Université des sciences et de la Technologie
Houari Boumediene
USTHB – Alger

Département d'Informatique

ADMINISTRATION ET TUNING DE BASES DE DONNÉES

RESPONSABLE
DR K. BOUKHALFA

CHAPITRE 4

POLITIQUES DE CONTRÔLES DES ACCÈS SOUS ORACLE

INTRODUCTION

Les données constituent une ressource essentielle et stratégique pour une organisation qui doivent donc demeurer **confidentielles** et **en sécurité**.

- La sécurité est la protection de la base de données contre les accès mal intentionnés ou accidentels.

INTRODUCTION

Comme pour la gestion de transactions, il va exister une granularité de l'objet à protéger:

- BD entière
- Une relation
- Une page
- Un champ.

CONCEPTS GÉNÉRAUX

Définition

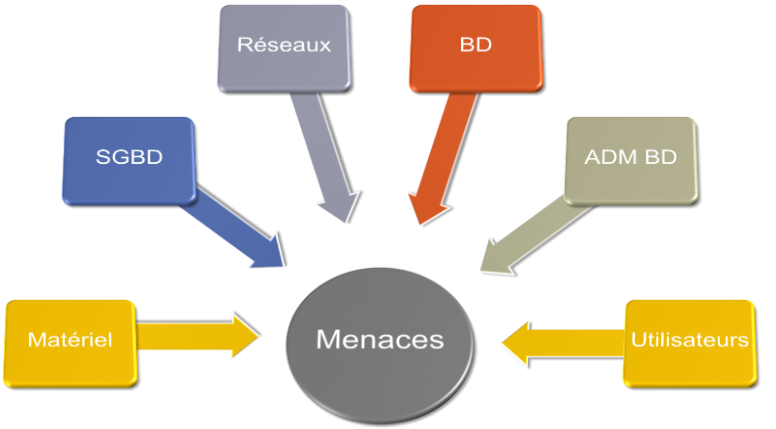
- la sécurité d'une BD est un ensemble de mécanismes de protection de la BD contre les **menaces** accidentelles ou intentionnelles

Une menace est toute situation ou tout événement intentionnel ou accidentel, qui risque de porter atteinte à un système et donc à l'organisation entière

Exemples

- Vol, fraude
- Perte de la confidentialité
- Les atteintes à la vie privée
- La perte d'intégrité, la perte de disponibilité

MENACES POTENTIELLES



MENACES POTENTIELLES

Matériels

- Incendie, inondation, échec des mécanismes de sécurité, vol d'équipement etc.

SGBD et logiciels d'application

- Echec des mécanismes de sécurité donnant un accès plus étendu que normalement, altération des programmes etc.

Réseaux de communication

- Branchement et écoute illicite
- Coupure de câbles etc.

MENACES POTENTIELLES

Bases de données

- Modification ou copie non autorisée
- Vol de données, etc.

Administrateur de la base de données

- Stratégies et procédures de sécurité inadéquates

Utilisateurs

- Utilisation par une personne non autorisée, entrée illégale d'un pirate etc.

CONTRE-MESURES
LES CONTRÔLES INFORMATIQUES

Le type de contre-mesure vont des contrôles physiques aux procédures administratives.

Les contrôles

- **Les autorisations**
- Les vues
- Les sauvegardes et restaurations
- L'intégrité
- Le cryptage

LES AUTORISATIONS

Une autorisation

- Attribution d'un droit ou d'un privilège qui permet à un sujet de disposer légitimement d'un accès à un système ou à un objet d'un système.

Une authentification est le mécanisme qui détermine si un utilisateur est celui ou celle qu'il ou qu'elle prétend être

CONTRÔLES DES DONNÉES ET DES D'ACCÈS

CONTRÔLE DES DONNÉES

- **La gestion des utilisateurs**
  - à qui on associe des espaces de stockage *(tablespaces) dans* lesquels se trouveront leurs objets (tables, index, séquences, etc.) ;
- **La gestion des privilèges**
  - permettent de donner des droits sur la base de données (privilèges système) et sur les données de la base (privilèges objets) ;
- **La gestion des rôles**
  - regroupent des privilèges système ou objets affectés par la suite à un ou plusieurs utilisateurs ;
- **La gestion des vues** ;
- **L'utilisation du dictionnaire des données**.

LES CONTRÔLES D'ACCÈS

Le contrôle d'accès repose sur l'attribution et la révocation de privilèges

Un privilège permet à un utilisateur de créer (écrire et modifier) un objet d'une BD, ou d'y accéder (lecture).

Les SGBD fournissent deux catégories d'approches de contrôle d'accès:

- **Contrôle discrétionnaire :** basé sur l'utilisateur et sur les privilèges ou autorisations
- **Contrôle obligatoire :** marquage de la donnée avec un niveau de classification

CONTRÔLES D'ACCÈS

Contrôle discrétionnaire

- Un utilisateur donné aura différents droits d'accès sur différents objets; des utilisateurs différents pourront avoir des droits différents sur le même objet

Contrôle obligatoire

- Chaque objet est marqué avec un niveau de classification et à chaque utilisateur est attribué un niveau d'habilitation

Remarque

- Dans la deuxième approche, un objet donné ne peut être accédé que si l'utilisateur a le niveau d'habilitation approprié, elle est donc plus rigide que l'approche discrétionnaire

CONTRÔLES D'ACCÈS

Les règles d'autorisation doivent être sauvegardées dans un catalogue

Une demande d'accès doit pouvoir âtre testée pour savoir si elle répond à la règle de sécurité:

- existence d'un sous-système de sécurité dans le SGBD appelé sous-système d'autorisation

Il faut que le système soit capable de détecter quelle règle doit être associé à une demande, pour cela il faut une authentification du demandeur à travers une identification et un mot de passe

Il faut un langage pour pouvoir décrire les règles d'autorisation : SQL

GESTION DES UTILISATEURS

Plusieurs utilisateurs sont créés dans la BD

Le nombre varie d'une BD à une autre

Il y a 5 catégories d'utilisateurs

- DBA : Administrateur de la BD
- Administrateur réseau (peut être le DBA)
- Développeurs
- Administrateurs d'applications
- Utilisateurs de la BD

DBA

- Il existe au moins un DBA.
- Une petite base peut n'avoir qu'un seul administrateur.
- Une base importante peut en regrouper plusieurs

Tâches :

- installation et mises à jour de la base et des outils éventuels ;
- gestion de l'espace disque et des espaces pour les données (*tablespaces) ;*
- gestion des utilisateurs et de leurs objets (s'ils ne les gèrent pas eux-mêmes) ;
- optimisation des performances ;
- sauvegardes, restaurations et archivages ;
- contact avec le support technique d'Oracle.

UTILISATEURS

- **L'administrateur réseaux**
  - se charge de la configuration de l'intergiciel (*middleware) au niveau des postes clients.*
- **Les développeurs**
  - conçoivent et mettent à jour la base. Ils peuvent aussi agir sur leurs objets (création et modification des tables, index, séquences, etc.). Ils transmettent au DBA leurs demandes spécifiques (stockage, optimisation, sécurité).

Les administrateurs d'applications :

- gèrent les données manipulées par l'application ou les applications. Pour les petites et les moyennes bases, le DBA joue ce rôle.

- **Les utilisateurs**
  - se connectent et interagissent avec la base à travers les applications ou à l'aide d'outils (interrogations pour la génération de rapports, ajouts, modifications ou suppressions d'enregistrements).

GESTION DES UTILISATEURS - OBJECTIFS

- **Création de nouveaux utilisateurs de la BD**
- **Modification et suppression d'utilisateurs existants**
- **Récupération des informations sur les utilisateurs existants**

19

CRÉATION DE SCHÉMA

- Un schéma est une collection (ou un ensemble) nommé d'objets tels que des tables, vues, clusters, procédure et packages associés à un utilisateur précis.
- Quand un utilisateur de base de données est crée, son schéma est automatiquement crée.
- Un utilisateur ne pourra alors être associé qu'à un seul schéma et réciproquement.
- Dans Oracle on pourra assimiler un utilisateur avec son schéma

GESTION DES UTILISATEURS - UTILISATEURS ET SÉCURITÉ

- **DBA définit les noms des users autorisés à accéder à une base**
- **Un domaine de sécurité définit les paramètres qui s'appliquent à un user**
- **Ces paramètres sont :**
  - Mécanisme d'authentification
  - Quotas de tablespace
  - Tablespace par défaut et tablespace temporaire
  - Verrous sur les comptes
  - Limites de ressources
  - Privilèges direct et privilèges de rôle

21

GESTION DES UTILISATEURS MÉCANISME D'AUTHENTIFICATION

Un user voulant accéder à la BD peut être authentifié par deux niveaux : OS, BD

- **OS :** le password de la BD est celui qui a été utilisé pour accéder à l'OS
  - Inconvénient: dans le cas de piratage de l'OS, la BD est à la merci du pirate
  - Syntaxe : **CREATE USER** name **IDENTIFIED EXTERNALLY;**

22

AUTHENTIFICATION

- **Oracle Server**
  - le serveur a besoin que vous confirmiez votre identité par un mot de passe.
  - Mécanisme d'identification fortement recommandé car il offre un niveau supplémentaire de sécurité
  - Syntaxe : **CREATE USER** name **IDENTIFIED BY** password;

GESTION DES UTILISATEURS - LISTE DE CONTRÔLE POUR LA CRÉATION D'USERS

1. Choisir un nom d'user et un mécanisme d'authentification
2. Identifier les tablespaces dans lesquels l'user doit stocker des objets
3. Décider les quotas pour chaque tablespace
4. Affecter un tablespace par défaut et un temporaire
5. Créer l'user
6. Accorder des privilèges et des rôles à l'user

24

SYNTAXE DE LA COMMANDE DE CRÉATION DES USERS

```
CREATE USER nom_user
  IDENTIFIED {BY password | EXTERNALLY}
  [DEFAULT TABLESPACE nom_tablespace_D]
  [TEMPORARY TABLESPACE nom_tablespace_T]
  [QUOTA {entier [K|M] | UNLIMITED} ON nom_tablespace…]
  [PASSWORD EXPIRE]
  [ACCOUNT {LOCK | UNLOCK}]
  [PROFILE {nom_profil | DEFAULT}]
```

- **UNLIMITED**: permet de spécifier que les objets d'un user peuvent utiliser autant d'espace qu'il y en a dans le tablespace
- **PASSWORD EXPIRE:** oblige l'user à réinitialiser le password lorsqu'il se connecte à la BD par l'intermédiaire de SQL*PLUS (valable juste lors de l'authentification par le Serveur Oracle).
- **ACCOUNT {LOCK | UNLOCK}:** verrouiller/déverrouiller explicitement le compte user

25

EXEMPLE

```
CREATE USER TABD
IDENTIFIED BY tabd10
DEFAULT TABLESPACE USERS
QUOTA 10M ON USERS
TEMPORARY TABLESPACE TEMP
QUOTA 5M ON TEMP
PASSWORD EXPIRE;
```

TABD est déclaré « utilisateur », ses objets (pas plus de 10 mégaoctets) seront stockés dans USERS, certaines de ses opérations nécessiteront de ranger des données dans TEMP (pas plus de 5 mégaoctets). Il devra changer son mot de passe à la première connexion.

```
CREATE USER TABD2
IDENTIFIED BY tabd22
DEFAULT TABLESPACE USERS
ACCOUNT LOCK;
```

TABD2 est déclaré « utilisateur », ses objets seront stockés dans USERS, son espace temporaire est SYSTEM.
Le compte est pour l'instant bloqué.

UTILISATEURS CONNUS

❑**SYS**

- ❑ Propriétaire des tables du dictionnaire de données.
- ❑ Il est préférable de ne jamais se connecter sous SYS en ligne

❑**SYSTEM**

- ❑ Un utilisateur DBA qu'Oracle offre.
- ❑ Il permettra d'effectuer les tâches administratives en ligne ou par la console Enterprise Manager

GESTION DES VERROUS ET DES PASSWORD

Syntaxe:

```
ALTER USER username
IDENTIFIED {BY password | EXTERNALLY}
[PASSWORD EXPIRE]
[ACCOUNT {LOCK | UNLOCK}];
```

Cette commande est utile dans les cas suivants:

- ❑ Réinitialisation du pasword dans le cas de l'oubli
- ❑ Pour déverrouiller un compte qui a été verrouillé
- ❑ Pour verrouiller un compte de façon explicite

28

MODIFICATION DES QUOTAS DE TABLESPACE DES USERS

Il peut être nécessaire de modifier les quotas de tablespace dans les cas suivants:

- Lorsque les tables d'un user montrent une croissance imprévue
- Lorsqu'une application est améliorée et nécessite des tables ou index supplémentaires

Syntaxe:

ALTER USER username
[**DEFAULT TABLESPACE** nom_tablespace_D]
[TEMPORARY TABLESPACE nom_tablespace_T]
[QUOTA {entier [K|M] | UNLIMITED} ON nom_tablespace…]

Exemple:

```
ALTER USER TABD
QUOTA 100 ON tablespace1;
```

29

GESTION DES UTILISATEURS - SUPPRESSION D'UN USER

Syntaxe:

- DROP USER username [CASCADE];

Règles

- L'option CASCADE supprime tous les objets du schéma avant de supprimer l'user
- Il est impossible de supprimer un user connecté au serveur Oracle

30

GESTION DES USERS

Plusieurs vues du dictionnaire existent pour donner des informations sur les caractéristiques des comptes:

- User_users, All_users, DBA_users
- L'accès à ces vues se fait grâce à l'ordre SELECT

31

LES PROFILES

PROFIL

- Un profil regroupe des caractéristiques système (ressources) qu'il est possible d'affecter à un ou plusieurs utilisateurs.
- Un profil est identifié par son nom.
- Un profil est :
  - créé par CREATE PROFILE
  - modifié par ALTER PROFILE
  - supprimé par DROP PROFILE.
- Il est affecté à un utilisateur lors de sa création par CREATE USER ou après que l'utilisateur est créé par ALTER USER.
- Le profil DEFAULT est affecté par défaut à chaque utilisateur si aucun profil défini n'est précisé.

GESTION DES PROFILS - OBJECTIFS

- Création et allocation des profils aux users
- Contrôle de la consommation des ressources avec les profils
- Modification et suppression des profils
- Gestion des mots de passe avec les profils
- Récupération d'information sur les profils

34

GESTION DES RESSOURCES À L'AIDE DES PROFILS

Pour gérer l'utilisation des ressources à l'aide des profils, il faut suivre ces étapes:

- Créez un profil pour déterminer les limites de ressources
- Affectez-les à l'user avec soit la commande CREATE USER ou ALTER USER
- Appliquez les limites de ressources avec ALTER SYSTEM

35

CRÉATION D'UN PROFIL

Syntaxe:

```
CREATE PROFILE profilename LIMIT
 [SESSIONS_PER_USER max_value]
 [CPU_PER_SESSION max_value]
[CONNECT_TIME max_value]
[IDLE_TIME max_value];
max_value:={integer | UNLIMITED | DEFAULT};
```

Exemple:

```
CREATE PROFILE developer_profile LIMIT
  SESSIONS_PER_USER 2
  CPU_PER_SESSION 10000
    CONNECT_TIME 480
    IDLE_TIME 60;
```

36

AFFECTATION DE PROFILS À UN USER

- Affectation se fait grâce à la commande CREATE USER ou ALTER USER
- Un seul profil peut être affecté à chaque user
- Les affectations de profil n'ont aucun effet sur les sessions en cours
- Dans la cas où on n'affecte pas de profil en créant un user, le profil DEFAULT lui est automatiquement affecté

37

ACTIVATION DES LIMITES DE RESSOURCES

L'activation se fait:

- En initialisant le paramètre RESOURCE_LIMIT à TRUE et puis en redémarrant l'instance.
- Ou en activant le paramètre avec la commande ALTER SYSTEM
- **Syntaxe:**
  - ALTER SYSTEM SET RESSOURCE_LIMIT=TRUE;
- Pour voir l'état de paramètre RESSOURCE_LIMIT
  - show parameter resource_limit

38

MODIFICATION D'UN PROFIL

Syntaxe:

```
ALTER PROFILE profilname LIMIT
   [SESSIONS_PER_USER max_value]
   [CPU_PER_SESSION max_value]
    [CONNECT_TIME max_value]
    [IDLE_TIME max_value];
```

Exemple:

```
ALTER PROFIL developer_profile LIMIT
  SESSIONS_PER_USER 5;
```

39

SUPPRESSION D'UN PROFIL

❑**Syntaxe:**

- ❑ DROP PROFILE profilename;

❑**Règles**

- ❑ Le profil DEFAULT ne peut pas être supprimé
- ❑ Lorsqu'un profil est supprimé, cette modification ne s'applique qu'aux nouvelles sessions et non pas aux sessions en cours.

40

AFFICHAGE DES LIMITES DE RESSOURCES

❑Plusieurs vues du dictionnaire existent pour afficher les limites de ressources:

- ❑ DBA_PROFILES, DBA_users

SELECT p.profile, p.resource_name, p_limit FROM dba_users u, dba_profiles p Where p.profile=u.profile and username='TABD';

41

GESTION DES MOTS DE PASSE À L'AIDE DES PROFILS

❑Pour accroître la sécurité des BD, Oracle a défini plusieurs fonctionnalités:

- ❑ Gestion des verrous
- ❑ Vieillissement et expiration des passwords
  - ❑ Définition de la durée de vie d'un password
- ❑ Journal des passwords
  - ❑ Afin de ne pas utiliser le même password
- ❑ Vérifier la complexité des passwords

42

CRÉATION D'UN PROFIL: PARAMÈTRES DES MOTS DE PASSE

Syntaxe:

CREATE PROFILE profilename LIMIT

[FAILED_LOGIN_ATTEMPTS max_value]

[PASSWORD_LIFE_TIME max_value]

[PASSWORD_REUSE_TIME max_value]

[PASSWORD_GRACE_TIME max_value]

[PASSWORD_VERIFY_FUNCTION PlsqlFunction];

43

FONCTION DE VÉRIFICATION DU MOT DE PASSE

- Longueur minimal de 4 caractères
- Password différent du login
- Password doit contenir au moins un caractère alphabétique, numérique et un spécial
- Différent du dernier password par au moins 3 caractères
- Oracle fournit une fonction PL/SQL par défaut appelé verify_function par le script utlpwdmg.sql et qui doit être exécuté dans le schéma SYS

44

AFFICHAGE DE L'INFORMATION SUR LE PASSWORD

DBA_USERS

- Profil
- Nomutil
- Etat_compte
- Date_verrou
- Date_exp

DBA_PROFILES

- Profil
- Nom_ressource

45

GESTION DES PRIVILÈGES - OBJECTIFS

- **Identification des privilèges système et objet**
- **Attribution et révocation des privilèges**

46

GESTION DES PRIVILÈGES

❑**Deux types de privilèges**

- **Privilège système:** permet aux users d'effectuer des opérations particulière dans la BD. Ces opérations comprennent la création, la suppression et la modification de tables, de vues, de procédures etc.
- **Privilège objet:** permet aux users d'accéder à un objet et de le manipuler.

47

PRIVILÈGE SYSTÈME

❑**Environ 80 privilèges système**

❑**Classé comme suit:**

- Privilège permettant des opérations sur l'ensemble du système (create tablespace…)
- Privilège permettant la gestion des objets dans le schéma propre à un user (create table, create procedure)
- Privilège permettant la gestion des objets dans n'importe quel schéma (create any table, create any procedure)

❑**La commande GRANT ajoute un privilège à un user ou un rôle**

❑**La commande REVOKE supprime les privilèges**

48

PROVILEGES SYSTÈMES

Privilège	ALTER	CREATE	DROP	Autre
INDEX		×		QUERY REWRITE (index basés sur des fonctions)
ANY INDEX	×	×	×	
TABLE		×		
ANY TABLE	×	×	×	BACKUP, INSERT, DELETE, SELECT, UPDATE
USER	×	×	×	BECOME (pour des importations de bases)
PROFILE	×	×	×	
SEQUENCE		×		
ANY SEQUENCE	×	×	×	SELECT (pour utiliser toute séquence)
ANY OBJECT PRIVILEGE				pour manipuler tout objet

ATTRIBUTION DE PRIVILÈGES SYSTÈME

❑**Syntaxe:**

GRANT {priv_système|rôle} [, {priv_système|rôle}]

TO {username|rôle|PUBLIC} [, {username|rôle|PUBLIC}]

[WITH ADMIN OPTION];

WITH ADMIN OPTION: permet au bénéficiaire d'accorder à son tour le privilège ou le rôle à d'autres users ou rôles

❑**Affichage des privilèges systèmes**

- ❑ DBA_SYS_PRIVS

50

RÉVOCATION DES PRIVILÈGES SYSTÈME

❑**Syntaxe:**

REVOKE {priv_système|rôle} [, {priv_système|rôle}]

FROM {username|rôle|PUBLIC} [, {username|rôle|PUBLIC}]

❑**Exemple:**

- ❑ Revoke create table from TABD;

51

PRIVILÈGE OBJET

Privilège Ojet	Table	Vue	Séquence	procédure
Alter	*		*	
Delete	*	*		
Execute				*
index	*			
Insert	*	*		
References	*			
Select	*	*	*	
update	*	*		

52

ATTRIBUTIONS DE PRIVILÈGES OBJET

❑**Syntaxe:**

GRANT {priv_objet [(liste_colonne)] [, priv_objet [(liste_colonne)]] | ALL [PRIVILEGES]}

ON [schéma.]objet

TO {username|rôle|PUBLIC} [, {username|rôle|PUBLIC}]

[WITH GRANT OPTION];

WITH GRANT OPTION: permet au bénéficiaire d'accorder à son tour les privilèges sur l'objet à d'autres users ou rôles

❑**Exemple:**

- Grant update (ename,sal) on emp to TABD;

❑**Affichage des privilèges objets**

- DBA_TAB_PRIVS

53

EXEMPLES

Accorder à l'utilisateur dont l'identification est *directeur* tous les privilèges sur la table *personnel.*

GRANT ALL PRIVILEGES

ON personnel

TO directeur

EXEMPLES

Accorder aux utilisateurs sous-directeur et chef-service les privilèges SELECT et UPDATE sur la colonne salaire de la table personnel

GRANT SELECT, UPDATE(salaire)

ON personnel

TO sous-directeur, chef-service

EXEMPLES

Accorder à tous les utilisateurs le privilège SELECT sur la table grille-salaire

GRANT SELECT

ON grille-salaire

TO PUBLIC

RETIRER UN PRIVILÈGE

REVOKE [GRANT OPTION FOR] (liste de privilèges/ ALL PRIVILEGES]

ON nom objet

FROM (liste autorisations/ PUBLIC) [RESTRICT/CASCADE]

Si un utilisateur A donne un certain privilège à un utilisateur B, A peut aussi révoquer ce privilège:

- **GRANT OPTION FOR** permet de supprimer tous les privilèges transmis par la clause **WITH GRANT OPTION**

ALL PRIVILEGES font références à tous les privilèges accordés à un utilisateur

EXEMPLES

Retirer à tous les utilisateurs le privilège SELECT sur la table grille-salaire

REVOKE SELECT

ON grille-salaire

FROM PUBLIC

Retirer à l'utilisateur chef-service tous les privilèges accordés sur la table personnel

REVOKE ALL PRIVILEGES

ON personnel

FROM chef-service

RESTRICT ET CASCADE

Supposons p un privilège, A accorde p à B, qui à son tour l'accorde à C

Si A révoque p à B

- **RESTRICT** : le privilège p détenu par C n'est pas abandonné.
- **CASCADE**: le privilège p détenu par C doit être abandonné:
- Cependant si le privilège p est aussi transmis par un autre utilisateur D à C alors, il peut garder celui-ci.

GESTION DES RÔLES

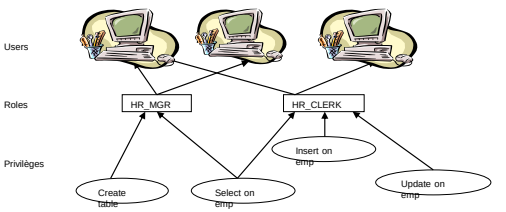
GESTION DES RÔLES - OBJECTIFS

- Création et modification des rôles
- Contrôle de la disponibilité des rôles
- Suppression des rôles
- Affichage d'information sur les rôles

61

RÔLES

- Les rôles sont des groupes nommés de privilèges accordés aux users ou à d'autres rôles.
- Conçu pour faciliter l'administration des privilèges d'une BD



62

AVANTAGES DES RÔLES

- **Gestion simplifiée des privilèges**
- **Disponibilité sélective des privilèges**
  - L'activation et la désactivation des rôles permettent d'accorder ou retirer temporairement des privilèges

63

CRÉATION DES RÔLES

- **Syntaxe**
  - CREATE ROLE rolename [NOT IDENTIFIED | IDENTIFIED { BY password}]
- **Exemple:**
  - Create role hr_clerk1;
  - Create role hr_clerk identified by bonus;

64

ACTIVATION ET DÉSACTIVATION DES RÔLES

Syntaxe:

```
SET ROLE { rolename [IDENTIFIED BY password] {, rolename [IDENTIFIED BY password]
         | ALL [EXCEPT rolename [, rolename] ..]
         | NONE }
```

IDENTIFIED BY password : indique le password exigé en activant le rôle

ALL: active tous les rôles accordé à l'user actuel, à l'exception de ceux mentionnés dans la clause EXCEPT. Non utilisable pour activer des rôles avec des mots de passe

EXCEPT rôle : n'active pas ces rôles

NONE: désactive tous les rôles de la session en cours

Exemple:

- SET ROLE hr_clerk;
- SET ROLE sales_clerk IDENTIFIED BY commission;
- SET ROLE ALL EXCEPT sales_clerk;
- SET ROLE NONE;

65

RÔLES PRÉDÉFINIS

❑Les rôles suivants sont automatiquement définis pour les BDs

Oracle:

- CONNECT
- RESOURCE
- DBA : tous le privilèges WITH ADMIN OPTION
- EXP_FULL_DATABASE : Privilèges d'export de la BD.
- IMP_FULL_DATABASE :Privilèges d'import de la BD.
- DELETE_CATALOG_ROLE, EXECUTE_CATALOG_ROLE, SELECT_CATALOG_ROLE: ont pour fonction de permettre l'accès aux vues du dictionnaire de datas

66

AFFICHAGE DES INFORMATIONS CONCERNANT LES RÔLES

Les vues sont:

- Dba_roles : tous les rôles existant dans la BD
- Dba_role_privs : rôles accordés aux users et aux roles
- Role_role_privs : rôles accordés aux rôles

67

LES CONTRÔLES D'ACCÈS DISCRÉTIONNAIRES

Gestion en SQL des privilèges grâce aux commandes :

GRANT(accorder) et REVOKE (révoquer)