Administration des bases de données

Jean-Yves Antoine

http://www.info.univ-tours.fr/~antoine/

Administration des bases de données

III — Protection des données : contrôles d'accès

OBJECTIFS

3.1. NOTIONS

3.1.1. Politiques de contrôle d'accès aux données

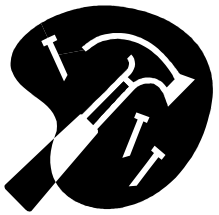
3.1.2. Contrôle discrétionnaire : privilèges

3.1.3. Contrôle à base de rôles

3.2. PRATIQUES

3.2.1. Contrôle discrétionnaire sous Oracle

3.2.2. Contrôle d'accès par rôle sous Oracle



POLITIQUES DE CONTRÔLE D'ACCES

Trois modèles principaux de contrôle des accès dans les systèmes d'information

Politique de contrôle discrétionnaire (DAC)

Politique de contrôle à base de rôles (RBAC)

Politique de contrôle obligatoire (MAC)

POLITIQUES DE CONTRÔLE D'ACCES

Politique de contrôle discrétionnaire

Privilèges spécifiques de chaque utilisateur sur chaque objet

Politique de contrôle à base de rôles

- **Privilèges** spécifiques à un rôle correspondant à une fonction dans l'institution utilisant le système d'information
- Utilisateurs rattachés à un rôle particulier.

Politique de contrôle obligatoire

Idée: les choix de protection ne doivent pas être pris par l'utilisateur

- **Niveaux de classification** des objets
- **Niveaux d'habilitation** des utilisateurs

Exemple

U peut accéder à objet O	si Niveau habilit. U	>	Niveau classif O
U peut modifier un O	si Niveau habilit. U	=	Niveau classif O

CONTRÔLE DISCRETIONNAIRE

Norme SQL (2008)

- Autorise la gestion de privilèges : contrôle d'accès discrétionnaire et/ou à base de rôles
- Ordres LCD (Langage de Contrôle de Données)

```
GRANT […] TO utilisateur | role

REVOKE […] FROM utilisateur | role

CREATE ROLE nom
…
```

- Standard SQL assez général dans la gestion de privilèges : extensions / spécificités propres à chaque SGBD.

CONTRÔLE DISCRETIONNAIRE

Type de privilège

– **Privilège système** : droit global d'exécuter un type d'ordre SQL

Exemple : CREATE TABLE, ALTER TABLE etc…

```
GRANT priv TO utilisateur | role
REVOKE priv FROM utilisateur | role
```

– **Privilège objet** : droit d'exécuter un type d'action (lecture, mise à jour…) sur un objet précis

Exemple: SELECT, UPDATE, INSERT etc…

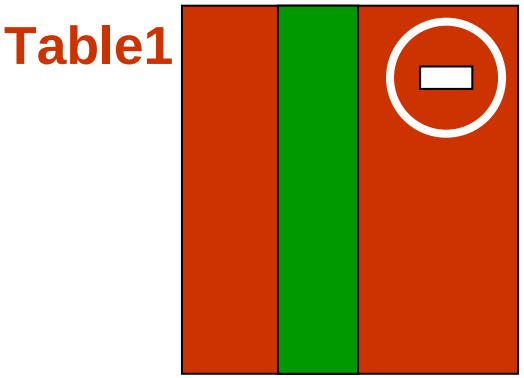
Par défaut, un utilisateur a tous les privilèges **objet** sur les objets qui lui appartiennent, les autres aucun (sauf DBA)

```
GRANT priv ON objet TO utilisateur | role
REVOKE priv ON objet FROM utilisateur | role
```

```
GRANT priv ON objet(att1,…attn) TO utilisateur | role
REVOKE priv ON obj(att1,…,attn) FROM utilisateur | role
```

VUES ET CONTRÔLE D'ACCES

Vues moyen aisé d'avoir un contrôle direct sur les accès



Att1 : select OK pour PUBLIC

GRANT sur attributs

```
GRANT SELECT ON Table1 (Att1) TO PUBLIC;
```

GRANT sur vue

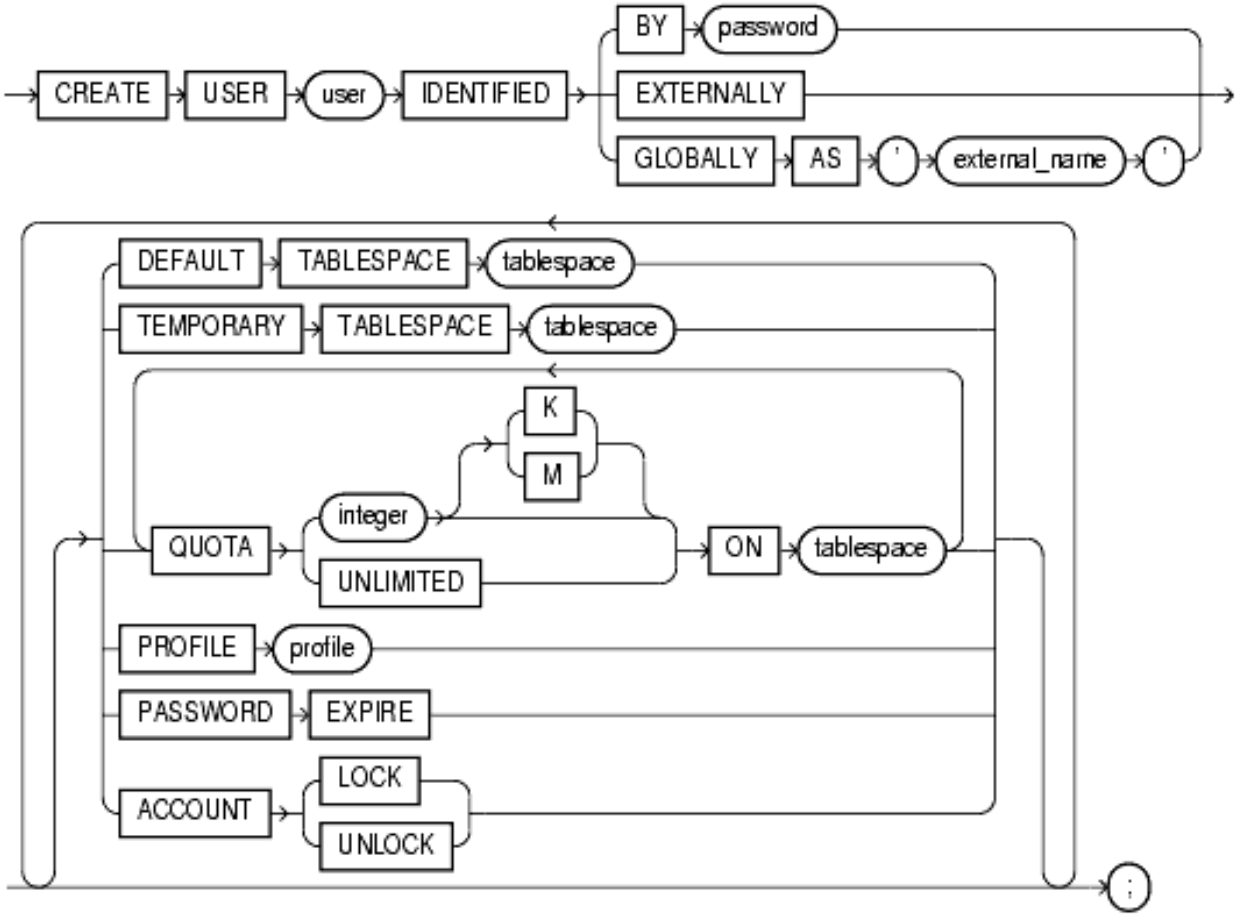
```
CREATE VIEW S_ATT1 AS
SELECT Attr1 FROM Table1;

GRANT SELECT ON  S_ATT1 TO PUBLIC;
```

ORACLE : UTILISATEURS

Création

- Droit de création limité au DBA (utilisateur prédéfini : SYSTEM)
- Accorde un droit de connexion à l'utilisateur



ORACLE : UTILISATEURS

Création

```
CREATE USER <nom_id>
IDENTIFIED BY { <password> | EXTERNALLY }
[ DEFAULT TABLESPACE <nomTableSp>
            [QUOTA { <n> [ K | M ] | UNLIMITED]]
[PROFILE <NomProfile>]
[PASSWORD EXPIRE]        [ACCOUNT { LOCK | UNLOCK } ]
```

DEFAULT TABLESPACE	espace disque de travail
EXTERNALLY	récupère le password du compte utilisateur sur l'O.S.
PROFILE	caractéristiques d'utilisation du serveur
PASSWORD EXPIRE	Demander à l'utilisateur de changer son password
ACCOUNT LOCK	création mais compte encore verrouillé

ORACLE : UTILISATEURS

Modification

Privilège DBA par défaut

- Mot de passe

```
ALTER USER <nom_id> IDENTIFIED BY <new_password>
[REPLACE <old_password> ]
```

- Toute autre propriété

Exemple ALTER USER <nom_id> ACCOUNT LOCK

Suppression

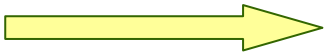
```
DROP USER <nom_id> [CASCADE]
```

CASCADE suppression des objets de l'utilisateur (nécessite sinon de les supprimer avant)

ORACLE : UTILISATEURS

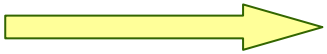
Dictionnaire Oracle

- ALL_USERS
- USER_USERS



USERNAME
USER_ID
CREATED

- DBA_USERS



USERNAME
USER_ID
PASSWORD
ACCOUNT_STATUS
LOCK_DATE
EXPIRY_DATE
DEFAULT_TABLESPACE
TEMPORARY_TABLESPACE
CREATED
PROFILE
…

ORACLE : PRIVILEGES

Privilèges systèmes : CREATE, ALTER et DROP

Exemple : CREATE TABLE, CREATE VIEW, CREATE SESSION…

Par défaut, pour les objets « courants » (table, vue, séquence, synonyme), droit généralement limité à CREATE.

Définition de privilège système

```
GRANT { privilège_système | ALL_PRIVILEGES}
TO { utilisateur | PUBLIC } [WITH ADMIN OPTION]
```

ADMIN OPTION

Transfert au bénéficiaire du droit d'attribuer les mêmes privilèges **systèmes** aux utilisateurs de son choix

Retrait de privilège système

```
REVOKE { privilege_systeme | ALL_PRIVILEGES}
FROM { utilisateur | PUBLIC }
```

ORACLE : PRIVILEGES

Dictionnaire Oracle

- ALL_TAB_PRIVS
- USER_TAB_PRIVS

GRANTOR
GRANTEE
TABLE_SCHEMA
TABLE_NAME
COLUMN_NAME
PRIVILEGE
GRANTABLE
HIERARCHY

- ALL_COL_PRIVS
- USER_COL_PRIVS

- ALL_ROLE_PRIVS

Gestion des privilèges sous Oracle

- **Interface SQL*Plus** : ordres LCD SQL (GRANT, REVOKE)
- **Interface *Oracle Entreprise Manager***

ORACLE : PRIVILEGES

Privilèges objets

- **ALTER** modification de la structure de l'objet
- **DELETE** suppression de l'objet
- **INDEX** définition d'un index sur l'objet
- **INSERT** insertion de tuple dans l'objet
- **REFERENCES** référence à des contraintes définies sur un objet
- **SELECT** consultation (droit de lecture)
- **UPDATE** droit de modification de l'objet (tuple, attribut)
- **EXECUTE** programmes PL/SQL

Privilège et type d'objet

Table	ALTER, DELETE, INDEX, INSERT, REFERENCES, SELECT, UPDATE
Vue	ALTER, DELETE, INSERT, SELECT, UPDATE
Séquence	ALTER, SELECT

droit "ALL"

ORACLE : PRIVILEGES

Définition de privilège sur un objet

```
GRANT { privilège_objet [, privilège objet ...] | ALL }
ON objet
TO { utilisateur [, utilisateur2 …]  | PUBLIC }
[WITH GRANT OPTION]
```

GRANT OPTION

droit au bénéficiaire d'accorder ce privilège à d'autres utilisateurs

Définition de privilège sur l'attribut d'un objet

Exemple GRANT SELECT ON ma_table(col1, col2) TO PUBLIC;

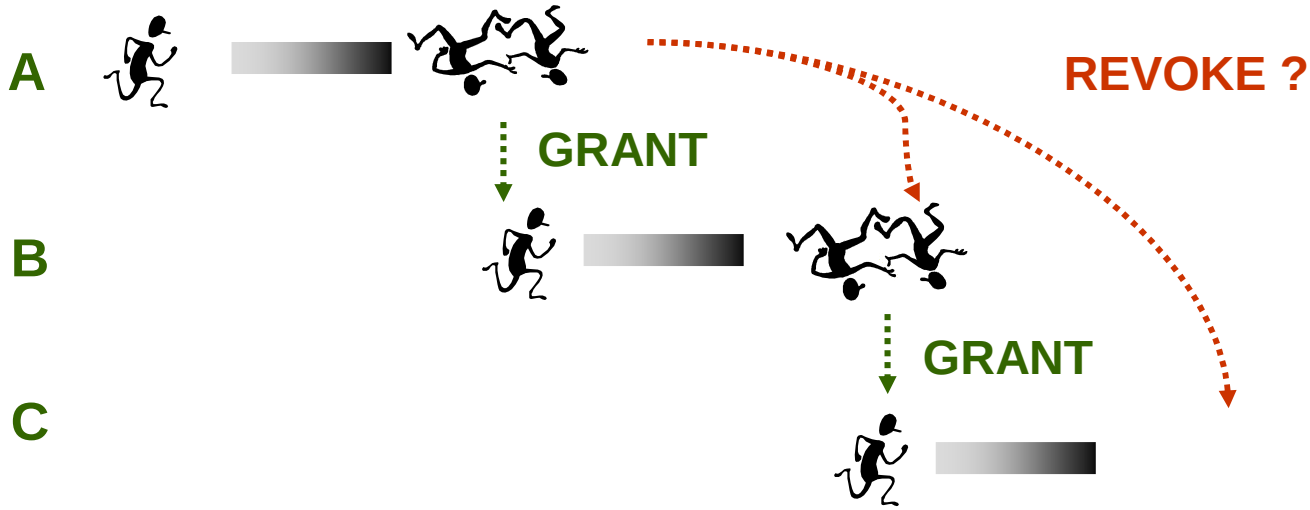
ORACLE : PRIVILEGES

Retrait de privilège

REVOKE [**GRANT OPTION FOR**] Priv1 [,Priv2 …] **ON** objet
FROM { utilisateur [, utilisateur2…] | PUBLIC }

[**RESTRICT** | **CASCADE**]

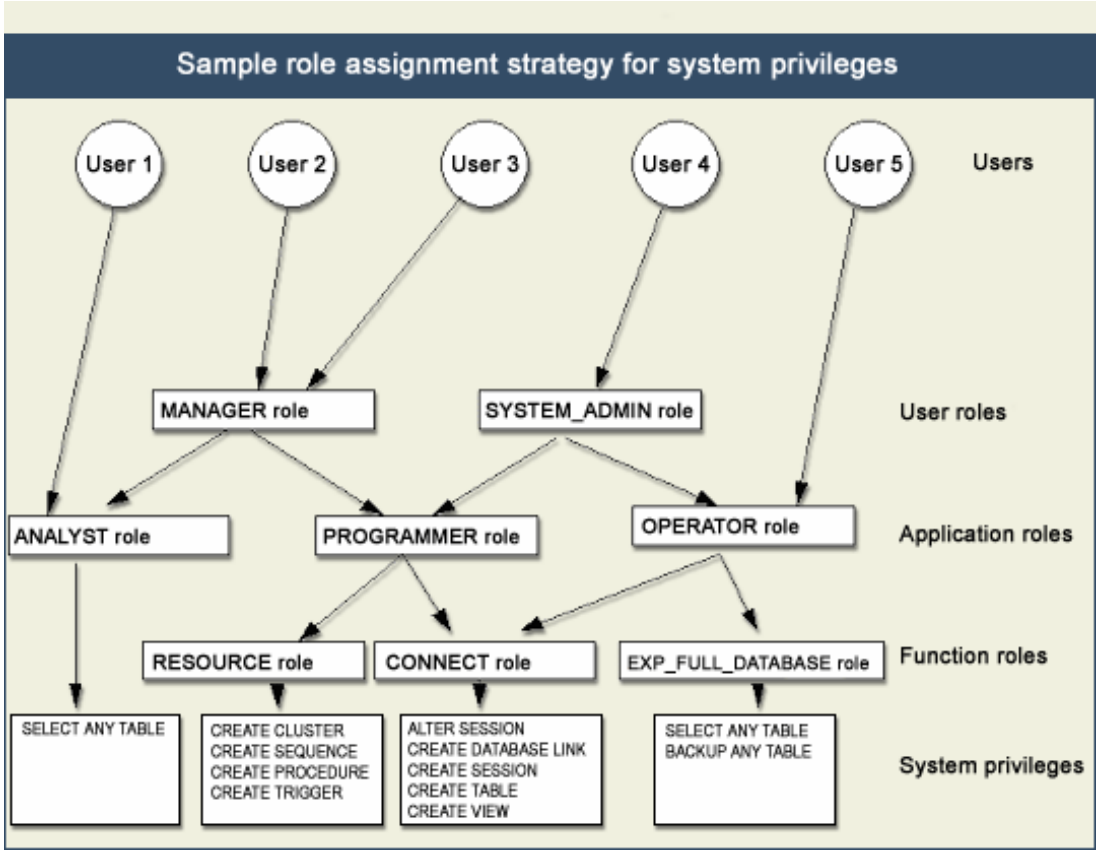
GRANT OPTION FOR	retrait uniquement du droit de transfert
CASCADE	retrait des droits accordés à des tiers (ADMIN option) par celui à qui on retire le privilège
RESTRICT	refus du retrait en cascade



CONTRÔLE A BASE DE ROLES

Rôle

- Regroupement d'utilisateurs qui partagent les mêmes privilèges
- Association d'un rôle à chaque utilisateur
- Attribution de privilèges à chaque rôle



CONTRÔLE A BASE DE ROLES

Création /suppression de rôles

```
CREATE ROLE
DROP ROLE
```

Rôle prédéfinis ORACLE

- CONNECT connexion, CREATE et SELECT sur les objets courants
- RESOURCE droits en création plus avancés (index, cluster, trigger…)
- DBA

Modification de rôle

```
ALTER ROLE
```

Ne concerne ni l'attribution de droits, ni l'affectation d'utilisateurs, qui sont gérés par les ordres GRANT / REVOKE

CONTRÔLE A BASE DE ROLES

Association d'un utilisateur

```
GRANT role TO utilisateur
```

Héritage de rôles

```
GRANT role TO role [WITH ADMIN OPTION]
```

Affectation d'un privilège

Les rôles s'utilisent aussi bien comme identifiant d'utilisateur que de privilège (ils représentent alors les droits associés au rôle

```
GRANT { priv_objet | role }  ON objet
TO { utilisateur | role | PUBLIC }
```

```
GRANT priv_system
TO { utilisateur | role | PUBLIC }
```

ORACLE : ROLES

Rôles prédéfinis

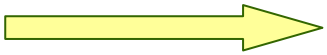
CONNECT	**Utilisateur de base** : CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW…
RESOURCE	**Complément pour utilisateur un peu plus avancé** : CREATE PROCEDURE, CREATE TRIGGER…
DBA	Tous les privilèges avec WITH ADMIN OPTION

EXP_FULL_DATABASE	Privilèges requis pour l'exportation
IMP_FULL_DATABASE	Privilèges requis pour l'importation
SELECT_CATALOG_ROLE	SELECT sur les objets du dictionnaire
EXECUTE_CATALOG_ROLE	EXECUTE sur les objets du dictionnaire

ORACLE : ROLES

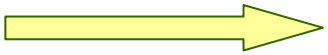
Dictionnaire Oracle

- ROLE_TAB_PRIVS



ROLE
OWNER
TABLE_NAME
COLUMN_NAME
PRIVILEGE
GRANTABLE

- ROLE_SYS_PRIVS
- DBA_ROLES
- DBA_ROLE_PRIVS
- USER_ROLE_PRIVS



- ROLE_ROLE_PRIVS

USERNAME
GRANTED_ROLE
ADMIN_OPTION
DEFAULT_ROLE
OS_GRANTED

CONCLUSION

Sécurisation des données

– Politique de contrôle des accès

Mais également

– Gestion des accès concurrents à une même donnée
– Gestion des pannes

➧ **Chap. IV : SGBD Transactionnels**

BIBLIOGRAPHIE

Ouvrages disponibles à la B.U.

RESSOURCES ELECTRONIQUES

Sur la Toile

Petit didacticiel sur la gestion des utilisateurs sous Oracle
http://oracle.developpez.com/guide/administration/adminuser/

Serveur de documentation Emery du département

- Oracle SQL Reference
- Oracle Database reference – Part. II The Static Data Dictionary