (suite)

- Affectation d'un rôle au niveau de l'OS

- Positionner le paramètre OS\_ROLES dans init.ora afin que l'affectation et la révocation des rôles se fassent au niveau de l'OS

OS\_ROLES = TRUE

- Déclarer (sous UNIX) dans le fichier de groupe chaque rôle comme étant un groupe

#### *Syntaxe*

ora\_<SID>\_<role>[\_[D][A] : [user1, [user2], [ ...]]

#### *Avec*

|      |                     |
|------|---------------------|
| SID  | : nom de l'instance |
| role | : nom du rôle       |
| D    | : rôle par défaut   |
| A    | : WITH ADMIN OPTION |

#### *Exemple :*

- ora\_COURS\_rl\_connect\_D:scott, mopol, tintin
- ora\_COURS\_rl\_admin\_secu\_DA:mopol,osmani

## 5.3 Les rôles

---

### □ Affectation d'un rôle à un utilisateur (suite)

- **NOTES sur l'affectation d'un rôle à partir de l'OS**
  - L'affectation et la **révocation de rôles ne se fait plus qu'au niveau de l'OS**. Impossible d'utiliser l'ordre GRANT role TO user
  - un rôle affecté via l'OS **peut être activé ou désactivé par l'utilisateur** avec la commande ALTER USER ... SET ROLE ...;
  - les rôles **non gérés au niveau de l'OS ne peuvent être activés ou désactivés** même s'ils avaient été affectés lorsque OS\_ROLES était égal à FALSE
  - le paramètre MAX\_ENABLED\_ROLES limite le nombre de rôles pouvant être activés. ATTENTION paramètre **Déprécié**.
  - Si les rôles sont gérés par l'OS et on est en architecture Multithread, les connexions distantes exploitant ses rôles ne seront possibles que si le paramètre de init.ora REMOTE\_OS\_ROLE=TRUE

## 5.3 Les rôles

---

### □ Rôles prédéfinis

| NOM DU ROLE                   | PRIVILEGES AFFECTES AU ROLE                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------|
| <i>CONNECT*</i>               | CREATE SESSION                                                                                                   |
| <i>RESOURCE</i>               | CREATE CLUSTER, CREATE PROCEDURE,<br>CREATE SEQUENCE, CREATE TABLE,<br>CREATE TRIGGER                            |
| <i>DBA</i>                    | tous les privilèges (Voir manuel SQL Oracle) WITH<br>ADMIN OPTION                                                |
| <i>exp_full_database</i>      | SELECT ANY TABLE, BACKUP ANY TABLE,<br>INSERT, DELETE AND UPDATE ON tables<br>SYS.INCVID, SYS.INCFIL, SYS.INCEXP |
| <i>imp_full_database</i>      | BECOME USER, WRITEDOWN (trusted Oracle)                                                                          |
| <i>Execute_catalog_role</i>   | Privilège d'exécuter les procédures du dictionnaire                                                              |
| <i>Select_catalog_role</i>    | Privilège de consulter tout le dictionnaire Oracle                                                               |
| <i>Recovery_catalog_owner</i> | Fournit les privilèges pour le propriétaire du catalogue de<br>recouvrement                                      |
| <i>Aq_administrator_role</i>  | Fournit les privilèges pour l'administration des Queues                                                          |
| <i>PDB_DBA, cdb_dba</i>       | Fourni les privilège d'un admin de PDB ou de cdb                                                                 |
| ...                           |                                                                                                                  |

\* Dans des version antérieures CONNECT Possède d'autres privilèges

## 5.3 Les rôles

---

### □ Rôles prédéfinis

#### NOTES :

. Les rôles CONNECT, RESOURCE, DBA correspondent aux anciens privilèges systèmes sous Oracle V6 mais modifiés en version 10

. l'affectation des rôles **RESOURCE** et **DBA** à un utilisateur entraîne un GRANT *unlimited tablespace*

## 5.3 Les rôles

---

### □ Utilisation d'un rôle

#### 1) Les rôles affectés à un utilisateur sont actifs par défaut.

```
Grant role rl_connect to scott;
```

```
connect scott/tiger
```

Si ce rôle contient bien le privilège create session, scott sera connecté.

#### 2) Les rôles avec un mot de passe affectés à un utilisateur

```
Grant role rl_admin_secu to scott;
```

```
-- utilisation
```

```
Set role rl_admin_secu identified by pass;
```

```
-- Le rôle est dès lors disponible
```

```
Drop user jamel cascade;
```

```
-- désactivation du role
```

```
Set role all except rl_admin;
```

#### 3) Définir un rôle comme étant un rôle par défaut

```
Alter user scott default role all except rl_connect;
```

#### 3) Désactivation de tous les rôles

```
SET ROLE NONE;
```

## 5.3 Les rôles

---

### □ Informations sur les rôles

- Les vues suivantes contiennent des informations sur les rôles :

```
SELECT TABLE_NAME  
FROM DICT WHERE table_name like '%ROLE%'  
order by table_name;
```

```
TABLE_NAME  
-----  
ALL_CODE_ROLE_PRIVS  
CDB_APPLICATION_ROLES  
CDB_CHECKED_ROLES  
CDB_CHECKED_ROLES_PATH  
CDB_CODE_ROLE_PRIVS  
CDB_CONNECT_ROLE_GRANTEES  
CDB_ROLE_PRIVS  
CDB_ROLES  
CDB_SCHEDULER_JOB_ROLES  
CDB_XS_DYNAMIC_ROLES  
CDB_XS_PROXY_ROLES  
CDB_XS_ROLE_GRANTS  
CDB_XS_ROLES  
CDB_XS_SESSION_ROLES  
DBA_CHECKED_ROLES  
DBA_CHECKED_ROLES_PATH  
DBA_CODE_ROLE_PRIVS  
DBA_CONNECT_ROLE_GRANTEES  
DBA_ROLE_PRIVS  
DBA_ROLES  
DBA_SCHEDULER_JOB_ROLES  
DBA_XS_DYNAMIC_ROLES  
DBA_XS_PROXY_ROLES  
DBA_XS_ROLE_GRANTS  
DBA_XS_ROLES  
DBA_XS_SESSION_ROLES  
GV$XS_SESSION_ROLE  
GV$XS_SESSION_ROLES  
ROLE_ROLE_PRIVS  
ROLE_SYS_PRIVS  
ROLE_TAB_PRIVS  
SESSION_ROLES  
USER_CODE_ROLE_PRIVS  
USER_ROLE_PRIVS  
V$XS_SESSION_ROLES  
35 lignes sélectionnées.
```

## 5.3 Les rôles

---

### □ Informations sur les rôles

- **Exemple 1** : listing de tous les rôles de la base

```
sql> DESC sys.dba_roles ;
```

| Nom                 | NULL ?   | Type          |
|---------------------|----------|---------------|
| -----               | -----    | -----         |
| ROLE                | NOT NULL | VARCHAR2(128) |
| ROLE_ID             | NOT NULL | NUMBER        |
| PASSWORD_REQUIRED   |          | VARCHAR2(8)   |
| AUTHENTICATION_TYPE |          | VARCHAR2(11)  |
| COMMON              |          | VARCHAR2(3)   |
| ORACLE_MAINTAINED   |          | VARCHAR2(1)   |
| INHERITED           |          | VARCHAR2(3)   |
| IMPLICIT            |          | VARCHAR2(3)   |



## 5.3 Les rôles

### □ Informations sur les rôles

- **Exemple 1** : listing de tous les rôles de la base

Col role format a30

```
SELECT * FROM sys.dba_roles order by role;
```

| ROLE                       | ROLE_ID    | PASSWORD | AUTHENTICAT | COM | O | INH | IMP |
|----------------------------|------------|----------|-------------|-----|---|-----|-----|
| ADM_PARALLEL_EXECUTE_TASK  | 28         | NO       | NONE        | YES | Y | NO  | NO  |
| APPLICATION_TRACE_VIEWER   | 17         | NO       | NONE        | YES | Y | NO  | NO  |
| AQ_ADMINISTRATOR_ROLE      | 24         | NO       | NONE        | YES | Y | NO  | NO  |
| AQ_USER_ROLE               | 25         | NO       | NONE        | YES | Y | NO  | NO  |
| AUDIT_ADMIN                | 6          | NO       | NONE        | YES | Y | NO  | NO  |
| AUDIT_VIEWER               | 7          | NO       | NONE        | YES | Y | NO  | NO  |
| AUTHENTICATEDUSER          | 66         | NO       | NONE        | YES | Y | NO  | NO  |
| CAPTURE_ADMIN              | 12         | NO       | NONE        | YES | Y | NO  | NO  |
| CDB_DBA                    | 16         | NO       | NONE        | YES | Y | NO  | NO  |
| CONNECT                    | 2          | NO       | NONE        | YES | Y | NO  | NO  |
| C##RL_COURS_ADMIN          | 115        | NO       | NONE        | YES | N | NO  | NO  |
| C##RL_COURS_SQL            | 114        | NO       | NONE        | YES | N | NO  | NO  |
| CSW_USR_ROLE               | 99         | NO       | NONE        | YES | Y | NO  | NO  |
| CTXAPP                     | 85         | NO       | NONE        | YES | Y | NO  | NO  |
| DATAPATCH_ROLE             | 71         | NO       | NONE        | YES | Y | NO  | NO  |
| DATAPUMP_EXP_FULL_DATABASE | 26         | NO       | NONE        | YES | Y | NO  | NO  |
| DATAPUMP_IMP_FULL_DATABASE | 27         | NO       | NONE        | YES | Y | NO  | NO  |
| DBA                        | 4          | NO       | NONE        | YES | Y | NO  | NO  |
| DBFS_ROLE                  | 19         | NO       | NONE        | YES | Y | NO  | NO  |
| DBJAVASCRIPT               | 80         | NO       | NONE        | YES | Y | NO  | NO  |
| DBMS_MDX_INTERNAL          | 38         | NO       | NONE        | YES | Y | NO  | NO  |
| DV_ACCTMGR                 | 1279991    | NO       | NONE        | YES | Y | NO  | NO  |
| DV_ADMIN                   | 1279993    | NO       | NONE        | YES | Y | NO  | NO  |
| DV_AUDIT_CLEANUP           | 2147483633 | NO       | NONE        | YES | Y | NO  | NO  |
| DV_DATAPUMP_NETWORK_LINK   | 2147483634 | NO       | NONE        | YES | Y | NO  | NO  |
| DV_GOLDENGATE_ADMIN        | 2147483630 | NO       | NONE        | YES | Y | NO  | NO  |
| DV_GOLDENGATE_REDO_ACCESS  | 2147483632 | NO       | NONE        | YES | Y | NO  | NO  |
| DV_MONITOR                 | 2147483628 | NO       | NONE        | YES | Y | NO  | NO  |

• • •

## 5.3 Les rôles

---

### □ Informations sur les rôles (suite)

- **Exemple 2** : liste des rôles affectés à un rôle ou un utilisateur.

```
sql> SELECT * FROM sys.dba_role_privs  
WHERE grantee = 'RL_ADMIN_SECU' ;
```

| <u>GRANTEE</u> | <u>GRANTED_ROLE</u> | <u>ADM DEF</u> | <u>Default</u> |
|----------------|---------------------|----------------|----------------|
| RL_ADMIN_SECU  | RL_CONNECT          | NO             | YES            |

- **Exemple 3** : liste des rôles actifs pour la session

```
sql> SELECT * FROM session_roles ;
```

```
ROLE  
-----  
DBA  
SELECT_CATALOG_ROLE  
EXECUTE_CATALOG_ROLE  
CAPTURE_ADMIN  
EXP_FULL_DATABASE  
IMP_FULL_DATABASE  
AQ_ADMINISTRATOR_ROLE  
DATAPUMP_EXP_FULL_DATABASE  
DATAPUMP_IMP_FULL_DATABASE  
GATHER_SYSTEM_STATISTICS  
OPTIMIZER_PROCESSING_RATE  
EM_EXPRESS_BASIC  
EM_EXPRESS_ALL  
SCHEDULER_ADMIN  
HS_ADMIN_SELECT_ROLE  
HS_ADMIN_EXECUTE_ROLE  
XDBADMIN  
XDB_SET_INVOKER  
WM_ADMIN_ROLE  
JAVA_ADMIN  
JAVA_DEPLOY  
OLAP_XS_ADMIN  
OLAP_DBA  
  
23 lignes sélectionnées.
```

## 5.3 Les rôles



### □ Informations sur les rôles via Enterprise Manager Express (EM Express)

← → ↻ ⚠ Non sécurisé | [https://localhost:5500/em/shell#/security/show\\_roles](https://localhost:5500/em/shell#/security/show_roles)

**ORACLE** Enterprise Manager Database Express 12c

DBTEST12 (12.2.0.1.0) Configuration ⌵ Stockage ⌵ Sécurité ⌵ Performances ⌵

#### Rôles communs ⓘ

Actions ⌵  Créer un rôle  Supprimer le rôle

| Nom de rôle ▲              | Authentification |
|----------------------------|------------------|
| ADM_PARALLEL_EXECUTE_TASK  | NONE             |
| APPLICATION_TRACE_VIEWER   | NONE             |
| AQ_ADMINISTRATOR_ROLE      | NONE             |
| AQ_USER_ROLE               | NONE             |
| AUDIT_ADMIN                | NONE             |
| AUDIT_VIEWER               | NONE             |
| AUTHENTICATEDUSER          | NONE             |
| C##RL_COURS_ADMIN          | NONE             |
| C##RL_COURS_SQL            | NONE             |
| CAPTURE_ADMIN              | NONE             |
| CDB_DBA                    | NONE             |
| CONNECT                    | NONE             |
| CSW_USR_ROLE               | NONE             |
| CTXAPP                     | NONE             |
| DATAPATCH_ROLE             | NONE             |
| DATAPUMP_EXP_FULL_DATABASE | NONE             |
| DATAPUMP_IMP_FULL_DATABASE | NONE             |
| DBA                        | NONE             |
| DBFS_ROLE                  | NONE             |
| DBJAVASCRIPT               | NONE             |

## 5.3 Les rôles

### □ Informations sur les rôles via Enterprise Manager Express (EM Express)

- Droits affectés au rôle datapump\_exp\_full\_database

DBTEST12 (12.2.0.1.0) Configuration Stockage Sécurité Performances

Visualiser le rôle : DATAPUMP\_EXP\_FULL\_DATABASE Page régénérée 10:14

Récapitulatif du compte

Nom de rôle DATAPUMP\_EXP\_FULL\_DATABASE  
Authentification NONE  
Commun Oui

Détails

Rôles & privilèges communs

Rôles & privilèges communs ⓘ

Modifier Révoquer Nom

| Privilège         | WITH ADMIN | Est un rôle | Rôle par défaut |
|-------------------|------------|-------------|-----------------|
| CREATE SESSION    |            |             |                 |
| CREATE TABLE      |            |             |                 |
| EXP_FULL_DATABASE |            | ✓           | ✓               |
|                   |            |             |                 |
|                   |            |             |                 |

## 5.4 Les profils

---

### □ Généralités

- Un **profil** est un concept Oracle qui **permet** à l'administrateur d'une base **de contrôler la consommation des ressources systèmes et des mots de passes**
- Il existe un profil par défaut appelé **DEFAULT**. Il est par défaut affecté à un utilisateur lors de sa création
- Les limites du profil DEFAULT sont positionnées à UNLIMITED
- Le profil DEFAULT ne peut être supprimé. *Les limites de ce profil peuvent par contre être modifiées*
- Le nom d'un profil créé au niveau **CDB\$ROOT** doit être précédé de la valeur du paramètre **common\_user\_prefix** qui est par défaut **C##** ou **c##**

## 5.4 Les profils

---

### □ Généralités

- **Activation et contrôle des limites :**
  - dans le fichier `initSID.ora` positionner :  
`RESOURCE_LIMIT = TRUE`
  - ou dynamiquement faire sous `sqlplus` par exemple :  
`SQL> ALTER SYSTEM SET resource_limit = true;`
  - **Attention !!!** : `TRUE` est maintenant la valeur par défaut à partir d'Oracle 12c
- **NOTE : Oracle recommande d'utiliser pour une gestion fine des ressources le « Database resource manager ». Pas traité dans ce cours**

## 5.4 Les profils

---

### □ Création d'un profil

- Privilège requis CREATE profil

#### Syntaxe partie limite des ressources

```
CREATE PROFILE profile LIMIT
[ SESSIONS_PER_USER { integer | UNLIMITED | DEFAULT } ]
[ CPU_PER_SESSION { integer | UNLIMITED | DEFAULT } ]
[ CPU_PER_CALL { integer | UNLIMITED | DEFAULT } ]
[ CONNECT_TIME { integer | UNLIMITED | DEFAULT } ]
[ IDLE_TIME { integer | UNLIMITED | DEFAULT } ]
[ LOGICAL_READS_PER_SESSION {integer | UNLIMITED|DEFAULT}]
[ LOGICAL_READS_PER_CALL {integer | UNLIMITED|DEFAULT}]
[ COMPOSITE_LIMIT { integer | UNLIMITED | DEFAULT } ]
[ PRIVATE_SGA {integer [K | M] | UNLIMITED | DEFAULT}]
[ CONTAINER={ALL | CURRENT}]
```

#### Mots clés et paramètres

**Session\_per\_user** : Nombre maximum de sessions par utilisateur

**Logical\_read\_per\_session**

: Nbre de blocs de données à lire pour une session

**cpu\_per\_session** : temps CPU max par session en % de secondes

**cpu\_per\_call** : temps CPU pour un appel (en cas de parse,  
execute ou fetch) en % de secondes

**connect\_time** : temps écoulé maximum (en minutes)

**idle\_time** : temps maximum d'inactivité.(en minutes)

**private\_sga** : taille privée de la SGA allouée à un utilisateur

**unlimited** : limite de la ressource illimitée

**default** : prend la limite par défaut de la ressource

## 5.4 Les profils

---

### □ Création d'un profil

- Privilège requis CREATE profil

#### Syntaxe partie password

```
CREATE PROFILE profile LIMIT
[FAILED_LOGIN_ATTEMPTS {expr | UNLIMITED | DEFAULT}]
[PASSWORD_LIFE_TIME {expr | UNLIMITED | DEFAULT}]
[PASSWORD_REUSE_TIME {expr | UNLIMITED | DEFAULT}]
[PASSWORD_REUSE_MAX {expr | UNLIMITED | DEFAULT}]
[PASSWORD_LOCK_TIME {expr | UNLIMITED | DEFAULT}]
[PASSWORD_GRACE_TIME {expr | UNLIMITED | DEFAULT}]
[PASSWORD_VERIFY_FUNCTION {function, NULL, DEFAULT}]
[CONTAINER={ALL | CURRENT}]
```

#### Mots clés et paramètres

##### **Failed\_login\_attempts**

: nombre d'échecs avant le blocage du compte

##### **password\_life\_time**

: durée en jours avant l'expiration du mot de passe

##### **password\_reuse\_time**

: durée en jours avant la réutilisation d'un password

##### **password\_reuse\_max**

: nombre de modif du password avant réutilisation

##### **password\_lock\_time**

: durée en jours du verrouillage d'un compte

##### **password\_grace\_time**

: délai de tolérance du password avant son expiration

##### **password\_verify\_function**

: fonction de contrôle des mots de passes



## 5.4 Les profils

---

### □ Création d'un profil

- Exemple au niveau PDB

#### Exemple 1

```
CREATE PROFILE pf_secretaire LIMIT
sessions_per_user          2
cpu_per_session            unlimited
cpu_per_call               1000
logical_reads_per_session  unlimited
logical_reads_per_call     100
idle_time                  30
connect_time               480 ;
```

#### Exemple 2

```
CREATE PROFILE pf_agent LIMIT
sessions_per_user          2
cpu_per_session            unlimited
cpu_per_call               1000
composite_limit            20000
private_sga                32K ;
```

#### Exemple 3

```
CREATE PROFILE pf_admin
PASSWORD_LIFE_TIME 200
LIMIT PASSWORD_REUSE_MAX DEFAULT
PASSWORD_REUSE_TIME UNLIMITED
CPU_PER_SESSION UNLIMITED
```

## 5.4 Les profils

---

### □ Création d'un profil

- Exemple au niveau CDB

#### Exemple 1

```
CREATE PROFILE c##pf_secretaire LIMIT
sessions_per_user      2
cpu_per_session        unlimited
cpu_per_call           1000
logical_reads_per_session unlimited
logical_reads_per_call 100
idle_time              30
connect_time           480 ;
```

## 5.4 Les profils

---

### □ Assignation d'un profil à un utilisateur

- A la création d'un nouvel utilisateur

```
CREATE USER rackham IDENTIFIED BY lerouge  
PROFILE pf_secretaire ;
```

- A la modification d'un utilisateur

```
ALTER USER rackham  
PROFILE pf_agent ;
```

## 5.4 Les profils

---

### □ Modification d'un profil

- Privilège requis : ALTER profil

#### Syntaxe partie limite des ressources

```
ALTER PROFILE profile LIMIT
[ SESSIONS_PER_USER { integer | UNLIMITED | DEFAULT } ]
[ CPU_PER_SESSION { integer | UNLIMITED | DEFAULT } ]
[ CPU_PER_CALL { integer | UNLIMITED | DEFAULT } ]
[ CONNECT_TIME { integer | UNLIMITED | DEFAULT } ]
[ IDLE_TIME { integer | UNLIMITED | DEFAULT } ]
[ LOGICAL_READS_PER_SESSION {integer | UNLIMITED|DEFAULT}]
[ LOGICAL_READS_PER_CALL {integer | UNLIMITED|DEFAULT}]
[ COMPOSITE_LIMIT { integer | UNLIMITED | DEFAULT } ]
[ PRIVATE_SGA {integer [K | M] | UNLIMITED | DEFAULT}]
[CONTAINER={ALL | CURRENT}]
```

#### Mots clés et paramètres

|                                 |                                                                                |
|---------------------------------|--------------------------------------------------------------------------------|
| <b>Session_per_user</b>         | : Nombre maximum de sessions par utilisateurs                                  |
| <b>Logical_read_per_session</b> | : blocs de données en lecture par session                                      |
| <b>cpu_per_session</b>          | : temps CPU max par session en % de secondes                                   |
| <b>cpu_per_call</b>             | : temps CPU pour un appel (en acs de parse, execute ou fetch) en % de secondes |
| <b>connect_time</b>             | : temps écoulé maximum (en minutes)                                            |
| <b>idle_time</b>                | : temps maximum d'inactivité.                                                  |
| <b>private_sga</b>              | : taille privée de SGA allouée à un utilisateur                                |
| <b>unlimited</b>                | : limite de la ressource illimitée                                             |
| <b>default</b>                  | : positionne la limite par défaut de la ressource                              |

## 5.4 Les profils

---

### □ Modification d'un profil

- Privilège requis : ALTER profil

#### Syntaxe partie password

```
ALTER PROFILE profil LIMIT
[FAILED_LOGIN_ATTEMPTS {expr | UNLIMITED | DEFAULT}]
[PASSWORD_LIFE_TIME {expr | UNLIMITED | DEFAULT}]
[PASSWORD_REUSE_TIME {expr | UNLIMITED | DEFAULT}]
[PASSWORD_REUSE_MAX {expr | UNLIMITED | DEFAULT}]
[PASSWORD_LOCK_TIME {expr | UNLIMITED | DEFAULT}]
[PASSWORD_GRACE_TIME {expr | UNLIMITED | DEFAULT}]
[PASSWORD_VERIFY_FUNCTION {function, NULL, DEFAULT}]
[CONTAINER={ALL | CURRENT}]
```

#### Mots clés et paramètres

##### **Failed\_login\_attempts**

: nombre d'échecs avant le blocage du compte

##### **password\_life\_time**

: durée en jours avant l'expiration du mot de passe

##### **password\_reuse\_time**

: durée en jours avant la réutilisation d'un password

##### **password\_reuse\_max**

: nombre de modif du password avant réutilisation

##### **password\_lock\_time**

: durée en jours du verrouillage d'un compte

##### **password\_grace\_time**

: délai de tolérance du password avant son expiration

##### **password\_verify\_function**

: fonction de contrôle des mots de passes

## 5.4 Les profils

---

### □ Modification d'un profil

#### Exemple 1 :

Modification des limites du profil par défaut  
DEFAULT

```
ALTER PROFILE default LIMIT  
CPU_PER_SESSION 600
```

#### Exemple 2 :

Modification des limites du profil *pf\_agent*

```
ALTER PROFILE pf_agent LIMIT  
CPU_PER_SESSION default
```

Que vaut CPU\_PER\_SESSION pour le profil *pf\_agent* ?

## 5.4 Les profils

---

### □ Utilisations des limites composites

- Généralités
  - Fixe le **coût total des limites** pour une session
  - **à chaque limite est associé un poids :**
    - par défaut les poids sont à 0
    - un fort poids implique un coût élevé de la limite
    - un poids ne peut être qu'associer aux limites suivantes (cpu\_per\_session, connect\_time, logical\_reads\_per\_session, private\_sga)
  - **privilege requis : ALTER RESOURCE COST**

## 5.4 Les profils

---

### □ Création de limites composites

#### Syntaxe

```
ALTER RESOURCE COST  
    [ CPU_PER_SESSION    integer ]  
    [ CONNECT_TIME       integer ]  
    [ LOGICAL_READS_PER_SESSION integer]  
    [ PRIVATE_SGA integer ]
```

#### Mots clés et paramètres

**integer** : poids pour chaque ressource  
**Logical\_read\_per\_session** : blocs de données en lecture par session  
**cpu\_per\_session** : temps CPU max par session en % de secondes  
**connect\_time** : temps écoulé maximum (en minutes)  
**private\_sga** : taille de la SGA privé à ne pas dépasser

La limite PRIVATE\_SGA est - t - elle toujours valide quel que soit l'architecture d'Oracle ?



## 5.4 Les profils

---

### □ Création d'une limite composite (suite)

**Formule d'évaluation du coût total des ressources pour une session.**

$$T = \sum \text{poids} * \text{consommation\_per\_resource\_limit}$$

**Exemple 1 :**

```
SQL> ALTER RESOURCE COST
      cpu_per_session      100
      connect_time         1;
```

$$T = 100 * \text{cpu\_per\_session\_consommé} + 1 * \text{connect\_time\_consommé} + 0 * \text{logical\_reads\_per\_session} + 0 * \text{private\_sga}$$

**Exemple 2 :**

```
SQL> ALTER RESOURCE COST
      logical_reads_per_session  2
      connect_time               0;
```

$$T = 100 * \text{cpu\_per\_session\_consommé} + 0 * \text{connect\_time\_consommé} + 2 * \text{logical\_reads\_per\_session} + 0 * \text{private\_sga}$$

**Note :**

Le résultat **T** est à comparer avec la valeur de **COMPOSITE\_LIMIT**

## 5.4 Les profils

---

### □ Suppression d'un profil

- En cas de suppression d'un profil existant affecté à un utilisateur, ce dernier se verra automatiquement attribué le profil DEFAULT
- Le profil DEFAULT ne peut être supprimé
- Privilège requis : DROP profile

#### Syntaxe

DROP PROFILE nom\_profil [CASCADE]

#### Mots clés et paramètres

|                   |                                                                         |
|-------------------|-------------------------------------------------------------------------|
| <b>nom_profil</b> | : nom du profil à supprimer                                             |
| <b>CASCADE</b>    | : retire le profil aux utilisateurs l'ayant puis, suppression du profil |

#### Exemple

```
sql>DROP PROFILE pf_secretaire CASCADE ;
```

## 5.4 Les profils

### □ Visualisation des informations des profils

- Vues contenant les informations sur les profils :
  - dba\_profiles, resource\_cost, user\_resource\_limit

#### Exemple 1 : Liste de tous les profils

```
sql> SELECT profile, resource_name, limit FROM dba_profiles  
ORDER BY profil, resource_name;
```

| PROFILE          | RESOURCE_NAME             | LIMIT                       |
|------------------|---------------------------|-----------------------------|
| C##PF_SECRETAIRE | COMPOSITE_LIMIT           | DEFAULT                     |
| C##PF_SECRETAIRE | CONNECT_TIME              | 480                         |
| C##PF_SECRETAIRE | CPU_PER_CALL              | 1000                        |
| C##PF_SECRETAIRE | CPU_PER_SESSION           | UNLIMITED                   |
| C##PF_SECRETAIRE | FAILED_LOGIN_ATTEMPTS     | DEFAULT                     |
| C##PF_SECRETAIRE | IDLE_TIME                 | 30                          |
| C##PF_SECRETAIRE | INACTIVE_ACCOUNT_TIME     | DEFAULT                     |
| C##PF_SECRETAIRE | LOGICAL_READS_PER_CALL    | 100                         |
| C##PF_SECRETAIRE | LOGICAL_READS_PER_SESSION | UNLIMITED                   |
| C##PF_SECRETAIRE | PASSWORD_GRACE_TIME       | DEFAULT                     |
| C##PF_SECRETAIRE | PASSWORD_LIFE_TIME        | DEFAULT                     |
| C##PF_SECRETAIRE | PASSWORD_LOCK_TIME        | DEFAULT                     |
| C##PF_SECRETAIRE | PASSWORD_REUSE_MAX        | DEFAULT                     |
| C##PF_SECRETAIRE | PASSWORD_REUSE_TIME       | DEFAULT                     |
| C##PF_SECRETAIRE | PASSWORD_VERIFY_FUNCTION  | DEFAULT                     |
| C##PF_SECRETAIRE | PRIVATE_SGA               | DEFAULT                     |
| C##PF_SECRETAIRE | SESSIONS_PER_USER         | 2                           |
| DEFAULT          | COMPOSITE_LIMIT           | UNLIMITED                   |
| DEFAULT          | CONNECT_TIME              | UNLIMITED                   |
| DEFAULT          | CPU_PER_CALL              | UNLIMITED                   |
| DEFAULT          | CPU_PER_SESSION           | UNLIMITED                   |
| DEFAULT          | FAILED_LOGIN_ATTEMPTS     | 10                          |
| DEFAULT          | IDLE_TIME                 | UNLIMITED                   |
| DEFAULT          | INACTIVE_ACCOUNT_TIME     | UNLIMITED                   |
| DEFAULT          | LOGICAL_READS_PER_CALL    | UNLIMITED                   |
| DEFAULT          | LOGICAL_READS_PER_SESSION | UNLIMITED                   |
| DEFAULT          | PASSWORD_GRACE_TIME       | 7                           |
| DEFAULT          | PASSWORD_LIFE_TIME        | 180                         |
| DEFAULT          | PASSWORD_LOCK_TIME        | 1                           |
| DEFAULT          | PASSWORD_REUSE_MAX        | UNLIMITED                   |
| DEFAULT          | PASSWORD_REUSE_TIME       | UNLIMITED                   |
| DEFAULT          | PASSWORD_VERIFY_FUNCTION  | NULL                        |
| DEFAULT          | PRIVATE_SGA               | UNLIMITED                   |
| DEFAULT          | SESSIONS_PER_USER         | UNLIMITED                   |
| ORA_STIG_PROFILE | COMPOSITE_LIMIT           | DEFAULT                     |
| ORA_STIG_PROFILE | CONNECT_TIME              | DEFAULT                     |
| ORA_STIG_PROFILE | CPU_PER_CALL              | DEFAULT                     |
| ORA_STIG_PROFILE | CPU_PER_SESSION           | DEFAULT                     |
| ORA_STIG_PROFILE | FAILED_LOGIN_ATTEMPTS     | 3                           |
| ORA_STIG_PROFILE | IDLE_TIME                 | 15                          |
| ORA_STIG_PROFILE | INACTIVE_ACCOUNT_TIME     | 35                          |
| ORA_STIG_PROFILE | LOGICAL_READS_PER_CALL    | DEFAULT                     |
| ORA_STIG_PROFILE | LOGICAL_READS_PER_SESSION | DEFAULT                     |
| ORA_STIG_PROFILE | PASSWORD_GRACE_TIME       | 5                           |
| ORA_STIG_PROFILE | PASSWORD_LIFE_TIME        | 60                          |
| ORA_STIG_PROFILE | PASSWORD_LOCK_TIME        | UNLIMITED                   |
| ORA_STIG_PROFILE | PASSWORD_REUSE_MAX        | 10                          |
| ORA_STIG_PROFILE | PASSWORD_REUSE_TIME       | 365                         |
| ORA_STIG_PROFILE | PASSWORD_VERIFY_FUNCTION  | ORA12C_STIG_VERIFY_FUNCTION |
| ORA_STIG_PROFILE | PRIVATE_SGA               | DEFAULT                     |
| ORA_STIG_PROFILE | SESSIONS_PER_USER         | DEFAULT                     |

51 lignes sélectionnées.

## 5.4 Les profils

---

### □ Visualisation des informations des profils

**Exemple 2 :** Liste des coûts (poids) des ressources pour la session courante

```
sql> SELECT resource_name, limit FROM resource_cost
```

| <u>RESOURCE_NAME</u>      | <u>UNIT_COST</u> |
|---------------------------|------------------|
| CPU_PER_SESSION           | 100              |
| LOGICAL_READS_PER_SESSION | 2                |
| CONNECT_TIME              | 0                |
| PRIVATE_SGA               | 0                |

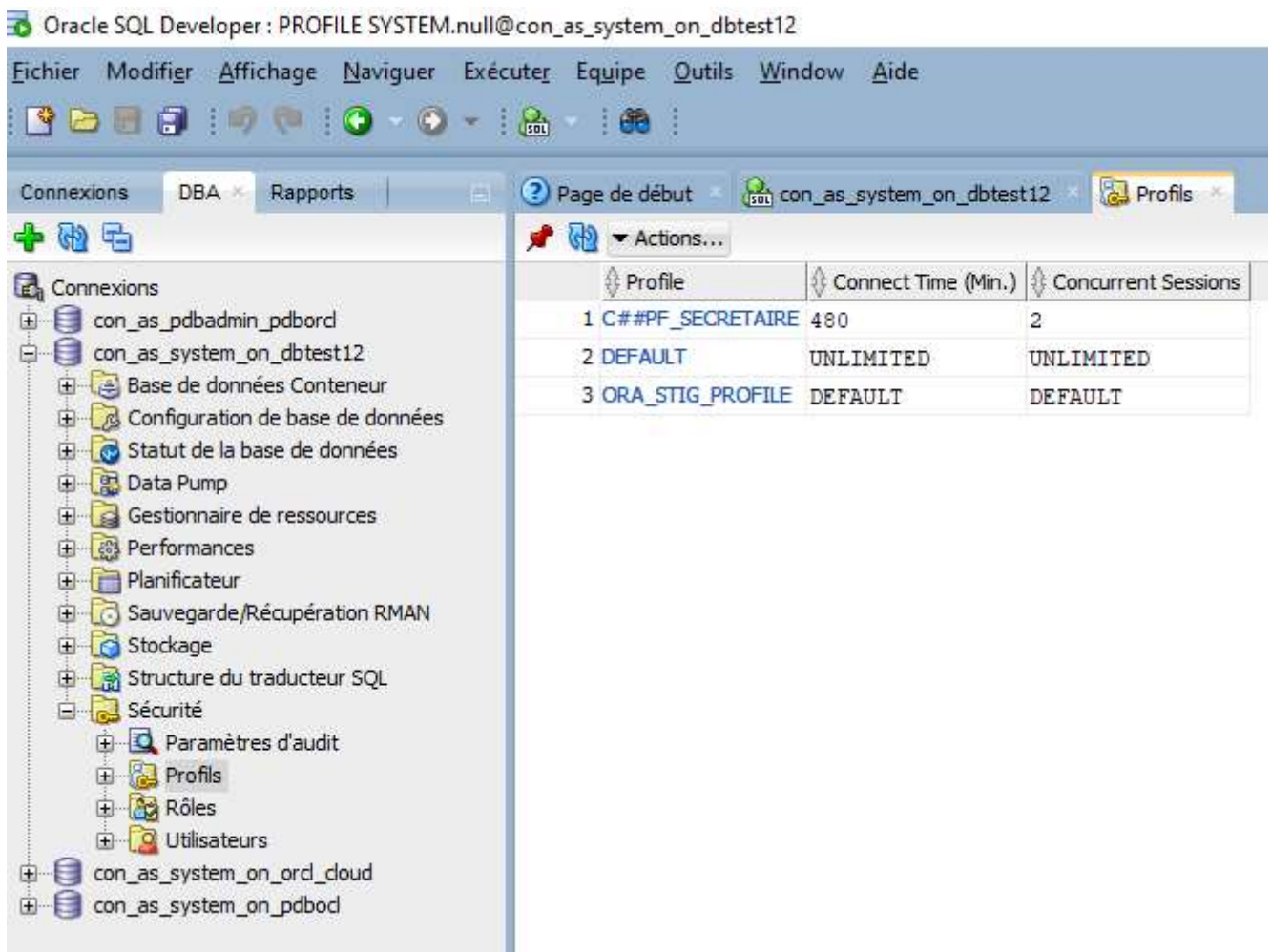
**Exemple 3 :** Liste des limites des ressources de l'utilisateur courant

```
sql> SELECT resource_name, limit FROM user_resource_limits
```

| <u>RESOURCE_NAME</u>      | <u>LIMIT</u> |
|---------------------------|--------------|
| COMPOSITE_LIMIT           | UNLIMITED    |
| SESSIONS_PER_USER         | UNLIMITED    |
| CPU_PER_SESSION           | 600          |
| CPU_PER_CALL              | UNLIMITED    |
| LOGICAL_READS_PER_SESSION | UNLIMITED    |
| LOGICAL_READS_PER_CALL    | UNLIMITED    |
| IDLE_TIME                 | UNLIMITED    |
| CONNECT_TIME              | UNLIMITED    |
| PRIVATE_SGA               | UNLIMITED    |

## 5.4 Les profils

### □ Visualisation des informations sur les profils VIA SQL DEVELOPER onglet DBA



Oracle SQL Developer : PROFILE SYSTEM.null@con\_as\_system\_on\_dbtest12

Fichier Modifier Affichage Naviguer Exécuter Equipe Outils Window Aide

Connexions DBA Rapports Page de début con\_as\_system\_on\_dbtest12 Profils

Connaissances

- con\_as\_pdbadmin\_pdbord
- con\_as\_system\_on\_dbtest12
  - Base de données Conteneur
  - Configuration de base de données
  - Statut de la base de données
  - Data Pump
  - Gestionnaire de ressources
  - Performances
  - Planificateur
  - Sauvegarde/Récupération RMAN
  - Stockage
  - Structure du traducteur SQL
  - Sécurité
    - Paramètres d'audit
    - Profils
    - Rôles
    - Utilisateurs
- con\_as\_system\_on\_ord\_cloud
- con\_as\_system\_on\_pdbod

Actions...

| Profile            | Connect Time (Min.) | Concurrent Sessions |
|--------------------|---------------------|---------------------|
| 1 C##PF_SECRETAIRE | 480                 | 2                   |
| 2 DEFAULT          | UNLIMITED           | UNLIMITED           |
| 3 ORA_STIG_PROFILE | DEFAULT             | DEFAULT             |

## 5.4 Les profils

### □ Visualisation des informations sur les profils VIA SQL DEVELOPER onglet DBA

Oracle SQL Developer : PROFILE SYSTEM.DEFAULT@con\_as\_system\_on\_dbtest12

Fichier Modifier Affichage Naviguer Exécuter Equipe Outils Window Aide

Connexions DBA Rapports

Page de début con\_as\_system\_on\_dbtest12 DEFAULT

Généralités Services de base de données Mot de passe SQL

Actions...

| Profile   | CPU/Session (Sec./100) | CPU/Call (Sec./100) | Connect Time (Minutes) | Idle Time (Minutes) |
|-----------|------------------------|---------------------|------------------------|---------------------|
| 1 DEFAULT | UNLIMITED              | UNLIMITED           | UNLIMITED              | UNLIMITED           |

Connexions

- con\_as\_pdbadmin\_pdbord
- con\_as\_system\_on\_dbtest12
  - Base de données Conteneur
  - Configuration de base de données
  - Statut de la base de données
  - Data Pump
  - Gestionnaire de ressources
  - Performances
  - Planificateur
  - Sauvegarde/Récupération RMAN
  - Stockage
  - Structure du traducteur SQL
  - Sécurité
    - Paramètres d'audit
    - Profils
      - C##PF\_SECRETARE
      - DEFAULT
      - ORA\_STIG\_PROFILE
    - Rôles
    - Utilisateurs
- con\_as\_system\_on\_ord\_cloud
- con\_as\_system\_on\_pdbod

## 5.5 Les utilisateurs

---

### □ Généralités

- La notion d'utilisateur est fondamentale pour accéder aux données d'une base Oracle
- Le site d'un client Oracle doit être tenu à jour au niveau des licences :
  - Durée des licences
    - perpétuelle
    - ou limitée (1 à 5 ans)
  - Les différents types de licences
    - Licences par **Utilisateurs Nommés Plus (UNP)**
    - Licences par CPU
    - Licence cloud
  - Les éditions
    - Oracle Express Edition (gratuite, base limitée à 11 Go, 1 CPU disponible jusqu'à Oracle Express 11G)
    - Oracle Personal Edition
    - Oracle standard édition 2
    - Oracle Enterprise Edition
    - **Nota** : Les éditions se différencient par des fonctionnalités différentes et des capacités différentes



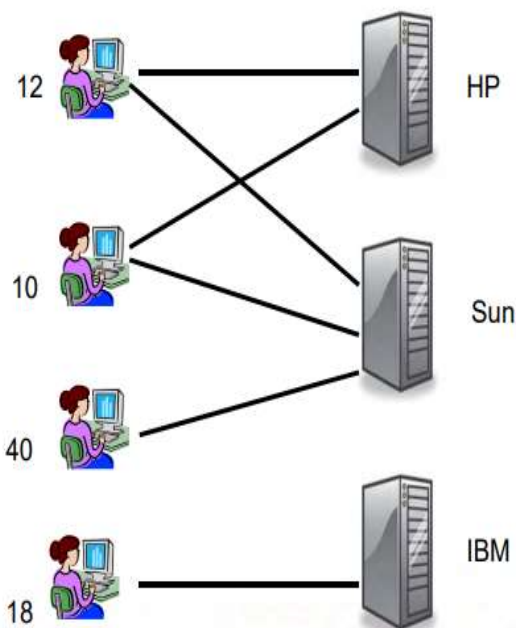
## 5.5 Les utilisateurs

---

### □ Généralités

- Licences par **Utilisateurs Nommés Plus (UNP)**

Personne physique identifiée, autorisée à utiliser le(s) logiciel(s) Oracle sur un ou plusieurs serveurs, indépendamment du fait qu'elle l'utilise ou non à un instant donné.



#### ❖ 80 Utilisateurs Nommés Plus

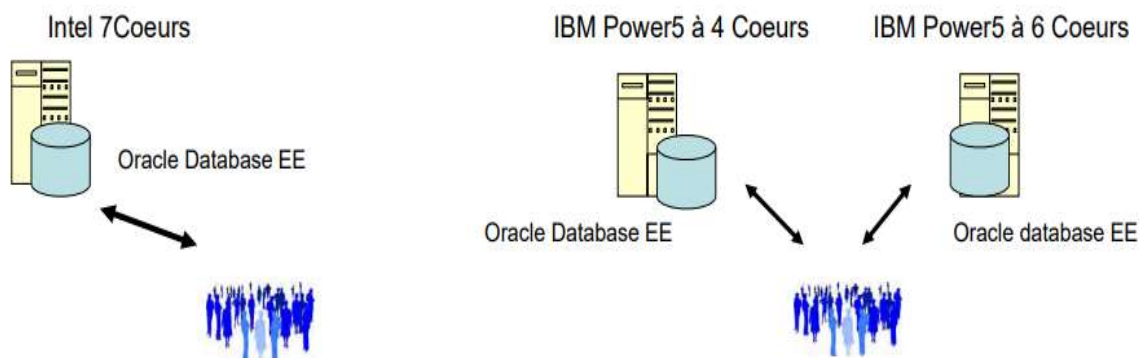
- Indépendants du constructeur
- Indépendants de l'OS
- Indépendant du nombre de serveur sauf pour le calcul des minima en Enterprise Edition
- Indépendants de la version du produit



## 5.5 Les utilisateurs

### □ Généralités

- Licences par CPU
  - Connexions illimitées !!!
  - Nombre CPU = Nb cœurs \* coefficients



Pour oracle EE installé sur un serveur Intel avec 7 cœurs :

$7 * 0,50 = 3,5$  arrondi au nombre entier supérieur soit 4.

**Besoin : 4 licences processeurs**

Pour Oracle EE sur 2 serveurs multi-cœurs IBM avec 10 cœurs :

$4 + 6 = 10 * 0,75 = 7,5$  arrondi au nombre entier supérieur soit 8.

**Besoin : 8 licences processeurs**

### Coefficients :

IBM power 6: 1,

IBM Power 5: 0,75

AMD /Inter 32bits, 64 bits : 0,5

Sun Ultra System T1 avec 4, 6 ou 8 cœurs : 0,25

## 5.5 Les utilisateurs

---

### □ Généralités

- Les tarifs dépendent de la durée de la licence, du type de licence et de l'édition. (Informations tirées en Mai 2019 site de vente en ligne

[https://shop.oracle.com/apex/f?p=DSTORE:2:::NO:RI R,RP,2:PROD\\_HIER\\_ID:4509881204651805720002\)](https://shop.oracle.com/apex/f?p=DSTORE:2:::NO:RI R,RP,2:PROD_HIER_ID:4509881204651805720002)

- **Exemple 1:** Oracle Enterprise Edition, Perpétuelle

- Par CPU : **41240** Euros. Maj logiciels
- Par utilisateur nommé plus (UNP): **825** Euros par UNP avec un minimum de 25 utilisateurs. Maj logiciels

- **Exemple 2:** Oracle standard Edition 2, Perpétuelle

- Par CPU : 15194 Euros
- Par utilisateur nommé : 304 Euros par UNP avec un minimum de 10 utilisateurs Nommés Plus (UNP)

## 5.5 Les utilisateurs

---

### □ Généralités

- Les tarifs dépendent de la durée de la licence, du type de licence et de l'édition. (Informations tirées en Mai 2019 site de vente en ligne)
  - **Exemple 3:** Oracle Personal Edition, Perpétuelle
    - 399 Euros par Utilisateur Nommé Plus
    - Pas de licence par CPU
    - Toujours perpétuelle
  - **Exemple 4 :** Oracle Enterprise Edition, durée limitée
    - Par CPU :
      - 1 an 8248 Euros
      - 2 ans 14434 Euros
      - 3 ans 20620 Euros
      - 4 ans 24744 Euros
      - 5 ans 28864 Euros
    - Par utilisateurs nommés plus(avec un minimum de 25) :
      - 1 an 26 Euros par UNP
      - 2 ans 46 Euros par UNP
      - 3 ans 65 Euros par UNP
      - 4 ans 78 Euros par UNP
      - 5 ans 91 Euros par UNP
  - **Note !!! :** Ajouter **environ 22% du prix de la licence** par an pour les mises à jour logiciels et le support.  
**Plusieurs options sont aussi payantes**

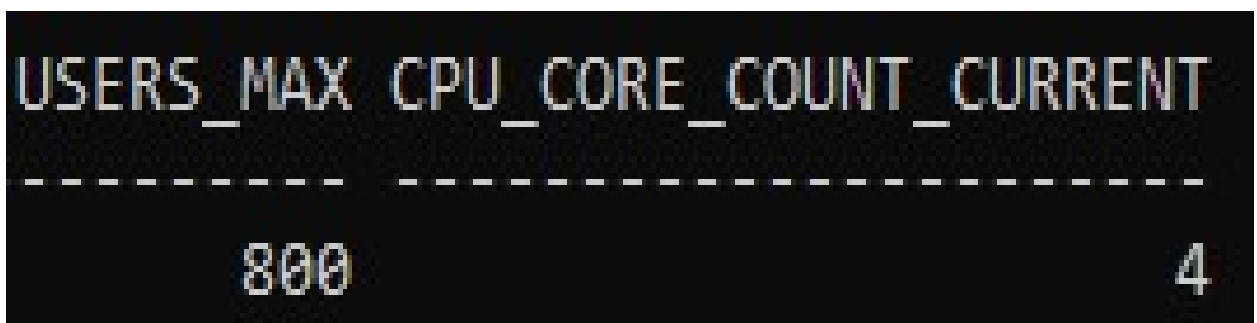
## 5.5 Les utilisateurs

---

### □ Généralités (suite)

- **Contrôle de la limitation du nombre d'utilisateurs en de licence Utilisateurs nommés**
  - Au moment du lancement d'une instance  
LICENSE\_MAX\_USERS = 80
  - Au moment ou l'instance tourne  
sqlplus >ALTER SYSTEM  
SET LICENSE\_MAX\_USERS=800;
- visualisation des limites des licences *v\$license*

*select users\_max, CPU\_CORE\_COUNT\_CURRENT  
from v\$license;*



| USERS_MAX | CPU_CORE_COUNT_CURRENT |
|-----------|------------------------|
| 800       | 4                      |

## 5.5 Les utilisateurs

---

### □ Généralités (suite)

- **Authentification des utilisateurs**

- A partir d'Oracle

`CREATE USER scott IDENTIFIED BY tiger ;`

- A partir de l'OS

`CREATE USER OPS$mopolo IDENTIFIED  
EXTERNALLY ;`

- Les utilisateurs authentifiés par l'OS sont précédés d'une chaîne définie par le paramètre de `initsid.ora`  
`OS_AUTHENT_PREFIX` qui vaut par défaut **OPS\$**

- Globalement à partir de l'annuaire LDAP

`CREATE USER scott  
IDENTIFIED GLOBALLY AS  
'CN=scott,OU=division1,O=oracle,C=US'`

## 5.5 Les utilisateurs

---

### □ Généralités (suite)

- **Utilisateur et schéma**
  - A chaque utilisateur est associé un schéma
  - Les objets appartenant à un schéma sont : tables, index, vues, séquences, synonymes, clusters, database links, fonction, procédures et package, ...
  - La **commande** *CREATE SCHEMA AUTHORIZATION* permet créer en un trait des *tables*, des *vues* et d'attribuer des *droits*. En cas d'erreur, un ROLLBACK peut être effectué. **Exemple :**

```
CREATE SCHEMA AUTHORIZATION ottocar
```

```
CREATE TABLE VOL (  
    vol#      number(4)  primary key,  
    plnum     number(4)  references pilote,  
    vd        char(12),  
    va        char(12))
```

```
CREATE TABLE PILOTE (  
    pl#       number(4)  primary key,  
    plnom     varchar2(20),  
    sal       number (5, 2)          not null)
```

```
GRANT select, update(plnom, sal) ON pilote TO tintin;
```

## 5.5 Les utilisateurs

---

### □ Création d'un utilisateur

- Lors de la création d'un utilisateur, il est possible de lui affecter : un mot de passe, un tablespace par défaut, un tablespace temporaire, un profil (explicite ou implicite), des quotas sur les tablespaces, etc.

#### Syntaxe

```
CREATE USER user
IDENTIFIED { BY password [[http] DIGEST {enable | disable}]
| EXTERNALLY [as ' {certificate dn | Kerberos principal name}']
| GLOBALLY [AS 'certificate DN' ]}
[DEFAULT COLLATION collation_name]
[ DEFAULT TABLESPACE tablespace ]
[ [LOCAL] TEMPORARY TABLESPACE {tablespace|
tablespaceGroup }
[ QUOTA { integer [ K | M ] | UNLIMITED } ON tablespace ] ...
[ PROFILE profile ]
[PASSWORD EXPIRE]
[ACCOUNT {LOCK | UNLOCK}]
[ENABLE EDITIONS]
[CONTAINER= {ALL | CURRENT}]
```

## 5.5 Les utilisateurs

---

### □ Création d'un utilisateur

#### **SMots clés et paramètres**

|                 |                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------|
| User            | : nom de l'utilisateur à créer                                                                         |
| password        | : mot de passe                                                                                         |
| Externally      | : utilisateur authentifié par l'OS                                                                     |
| tablespace      | : nom du tablespace                                                                                    |
| profil          | : nom du profil                                                                                        |
| globally as     | : accès autorisé l'annuaire LDAP                                                                       |
| enable editions | : permet à l'utilisateur de créer des releases<br>d'objets telque du code PL/SQL. Utiliser pour migrer |



## 5.5 Les utilisateurs

---

### □ Création d'un utilisateur

**Exemple 1 : création d'un utilisateur nommé TINTIN identifié au niveau de l'OS dont le tablespace par défaut est USERS. Cet utilisateur à un quota de 2Mo sur les tablespaces SYSTEM et USERS.**

```
sql> CREATE USER OPS$tintin IDENTIFIED EXTERNALLY  
      DEFAULT TABLESPACE users  
      QUOTA 2 M ON system  
      QUOTA 2 M ON users;
```

**Exemple 2 : Création d'un utilisateur nommé DUPOND ayant DUPONT comme mot de passe.**

```
sql> CREATE USER dupond IDENTIFIED BY dupont ;
```

#### Notes

- . le tablespace temporaire par défaut est SYSTEM
- . le tablespace par défaut est SYSTEM
- . il est *obligatoire d'affecter des quotas sur les tablespaces* ou d'affecter le privilège UNLIMITED TABLESPACE
- . les rôles affectés lors de la création d'un utilisateur sont par défaut
- . le privilège CREATE USER est requis.

## 5.5 Les utilisateurs

---

### □ Modification d'un utilisateur

#### Syntaxe

```
ALTER USER user
IDENTIFIED { BY password [[http] DIGEST {enable | disable}]
| EXTERNALLY [as ' {certificate dn | Kerberos principal name}']
| GLOBALLY [AS 'certificate DN' ]}
[DEFAULT COLLATION collation_name]
[ DEFAULT TABLESPACE tablespace ]
[ [LOCAL] TEMPORARY TABLESPACE {tablespace|
tablespaceGroup }
[ QUOTA { integer [ K | M ] | UNLIMITED } ON tablespace ] ...
[ PROFILE profile ]
[DEFAULT ROLE { role [, role ] ...
| ALL [ EXCEPT role [, role ] ... ] | NONE } ]
[PASSWORD EXPIRE]
[ACCOUNT {LOCK | UNLOCK}]
[ENABLE EDITIONS]
[CONTAINER= {ALL | CURRENT}]
```

## 5.5 Les utilisateurs

---

### □ Modification d'un utilisateur

#### Syntaxe

#### Mots clés et paramètres

password : Nouveau mot de passe  
tablespace : Nom du tablespace par défaut et/ou du tablespace temporaire  
profile : Nom du nouveau profil de l'utilisateur  
role : Nom du ou des nouveaux rôles par défaut ou à exclure  
ALL : Tous les rôles deviennent par défaut  
NONE : Aucun rôle par défaut  
EXECPT : Les rôles à exclure apparaissent après ce mot clé  
Proxy\_clause : Authentification des utilisateurs via un proxy

#### NOTES :

**Rôle par défaut** = Rôle affecté directement à un utilisateur

## 5.5 Les utilisateurs

---

### □ Modification d'un utilisateur

- **Exemple 1**

Modification de l'utilisateur DUPONT: nouveau mot de passe BOULES, **tablespace** par défaut USER quota sur ce tablespace illimité et 0 sur le tablespace SYSTEM

```
sql> ALTER USER dupont IDENTIFIED BY boules  
      DEFAULT TABLESPACE user  
      QUOTA UNLIMITED ON user  
      QUOTA 0 ON system ;
```

- **Exemple 2**

Modification de l'utilisateur TINTIN : assignation d'un nouveau tablespace temporaire TEMP et assignation de tous les rôles par défaut sauf rl\_admin\_secu.

```
sql> ALTER USER tintin  
      TEMPORARY TABLESPACE temp  
      DEFAULT ROLE ALL EXCEPT rl_admin_secu;
```

## 5.5 Les utilisateurs

---

### □ Suppression d'un utilisateur

- La suppression d'un utilisateur entraîne la suppression des objets de son schéma (tables, vues, séquences, synonymes, indexes, clusters indexés, clusters hashés, ...)
- Privilège requis : DROP USER

#### Syntaxe

DROP USER user [ CASCADE ]

#### Mots clés et paramètres

|         |                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------|
| user    | : Nom de l'utilisateur à supprimer                                                                  |
| CASCADE | : supprime aussi les objets du schéma de l'utilisateur et les contraintes d'intégrité de référence. |

#### Exemple

```
DROP USER tsang ;  
DROP USER dupont CASCADE ;
```

## 5.5 Les utilisateurs

---

### □ Affectation de droits à un Utilisateur

- **Exemple 1** : Affectation de droits systèmes

```
sql> GRANT create tablespace, create user TO tintin ;
```

- **Exemple 2** : Affectation d'un rôle à un utilisateur

```
sql> GRANT rl_admin_secu TO tintin ;
```

- **Exemple 3** : Affectation d'un privilège objet à un utilisateur

```
sql> GRANT SELECT, UPDATE (ename, sal)  
      ON EMP TO tintin ;
```

- **Exemple 4** : Affectation de privilèges à tous les utilisateurs

```
sql> GRANT drop any table TO PUBLIC ;
```

**NOTE !!!** Attention danger

## 5.5 Les utilisateurs

---

### □ Informations sur les utilisateurs

- Quelques vues sur les utilisateurs

USER\_USERS,  
USER\_XS\_USERS,  
ALL\_USERS,  
DBA\_USERS,  
DBA\_USERS\_WITH\_DEFPWD,  
DBA\_XS\_USERS, CDB\_USERS,  
CDB\_USERS\_WITH\_DEFPWD,  
CDB\_XS\_USERS,  
GV\$PWFILERS\_USERS,  
V\$PWFILERS\_USERS

## 5.5 Les utilisateurs

---

### □ Informations sur les utilisateurs

**Exemple 1:** informations concernant l'utilisateur connecté

col username format a10

col default\_tablespace format A10

col temporary\_tablespace format A10

SELECT username, user\_id, default\_tablespace,  
temporary\_tablespace, created FROM user\_users;

| USERNAME | USER_ID | DEFAULT_TA | TEMPORARY_ | CREATED  |
|----------|---------|------------|------------|----------|
| -----    | -----   | -----      | -----      | -----    |
| SYSTEM   | 9       | SYSTEM     | TEMP       | 08/03/17 |

**Exemple 2 :** informations sur tous les utilisateurs

SELECT username, user\_id, created FROM all\_users  
order by username;

| USERNAME   | USER_ID | CREATED  |
|------------|---------|----------|
| -----      | -----   | -----    |
| ANONYMOUS  | 63      | 08/03/17 |
| APPQOSSYS  | 55      | 08/03/17 |
| AUDSYS     | 8       | 08/03/17 |
| C##MOPOLO  | 106     | 03/11/18 |
| C##MOPOLO2 | 107     | 05/11/18 |
| C##ORS1    | 108     | 03/12/18 |
| C##ORS2    | 110     | 17/12/18 |
| C##SCOTT   | 117     | 19/12/18 |
| C##SCOTT2  | 118     | 19/12/18 |
| C##SQL3    | 119     | 07/01/19 |
| C##TESTBIG | 116     | 18/12/18 |



## 5.5 Les utilisateurs

---

### □ Informations sur les utilisateurs (suite)

**Exemple 3** : toutes les informations sur tous les utilisateurs

SELECT username, user\_id, password, default\_tablespace,  
temporary\_tablespace, created FROM dba\_users;

| USERNAME  | USER_ID    | PASSWORD | DEFAULT_TA | TEMPORARY_ | CREATED  |
|-----------|------------|----------|------------|------------|----------|
| SYS       | 0          |          | SYSTEM     | TEMP       | 08/03/17 |
| SYSTEM    | 9          |          | SYSTEM     | TEMP       | 08/03/17 |
| XS\$NULL  | 2147483638 |          | SYSTEM     | TEMP       | 08/03/17 |
| OJMSYS    | 81         |          | SYSTEM     | TEMP       | 08/03/17 |
| LBACSYS   | 101        |          | SYSTEM     | TEMP       | 08/03/17 |
| OUTLN     | 13         |          | SYSTEM     | TEMP       | 08/03/17 |
| SYS\$UMF  | 46         |          | SYSTEM     | TEMP       | 08/03/17 |
| DBSNMP    | 54         |          | SYSAUX     | TEMP       | 08/03/17 |
| APPQOSSYS | 55         |          | SYSAUX     | TEMP       | 08/03/17 |
| DBSFUSER  | 35         |          | SYSAUX     | TEMP       | 08/03/17 |
| GGSYS     | 60         |          | SYSAUX     | TEMP       | 08/03/17 |

...

## 5.5 Les utilisateurs

---

### □ Informations sur les utilisateurs (suite)

**Exemple 4 :** Informations sur les quotas de l'utilisateur actuel

```
SELECT * FROM user_ts_quotas;
```

| TABSPACE_NAME          | BYTES     | MAX_BYTES | BLOCKS | MAX_BLOCKS | DRO |
|------------------------|-----------|-----------|--------|------------|-----|
| TS_TAB_AIRBASE_UNIFORM | 2867200   | -1        | 350    | -1         | NO  |
| TS_IND_AIRBASE_AUTO    | 524288    | -1        | 64     | -1         | NO  |
| TS_ETUDIANT_BIG        | 35848192  | -1        | 4376   | -1         | NO  |
| TS_TAB_AIRBASE_AUTO    | 1245184   | -1        | 152    | -1         | NO  |
| USERS                  | 236978176 | -1        | 28928  | -1         | NO  |

## 5.5 Les utilisateurs

### □ Informations sur les utilisateurs (suite)

**Exemple 5 :** Informations sur les quotas de tous les utilisateurs au niveau CDB

set linesize 200

set pagesize 100

col username format a18

SELECT \* FROM dba\_ts\_quotas;

| TABSPACE_NAME | USERNAME          | BYTES     | MAX_BYTES | BLOCKS | MAX_BLOCKS | DRO |
|---------------|-------------------|-----------|-----------|--------|------------|-----|
| SYSAUX        | AUDSYS            | 3407872   | -1        | 416    | -1         | NO  |
| SYSAUX        | GSMADMIN_INTERNAL | 917504    | -1        | 112    | -1         | NO  |
| SYSAUX        | DBSFUSER          | 0         | -1        | 0      | -1         | NO  |
| SYSAUX        | APPQOSSYS         | 0         | -1        | 0      | -1         | NO  |
| SYSAUX        | GGSYS             | 0         | -1        | 0      | -1         | NO  |
| SYSAUX        | OLAPSYS           | 0         | -1        | 0      | -1         | NO  |
| USERS         | C##MOPOL0         | 113639424 | -1        | 13872  | -1         | NO  |
| USERS         | C##MOPOL02        | 0         | -1        | 0      | -1         | NO  |
| USERS         | C##ORS1           | 51707904  | -1        | 6312   | -1         | NO  |
| USERS         | C##TESTBIG        | 579534848 | -1        | 70744  | -1         | NO  |
| USERS         | C##ORS2           | 137756672 | -1        | 16816  | -1         | NO  |
| USERS         | C##USECURE        | 131072    | -1        | 16     | -1         | NO  |
| USERS         | C##SCOTT          | 393216    | -1        | 48     | -1         | NO  |
| USERS         | C##SCOTT2         | 327680    | -1        | 40     | -1         | NO  |
| USERS         | C##SQL3           | 196608    | -1        | 24     | -1         | NO  |

15 lignes sélectionnées.

Max\_bytes : quota disque en octets autorisés pour un utilisateur

bytes : nombre d'octets déjà consommés

blocks : nombre de blocs déjà consommés

Max\_blocks : quota disque en blocs pour un utilisateur

## 5.5 Les utilisateurs

---

### □ Informations sur les utilisateurs (suite)

#### Exemple 6 :

Informations sur les utilisateurs connectés

```
set linesize 200
```

```
set pagesize 100
```

```
col username format a18
```

```
col osuser format a20
```

```
col terminal format a18
```

```
col program format a18
```

```
SELECT sid, serial#, username, osuser, status, terminal, program FROM v$session;
```

## 5.5 Les utilisateurs

### □ Informations sur les utilisateurs (suite)

#### Exemple 6 :

#### Informations sur les utilisateurs connectés

| SID | SERIAL# | USERNAME | OSUSER              | STATUS   | TERMINAL | PROGRAM           |
|-----|---------|----------|---------------------|----------|----------|-------------------|
| 1   | 29231   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (CKPT) |
| 2   | 52168   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (DBW0) |
| 3   | 24061   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (LG01) |
| 4   | 29139   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (TMON) |
| 5   | 29964   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (TT00) |
| 9   | 55188   | UAIRBASE | GABRIEL\Utilisateur | INACTIVE | GABRIEL  | sqlplus.exe       |
| 124 | 39278   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (GEN1) |
| 125 | 11904   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (LGWR) |
| 126 | 34084   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (PXMN) |
| 127 | 41512   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (TT01) |
| 129 | 48158   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (Q004) |
| 247 | 42041   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (PMON) |
| 248 | 30924   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (DIAG) |
| 249 | 58929   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (LG00) |
| 250 | 24449   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (W004) |
| 252 | 975     |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (TT02) |
| 370 | 26598   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (CLMN) |
| 371 | 37193   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (PMAN) |
| 372 | 32670   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (SMON) |
| 375 | 59252   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (AQPC) |
| 377 | 52413   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (W000) |
| 493 | 11365   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (PSP0) |
| 494 | 2498    |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (DBRM) |
| 495 | 35002   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (SMCO) |
| 496 | 33094   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (MMON) |
| 499 | 26667   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (Q001) |
| 501 | 27964   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (W002) |
| 616 | 39383   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (VKTm) |
| 617 | 24651   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (VKRM) |
| 618 | 3612    |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (RECO) |
| 619 | 43719   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (MMNL) |
| 620 | 63399   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (QM02) |
| 624 | 58680   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (W005) |
| 739 | 18377   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (GEN0) |
| 740 | 7990    |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (SVCB) |
| 747 | 535     |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (W008) |
| 748 | 17114   | SYSTEM   | GABRIEL\Utilisateur | ACTIVE   | GABRIEL  | sqlplus.exe       |
| 749 | 59928   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (W007) |
| 863 | 57458   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (MMAN) |
| 864 | 45973   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (DIA0) |
| 865 | 50064   |          | Mondi12             | ACTIVE   | GABRIEL  | ORACLE.EXE (LG00) |

## 5.5 Les utilisateurs

---

### □ Informations sur les utilisateurs (suite)

#### Exemple 6 :

Informations sur les utilisateurs connectés

```
slq> SELECT sid, serial#, username, osuser, status,  
terminal, program FROM v$session;
```

|           |                                                          |
|-----------|----------------------------------------------------------|
| Sid :     | Numéro de la session                                     |
| Serial# : | Numéro de série de la session                            |
| username: | Nom oracle de l'utilisateur connecté                     |
| osuser :  | Nom de l'utilisateur au niveau du système d'exploitation |
| status :  | Etat de session (active, inactive)                       |
| Terminal: | Poste client à partir duquel la session a été initiée    |
| Program:  | Programme exécuté par le client                          |



## 5.5 Les utilisateurs

### □ Informations sur les utilisateurs VIA EM EXPRESS

← → ↻ ⚠ Non sécurisé | [https://localhost:5500/em/shell#/security/show\\_users](https://localhost:5500/em/shell#/security/show_users) 📄 ☆ 🔒 ⓘ

ORACLE Enterprise Manager Database Express 12c Aide ▾ SYSTEM Déconnexion ⓘ

DBTEST12 (12.2.0.1.0) Configuration ▾ Stockage ▾ Sécurité ▾ Performances ▾ GABRIEL

Utilisateurs communs ⓘ Page régénérée 24:29:45 GMT+0200 ⓘ

Actions ▾ Créer un utilisateur Créer comme ✕ Supprimer un utilisateur ☐ Ouvrir Nom

| Nom               | Statut du compte | Date d'expiration           | Tablespace par défaut | Tablespace temporaire | Profil  | Créé                       |
|-------------------|------------------|-----------------------------|-----------------------|-----------------------|---------|----------------------------|
| ANONYMOUS         | 🕒🔒               | mer. 8 mars 2017 18:01:40*  | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 16:21:52  |
| APPQOSSYS         | 🕒🔒               | mer. 8 mars 2017 16:40:03*  | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 16:17:38  |
| AUDSYS            | 🕒🔒               | mer. 8 mars 2017 15:57:49   | USERS                 | TEMP                  | DEFAULT | mer. 8 mars 2017 15:57:49  |
| C#MOPOL0          | ✅                | lun. 28 oct. 2019 13:52:49* | USERS                 | TEMP                  | DEFAULT | sam. 3 nov. 2018 01:36:57  |
| C#MOPOL02         | ✅                | sam. 4 mai 2019 15:59:51*   | USERS                 | TEMP                  | DEFAULT | lun. 5 nov. 2018 15:55:18  |
| C#ORS1            | ✅                | sam. 1 juin 2019 08:06:21*  | USERS                 | TEMP                  | DEFAULT | lun. 3 déc. 2018 08:06:21  |
| C#ORS2            | ✅                | sam. 15 juin 2019 24:28:07* | USERS                 | TEMP                  | DEFAULT | lun. 17 déc. 2018 24:28:07 |
| C#SCOTT           | ✅                | lun. 17 juin 2019 10:50:49* | USERS                 | TEMP                  | DEFAULT | mer. 19 déc. 2018 10:50:49 |
| C#SCOTT2          | ✅                | lun. 17 juin 2019 12:15:23* | USERS                 | TEMP                  | DEFAULT | mer. 19 déc. 2018 12:15:23 |
| C#SQL3            | ✅                | sam. 6 juil. 2019 12:03:20* | USERS                 | TEMP                  | DEFAULT | lun. 7 janv. 2019 12:03:20 |
| C#TESTBIG         | ✅                | dim. 16 juin 2019 08:36:50* | USERS                 | TEMP                  | DEFAULT | mar. 18 déc. 2018 08:36:50 |
| C#TOTO            | ✅                | sam. 2 nov. 2019 11:47:42*  | USERS                 | TEMP                  | DEFAULT | lun. 6 mai 2019 11:47:42   |
| C#USECURE         | ✅                | sam. 15 juin 2019 14:22:21* | USERS                 | TEMP                  | DEFAULT | lun. 17 déc. 2018 14:22:21 |
| CTXSYS            | 🕒🔒               | sam. 3 nov. 2018 24:42:42*  | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 17:03:16  |
| DBSPWUSER         | 🕒🔒               | mer. 8 mars 2017 16:28:02*  | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 16:04:42  |
| DBSNMP            | ✅                | ven. 3 mai 2019 23:41:41*   | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 16:17:35  |
| DIP               | 🕒🔒               | mer. 8 mars 2017 16:26:53*  | USERS                 | TEMP                  | DEFAULT | mer. 8 mars 2017 16:03:52  |
| DVF               | 🕒🔒               | mer. 8 mars 2017 18:01:40*  | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 17:56:48  |
| DVSY              | 🕒🔒               | mer. 8 mars 2017 17:58:23*  | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 17:56:48  |
| GGSYS             | 🕒🔒               | mer. 8 mars 2017 16:40:22*  | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 16:18:33  |
| GSMADMIN_INTERNAL | 🕒🔒               | mer. 8 mars 2017 16:26:34*  | SYSAUX                | TEMP                  | DEFAULT | mer. 8 mars 2017 16:03:31  |

## 5.5 Les utilisateurs

### □ Informations sur les utilisateurs VIA EM EXPRESS

The screenshot shows the Oracle Enterprise Manager interface for Database Express 12c. The browser address bar indicates a non-secure connection to the local host. The page title is "Visualiser un utilisateur : C##MOPOLO". The user details section shows the following information:

- Nom: C##MOPOLO
- Profil: DEFAULT
- Authentification: PASSWORD
- Commun: Oui
- Date d'expiration: lun. 28 oct. 2019 13:52:49\*
- Tablespace par défaut: USERS
- Tablespace temporaire: TEMP
- Statut du compte: OPEN
- Créé: sam. 3 nov. 2018 01:36:57

The "Détails" section is expanded, showing the "Rôles & privilèges communs" tab. Below this, there is a table with the following columns: "Privilège", "WITH ADMIN", "Est un rôle", and "Rôle par défaut". The table is currently empty, displaying "Aucune donnée".



## 5.5 Les utilisateurs

---

### □ Suppression d'une session

- En cas de problèmes avec une session (interblocage, consommation excessive de ressources, ...), sa suppression peut être décidée
- cette suppression entraîne :
  - l'annulation de la transaction concernée,
  - la libération des verrous et des ressources consommées
- la commande *Alter System Kill Session ...* permet de supprimer une session.

```
select sid, serial#, username FROM v$session ;
```

| <u>sid</u> | <u>Serial#</u> | <u>Username</u> |
|------------|----------------|-----------------|
| 13         | 8              | tintin          |
| 14         | 11             | sadm            |

```
ALTER SYSTEM KILL SESSION '13, 8';
```

**Note :** Si l'on tente de supprimer une session active, Oracle note la demande. La suppression aura lieu dès que la session cesse d'être active.

## 5.6 L'audit traditionnel

---

### □ Généralités

- L'objectif de l'audit est de **contrôler les accès mal intentionnés** ou non autorisés à la base
- **Règles pour un bon audit**
  - Bien choisir le lieu de mise en oeuvre de l'audit
    - Audit au niveau Oracle(**audit\_trail**=DB). Avantage :
      - audit ciblé grâce à SQL avec possibilité d'exploiter les outils Oracle pour générer des rapports
    - Audit au niveau Oracle(**audit\_trail**=DB, EXTENDED). Idem Audit DB mais récolte aussi les infos sur les Bind et textes des requêtes SQL et les colonnes CLOB
    - Audit au niveau de l'OS(**audit\_trail** = OS). Avantage :
      - possibilité de consolider des audits de sources diverses
    - Audit au niveau de l'OS (**audit\_trail** = XML et xml extended). Audit OS en format XML
    - Inhiber l'audit (**audit\_trail** = NONE)
  - Génération de Log sur DDL (trace les commandes DDL dans des fichiers sans activer l'audit). Le paramètre **audit\_sys\_operations** vaut par défaut TRUE

## 5.6 L'audit traditionnel

---

### □ Généralités

- **Règles pour un bon audit**
  - Bien cibler l'audit pour en limiter le volume
  - Avoir une démarche d'audit par raffinement successif
  - Protéger la table d'audit (sys.aud\$) en limitant l'affectation du privilège DROP ANY TABLE
  - Créer les vues d'audit en exécutant le script cataudit.sql (catnoaudit.sql permet de les supprimer)
- **Privilèges pour gérer l'AUDIT**
  - **AUDIT\_ADMIN** : permet de positionner les actions d'audit
  - **AUDIT\_VIEWER** : permet d'accéder aux tables d'audit et d'effectuer des analyses
- **Un nouveau type d'audit a été introduit depuis Oracle 12c : **AUDIT UNIFIED** (voir le chapitre 5.7)**

## 5.6 L'audit traditionnel

---

### □ Types d'audits

- **Par utilisateur** : auditer l'activité d'un ou plusieurs utilisateurs
- **Par session** (en cas de succès ou d'insuccès) : Pour N activations d'une action dans une session, conserver une seule trace
- **Par accès** (en cas de succès ou d'insuccès) : Pour N activations d'une action dans une session, conserver N trace

### □ Types de surveillance

- Audit sur les ordres SQL et les privilèges systèmes
- Audit sur les objets.

## 5.6.1 L'audit traditionnel

---

### □ Audit des ordres sql et des privilèges systèmes

#### Syntaxe

```
AUDIT
{
  { sql_statement_short_cut1, ...
    | ALL
    | ALL STATEMENTS
    | ALL PRIVILEGES
    | system_privilege1, ...
  } [{BY User1,... | IN SESSION CURRENT}]
  | NETWORK
  | DIRECT PATH LOAD [BY User1,...]
} [BY {SESSION | ACCESS}] [WHENEVER [[NOT] SUCCESSFUL]] [CONTAINER={ALL | CURRENT}]
```

#### Mots clés et paramètres

sql\_stmt\_short\_cut1,.. : audit des groupes de d'instruction SQL (voir plus loin)  
system\_privilege1, ... : audit de 1 ou plusieurs privilège systèmes  
user : audit des ordres sql et/ou privilèges pour un user  
BY SESSION : audit des ordres sql et/ou privilèges par session  
BY ACCESS : audit des ordres sql et/ou privilèges par accès  
SUCCESSFUL : audit des ordres sql et/ou privilèges si succès  
ALL : audit de tous les ordres SQL  
ALL STATEMENTS : audit de tous les ordres SQL  
ALL PRIVILEGES : audit de tous les privilèges  
DIRECT PATH LOAD : Audit de l'utilisation du chargement direct (sqlloader)  
NETWORK : Audit des erreurs internes des couches réseau  
BY user1, ... : Audit de 1 ou plusieurs utilisateurs  
CONTAINER : Auditer dans tous les container ou dans l'actuel

## 5.6 L'audit traditionnel

---

### □ Audit des ordres SQL et des privilèges systèmes (suite)

#### Exemples 1

auditer les connexions et déconnexions des utilisateurs *rackham* et *cyclone* (en cas de succès ou d'insuccès).

```
sql> AUDIT SESSION BY rackham, cyclone ;
```

#### Exemples 2

auditer les ordres *select*, *insert*, *delete* pour toutes les tables et le privilège *execute any procedure* par accès et ceci en cas d'échec.

```
sql> AUDIT select table, insert table, delete table  
      BY ACCESS WHENEVER NOT SUCCESSFUL ;
```

```
sql> AUDIT execute any procedure  
      BY ACCESS WHENEVER NOT SUCCESSFUL ;
```

**ou**

```
sql> AUDIT execute any procedure  
      BY ACCESS WHENEVER NOT SUCCESSFUL ;
```

## 5.6 L'audit traditionnel

---

### □ Options d'audit des ordres SQL

| Options            | Ordres SQL audités                                                             |
|--------------------|--------------------------------------------------------------------------------|
| alter system       | alter system                                                                   |
| cluster            | create cluster, alter cluster, drop cluster, truncate cluster                  |
| context            | create context, drop context                                                   |
| database link      | {create   alter  drop} database link,                                          |
| Dimension          | {create  alter drop} dimension                                                 |
| Directory          | {create   drop} Directory                                                      |
| index              | {create   alter   drop   analyze} index                                        |
| Materialized view  | {create  alter drop} Materialized view                                         |
| not exists         | tout ordre sql qui retourne l'erreur :<br>objet inexistant (create table, ...) |
| Outline            | {create   alter   drop} outline                                                |
| Pluggable database | {create   alter   drop} pluggabke database                                     |

## 5.6 L'audit traditionnel

---

### □ Options d'audit des ordres SQL(suite)

| Options              | Ordres SQL audités                                                                                                                              |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| procedure            | {create   drop} function,<br>{create   drop} package,<br>{create   drop} package body,<br>{create   drop} procedure,<br>{create   drop} library |
| profile              | {create  alter drop} profile                                                                                                                    |
| Public database link | {create public   drop public} database link,                                                                                                    |
| public synonym       | {create   drop} public synonym                                                                                                                  |
| role                 | {create   alter   drop   set} p role                                                                                                            |
| rollback segment     | create   alter  drop} rollback segment,                                                                                                         |
| sequence             | create sequence, drop sequence                                                                                                                  |
| Session              | les connexions                                                                                                                                  |
| synonym              | {create   drop} synonym                                                                                                                         |
| system audit         | {audit   no audit} sql_statements                                                                                                               |
| system grant         | grant system_privileges_and_roles<br>revoke system_privileges_and_roles                                                                         |



## 5.6 L'audit traditionnel

---

### □ Options d'audit des ordres SQL(suite)

| Options    | Ordres SQL audités                                                                                   |
|------------|------------------------------------------------------------------------------------------------------|
| table      | {create   alter   drop   truncate} table                                                             |
| tablespace | {create   alter   drop} tablespace                                                                   |
| Trigger    | create trigger, alter trigger enable or disable<br>alter table with enable, disable and drop clauses |
| Type       | {create   alter   drop} type<br>{create   drop } type body                                           |
| user       | create user, alter user, drop user                                                                   |
| view       | create view, drop view                                                                               |

## 5.6 L'audit traditionnel

---

### □ Options d'audit des ordres SQL(suite)

| Options additionnels | Ordres SQL audités                                                                                              |
|----------------------|-----------------------------------------------------------------------------------------------------------------|
| alter sequence       | alter sequence nom_sequence                                                                                     |
| alter table          | alter table nom_table                                                                                           |
| comment table        | comment on table, vue, snapshot, colonne                                                                        |
| delete table         | delete from nom_table, bnom_vue                                                                                 |
| execute procedure    | appel de procedure et de fonction                                                                               |
| Grant directory      | {grant revoke} privilege on directory                                                                           |
| grant procedure      | <b>grant</b> privilège <b>on</b> procedure,<br><b>revoke</b> privilège <b>on</b> procedure                      |
| grant table          | <b>grant</b> privilège <b>on</b> table, vue, snapshot<br><b>revoke</b> privilège <b>on</b> table, vue, snapshot |
| Grant type           | {grant revoke} privilege on type                                                                                |
| insert table         | insert into table, vue                                                                                          |
| lock table           | lock table table, vue                                                                                           |
| select sequence      | référence à une séquence                                                                                        |
| select table         | select * from table, vue, snapshot                                                                              |
| update table         | update, vue                                                                                                     |
| Write directory      | write operation on directory                                                                                    |

## 5.6 L'audit traditionnel

---

### □ Options d'audit des ordres SQL(suite)

#### Exemple 1 : Audit de l'option TABLE

```
sql> AUDIT table BY ACCESS WHENEVER  
      NOT SUCCESSFUL ;
```

Permet d'auditer d'un coté les ordres SQL :

```
{create | alter | drop | truncate} table
```

## 5.6 L'audit traditionnel

---

### □ Audit des objets du schéma

- Privilège Requis : AUDIT ANY

#### Syntaxe

AUDIT {ALL | object\_option[, object\_option]...}

[BY {SESSION | ACCESS} ]

[WHENEVER [NOT] SUCCESSFUL]

**schema\_object\_clause ::=**

{ ALL | sql\_operation[, | sql\_operation]...}

ON {schema.object | DIRECTORY directory\_name|

MINING MODEL [schema.]model

| SQL TRANSLATION PROFILE schema.profile |DEFAULT}

|               |                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| schema.object | : nom de l'objet à auditer appartenant à un schéma                                                                                                              |
| DEFAULT       | : option d'audit par défaut pour les nouveaux objets à créer ultérieurement                                                                                     |
| BY SESSION    | : audit des ordres sql et/ou privilèges par session                                                                                                             |
| BY ACCESS     | : audit des ordres sql et/ou privilèges par accès                                                                                                               |
| SUCCESSFUL    | : audit des ordres sql et/ou privilèges si succès                                                                                                               |
| DIRECTORY     | : audit des Directories                                                                                                                                         |
| sql_operation | : option d'audit des objets (table, vue, séquence, procédure, vue matérialisée, directory, librairie, type , context, ... : voir le table dans pages suivantes) |
| Mining model  | : Option d'audit d'un mining model                                                                                                                              |

## 5.6 L'audit traditionnel

---

### □ Audit des objets du schéma (suite)

- Les options d'audit des objets

| Option    | Table | Vue | Seq. | Proc. | Mat. | Dir. | Lib. | Type | Context | mm |
|-----------|-------|-----|------|-------|------|------|------|------|---------|----|
| alter     | x     |     | x    |       | x    |      |      | x    |         |    |
| audit     | x     | x   | x    | x     | x    | x    |      | x    | x       | x  |
| comment   | x     | x   |      |       | x    |      |      |      |         | x  |
| delete    | x     | x   |      |       | x    |      |      |      |         |    |
| execute   |       |     |      | x     |      |      | x    |      |         |    |
| Flashback | x     | x   |      |       |      |      |      |      |         |    |
| grant     | x     | x   | x    | x     |      | x    | x    | x    | x       | x  |
| index     | x     |     |      |       | x    |      |      |      |         |    |
| insert    | x     | x   |      |       | x    |      |      |      |         |    |
| lock      | x     | x   |      |       | x    |      |      |      |         |    |
| Read      |       |     |      |       |      | x    |      |      |         |    |
| rename    | x     | x   |      |       |      |      |      |      |         | x  |
| select    | x     | x   | x    |       | x    |      |      |      |         | x  |
| update    | x     | x   |      |       | x    |      |      |      |         |    |

**Notes :** **Seq.** : Séquence, **Proc.** : procédure, fonction, package; **Mat.** : vue matérialisée, **dir.** : directory, **lib.** : library  
**mm** : Mining Model

---

## 5.6 L'audit traditionnel

---

### □ Audit des objets du schéma (suite)

#### Exemple 1

auditer l'ordre SQL *select* sur la table *tintin.emp* en cas d'échec d'exécution de cet ordre.

```
sql> AUDIT select ON scott.emp  
      WHENEVER NOT SUCCESSFUL ;
```

#### Exemple 2

auditer l'*insertion*, la *modification* et la *sélection* sur la table *haddock.dept* par accès.

```
sql> AUDIT insert, update, select  
      ON scott.dept BY ACCESS ;
```

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit

- la **table de base AUD\$** contient l'ensemble des informations sur les audits
- les **vues d'audit** :Elles sont créées en lançant le script *cataudit.sql* et supprimées en lançant *catnoaudit.sql*

ALL\_AUDIT\_POLICIES, USER\_AUDIT\_POLICIES,  
DBA\_AUDIT\_POLICIES, CDB\_AUDIT\_POLICIES : définit des règles fines d'audits

ALL\_AUDIT\_POLICY\_COLUMNS, DBA\_AUDIT\_POLICY\_COLUMNS,  
CDB\_AUDIT\_POLICY\_COLUMNS : définit des règles fines des colonnes d'audits

ALL\_DEF\_AUDIT\_OPTS : Les différentes options d'audit objets

ALL\_REPAUDIT\_ATTRIBUTE, USER\_REPAUDIT\_ATTRIBUTE,  
DBA\_REPAUDIT\_ATTRIBUTE :

ALL\_REPAUDIT\_COLUMN, USER\_REPAUDIT\_COLUMN,  
DBA\_REPAUDIT\_COLUMN

AUDIT\_ACTIONS : code des actions d'audit

DBA\_AUDIT\_EXISTS, CDB\_AUDIT\_EXISTS : fournit les entrées d'audit produit avec AUDIT EXISST ou AUDIT NOT EXISTS

USER\_AUDIT\_OBJECT, DBA\_AUDIT\_OBJECT, CDB\_AUDIT\_OBJECT :  
Contient les lignes d'audits objets

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit

- les vues d'audit

USER\_AUDIT\_SESSION, DBA\_AUDIT\_SESSION, CDB\_AUDIT\_SESSION : contient les lignes d'audit de connexion et déconnexion

USER\_AUDIT\_STATEMENT, DBA\_AUDIT\_STATEMENT, CDB\_AUDIT\_STATEMENT : contient les lignes d'audit concernant les ordres GRANT, REVOKE, AUDIT, NOAUDIT et ALTER SYSTEM

USER\_AUDIT\_TRAIL, DBA\_AUDIT\_TRAIL, CDB\_AUDIT\_TRAILS : contient toutes les lignes d'audits

DBA\_COMMON\_AUDIT\_TRAIL, CDB\_COMMON\_AUDIT\_TRAIL : contient les lignes d'audits standard, grain fin, mandatory et sys écrit en format XML

DBA\_FGA\_AUDIT\_TRAIL, CDB\_FGA\_AUDIT\_TRAIL : contient les entrées d'audits grain fin

USER\_OBJ\_AUDIT\_OPTS, DBA\_OBJ\_AUDIT\_OPTS, CDB\_OBJ\_AUDIT\_OPTS : entrées d'audits sur les objets

DBA\_PRIV\_AUDIT\_OPTS, CDB\_PRIV\_AUDIT\_OPTS : privilèges system en cours d'audit et par utilisateur

DBA\_STMT\_AUDIT\_OPTS, CDB\_STMT\_AUDIT\_OPTS : décrits les options d'audit système



## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Les colonnes représentatives des vues d'audit

| Colonne       | Description                                                |
|---------------|------------------------------------------------------------|
| OS_USERNAME   | Nom au niveau OS de l'utilisateur à auditer                |
| USERNAME      | Nom Oracle de l'utilisateur à auditer                      |
| USERHOST      | Numéro de l'instance de connexion du user                  |
| TERMINAL      | identification du terminal de l'utilisateur                |
| TIMESTAMP     | date et heure d'enregistrement de l'action                 |
| OWNER         | propriétaire de l'objet concerné par l'action              |
| OBJ_NAME      | nom de l'objet concerné par l'action                       |
| ACTION        | code de l'action                                           |
| ACTION_NAME   | nom de l'action                                            |
| NEW_OWNER     | propriétaire de l'objet désigné dans la colonne new_name   |
| NEW_NAME      | nouveau nom de l'objet après RENAME                        |
| OBJ_PRIVILEGE | privilèges objets affectés ou retirés à l'objet            |
| SYS_PRIVILEGE | privilèges systèmes affectés ou retirés                    |
| ADMIN_OPTION  | privilèges systèmes ou rôles donnés avec with ADMIN OPTION |

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Les colonnes des vues d'audit (suite)

| Colonne       | Description                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GRANTEE       | nom de celui qui reçoit le privilège                                                                                                                                                                                                                  |
| AUDIT_OPTION  | options d'audit positionnées avec AUDIT                                                                                                                                                                                                               |
| SES_ACTIONS   | chaîne de 11 caract. chacun vaut "-" pour none ou "S" pour success ou "F" pour failure ou "B" pour les deux. Chaque position correspond dans l'ordre aux actions : alter, audit, comment, delete, grant, index, insert, lock, rename, select, update. |
| LOGOFF_TIME   | date et heure de déconnexion                                                                                                                                                                                                                          |
| LOGOFF_LREAD  | nbre de lectures logiques dans la session                                                                                                                                                                                                             |
| LOGOFF_PREAD  | nbre de lectures physiques dans la session                                                                                                                                                                                                            |
| LOGOFF_LWRITE | nbre de blocs Oracle modifiés dans session                                                                                                                                                                                                            |
| LOGOFF_DLOCK  | nbre de deadlocks détectés durant la session                                                                                                                                                                                                          |
| COMMENT_TEXT  | Commentaire sur la trace de l'action                                                                                                                                                                                                                  |
| SESSIONID     | Numéro de la session Oracle                                                                                                                                                                                                                           |
| ENTRYID       | Numéro de l'ordre exécuté                                                                                                                                                                                                                             |
| STATEMENTID   | numéro de la requête exécutée                                                                                                                                                                                                                         |
| RETURNCODE    | Erreur oracle provoquée par l'action                                                                                                                                                                                                                  |
| PRIV_USED     | Privilèges systèmes utilisés par l'action                                                                                                                                                                                                             |
| CLIENT_ID     | Identificateur du client dans chaque session                                                                                                                                                                                                          |
| OBJECT_LABEL  | Label de l'objet (Oracle sécurisé)                                                                                                                                                                                                                    |
| SESSION_LABEL | Label associé à la session (Oracle sécurisé)                                                                                                                                                                                                          |

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Les colonnes des vues d'audit (suite)

| Colonne            | Description                                                                  |
|--------------------|------------------------------------------------------------------------------|
| ECONTEXT_ID        | id du Contexte d'exécution de l'application                                  |
| SESSION_CPU        | Temps CPU consommé par la session                                            |
| EXTENDED_TIMESTAMP | Timestamp de la création de l'enregistrement                                 |
| PROXY_SESSIONID    | Numéro sérial du proxy                                                       |
| GLOBAL_UID         | Identificateur Global de l'utilisateur (annuaire)                            |
| INSTANCE_NUMBER    | Numéro de l'instance fixé avec le paramètre d'initialisation instance_number |
| OS_PROCESS         | Nr. Du processus du système d'exploitation                                   |
| TRANSACTIONID      | Nr. De la transaction ou l'objet est accédé                                  |
| SQL_BIND           | Bind variable de la requête                                                  |
| SQL_TEXT           | Texte de la requête                                                          |

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Exemple

##### Problème

Nous souhaitons effectuer l'audit sur les activités suspectes suivantes :

- l'affectation des mots de passes, *tablespace* et quotas pour certains utilisateurs ont été modifiés sans autorisation
- un trop grand nombre de verrous exclusifs est posé
- des lignes sont supprimées arbitrairement de la table *emp* de l'utilisateur *Scott*

Nous suspectons pour cela les utilisateurs *rackham* et *cyclone*.

##### Actions effectuées par l'administrateur

```
sql> AUDIT ALTER, INDEX, RENAME ON DEFAULT  
      BY SESSION ;  
sql> CREATE VIEW scott.employees  
      AS SELECT * FROM scott.emp ;  
sql> AUDIT session BY rackham, cyclone;  
sql> AUDIT alter user, drop user ;  
sql> AUDIT lock table BY ACCESS WHENEVER SUCCESSFUL ;  
sql> AUDIT delete ON scott.emp BY ACCESS  
      WHENEVER SUCCESSFUL ;  
sql> CREATE USER UTEST1 IDENTIFIED BY Utest11;
```

## 5.6 L'audit traditionnel

---

### □ Exploitation d'audit (suite)

#### Exemple (suite)

##### Actions effectuées par *rackham*

```
sql> ALTER USER scott QUOTA 0 ON users;  
sql> DROP USER utest1;
```

##### Actions effectuées par *cyclone*

```
sql> LOCK TABLE scott.emp IN EXCLUSIVE MODE ;  
sql> DELETE FROM scott.emp WHERE empno=7934 ;  
sql> ALTER TABLE scott.emp  
    ALLOCATE EXTENT (SIZE 100K) ;  
sql> CREATE INDEX scott.idx_ename ON  
    scott.emp(ename);  
sql> CREATE OR REPLACE PROCEDURE  
    scott.fire_employe(idemp NUMBER) AS  
    BEGIN  
        DELETE FROM scott.emp WHERE empno=idemp;  
    END;  
/  
sql> EXECUTE scott.fire_employe(7902);
```

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Exemple (suite)

##### Visualisation des options d'audit des ordres SQL actives

Col user\_name format A10

Col audit\_option format A20

col success format A10

col failure format a20

```
SELECT user_name, audit_option, success, failure FROM  
dba_stmt_audit_opts ;
```

| USER_NAME | AUDIT_OPTION   | SUCCESS   | FAILURE   |
|-----------|----------------|-----------|-----------|
| -----     | -----          | -----     | -----     |
| RACKHAM   | CREATE SESSION | BY ACCESS | BY ACCESS |
| CYCLONE   | CREATE SESSION | BY ACCESS | BY ACCESS |
|           | ALTER USER     | BY ACCESS | BY ACCESS |
|           | DROP USER      | BY ACCESS | BY ACCESS |
|           | LOCK TABLE     | BY ACCESS | NOT SET   |

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Exemple (suite)

##### Visualisation des options actives d'audit des privilèges

Col user\_name format A10

Col privilege format A20

col success format A10

col failure format a20

```
SELECT user_name, privilege, success, failure FROM  
dba_priv_audit_opts;
```

| USER_NAME | PRIVILEGE      | SUCCESS   | FAILURE   |
|-----------|----------------|-----------|-----------|
|           | DROP USER      | BY ACCESS | BY ACCESS |
|           | ALTER USER     | BY ACCESS | BY ACCESS |
| RACKHAM   | CREATE SESSION | BY ACCESS | BY ACCESS |
| CYCLONE   | CREATE SESSION | BY ACCESS | BY ACCESS |

## 5.6 L'audit traditionnel

### □ Exploitation de l'audit (suite)

#### Exemple (suite)

Visualisation des options d'audit objet sur la table *scott.emp*

col OWNER format A10

col OBJECT\_NAME format A10

col OBJECT\_TYPE format A10

```
SELECT * FROM dba_obj_audit_opts
where owner = 'SCOTT' AND object_name like 'EMP%';
```

| OWNER | OBJECT_NAME | OBJECT_TYPE | ALT | AUD | COM | DEL | GRA | IND | INS | LOC | REN | SEL | UPD | REF | EXE | CRE | REA | WR1 | FBK |
|-------|-------------|-------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| SCOTT | EMP         | TABLE       | -/- | -/- | -/- | A/- | -/- | -/- | -/- | -/- | -/- | -A  | -/- | -/- | -/- | -/- | -/- | -/- | -/- |
| SCOTT | EMPLOYEES   | VIEW        | -/- | -/- | -/- | -/- | -/- | -/- | -/- | -/- | S/S | -/- | -/- | -/- | -/- | -/- | -/- | -/- | -/- |

-/- : Audit non positionné (ni en cas de succès ou d'insuccès)

S/- : Option d'audit positionnée par Session

A/- : Option d'audit positionnée par accès (en cas de succès)

S/S : Par session ( en cas de succès ou d'insuccès)



## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Exemple (suite)

Visualisation des options d'audit objet par défaut

```
sql> SELECT * FROM all_def_audit_opts;
```

| ALT | AUD | COM | DEL | GRA | IND | INS | LOC | REN | SEL | UPD | REF EXE | FBK | REA |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|---------|-----|-----|
| S/S | -/- | -/- | -/- | -/- | S/S | -/- | -/- | S/S | -/- | -/- | -/- -/- | -/- | -/- |

#### Notes :

-/- : Audit non positionné (ni en cas de succès ou d'insuccès)

S/- : Option d'audit positionnée par Session

A/- : Option d'audit positionnée par accès (en cas de succès)

S/S : Par session ( en cas de succès ou d'insuccès)

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Exemple (suite)

**Listing des lignes d'audit générées par l'audit des ordres et audit des objets**

```
sql> SELECT OS_USERNAME, username, USERHOST, obj_name,  
action_name, TIMESTAMP FROM dba_audit_object  
where username in ('RACKHAM', 'CYCLONE');
```

| OS_USERNAME         | USERNAME | USERHOST          | OBJ_NAME | ACTION_NAME | TIMESTAMP |
|---------------------|----------|-------------------|----------|-------------|-----------|
| GABRIEL\Utilisateur | CYCLONE  | WORKGROUP\GABRIEL | EMP      | DELETE      | 26/05/19  |
| GABRIEL\Utilisateur | CYCLONE  | WORKGROUP\GABRIEL | EMP      | LOCK        | 26/05/19  |
| GABRIEL\Utilisateur | CYCLONE  | WORKGROUP\GABRIEL | EMP      | DELETE      | 26/05/19  |
| GABRIEL\Utilisateur | CYCLONE  | WORKGROUP\GABRIEL | EMP      | LOCK        | 26/05/19  |
| GABRIEL\Utilisateur | RACKHAM  | WORKGROUP\GABRIEL | UTEST1   | DROP USER   | 26/05/19  |
| GABRIEL\Utilisateur | RACKHAM  | WORKGROUP\GABRIEL | SCOTT    | ALTER USER  | 26/05/19  |
| GABRIEL\Utilisateur | CYCLONE  | WORKGROUP\GABRIEL | EMP      | DELETE      | 26/05/19  |

7 lignes sélectionnées.

## 5.6 L'audit traditionnel

---

### □ Exploitation de l'audit (suite)

#### Exemple (suite)

##### Listing des lignes d'audit pour l'audit des sessions

```
sql> SELECT username, logoff_time, logoff_lread, logoff_pread,  
        logoff_lwrite, logoff_dlock  
FROM dba_audit_session  
WHERE username in ('RACKHAM', 'CYCLONE');
```

| USERNAME | LOGOFF_T | LOGOFF_LREAD | LOGOFF_PREAD | LOGOFF_LWRITE | LOGOFF_DLOCK |
|----------|----------|--------------|--------------|---------------|--------------|
| -----    |          |              |              |               |              |
| RACKHAM  |          |              |              |               |              |
| CYCLONE  |          |              |              |               |              |
| CYCLONE  |          |              |              |               |              |
| RACKHAM  | 26/05/19 | 16745        | 413          | 391           | 0            |
| CYCLONE  | 26/05/19 | 2188         | 45           | 372           | 0            |

## 5.6 L'audit traditionnel

### □ Informations d'audit via sql developer onglet DBA)

Oracle SQL Developer : AUDITSETTING PDBADMIN.null@con\_as\_pdbadmin\_pdborcl

Fichier Modifier Affichage Naviguer Exécuter Equipe Outils Window Aide

Connexions DBA Rapports Page de début con\_as\_pdbadmin\_pdborcl Paramètres d'audit

Configuration Options par défaut Trace des connexions ayant échoué Trace des privilèges Privilèges soumis à un audit Objets soumis à un audit Instructions soumises à un audit

Actions...

|     | Schema  | Object Name         | Statement | Success | Failure | Object Type |
|-----|---------|---------------------|-----------|---------|---------|-------------|
| 74  | DVSY    | COMMAND_RULE\$      | DELETE    | ACCESS  | ACCESS  | TABLE       |
| 75  | DVSY    | AUDIT_TRAIL\$       | DELETE    | ACCESS  | ACCESS  | TABLE       |
| 76  | LBACSYS | OLS\$PROPS          | DELETE    | ACCESS  | ACCESS  | TABLE       |
| 77  | SCOTT   | EMP                 | DELETE    | ACCESS  | NOT...  | TABLE       |
| 78  | DVSY    | IDENTITY\$          | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 79  | DVSY    | IDENTITY_MAP\$      | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 80  | DVSY    | MAC_POLICY\$        | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 81  | DVSY    | MAC_POLICY_FACTOR\$ | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 82  | DVSY    | POLICY_LABEL\$      | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 83  | DVSY    | REALM\$             | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 84  | DVSY    | REALM_AUTH\$        | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 85  | DVSY    | REALM_OBJECT\$      | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 86  | DVSY    | ROLE\$              | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 87  | DVSY    | RULE\$              | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 88  | DVSY    | RULE_SET\$          | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 89  | DVSY    | RULE_SET_RULE\$     | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 90  | DVSY    | FACTOR\$            | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 91  | DVSY    | FACTOR_LINK\$       | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 92  | DVSY    | FACTOR_TYPE\$       | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 93  | DVSY    | CODE\$              | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 94  | DVSY    | COMMAND_RULE\$      | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 95  | DVSY    | AUDIT_TRAIL\$       | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 96  | LBACSYS | OLS\$PROPS          | GRANT     | ACCESS  | ACCESS  | TABLE       |
| 97  | DVSY    | IDENTITY\$          | INDEX     | ACCESS  | ACCESS  | TABLE       |
| 98  | DVSY    | IDENTITY_MAP\$      | INDEX     | ACCESS  | ACCESS  | TABLE       |
| ... |         |                     |           |         |         |             |

## 5.6 L'audit traditionnel

---

### □ Désactivation de l'audit sur les Ordres SQL et les privilèges systèmes

#### Syntaxe

```
NOAUDIT
{
    sql_statement_shortcut [, sql_statement_shortcut, ...]
    | ALL
    | ALL STATEMENTS
    | system_privilege[,system_privilege, ...]
    | ALL PRIVILEGES
} [BY user[,user, ...]] [CONTAINER= {CURRENT | ALL}]
```

#### Mots clés et paramètres

|                        |                                                 |
|------------------------|-------------------------------------------------|
| Sql_statement_shortcut | : option des ordres sql à ne plus auditer       |
| system_privilege       | : privilège système à ne plus auditer           |
| user                   | : désactiver l'audit des ordres SQL sur un user |

## 5.6 L'audit traditionnel

---

### □ Désactivation de l'audit sur les Ordres SQL et les privilèges systèmes

#### Syntaxe

#### Exemples

```
sql>NOAUDIT session;  
sql>NOAUDIT role;  
sql>NOAUDIT session BY tintin, cyclone ;  
sql>NOAUDIT delete any table;  
sql>NOAUDIT select any table, insert any table,  
      delete any table, execute any procedure;  
sql>NOAUDIT select table, insert table, delete table;  
sql>NOAUDIT ALL ;  
sql>NOAUDIT ALL PRIVILEGES ;
```

**Note :** le privilège requis est AUDIT SYSTEM

## 5.6 L'audit traditionnel

---

### □ Désactivation de l'audit des objets du schéma

#### Syntaxe

```
NOAUDIT
{
    ALL
    | sql_operation[,sql_operation, ...]
} ON{ [schema.]object
    | DIRECTORY directoryName
    | MINING MODEL [schema.]model
    | SQL TRANSACTION PROFILE [schema.]profile
    | DEFAULT
} [CONTAINER= {CURRENT | ALL}]
```

#### Mots clés et paramètres

|               |                                                       |
|---------------|-------------------------------------------------------|
| sql_operation | : option d'objet d'audit à désactiver                 |
| object        | : nom de l'objet sur lequel l'audit va être désactivé |
| DEFAULT       | : désactiver les options d'audit par défaut           |
| schema        | : nom du propriétaires d'objets                       |

#### Exemples

```
sql>NOAUDIT select ON tintin.emp ;
sql>NOAUDIT select
    ON tintin.emp WHENEVER SUCCESSFUL;
sql>NOAUDIT ALL ON tintin.emp ;
sql>NOAUDIT ALL ON DEFAULT ;
```

**Note :** le privilège requis est AUDIT SYSTEM

---



## 5.6 L'audit traditionnel

---

### □ Administration et utilisation de l'audit

1. **Activation de l'audit.** Positionner au niveau du fichier init.ora le paramètre init.ora :

- `AUDIT_TRAIL = { none | os | db [, extended] | xml [, extended] }`

2. **installer les vues d'audit** (cataudit.sql)

3. **Utiliser la commande AUDIT** pour positionner l'audit

4. **Sécuriser de la table d'audit** : attribuer le privilège *delete any table* à l'administrateur de sécurité uniquement. Auditer la table d'audit.

`AUDIT insert, update, delete ON sys.aud$ BY ACCESS`

5. **Utiliser si nécessaire la commande NOAUDIT** pour annuler les positionnements faits avec AUDIT

6. **Exploiter les résultats d'audit**

7. **Purger ou réduire la taille de l'audit**

`DELETE FROM sys.aud$`

`DELETE FROM sys.aud$ where obj$name='EMP'; ...`

•8. **Désactiver l'audit** (dans init.ora `AUDIT_TRAIL = NONE`)



## 5.7 L'audit unifié

---

### □ Plan

- Généralités
- Configuration/Activation de l'audit unifié
- Affectation à l'utilisateur SEC\_ADMIN du role AUDIT\_ADMIN
- Etapes de l'audit UNIFIE
- Création d'une police d'audit
- Modification d'une police d'audit
- Suppression d'une police d'audit
- Commande d'audit pour l'audit unifié
- Visualisation des résultats d'audit unifié
- Commande noaudit pour l'audit unifié
- Purge des enregistrements l'audit unifié

## 5.7 L'audit unifié

---

### □ Généralités

- **Audit UNIFIE regroupant**
  - Les enregistrements d'audit (y compris ceux de SYS) venant des options d'audit et de la politique d'audit
  - Enregistrements d'Audit fin venant du pakacge DBMS\_FGA
  - Enregistrements d'audit de RAS (Real Application Security)
  - Enregistrements d'audit venant de RMAN (Recovery Manager)
  - Enregistrements d'audit venant de Database VAULT
  - Enregistrements d'audit venant de Label Security
- **L'accès à l'audit unifié se fait à partir des vues**
  - UNIFIED\_AUDIT\_TRAIL
  - GV\$UNIFIED\_AUDIT\_TRAIL : en architecture RAC
- **Autres activités d'AUDIT FIN :**
  - Audit des colonnes spécifiques par exemple le salaire
  - Notification de la violation des actions d'audit à l'administrateur de sécurité

## 5.7 L'audit unifié

---

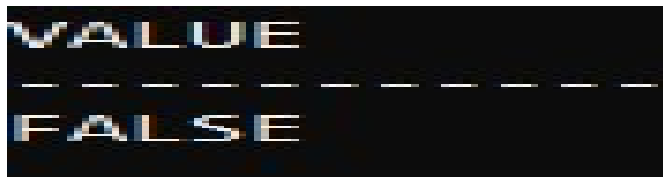
### □ Configuration/Activation de l'audit unifié

**1. se connecter sur votre base CDB\$ROOT avec le privilège SYSDBA**

Sqlplus sys@dbtest12/Pass as sysdba

**2. Vérification si la base a été migrée pour utiliser l'AUDIT UNIFIE**

```
SELECT VALUE FROM V$OPTION WHERE  
PARAMETER = 'Unified Auditing';
```



```
VALUE  
-----  
FALSE
```

**3. Si la réponse en 2 est FALSE**

– il faut arrêter la base

```
Sql> shutdown immediate;
```

```
Sql> exit
```

– Arrêter aussi le service Windows

```
C:\> net stop OracleService%ORACLE_SID%
```

```
C:\> net stop OracleServiceDBTEST12
```

## 5.7 L'audit unifié

---

### □ Configuration/Activation de l'audit unifié

#### 4. Arrêter le LISTENER

C:\> lsnrctl stop listener\_name

C:\> lsnrctl stop listener

#### 5. Se déplacer dans le dossier

\$ORACLE\_HOME/rdbms/lib

#### 6. Activer les exécutable de l'audit unifié

- Sous Linux exécuter la commande suivante

\$ make -f ins\_rdbms.mk uniaud\_on ioracle

ORACLE\_HOME=\$ORACLE\_HOME

- Sous Windows Renommer le fichier

%ORACLE\_HOME%/bin/orauniaud12.dll.option en

%ORACLE\_HOME%/bin/orauniaud12.dll

## 5.7 L'audit unifié

---

### □ Configuration/Activation de l'audit unifié

#### 7. Redémarrer le Listener

```
lsnrctl start listener_name
```

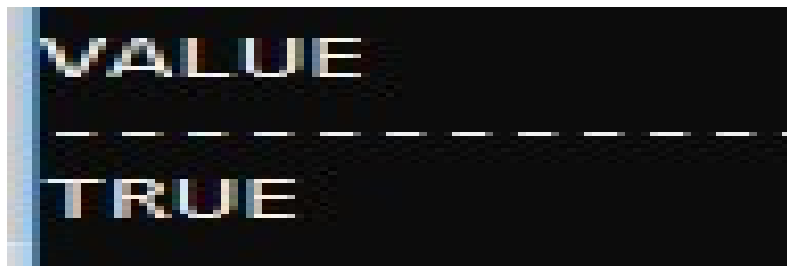
#### 8. Redémarrer la base

```
Sql> connect sys@dbtest12/pass as sysdba  
Sql> startup;
```

Sous Windows Redémarrer le service windows de la base  
`net start OracleService%ORACLE_SID%`

#### 9. Vérification de l'activation de l'audit unifié

```
Sql> SELECT VALUE FROM V$OPTION WHERE  
PARAMETER = 'Unified Auditing';
```



A screenshot of a SQL query result. The text 'VALUE' is at the top, followed by a dashed line, and then 'TRUE'.

## 5.7 L'audit unifié

---

### □ Affectation à l'utilisateur SEC\_ADMIN du role AUDIT\_ADMIN

#### 1. Vérifier que l'utilisateur SEC\_ADMIN existe

```
Sql> select username from dba_users where username like  
'%SEC%';  
NO ROWS
```

#### 2. Si SEC\_ADMIN n'existe pas, le créer

```
-- modifier ce parameter interne pour créer un  
-- un utilisateur dans cdb$root sans le préfixe c##  
Sql> alter session set "_ORACLE_SCRIPT"=true;
```

```
Sql> Create user Sec_admin identified by SecAdmin01  
Default tablespace users Temporary tablespace temp  
Quota unlimited on users;
```

## 5.7 L'audit unifié

---

### □ Affectation à l'utilisateur SEC\_ADMIN du role AUDIT\_ADMIN

#### 2. Si SEC\_ADMIN n'existe pas, le créer

```
Sql> Grant CREATE PROCEDURE, CREATE ROLE,  
CREATE SESSION, INHERIT ANY PRIVILEGES,  
SELECT ANY DICTIONARY to SEC_ADMIN ;
```

```
Sql> grant AUDIT_ADMIN to Sec_admin;
```

```
-- remettre le parameter ci-dessous à False
```

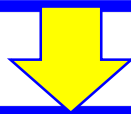
```
Sql> alter session set "_ORACLE_SCRIPT"=false;
```

## 5.7 L'audit unifié

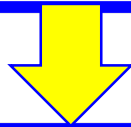
---

### □ Etapes de l'audit UNIFIE

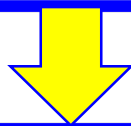
Après la configuration / activation de l'audit unifié



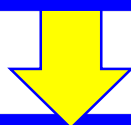
**Créer** des polices d'audit Unifiées  
ou, **Modifier** des polices d'audit Unifiées  
ou, **Supprimer** des polices d'audit unifiées



**Lancer** l'audit (AUDIT) d'une Police d'audit Unifiée  
ou, **Désactiver** l'audit (NOAUDIT) d'une police  
d'audit unifiée



Visualiser les enregistrements d'audit unifiée (vue  
**Unified\_audit\_trail**)



Purger les enregistrements d'audit (fonction  
DBMS\_AUDIT\_MGMT.**clean\_audit\_trail**)



## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

```
CREATE AUDIT POLICY policy
[PRIVILEGES system_privilege[, system_privilege, ...]
{ ACTIONS {{object_action | ALL} ON{          DIRECTORY directory_nam
| MINING MODEL [schema.]object_name
| [schema.]object_name
}
[{object_action | ALL} ON{...}, ...]
|
{ system_actions
|ALL
}
}
| ACTIONS COMPONENT = { { DATAPUMP
|DIRECT LOAD
|OLS
|XS
} component_action[, component_action, ...]
|DV component_action ON object_name
[, component_action ON object_name, ...]
}
| ROLES role[,role, ...]
} [WHEN 'audit_condition' EVALUATE PER {STATEMENT | SESSION | INSTANCE}
CONTAINER = {ALL | CURRENT}
]
```

## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

| Clause               | Description                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Policy               | Nom de la police d'audit unifiée à créer                                                                                       |
| system_privilege     | privilege système : un ou plusieurs                                                                                            |
| object_action ON     | Permet d'auditer une action sur l'objet spécifié (voir le tableau page suivante)                                               |
| ALL ON               | Permet d'auditer toutes les actions sur l'objet spécifié (voir le tableau page suivante)                                       |
| directory_name       | type d'objet directory                                                                                                         |
| [schema.]object_name | type d'objet (table, vue, vue matérialisé, ...)                                                                                |
| system_actions       | Audit des action Système sur la base<br>select name from auditable_system_actions where component='Standard';                  |
| ALL                  | Permet d'auditer toutes les System_actions                                                                                     |
| component_action     | Clause pour auditer les actions sur les composants tels que : datapump, direct path, label security, real application security |
| DV                   | Audit des actions Oracle Database Vault                                                                                        |
| WHEN clause          | Permet de controller quand prend effet l'audit                                                                                 |
| Audit_condition      | Permet de specifier la condition de prise d'effet si true                                                                      |
| DATAPUMP             | Audit des actions DATAPUMP                                                                                                     |
| DIRECT_LOAD          | Audit des actions Oracle Direct Path                                                                                           |
| OLS                  | Audit des actions Oracle Label >Security                                                                                       |
| XS                   | Audit des actions Oracle DB real Application Security                                                                          |

## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

| Type d'objets                                    | Actions                                                                                            |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Directory                                        | AUDIT, GRANT, READ                                                                                 |
| Function                                         | AUDIT, EXECUTE (Notes 1 and 2), GRANT                                                              |
| Java Schema Objects<br>(Source, Class, Resource) | AUDIT, EXECUTE, GRANT                                                                              |
| Library                                          | EXECUTE, GRANT                                                                                     |
| Materialized Views                               | ALTER, AUDIT, COMMENT, DELETE, INDEX,<br>INSERT, LOCK, SELECT, UPDATE                              |
| Mining Model                                     | AUDIT, COMMENT, GRANT, RENAME,<br>SELECT                                                           |
| Object Type                                      | ALTER, AUDIT, GRANT                                                                                |
| Package                                          | AUDIT, EXECUTE, GRANT                                                                              |
| Procedure                                        | AUDIT, EXECUTE, GRANT                                                                              |
| Sequence                                         | ALTER, AUDIT, GRANT, SELECT                                                                        |
| Table                                            | ALTER, AUDIT, COMMENT, DELETE,<br>FLASHBACK, GRANT, INDEX, INSERT,<br>LOCK, RENAME, SELECT, UPDATE |
| View                                             | AUDIT, DELETE, FLASHBACK, GRANT,<br>INSERT, LOCK, RENAME, SELECT, UPDATE                           |

## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

- Exemple 1 : Police d'audit des privileges systèmes
- Exemple 2 : Police d'audit des Actions sur les objets
- Exemple 3 : Police d'audit des actions systèmes
- Exemple 4 : Police d'audit des actions sur composants
- Exemple 5 : Police d'audit des rôles
- Exemple 6 : Police d'audit des privileges systems, des actions sur des objets et des rôles
- Exemple 7 : Police d'audit avec contrôle du déclenchement
- Exemple 8 : Police d'audit dans le container courant
- Exemple 9 : Police d'audit dans tous les containers

## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

- **Exemple 1** : Police d'audit des privileges systems

```
CREATE AUDIT POLICY sys_privs_on_tables_pol  
PRIVILEGES CREATE ANY TABLE, DROP ANY  
TABLE;
```

```
-- Vérification
```

```
col policy_name format A30
```

```
col AUDIT_OPTION format a20
```

```
SELECT policy_name, AUDIT_OPTION
```

```
FROM audit_unified_policies
```

```
WHERE policy_name'SYS_PRIVS_ON_TABLES_POL';
```

| POLICY_NAME             | AUDIT_OPTION     |
|-------------------------|------------------|
| SYS_PRIVS_ON_TABLES_POL | DROP ANY TABLE   |
| SYS_PRIVS_ON_TABLES_POL | CREATE ANY TABLE |

## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

- **Exemple 2** : Police d'audit des **Actions sur les objets**

```
CREATE AUDIT POLICY maj_etudiant_pilote_pol  
ACTIONS DELETE on uairbase.etudiant, INSERT on  
uairbase.etudiant, UPDATE on uairbase.etudiant, ALL on  
uairbase.pilote;
```

```
CREATE AUDIT POLICY read_directory_pol ACTIONS  
READ ON DIRECTORY DATA_PUMP_DIR;
```

## 5.7 L'audit unifié

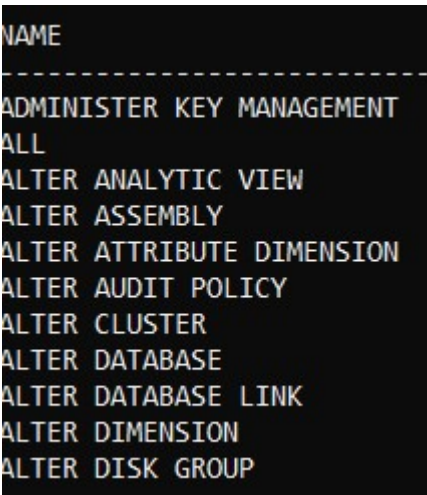
---

### □ Création d'une police d'audit

- **Exemple 3 : Police d'audit des actions systèmes**

La requête suivante liste l'ensemble des Ordres SQL pouvant être audités

```
select name from auditable_system_actions  
where component='Standard' order by name;
```



```
NAME  
-----  
ADMINISTER KEY MANAGEMENT  
ALL  
ALTER ANALYTIC VIEW  
ALTER ASSEMBLY  
ALTER ATTRIBUTE DIMENSION  
ALTER AUDIT POLICY  
ALTER CLUSTER  
ALTER DATABASE  
ALTER DATABASE LINK  
ALTER DIMENSION  
ALTER DISK GROUP
```

...

- Audit des ordres SQL suivants

Create audit smt\_pol **ACTIONS** create table, alter table, create cluster, alter cluster, create tablespace, alter tablespace, drop tablespace;

- Audit de toutes les actions systèmes (ordre sql)

Create audit policy all\_stmt\_pol **ACTIONS all;**

## 5.7 L'audit unifié

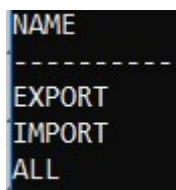
---

### □ Création d'une police d'audit

- **Exemple 4** : Police d'audit des actions sur composants
  - Police d'audit sur le composant DATAPUMP

- Visualisation des action à auditer

```
SELECT name FROM auditable_system_actions WHERE  
component = 'Datapump';
```



| NAME   |
|--------|
| EXPORT |
| IMPORT |
| ALL    |

- Création de la police

```
CREATE AUDIT POLICY dp_actions_pol ACTIONS  
COMPONENT = datapump IMPORT;
```



## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

- **Exemple 5** : Police d'audit des rôles

- Auditer des rôles prédéfinis java

```
CREATE AUDIT POLICY java_pol ROLES java_admin,  
java_deploy;
```

- Auditer les rôles prédéfinis sur le catalogue

```
CREATE AUDIT POLICY catalog_pol ROLES  
Execute_catalog_role, Select_catalog_role;
```

## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

- **Exemple 6 :** Police d'audit des privileges systèmes, des actions sur des objets et des rôles

```
CREATE AUDIT POLICY uairbase_admin_pol  
PRIVILEGES CREATE ANY TABLE, DROP ANY  
TABLE
```

```
ACTIONS DELETE ON uairbase.etudiant, INSERT ON  
uairbase.etudiant, UPDATE ON uairbase.etudiant, ALL  
ON uairbase.pilote, LOCK TABLE
```

```
ROLES audit_admin, audit_viewer;
```

## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

- **Exemple 7** : Police d'audit avec contrôle du déclenchement
  - Audit sera active pour les utilisateurs ayant les id

```
CREATE AUDIT POLICY etudiant_updates_pol ACTIONS  
DELETE ON uairbase.etudiant, INSERT ON  
uairbase.etudiant, UPDATE ON uairbase.etudiant  
WHEN 'UID NOT IN (128, 130, 132)' EVALUATE PER  
STATEMENT;
```

## 5.7 L'audit unifié

---

### □ Création d'une police d'audit

- **Exemple 8** : Police d'audit dans le container courant

```
CREATE AUDIT POLICY local_table_pol PRIVILEGES  
CREATE ANY TABLE, DROP ANY TABLE  
CONTAINER = CURRENT;
```

- **Exemple 9** : Police d'audit dans tous les containers

```
CREATE AUDIT POLICY common_role1_pol ROLES  
C##RL_COURS_SQL CONTAINER = ALL;
```

## 5.7 L'audit unifié

### □ Modification d'une police d'audit

```
ALTER AUDIT POLICY policy
{
  {ADD | DROP}
  [PRIVILEGES system_privilege[, system_privilege, ...]
  { ACTIONS {{object_action | ALL} ON{          DIRECTORY directory_name
          | MINING MODEL [schema.]object_name
          | [schema.]object_name
          }
          [{object_action | ALL} ON{...}, ...]
          |
          { system_actions
            |ALL
          }
        }
    | ACTIONS COMPONENT = { { DATAPUMP
                          |DIRECT LOAD
                          |OLS
                          |XS
                          } component_action[, component_action, ...]
                          |DV component_action ON object_name
                          [, component_action ON object_name, ...]
                        }
    | ROLES role[,role, ...]
  } [WHEN 'audit_condition' EVALUATE PER {STATEMENT | SESSION | INSTANCE}
    CONTAINER = {ALL | CURRENT}
  ]
  | CONDITION {DROP | 'condition_drop' EVALUATE PER {STATEMENT | SESSION | INSTANCE}
}
```

## 5.7 L'audit unifié

---

### □ Modification d'une police d'audit

| Clause               | Description                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Policy               | Nom de la police d'audit unifiée à créer                                                                                       |
| system_privilege     | privilege système : un ou plusieurs                                                                                            |
| object_action ON     | Permet d'auditer une action sur l'objet spécifié (voir le tableau page suivante)                                               |
| ALL ON               | Permet d'auditer toutes les actions sur l'objet spécifié (voir le tableau page suivante)                                       |
| directory_name       | type d'objet directory                                                                                                         |
| [schema.]object_name | type d'objet (table, vue, vue matérialisé, ...)                                                                                |
| system_actions       | Audit des action Système sur la base<br>select name from auditable_system_actions where component='Standard';                  |
| ALL                  | Permet d'auditer toutes les System_actions                                                                                     |
| component_action     | Clause pour auditer les actions sur les composants tels que : datapump, direct path, label security, real application security |
| DV                   | Audit des actions Oracle Database Vault                                                                                        |
| WHEN clause          | Permet de controller quand prend effet l'audit                                                                                 |
| Audit_condition      | Permet de specifier la condition de prise d'effet si true                                                                      |
| DATAPUMP             | Audit des actions DATAPUMP                                                                                                     |
| DIRECT_LOAD          | Audit des actions Oracle Direct Path                                                                                           |
| OLS                  | Audit des actions Oracle Label >Security                                                                                       |
| XS                   | Audit des actions Oracle DB real Application Security                                                                          |

## 5.7 L'audit unifié

---

### □ Modification d'une police d'audit

- Exemple 1 : Ajout de PRIVILEGE dans une police d'audit
- Exemple 2 : Ajout d'actions dans une police d'audit
- Exemple 3 : Ajout de role dans une police d'audit
- Exemple 4 : Suppression de privileges dans une police d'audit

## 5.7 L'audit unifié

---

### □ Modification d'une police d'audit

- **Exemple 1** : Ajout de PRIVILEGE dans une police d'audit

```
ALTER AUDIT POLICY uairbase_admin_pol ADD  
PRIVILEGES CREATE ANY TABLE, DROP ANY  
TABLE;
```

- **Exemple 2** : Ajout d'actions dans une police d'audit

```
ALTER AUDIT POLICY java_pol ADD ACTIONS  
CREATE JAVA, ALTER JAVA, DROP JAVA;
```

- **Exemple 3** : Ajout de role dans une police d'audit

```
ALTER AUDIT POLICY local_table_pol ADD ROLES  
dba;
```

- **Exemple 4** : Suppression de privileges dans une police d'audit

```
ALTER AUDIT POLICY local_table_pol DROP  
PRIVILEGES CREATE ANY TABLE;
```

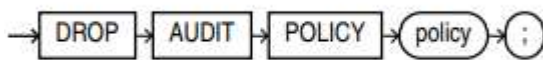


## 5.7 L'audit unifié

---

### □ Suppression d'une police d'audit

- Syntaxe



- Exemple 1: Suppression de la police d'audit `common_role1_pol`  
`DROP AUDIT POLICY common_role1_pol;`
- Exemple 2 : Suppression de la police d'audit `maj_etudiant_pilote_pol` ;  
`DROP AUDIT POLICY maj_etudiant_pilote_pol ;`

```
SYSTEM pdborc1>DROP AUDIT POLICY maj_etudiant_pilote_pol ;
DROP AUDIT POLICY maj_etudiant_pilote_pol
*
ERREUR Ó la ligne 1 :
ORA-46361: Impossible de supprimer la stratégie d'audit puisqu'elle est actuellement activée.
```

## 5.7 L'audit unifié

---

### □ Commande d'audit pour l'audit unifié

```
AUDIT
{
  {POLICY policy {{BY | EXCEPT} [user, user,...]
    |BY USER WITH GRANTED ROLES role[role,...]
    }[WHENEVER [NOT] [SUCCESSFUL]
  }
  |
  CONTEXT NAMESPACE namespace attribute
  [, CONTEXT NAMESPACE namespace attribute, ...]
  [BY user[, user, ...]
}

```

## 5.7 L'audit unifié

---

### □ Commande d'audit pour l'audit unifié

| Clause                                         | Description                                                            |
|------------------------------------------------|------------------------------------------------------------------------|
| POLICY Policy                                  | Désigne la police d'audit unifiée à auditer                            |
| By user with granted<br>role role1, role2, ... | Audit par utilisateurs ayant reçus les role : role1,<br>role2,..       |
| When ever [not]<br>successful                  | En cas de succès ou d'insuccès                                         |
| CONTEXT<br>NAMESPACE<br>namespace              | Introduit les valeurs d'un contexte dans les<br>enregistrement d'audit |
| BY user1, [user2, ..]                          | Audit par utilisateur de user1, user2, etc.                            |
| Except user1, [user2, ..]                      | Audit sauf les utilisateurs user1, user2, etc.                         |

## 5.7 L'audit unifié

---

### □ Commande d'audit pour l'audit unifié

- Exemple d'activation d'audit
  - **Exemple 1:** AUDIT de la police d'audit  
maj\_etudiant\_pilote\_pol pour tous les utilisateurs
  - **Exemple 2:** Audit de la police d'audit  
maj\_etudiant\_pilote\_pol pour un utilisateur particulier
  - **Exemple 3:** audit de la police d'audit ? En cas d'insuccès
  - **Exemple 4:** Audit de la police d'audit  
maj\_etudiant\_pilote\_pol en integrant les informations de contexte

## 5.7 L'audit unifié

---

### □ Commande d'audit pour l'audit unifié

- Exemple d'activation d'audit
  - **Exemple 1:** AUDIT de la police d'audit maj\_etudiant\_pilote\_pol pour tous les utilisateurs

```
AUDIT POLICY maj_etudiant_pilote_pol ;
```

- **Visualisation des information d'audit**

Col user\_name format A20

```
SELECT policy_name, enabled_opt, user_name FROM  
audit_unified_enabled_policies WHERE policy_name =  
'MAJ_ETUDIANT_PILOTE_POL';
```

| POLICY_NAME             | ENABLED | USER_NAME |
|-------------------------|---------|-----------|
| MAJ_ETUDIANT_PILOTE_POL | BY      | ALL USERS |

## 5.7 L'audit unifié

---

### □ Commande d'audit pour l'audit unifié

- Exemple d'activation d'audit
  - **Exemple 2:** Audit de la police d'audit  
maj\_etudiant\_pilote\_pol pour un utilisateur particulier  
AUDIT POLICY maj\_etudiant\_pilote\_pol BY  
UAIRBASE, SCOTT;
  - **Exemple 3:** audit de la police d'audit  
**sys\_privs\_on\_tables\_pol** En cas d'insuccès  
AUDIT POLICY **sys\_privs\_on\_tables\_pol** BY uairbase  
WHENEVER NOT SUCCESSFUL;
  - **Exemple 4:** Audit de la police d'audit  
maj\_etudiant\_pilote\_pol en integrant les informations  
de context  
AUDIT **CONTEXT NAMESPACE** userenv ATTRIBUTES  
current\_user, db\_name BY scott, uairbase;
  - **Exemple 5 :** Audit de la police d'audit  
uairbase\_admin\_pol  
**AUDIT POLICY uairbase\_admin\_pol;**

## 5.7 L'audit unifié

---

### □ Visualisation des résultats d'audit unifié

- Pour visualiser les résultats d'audit unifié il faut consulter la vue :

— **unified\_audit\_trail**

- Supposons que l'utilisateur uairbase une action de création d'une table dans le schéma d'un autre utilisateur. Cette action est en cours d'audit dans la police : **uairbase\_admin\_pol**

DROP TABLE scott.ttest;

CREATE TABLE scott.ttest1(C1 char);

## 5.7 L'audit unifié

### □ Visualisation des résultats d'audit unifié

- Visualisation du résultat de la surveillance

```
set linesize 200
col os_username format A25
col terminal format A10
col dbusername format a10
col action_name format A25
Col event_timestamp format a25
select EVENT_TIMESTAMP, os_username, terminal,
dbusername, action_name
from unified_audit_trail where dbusername='UAIRBASE'
order by EVENT_TIMESTAMP;
```

| EVENT_TIMESTAMP          | OS_USERNAME         | TERMINAL | DBUSERNAME | ACTION_NAME |
|--------------------------|---------------------|----------|------------|-------------|
| 09/05/19 10:04:52,657000 | GABRIEL\Utilisateur | GABRIEL  | UAIRBASE   | LOGON       |
| 09/05/19 11:20:35,638000 | GABRIEL\Utilisateur | GABRIEL  | UAIRBASE   | ALTER USER  |
| 09/05/19 11:21:01,799000 | GABRIEL\Utilisateur | GABRIEL  | UAIRBASE   | ALTER USER  |
| 11/05/19 21:50:40,696000 | GABRIEL\Utilisateur | GABRIEL  | UAIRBASE   | LOGON       |
| 13/05/19 14:48:43,802000 | GABRIEL\Utilisateur | GABRIEL  | UAIRBASE   | ALTER USER  |
| 13/05/19 22:52:44,127000 | Utilisateur         | unknown  | UAIRBASE   | PURGE TABLE |

...

|                          |                     |         |          |              |
|--------------------------|---------------------|---------|----------|--------------|
| 26/05/19 21:44:43,940000 | GABRIEL\Utilisateur | GABRIEL | UAIRBASE | CREATE USER  |
| 26/05/19 21:52:17,911000 | GABRIEL\Utilisateur | GABRIEL | UAIRBASE | ALTER USER   |
| 03/06/19 02:05:18,592000 | GABRIEL\Utilisateur | GABRIEL | UAIRBASE | CREATE TABLE |
| 03/06/19 02:24:57,815000 | GABRIEL\Utilisateur | GABRIEL | UAIRBASE | DROP TABLE   |
| 03/06/19 02:25:14,776000 | GABRIEL\Utilisateur | GABRIEL | UAIRBASE | CREATE TABLE |

34 lignes sélectionnées.



## 5.7 L'audit unifié

---

### □ Commande **noaudit** pour l'audit unifié

```
NOAUDIT
{
  {POLICY policy {BY user [, user,...]
    |BY USER WITH GRANTED ROLES role[role,...]
  }
  |
  CONTEXT NAMESPACE namespace attribute
  [, CONTEXT NAMESPACE namespace attribute, ...]
  [BY user[, user, ...]
}
```

## 5.7 L'audit unifié

---

### □ Commande **noaudit** pour l'audit unifié

| Clause                                         | Description                                                               |
|------------------------------------------------|---------------------------------------------------------------------------|
| POLICY Policy                                  | Désigne la police d'audit unifiée à ne pas auditer                        |
| By user with granted<br>role role1, role2, ... | Ne pas auditer par utilisateurs ayant reçus les role :<br>role1, role2,.. |
| CONTEXT<br>NAMESPACE<br>namespace              | Enlève les valeurs d'un contexte dans les<br>enregistrement d'audit       |
| BY user1, [user2, ..]                          | Ne pas audit par utilisateur user1, user2, etc.                           |

## 5.7 L'audit unifié

---

### □ Commande **noaudit** pour l'audit unifié

- **Exemple 1:** désactivation de l'audit unifié sur la police d'audit maj\_etudiant\_pilote\_pol pour tous les users

```
NOAUDIT POLICY maj_etudiant_pilote_pol ;
```

- **Exemple 2:** désactivation de l'audit unifié sur la police d'audit **sys\_privs\_on\_tables\_pol** pour l'utilisateur uairbase

```
NOAUDIT POLICY sys_privs_on_tables_pol BY  
uairbase;
```

- **Exemple 3 :** Exclusion de l'inclusion des valeurs de contexte dans l'audit

```
NOAUDIT CONTEXT NAMESPACE userenv  
ATTRIBUTES current_user, db_name BY scott;
```

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- Le package **DBMS\_AUDIT\_MGMT** fournit des fonction pour administrer les enregistrement d'audit
- **Etape à suivre pour purger les enregistrements d'audit unifié**
  - 1. Initialisation : avant de commencer la purge, il est nécessaire d'initialiser les enregistrements d'audit à traiter en fonction du type d'audit. Fonction **dbms\_audit\_mgmt.init\_cleanup**
  - 2. Définir les enregistrement à purger en appelant la fonction **dbms\_audit\_mgmt.SET\_LAST\_ARCHIVE\_TIMESTAMP**
  - 3. Purge des enregistrements d'audit unifié en appelant la fonction **DBMS\_AUDIT\_MGMT.CLEAN\_AUDIT\_TRAIL**
  - 4. Automatisation de la purge des enregistrements d'audit unifié en appelant la fonction **DBMS\_AUDIT\_MGMT.CREATE\_PURGE\_JOB**

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 1. Initialisation
  - Avant de commencer la purge, il est nécessaire d'initialiser les enregistrements d'audit à traiter en fonction du type d'audit. Fonction `dbms_audit_mgmt.init_cleanup`
  - Cette fonction permet, sauf pour l'audit unifié de déplacer les enregistrements d'audit à supprimer du tablespace SYSTEM vers le tablespace SYSAUX

## 5.7 L'audit unifié

### □ Purge des enregistrements l'audit unifié

- 1. Initialisation

- Les types d'audit possibles sont représentés par les constantes suivantes:

| Constant            | Type        | Description                                                                                                                                                                                   |
|---------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AUDIT_TRAIL_ALL     | PLS_INTEGER | All audit trail types. This includes the standard database audit trail (SYS.AUD\$, SYS.FGA_LOG\$ and unified audit trail tables), operating system (OS) audit trail, and XML audit trail.     |
| AUDIT_TRAIL_AUD_STD | PLS_INTEGER | Standard database audit records in the SYS.AUD\$ table                                                                                                                                        |
| AUDIT_TRAIL_DB_STD  | PLS_INTEGER | Both standard audit (SYS.AUD\$) and FGA audit(SYS.FGA_LOG\$) records                                                                                                                          |
| AUDIT_TRAIL_FGA_STD | PLS_INTEGER | Standard database fine-grained auditing (FGA) records in the SYS.FGA_LOG\$ table                                                                                                              |
| AUDIT_TRAIL_FILES   | PLS_INTEGER | Both operating system (OS) and XML audit trails                                                                                                                                               |
| AUDIT_TRAIL_OS      | PLS_INTEGER | Operating system audit trail. This refers to the audit records stored in operating system files.                                                                                              |
| AUDIT_TRAIL_UNIFIED | PLS_INTEGER | Unified audit trail. In unified auditing, all audit records are written to the unified audit trail and are made available through the unified audit trail views, such as UNIFIED_AUDIT_TRAIL. |
| AUDIT_TRAIL_XML     | PLS_INTEGER | XML audit trail. This refers to the audit records stored in XML files.                                                                                                                        |

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 1. Initialisation
  - Appel de la fonction `dbms_audit_mgmt.init_cleanup` pour initialiser les enregistrements d'audit à supprimer pour tous les types d'audit.
  - Cette fonction possède trois paramètres :
    - `audit_trail_type` : voir le tableau précédent
    - `default_cleanup_interval`: temps par défaut en heure avant l'appel de la fonction de purge. Valeurs possibles 1 à 999
    - `Container` : Container DB : Valeurs possibles: `CONTAINER_CURRENT`, `CONTAINER_ALL`

```
BEGIN
  DBMS_AUDIT_MGMT.INIT_CLEANUP(
    audit_trail_type      =>
    DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
    default_cleanup_interval => 24
  );
END;
/
```

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 2. Définir les enregistrement à purger en appelant la fonction `dbms_audit_mgmt`.

**SET\_LAST\_ARCHIVE\_TIMESTAMP**

- Cette fonction permet de dater les enregistrements à purger. Ces enregistrements sont archivés dans un autre tablespace que System par exemple Sysaux. Exemple supprimer les archives d'il y a 7 jours
- Les paramètres de cette fonction sont :
  - **audit\_trail\_type**: type d'audit
  - **last\_archive\_time** : supprimer les archives d'avant cette date
  - **rac\_instance\_number**: designe le nr. D'instance (RAC)
  - **Container**: `container_current` ou `container_all`
  - **database\_id** : dbid de la base
  - **container\_guid**: container global unified identifier



## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 2. Définir les enregistrement à purger en appelant la fonction dbms\_audit\_mgmt.

#### SET\_LAST\_ARCHIVE\_TIMESTAMP

- Cette fonction permet de dater les enregistrements à purger. Ces enregistrements sont archivés dans un autre tablespace que System par exemple Sysaux. Exemple supprimer les archives d'il y a 7 jours

```
BEGIN
```

```
    DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP( AUDIT_TRAIL_TYPE =>  
    DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,  
    LAST_ARCHIVE_TIME => SYSTIMESTAMP -1);  
END;
```

```
/
```

```
BEGIN
```

```
    DBMS_AUDIT_MGMT.SET_LAST_ARCHIVE_TIMESTAMP( AUDIT_TRAIL_TYPE =>  
    DBMS_AUDIT_MGMT.AUDIT_TRAIL_OS,  
    LAST_ARCHIVE_TIME => SYSTIMESTAMP -1);  
END;
```

```
/
```

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 3. Purge des enregistrements d'audit unifié en appelant la fonction

DBMS\_AUDIT\_MGMT.**CLEAN\_AUDIT\_TRAIL**

```
BEGIN
DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL(
audit_trail_type =>
DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,
use_last_arch_timestamp => TRUE
);
END;
/
```

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 4. Automatisation de la purge des enregistrements d'audit unifié en appelant la fonction DBMS\_AUDIT\_MGMT.CREATE\_PURGE\_JOB
  - Afin d'automatiser les purges, il est possible de programmer des job de purge automatique BEGIN

```
DBMS_AUDIT_MGMT.CREATE_PURGE_JOB(  
audit_trail_type =>  
DBMS_AUDIT_MGMT.AUDIT_TRAIL_ALL,  
audit_trail_purge_interval => 24,  
audit_trail_purge_name =>  
'CLEANUP_AUDIT_AUD_STD',  
use_last_arch_timestamp => TRUE  
);  
END;  
/
```

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 5. Vérification datage des enregistrement à supprimer

```
select AUDIT_TRAIL, RAC_INSTANCE,  
LAST_ARCHIVE_TS  
from DBA_AUDIT_MGMT_LAST_ARCH_TS;
```

| AUDIT_TRAIL          | RAC_INSTANCE | LAST_ARCHIVE_TS                 |
|----------------------|--------------|---------------------------------|
| -----                |              |                                 |
| STANDARD AUDIT TRAIL | 0            | 02/06/19 19:03:13,000000 +00:00 |
| OS AUDIT TRAIL       | 1            | 02/06/19 19:06:07,000000 +02:00 |

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 6. Vérification de la programmation de la purge

```
col CLEANUP_TIME format A35
```

```
select * from DBA_AUDIT_MGMT_CLEAN_EVENTS;
```

| AUDIT_TRAIL          | RAC_INSTANCE | CLEANUP_TIME                      | DELETE_COUNT | WAS |
|----------------------|--------------|-----------------------------------|--------------|-----|
| -----                | -----        | -----                             | -----        | --- |
| STANDARD AUDIT TRAIL |              | 0 03/06/19 17:09:57,064000 +00:00 | 12           | NO  |

## 5.7 L'audit unifié

---

### □ Purge des enregistrements l'audit unifié

- 7. Vérification des jobs

```
set linesize 200
col JOB_NAME                format A25
col JOB_STATUS              format A8
col AUDIT_TRAIL              format A20
col JOB_FREQUENCY            format A25

select * from DBA_AUDIT_MGMT_CLEANUP_JOBS;
```

| JOB_NAME              | JOB_STAT | AUDIT_TRAIL      | JOB_FREQUENCY           | USE JOB_CON |
|-----------------------|----------|------------------|-------------------------|-------------|
| CLEANUP_AUDIT_AUD_STD | ENABLED  | ALL AUDIT TRAILS | FREQ=HOURLY;INTERVAL=24 | YES CURRENT |