Administration des bases de données
Chapitre 3 : Administrer la sécurité utilisateur

Ines BAKLOUTI

Ecole Supérieure Privée d'Ingénierie et de Technologies

Plan

1 Compte utilisateur de base de données
- Compte utilisateur de base de données
- Comptes prédéfinis : SYS et SYSTEM
- Authentification des utilisateurs
- Création de compte utilisateur

2 Privilèges
- Privilèges système
- Privilèges objet
- Options d'administration

3 Rôles
- Avantages des rôles
- Affecter des privilèges à des rôles et des rôles à des utilisateurs
- Rôles prédéfinis
- Créer un rôle

4 Profils
- Gestion des mots de passe
- Gestion des ressources
- Créer un profil

Plan

1 Compte utilisateur de base de données
- Compte utilisateur de base de données
- Comptes prédéfinis : SYS et SYSTEM
- Authentification des utilisateurs
- Création de compte utilisateur

2 Privilèges
- Privilèges système
- Privilèges objet
- Options d'administration

3 Rôles
- Avantages des rôles
- Affecter des privilèges à des rôles et des rôles à des utilisateurs
- Rôles prédéfinis
- Créer un rôle

4 Profils
- Gestion des mots de passe
- Gestion des ressources
- Créer un profil

Compte utilisateur de base de données

- Chaque compte utilisateur de base de données comporte :
  - un nom utilisateur unique
  - une méthode d'authentification
  - un tablespace par défaut
  - quotas sur un ou plusieurs tablespaces
  - un tablespace temporaire
  - un profil utilisateur
  - un statut de compte (verrouillé ou expiré)
  - ...
- Ces attributs doivent être spécifiés au moment du création de l'utilisateur. On doit obligatoirement définir le nom de l'utilisateur et la méthde d'authentification, le reste des attributs peuvent prendre des valeurs par défaut.
- Pour consulter les informations des utilisateurs, on utilise la vue DBA_USERS
- Une fois créé, le nom de l'utilisateur ne peut pas être modifié

Comptes prédéfinis : SYS et SYSTEM

- Caractéristiques du compte SYS :
  - Reçoit le rôle d'administrateur de base de données (DBA)
  - Dispose de tous les privilèges associés à ADMIN OPTION
  - Est requis pour les opérations de démarrage et d'arrêt, ainsi que pour certaines commandes de maintenance
  - Est propriétaire du dictionnaire de données
- Le compte SYSTEM reçoit le rôle d'administrateur de base de données (DBA)

Authentification des utilisateurs

- **Operating System (authentification par le système d'exploitation)**
  - Mode d'authentification qui nécessite le privilège SYSDBA ou SYSOPER (ce qui permet de copier les mots de passe des utilisateurs du dictionnaire de données dans un fichier de mots de passe externe (external password file) qui peut être lu par l'instance (même si la base de données non ouverte))
  - Syntaxe de connexion : CONNECT / AS [SYSOPER | SYSDBA] ;
- **Password File Authentication**
  - Mode d'authentification qui nécessite le privilège SYSDBA ou SYSOPER
  - Syntaxe de connexion : CONNECT username / password AS [SYSOPER | SYSDBA] ;
- **Password (authentification par la base de données Oracle)**
  - Associer à chaque utilisateur crée un mot de passe qu'il devra saisir lors de chaque connexion.
  - Lorsque vous définissez un mot de passe, vous pouvez le configurer afin qu'il expire immédiatement, ce qui oblige l'utilisateur à le changer lors de la première connexion.
  - Syntaxe : CREATE USER <name> IDENTIFIED BY <password> ;

Authentification des utilisateurs

- **External**
  - Oracle délègue la tâche d'authentification à un service externe.
  - Si l'option de sécurité avancée est autorisée, le service externe peut être un serveur Kerberos, un serveur RADIUS, ou (dans l'environnement Windows), le service d'authentification natif de Windows.
    - Si l'option de sécurité avancée n'est autorisée, le seul moyen d'authentification externe est par le système d'exploitation. Dans ce cas il faut créer les utilisateurs ayant les mêmes noms d'utilisateur du système d'exploitation préfixés avec la valeur du paramètre OS_ AUTHENT_PREFIX (sous windows on doit ajouter le domaine windows aussi au préfixe)
  - Syntaxe :
    - CREATE USER <name> IDENTIFIED EXTERNALLY ; (authentification par un service externe)
    - create user ops$<name> identified externally ; (authentification par système d'exploitation sous unix) –ops$ est le OS_ AUTHENT_PREFIX
    - create user "OPS$<windows domain>\name" identified externally ;
- **Global**
  - Ce mode d'authentification permet d'identifier les utilisateurs via Oracle Internet Directory.
  - Syntaxe : CREATE USER <name> IDENTIFIED GLOBALLY ;

Créer un compte utilisateur

Syntaxe

CREATE USER nom IDENTIFIED BY mot_de_passe
[DEFAULT TABLESPACE nom_tablespace]
[TEMPORARY TABLESPACE nom_tablespace]
[QUOTA { valeur [K|M] | UNLIMITED } ON nom_tablespace [,...]]
[PROFILE nom_profil]
[PASSWORD EXPIRE]
[ACCOUNT { LOCK | UNLOCK }] ;

Exemple

CREATE USER scott identified by pwdscott
DEFAULT TABLESPACE users
QUOTA unlimited on users
PASSWORD EXPIRE ;

Plan

1 Compte utilisateur de base de données
- Compte utilisateur de base de données
- Comptes prédéfinis : SYS et SYSTEM
- Authentification des utilisateurs
- Création de compte utilisateur

2 Privilèges
- Privilèges système
- Privilèges objet
- Options d'administration

3 Rôles
- Avantages des rôles
- Affecter des privilèges à des rôles et des rôles à des utilisateurs
- Rôles prédéfinis
- Créer un rôle

4 Profils
- Gestion des mots de passe
- Gestion des ressources
- Créer un profil

Privilèges

Privilège : le droit d'exécuter un type particulier d'instruction SQL ou d'accéder à l'objet d'un autre utilisateur. Il existe deux types de privilèges utilisateur :

- **Privilèges système :**
  - Autorisent un utilisateur à effectuer certaines opérations de base de données, par exemple, le privilège permettant de créer des tablespaces, des sessions, etc.
  - Peuvent être accordés par l'administrateur ou par quelqu'un à qui la permission d'administrer ces privilèges a été accordée explicitement.
- **Privilèges objet :**
  - Permettent à un utilisateur d'effectuer une action particulière sur un objet spécifique, tel qu'une table, une vue, une séquence, une procédure, une fonction ou un package.
  - Sans permission spécifique (privilège), les utilisateurs ne peuvent accéder qu'à leurs propres objets.
  - Peuvent être octroyés par le propriétaire d'un objet, par l'administrateur, ou par un utilisateur auquel la permission d'accorder des privilèges sur l'objet a été attribuée explicitement.

Privilèges

- Attribution de privilège : GRANT
  - exemples :
    - GRANT CREATE SESSION TO HR
    - GRANT SELECT, UPDATE(SALARY) ON EMPLOYEES TO SCOTT ;
- Déclination de privilège : REVOKE
  - exemples :
    - REVOKE CREATE SESSION FROM HR
    - REVOKE SELECT, UPDATE(SALARY) ON EMPLOYEES FROM SCOTT ;

Privilèges système

Privilèges système	Opérations permises
CLUSTER (Segments de données)	
CREATE CLUSTER	Création des clusters dans le schéma propriétaire
CREATE ANY CLUSTER	Création des clusters dans n'importe quel schéma. Comportement similaire à CREATE ANY TABLE.
ALTER ANY CLUSTER	modifie n'importe quels clusters dans la base de données
DROP ANY CLUSTER	Supprime n'importe quel cluster de la base de données
BASE DE DONNEES	
ALTER DATABASE	Modification base de données; ajout des fichiers système
INDEX	
CREATE ANY INDEX	Création des index dans n'importe quel schéma sur n'importe quelle table
ALTER ANY INDEX	Modification de n'importe quel index dans la base de données.
DROP ANY INDEX	Supprime n'importe quel index dans la base de données
PRIVILEGE	
GRANT ANY PRIVILEGE	Affecter n'importe quel privilège système (et non objet)

Privilèges système

PROCEDURE	
CREATE PROCEDURE	Création des procédures et fonctions stockées et gérer les packages dans son propre schéma.
CREATE ANY PROCEDURE	Création des procédures et fonctions stockées et gérer les packages dans n'importe quel schéma (nécessite aussi les privilèges ALTER ANY TABLE, BACKUP ANY TABLE, DROP ANY TABLE, SELECT ANY TABLE, INSERT ANY TABLE, UPDATE ANY TABLE, DELETE ANY TABLE, or GRANT ANY TABLE)
ALTER ANY PROCEDURE	Recompile n'importe quelle procédure ou fonction et modifie n'importe quel package dans n'importe quel schéma.
DROP ANY PROCEDURE	supprime n'importe quelle procédure ou fonction et supprime n'importe quel package dans n'importe quel schéma
EXECUTE ANY PROCEDURE	Exécute n'importe quelle procedure ou fonction (stand-alone ou packaged), or reference any public package variable in any schema.
ROLE	
CREATE ROLE	Création d'un rôle
ALTER ANY ROLE	Modification de n'importe quel rôle dans une base de données
DROP ANY ROLE	Suppression de n'importe quel rôle dans une base de données
GRANT ANY ROLE	Attribution de n'importe quel rôle dans la base de données

Privilèges système

SESSION	
CREATE SESSION	Connexion à la base de données
ALTER SESSION	Modification état de connexion
RESTRICTED SESSION	Connexion quand la base est ouverte en mode STARTUP RESTRICT
SYNONYME	
CREATE SYNONYM	Création des synonymes dans son propre schéma.
CREATE ANY SYNONYM	Création des synonymes dans n'importe quel schéma
DROP ANY SYNONYM	Supprimer les synonymes dans n'importe quel schéma
TABLE	
CREATE TABLE	Création des tables dans son propre schéma. Permet aussi d'ajouter le privilège d'ajout des index sur les tables crées. l'attribution doit indiquer une valeur limite des espaces disques logiques sinon le privilège UNLIMITED TABLESAPACE doit être attribué.
CREATE ANY TABLE	Création des tables dans n'importe quel schéma.
BACKUP ANY TABLE	Exécute une opération d'export incrémental sur les tables d'un schéma

Privilèges système

TABLE	
DROP ANY TABLE	Supprime ou tronque n'importe quelle table de n'importe quel schéma.
LOCK ANY TABLE	Verrouillage ou déverrouillage de n'importe quelle table de n'importe quel schéma.
COMMENT ANY TABLE	Commenter n'importe quelle table dans n'importe quel schéma
SELECT ANY TABLE	Interroger n'importe quelle table dans n'importe quel schéma
INSERT ANY TABLE	Insertion des enregistrements dans n'importe quelle table ou vue dans n'importe quel schéma
UPDATE ANY TABLE	Modification des enregistrements dans n'importe quelle table ou vue de n'importe quel schéma.
DELETE ANY TABLE	Suppression des enregistrements dans n'importe quelle table ou vue de n'importe quel schéma
TRANSACTION	
FORCE TRANSACTION	Force le Commit ou Rollback des transactions propriétaires dans une base de données locale.
FORCE ANY TRANSACTION	Force le Commit ou Rollback de n'importe quelle transactions dans une base de données locale.

Privilèges système

TRIGGER	
CREATE TRIGGER	Création des déclencheurs dans son propre schéma
CREATE ANY TRIGGER	Création des déclencheurs dans n'importe quel schéma de la base de données.
ALTER ANY TRIGGER	Active, désactive, ou recompile n'importe quel déclencheur dans n'importe quel schéma de la base de données.
DROP ANY TRIGGER	Supprime des déclencheurs de n'importe quel schéma
USER	
CREATE ANY USER	Création des utilisateurs, nom et mot de passe, affectation des tablespaces par défaut et temporaire et affectation aux groupes
BECOME ANY USER	Devenir n'importe quel utilisateur (Permet de réaliser un import intégral)
ALTER USER	Modifier le profil des autres utilisateurs BD : changer leur mot de passe, modifier les tablespaces et les valeurs limites, modifier les rôles et privilèges.
DROP USER	Supprimer un autre utilisateur

Privilèges objet

- Chaque type d'objet possède des privilèges particuliers :

Privilège Objet	SQL
ALTER	ALTER object (table ou sequence)
DELETE	DELETE FROM object (table ou vue)
EXECUTE	EXECUTE object (procedure ou fonction). Références to public package variables
INDEX	CREATE Index ON object (Table)
INSERT	INSERT on object (Table ou vue)
REFERENCES	CREATE or ALTER TABLE <<définition Clé étrangère>> on Object (table) REFERENCES.....
SELECT	SELECT ..... FROM ..... (vue, table, sequence)
UPDATE	UPDATE object (table ou vue)

Options d'administration

- Les options d'administration WITH ADMIN OPTION et WITH GRANT OPTION permettent de déléguer l'administration des privilèges à un autre utilisateur
- Déléguer un privilège système avec WITH ADMIN OPTION
  - exemple :
    - GRANT CREATE SESSION TO HR WITH ADMIN OPION ;
    - connect hr/hr
    - GRANT CREATE SESSION TO SCOTT ;

  NB : un REVOKE du privilège système CREATE SESSION pour l'utilisateur HR ne sera pas transmis à SCOTT. SCOTT gardera le privilège CREATE SESSION.
- Déléguer un privilège objet avec WITH GRANT OPTION
  - exemple :
    - GRANT SELECT ON EMPLOYEES to STOCK WITH GRANT OPTION ;
    - connect STOCK/STOCK
    - GRANT SELECT ON EMPLOYEES to USER1 WITH GRANT OPTION ;

  NB : un REVOKE du privilège objet SELECT pour l'utilisateur STOCK sera transmis au utilisateur USER1. USER1 n'aura plus le privilège SELECT ON EMPLOYEES.

Plan

1 Compte utilisateur de base de données
- Compte utilisateur de base de données
- Comptes prédéfinis : SYS et SYSTEM
- Authentification des utilisateurs
- Création de compte utilisateur

2 Privilèges
- Privilèges système
- Privilèges objet
- Options d'administration

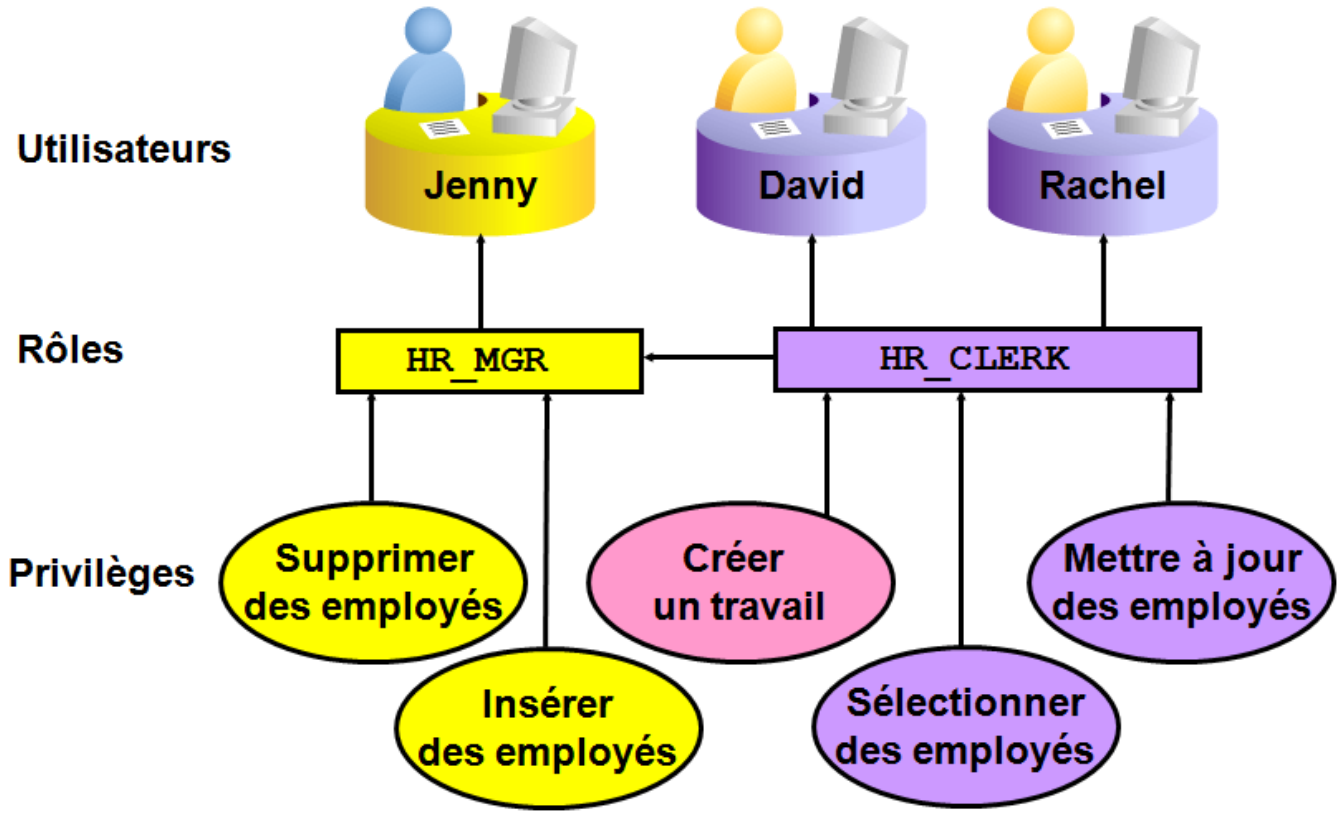
3 Rôles
- Avantages des rôles
- Affecter des privilèges à des rôles et des rôles à des utilisateurs
- Rôles prédéfinis
- Créer un rôle

4 Profils
- Gestion des mots de passe
- Gestion des ressources
- Créer un profil

Avantages des rôles

- Gestion simplifiée (plus facile) des privilèges :
  Utilisez des rôles pour simplifier la gestion des privilèges. Plutôt que d'accorder le même ensemble de privilèges à plusieurs utilisateurs, vous pouvez accorder les privilèges à un rôle, puis accorder ce rôle à chaque utilisateur.
- Gestion dynamique des privilèges :
  Si les privilèges associés à un rôle sont modifiés, tous les utilisateurs auxquels ce rôle est accordé bénéficient automatiquement et immédiatement des privilèges modifiés.
- Disponibilité sélective des privilèges :
  Les rôles peuvent être activés et désactivés afin d'activer ou de désactiver temporairement les privilèges. L'activation d'un rôle peut également être utilisée pour vérifier que le rôle a été accordé à un utilisateur.

Affecter des privilèges à des rôles et des rôles à des utilisateurs



Rôles prédéfinis

- Parmis les rôles prédéfinis on trouve :

Rôle	Privilèges
CONNECT	CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE SYNONYM, CREATE SEQUENCE, CREATE DATABASE LINK, CREATE CLUSTER, ALTER SESSION
RESOURCE	CREATE TABLE, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, CREATE TYPE, CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR
SCHEDULER_ADMIN	CREATE ANY JOB, CREATE JOB, EXECUTE ANY CLASS, EXECUTE ANY PROGRAM, MANAGE SCHEDULER
DBA	La plupart des privilèges système et plusieurs autres rôles. Ce rôle ne doit pas être accordé aux utilisateurs qui ne sont pas administrateurs.
SELECT_ CATALOG_ROLE	Pas de privilèges système, mais plus de 1600 privilèges objet sur le dictionnaire de données.

Créer un rôle

- **Création d'un rôle SUPERDBA avec mot de passe et intégrant le rôle DBA et des privilèges système**

```
CREATE ROLE "SUPERDBA" IDENTIFIED BY "sup"; -- le mot de passe sera demandé lors de l'activation du rôle
GRANT ALTER ANY INDEXTYPE TO "SUPERDBA"
GRANT ALTER ANY PROCEDURE TO "SUPERDBA"
GRANT ALTER ANY TABLE TO "SUPERDBA"
GRANT "DBA" TO "SUPERDBA" WITH ADMIN OPTION;
```

- **Affectation du rôle SUPERDBA à l'utilisateur STOCK**

```
GRANT "SUPERDBA" TO STOCK WITH ADMIN OPTION;
```

Plan

1 Compte utilisateur de base de données
- Compte utilisateur de base de données
- Comptes prédéfinis : SYS et SYSTEM
- Authentification des utilisateurs
- Création de compte utilisateur

2 Privilèges
- Privilèges système
- Privilèges objet
- Options d'administration

3 Rôles
- Avantages des rôles
- Affecter des privilèges à des rôles et des rôles à des utilisateurs
- Rôles prédéfinis
- Créer un rôle

4 Profils
- Gestion des mots de passe
- Gestion des ressources
- Créer un profil

Profils et utilisateurs

- Un seul profil est affecté à un utilisateur à un instant donné.
- Les profils :
  - gèrent les fonctionnalités de mots de passe (statut de compte, durée de vie du mdp, tentatives de connexion, etc). Option toujours activée.
  - contrôlent la consommation des ressources (taille en cpu, temps de connexion, nombre de sessions ouvertes, etc). Option activée si la valeur de paramètre d'initilisation RESOURCE_LIMIT est à TRUE (valeur par défaut FALSE).

Gestion des mots de passe

Verrouillage des comptes

Paramètre	Description
FAILED_LOGIN_ATTEMPTS	Nombre d'échecs de connexion avant le verrouillage du compte
PASSWORD_LOCK_TIME	Nombre de jours pendant lesquels le compte est verrouillé après le nombre déterminé d'échecs de connexion

Expiration et durée de vie des mots de passe

Paramètre	Description
PASSWORD_LIFE_TIME	Durée de vie du mot de passe, en jours, avant expiration
PASSWORD_GRACE_TIME	Période de grâce, en jours, permettant le changement de mot de passe après la première connexion réussie suite à l'expiration du mot de passe

Historique des mots de passe

Paramètre	Description
PASSWORD_REUSE_TIME	Nombre de jours pendant lesquels le mot de passe ne peut pas être réutilisé
PASSWORD_REUSE_MAX	Nombre de fois le mot de passe actuel peut être utilisé

Vérification des mots de passe

Paramètre	Description
PASSWORD_VERIFY_FUNCTION	Fonction PL/SQL qui effectue une vérification de complexité avant l'affectation d'un mot de passe

- Les fonctions de vérification des mots de passe doivent :
  - Appartenir à l'utilisateur SYS
  - Renvoyer une valeur booléenne (true ou false)

Gestion des ressources

- Les profils peuvent gérer les limites appliquées à l'utilisation des ressources. Les limites possibles les plus utilisées :

Paramètre	Description
SESSIONS_PER_USER	Nombre de sessions concurrentes pour un compte utilisateur
CPU_PER_SESSION	Temps CPU (en centisecondes) que le processus serveur d'une session peut consommer avant que la session soit automatiquement déconnectée
CPU_PER_CALL	Temps CPU (en centisecondes) que le processus serveur d'une session peut consommer pour exécuter une requête SQL avant arrêt automatique de l'exécution
CONNECT_TIME	Temps de connexion (en secondes) pour une session
IDLE_TIME	Temps d'inactivité (en secondes) pour une session

Créer un profil

Syntaxe

CREATE PROFILE <profile_name> LIMIT
[Limit_ressourse> value]
[Limit_passowrd> value] ;
value :={integer | UNLIMITED | DEFAULT} ;
value :={function | null | DEFAULT} pour le paramètre PASSWORD_VERIFY_FUNCTION

Exemple

CREATE PROFILE developer_profile LIMIT
SESSIONS_PER_USER 2
CPU_PER_SESSION 10000
CONNECT_TIME 480
IDLE_TIME 60
FAILED_LOGIN_ATTEMPTS 3
PASSWORD_LIFE_TIME 90
PASSWORD_REUSE_TIME 2
PASSWORD_VERIFY_FUNCTION my_function ;