Gestion des Droits

Oracle Database

USTHB - Faculté d'Informatique

Module : ASGBD

M1 SII/IL/MIV

Année 2025/2026

TP3 : Privilèges d'accès à la base de données

Cours Complet - Gestion des Droits et Sécurité Oracle

1. Introduction à la Sécurité Oracle

La sécurité dans Oracle Database repose sur trois piliers :

- Authentification : Vérifier l'identité des utilisateurs
- Autorisation : Contrôler l'accès aux ressources
- Audit : Tracer les actions effectuées

2. Architecture de Stockage Oracle

2.1 Tablespaces

Un tablespace est un espace de stockage logique qui contient les objets de la base de données (tables, index, etc.).

Types de tablespaces :

- Tablespace permanent : Stocke les données persistantes (tables, index)
- Tablespace temporaire : Stocke les données temporaires (tri, jointures)

Création d'un tablespace permanent :

```
    CREATE TABLESPACE agricolTBS
DATAFILE 'C:\oracle\data\agricol.dbf'
SIZE 100M
AUTOEXTEND ON NEXT 10M
MAXSIZE 500M;
```

Création d'un tablespace temporaire :

```
    CREATE TEMPORARY TABLESPACE agricolTempTBS
TEMPFILE 'C:\oracle\temp\agricol_temp.dbf'
SIZE 50M
AUTOEXTEND ON NEXT 5M
MAXSIZE 200M;
```

Paramètres importants :

- SIZE : Taille initiale du fichier
- AUTOEXTEND ON : Extension automatique
- NEXT : Taille de chaque extension
- MAXSIZE : Taille maximale

3. Gestion des Utilisateurs

3.1 Création d'un utilisateur

Syntaxe complète :

```
    CREATE USER nom_utilisateur
IDENTIFIED BY mot_de_passe
```

```
DEFAULT TABLESPACE nom_tablespace
TEMPORARY TABLESPACE nom_tablespace_temp
QUOTA taille ON nom_tablespace
PROFILE nom_profil
PASSWORD EXPIRE
ACCOUNT LOCK | UNLOCK;
```

Exemple pratique :

```
     CREATE USER DBAGRICOL
IDENTIFIED BY mdp123
DEFAULT TABLESPACE agricolTBS
TEMPORARY TABLESPACE agricolTempTBS
QUOTA UNLIMITED ON agricolTBS;
```

3.2 Modification d'un utilisateur

```
-- Changer le mot de passe
     ALTER USER DBAGRICOL IDENTIFIED BY nouveau_mdp;

-- Modifier le quota
     ALTER USER DBAGRICOL QUOTA 200M ON agricolTBS;

-- Verrouiller/déverrouiller le compte
     ALTER USER DBAGRICOL ACCOUNT LOCK;
     ALTER USER DBAGRICOL ACCOUNT UNLOCK;
```

3.3 Suppression d'un utilisateur

```
-- Suppression simple
     DROP USER nom_utilisateur;

-- Suppression avec tous ses objets
     DROP USER nom_utilisateur CASCADE;
```

4. Les Privilèges Oracle

4.1 Types de privilèges

Il existe deux catégories de privilèges :

A. Privilèges Système
Permettent d'effectuer des actions au niveau de la base de données.

Principaux privilèges système :

- CREATE SESSION : Se connecter à la base
- CREATE TABLE : Créer des tables
- CREATE VIEW : Créer des vues
- CREATE INDEX : Créer des index
- CREATE USER : Créer des utilisateurs
- CREATE ROLE : Créer des rôles
- ALTER USER : Modifier des utilisateurs
- DROP USER : Supprimer des utilisateurs

B. Privilèges Objet

Permettent d'effectuer des actions sur des objets spécifiques (tables, vues, etc.).

Principaux privilèges objet :

- SELECT : Lire les données
- INSERT : Insérer des données
- UPDATE : Modifier des données
- DELETE : Supprimer des données
- ALTER : Modifier la structure
- INDEX : Créer des index
- REFERENCES : Créer des clés étrangères
- EXECUTE : Exécuter (procédures, fonctions)

4.2 Attribution de privilèges

Syntaxe pour les privilèges système :

```
GRANT privilege_systeme TO utilisateur [WITH ADMIN OPTION];
```

Exemples :

```
-- Donner le droit de connexion
GRANT CREATE SESSION TO Admin;

-- Donner plusieurs privilèges
GRANT CREATE TABLE, CREATE VIEW TO Admin;

-- Donner tous les privilèges
GRANT ALL PRIVILEGES TO DBAGRICOL;

-- Avec option de transmission
GRANT CREATE USER TO Admin WITH ADMIN OPTION;
```

Syntaxe pour les privilèges objet :

```
GRANT privilege_objet ON schema.objet TO utilisateur [WITH GRANT OPTION];
```

Exemples :

```
-- Droit de lecture sur une table
GRANT SELECT ON DBAGRICOL.AGRICULTEUR TO Admin;

-- Plusieurs droits
GRANT SELECT, INSERT, UPDATE ON DBAGRICOL.PRODUCTION TO Admin;

-- Tous les droits sur une table
GRANT ALL ON DBAGRICOL.MARCHE TO Admin;

-- Avec option de transmission
GRANT SELECT ON DBAGRICOL.PRODUIT TO Admin WITH GRANT OPTION;

-- Droit de créer des index
GRANT INDEX ON DBAGRICOL.PRODUIT TO Admin;
```

4.3 Révocation de privilèges

Pour les privilèges système :

```
REVOKE privilege_systeme FROM utilisateur;
```

Exemples :

```
REVOKE CREATE TABLE FROM Admin;
REVOKE CREATE USER, CREATE VIEW FROM Admin;
```

Pour les privilèges objet :

```
REVOKE privilege_objet ON schema.objet FROM utilisateur;
```

Exemples :

```
REVOKE SELECT ON DBAGRICOL.AGRICULTEUR FROM Admin;
REVOKE INSERT, UPDATE ON DBAGRICOL.PRODUCTION FROM Admin;
REVOKE INDEX ON DBAGRICOL.PRODUIT FROM Admin;
```

4.4 Options WITH GRANT OPTION et WITH ADMIN OPTION

```
WITH GRANT OPTION (privilèges objet)
```

Permet à l'utilisateur de transmettre le privilège à d'autres utilisateurs.

```
-- Admin peut maintenant donner le droit SELECT à d'autres
GRANT SELECT ON DBAGRICOL.AGRICULTEUR TO Admin WITH GRANT OPTION;
```

```
Cascade de révocation : Si vous révoquez un privilège donné avec WITH GRANT
OPTION,
```

tous les privilèges transmis en cascade sont également révoqués.

WITH ADMIN OPTION (privilèges système)

Permet à l'utilisateur de transmettre le privilège système à d'autres.

```
-- Admin peut maintenant créer d'autres utilisateurs
GRANT CREATE SESSION TO Admin WITH ADMIN OPTION;
```

Pas de cascade : La révocation d'un privilège système ne révoque pas les privilèges transmis.

5. Les Rôles

5.1 Concept de rôle

Un rôle est un ensemble nommé de privilèges. Les rôles simplifient la gestion des privilèges.

Avantages :

- Gestion centralisée des privilèges
- Facilite l'administration
- Modification facile des droits pour un groupe d'utilisateurs

5.2 Création d'un rôle

Syntaxe :

```
CREATE ROLE nom_role
[NOT IDENTIFIED | IDENTIFIED BY mot_de_passe];
```

Exemples :

```
-- Rôle sans mot de passe
     CREATE ROLE MARCHE_MANAGER;

-- Rôle avec mot de passe
     CREATE ROLE GESTIONNAIRE IDENTIFIED BY mdp_role;
```

5.3 Attribution de privilèges à un rôle

```
-- Privilèges de lecture
     GRANT SELECT ON DBAGRICOL.AGRICULTEUR TO MARCHE_MANAGER;
     GRANT SELECT ON DBAGRICOL.PRODUCTION TO MARCHE_MANAGER;

-- Privilèges de modification
     GRANT INSERT, UPDATE, DELETE ON DBAGRICOL.MARCHE TO MARCHE_MANAGER;
```

5.4 Assignation d'un rôle à un utilisateur

```
     GRANT nom_role TO utilisateur;
```

Exemple :

```
     GRANT MARCHE_MANAGER TO Admin;
```

5.5 Révocation d'un rôle

```
     REVOKE nom_role FROM utilisateur;
```

5.6 Rôles prédéfinis Oracle

Oracle propose des rôles prédéfinis :

- CONNECT : Privilèges de connexion basiques
- RESOURCE : Créer des objets (tables, vues, etc.)
- DBA : Tous les privilèges d'administration

Exemple :

```
     GRANT CONNECT, RESOURCE TO nouvel_utilisateur;
```

6. Les Profils

6.1 Concept de profil

Un profil définit des limites sur les ressources système et les politiques de mots de passe

pour un utilisateur.

6.2 Création d'un profil

Syntaxe :

```
     CREATE PROFILE nom_profil LIMIT
    -- Paramètres de ressources
```

```
    SESSIONS_PER_USER valeur
    CPU_PER_SESSION valeur
    CPU_PER_CALL valeur
    CONNECT_TIME valeur
    IDLE_TIME valeur
    LOGICAL_READS_PER_SESSION valeur
    LOGICAL_READS_PER_CALL valeur
    PRIVATE_SGA valeur
    -- Paramètres de mot de passe
    FAILED_LOGIN_ATTEMPTS valeur
    PASSWORD_LIFE_TIME valeur
    PASSWORD_REUSE_TIME valeur
    PASSWORD_REUSE_MAX valeur
    PASSWORD_LOCK_TIME valeur
    PASSWORD_GRACE_TIME valeur;
```

Exemple complet (selon le TP) :

```
     CREATE PROFILE AGRICOL_Profil LIMIT
    SESSIONS_PER_USER 3
    CPU_PER_CALL 3500
    CONNECT_TIME 90
    LOGICAL_READS_PER_CALL 1200
    PRIVATE_SGA 25K
    IDLE_TIME 30
    FAILED_LOGIN_ATTEMPTS 5
    PASSWORD_LIFE_TIME 50
    PASSWORD_REUSE_TIME 40
    PASSWORD_LOCK_TIME 1
    PASSWORD_GRACE_TIME 5;
```

6.3 Paramètres de ressources

SESSIONS_PER_USER : Nombre de sessions concurrentes
CPU_PER_SESSION : Temps CPU total pour une session (centièmes de seconde)
CPU_PER_CALL : Temps CPU par appel système (centièmes de seconde)
CONNECT_TIME : Durée maximale d'une session (minutes)
IDLE_TIME : Temps d'inactivité autorisé (minutes)
LOGICAL_READS_PER_SESSION : Blocs lus pendant la session
LOGICAL_READS_PER_CALL : Blocs lus par appel
PRIVATE_SGA : Mémoire privée dans la SGA (Ko ou Mo)

6.4 Paramètres de mot de passe

FAILED_LOGIN_ATTEMPTS : Tentatives avant blocage du compte
PASSWORD_LIFE_TIME : Durée de validité du mot de passe (jours)
PASSWORD_REUSE_TIME : Délai avant réutilisation d'un mot de passe (jours)
PASSWORD_REUSE_MAX : Nombre de changements avant réutilisation
PASSWORD_LOCK_TIME : Durée de blocage après échecs de connexion (jours)
PASSWORD_GRACE_TIME : Période de grâce après expiration (jours)

Note : Si PASSWORD_REUSE_TIME est un entier, alors PASSWORD_REUSE_MAX doit être UNLIMITED

et vice-versa.

6.5 Affectation d'un profil

```
-- Lors de la création
     CREATE USER Admin IDENTIFIED BY mdp PROFILE AGRICOL_Profil;

-- Modification ultérieure
     ALTER USER Admin PROFILE AGRICOL_Profil;
```

6.6 Modification et suppression d'un profil

```
-- Modifier un profil
     ALTER PROFILE AGRICOL_Profil LIMIT IDLE_TIME 45;

-- Supprimer un profil
     DROP PROFILE AGRICOL_Profil;

-- Supprimer avec réaffectation au profil DEFAULT
     DROP PROFILE AGRICOL_Profil CASCADE;
```

7. Le Dictionnaire de Données

Le dictionnaire de données Oracle contient des informations sur tous les objets de la base.

7.1 Vues principales pour la gestion des droits

Vérifier les tablespaces :

```
-- Tous les tablespaces
     SELECT tablespace_name, status FROM DBA_TABLESPACES;

-- Fichiers de données
     SELECT file_name, tablespace_name, bytes/1024/1024 AS size_mb
FROM DBA_DATA_FILES;
```

Vérifier les utilisateurs :

```
-- Liste des utilisateurs
     SELECT username, account_status, default_tablespace, profile
FROM DBA_USERS;

-- Quotas des utilisateurs
     SELECT username, tablespace_name, max_bytes
FROM DBA_TS_QUOTAS;
```

Vérifier les privilèges système :

```
-- Privilèges système d'un utilisateur
     SELECT * FROM DBA_SYS_PRIVS WHERE grantee = 'ADMIN';

-- Privilèges système accordés par un utilisateur
     SELECT * FROM USER_SYS_PRIVS;
```

Vérifier les privilèges objet :

```
-- Privilèges objet accordés à un utilisateur
     SELECT * FROM DBA_TAB_PRIVS WHERE grantee = 'ADMIN';

-- Privilèges objet sur vos objets
     SELECT * FROM USER_TAB_PRIVS_MADE;

-- Privilèges objet reçus
     SELECT * FROM USER_TAB_PRIVS_RECD;
```

Vérifier les rôles :

```
-- Tous les rôles
     SELECT * FROM DBA_ROLES;

-- Rôles d'un utilisateur
     SELECT * FROM DBA_ROLE_PRIVS WHERE grantee = 'ADMIN';

-- Privilèges d'un rôle
     SELECT * FROM ROLE_SYS_PRIVS WHERE role = 'MARCHE_MANAGER';

     SELECT * FROM ROLE_TAB_PRIVS WHERE role = 'MARCHE_MANAGER';
```

Vérifier les profils :

```
-- Tous les profils
     SELECT * FROM DBA_PROFILES;

-- Profil d'un utilisateur spécifique
     SELECT * FROM DBA_PROFILES WHERE profile = 'AGRICOL_PROFIL';
```

Vérifier les tables :

```
-- Tables d'un schéma
     SELECT table_name, tablespace_name
FROM DBA_TABLES WHERE owner = 'DBAGRICOL';

-- Vos propres tables
     SELECT table_name FROM USER_TABLES;
```

8. Cas Pratiques et Résolution de Problèmes

8.1 Problème : Impossible de se connecter

```
     Erreur : ORA-01045: user ADMIN lacks CREATE SESSION privilege
```

Solution :

```
-- Se connecter en tant qu'utilisateur privilégié
     GRANT CREATE SESSION TO Admin;
```

8.2 Problème : Impossible d'accéder aux tables d'un autre schéma

```
Erreur : ORA-00942: table or view does not exist
```

Raisons possibles :
1. L'utilisateur n'a pas le privilège SELECT
2. La table n'existe pas

3. Mauvaise syntaxe (oubli du préfixe schéma)

Solutions :

```
-- Vérifier l'existence de la table
     SELECT * FROM DBA_TABLES WHERE table_name = 'AGRICULTEUR';

-- Donner le privilège
     GRANT SELECT ON DBAGRICOL.AGRICULTEUR TO Admin;

-- Utiliser la syntaxe complète
     SELECT * FROM DBAGRICOL.AGRICULTEUR;
```

8.3 Problème : Impossible de créer un index

Erreur : Manque de privilège INDEX

Solution :

```
-- Donner le privilège INDEX
     GRANT INDEX ON DBAGRICOL.PRODUIT TO Admin;

-- Créer l'index
     CREATE INDEX NAMEPROD_IX ON DBAGRICOL.PRODUIT(NOM);
```

8.4 Problème : Impossible de créer une vue

Raisons :

- Manque du privilège CREATE VIEW
- Manque des privilèges SELECT sur les tables source

Solution :

```
-- Donner le privilège système
     GRANT CREATE VIEW TO Admin;

     -- Donner les privilèges SELECT sur les tables nécessaires
     GRANT SELECT ON DBAGRICOL.AGRICULTEUR TO Admin;
     GRANT SELECT ON DBAGRICOL.PRODUCTION TO Admin;
     GRANT SELECT ON DBAGRICOL.PRODUIT TO Admin;

-- Créer la vue
     CREATE VIEW AGRI_PROD AS
     SELECT a.nom, a.prenom, p.nom_produit
FROM DBAGRICOL.AGRICULTEUR a
JOIN DBAGRICOL.PRODUCTION pr ON a.id = pr.id_agriculteur
JOIN DBAGRICOL.PRODUIT p ON pr.id_produit = p.id;
```

9. Bonnes Pratiques de Sécurité

9.1 Principe du moindre privilège

- N'accordez que les privilèges strictement nécessaires
- Évitez d'utiliser GRANT ALL sauf pour les administrateurs

9.2 Utilisation des rôles

- Créez des rôles par fonction métier
- Assignez des privilèges aux rôles, pas directement aux utilisateurs
- Facilite la gestion et l'audit

9.3 Gestion des mots de passe

- Utilisez des profils avec des politiques de mot de passe strictes
- Définissez PASSWORD_LIFE_TIME pour forcer le changement régulier
- Limitez les tentatives de connexion avec FAILED_LOGIN_ATTEMPTS

9.4 Surveillance et audit

- Vérifiez régulièrement les privilèges accordés
- Révoquez les privilèges inutilisés
- Utilisez les vues du dictionnaire pour auditer les droits

9.5 Séparation des environnements

- Utilisez des tablespaces distincts par application
- Créez des utilisateurs spécifiques par application
- Ne partagez jamais les mots de passe

10. Exercices Pratiques

Exercice 1 : Création complète d'un environnement

```
-- 1. Créer les tablespaces
     CREATE TABLESPACE vente_tbs DATAFILE 'vente.dbf' SIZE 100M;
     CREATE TEMPORARY TABLESPACE vente_temp TEMPFILE 'vente_temp.dbf' SIZE 50M;

-- 2. Créer un utilisateur administrateur
     CREATE USER DBA_VENTE
IDENTIFIED BY mdp123
DEFAULT TABLESPACE vente_tbs
TEMPORARY TABLESPACE vente_temp
QUOTA UNLIMITED ON vente_tbs;

-- 3. Donner tous les privilèges
     GRANT ALL PRIVILEGES TO DBA_VENTE;

-- 4. Créer un utilisateur standard
     CREATE USER Vendeur
IDENTIFIED BY vendeur123
DEFAULT TABLESPACE vente_tbs
TEMPORARY TABLESPACE vente_temp
QUOTA 50M ON vente_tbs;

-- 5. Privilèges de base
     GRANT CREATE SESSION, CREATE TABLE TO Vendeur;
```

Exercice 2 : Gestion avec rôles

```
-- 1. Créer un rôle consultant
     CREATE ROLE CONSULTANT;
```

```
-- 2. Attribuer des privilèges de lecture
    GRANT SELECT ON DBA_VENTE.CLIENT TO CONSULTANT;
    GRANT SELECT ON DBA_VENTE.COMMANDE TO CONSULTANT;

-- 3. Créer un rôle gestionnaire
    CREATE ROLE GESTIONNAIRE;

-- 4. Inclure le rôle consultant
    GRANT CONSULTANT TO GESTIONNAIRE;

-- 5. Ajouter des privilèges de modification
    GRANT INSERT, UPDATE ON DBA_VENTE.COMMANDE TO GESTIONNAIRE;

-- 6. Assigner aux utilisateurs
    GRANT CONSULTANT TO user1;
    GRANT GESTIONNAIRE TO user2;
```

Exercice 3 : Création d'un profil restrictif

```
    CREATE PROFILE PROFIL_STAGIAIRE LIMIT
   SESSIONS_PER_USER 2
   CONNECT_TIME 120
   IDLE_TIME 15
   FAILED_LOGIN_ATTEMPTS 3
   PASSWORD_LIFE_TIME 30
   PASSWORD_LOCK_TIME 1;

    ALTER USER Stagiaire PROFILE PROFIL_STAGIAIRE;
```

11. Résumé des Commandes Essentielles

Connexion

```
CONNECT username/password@database
```

Tablespaces

```
    CREATE TABLESPACE nom DATAFILE 'fichier' SIZE taille;
    CREATE TEMPORARY TABLESPACE nom TEMPFILE 'fichier' SIZE taille;
```

Utilisateurs

```
    CREATE USER nom IDENTIFIED BY mdp DEFAULT TABLESPACE tbs;
    ALTER USER nom IDENTIFIED BY nouveau_mdp;
    DROP USER nom CASCADE;
```

Privilèges

```
    GRANT privilege TO user [WITH GRANT/ADMIN OPTION];
    REVOKE privilege FROM user;
```

Rôles

```
CREATE ROLE nom;
GRANT privilege TO role;
GRANT role TO user;
```

Profils

```
CREATE PROFILE nom LIMIT parametre valeur;
ALTER USER nom PROFILE profil;
```

Consultation

```
SELECT * FROM DBA_USERS;
SELECT * FROM DBA_SYS_PRIVS WHERE grantee = 'USER';
SELECT * FROM DBA_TAB_PRIVS WHERE grantee = 'USER';
SELECT * FROM DBA_ROLE_PRIVS WHERE grantee = 'USER';
```

Conclusion

La gestion des droits dans Oracle est un système complet et hiérarchisé qui permet de :

- Contrôler finement l'accès aux données
- Organiser les privilèges via des rôles
- Limiter les ressources via des profils
- Auditer et tracer les accès

La maîtrise de ces concepts est essentielle pour tout administrateur de bases de données Oracle.

Cours préparé pour le TP3 - Gestion des Droits d'Accès

USTHB - Faculté d'Informatique 2025/2026

Module : ASGBD - M1 SII/IL/MIV