HEIG VD | MEI
Media Engineering Institute

06 – Sécurité & Rôles

Infrastructure de données 1

Noemi Romano | 01 mai 2025

Pourquoi sécuriser ?

Sécurité

Confidentialité Protéger les données sensibles.

Contrôle d’accès Empêcher les intrusions non autorisées.

Prévention des pertes Éviter la suppression ou corruption accidentelle.

Intégrité Garantir des données fiables et cohérentes.

Conformité Respecter les lois et régulations.

Protection financière Réduire les risques d’amendes et de perte d’image.

Concepts de base

Utilisateur·rice·s

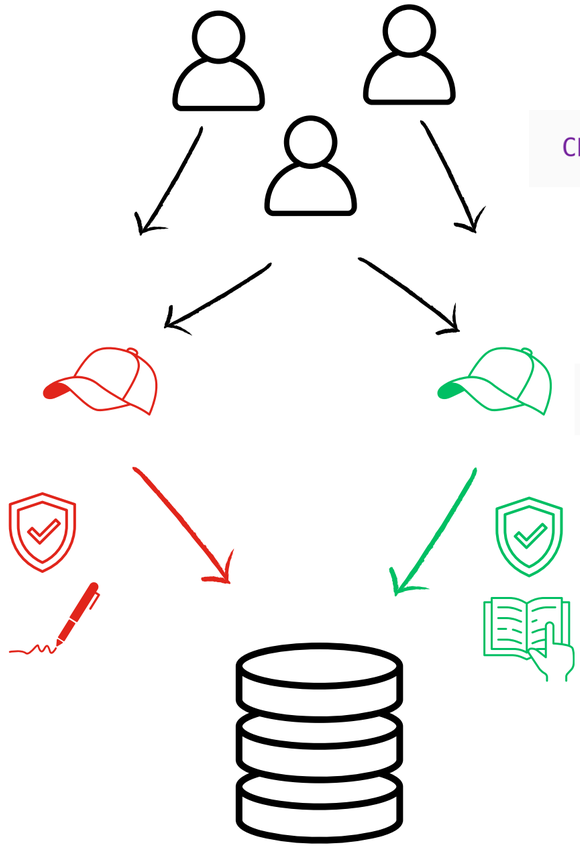
- **Une identité** reconnue par le système de gestion de base de données (SGBD).
- Identifiants (login/mot de passe) et des droits d'accès définis.

Rôles

- **Groupe de permissions** attribuables à plusieurs utilisateur·rice·s.

Privilèges

- **Actions autorisées** à un·e utilisateur·rice ou à un rôle donné (lire, mettre à jour, supprimer etc.)



Utilisateur·rice·s

```
CREATE USER nom_utilisateur;
```

Rôles

```
CREATE ROLE nom_role;
```

Privilèges

Créer

Utilisateur·rice·s

```
CREATE USER nom_utilisateur;
```

Rôles

```
CREATE ROLE nom_role;
```

Commandes principales

GRANT

Permet d'**accorder** un privilège à une personne utilisatrice ou à un rôle

```
GRANT <privilège> ON <objet>
TO <utilisateur·rice ou rôle>;
```

REVOKE

Permet de **retirer** un privilège précédemment accordé

```
REVOKE <privilège> ON <objet>
FROM <utilisateur·rice ou rôle>;
```

Types de privilèges

Privilège	Description
SELECT	Lire les données d'une table
INSERT	Ajouter de nouvelles lignes
UPDATE	Modifier des lignes existantes
DELETE	Supprimer des lignes
CREATE	Créer de nouveaux objets (tables, vues…)
DROP	Supprimer des objets
EXECUTE	Exécuter des procédures stockées

```
GRANT SELECT, UPDATE ON produits TO employe;

GRANT ALL PRIVILEGES ON ventes TO responsable;

GRANT SELECT ON clients TO lectrice;

REVOKE INSERT ON commandes FROM editeur;
```

Les **privilèges** peuvent être accordés :

- Sur toute la base,
- Sur des tables spécifiques
- Ou même sur des colonnes individuelles

PRIVILEGES PostgreSQL

Utiliser des rôles

- **Simplifie** l'attribution des permissions
- Permet une gestion **cohérente** et **évolutive**
- Facilite le respect du principe du **moindre privilège**

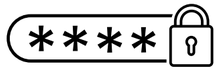
```
CREATE ROLE lectrice;

GRANT SELECT ON clients TO lectrice;

GRANT lectrice TO utilisateur1;
```

Le principe du **moindre privilège** (en anglais : **P**rinciple **o**f **L**east **P**rivilege, ou **PoLP**) consiste à n'accorder à une personne utilisatrice que les permissions strictement nécessaires pour effectuer ses tâches — **ni plus, ni moins**.

Bonnes pratiques générales

Moindre privilège Donner uniquement les droits nécessaires.

Utiliser des rôles Gérer les permissions par groupes, pas individuellement.



Mots de passe forts & changés Sécurité de base, mais essentielle.

Supprimer les accès inutiles Réduire la surface d’attaque

Monitorer Surveiller et auditer les accès

Projet

Nouveaux besoins

- Séance avec *Chef·fes de projet*
  - *Gestion des rôles*
  - *Requêtes SQL répondants aux besoins*

Livrable requêtes

- Délai : ~~2 mai 2025~~ 16 mai 2025