Faculté des Sciences de Gabès

Cours Administration BD

Chapitre 4 : Administrer la sécurité utilisateur

Gestion des utilisateurs et des Profils

(Partie 1)

Faîçal Felhi

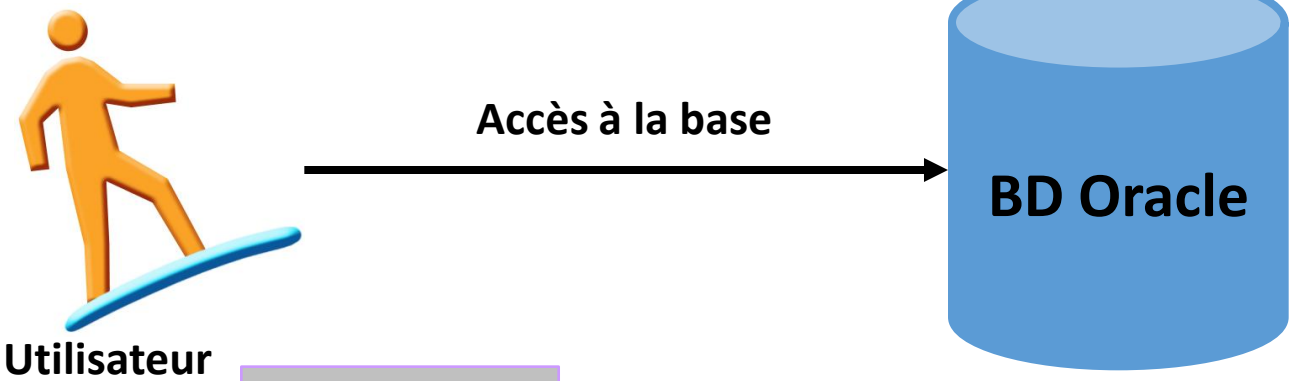
felhi_fayssal@yahoo.fr

Introduction

Un SGBD oracle est un système **multiutilisateur complexe**

Il doit **protéger** les données de l'utilisateur

Il doit permettre un **partage contrôlé** des données utilisateurs



Objectifs

- Il s’agit de répartir et de sélectionner les **droits** des utilisateurs de la BD afin d’en assurer la protection :
  - Gestion des accès à la BD
  - Gestion des accès aux données de la base
  - Limitation des ressources accessibles aux utilisateurs
  - Attribution des droits d’accès par défaut

Principe

Pour la gestion de la sécurité, Oracle permet :

- De définir les utilisateurs qui peuvent se connecter à la BD (avec une identification par le système d'exploitation ou par la BD)
- De définir dans quel(s) tablespace(s) un utilisateur peut créer des objets
- De limiter l'utilisation des ressources système
- D'imposer une politique de gestion de MdP
- De définir les droits de chaque utilisateur à l'intérieur de la BD

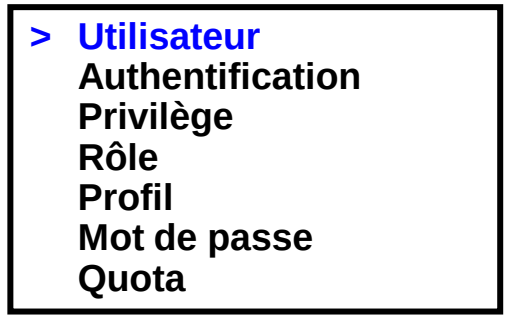
- Dans une BD, les droits des utilisateurs sont gérés avec la notion de **privilège**
- Un privilège est le droit :
  - D'exécuter un ordre SQL (par exemple créer une table) : c'est la notion de **privilège système**
  - D'accéder à un objet d'un autre utilisateur (par exemple mettre à jour les données de la table CLIENT) : c'est la notion de **privilège objet**

- Les privilèges peuvent être attribués directement aux utilisateurs ou par l'intermédiaire de **rôles**
- Un rôle est un regroupement nommé de privilège (systèmes ou objets) qui peut être attribué en tant que tel à un utilisateur.
- Cet utilisateur reçoit alors automatiquement les privilèges contenus dans le rôle
- Les rôles facilitent la gestion des droits
- créer et gérer des comptes utilisateur de base de données
  - authentifier les utilisateurs
  - affecter des zones de stockage par défaut (tablespaces)
- accorder et révoquer des privilèges
- créer et gérer des rôles
- créer et gérer des profils
  - implémenter des fonctionnalités standard de sécurité utilisant des mots de passe
  - contrôler l'utilisation des ressources par les utilisateurs

- Un **compte utilisateur de base de données** constitue un moyen d'organiser l'appartenance des objets de base de données et l'accès à ces objets.
- Un **mot de passe** est un mode d'authentification par la base de données Oracle.
- On nomme **privilège** le droit d'exécuter un type particulier d'instruction SQL ou d'accéder à l'objet d'un autre utilisateur.
- Un **rôle** est un groupe nommé de privilèges liés qui sont accordés à des utilisateurs ou à d'autres rôles.
- Les **profils** imposent un ensemble nommé de limites concernant l'utilisation de la base de données et les ressources des instances.
- Un **quota** est une allocation d'espace dans un tablespace donné. Il constitue l'un des moyens permettant de contrôler l'utilisation des ressources par les utilisateurs.

Chaque compte utilisateur de base de données comporte :

- un nom utilisateur unique
- une méthode d'authentification
- un tablespace par défaut
- un tablespace temporaire
- un profil utilisateur
- un groupe de consommateurs de ressources
- un statut de verrouillage



Comptes prédéfinis : SYS et SYSTEM

- Le 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 le propriétaire du dictionnaire de données
- Le compte SYSTEM a le rôle d'administrateur de base de données (DBA).

A. Créer et modifier un utilisateur

1/ mode d'identification de l'utiliateur

Un utilisateur peut être identifié par Oracle ou par le système d'exploitation

a/ Identification par Oracle

- l'utilisateur se connecte à la base en utilisant un nom et un mot de passe.
- Oracle vérifie le nom et le MdP

SQL> CONNECT *nom*/*MdP*

Connecté

b/ Identification par le SE

- l'utilisateur se connecte à la base sans saisir de nom de MdP.
- Oracle ne vérifie pas le MdP, mais contrôle simplement que le nom de l'utilisateur au niveau du SE correspond à un nom d'utilisateur dans la BD. L'identification initiale a été réalisée par le SE.

SQL> CONNECT *nom*/*MdP*

Connecté

2/ Création d'un utiliateur

Syntaxe:

```
CREATE USER nom IDENTIFIED { BY  mdp | EXTERNALLY }
[DEFAULT TABLESPACE nom_tablespace  ]
[TEMPORARY TABLEPACE nom_tablespace ]
[QUOTA  { valeur [K |M]  | UNLIMITED } ON nom_tablespace[,…] ]
[PROFIE nom_profile]
[PASSWORD EXPIRE  ]
[ACCOUNT {LOCK | UNLOCK}  ];
```

Nom : doit respecter les règles de nommage

IDENTIFIED : indique si l'utilisateur est identifié par le SE (EXTERNALLY) ou par Oracle (BY mdp)

DEFAULT TABLESPACE indique dans quel tablespace les segments de l'utilisateur sont crées par défauts (si aucune TABLESPACE n'est présente lors de la création du segment)

TEMPORARY TABLEPACE indique dans quel tablespace les segments temporaires de l'utilisateur sont crées

QUOTA indique dans quel tablespace(s) l'utilisateur peut créer des objets et jusqu'à quelle limite

PROFIE indique le profile de l'utilisateur

PASSWORD EXPIRE permet de forcer une modification du mdp lors de la première connexion

ACCOUNT: LOCK le compte est verrouillé et la connexion est interdide, UNLOCK le compte n'est pas verrouillé et la connexion est autorisée

3/ modification d’un utiliateur

Syntaxe:

ALTER USER nom

[IDENTIFIED { BY mdp | EXTERNALLY }]

[DEFAULT TABLESPACE nom_tablespace]

[TEMPORARY TABLEPACE nom_tablespace]

[QUOTA { valeur [K |M] | UNLIMITED } ON nom_tablespace[,…]]

[PROFIE nom_profile]

[PASSWORD EXPIRE]

[ACCOUNT {LOCK | UNLOCK}];

Exemple de modification d’un utilisateur

- **Modification de mdp :**
  ALTER USER _salim IDENTIFIED BY mypass2

- **Modification des quotas:**
  ALTER USER _salim QUOTA 15M ON tbs_users;

- **Modification de status**
  ALTER USER _salim ACCOUNT LOCK; Verrouillage
  ALTER USER _salimt ACCOUNT UNLOCK; Activation

4/ Suppression d’un utiliateur

Syntaxe:

DROP USER nom [CASCADE];

Si l’utilisateur possède des objets, l’option CASCADE doit être présente pour forcer la suppression préalable de objets

Si l’utilisateur possède des objets et l’option CASCADE n’est pas présente : Erreur

Un utilisateur connecté ne peut pas être supprimé

5/ Trouver des informations sur les utiliateurs

Plusieurs vues du dictionnaire de données permettent d'obtenir des informations sur les utilisateurs : DBA_USERS et DBA_TS_QUOTAS

- DBA_USERS : informations sur les utilisateurs
  - USERNAME
  - USER_ID
  - PASSWORD
  - ACCOUNT_STATUS
  - etc
- DBA_TS_QUOTAS : informations sur les quotas des utilisateurs
  - USERNAME
  - BYTES
  - BLOCKS
  - etc

B. Utiliser les profils

1/Introduction

- Afin d'augmenter la sécurité de la base de données il peut être très intéressant de mettre en place une gestion des mots de passe comme le nombre maximal de tentatives de connexion à la base, le temps de verrouillage d'une compte, etc.
- Il peut parfois aussi être intéressant de limiter les ressources système allouées à un utilisateur afin d'éviter une surcharge inutile du serveur.
- Oracle propose une solution efficace et pratique pour mettre en place ce type d'action : les PROFILS.

2/ Définition

- Un profil est un ensemble nommé de limitations de ressources qui peut être attribué à un utilisateur
- Les ressources qui peuvent être limitées:
  - Temps CPU (Central Processing Unit ou unité centrale de traitement ou processeur) par appel et/ou par session
  - Nombre de lectures logique par appel et/ou par session
  - Nombre de sessions ouvertes simultanément
  - Temps d'inactivité par session
  - Durée totale de la session

3/ Création d'un profile

Syntaxe:

CREATE PROFILE nom LIMIT

[SESSIONS_PER_USER {valeur | UNLIMITED | DEFAULT }]

[CPU_PER_SESSION {valeur | UNLIMITED | DEFAULT }]

[CPU_PER_CALL {valeur | UNLIMITED | DEFAULT }]

[CONNECT_TIME {valeur | UNLIMITED | DEFAULT }]

[IDLE_TIME {valeur | UNLIMITED | DEFAULT }]

[LOGICAL_READS_PER_SESSION {valeur | UNLIMITED | DEFAULT }]

[LOGICAL_READS_PER_CALL {valeur | UNLIMITED | DEFAULT }]

[COMPOSITE LIMIT {valeur | UNLIMITED | DEFAULT }]

[PRIVATE_SGA{valeur | UNLIMITED | DEFAULT }]

[FAILED_LOGIN_ATTEMPTS {valeur | UNLIMITED | DEFAULT }]

[PASSWORD_LIFE_TIME {valeur | UNLIMITED | DEFAULT }]

[PASSWORD_REUSE_TIME {valeur | UNLIMITED | DEFAULT }]

[PASSWORD_REUSE_MAX {valeur | UNLIMITED | DEFAULT }]

[PASSWORD_LOCK_TIME {valeur | UNLIMITED | DEFAULT }]

[PASSWORD_GRACE_TIME {valeur | UNLIMITED | DEFAULT }]

[PASSWORD_VERIFY_FUNCTION {nom_fonction | NULL | DEFAULT }]

CPU :

- Les ressources CPU peuvent être limitées par session ou par appel.
- Avec une limite CPU/Session de 1 000, une session qui utilise ce profile et qui consomme plus de 10 secondes de temps CPU (les limites de temps CPU étant exprimées en centièmes de seconde) reçoit une erreur et est déconnectée :
    - ORA-02392: exceeded session limit on CPU usage, you are being logged off
- Une limitation par appel a le même effet, mais au lieu de limiter la session globale de l'utilisateur, elle empêche chaque commande de consommer trop de temps CPU. Si une limite CPU/Call est définie et que l'utilisateur la dépasse, la commande s'arrête et l'utilisateur reçoit un message d'erreur semblable à ce qui suit :
    - ORA-02393: exceeded call limit on CPU usage

Network/Memory :

- Chaque session de base de données consomme des ressources mémoire du système et des ressources réseau (si la session est ouverte par un utilisateur qui ne se trouve pas en local sur le serveur) .
- Vous pouvez définir les éléments suivants :
  - Connect Time : Indique le nombre de minutes pendant lesquelles un utilisateur peut rester connecté avant d'être automatiquement déconnecté.
  - Idle Time : Définit le nombre de minutes pendant lesquelles la session d'un utilisateur peut rester inactive avant d'être automatiquement déconnectée. Le temps d'inactivité est calculé pour le processus serveur uniquement. Il ne tient pas compte de l'activité des applications.
  - Concurrent Sessions : Indique le nombre de sessions simultanées pouvant être créées à l'aide d'un compte utilisateur de base de données.
  - Private SGA : Limite la quantité d'espace consommé dans la mémoire SGA . Cette restriction ne prend effet que si la session utilise un serveur partagé.

- **Disk I/O :**
  - Cette option limite la quantité de données qu'un utilisateur peut lire, par session ou par appel.
  - Les options Reads/Session et Reads/Call limitent le nombre total de lectures réalisées à partir de la mémoire et du disque. Elles permettent de s'assurer, par exemple, qu'aucune instruction consommant beaucoup d'E/S n'utilise trop intensément la mémoire et les disques.

Implémenter des fonctionnalités de sécurité utilisant des mots de passe

- La gestion des mots de passe Oracle est implémentée par l'intermédiaire de profiles utilisateur. Les profiles peuvent fournir de nombreuses fonctionnalités de sécurité standard, telles que :
  1. **Verrouillage des comptes :** Permet le verrouillage automatique des comptes pour une durée définie lorsque les utilisateurs ne parviennent pas à se connecter au système après un nombre déterminé de tentatives.
     - Le paramètre `FAILED_LOGIN_ATTEMPTS` indique le nombre d'échecs de connexion autorisés avant le verrouillage du compte.
     - Le paramètre `PASSWORD_LOCK_TIME` définit le nombre de jours pendant lesquels le compte est verrouillé une fois le nombre d'échecs de connexion atteint.

2. Durée de vie des mots de passe et expiration :

Permet de définir la durée de vie des mots de passe utilisateur. Au terme de cette durée, ils expirent et doivent être modifiés.

- Le paramètre `PASSWORD_LIFE_TIME` détermine la durée de vie du mot de passe (en nombre de jours). Au terme de cette durée, le mot de passe expire.
- Le paramètre `PASSWORD_GRACE_TIME` définit la période de grâce (en nombre de jours) permettant de changer le mot de passe après la première connexion réussie suite à l'expiration du mot de passe.

3. **Historique des mots de passe :**

Vérifie le nouveau mot de passe afin de garantir qu'il n'est pas réutilisé pendant une durée déterminée ou avant un certain nombre de changements de mot de passe. Ces vérifications peuvent être implémentées via l'un des paramètres suivants :

- `PASSWORD_REUSE_TIME` : Indique qu'un utilisateur ne peut pas réutiliser un mot de passe pendant un nombre déterminé de jours.
- `PASSWORD_REUSE_MAX` : Indique le nombre de changements de mot de passe requis avant réutilisation du mot de passe actuel.

4. Vérification de la complexité des mots de passe :

- Effectue une vérification de complexité du mot de passe afin de garantir qu'il respecte certaines règles. La vérification doit permettre de garantir que le mot de passe est suffisamment complexe pour offrir une protection contre les intrus qui tenteraient de pénétrer dans le système en devinant le mot de passe.
- Le paramètre `PASSWORD_VERIFY_FUNCTION` nomme une 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` et renvoyer une valeur booléenne (`TRUE` ou `FALSE`).

Création d'un profile (3)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]

Limite le **nombre de session actives simultanément** pour un utilisateur

Création d'un profile (4)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]

Indique la **durée CPU (d'utilisation du processus) maximale autorisée pour la session active**, (exprimée en **centièmes de secondes**)

Les ressources CPU peuvent être limitées par session.

Ex : Avec une limite CPU/Session de 1 000, une session qui utilise ce profile et qui consomme plus de 10 secondes de temps CPU (les limites de temps CPU étant exprimées en centièmes de seconde) reçoit une erreur et est déconnectée :

ORA-02392: exceeded session limit on CPU usage, you are being logged off

Création d'un profile (5)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]

Indique la **durée CPU (d'appel serveur) maximale autorisée pour la session active** (exprimée en **centièmes de secondes**)

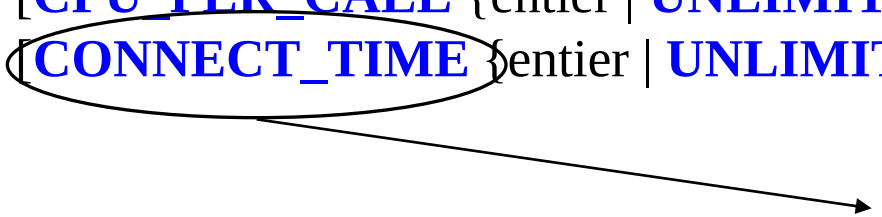
Les ressources CPU peuvent être limitées par appel.

Elle a le même effet que limitation du CPU par session, mais au lieu de limiter la session globale de l'utilisateur, elle **empêche chaque commande de consommer trop de temps CPU**. Si une limite CPU/Call est définie et que l'utilisateur la dépasse, la commande s'arrête et l'utilisateur reçoit un message d'erreur semblable à ce qui suit :

ORA-02393: exceeded call limit on CPU usage

Création d'un profile (6)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]



Indique **la durée maximale de connexion autorisée pour la session active**, (exprimée en **minutes**)

Création d'un profile (7)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]

Exprime **la durée maximale d'inactivité autorisée avant fermeture automatique de la session** (exprimée en **minutes**)

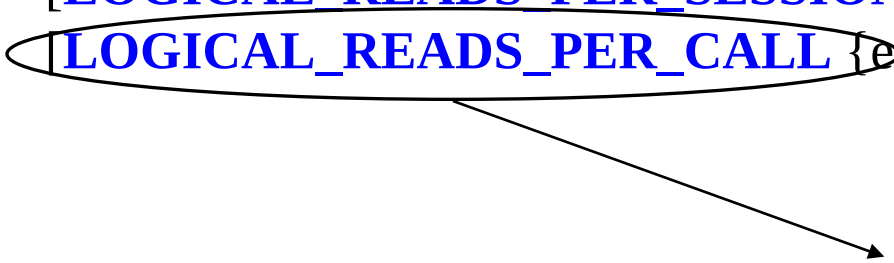
Création d'un profile (8)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]

Indique **le nombre maximal de blocs** qui peuvent être transférés **durant la session**

Création d'un profile (9)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]



Indique **le nombre maximal de blocs** qui peuvent être transférés **lors d'un appel serveur**

Création d'un profile (10)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**PRIVATE_SGA** {entier [K|M]| **UNLIMITED** | **DEFAULT**}]

Permet de gérer la taille allouée à la SGA privée (exprimée en **KO** ou **MO**)
(utilisée uniquement avec l'architecture serveurs partagés)

Création d'un profile (11)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**PRIVATE_SGA** {entier [K|M]| **UNLIMITED** | **DEFAULT**}]
[**FAILED_LOGIN_ATTEMPTS** {entier | **UNLIMITED** | **DEFAULT**}]

Nombre d'essais de connexion infructueux (échoué) avant le blocage du compte

Création d'un profile (12)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**PRIVATE_SGA** {entier [K|M]| **UNLIMITED** | **DEFAULT**}]
[**FAILED_LOGIN_ATTEMPTS** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LIFE_TIME** {entier | **UNLIMITED** | **DEFAULT**}]

Durée maximale d'un mot de passe (période normale)

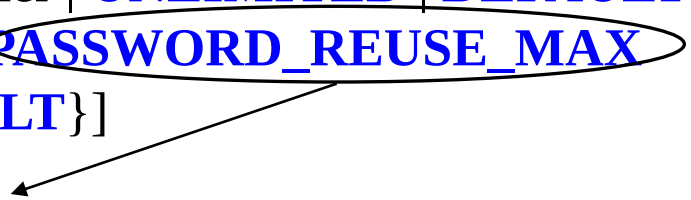
Création d'un profile (13)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**PRIVATE_SGA** {entier [K|M]| **UNLIMITED** | **DEFAULT**}]
[**FAILED_LOGIN_ATTEMPTS** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LIFE_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_REUSE_TIME**| **PASSWORD_REUSE_MAX**
{entier | **UNLIMITED** | **DEFAULT**}]

Nombre de jours qui doit s'écouler avant de pouvoir réutiliser un mot de passe périmé

Création d'un profile (14)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**PRIVATE_SGA** {entier [K|M]| **UNLIMITED** | **DEFAULT**}]
[**FAILED_LOGIN_ATTEMPTS** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LIFE_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_REUSE_TIME** | **PASSWORD_REUSE_MAX**
{entier | **UNLIMITED** | **DEFAULT**}]



Nombre maximal de réutilisation d'un même mot de passe

Création d'un profile (15)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**PRIVATE_SGA** {entier [K|M]| **UNLIMITED** | **DEFAULT**}]
[**FAILED_LOGIN_ATTEMPTS** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LIFE_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_REUSE_TIME** | **PASSWORD_REUSE_MAX**
{entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LOCK_TIME** {entier | **UNLIMITED** | **DEFAULT**}]

Nombre de jours du blocage du compte après un FAILED_LOGIN_ATTEMPS

Création d'un profile (16)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**PRIVATE_SGA** {entier [K|M]| **UNLIMITED** | **DEFAULT**}]
[**FAILED_LOGIN_ATTEMPTS** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LIFE_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_REUSE_TIME** | **PASSWORD_REUSE_MAX**
{entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LOCK_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_GRACE_TIME** {entier | **UNLIMITED** | **DEFAULT**}]

Nombre de jours après la fin de la période normale (PASSWORD_LIFE_TIME) avant que le compte ne soit bloqué

Création d'un profile (17)

CREATE PROFILE nom_profile **LIMIT**
[**SESSIONS_PER_USER** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**CPU_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**CONNECT_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**IDL_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_SESSION** {entier | **UNLIMITED** | **DEFAULT**}]
[**LOGICAL_READS_PER_CALL** {entier | **UNLIMITED** | **DEFAULT**}]
[**PRIVATE_SGA** {entier [K|M]| **UNLIMITED** | **DEFAULT**}]
[**FAILED_LOGIN_ATTEMPTS** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LIFE_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_REUSE_TIME** | **PASSWORD_REUSE_MAX**
{entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_LOCK_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_GRACE_TIME** {entier | **UNLIMITED** | **DEFAULT**}]
[**PASSWORD_VERIFY_FUNCTION** {fonction | **NULL** | **DEFAULT**}] ;

Permet de définir l'algorithme de vérification du mot de passe

Exemple :

```
CREATE PROFILE app_user    LIMIT
SESSIONS_PER_USER          UNLIMITED
CPU_PER_SESSION            UNLIMITED
CPU_PER_CALL               3000
CONNECT_TIME               45
LOGICAL_READS_PER_SESSION  DEFAULT
LOGICAL_READS_PER_CALL     1000
PRIVATE_SGA                15K;
```

3/ Modification d’un profile

Syntaxe:

ALTER PROFILE nom LIMIT

[SESSIONS_PER_USER {valeur | UNLIMITED | DEFAULT }]

….

```
ALTER PROFILE app_user LIMIT
FAILED_LOGIN_ATTEMPTS 5
PASSWORD_LOCK_TIME 1;
```

4/ Affectation d’un profile à un utilisateur

Un profile peut être attribué à un utilisateur

- Lors de la création de l’utilisateur (CREATE USER)
- Lors de la modification de l’utilisateur (ALTER USER)

5/ Suppression d’un profile

DROP PROFILE nom [CASCADE]

Si le profile est attribué à des utilisateurs, l’option CASCADE doit être présente.

Trouver des informations sur les profiles

Plusieurs vues du dictionnaire de données permettent d'obtenir des informations sur les profiles : DBA_USERS et DBA_PROFILES

- DBA_USERS : informations sur les utilisateurs dont le profile attribué
- DBA_PROFILES : informations sur les profiles
  - PROFILE : nom du profil
  - RESSOURCE_NAME : nom de la ressource contrôlée
  - RESSOURCE_TYPE : type de la ressource contrôlée (KERNEL ou PASSWORD)
  - LIMIT : limite de la ressource