- Gestion des utilisateurs
- Gestion des profils
- Gestion des privilèges
- Gestion des rôles

Gestion des utilisateurs

Schéma de base de données

- Schéma
  - Peut être vu comme un compte Oracle
  - Collection
    - De tables
    - De vues
    - D'index
    - ...(cf Oracle Schema Manager)
- Utilisateur de BD = Schéma
  - Souvent utilisé de façon indifférente

Liste de contrôle pour la création d'utilisateur

- Choisir un nom d'utilisateur et un mécanisme d'authentification
- Identifier les tablespaces dans lesquels l'utilisateur va stocker ses objets
- Décider des quotas pour chaque tablespaces
- Affecter un tablespace par défaut et un tablespace temporaire
- Créer un utilisteur
- Accorder des privilèges et des rôles à l'utilisateur

Exemples

- Avec svrmrg :
  - Authentification par Oracle
    - CREATE USER Paul IDENTIFIED BY edze!2z
      DEFAULT TABLESPACE data01
      TEMPORARY TABLESPACE temp QUOTA 1M ON data01;
  - Authentification par le SE
    - CREATE USER Paul IDENTIFIED EXTERNALLY
      DEFAULT TABLESPACE data01
      TEMPORARY TABLESPACE temp QUOTA 1M ON data01;
    - *Conseil Oracle :* A utiliser avec modération !
- Avec OEM
  - *Oracle Security Manager*

Modification

- Avec ordre ALTER USER
- Exemples :
  - Changement de compte
    - ALTER USER Paul IDENTIFIED BY edze!2z
      PASSWORD EXPIRE; → force l'utilisateur à changer son mdp
  - Suppression de quota
    - ALTER USER Paul QUOTA 0 ON data01;
      - Les données existantes restent
      - Mais plus possible d'en insérer d'autres
  - Quota illimité
    - ALTER USER Paul QUOTA UNLIMITED ON data01;

Cf) si aucun quota n'a été spécifié, l'utilisateur ne peut pas créer d'objets dans la base.

Suppression

- Syntax :
  - DROP USER utilisateur [CASCADE]
- Option CASCADE
  - Supprime tous les objets du schéma
  - Puis supprime l'utilisateur
- Impossible de supprimer un utilisateur connecté
- Exemple :
  - DROP USER Paul CASCADE;

Informations sur les utilisateurs

- Utiliser les vues
  - DBA_USERS
  - DBA_TS_QUOTAS
- Exemples :
  - Select username, default_tablespace,
    temporary_tablespace
    from dba_users
    where username = 'PAUL';
  - Select * from dba_ts_quotas
    where username = 'PAUL'

Gestion des profils

- Pour limiter les ressources (et de mot de passe V8)
  - E.g. nombre de connexions simultanées par utilisteur
- Affectés aux utilisateurs
  - Lors de leur création
  - Par modification
  - Peuvent dériver du profil DEFAULT (une utilisation illimitée des ressources)

Quelques ressources limitées par des profils

- Sessions_per_user : nombre de sessions concurrentes d'un utilisateur dans une instance
- Connect_time : temps de connexion d'une session à la base (en minutes)
- Idle_time : temps de connexion d'une session à la base sans être activement utilisée (en minutes)
- Failed_login_attempts : nombre d'échecs de tentatives de login qui provoquent le blocage d'un compte
- Password_life_time : nombre de jours d'utilisation d'un mot de passe restants avant qu'il n'expire
- Password_reuse_time : nombre de jours qui doivent s'écouler avant qu'un mot de passe puisse être réutilisé
- Password_lock_time : nombre de jours de verrouillage d'un compte lorsque la valeur du paramètre failed_login_attempts est dépassée. ...
  - Cf) alter user paul account unlock [lock] : pour déverrouiller un compte bloqué [pour bloquer un compte]

Gestion des ressource à l'aide des profils

- Etapes à suivre :
  - Créer les profils
    - Ordre CREATE PROFIL
  - Les affecter à l'utilisateur
    - Ordre CREATE/ALTER USER
  - Activer les limites de ressources
    - Soit ALTER SYSTEM
    - Soit fichier de paramètres d'initialisation
  - Exemple)

```
create profile new_prof limit sessions_per_user 2
                                        idle_time 1;
alter user Paul profile new_prof;
alter system set RESOURCE_LIMIT=true;
```


Modification/Suppression

- Modification
  - Ordre ALTER PROFILE
  - Exemple :
    - Alter profile new_prof limit sessions_per_user 3 idle_time 2;
- Suppression
  - Ordre DROP PROFILE
    - Option CASCADE : assure que tous les utilisateurs ayant ce profil seront mis à jour !
  - Le profile DEFAULT ne peut être supprimé
  - Exemple : drop profile new_prof cascade;
- Entre en vigueur pour les sessions suivantes

Informations sur les profils

- Utiliser les vues
  - DBA_USERS
  - DBA_PROFILES

- Exemples :

```
Select distinct profile from dba_profiles;
Select * from dba_profiles where
                    profile='DEFAULT';
Select resource_name, limite from
  dba_profiles where profile='DEFAULT';
```


Gestion des privilèges

Privilèges

- Deux types de Privilèges
  - SYSTEM
    - Permet aux utilisateurs d'effectuer des opérations dans les base de données
    - Environ 80 privilèges systèmes
    - Ex) create session, create table, create any table, drop any table, select any table, create user, alter user, create view, create any view,create cluster, create tablespace, ...
    - Note) *create session* : pour que l'utilisateur puisse se connecter au serveur
  - OBJET
    - Permet aux utilisateurs d'accéder à/manipuler un objet particulier

- Ordre GRANT permet d'ajouter un privilège à un utilisateur
  - Exemple : GRANT create session, create table TO Paul;
- Ordre REVOKE pour le supprimer
  - Exemple : REVOKE create table FROM Paul;
  - REVOKE all FROM Paul;

Attribution de privilèges systèmes

- Avec l'option
  - GRANT...TO...WITH ADMIN OPTION;
- Pour accorder un privilège système, il faut posséder le privilège WITH ADMIN OPTION => avec cette option l'utilisateur ayant reçu le privilège peut le donner lui aussi (il peut transmettre le privilège)
- Avec OEM, utiliser Oracle Security Manager
- Privilèges SYSDBA et SYSOPER
  - SYSDBA = privilèges de SYSOPER WITH ADMIN OPTION + CREATE DATABASE...

Privilèges Objets

- Permet aux utilisateurs d'accéder à des objets (une table, vue, procédure, index, ...) dont ils ne sont pas propriétaires.
  - => on peut utiliser des rôles afin de faciliter l'administration des privilèges.
- Les principaux privilèges Objet :
  - SELECT, INSERT, UPDATE, DELETE, ALTER, (pour les tables),INDEX (créer des index sur la table), EXECUTE (pour les procédures, fonctions)
- Exemples :
  - GRANT execute ON dbms_pipe TO public;
  - GRANT select ON emp TO Bob WITH GRANT OPTION;
  - REVOKE execute ON dbms_pipe FROM scott;

- Ex) with grant option
- Connect paul/paul
  - Grant select, update(name) on empoyee to bob with grant option;
- Connect bob/bob
  - Grant select on paul.employee to sylvie ;
- Connect paul/paul
  - REVOKE select on employee FROM bob;
- Connect sylvie/sylvie
  - Select * from paul.employee ; ? pas accès

Informations sur les privilèges

- Interroger les vues
  - Pour les privilèges SYSTEM :
    - DBA_SYS_PRIVS
  - Pour les privilèges OBJET :
    - DBA_TAB_PRIVS : privilèges sur des tables
    - DBA_COL_PRIVS : privilèges sur des colonnes
- Exemples :
  - Select * from DBA_SYS_PRIVS;
  - Select * from DBA_TAB_PRIVS where grantee='BOB';

Gestion des rôles

Rôles

- A mi-chemin entre
  - les utilisateurs
    - Ordre de création de rôle similaire
  - Les privilèges
    - Assure l'affectation de plusieurs privilèges
- Gestion simplifiée des privilèges
- Disponibilité sélective des privilèges

Création/affectation de rôles

- Création
  - Ordre CREATE ROLE
  - Exemple svrmgr :
    - CREATE ROLE Vente;
    - CREATE ROLE Vente IDENTIFIED BY Bonus;
    - CREATE ROLE Vente IDENTIFIED EXTERNALLY;
  - Sous OEM :
    - Oracle Security Manager
- Affectation
  - Ordre GRANT
  - Exemples :
    - GRANT create any table TO Vente;
    - GRANT Vente TO scott;
    - GRANT Vente TO scott WITH ADMIN OPTION;

    => permet de transmettre à d'autre utilisateur le rôle

Quelques rôles fournis par Oracle

- CONNECT : ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW

  => attribué en général aux utilisateurs finaux. Bien qu'il autorise la création d'objets (create table), il n'accorde aucun quota sur aucun tablespace. Les utilisateurs ne peuvent pas créer de tables.
- DBA : tous les privilèges système en plus de WITH ADMIN OPTION
- RESOURCE : CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE

  => accordé aux développeurs.

- SELECT_CATALOG_ROLE : privilège select sur toutes les tables et vues de catalogue (dictionnaire de données)
- DELETE_CATALOG_ROLE : privilège DELETE sur tous les packages de dictionnaire
- EXP_FULL_DATABASE : SELECT ANY TABLE, BACKUPANY TABLE, EXECUTE ANY PROCEDURE, EXECUTE ANY TYPE, INSERT,DELETE, et UPDATE sur les tables SYS.INCVID, SYS.INCFIL, et SYS.INCEXP.

Rôles par défaut aux utilisateurs

- Syntaxe :
  - ALTER USER...DEFAULT ROLE [...|ALL] [EXCEPT...];
- Exemples :
  - ALTER USER scott DEFAULT ROLE Vente, Achat;
  - ALTER USER scott DEFAULT ROLE ALL;
  - ALTER USER scott DEFAULT ROLE ALL EXCEPT Vente;
  - ALTER USER scott DEFAULT ROLE NONE;
- Suppression des rôles :
  - DROP ROLE role
- Suppression des rôles d'un utilisateur
  - REVOKE role FROM [util|PUBLIC];

Conseils

- Créer un rôle pour chaque tâche d'application
  - E.g. traitement du salaire
- Attribuer aux rôles d'application les privilèges nécessaires pour exécuter la tâche
- Créer un rôle pour chaque type d'utilisateur
  - E.g. chef de service
- N'attribuer aux rôles d'utilisateur que des rôles d'application
  - Ne pas affecter des privilèges individuels
- Accorder des rôles d'utilisateurs aux utilisateurs

Information sur les rôles

- Interroger les vues
  - DBA_ROLES
    - Tous les rôles de la bd
  - DBA_ROLE_PRIVS
    - Rôles accordés aux utilisateurs et aux rôles
  - ROLE_ROLE_PRIVS
    - Rôles accordés aux rôles
  - DBA_SYS_PRIVS
    - Privilèges accordés aux utilisateurs et aux rôles
  - ROLE_SYS_PRIVS
    - Privilèges accordés aux rôles
  - ROLE_TAB_PRIVS
    - Privilèges de table accordés aux rôles
  - SESSION_ROLES
    - Rôles d'un utilisateur actuellement activés

Sauvegarde et restauration

Notion de base

- Sauvegarde : copie de données
  - Englobe une grande parties de la BD (fichiers de données, fichier de contrôles ...)
  - Une sécurité contre le risque de perte de données
- Restauration
  - Reconstruction d'une (partie) de la BD à partir d'une sauvegarde

Deux type de sauvegarde

- Sauvegarde logique :
  - Ecriture d'un ensemble d'enregistrements de la base données dans un fichier binaire
  - Indépendance par rapport à la localisation physique
  - Outil : oracle Export utility, OEM ou RMAN
  - Méthodes : Export (Import)
- Sauvegarde physique
  - Copie des fichiers indépendamment de leur contenu logique,
  - Outil : RMAN ou utilitaires/commandes de sauvegarde du S.E
  - Méthodes :
    - 1. Sauvegarde base fermée : Dites sauvegarde à froid
    - 2. Sauvegarde base ouvert : Dite sauvegarde à chaud

Export/Import

- Export
  - lire la BD et écrit des informations dans un fichier appelé fichier d'export (dump)
  - possibilité d'exporter une BD complète, certains utilisateurs ou certains tables, dictionnaire de données
    - Ex) exp help=y : visualiser l'ensemble des paramètres
- Import
  - lire le fichier dump et exécute les commandes qu'il y trouve.

Ex) copier les objets de bob dans le compte de kay

```
exp file=bob.dat owner=bob grant=N;
imp file=bob.dat fromuser=bob touser=kay
```

Utilitaire d'exportation

- Trois niveau de fontionnalités
  - table
  - utilisateur
  - base de données
- Mode table (Table mode)
  - Exportation d'une table particulière (structure, index, ...) avec/sans les données
  - Ex) `exp scott/tiger grants=Y tables=(EMP,DEPT)`
- Mode utilisateur (User mode)
  - Exportation des objets d'un utilisateur
- Mode base de données (Full mode)
  - Exportation de la base de données complète
  - nécessite le privilège cf EXP_FULL_DATABASE

Utilitaire : exp

- Commande
  - EXP KEYWORD=value or KEYWORK=(value1, value2,..., valueN)
  - EX) exp scott/tiger grants=Y tables=(EMP,DEPT)
  - Ex) Exp help=Y
- Options
  - Help aide :affiche les otions possibles (N)
  - USERID : user et password de connexion
  - BUFFER : taille du data buffer
  - FILE : fichier de sortie ou d'export (EXPDAT.DMP)
  - GRANTS : export des grants (Y)
  - INDEXES : export des index (Y)
  - CONSTRAINTS : export des constraintes (Y)
  - ROWS : export des données aussi (Y)

- FULL : export du fichier entier (N)
- OWNER : liste des utilisateurs a exporter (en mode User)
- TABLES : liste des tables
- QUERY : select clause used to export a subset of a table
- INCTYPE : export différentiel de type (incrémental, cumulative ou complete)
- FEEDBACK n : indique la progression de l'export table par table. 1 caractère affiché pour n lignes exportées
- RECORD : marquage des export incrementaux (différentiels) dans le dictionnaire (Y)
- CONSISTENT : image avant consistante de l'export (mises a jour autorisées)
- LOG : log file of screen output

Différentes type d'export

- Complet
  - Exportation de toutes les tables spécifiées
- Cumulatif
  - Exportation de toutes les tables qui ont changé depuis le dernier exp (complet ou cumulatif)
- Incrémental
  - Exportation de toutes les tables qui ont changé depuis le dernier exp (tous types)

=> Paramètre INCTYPE

- Valeurs : complet (par défaut), cumulative, incremental

Import

- Ordre dans lequel les objets sont 'importés :
  - structures de tables
  - données
  - index
  - contraintes d'intégrité et triggers

- Pour faire un import FULL, il faut être DBA ou posséder le role IMP_FULL_DATABASE

- Ex) imp scott/tiger file=emp.dmp log=imp.log ignore=y

- HELP : décrit les paramètres de l'import
- USERID : username/password de connexion
- FULL : import complet (N)
- BUFFER : taille du data buffer
- FROMUSER : liste des propriétaires exportés
- FILE : fichier d'entrée (EXPDAT.DMP)
- TOUSER: liste des propriétaires cibles de l'import
- SHOW : liste les objets à importer, sans importer ! (N)
- TABLES : liste des tables
- IGNORE : ignore les erreurs due aux objets déjà existants (N)
- GRANTS : import des droits (Y)
- INDEXES : import les indexs aussi (Y)
- ROWS : importe aussi le contenu des tables (Y)
- INCTYPE : import de type différentiel
- LOG : trace des sorties écran
- DESTROY : écrase le fichier du tablespace (N)
- CHARSETcharacter set du fichier d'export (NLS_LANG)
- FEEDBACK n : indique la progression de l'import table par table. 1 caractère affiché pour n lignes importées

Sauvegarde physique

- Sauvegarde base fermée
  - Dite sauvegarde à froid
- Sauvegarde base ouvert
  - Dite sauvegarde à chaud
- Différentes possibilités liées
  - Au choix du mode d'archivage des fichiers de reprise
    - Mode NoArchibelog
      - La sauvegarde la plus récente est utilisée pour restaurer la base
        - » Perte d'information possible
    - Mode Archivelog
      - Idem + fichiers de reprise archivés
        - » Pas de perte d'information

Sauvegarde à froid

- La plus simple à mettre en œuvre
- Les étapes :
  - Identification des fichiers
    - Select name from v$datafile;
    - Select member from v$logfile;
    - Select name from v$controlfile;
  - Arrêter la base
  - Sauvegarder tous ces fichiers et (éventuellement) le fichier init.ora
  - Redémarrer la base

- En cas d'erreur, copie de ces fichiers pour redémarrer
  - Perte d'information possible

Sauvegarde à chaud

- Plus difficile à mettre en œuvre
  - Nécessite le mode ARCHIVELOG
    - Possible aussi en mode Noarchivelog mais les fichiers sauvés ne sont pas utilisables pour une restauration
- Sauvegarde des fichiers de données
  - Tablespace déactivés
    - Alter tablespace tbs offline;
    - Copier les fichiers à partir du SE
    - Alter tablespace tbs online;
  - Tablespace activés
    - Alter tablespace tbs BEGIN BACKUP;
    - Copier les fichiers à partir du SE
    - Alter tablespace tbs end backup;
- Sauvegarde des fichiers de contrôles
  - Alter database backup controlfile to 'e:\backup\control01.ctl' ;

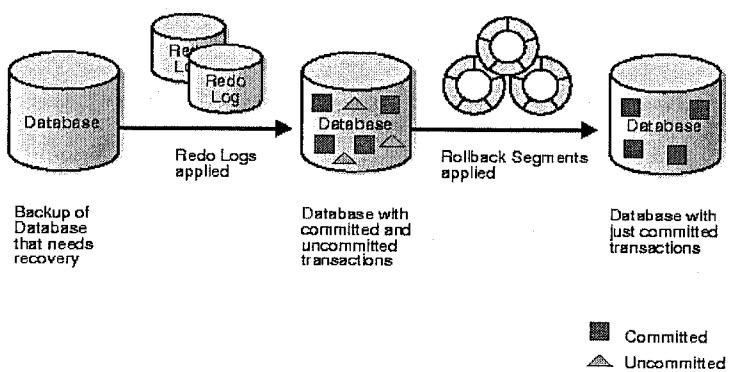
Requêtes

- Sur le mode d'archivage
  - Select log_mode from v$database;
- En mode archivage
  - Informations sur les tablespaces actuellement sauvegardés
    - V$backup, v$datafile_header

Restauration

- Mode Noarchivelog
  - Perte des données saisies depuis la dernière sauvegarde
  - Restauration de tous les fichiers
- Mode Archivelog
  - Différentes restauration :
    - Restauration complète
      - Bd fermée
      - BD ouverte, tablespaces déactivés
      - BD ouverte, tablespaces désactivés, fichiers de données endommagés
      - Fichier de contrôle corrompu
    - Restauration incomplète
      - Basé sur l'annulation
      - Basé sur les modications et sur le temps
    - Commande 'Recover' (dans SQL*PLUS)

Restauration: le principe



Restauration complète

- Mode Noarchivage

- Les étapes :
  - Fermer la base
  - Réparer la panne disque
  - Restaurer tous les fichiers de la sauvegarde la plus récente
  - Ouvrir la base à l'étape open
    - Si les emplacements des fichiers ont changé, il faut renommer ces fichiers au niveau du fichier de contrôle
      - Redémarrer la base à l'étape MOUNT
    - Des donnés peuvent avoir été perdues

Restauration en mode Archivelog

- Commande recover
  - Recover database

```
RECOVER [AUTOMATIC] [FROM location]
   {[STANDBY] DATABASE [UNTIL options]
                       [USING BACKUP CONTROLFILE]
    |TABLESPACE {tablespace [, tablespace ...]}
    |DATAFILE {datafilename [, datafilename ...]}
    |STANDBY {TABLESPACE tablespace [,tablespace ...]
      |DATAFILE datafilename [, datafilename ...]}
                       UNTIL CONTROLFILE
    |LOGFILE filename
    |CONTINUE [DEFAULT]
    |CANCEL}
   [PARALLEL clause]
```

- Possibilité de restaurer
  - toute la base, des tablespaces, la fichier de contrôle ou des fichiers de données

Exemple de restauration partielle

Ex) Mode Archivlog, base ouverte, tablespace désactivé

1. Ouvrir la base à l'étape OPEN
2. Désactiver le(s) tablespace(s) : ALTER TABLESPACE nom OFFLINE
3. Réparer la panne disque
4. Restaurer seulement les fichiers endommagés
5. Lancer la restauration

   RECOVER TABLESPACE tablespace

   ou pour chaque fichier de données

   RECOVER DATAFILE nom_fich
7. Activer le tablespace : ALTER TABLESPACE nom ONLINE