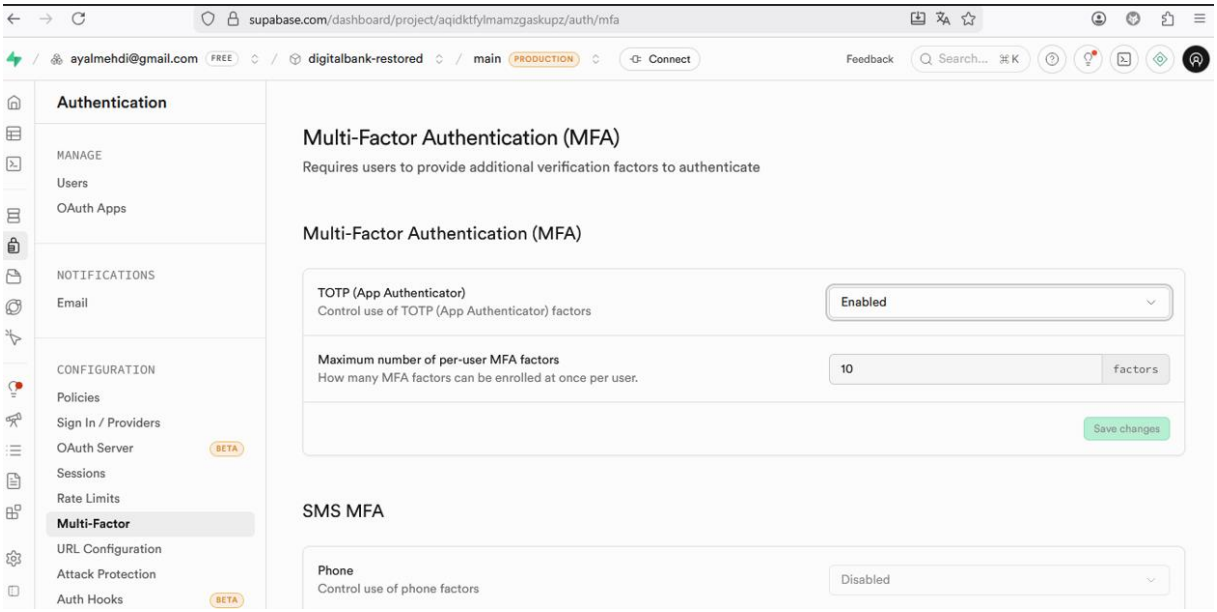
Vérifier MFA dans Supabase

1. Dans Supabase → **Authentication → Settings → MFA**
2. Tu devrais voir 3 options : `Enabled`, `Verify Enabled`, `Disabled`
   - Pour ton projet : **Verify Enabled** ✓
   - Cela force l'utilisateur à confirmer un second facteur (mail/SMS)
3. Si tu veux renforcer la sécurité, active **Enhanced MFA Security** (limite de session AAL1)
4. Sauvegarde / Apply

Voici la capture d'écran



Étape 3.1.b — Créer un système de gestion des rôles

1 Créer la table `user_roles` (si ce n'est pas fait)

```
CREATE TABLE IF NOT EXISTS user_roles (
    user_id UUID REFERENCES auth.users(id),
    role TEXT CHECK (role IN ('admin', 'analyst',
'customer_service', 'customer')),
    PRIMARY KEY (user_id)
);
```

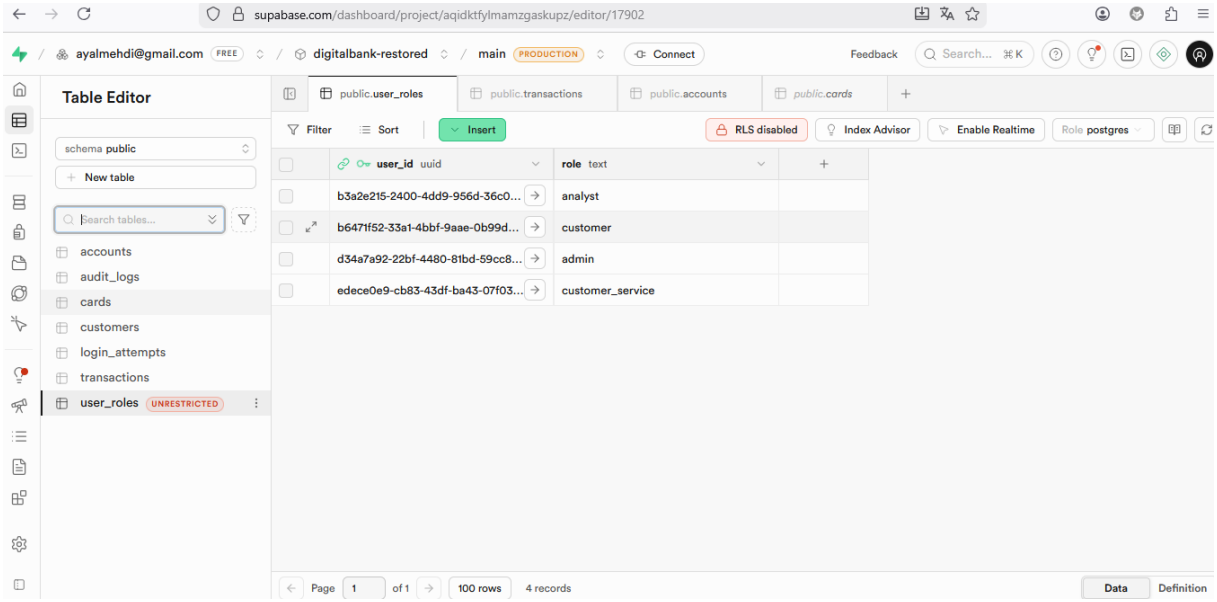
- Cette table lie **chaque utilisateur** à un **rôle**.

2 Ajouter les rôles aux utilisateurs

```
INSERT INTO user_roles (user_id, role)
VALUES
```

```
('UUID_ADMIN', 'admin'),
('UUID_ANALYST', 'analyst'),
('UUID_CS', 'customer_service'),
('UUID_CUSTOMER', 'customer')
ON CONFLICT (user_id) DO NOTHING;
```

Voici la capture d'écran de table `user_roles` remplie



3.1.c – Implémentation de Row Level Security (RLS)

Pour garantir la sécurité et la confidentialité des données dans notre projet, nous avons activé **Row Level Security (RLS)** sur toutes les tables sensibles de la base de données Supabase, notamment :

- `transactions`
- `accounts`
- `customers`
- `cards`
- `audit_logs`

Fonctionnement

RLS permet de contrôler **l'accès aux lignes de chaque table en fonction du rôle de l'utilisateur**. Grâce à cette sécurité :

- Un **admin** peut accéder à toutes les données et effectuer des modifications.
- Un **analyst** peut consulter toutes les transactions et les logs, mais ne peut pas modifier les données.
- Un **customer_service** peut consulter les informations des clients et leurs transactions, mais les modifications sont limitées.

- Un **customer** ne peut voir que **ses propres données personnelles et transactions**, et n'a aucun accès aux informations des autres clients.

Mise en œuvre dans Supabase

- Dans le **Table Editor**, RLS est activé pour chaque table sensible. Le bouton "Disable RLS" est visible, ce qui confirme son activation.
- Les **policies RLS** sont configurées pour chaque rôle, déterminant exactement quelles lignes et quelles actions sont autorisées.
- Cette configuration garantit que **chaque utilisateur ne peut voir et modifier que les données correspondant à son rôle**, conformément aux bonnes pratiques de sécurité et au principe du moindre privilège.

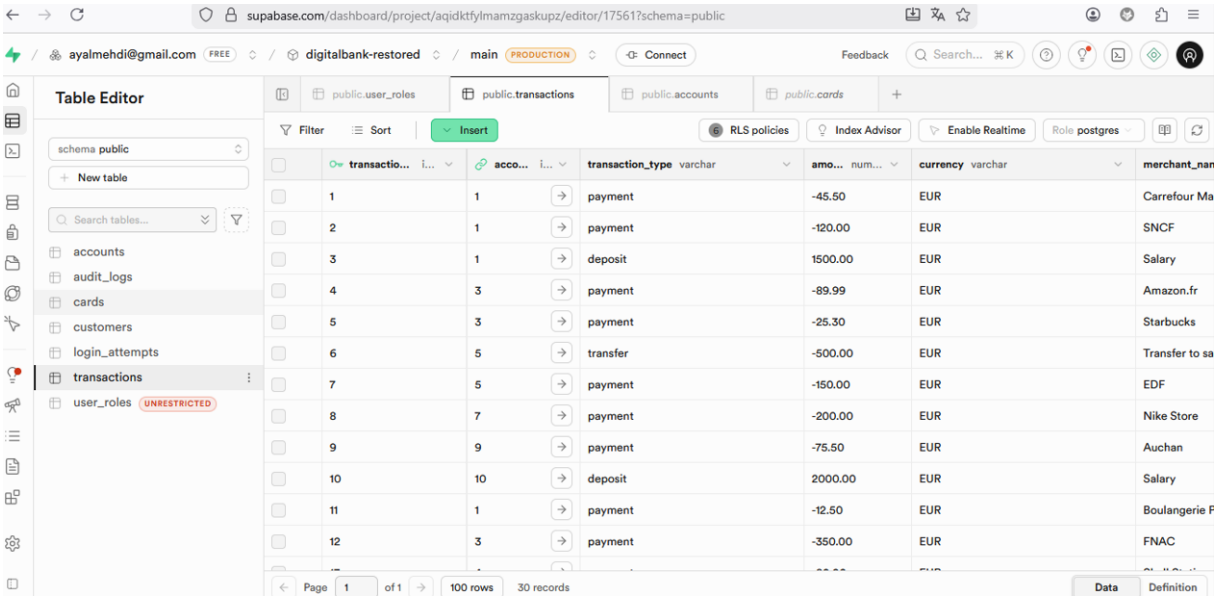
Preuves

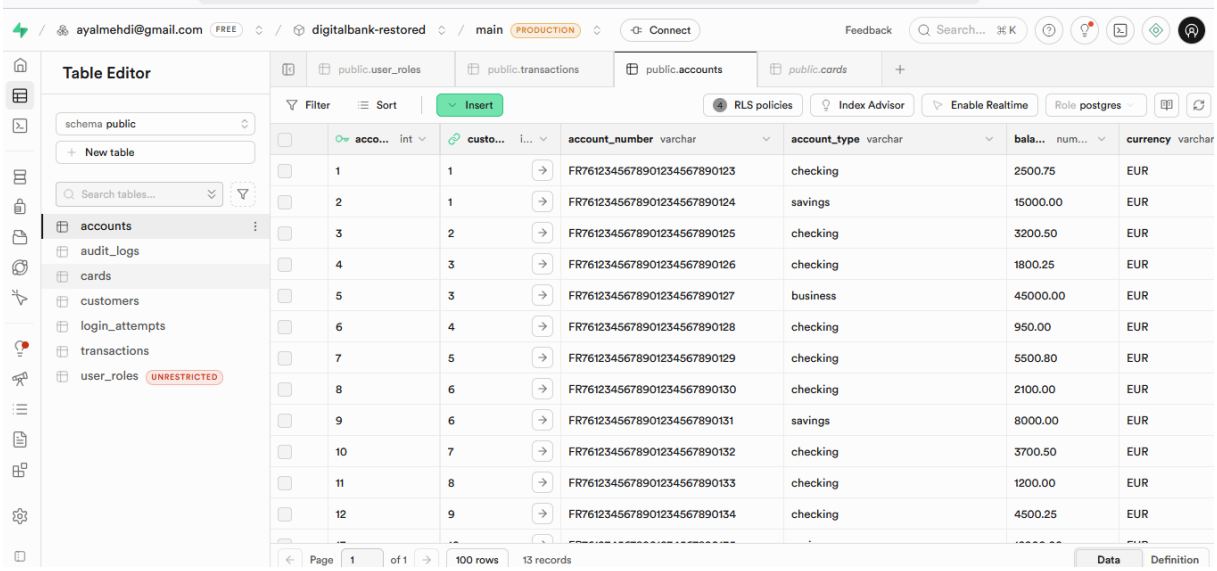
Pour valider l'efficacité de RLS :

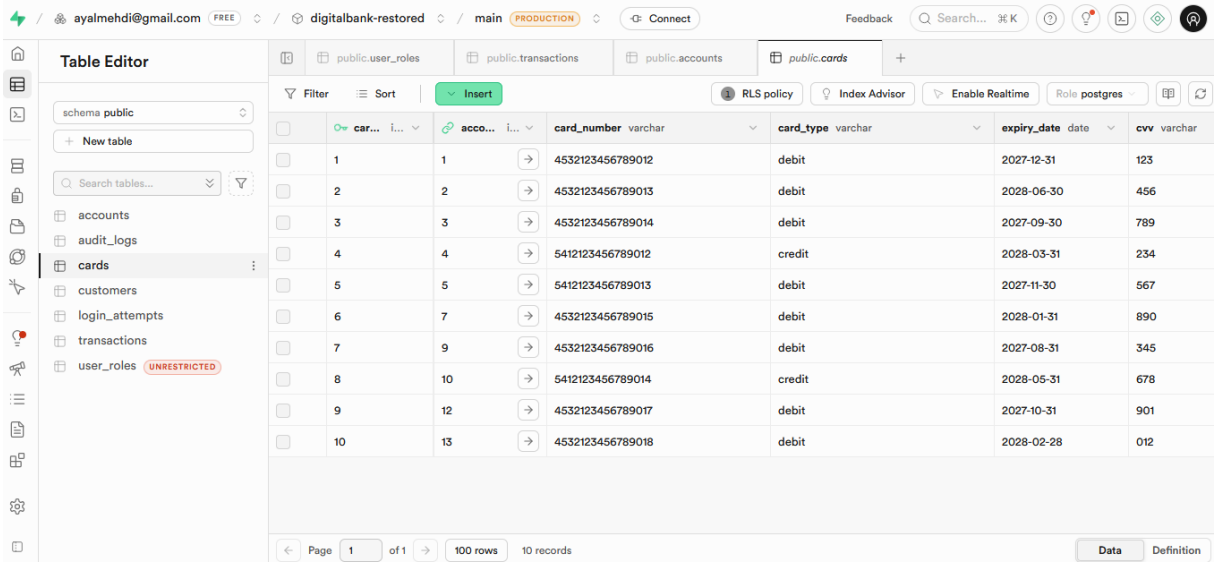
- Des captures d'écran ont été prises dans Supabase, montrant que **RLS est activé** sur chaque table.
- Les policies visibles démontrent que **chaque rôle a bien ses restrictions d'accès**.

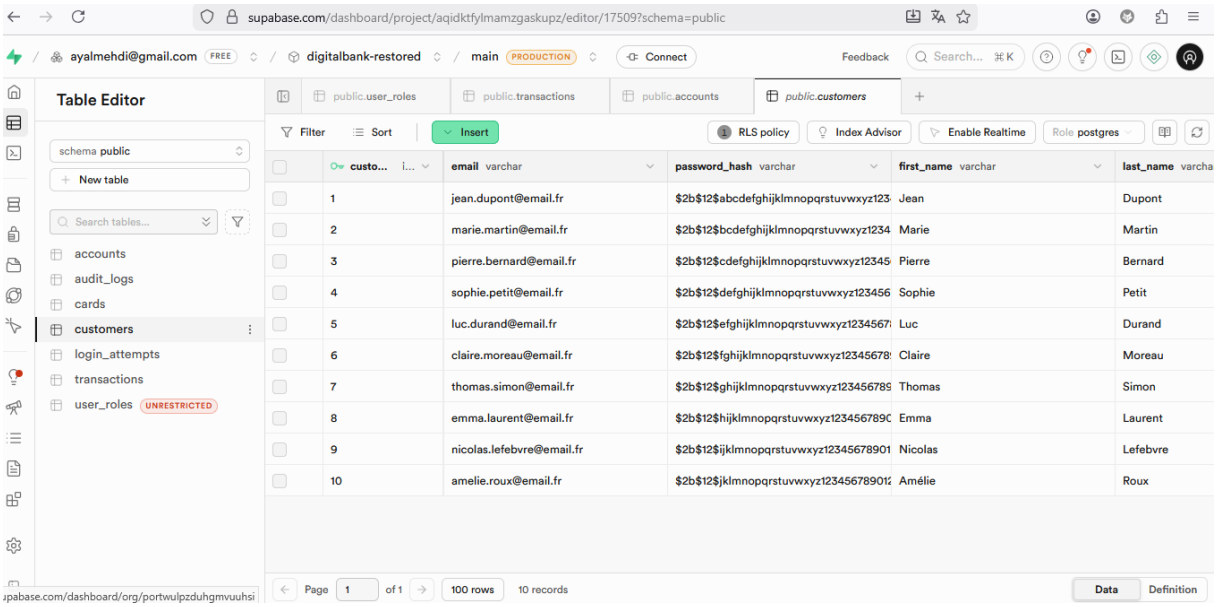
Ainsi, Row Level Security assure que la confidentialité des données est respectée, tout en permettant un accès contrôlé selon le rôle de chaque utilisateur.

🔻 La requête SQL complète des policies RLS peut être consultée dans le fichier **Bloc-notes** fourni avec ce projet.




ayalmehdi@gmail.com FREE
digitalbank-restored
main PRODUCTION
Connect
Feedback
Search... ⌘K
Table Editor
schema public
New table
Search tables...
accounts
audit_logs
cards
customers
login_attempts
transactions
user_roles UNRESTRICTED
public.user_roles
public.transactions
public.accounts
public.cards
Filter
Sort
Insert
RLS policies
Index Advisor
Enable Realtime
Role postgres
acco... int
custo... i...
account_number varchar
account_type varchar
bala... num...
currency varchar
1 1 FR7612345678901234567890123 checking 2500.75 EUR
2 1 FR7612345678901234567890124 savings 15000.00 EUR
3 2 FR7612345678901234567890125 checking 3200.50 EUR
4 3 FR7612345678901234567890126 checking 1800.25 EUR
5 3 FR7612345678901234567890127 business 45000.00 EUR
6 4 FR7612345678901234567890128 checking 950.00 EUR
7 5 FR7612345678901234567890129 checking 5500.80 EUR
8 6 FR7612345678901234567890130 checking 2100.00 EUR
9 6 FR7612345678901234567890131 savings 8000.00 EUR
10 7 FR7612345678901234567890132 checking 3700.50 EUR
11 8 FR7612345678901234567890133 checking 1200.00 EUR
12 9 FR7612345678901234567890134 checking 4500.25 EUR
Page 1 of 1
100 rows
13 records
Data
Definition


ayalmehdi@gmail.com FREE
digitalbank-restored
main PRODUCTION
Connect
Feedback
Search... ⌘K
Table Editor
schema public
New table
Search tables...
accounts
audit_logs
cards
customers
login_attempts
transactions
user_roles UNRESTRICTED
public.user_roles
public.transactions
public.accounts
public.cards
Filter
Sort
Insert
RLS policy
Index Advisor
Enable Realtime
Role postgres
car... i...
acco... i...
card_number varchar
card_type varchar
expiry_date date
cvv varchar
1 1 4532123456789012 debit 2027-12-31 123
2 2 4532123456789013 debit 2028-06-30 456
3 3 4532123456789014 debit 2027-09-30 789
4 4 5412123456789012 credit 2028-03-31 234
5 5 5412123456789013 debit 2027-11-30 567
6 7 4532123456789015 debit 2028-01-31 890
7 9 4532123456789016 debit 2027-08-31 345
8 10 5412123456789014 credit 2028-05-31 678
9 12 4532123456789017 debit 2027-10-31 901
10 13 4532123456789018 debit 2028-02-28 012
Page 1 of 1
100 rows
10 records
Data
Definition


supabase.com/dashboard/project/aqidktfylmamzgaskupz/editor/17509?schema=public
ayalmehdi@gmail.com FREE
digitalbank-restored
main PRODUCTION
Connect
Feedback
Search... ⌘K
Table Editor
schema public
New table
Search tables...
accounts
audit_logs
cards
customers
login_attempts
transactions
user_roles UNRESTRICTED
public.user_roles
public.transactions
public.accounts
public.customers
Filter
Sort
Insert
RLS policy
Index Advisor
Enable Realtime
Role postgres
custo... i...
email varchar
password_hash varchar
first_name varchar
last_name varcha
1 jean.dupont@email.fr $2b$12$abcdefghijklmnopqrstuvwxyz123 Jean Dupont
2 marie.martin@email.fr $2b$12$bcdefghijklmnopqrstuvwxyz1234 Marie Martin
3 pierre.bernard@email.fr $2b$12$cdefghijklmnopqrstuvwxyz12345 Pierre Bernard
4 sophie.petit@email.fr $2b$12$defghijklmnopqrstuvwxyz123456 Sophie Petit
5 luc.durand@email.fr $2b$12$efghijklmnopqrstuvwxyz1234567 Luc Durand
6 claire.moreau@email.fr $2b$12$fghijklmnopqrstuvwxyz12345678 Claire Moreau
7 thomas.simon@email.fr $2b$12$ghijklmnopqrstuvwxyz123456789 Thomas Simon
8 emma.laurent@email.fr $2b$12$hijklmnopqrstuvwxyz1234567890 Emma Laurent
9 nicolas.lefebvre@email.fr $2b$12$ijklmnopqrstuvwxyz12345678901 Nicolas Lefebvre
10 amelie.roux@email.fr $2b$12$jklmnopqrstuvwxyz123456789012 Amélie Roux
Page 1 of 1
100 rows
10 records
Data
Definition
upabase.com/dashboard/org/portwulpzduhgmvuuhsi

3.1.d – Test des permissions

Introduction

Pour vérifier que le système de **gestion des rôles** et les **policies RLS** fonctionnent correctement, nous avons testé chaque rôle en conditions réelles. L'objectif était de confirmer que **chaque utilisateur voit uniquement les données autorisées par son rôle**, et ne peut pas accéder ou modifier les données d'autres utilisateurs.

Les rôles testés sont :

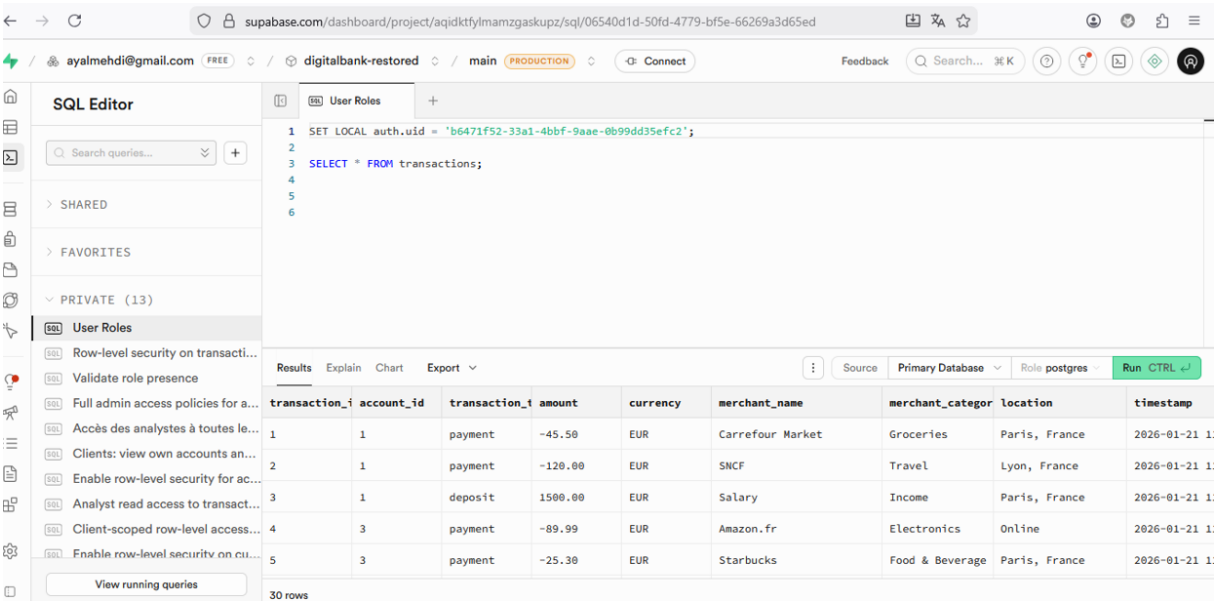
- **Admin** : accès complet, lecture et modification de toutes les données
- **Analyst** : lecture seule sur les transactions et logs
- **Customer Service** : lecture des informations clients et de leurs transactions, modifications limitées
- **Customer** : accès uniquement à ses propres données

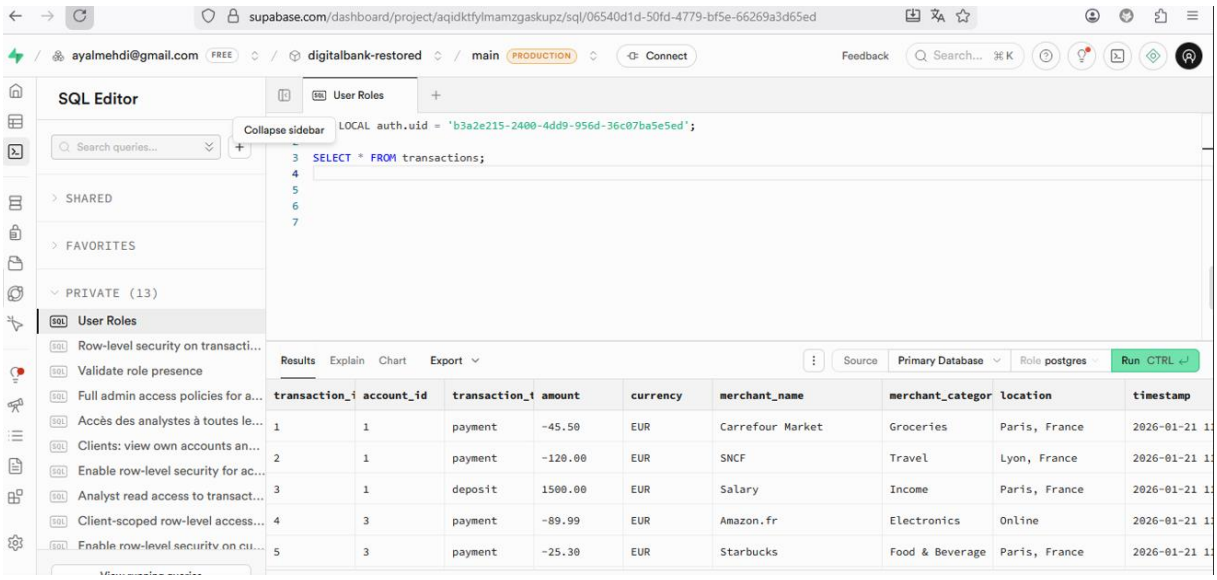
Méthodologie

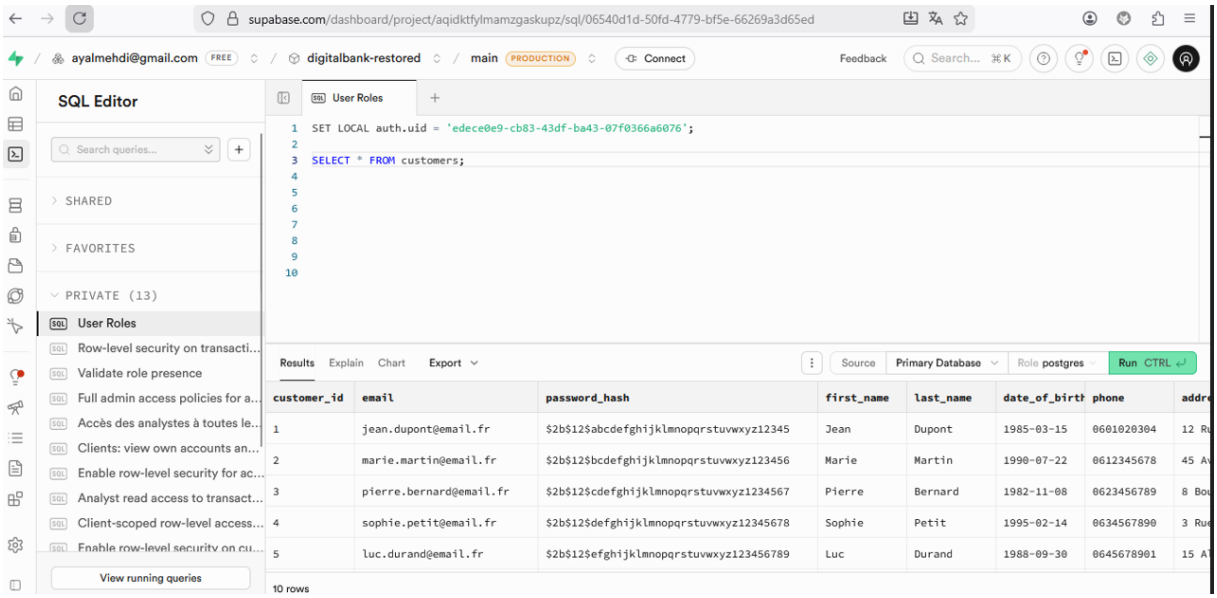
Les tests ont été réalisés directement dans **Supabase Table Editor**, en utilisant les comptes utilisateurs correspondant à chaque rôle.

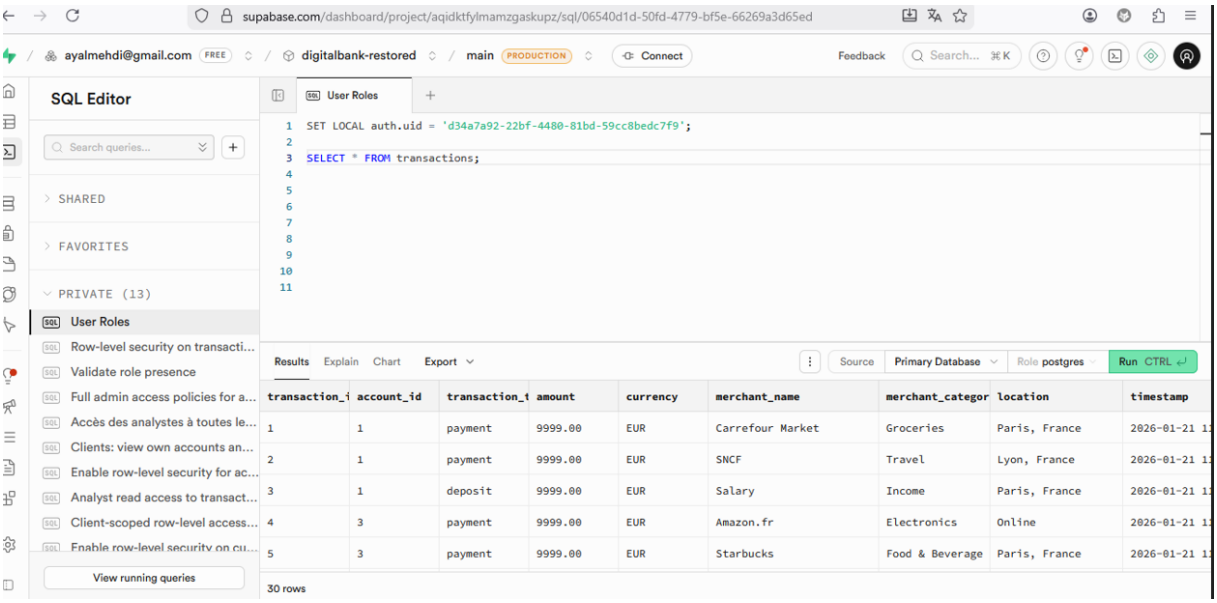
Pour chaque rôle :

1. Connexion avec l'email et le mot de passe de l'utilisateur
2. Ouverture des tables sensibles : `transactions`, `accounts`, `cards`, `customers`, `audit_logs`, `login_attempts`
3. Vérification des données visibles et des possibilités de modification
4. Captures d'écran réalisées pour documenter les résultats


supabase.com/dashboard/project/aqidktfylmamzgaskupz/sql/06540d1d-50fd-4779-bf5e-66269a3d65ed
ayalmehdi@gmail.com FREE / digitalbank-restored / main PRODUCTION Connect Feedback Search... ⌘K
SQL Editor
User Roles
SHARED
FAVORITES
PRIVATE (13)
User Roles
Row-level security on transacti...
Validate role presence
Full admin access policies for a...
Accès des analystes à toutes le...
Clients: view own accounts an...
Enable row-level security for ac...
Analyst read access to transact...
Client-scoped row-level access...
Enable row-level security on cu...
View running queries
1 SET LOCAL auth.uid = 'b6471f52-33a1-4bbf-9aae-0b99dd35efc2';
2
3 SELECT * FROM transactions;
4
5
6
Results Explain Chart Export
Source Primary Database Role postgres Run CTRL
transaction_i account_id transaction_t amount currency merchant_name merchant_categor location timestamp
1 1 payment -45.50 EUR Carrefour Market Groceries Paris, France 2026-01-21 1
2 1 payment -120.00 EUR SNCF Travel Lyon, France 2026-01-21 1
3 1 deposit 1500.00 EUR Salary Income Paris, France 2026-01-21 1
4 3 payment -89.99 EUR Amazon.fr Electronics Online 2026-01-21 1
5 3 payment -25.30 EUR Starbucks Food & Beverage Paris, France 2026-01-21 1
30 rows


supabase.com/dashboard/project/aqidktfylmamzgaskupz/sql/06540d1d-50fd-4779-bf5e-66269a3d65ed
ayalmehdi@gmail.com FREE / digitalbank-restored / main PRODUCTION Connect Feedback Search... ⌘K
SQL Editor
Collapse sidebar
User Roles
SHARED
FAVORITES
PRIVATE (13)
User Roles
Row-level security on transacti...
Validate role presence
Full admin access policies for a...
Accès des analystes à toutes le...
Clients: view own accounts an...
Enable row-level security for ac...
Analyst read access to transact...
Client-scoped row-level access...
Enable row-level security on cu...
LOCAL auth.uid = 'b3a2e215-2400-4dd9-956d-36c07ba5e5ed';
SELECT * FROM transactions;
Results Explain Chart Export
Source Primary Database Role postgres Run CTRL
transaction_i account_id transaction_t amount currency merchant_name merchant_categor location timestamp
1 1 payment -45.50 EUR Carrefour Market Groceries Paris, France 2026-01-21 1
2 1 payment -120.00 EUR SNCF Travel Lyon, France 2026-01-21 1
3 1 deposit 1500.00 EUR Salary Income Paris, France 2026-01-21 1
4 3 payment -89.99 EUR Amazon.fr Electronics Online 2026-01-21 1
5 3 payment -25.30 EUR Starbucks Food & Beverage Paris, France 2026-01-21 1


supabase.com/dashboard/project/aqidktfylmamzgaskupz/sql/06540d1d-50fd-4779-bf5e-66269a3d65ed
ayalmehdi@gmail.com FREE / digitalbank-restored / main PRODUCTION Connect Feedback Search... ⌘K
SQL Editor
User Roles
SHARED
FAVORITES
PRIVATE (13)
User Roles
Row-level security on transacti...
Validate role presence
Full admin access policies for a...
Accès des analystes à toutes le...
Clients: view own accounts an...
Enable row-level security for ac...
Analyst read access to transact...
Client-scoped row-level access...
Enable row-level security on cu...
View running queries
1 SET LOCAL auth.uid = 'edece0e9-cb83-43df-ba43-07f0366a6076';
2
3 SELECT * FROM customers;
4
5
6
7
8
9
10
Results Explain Chart Export
Source Primary Database Role postgres Run CTRL
customer_id email password_hash first_name last_name date_of_birth phone addr
1 jean.dupont@email.fr $2b$12$abcdefghijklmnopqrstuvwxyz12345 Jean Dupont 1985-03-15 0601020304 12 R
2 marie.martin@email.fr $2b$12$bcdefghijklmnopqrstuvwxyz123456 Marie Martin 1990-07-22 0612345678 45 A
3 pierre.bernard@email.fr $2b$12$cdefghijklmnopqrstuvwxyz1234567 Pierre Bernard 1982-11-08 0623456789 8 Bo
4 sophie.petit@email.fr $2b$12$defghijklmnopqrstuvwxyz12345678 Sophie Petit 1995-02-14 0634567890 3 Ru
5 luc.durand@email.fr $2b$12$efghijklmnopqrstuvwxyz123456789 Luc Durand 1988-09-30 0645678901 15 A
10 rows


supabase.com/dashboard/project/aqidktfylmamzgaskupz/sql/06540d1d-50fd-4779-bf5e-66269a3d65ed
ayalmehdi@gmail.com
FREE
digitalbank-restored
main
PRODUCTION
Connect
Feedback
Search... ⌘K
SQL Editor
Search queries...
SHARED
FAVORITES
PRIVATE (13)
User Roles
Row-level security on transacti...
Validate role presence
Full admin access policies for a...
Accès des analystes à toutes le...
Clients: view own accounts an...
Enable row-level security for ac...
Analyst read access to transact...
Client-scoped row-level access...
Enable row-level security on cu...
View running queries
User Roles
1 SET LOCAL auth.uid = 'd34a7a92-22bf-4480-81bd-59cc8bedc7f9';
2
3 SELECT * FROM transactions;
4
5
6
7
8
9
10
11
Results
Explain
Chart
Export
Source
Primary Database
Role postgres
Run CTRL
transaction_i
account_id
transaction_t
amount
currency
merchant_name
merchant_categor
location
timestamp
1 1 payment 9999.00 EUR Carrefour Market Groceries Paris, France 2026-01-21 1
2 1 payment 9999.00 EUR SNCF Travel Lyon, France 2026-01-21 1
3 1 deposit 9999.00 EUR Salary Income Paris, France 2026-01-21 1
4 3 payment 9999.00 EUR Amazon.fr Electronics Online 2026-01-21 1
5 3 payment 9999.00 EUR Starbucks Food & Beverage Paris, France 2026-01-21 1
30 rows