KoraMarket - Auth-Service

Documentation technique et fonctionnelle - v1.0

Juillet 2025

1. Presentation

Le microservice auth-service est le coeur de l'authentification et de la gestion des utilisateurs pour la plateforme KoraMarket.

Il gere :

- Les comptes utilisateurs
- L'authentification securisee (JWT)
- Les roles et permissions
- L'audit de securite (logs d'action)
- Les sessions (access/refresh tokens)
- Les clients OAuth2 (pour integrations externes)
- L'integration avec l'ecosysteme microservices via Spring Cloud

2. Fonctionnalites

- Inscription d'utilisateur
- Connexion (login)
- Delivrance de tokens JWT (access, refresh)
- Rafraichissement du token d'acces
- Consultation du profil utilisateur
- Gestion des roles
- Gestion des permissions
- Association role-permission et user-role
- Gestion des sessions JWT
- Gestion des clients OAuth2 (oauth_clients)
- Audit et journalisation avancee de toutes les actions critiques

3. Architecture et Technologies

- Langage : Java 21
- Framework : Spring Boot 3.5.x

- Gestion des dependances : Maven
- Base de donnees : PostgreSQL 17 (schema dedie : auth_service)
- ORM : Spring Data JPA
- Securite : Spring Security, JWT (avec refresh token)
- Decouverte de service : Eureka (Netflix OSS)
- Configuration centralisee : Spring Cloud Config
- API Gateway : Spring Cloud Gateway
- Audit : AspectJ + AuditLog en base
- Tests : Postman (recettes manuelles ou automatisees)

4. Securite

- Authentication JWT :
  - Token access d'1 jour, refresh token de 7 jours
  - Token genere a la connexion, valide a chaque requete via un filtre personnalise
  - Refresh possible via endpoint dedie /refresh
- Gestion des roles et permissions RBAC
- Controle d'acces fin sur les endpoints :
  - Exemple : /api/admin seulement pour les utilisateurs avec le role ADMIN
  - Possibilite d'affiner sur des permissions precises
- Audit de toutes les actions sensibles
- Protection contre les CSRF et attaques courantes

5. Endpoints principaux

Exemples d'API :

POST	/api/auth/register	Inscription d'un utilisateur	Public
POST	/api/auth/login	Authentification, retourne JWT	Public
POST	/api/auth/refresh	Rafraichit l'accessToken	Public (token)
GET	/api/auth/me	Profil de l'utilisateur courant	Authentifie
GET	/api/roles	Liste des roles	Admin
POST	/api/roles	Creation de role	Admin
GET	/api/permissions	Liste des permissions	Admin
POST	/api/permissions	Creation de permission	Admin
GET	/api/role-permissions	Liste des associations role-perm	Admin

POST	/api/role-permissions	Associer role et permission	Admin
GET	/api/user-roles	Liste des associations user-role	Admin
POST	/api/user-roles	Associer utilisateur et role	Admin
GET	/api/oauth-clients	Liste des clients OAuth2	Admin
POST	/api/oauth-clients	Creation d'un client OAuth2	Admin
DELETE	/api/oauth-clients/id	Suppression d'un client OAuth2	Admin

6. Utilisation - Scenarios types

A. Inscription

POST /api/auth/register

Payload :

```
{
  "nom": "Doe",
  "prenom": "John",
  "email": "john@gmail.com",
  "motDePasse": "password123",
  "telephone": "22670123456",
  "statut": "ACTIF"
}
```

B. Login

POST /api/auth/login

Payload :

```
{
  "email": "john@gmail.com",
  "motDePasse": "password123"
}
```

C. Recuperer le profil

GET /api/auth/me

Header : Authorization: Bearer accessToken

D. Rafraichir un token

POST /api/auth/refresh

Payload :

{ "refreshToken": "xxxx-xxxx-xxxx-xxxx" }

E. Associer un role a un utilisateur

POST /api/user-roles

Payload :

{ "userId": 1, "roleId": 2 }

F. Creer un client OAuth2

POST /api/oauth-clients

Payload :

```
{
  "clientId": "client-tuto",
  "clientSecret": "mySuperSecret",
  "scopes": "read,write",
  "redirectUri": "https://koramarket.com/callback"
}
```

7. Points d'extension et recommandations

- Integration Keycloak ou Auth0 possible
- Ajouter reset password, activation, 2FA, etc.
- Swagger OpenAPI pour la doc interactive
- Auditer tous les acces critiques par AOP deja amorce
- Securiser la sauvegarde des secrets hash, vault...

8. Structure du code schema rapide

com.koramarket.auth

controller

service

model

dto

mapper

repository

security

audit

Contact et Contributeurs

Sidiki NIKIEMA - lead developer KoraMarket Burkina Faso

ChatGPT supporte par OpenAI code doc audit