

Administration Oracle

abdellah_madani@yahoo.fr

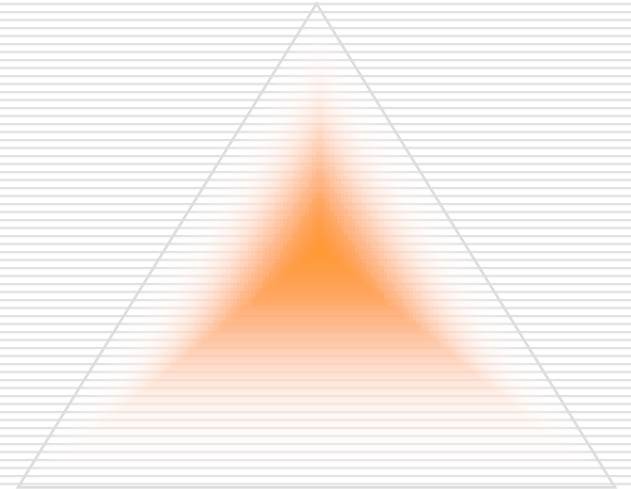
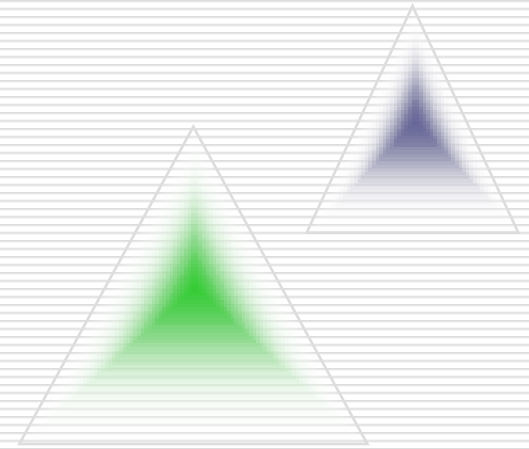


Plan

- Introduction
- Architecture interne d'Oracle
- Gestion des instances
- Privilèges et rôle
- Profil
- Gestion des utilisateurs
- Sauvegarde et restauration
- Quelques utilitaires

Administration Oracle

Privilèges et rôles





Privilèges et Rôles

- Concepts mis en œuvre pour protéger une BD en accordant/retirant des droits à des utilisateurs.
- Privilège : droit
- Rôle : ensemble de privilèges



Types de Privilèges

Deux types de privilèges :

- Privilège Système : création, modification et suppression d'objets (tables, vues, ...)

Grant create table to scott

- Privilège Objet : manipulation des objets d'une BD.

Grant select on Emp to scott



Octroi d'un Privilège Système

Grant sys_priv to user | rôle | all [with admin option]

où

Sys_priv : liste de privilèges systèmes

User : nom d'un utilisateur

Rôle : rôle déjà créé

All : tous les utilisateurs

With admin option : droit d'assigner, retirer, modifier ou supprimer les privilèges reçus



Octroi d'un Privilège Système

Exemple : supposons que nous avons deux utilisateurs abdou et yassine

Grant create session to abdou

droit de se connecter à la base

***Grant create table, create view to abdou
with admin option***

droit de créer des tables et des vues. Abdou peut donner ce droit (à yassine, par exemple)



Retrait d'un Privilège Système

Revoke sys_priv From user | rôle | all

Exemple

Revoke create session from yassine

Yassine n'a plus le droit de se connecter,
même s'il possède un compte



Octroi d'un Privilège Objet

Grant *Obj_Priv* *on* *Objets* *to* *user* | *rôle* | *all* [*with*
grant option]

Où

Obj_priv : liste de privilèges objets

User : nom d'un utilisateur

Rôle : rôle déjà créé

All : tous les utilisateurs

With grant option : droit d'assigner, retirer,
modifier ou supprimer les privilèges reçus



Octroi d'un Privilège Objet

Grant select, insert on scott.emp to yassine

Yassine peut consulter et alimenter la table
Emp de scott

Grant select, update (job, Mgr) on scott.emp to abdou

Abdou peut consulter la table emp de scott,
mais ne peut modifier que la fonction et
le numéro du supérieur



Octroi d'un Privilège Objet

- Un utilisateur ne peut pas donner des droits sur les objets qui ne lui appartiennent pas, même s'il est DBA.
- Un utilisateur possède automatiquement tous les droits sur ses propres objets



Retrait d'un Privilège Objet

**Revoke obj_priv on objet From
user | rôle | all**

Exemple

**Revoke all privileges on scott.emp From
yassine**

Retire tous les privilèges de yassine



Utilisation d'un Rôle

- Un rôle est un ensemble de privilèges
- Permet de faciliter l'administration
- Étapes d'utilisation d'un rôle :
 - Création d'un rôle vide
 - Assignment des privilèges à un rôle
 - Assignment du rôle crée à un utilisateur



Utilisation d'un Rôle

Create role compt;

Création d'un rôle vide (ne contient aucun privilège)

Grant select, insert, update(job) on scott.emp to compt

Assignation des privilèges au rôle compt

Grant compt to yassine, abdou

Octroi du rôle compt to yassine et abdou

Revoke compt from yassine, abdou

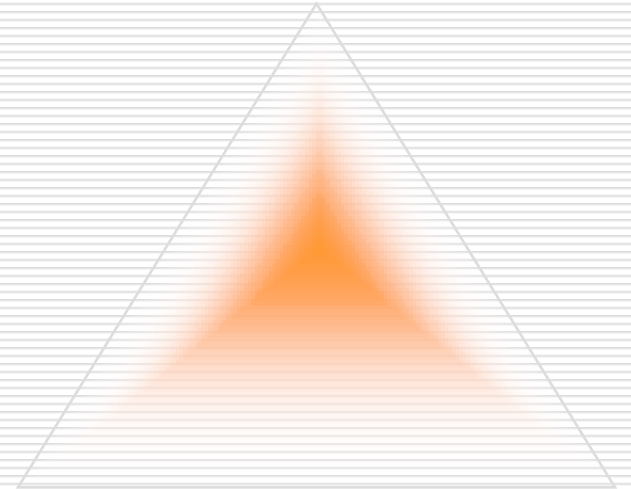
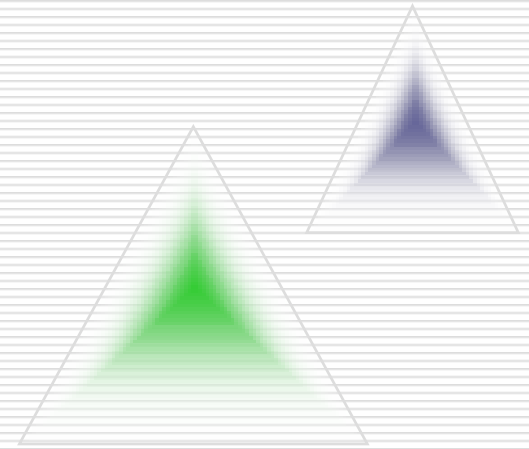
Retrait du rôle compt des utilisateurs yassine et abdou

Drop role compt

Supression du rôle compt

Administration Oracle

Gestion des profiles





Profiles

- Ensemble d'actions permettant de limiter l'accès aux ressources système
- Une fois qu'un profile est crée, on ne peut pas dépasser les limites imposées.
- Deux types de limitations :
 - Limitation des mots de passe
 - Limitation des ressources système

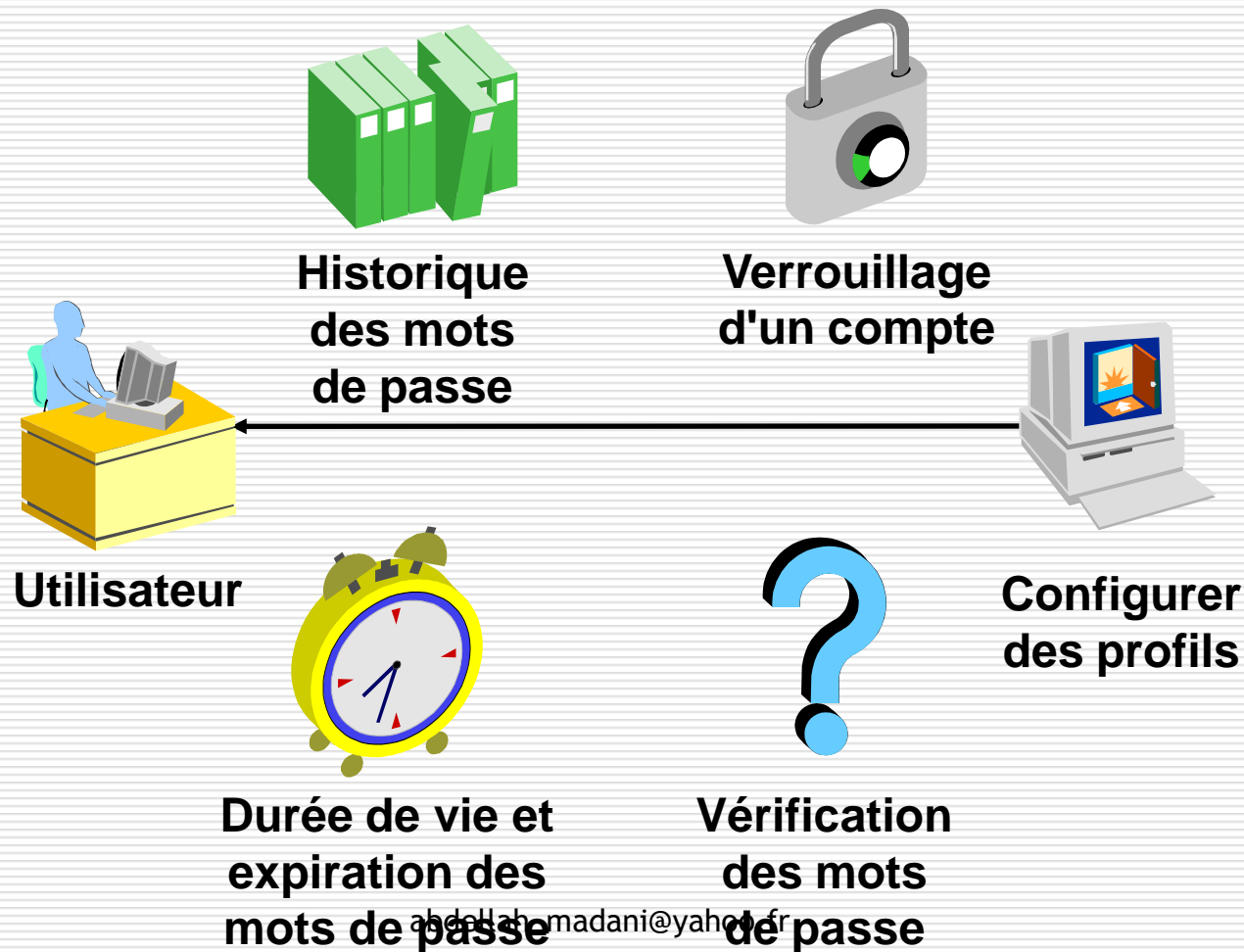


Limitation des mots de passe

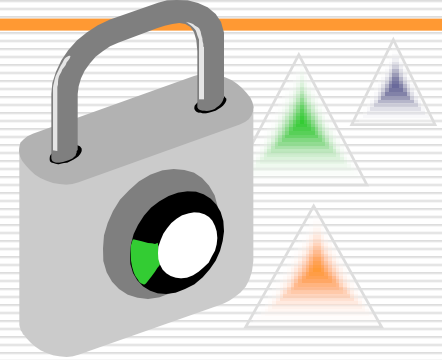
Plusieurs options permettant d'augmenter la sécurité des mots de passe :

- Failed_Login_Attempts
- Password_Lock_Time
- Password_Life_Time
- Password_Reuse_Time
- Password_Verify_Time
- ...

Gestion des mots de passe

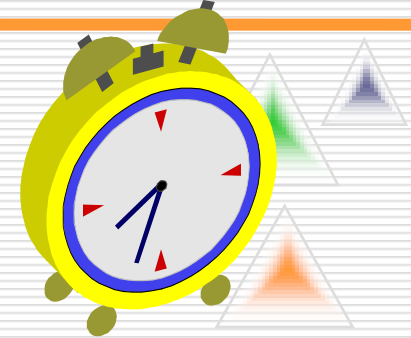


Verrouillage d'un compte



Paramètre	Description
FAILED_LOGIN_ATTEMPTS	Nombre d'échecs de connexion avant verrouillage du compte
PASSWORD_LOCK_TIME	Durée, en jours, de verrouillage du compte après le nombre d'échecs de connexion défini

Durée de vie et expiration des mots de passe



Paramètre	Paramètre
<code>PASSWORD_LIFE_TIME</code>	Durée de vie, en jours, du mot de passe avant expiration
<code>PASSWORD_REUSE_MAX</code>	Nombre maximum de réutilisations d'un mot de passe



Vérifier les mots de passe

Paramètre	Description
<code>PASSWORD_VERIFY_FUNCTION</code>	Fonction PL/SQL qui vérifie la complexité d'un mot de passe avant que celui-ci ne soit affecté



Exemple

```
CREATE PROFILE grace_5 LIMIT  
  FAILED_LOGIN_ATTEMPTS 3  
  PASSWORD_LOCK_TIME UNLIMITED  
  PASSWORD_LIFE_TIME 30  
  PASSWORD_REUSE_Max 30;
```



Limitations des ressources système

Restreindre l'accès à des ressources du système : processeur, mémoire, ...

- Sessions_Per_User
- CPU_Per_Session
- Connect_Time
- Private_SGA
- ...



Gestion des ressources

- Les limites relatives à la gestion des ressources peuvent s'appliquer au niveau session, au niveau appel ou aux deux.
- Les limites peuvent être définies par des profils via la commande CREATE PROFILE.



Définir des limites relatives aux ressources au niveau session

Ressource	Description
<code>CPU_PER_SESSION</code>	Temps CPU total calculé en centièmes de secondes
<code>SESSIONS_PER_USER</code>	Nombre de sessions simultanées autorisées pour chaque nom utilisateur
<code>CONNECT_TIME</code>	Temps de connexion calculé en minutes
<code>IDLE_TIME</code>	Périodes d'inactivité calculées en minutes
<code>LOGICAL_READS_PER_SESSION</code>	Nombre de blocs de données (lectures physiques et logiques)
<code>PRIVATE_SGA</code>	Espace privé de la mémoire SGA mesuré en octets (dans le cas d'un serveur partagé uniquement)

Définir des limites relatives aux ressources au niveau appel



Ressource	Description
<code>CPU_PER_CALL</code>	Temps CPU par appel en centièmes de secondes
<code>LOGICAL_READS_PER_CALL</code>	Nombre de blocs de données pouvant être lus par appel



Exemple

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



Création d'un profile

Étapes à suivre :

- Établir les limitations des mots de passe
- Établir les limitations des ressources système
- Créer le profile (**Create Profile... Limit...**)
- Attribuer le profile aux utilisateurs qui devront être limités



Création d'un profile

Create profile prof_user

Limit

Sessions Per User unlimited

Connect_Time 45

Private_SGA 15K

Failed_Login_Attempts 3



Assignment d'un profile

- L'attribution d'un profile à un utilisateur se fait
 - Au moment de la création de l'utilisateur (voir gestion des utilisateur)
 - Avec l'instruction Alter
 - Alter user yassine profile prof_user*
- Par défaut, un utilisateur se voit assigner le profile DEFAULT



Suppression d'un profile

- Suppression d'un profile non assigné à aucun utilisateur

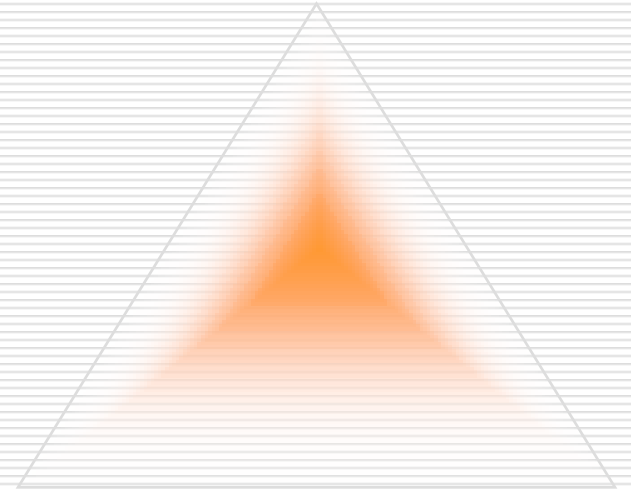
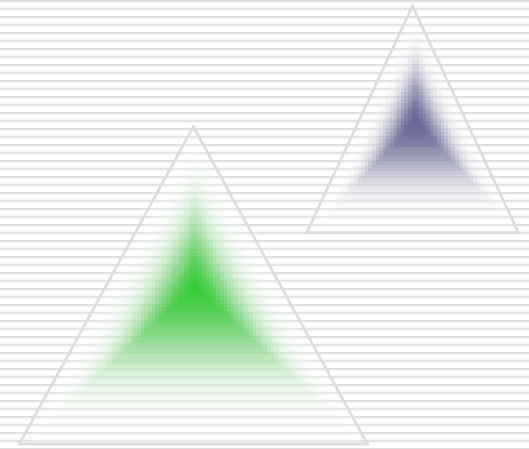
Drop profile prof_user

- Suppression d'un profile assigné à un utilisateur

Drop profile prof_user cascade

Administration Oracle

Gestion des utilisateurs





Gestion des utilisateurs

Objectif

- Créer et configurer un utilisateur d'une BD.
- Se connecter et effectuer des actions sur la BD.

Quand un utilisateur est crée, il ne possède aucun droit, même pas la possibilité de se connecter



Etapes de création d'un utilisateur

- choisir un nom d'utilisateur
- choisir une méthode d'authentification
- Créer l'utilisateur
- Assigner les rôles et privilèges à l'utilisateur

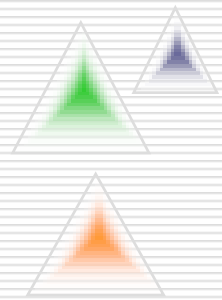


Méthode d'authentification

Deux types très utilisés

- Par la Base de Données.
- Par le système d'exploitation

Authentification par la BASE DE DONNÉES.



- Mode le plus courant, par défaut
- Utilisation de : *Identified by*

Exemple

- *Create user yassine identified by Yassine*
- *Connect yassine/Yassine*



Authentification par SE

- Oracle se base sur l'authentification du SE
- On n'a pas besoin qu'une seule fois (avantage)
- Si on oublie de fermer sa session SE (se déconnecter), un autre peut accéder la BD (inconvenient).

Exemple

Create user yassine identified externally



Création de l'utilisateur

Create user yassine identified by Yassine

Profile prof_users

Password expire

Account lock|unlock



Manipulation des utilisateurs

Modification

- Alter user yassine identified by 123
- Alter user yassine account unlock
- ..



Manipulation des utilisateurs

Suppression

➤ ***Drop user yassine***

Supprime un schéma vide

➤ ***Drop user yassine cascade***

Supprime un utilisateur avec tous ses objets

➤ Un utilisateur connecté ne pourra pas être supprimé !