**Sécurité application**

**Présenté par:**

**Mathis Douangpanya**

**Table de matière:**

[Création de rôles: 2](#_Toc1063568181)

[Réponse : 2](#_Toc880728352)

[1. role\_dba : 3](#_Toc665217755)

[2. role\_gestionnaire : 3](#_Toc1869825159)

[3. role\_registrariat : 3](#_Toc1989674182)

[4. role\_api : 4](#_Toc776637765)

[5. role\_enseignant : 4](#_Toc1494941612)

[Création de profils : 4](#_Toc952098847)

[Profil Gestionnaire : 5](#_Toc41169599)

[Profil Restrictif : 5](#_Toc2118885646)

[Traces d’exécutions : 5](#_Toc504442744)

[Sauvegarde de base de donnée: 12](#_Toc976711261)

[Connexion des utilisateurs crées: 13](#_Toc112577341)

# Création de rôles:

Question :

Vous devez poser et expliquer les hypothèses que vous appliquez à chacun des rôles en fonction des responsabilités de chaque utilisateur

#### Réponse :

#### **1. role\_dba :**

* **Responsabilité** : Ce rôle est destiné aux administrateurs de la base de données (DBA), qui sont responsables de la gestion complète de la base de données, y compris la création, la modification et la suppression d'objets tels que les tables et les vues.
* **Hypothèses** :
  + Les utilisateurs avec ce rôle doivent avoir un accès complet à toutes les fonctionnalités de la base de données.
  + Le privilège CREATE SESSION est accordé pour permettre la connexion à la base de données.
  + Les privilèges de niveau système tels que CREATE ANY TABLE, DROP ANY TABLE, ALTER ANY TABLE, etc., sont attribués directement à l'utilisateur Mathis puisque le rôle DBA doit permettre la gestion totale de la base de données.
* **Explication** : Ce rôle a été conçu pour permettre un contrôle total de la base de données, ce qui est nécessaire pour un DBA principal ou un collègue DBA.

#### **2. role\_gestionnaire :**

* **Responsabilité** : Ce rôle est destiné au gestionnaire principal de la base de données. Cet utilisateur doit avoir un accès complet pour gérer les informations des étudiants, les cours, les groupes, les semestres et les évaluations.
* **Hypothèses** :
  + Le gestionnaire principal doit pouvoir ajouter, mettre à jour, lire et supprimer des enregistrements dans les tables liées aux étudiants, aux cours, aux groupes, aux semestres, et aux évaluations.
  + Les privilèges SELECT, INSERT, UPDATE, DELETE sont nécessaires sur ces tables spécifiques.
  + Le rôle a le privilège CREATE SESSION pour se connecter à la base de données.
* **Explication** : Ce rôle a été créé pour permettre une gestion complète des données administratives, tout en limitant les actions à des tables spécifiques afin de contrôler l'accès aux données sensibles.

#### **3. role\_registrariat :**

* **Responsabilité** : Ce rôle est destiné aux utilisateurs du registrariat, qui sont chargés de gérer les informations des étudiants et des cours.
* **Hypothèses** :
  + Les utilisateurs de ce rôle doivent pouvoir ajouter, lire et mettre à jour les informations des étudiants et des cours, mais ils n'ont pas besoin de pouvoir supprimer des enregistrements.
  + Les privilèges SELECT, INSERT, UPDATE sont attribués sur la table étudiant et cours.
  + Le privilège CREATE SESSION permet à ces utilisateurs de se connecter à la base de données.
* **Explication** : Ce rôle est conçu pour limiter l'accès des utilisateurs du registrariat afin qu'ils ne puissent pas supprimer accidentellement ou intentionnellement des données critiques.

#### **4. role\_api :**

* **Responsabilité** : Ce rôle est destiné à l'utilisateur API qui gère les groupes et les semestres.
* **Hypothèses** :
  + L'utilisateur API doit pouvoir créer, mettre à jour et consulter des informations concernant les groupes et les semestres, mais n'a pas besoin de droits de suppression.
  + Les privilèges SELECT, INSERT, UPDATE sont attribués sur les tables groupe et semestre.
  + Le privilège CREATE SESSION permet à l'utilisateur de se connecter.
* **Explication** : Ce rôle permet à l'utilisateur API d'interagir avec les données nécessaires à la gestion des groupes et semestres, tout en empêchant la suppression accidentelle de ces enregistrements.

#### **5. role\_enseignant :**

* **Responsabilité** : Ce rôle est destiné à l'utilisateur enseignant, qui gère les évaluations.
* **Hypothèses** :
  + L'enseignant doit pouvoir créer, mettre à jour, lire, et supprimer les évaluations des étudiants.
  + Les privilèges SELECT, INSERT, UPDATE, DELETE sont attribués à la table évalutation.
  + Le privilège CREATE SESSION est également attribué pour permettre la connexion.
* **Explication** : Ce rôle est conçu pour donner un accès complet à la gestion des évaluations tout en limitant les actions de l'utilisateur à cette table spécifique.

# Création de profils :

Question :

Vous devez poser des hypothèses et expliquer les décisions que vous prendrez pour chacun des profils, c’est-à-dire, expliquer pourquoi vous utilisez les paramètres et expliquer les valeurs utilisées.

Réponse :

#### **Profil Gestionnaire :**

* **Hypothèses :**
  + Le gestionnaire a besoin d'un accès plus flexible et doit se connecter fréquemment.
  + Le risque d'erreurs est moindre, car il s'agit d'un utilisateur de haut niveau.
* **Décisions :**
  + Permet 10 tentatives de connexion échouées pour réduire les interruptions.
  + Le mot de passe doit être changé tous les 180 jours pour équilibrer sécurité et praticité.
  + 30 jours de période de grâce pour laisser le temps au gestionnaire de changer son mot de passe.
  + Le mot de passe peut être réutilisé après 365 jours sans limite pour offrir une certaine flexibilité.

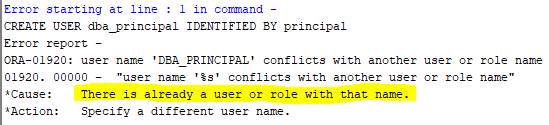
#### **Profil Restrictif :**

* **Hypothèses :**
  + Les autres utilisateurs ont besoin d'un contrôle plus strict pour réduire les risques d'accès non autorisé.
  + Ces utilisateurs se connectent moins souvent et doivent respecter des règles de sécurité plus élevées.
* **Décisions :**
  + 5 tentatives de connexion échouées pour limiter les risques de piratage.
  + Changement de mot de passe tous les 90 jours pour renforcer la sécurité.
  + 15 jours de période de grâce pour encourager un changement rapide du mot de passe.
  + Un mot de passe ne peut être réutilisé que 5 fois au maximum après 365 jours pour renforcer la sécurité et éviter les répétitions.

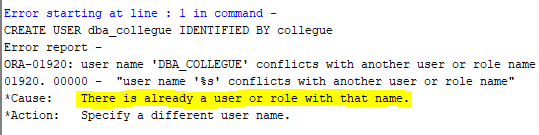
# Traces d’exécutions :

**(J’ai pris les captures après avoir fait les commandes la première fois)**

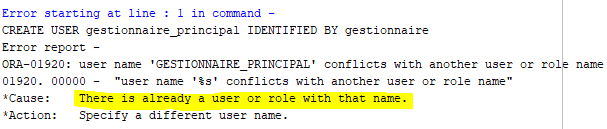




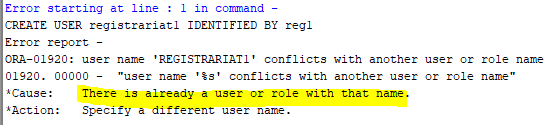




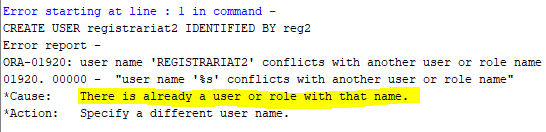




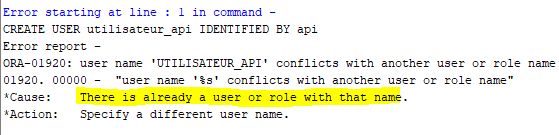




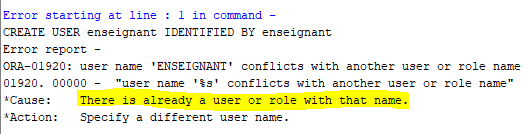




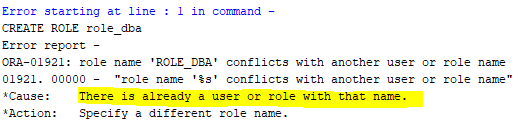




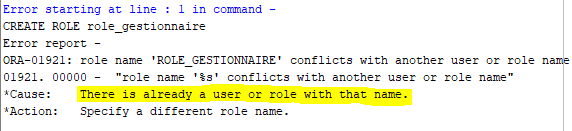


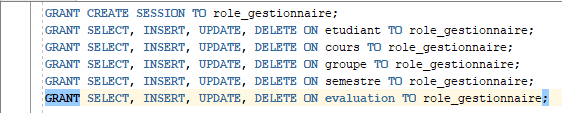


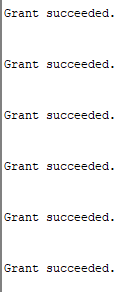




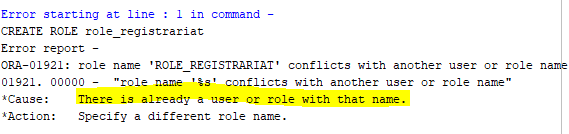


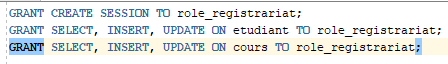


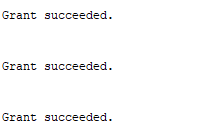




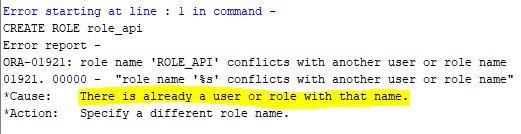


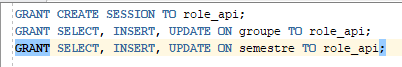


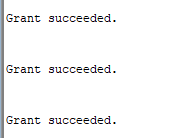




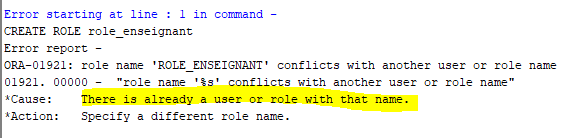




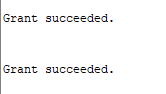


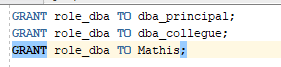


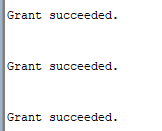








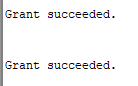










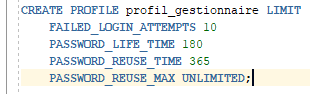


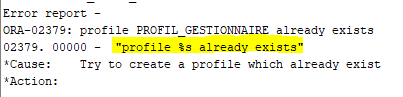


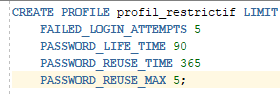


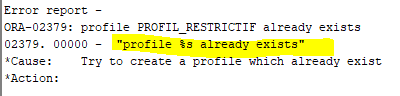


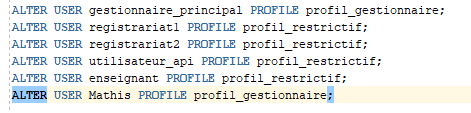


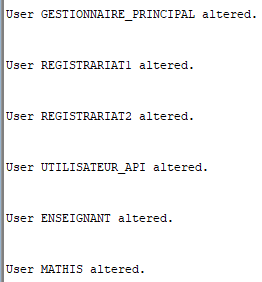






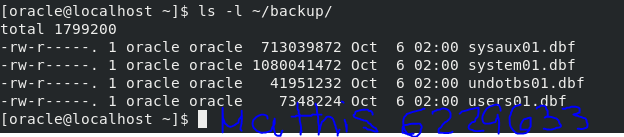






# Sauvegarde de base de donnée:





# Connexion des utilisateurs crées:

