Expose :

LA GESTION DES DROITS D'UTILISATEUR SUR MYSQL

Nom des exposants :

- NGUIMOUT PAUL
- SIMO KAMKUMO ROSTAND
- SOPGOUI MBEUKAM LIONEL

INTRODUCTION

Comme dans tout système multi-utilisateur, l'usager d'un SGBD doit être identifié avant de pouvoir utiliser des ressources. L'accès aux informations et à la base de données doit être contrôlé à des fins de sécurité et de cohérence. Le theme de notre travail porte sur la gestion des droits d'utilisateurs. Pour ce faire nous allons :

- - la gestion des utilisateurs à qui on associe des espaces de stockage (tablespaces) dans lesquels se trouveront leurs objets (tables, index, séquences, etc.) ;
- la gestion des privilèges qui permettent de donner des droits sur la base de données (privilèges système) et sur les données de la base (privilèges objets) ;

- - Les différentes méthodes d’implémentation;

I. CLASSIFICATION

Les types d'utilisateurs, leurs fonctions et leur nombre peuvent varier d'une base à une autre. Néanmoins, pour chaque base de données en activité, on peut classifier les utilisateurs de la

manière suivante :

- Le DBA (DataBase Administrator). Il en existe au moins un. Une petite base peut n'avoir qu'un seul administrateur. Une base importante peut en regrouper plusieurs qui se partagent les tâches suivantes :

– installation et mises à jour de la base et des outils éventuels ;

– gestion de l'espace disque et des espaces pour les données (tablespaces) ;

– gestion des utilisateurs et de leurs objets (s'ils ne les gèrent pas eux-mêmes) ;

– optimisation des performances ;

– sauvegardes, restaurations et archivages ;

– contact avec le support technique d'Oracle.

- L’administrateur réseaux (qui peut être le DBA) se charge de la configuration de l’intergiciel (middleware) Oracle Net au niveau des postes clients.
- Les développeurs qui conçoivent et mettent à jour la base. Ils peuvent aussi agir sur leurs objets (création et modification des tables, index, séquences, etc.). Ils transmettent au DBA leurs demandes spécifiques (stockage, optimisation, sécurité).
- Les administrateurs d’applications qui gèrent les données manipulées par l’application ou les applications. Pour les petites et les moyennes bases, le DBA joue ce rôle.
- Les utilisateurs qui se connectent et interagissent avec la base à travers les applications ou à l’aide d’outils (interrogations pour la génération de rapports, ajouts, modifications ousuppressions d’enregistrements).

Tous seront des utilisateurs (au sens Oracle) avec des privilèges différents

- II. CREATION D'UN UTILISATEUR

Pour pouvoir créer un utilisateur vous devez posséder le privilège CREATE USER.

Syntaxe:

```
CREATE USER utilisateurIDENTIFIED
{ BY motdePasse| EXTERNALLY | GLOBALLY AS 'nomExterne'}
[ DEFAULT TABLESPACE nomTablespace
[QUOTA { entier[ K | M ] | UNLIMITED } ON nomTablespace] ]
[TEMPORARY TABLESPACE nomTablespace
[QUOTA { entier[ K | M ] | UNLIMITED } ON nomTablespace ].]
[PROFILE nomProfil] [PASSWORD EXPIRE ] [ ACCOUNT { LOCK |
UNLOCK } ] ;
```

EXPLICATION:

- IDENTIFIED BY motdePasse permet d'affecter un mot de passe à un utilisateurlocal (cas le plus courant et le plus simple).
- IDENTIFIED BY EXTERNALLYpermet de se servir de l'authenticité du système d'exploitation pour s'identifier à Oracle (cas des compte OPS$pour Unix).
- IDENTIFIED BY GLOBALLYpermet de se servir de l'authenticité d'un système d'annuaire.
- DEFAULT TABLESPACE nomTablespace associe un espace disque de travail (appelé tablespace) à l'utilisateur.
- TEMPORARY TABLESPACE nomTablespace associe un espace disque temporaire (dans lequel certaines opérations se dérouleront) à l'utilisateur.
- QUOTApermet de limiter ou pas chaque espace alloué.
- PROFILE nomProfilaffecte un profil (caractéristiques système relatives au CPU et aux connexions) à l'utilisateur.

- PASSWORD EXPIRE pour obliger l'utilisateur à changer son mot de passe à la première connexion (par défaut il est libre). Le DBA peut aussi changer ce mot de passe.
- ACCOUNT pour verrouiller ou libérer l'accès à la base (par défaut UNLOCK).

En l'absence de clause sur les espaces disque, le tablespace SYSTEM est associé à l'utilisateur en tant qu'espace de travail et d'espace temporaire. Il existe d'autres tablespaces créés par Oracle, citons USERS (celui que vous devriez utiliser pour votre espace par défaut) et TEMP

(celui que vous devriez employer pour votre espace temporaire). Vous pouvez aussi créer vos espaces via la console d'administration La clause ALTER USER permet d'affecter un espace de travail ou temporaire différent de celui du départ.

- **En l'absence de profil, le profil DEFAULTest affecté à l'utilisateur.**

Par défaut, les utilisateurs, une fois créés n’ont aucun droit sur la base de données sur laquelle ils sont connectés. La section « Privilèges » étudie ces droits.

II. MODIFICATEUR D'UN UTILISATEUR

Pour pouvoir modifier les caractéristiques d'un utilisateur (autres que celle du mot de passe)
vous devez posséder le privilège ALTER USER

Syntaxe

Les instructions utilisées reprennent les options étudiée lors de la création d'un utilisateur.

ALTER USER *utilisateur*

- Pour pouvoir modifier les caractéristiques d'un utilisateur (autres que celle du mot de passe)
  vous devez posséder le privilège ALTER USER

- ***Syntaxe***
  Les instructions utilisées reprennent les options étudiée lors de la création d'un utilisateur.

- **ALTER USER** *utilisateur*

- [IDENTIFIED { BY *password* [REPLACE *old_password*] | EXTERNALLY | GLOBALLY AS ' *external_name*' }]
  [DEFAULT TABLESPACE *nomTablespace*
  [QUOTA { *entier* [K | M] | UNLIMITED } ON *nomTablespace*]]
  [TEMPORARY TABLESPACE *nomTablespace*
  [QUOTA { *entier* [K | M] | UNLIMITED } ON *nomTablespace*].]
  [PROFILE *nomProfil*]
  [DEFAULT ROLE { *rôle1* [, *rôle2*]… | ALL [EXCEPT *rôle1* [, *rôle2*]…] | NONE }
  [PASSWORD EXPIRE] [ACCOUNT { LOCK | UNLOCK }] ;

- PASSWORD EXPIRE oblige l’utilisateur à changer son mot de passe à la prochaine connexion.

- DEFAULT ROLE affecte à l’utilisateur des rôles qui sont en fait des ensembles de privilèges.

- Chaque utilisateur peut changer son propre mot de passe à l’aide de cette instruction. Les autres changements seront opérationnels aux prochaines sessions de l’utilisateur mais pas à la session courante.

- Exemple

- **ALTER USER** Paul
  IDENTIFIED BY X_Men
  TEMPORARY TABLESPACE TEMP
  QUOTA UNLIMITED ON TEMP;

- *Paul* a changé de mot de passe, son espace temporaire est illimité dans TEMP. Il ne devra plus changer son mot de passe à la première connexion

III. SUPPRESSION DES UTILISATEURS

Pour pouvoir supprimer un utilisateur vous devez posséder le privilège DROP USER.

- Un utilisateur connecté ne peut pas être supprimé en direct avec cette commande. Pour forcer cette suppression, il faut arrêter ses sessions par la commande ALTER SYSTEM et l'option KILL SESSION.
- Si vous désirez effacer juste l'utilisateur en tant qu'entrée dans la base sans supprimer ses objets, préférez le retrait par REVOKE du privilège CREATE SESSION.

SYNTAXE

La syntaxe SQL pour supprimer un utilisateur est la suivante :

DROP USER utilisateur[CASCADE];

Oracle ne supprime pas par défaut un utilisateur s'il possède des objets (tables, séquences, index, déclencheurs, etc.). L'option CASCADEforce la suppression et détruit tous les objets du schéma de l'utilisateur.

Conséquences

- Les contraintes d'intégrité d'autres schémas qui référençaient des tables du schéma à détruire sont aussi supprimées.
- Les vues, synonymes, procédures ou fonctions cataloguées définis à partir du schéma détruit mais présents dans d'autres schémas ne sont pas supprimés mais invalidés.
- Les rôles définis par l'utilisateur à supprimer ne sont pas détruits par l'instruction DROP USER.

Profils

- Un profil regroupe des caractéristiques système (ressources) qu'il est possible d'affecter à un ou plusieurs utilisateurs

.Un profil est identifié par son nom. Un profil est créé par CREATE PROFILE, modifié par ALTER PROFILEet supprimé par DROP PROFILE. Il est affecté à un utilisateur lors de sa création par CREATE USERou après que l'utilisateur est créé par ALTER USER. Le profil DEFAULTest affecté par défaut à chaque utilisateur si aucun profil défini n'estprécisé.
Création d'un profil (CREATE PROFILE)

Pour pouvoir créer un profil vous devez posséder le privilège CREATE PROFILE.

SYNTAXE

CREATE PROFILE nomProfil LIMIT

{ ParamètreRessource| ParamètreMotdePasse}

[ParamètreRessource| ParamètreMotdePasse]…;

ParamètreRessource:

{ { SESSIONS_PER_USER | CPU_PER_SESSION | CPU_PER_CALL| CONNECT_TIME | IDLE_TIME | LOGICAL_READS_PER_SESSION| LOGICAL_READS_PER_CALL | COMPOSITE_LIMIT } { entier| UNLIMITED | DEFAULT }| PRIVATE_SGA {entier[K|M] | UNLIMITED | DEFAULT}}

ParamètreMotdePasse:

{ FAILED_LOGIN_ATTEMPTS | PASSWORD_LIFE_TIME | PASSWORD_REUSE_TIME

| PASSWORD_REUSE_MAX | PASSWORD_LOCK_TIME | PASSWORD_GRACE_TIME }

{ expression| UNLIMITED | DEFAULT } }

- ● SESSIONS_PER_USER: nombre de sessions concurrentes autorisées.
- ● CPU_PER_SESSION: temps CPU maximal pour une session en centièmes de secondes.
- ● CPU_PER_CALL: temps CPU autorisé pour un appel noyau en centièmes de secondes.
- ● CONNECT_TIME: temps total autorisé pour une session en minutes (pratique pour les
- examens de TP minutés).
- ● IDLE_TIME: temps d'inactivité autorisé, en minutes, au sein d'une même session (pour
- les étudiants qui ne clôturent jamais leurs sessions).
- ● PRIVATE_SGA: espace mémoire privé alloué dans la SGA (System Global Area).
- ● FAILED_LOGIN_ATTEMPTS: nombre de tentatives de connexion avant de bloquer l'utilisateur (pour la carte bleue, c'est trois).
- ● PASSWORD_LIFE_TIME: nombre de jours de validité du mot de passe (il expire s'il n'est
- pas changé au cours de cette période).

- PASSWORD_REUSE_TIME: nombre de jours avant que le mot de passe puisse être utilisé à nouveau. Si ce paramètre est initialisé à un entier, le paramètre PASSWORD_REUSE_MAX doit être passé à UNLIMITED.
- PASSWORD_REUSE_MAX: nombre de modifications de mot de passe avant de pouvoir réutiliser le mot de passe courant. Si ce paramètre est initialisé à un entier, le paramètre PASSWORD_REUSE_TIME doit être passé à UNLIMITED.
- PASSWORD_LOCK_TIME: nombre de jours d'interdiction d'accès à un compte après que le nombre de tentatives de connexions a été atteint (pour la carte bleue, ça dépend de plein de choses, de toute façon vous en recevrez une autre toute neuve mais toute chère…).
- PASSWORD_GRACE_TIME: nombre de jours d'une période de grâce qui prolonge l'utilisation du mot de passe avant son changement (un message d'avertissement s'affiche lors des connexions). Après cette période le mot de passe expire.

Les limites des ressources qui ne sont pas spécifiées sont initialisées avec les valeurs du profil DEFAULT.

Par défaut toutes les limites du profil DEFAULT sont à UNLIMITED. Il est possible de visualiser chaque paramètre de tout profil en interrogeant certaines vues du dictionnaire de données (voir le chapitre suivant).

CONCLUSION

- Sur Mysql, la gestion des utilisateurs passe par plusieurs prérequis, à savoir, la création, la modification, ainsi que la suppression des utilisateurs.
- Pour ce faire, de nombreuses méthodes sont mises à notre disposition. Méthodes dont la quintéssance vous a été présenté plus haut.
- Il est à noter que Mysql permet aussi de modifier les utilisateurs de tel sorte que chacun puisse gérer les droits d’accès comme un administrateur principal.