Authentification et Gestion des Accès

Présentation des rôles et permissions

1. **Les rôles**

Rôle	Description	Permissions principales
Admin	Accès complet à toutes les tables et toutes les actions	SELECT, INSERT, UPDATE, DELETE sur toutes les tables
Analyst	Lecture seule des transactions et détection fraude	SELECT sur transactions ; pas de modification
Customer Service	Lecture clients/transactions et modification limitée	SELECT sur clients, transactions ; UPDATE limité sur certains champs
Customer	Lecture et modification limitées à ses propres données	SELECT / UPDATE sur ses propres lignes uniquement (via supabase_id)

2. **Explication du fonctionnement**

3. Les rôles ne sont pas des rôles SQL classiques (CREATE ROLE) mais sont **définis via Supabase Auth et les policies RLS**.
4. **Admin, Analyst, Customer Service** : rôle défini par auth.role() dans Supabase Auth.
5. **Customer** : rôle simulé via supabase_id = auth.uid().
6. Les **policies RLS** limitent les actions sur chaque table selon le rôle de l'utilisateur.

Tableau de test des permissions et code SQL

- **Tableau des tests de permissions**

Rôle	Table	Requête test	Résultat attendu
Admin	customers	SELECT * FROM customers;	Tous les clients visibles
Admin	accounts	UPDATE accounts SET status='frozen' WHERE account_id=1;	Autorisé
Analyst	transactions	SELECT * FROM transactions;	Lecture autorisée
Analyst	transactions	UPDATE transactions SET amount=0 WHERE transaction_id=1;	Refusé

Customer Service	customers	SELECT * FROM customers;	Lecture autorisée
Customer Service	accounts	UPDATE accounts SET status='frozen' WHERE account_id=1;	Modification limitée
Customer Service	customers	DELETE FROM customers WHERE customer_id=1;	Refusé
Customer	customers	SELECT * FROM customers WHERE supabase_id='UUID_CUSTOMER';	Lecture de son profil uniquement
Customer	accounts	SELECT * FROM accounts WHERE customer_id=(SELECT customer_id FROM customers WHERE supabase_id='UUID_CUSTOMER');	Lecture de ses comptes
Customer	accounts	UPDATE accounts SET balance=999 WHERE account_id=1;	Refusé
Customer	transactions	SELECT * FROM transactions WHERE account_id IN (SELECT account_id FROM accounts WHERE customer_id=(SELECT customer_id FROM customers WHERE supabase_id='UUID_CUSTOMER'));	Lecture de ses transactions