CONTRÔLE D'ACCÈS

DAC (Discretionary Access Control)
RBAC (Role-Based Access Control)

TODO

- Lire ce polycopié avant le cours
- Visioner
- Coirs Stanford sur Autorisations https://www.youtube.com/watch?v=0JMmifkP4K8&list=PLroEs25KGvwzmvIxYHRhoGTz9w8LeXek0&index=47

CONCEPTS DE BASE

- **Sujets**
  - Utilisateurs ou applications
  - PUBLIC : n'importe quel utilisateur de la BD

- **Objets**
  - Tables, objets, vues, fonctions/procédures

- **Privilèges** ou autorisations
  - SELECT : privilège pour lire toutes le colonnes de la donnée ainsi que les colonnes insérées plus tard avec ALTER TABLE
  - INSERT/UPDATE : privilège pour insérer/modifier des lignes
  - DELETE : privilège pour supprimer des lignes
  - REFERENCES : privilège pour définir des clés étrangères (référencier d'autres tables ou vues)
  - EXECUTE : privilège pour exécuter une fonction/procédure

DAC

Discretionary Access Control

DAC

- Consiste à attribuer directement aux sujets des privilèges sur les objets et à les vérifier lors de l'accès
- Gestion de privilèges
  - Le sujet qui crée une table automatiquement a tous les privilèges sur celle-ci
  - GRANT : permet d'attribuer un privilège
    - GRANT <liste de privilèges> ON <objet> TO <liste de sujets>
  - GRANT OPTION : cette option permet au sujet recevant le privilège de l'attribuer à d'autres utilisateurs
    - GRANT <liste de privilèges> ON <objet> TO <liste de sujets> WITH GRANT OPTION

EXEMPLES

- Considérez les tables suivantes crées par Joe.

Sailors	Boats	Reservs
sid: integer sname: string rating: integer age: real	bid: integer bname: string color: string	sid: integer bid: integer day: date

```
GRANT INSERT, DELETE ON Reservs TO Yuppy WITH GRANT OPTION
GRANT SELECT ON Reservs TO Michel

GRANT SELECT ON Sailors TO Michel WITH GRANT OPTION
GRANT INSERT (sid,sname,age) ON Sailors TO Michel

GRANT REFERENCES (bid) ON Boats TO Bill
```

REVOKE

- REVOKE [CASCADE|RESTRICT]: permet de révoquer un privilège.
  - CASCADE : révoque un privilège et ceux qui en découlent
  - RESTRICT : rejette la révocation si en plus de l'utilisateur spécifié d'autres utilisateurs vont voir ses privilèges affectés. *Cette option est celle par défaut.*

EXEMPLES

- Considérer les commandes suivantes :

- Joe (qui a crée Sailors) exécute :
  - GRANT SELECT ON Sailors TO Art WITH GRANT OPTION

- Art exécute :
  - GRANT SELECT ON Sailors TO Bob WITH GRANT OPTION

- Qu'est-ce qui se passe si Joe exécute :
  - REVOKE SELECT ON Sailors FROM Art CASCADE

  ou
  - REVOKE GRANT OPTION FOR SELECT ON Sailors FROM Art CASCADE

GRAPHES D'AUTORISATION

- Les effets des commandes GRANT et REVOKE peuvent être décrits dans un graphe d'autorisations
- Un graphe concerne une seule donnée
- Les nœuds sont les utilisateurs
- Les arcs indiquent comment les privilèges sont accordés

EXEMPLE DE GRAPHE D'AUTORISATION

- Joe exécute :
  1. GRANT SELECT ON Sailors TO Art WITH GRANT OPTION

- Art exécute :
  2. GRANT SELECT ON Sailors TO Bob WITH GRANT OPTION

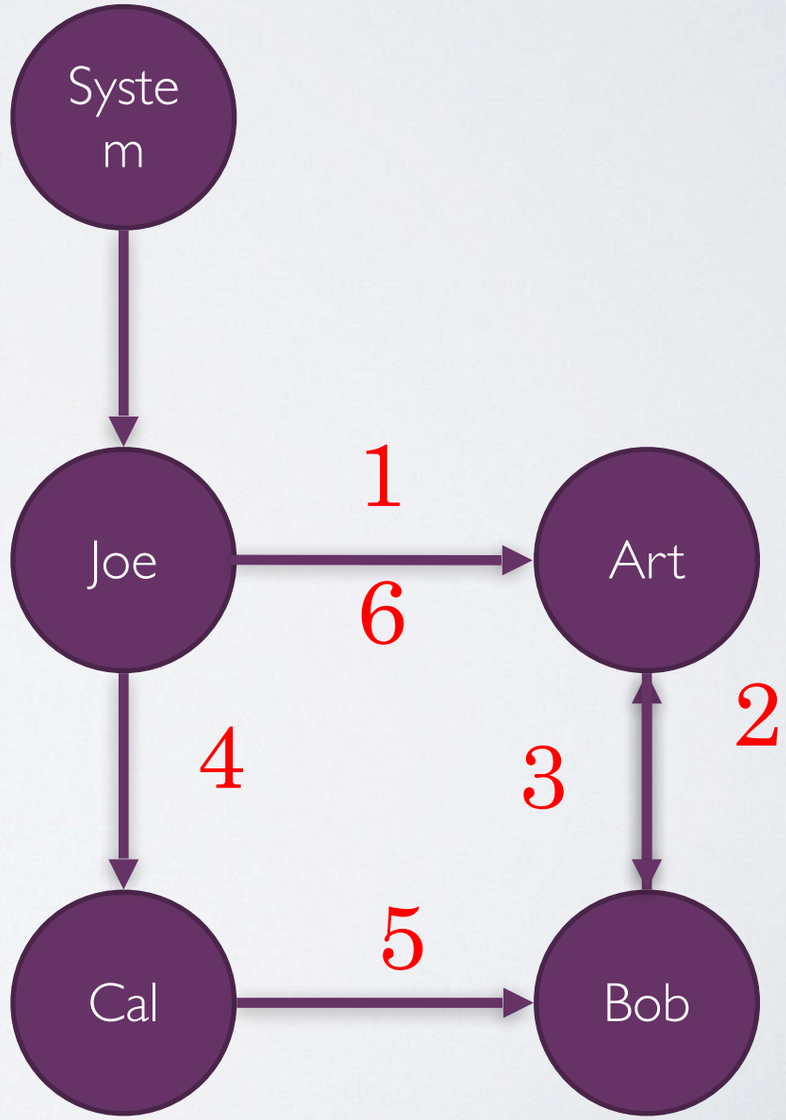
- Bob exécute
  3. GRANT SELECT ON Sailors TO Art WITH GRANT OPTION

- Joe exécute
  4. GRANT SELECT ON Sailors TO Cal WITH GRANT OPTION

- Cal exécute
  5. GRANT SELECT ON Sailors TO Bob WITH GRANT OPTION

- Joe exécute
  6. REVOKE SELECT ON Sailors FROM Art CASCADE

Graphe d'autorisation de la table Sailors



RBAC

RBAC

- DAC n'est pas applicable à des systèmes complexes avec des centaines/milliers d'utilisateurs
- Inconvénients de DAC
- Approche basée sur l'attribution de droits par sujet (utilisateur) donc difficulté pour gérer la dynamicité des privilèges
  - Sorties du système (entreprise)
  - Modification des droits (changement de responsabilités)

RBAC

- Proposé pour des systèmes très grands avec un important nombre d'utilisateurs et de données

- Contrôle d'accès à base de rôles
  - Modèle dans lequel les décisions d'accès dépendent du rôle auquel l'utilisateur est attaché

- Concepts de base
  - Sujets (utilisateurs)
  - Privilège. Concerne un droit (opération) quelconque sur une donnée, plusieurs droits sur une donnée ou plusieurs droits sur plusieurs données
  - Rôles. Entité déterminant une activité d'entreprise (comptable, chef de projet, chef de département, cassier, etc.)

- Deux approches : modèles ANSI et *role graphe*

LES RÔLES

- Sont définis par une autorité centrale
- Sont identifiés par un nom unique
- Peuvent être organisés en une hiérarchie ou un graphe. Attention aux
  - Cycles (redondance)
  - Conflits d'intérêt
- Sont attribués aux utilisateurs ou groups d'utilisateurs
  - Mapping rôle-utilisateur
  - Plusieurs rôles peuvent être attribués à un utilisateur
  - Plusieurs utilisateurs peuvent partager plusieurs rôles
- Facilité de gestion rôle-utilisateur

LES GROUPES D'UTILISATEURS ET LES RÔLES

- Groupes d'utilisateurs
  - Facilite la gestion des utilisateurs
  - Les membres du groupe peuvent changer fréquemment
  - La gestion des groupes peut se faire par le gestionnaire des ressources humaines

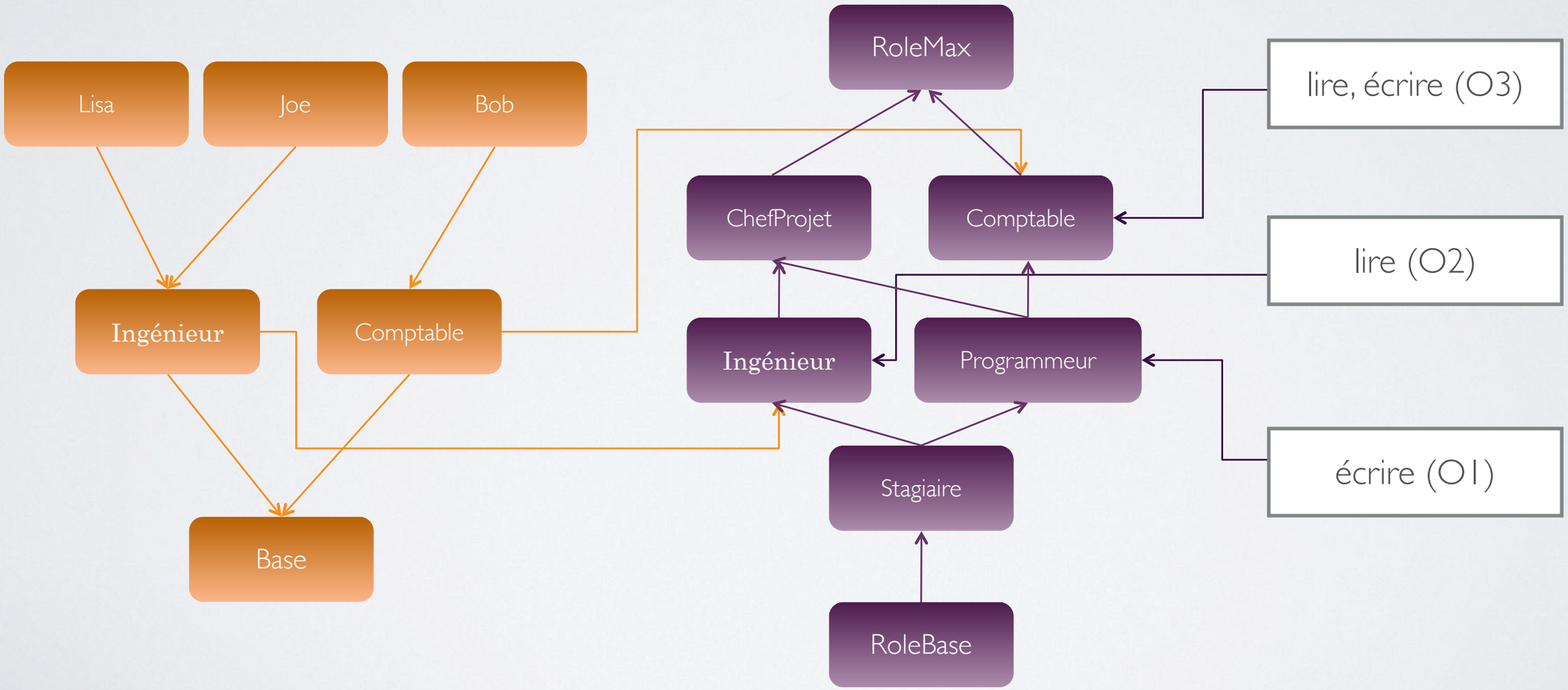
- Rôles
  - les rôles sont définis avant la mise en place du système
  - Les privilèges attribués aux rôles varient très peu
  - La gestion des rôles doit se faire par un utilisateur de confiance

COMPOSANTS DU MODÈLE BASÉ SUR LES RÔLES

Graphe de groupes

Graphe de rôles

Privilèges



PROPRIÉTÉS DU GRAPHE DE RÔLES

- Héritage
  - r1 → r2 indique que r1 est junior de r2 et que les privilèges de r1 sont hérités à r2
  - privilèges(r1) ⊆ privilèges(r2)

- Privilèges directs
  - Privilèges attribués directement au rôle par l'administrateur du graphe

- Privilèges effectifs
  - Privilèges directs plus privilèges hérités

- Graphe acyclique

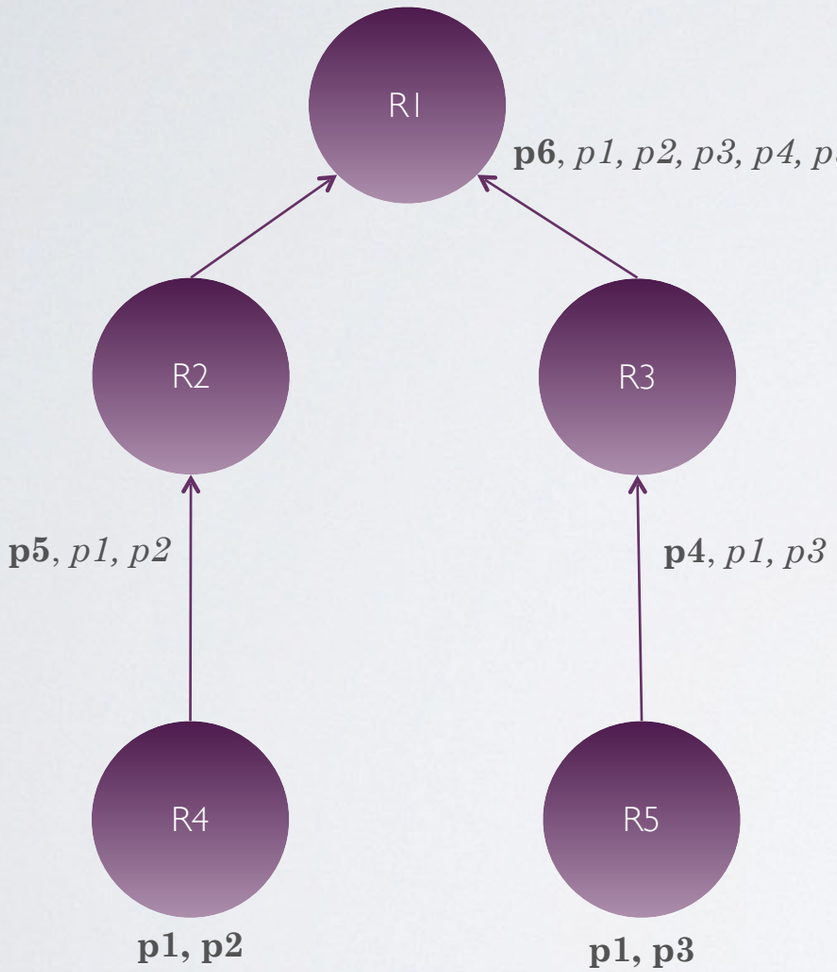
- Pas de redondance de privilèges
  - Un arc r1 → r2 doit être ajouté si privilèges(r1) ⊂ privilèges(r2)

GESTION DU GRAPHE DE RÔLES

- roleAddition
  - Si pas de cycle, le rôle est ajouté
- permitionAddition
  - Un nouveau privilège est ajouté à un rôle
- permitionDeletion
  - Suppression d'un privilège d'un rôle
- roleDeletion
  - Suppression d'un rôle
- edgeInsertion
  - Insertion d'un arc si pas de cycle
- edgeDeletion
  - Suppression d'un arc si pas de cycle
- Dans toutes les fonctions, si nécessaire, les privilèges/arcs sont réorganisés pour éviter les redondances

EXEMPLE DE GESTION DE GRAPHE DE RÔLES

Graphe A



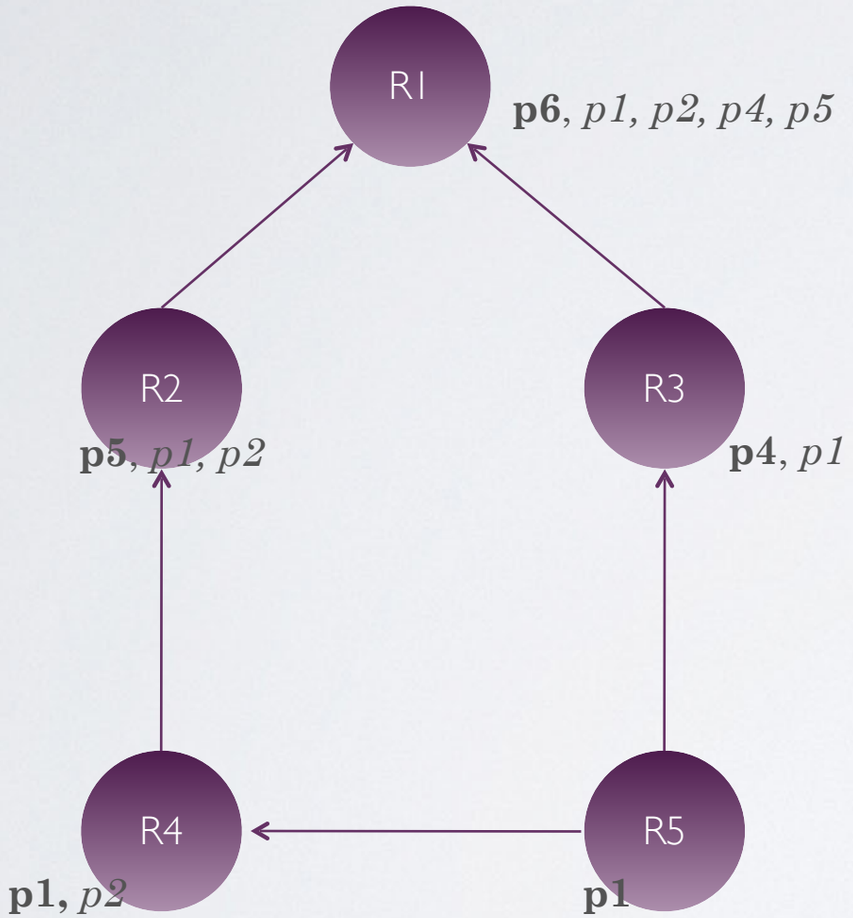
Graphe A avec p3 de R5 supprimé

Pas de cycle

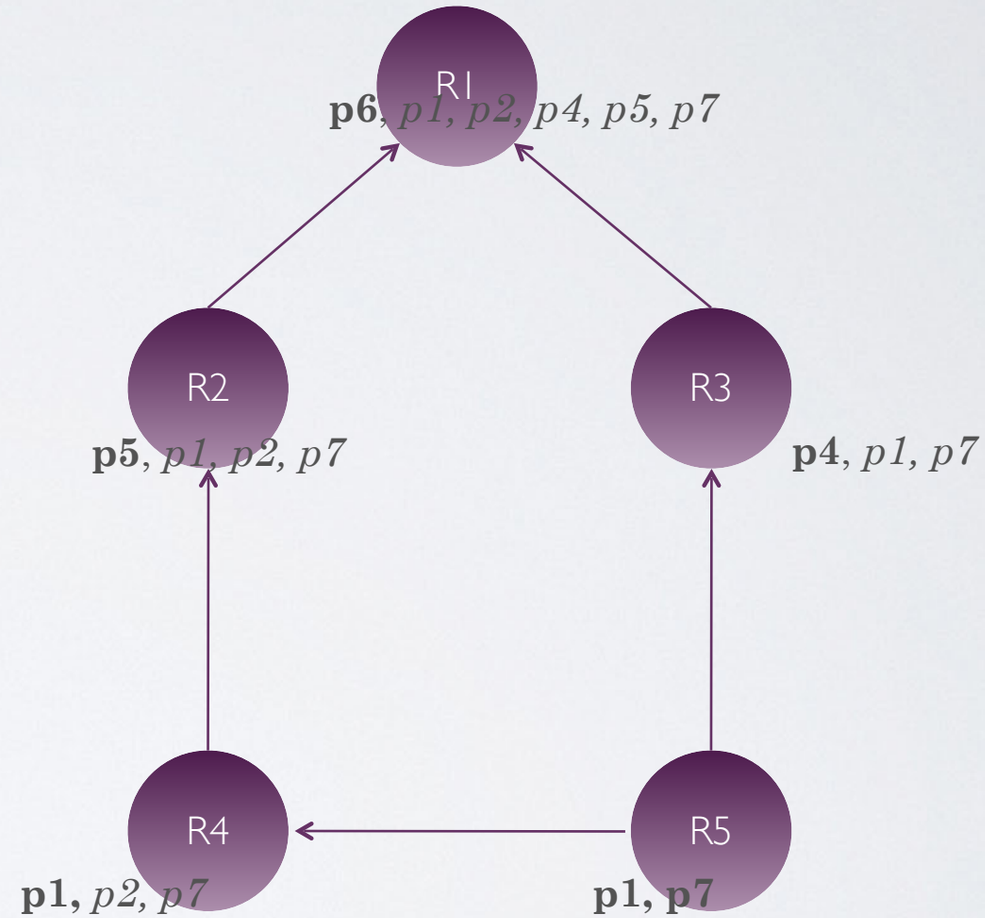
Pas de redondance de privilèges i.e., ⌐(privilèges(r1) ⊂ privilèges(r2))

CONT.

Graphe A, la suite

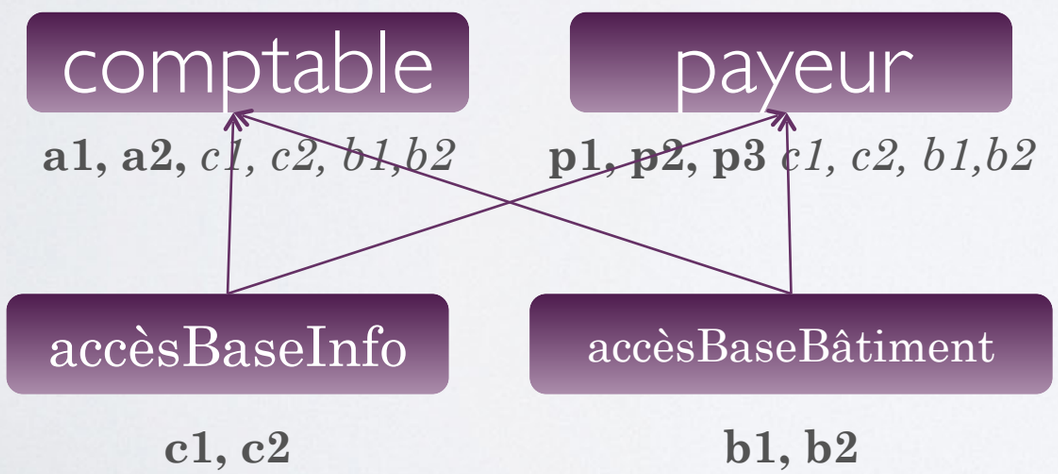


Graphe A avec p7 ajouté à R5



CONSEILS POUR DÉFINIR UNE HIÉRARCHIE DE RÔLES

- Ne pas faire de la hiérarchie de rôles un miroir de la hiérarchie de l'entreprise
- Surveiller les privilèges des rôles
- Considérer les groupes d'utilisateurs
- Considérer de rôles abstraits



Avec des rôles abstraits

Sans des rôles abstraits

CONCLUSION

- Le control d'accès est vital pour assurer la confidentialité des données

- DAC, RBAC : deux grandes approches
  - Chacun a ses avantages et désavantages
  - RBAC se révèle le plus adapté aux systèmes actuels

BIBLIOGRAPHIE

- Security, Privacy, and Trust in Data Management. Milan Petkovic, Willem Jonker Eds. 2007.
- Database Management Systems. Raghu Ramakrishnan, Johannes Gehrke. International 3rd Edition, 2003.

LES RÔLES DANS ORACLE

LES RÔLES DANS ORACLE

- **Privilège**
  - Droit d'exécuter une sentence SQL ou d'accéder les objets (tables, vues, objets, etc.) d'un autre utilisateur
  - Un privilège représente le couple (objet, privilège)
  - 173 privilèges dans Oracle 10g (SYSTEM_PRIVILEGE_MAP)

- **Rôle**
  - Ensemble de privilèges qui peut être attribué aux utilisateurs ou aux rôles

TYPES DE PRIVILÈGES

- Privilèges objets
  - Privilèges permettant la gestion des objets crées par les utilisateurs
  - CREATE, SELECT, INSERT, etc.

- Privilèges système
  - Privilèges permettant la gestion du système de bases de données
  - Ne sont pas liés à un objet ou schéma
  - CREATE SESSION, CREATE ROLE, ALTER ROLE, etc.

- Rôles
  - Peuvent contenir de privilèges objets et système

PRIVILÈGES OBJETS

Objet	Privilège
Tables	select, insert, update, delete, alter, debug, flashback, on commit refresh, query rewrite, references, all, index
Views	select, insert, update, delete, under, references, flashback, debug
Sequence	alter, select
Packeges, Procedures, Functions (Java classes,	execute, debug
Materialized Views	delete, flashback, insert, select, update
Directories	read, write
Libraries	execute
User defined types	execute, debug, under
Operators	execute
Indextypes	execute

24

PRIVILÈGES SUR LES OBJETS

Object Privilege	Table	View	Sequence	Procedures, Functions, Packages[a]	Materialized View	Directory	Library	User-defined Type	Operator	Index-type
ALTER	X		X							
DELETE	X	X			X[b]					
EXECUTE				X[c]			X[c]	X[c]	X[c]	X[c]
DEBUG	X	X		X				X		
FLASHBACK	X	X			X					
INDEX	X									
INSERT	X	X			X[b]					
ON COMMIT REFRESH	X									
QUERY REWRITE	X									
READ						X				
REFERENCES	X	X								
SELECT	X	X	X		X					
UNDER		X						X		
UPDATE	X	X			X[b]					
WRITE						X				

PRIVILÈGES SYSTÈME

- Définis par Oracle et pas modifiables par les utilisateurs
- Peuvent être attribués uniquement par les administrateurs du système ayant comme privilèges
  - Le privilège à attribuer avec l'option ADMIN OPTION
  - Le privilège général GRANT ANY PRIVILEGE
- Les privilèges sur les objets ne peuvent pas être attribués avec des privilèges systèmes ou rôles dans la même sentence GRANT

L'OPTION ADMIN OPTION

- Utilisable avec les rôles et les privilèges système
- Semblable à WITH GRANT OPTION des privilèges objets
- Le receveur peut
  - Attribuer ou révoquer le rôle ou le privilège système
  - Attribuer le rôle ou le privilège système avec l'option ADMIN OPTION
  - Modifier (ALTER) ou supprimer le rôle
- Pour annuler l'option, il faut révoquer le privilège
- Exemples
  - GRANT myRole TO alice WITH ADMIN OPTION;
  - REVOKE myRole FROM alice;

AVANTAGES DE L'UTILISATION DE RÔLES

- Gestion de privilèges réduite
  - Au lieu d'attribuer un ensemble de privilèges aux utilisateurs, un par un, les privilèges sont attribués à un rôle et uniquement le rôle est attribué aux utilisateurs
- Gestion dynamique des privilèges
  - Si les privilèges d'un groupe change, uniquement le rôle sera modifié
- Surveillance plus simple
  - Plus facile de vérifier les privilèges des utilisateurs

UTILISATION DES RÔLES

- Pour la gestion des privilèges d'un groupe d'utilisateurs
- Pour la gestion des privilèges d'une application de base de données
  - Attribution à un rôle des privilèges nécessaires à l'exécution d'une application
  - Le rôle d'application crée sera attribué aux utilisateurs de l'application

RÔLES PRÉDÉFINIS D'ORACLE

- Définis automatiquement lors de l'installation d'Oracle
- Aident à la gestion de la base de données
- Peuvent être gérés comme les rôles définis par un utilisateur
- Exemples
  - CONNECT : CREATE VIEW, CREATE TABLE, ALTER SESSION, CREATE CLUSTER, CREATE SESSION, CREATE SYNONYM, CREATE SEQUENCE, CREATE DATABASE LINK
  - RESOURCE : CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE

GESTION DE RÔLES

- Création/suppression
  - Un rôle peut être crée et supprimé
- Sécurisation
  - Les rôles peuvent être protégés par un mot de passe pour éviter que n'importe qui ajoute/supprime/attribue de privilèges
- Attribution
  - Un rôle peut être attribué aux utilisateurs ou aux rôles
  - On peut attribuer des privilèges aux rôles

CRÉATION/SUPPRESSION DE RÔLES

- Création de rôles
  - Uniquement par des utilisateurs
    - Ayant le privilège CREATE ROLE

- Modification de rôles
  - Par les utilisateurs
    - Ayant eu attribué le rôle avec l'option ADMIN OPTION
    - Ayant le privilège ALTER ANY ROLE

- Suppression de rôles
  - Par les utilisateurs
    - Ayant créé le rôle
    - Ayant eu attribué le rôle avec l'option ADMIN OPTION
    - Ayant le privilège DROP ANY ROLE

CRÉATION/SUPPRESSION DE RÔLES

- Création et sécurisation
  - Les rôles peuvent être crées avec un mot de passe
    - CREATE ROLE myRole;
    - CREATE ROLE myRole IDENTIFIED BY my_pwd;
  - Un mot de passe peut également être attribué à un rôle existant
    - ALTER ROLE myRole IDENTIFIED BY my_pwd;

- Suppression
  - DROP ROLE myRole;

ATTRIBUTION DE PRIVILÈGES À UN RÔLE

- L'attribution peut être fait par les utilisateurs
  - Ayant créé le rôle
  - Ayant eu le rôle attribué (avec ou sans l'option ADMIN OPTION)
  - Ayant le privilège système GRANT ANY OBJECT PRIVILEGE (pour les privilèges objets)
  - Ayant le privilège système GRANT ANY PRIVILEGE (pour les privilèges système)
  - Exemples
    - GRANT SELECT ON myTable TO myRole;
    - GRANT SELECT ON myTable TO myRole1, myRole2;
    - GRANT SELECT, UPDATE ON myTable TO myRole;

SUPPRESSION DE PRIVILÈGES À UN RÔLE

- La suppression peut être faite par des utilisateurs
  - Ayant préalablement attribué le privilège au rôle
  - Ayant le privilège système GRANT ANY OBJECT PRIVILEGE
  - Exemples
    - REVOKE SELECT ON myTable FROM myRole;
    - REVOKE ALL ON myTable FROM myRole;

ATTRIBUTION DE RÔLES

- Les rôles peuvent être attribués uniquement par les utilisateurs
  - Ayant eu le rôle attribué avec l'option ADMIN OPTION
  - Le privilège général GRANT ANY ROLE
  - Exemples
- Attribution de rôle à rôle
  - GRANT myRole TO myRole2;
  - GRANT myRole, myRole3 TO myRole2, myRole4;
  - Interdiction de cycles ! -> ~~GRANT myRole2 TO myRole;~~
- Attribution de rôle aux utilisateurs
  - GRANT myRole TO bob, alice;
  - REVOKE myrole TO bob;

RÉVOCATION DE RÔLES

- Un rôle peut être révoqué par les utilisateurs
  - Ayant attribué le rôle
  - Ayant eu le rôle attribué avec l'option ADMIN OPTION
  - Ayant le privilège système GRANT ANY ROLE
  - Exemples
    - REVOKE myRole TO bob;
    - REVOKE myRole TO medecins;

LE PRIVILÈGE GRANT ANY OBJECT PRIVILEGE

- Permet d'attribuer/révoquer des privilèges à la place d'autres utilisateurs
  - Trois utilisateurs : A, B, C
  - A est un administrateur de la BD qui possède le privilège GRANT ANY OBJECT PRIVILEGE
  - B a créé la table table_b
  - L'utilisateur A exécute

GRANT SELECT ON B.table_b TO C;

- Cela est comme si B a attribué le droit directement à C
- La même opération peut être faite avec REVOKE

OÙ TROUVER L'INFORMATION SUR LES PRIVILÈGES ?

- Dans les **dictionnaires d'Oracle**
  - Un dictionnaire est une vue gérée automatiquement par Oracle
- Les dictionnaires portent sur tout type d'information liée à la BD
  - Utilisateurs
  - Sessions
  - Les objets
  - Les privilèges
  - Les rôles
  - Etc.

QUELQUES DICTIONNAIRES

- Privilèges
  - USER_COL_PRIVS : montre les colonnes des objets sur lesquelles l'utilisateur actuel est le owner/grantor/grantee
  - USER_TAB_PRIVS : montre les privilèges sur les objets où l'utilisateur est le grantee
- Rôles
  - DBA_ROLES : montre tous les rôles du système
  - USER_ROLE_PRIVS : montre les rôles attribués à l'utilisateur
- Système
  - USER_SYS_PRIVS : montre les privilèges système attribués à l'utilisateur
  - SYSTEM_PRIVILEGE_MAP : montre tous les privilèges du système

EXEMPLES DE REQUÊTES

- Afin de connaitre les attributs d'un dictionnaire, ex. :

Desc USER_SYS_PRIVS;

Select username, privilege, admin_option
FROM USER_SYS_PRIVS;

Select username, granted_role
FROM USER_ROLE_PRIVS;

Select owner, table_name, privilege
FROM USER_TAB_PRIVS;

Select grantee, privilege
FROM DBA_SYS_PRIVS
WHERE grantee LIKE 'L3_*';

Select grantee, granted_role
FROM DBA_ROLE_PRIVS
WHERE grantee IN ('L3_1', 'L3_2');

Table 4–7 Views That Display Grant Information about Privileges and Roles

View	Description
ALL_COL_PRIVS	Describes all column object grants for which the current user or PUBLIC is the object owner, grantor, or grantee
ALL_COL_PRIVS_MADE	Lists column object grants for which the current user is object owner or grantor.
ALL_COL_PRIVS_RECD	Describes column object grants for which the current user or PUBLIC is the grantee
ALL_TAB_PRIVS	Lists the grants on objects where the user or PUBLIC is the grantee
ALL_TAB_PRIVS_MADE	Lists the all object grants made by the current user or made on the objects owned by the current user.
ALL_TAB_PRIVS_RECD	Lists object grants for which the user or PUBLIC is the grantee
DBA_COL_PRIVS	Describes all column object grants in the database
DBA_TAB_PRIVS	Lists all grants on all objects in the database
DBA_ROLES	This view lists all roles that exist in the database, including secure application roles
DBA_ROLE_PRIVS	Lists roles granted to users and roles
DBA_SYS_PRIVS	Lists system privileges granted to users and roles
ROLE_ROLE_PRIVS	This view describes roles granted to other roles. Information is provided only about roles to which the user has access.

View	Description
ROLE_SYS_PRIVS	This view contains information about system privileges granted to roles. Information is provided only about roles to which the user has access.
ROLE_TAB_PRIVS	This view contains information about object privileges granted to roles. Information is provided only about roles to which the user has access.
USER_COL_PRIVS	Describes column object grants for which the current user is the object owner, grantor, or grantee
USER_COL_PRIVS_MADE	Describes column object grants for which the current user is the grantor
USER_COL_PRIVS_RECD	Describes column object grants for which the current user is the grantee
USER_ROLE_PRIVS	Lists roles granted to the current user
USER_TAB_PRIVS	Lists grants on all objects where the current user is the grantee
USER_SYS_PRIVS	Lists system privileges granted to the current user
USER_TAB_PRIVS_MADE	Lists grants on all objects owned by the current user
USER_TAB_PRIVS_RECD	Lists object grants for which the current user is the grantee
SESSION_PRIVS	Lists the privileges that are currently enabled for the user
SESSION_ROLES	Lists the roles that are currently enabled to the user

D'AUTRES DICTIONNAIRES

- SESSION_ROLES
  - Tous les rôles actifs
- USER_SOURCE
  - Le code des procédures appartenant à l'utilisateur
- ALL_SOURCE
  - Le code des procédures appartenant à l'utilisateur ou à ceux auxquels il a accès
- DBA_SOURCE
  - Toutes les procédures de la BD
- USER_CATALOG
  - Information sur les tables, vues, séquences et synonymes de l'utilisateur
- USER_OBJECTS
  - Tout type d'objet Oracle (*clusters, database links, directories, functions, indexes, libraries, packages, java classes, abstract datatypes, resource plans, sequences, synonyms, tables, triggers, materialized views, LOBs, and views*)

CONCLUSION

- DAC et RBAC ne permettent pas un contrôle d'accès à niveau fin (tuples ou cellules)

- Oracle propose les VPD (Virtual Private Databases)
  - Ré-écriture de requêtes
  - Politiques de sécurité
  - Fonctions PL/SQL

- Oracle Security Guide 11g, novembre 2012http://docs.oracle.com/cd/B28359_01/network.111/b28531.pdf