**Documentação: Sistema de Gerenciamento de Usuários com Autenticação Avançada**

**1. Introdução**

O **Sistema de Gerenciamento de Usuários com Autenticação Avançada** é uma API RESTful projetada para gerenciar usuários com autenticação e autorização. Ele permite realizar operações como registro, login, controle de permissões e gerenciamento de perfis, além de oferecer funcionalidades avançadas de segurança, como proteção de endpoints e recuperação de senha.

**2. Tecnologias Utilizadas**

* **Spring Boot** (Web, Data JPA, Security)
* **JWT (JSON Web Tokens)** para autenticação sem estado
* **BCrypt** para hashing de senhas
* **PostgreSQL** como banco de dados
* **Swagger/OpenAPI** para documentação da API
* **JUnit e Mockito** para testes automatizados

**3. Funcionalidades Principais**

1. Cadastro de usuários com validação de e-mail.
2. Login e geração de token JWT.
3. Controle de acesso baseado em papéis (ADMIN, USER, etc.).
4. Recuperação de senha com tokens de recuperação.
5. Atualização de perfil do usuário autenticado.
6. Proteção contra ataques comuns (CSRF, XSS, SQL Injection).
7. Logs de auditoria para atividades sensíveis.

**4. Endpoints**

**4.1. Autenticação**

* **POST /api/auth/register**
  + **Descrição:** Cadastro de um novo usuário.
  + **Body Exemplo:**

json

Copiar código

{

"username": "johndoe",

"email": "johndoe@example.com",

"password": "securePassword123",

"role": "USER"

}

* + **Respostas:**
    - **201 Created:** Usuário cadastrado com sucesso.
    - **400 Bad Request:** Dados inválidos ou usuário já existente.
* **POST /api/auth/login**
  + **Descrição:** Login e geração de token JWT.
  + **Body Exemplo:**

json

Copiar código

{

"username": "johndoe",

"password": "securePassword123"

}

* + **Respostas:**
    - **200 OK:** Retorna o token JWT.
    - **401 Unauthorized:** Credenciais inválidas.
* **POST /api/auth/forgot-password**
  + **Descrição:** Solicitação de recuperação de senha.
  + **Body Exemplo:**

json

Copiar código

{

"email": "johndoe@example.com"

}

* + **Respostas:**
    - **200 OK:** E-mail de recuperação enviado.
    - **404 Not Found:** E-mail não registrado.
* **POST /api/auth/reset-password**
  + **Descrição:** Reset de senha com token de recuperação.
  + **Body Exemplo:**

json

Copiar código

{

"token": "recoveryToken123",

"newPassword": "newSecurePassword123"

}

* + **Respostas:**
    - **200 OK:** Senha atualizada com sucesso.
    - **400 Bad Request:** Token inválido ou expirado.

**4.2. Gerenciamento de Usuários**

* **GET /api/users**
  + **Descrição:** Lista todos os usuários (somente para ADMIN).
  + **Headers Necessários:** Authorization: Bearer <token>
  + **Respostas:**
    - **200 OK:** Retorna a lista de usuários.
    - **403 Forbidden:** Acesso negado.
* **GET /api/users/{id}**
  + **Descrição:** Retorna detalhes de um usuário específico.
  + **Headers Necessários:** Authorization: Bearer <token>
  + **Respostas:**
    - **200 OK:** Retorna os detalhes do usuário.
    - **404 Not Found:** Usuário não encontrado.
* **DELETE /api/users/{id}**
  + **Descrição:** Exclui um usuário (somente para ADMIN).
  + **Headers Necessários:** Authorization: Bearer <token>
  + **Respostas:**
    - **204 No Content:** Usuário excluído.
    - **403 Forbidden:** Acesso negado.

**4.3. Perfil**

* **GET /api/profile**
  + **Descrição:** Retorna os dados do usuário autenticado.
  + **Headers Necessários:** Authorization: Bearer <token>
  + **Respostas:**
    - **200 OK:** Retorna os dados do perfil.
* **PUT /api/profile**
  + **Descrição:** Atualiza os dados do usuário autenticado.
  + **Headers Necessários:** Authorization: Bearer <token>
  + **Body Exemplo:**

json

Copiar código

{

"username": "johnupdated",

"email": "johnupdated@example.com"

}

* + **Respostas:**
    - **200 OK:** Perfil atualizado.
    - **400 Bad Request:** Dados inválidos.

**5. Segurança**

**5.1. Configuração de Segurança**

* **Criptografia de Senhas:** Todas as senhas são armazenadas como hashes usando **BCrypt**.
* **JWT:** Tokens gerados para autenticação incluem informações como usuário e data de expiração.
* **Autorização baseada em papéis:** Controle granular de acesso aos endpoints com base nos papéis atribuídos.
* **Headers HTTP seguros:**
  + X-Content-Type-Options: nosniff
  + X-Frame-Options: DENY
  + Content-Security-Policy

**6. Estrutura do Banco de Dados**

**Tabela: users**

| **Campo** | **Tipo** | **Descrição** |
| --- | --- | --- |
| id | String | Identificador único (UUID). |
| username | String | Nome de usuário. |
| email | String | E-mail único. |
| password | String | Senha hashada. |
| role | String | Papel do usuário (ADMIN, USER) |
| created\_at | Timestamp | Data de criação. |
| updated\_at | Timestamp | Data de última atualização. |

**Tabela: password\_recovery\_tokens**

| **Campo** | **Tipo** | **Descrição** |
| --- | --- | --- |
| token | String | Token único. |
| user\_id | String | ID do usuário associado. |
| expires\_at | Timestamp | Data de expiração do token. |

**7. Testes Automatizados**

**Casos de Teste Incluídos:**

1. Teste de cadastro com dados válidos/invalidos.
2. Login com credenciais corretas e incorretas.
3. Acesso a endpoints protegidos sem autenticação.
4. Atualização de perfil com dados inválidos.
5. Recuperação de senha com token expirado.

**8. Ferramentas de Integração**

* **Swagger UI:** Disponível em /swagger-ui.html.
* **Postman Collection:** Fornecida para facilitar testes (disponível sob solicitação).

**9. Deploy**

**Pré-requisitos:**

* Banco de dados PostgreSQL configurado.
* Variáveis de ambiente:
  + JWT\_SECRET
  + DB\_URL
  + DB\_USERNAME
  + DB\_PASSWORD

**Comandos:**

* **Build:** mvn clean package
* **Run:** java -jar target/app.jar

Essa documentação cobre os principais aspectos do sistema, mas pode ser expandida com mais detalhes sobre logs, métricas e monitoramento conforme necessário! Se precisar de algo mais, é só pedir! 🚀

Aqui está a **modelagem da base de dados** para o Sistema de Gerenciamento de Usuários com Autenticação Avançada. Vamos usar um modelo relacional com 3 tabelas principais: users, roles e password\_recovery\_tokens.

**Entidades e Relacionamentos**

1. **Tabela: users**
   * Responsável por armazenar as informações dos usuários do sistema.
   * Relacionamento: Cada usuário pode ter um único papel (role).

| **Campo** | **Tipo** | **Descrição** |
| --- | --- | --- |
| id | VARCHAR(255) | Identificador único do usuário (UUID ou String). |
| username | VARCHAR(255) | Nome de usuário único. |
| email | VARCHAR(255) | E-mail do usuário (único). |
| password | VARCHAR(255) | Senha criptografada do usuário. |
| role\_id | VARCHAR(255) | ID do papel do usuário (FK para a tabela roles). |
| created\_at | TIMESTAMP | Data de criação do usuário. |
| updated\_at | TIMESTAMP | Data da última atualização do usuário. |

1. **Chave Primária:**
   * id (String)

**Chave Estrangeira:**

* + role\_id (referência para a tabela roles)

**Exemplo de Dados:**

sql

Copiar código

INSERT INTO users (id, username, email, password, role\_id, created\_at, updated\_at)

VALUES ('1', 'johndoe', 'johndoe@example.com', 'hashedPassword', 'user\_role', '2024-11-15 09:00:00', '2024-11-15 09:00:00');

1. **Tabela: roles**
   * Armazena os papéis de usuário no sistema (por exemplo: ADMIN, USER).
   * Relacionamento: Um papel pode ser atribuído a vários usuários.

| **Campo** | **Tipo** | **Descrição** |
| --- | --- | --- |
| id | VARCHAR(255) | Identificador único do papel. |
| name | VARCHAR(255) | Nome do papel (por exemplo, 'USER', 'ADMIN'). |
| description | TEXT | Descrição do papel (opcional). |

1. **Chave Primária:**
   * id (String)

**Exemplo de Dados:**

sql

Copiar código

INSERT INTO roles (id, name, description)

VALUES ('user\_role', 'USER', 'Usuário com acesso básico'),

('admin\_role', 'ADMIN', 'Administrador com acesso total');

1. **Tabela: password\_recovery\_tokens**
   * Armazena tokens gerados para recuperação de senha.
   * Relacionamento: Um token está associado a um único usuário.

| **Campo** | **Tipo** | **Descrição** |
| --- | --- | --- |
| token | VARCHAR(255) | Token único para recuperação de senha. |
| user\_id | VARCHAR(255) | ID do usuário associado (FK para a tabela users). |
| expires\_at | TIMESTAMP | Data de expiração do token. |
| created\_at | TIMESTAMP | Data de criação do token. |

1. **Chave Primária:**
   * token (String)

**Chave Estrangeira:**

* + user\_id (referência para a tabela users)

**Exemplo de Dados:**

sql

Copiar código

INSERT INTO password\_recovery\_tokens (token, user\_id, expires\_at, created\_at)

VALUES ('recoveryToken123', '1', '2024-11-16 09:00:00', '2024-11-15 09:00:00');

**Relacionamentos Entre as Tabelas**

* **users -> roles**:
  + Relacionamento: Cada usuário tem um único papel, mas um papel pode ser atribuído a vários usuários.
  + Tipo: **Muitos-para-Um** (Many-to-One).
  + A chave estrangeira role\_id na tabela users aponta para id na tabela roles.
* **users -> password\_recovery\_tokens**:
  + Relacionamento: Um usuário pode ter vários tokens de recuperação de senha, mas cada token pertence a um único usuário.
  + Tipo: **Um-para-Muitos** (One-to-Many).
  + A chave estrangeira user\_id na tabela password\_recovery\_tokens aponta para id na tabela users.

**Diagrama de Entidades**

Aqui está uma visão geral das entidades e seus relacionamentos:

lua

Copiar código

+-------------------+ +-------------------+

| users | | roles |

+-------------------+ +-------------------+

| id (PK) |<----- | id (PK) |

| username | | name |

| email | | description |

| password | +-------------------+

| role\_id (FK) |

| created\_at |

| updated\_at |

+-------------------+

|

|

v

+----------------------------+

| password\_recovery\_tokens |

+----------------------------+

| token (PK) |

| user\_id (FK) |

| expires\_at |

| created\_at |

+----------------------------+

**Considerações de Segurança**

* **Criptografia de Senhas:** As senhas são armazenadas de forma segura usando **BCrypt** no campo password da tabela users.
* **Tokens de Recuperação de Senha:** Os tokens de recuperação de senha na tabela password\_recovery\_tokens são temporários e expiram após um período de tempo (geralmente 1-2 horas).
* **Controle de Acesso:** O papel de cada usuário (role\_id) é utilizado para garantir que o acesso aos recursos da aplicação seja restrito de acordo com o nível de permissões do usuário (ADMIN, USER, etc.).

**SQL para Criação das Tabelas**

sql

Copiar código

CREATE TABLE roles (

id VARCHAR(255) PRIMARY KEY,

name VARCHAR(255) NOT NULL,

description TEXT

);

CREATE TABLE users (

id VARCHAR(255) PRIMARY KEY,

username VARCHAR(255) NOT NULL UNIQUE,

email VARCHAR(255) NOT NULL UNIQUE,

password VARCHAR(255) NOT NULL,

role\_id VARCHAR(255),

created\_at TIMESTAMP DEFAULT CURRENT\_TIMESTAMP,

updated\_at TIMESTAMP DEFAULT CURRENT\_TIMESTAMP,

FOREIGN KEY (role\_id) REFERENCES roles(id)

);

CREATE TABLE password\_recovery\_tokens (

token VARCHAR(255) PRIMARY KEY,

user\_id VARCHAR(255),

expires\_at TIMESTAMP NOT NULL,

created\_at TIMESTAMP DEFAULT CURRENT\_TIMESTAMP,

FOREIGN KEY (user\_id) REFERENCES users(id)

);

**Considerações Finais**

A modelagem do banco de dados apresentada visa garantir segurança e flexibilidade para o gerenciamento de usuários e autenticação. O uso de **papéis** e **tokens de recuperação** proporciona uma abordagem robusta para segurança e controle de acesso. Se houver necessidade de escalar ou adaptar o sistema, a estrutura pode ser facilmente estendida com mais tabelas ou relacionamentos.

O código que você forneceu para o controlador UserController no Spring Boot está bem estruturado e segue boas práticas para um sistema de gerenciamento de usuários com autenticação JWT. Vou fazer algumas observações e ajustes para melhorar a clareza e o funcionamento correto de alguns detalhes.

**Observações e Ajustes:**

1. **Erro no JwtTokenUtil**: O código está tentando acessar o token JWT atual com jwtTokenUtil.getCurrentJwtToken(), mas essa abordagem pode não ser correta, dependendo da implementação do JwtTokenUtil. Uma abordagem mais comum é recuperar o token do cabeçalho da requisição HTTP, normalmente no campo Authorization.
2. **Autorização**: Para a segurança, a classe de segurança deve garantir que apenas usuários autenticados possam acessar endpoints como /profile e /getAllUsers. Caso contrário, um usuário não autenticado poderia acessar essas rotas.
3. **Validação de Dados de Entrada**: Você usa @Valid no método de registro para validar as entradas. Isso é ótimo, mas você pode querer adicionar uma camada de validação personalizada para os dados do usuário (se necessário).

**Ajustes Propostos:**

1. **Obter o token JWT no método getProfile**: A maneira de pegar o JWT na requisição HTTP geralmente é via o cabeçalho Authorization. Você pode adaptar o método para pegar o token da requisição.
2. **Configuração do Spring Security**: Para proteger as rotas, você provavelmente precisará configurar os filtros de segurança do Spring Security para garantir que os endpoints de login e perfil de usuário sejam acessíveis somente com um token JWT válido.

**Código Ajustado do UserController:**

java

Copiar código

package com.example.usermanagement.controller;

import com.example.usermanagement.model.User;

import com.example.usermanagement.security.JwtTokenUtil;

import com.example.usermanagement.service.UserService;

import com.example.usermanagement.dto.UserDTO;

import org.springframework.beans.factory.annotation.Autowired;

import org.springframework.http.HttpStatus;

import org.springframework.http.ResponseEntity;

import org.springframework.security.authentication.AuthenticationManager;

import org.springframework.security.authentication.UsernamePasswordAuthenticationToken;

import org.springframework.security.core.Authentication;

import org.springframework.security.core.context.SecurityContextHolder;

import org.springframework.web.bind.annotation.\*;

import javax.servlet.http.HttpServletRequest;

import javax.validation.Valid;

@RestController

@RequestMapping("/api/v1/users")

public class UserController {

@Autowired

private UserService userService;

@Autowired

private JwtTokenUtil jwtTokenUtil;

@Autowired

private AuthenticationManager authenticationManager;

// Endpoint para registro de novos usuários

@PostMapping("/register")

public ResponseEntity<?> register(@Valid @RequestBody UserDTO userDTO) {

User newUser = userService.registerUser(userDTO);

return new ResponseEntity<>(newUser, HttpStatus.CREATED);

}

// Endpoint para login de usuários (gera token JWT)

@PostMapping("/login")

public ResponseEntity<?> login(@RequestBody UserDTO userDTO) {

Authentication authentication = authenticationManager.authenticate(

new UsernamePasswordAuthenticationToken(userDTO.getUsername(), userDTO.getPassword())

);

SecurityContextHolder.getContext().setAuthentication(authentication);

String jwt = jwtTokenUtil.generateToken(authentication);

return ResponseEntity.ok(jwt);

}

// Endpoint para obter informações do usuário (apenas para usuários autenticados)

@GetMapping("/profile")

public ResponseEntity<User> getProfile(HttpServletRequest request) {

// Obtém o token do cabeçalho Authorization

String token = jwtTokenUtil.getTokenFromRequest(request);

if (token == null || !jwtTokenUtil.validateToken(token)) {

return ResponseEntity.status(HttpStatus.UNAUTHORIZED).build();

}

String username = jwtTokenUtil.getUsernameFromToken(token);

User user = userService.getUserByUsername(username);

return ResponseEntity.ok(user);

}

// Endpoint para listar todos os usuários (somente administradores)

@GetMapping

public ResponseEntity<?> getAllUsers() {

// Este endpoint pode ser restrito para administradores através do Spring Security

return ResponseEntity.ok(userService.getAllUsers());

}

// Endpoint para atualizar um usuário

@PutMapping("/{id}")

public ResponseEntity<User> updateUser(@PathVariable String id, @RequestBody UserDTO userDTO) {

User updatedUser = userService.updateUser(id, userDTO);

return ResponseEntity.ok(updatedUser);

}

// Endpoint para deletar um usuário

@DeleteMapping("/{id}")

public ResponseEntity<?> deleteUser(@PathVariable String id) {

userService.deleteUser(id);

return ResponseEntity.noContent().build();

}

}

**Alterações Feitas:**

1. **getProfile(HttpServletRequest request)**: Agora o método getProfile recebe o HttpServletRequest e extrai o token do cabeçalho Authorization. O JwtTokenUtil agora precisa de um método adicional getTokenFromRequest para lidar com a extração do token.

Aqui está a implementação sugerida do getTokenFromRequest no JwtTokenUtil:

java

Copiar código

public String getTokenFromRequest(HttpServletRequest request) {

String bearerToken = request.getHeader("Authorization");

if (bearerToken != null && bearerToken.startsWith("Bearer ")) {

return bearerToken.substring(7); // Remove "Bearer " do começo

}

return null;

}

1. **Validação do Token**: Antes de tentar obter o nome de usuário a partir do token, o código agora verifica se o token é válido usando o método validateToken. Isso ajuda a proteger o sistema contra tokens inválidos ou expirados.

**Configuração de Segurança no Spring Security:**

Para proteger o acesso aos endpoints, você também pode precisar configurar o Spring Security. Um exemplo de configuração para proteger as rotas e permitir apenas usuários autenticados acessar os endpoints:

java

Copiar código

package com.example.usermanagement.security;

import org.springframework.context.annotation.Bean;

import org.springframework.context.annotation.Configuration;

import org.springframework.http.HttpMethod;

import org.springframework.security.authentication.AuthenticationManager;

import org.springframework.security.config.annotation.authentication.builders.AuthenticationManagerBuilder;

import org.springframework.security.config.annotation.web.builders.HttpSecurity;

import org.springframework.security.config.annotation.web.configuration.EnableWebSecurity;

import org.springframework.security.config.annotation.web.configuration.WebSecurityConfigurerAdapter;

import org.springframework.security.core.userdetails.UserDetailsService;

import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;

import org.springframework.security.crypto.password.PasswordEncoder;

@Configuration

@EnableWebSecurity

public class SecurityConfig extends WebSecurityConfigurerAdapter {

@Autowired

private JwtAuthenticationEntryPoint jwtAuthenticationEntryPoint;

@Autowired

private JwtRequestFilter jwtRequestFilter;

@Autowired

private UserDetailsService userDetailsService;

@Override

protected void configure(HttpSecurity http) throws Exception {

http.csrf().disable()

.authorizeRequests()

.antMatchers("/api/v1/users/login", "/api/v1/users/register").permitAll() // Permitir login e registro sem autenticação

.antMatchers(HttpMethod.GET, "/api/v1/users/profile").authenticated() // Requer autenticação para perfil

.antMatchers(HttpMethod.GET, "/api/v1/users").hasRole("ADMIN") // Somente admin pode ver todos os usuários

.anyRequest().authenticated() // Qualquer outra requisição exige autenticação

.and()

.exceptionHandling().authenticationEntryPoint(jwtAuthenticationEntryPoint)

.and()

.addFilterBefore(jwtRequestFilter, UsernamePasswordAuthenticationFilter.class);

}

@Override

@Bean

public AuthenticationManager authenticationManagerBean() throws Exception {

return super.authenticationManagerBean();

}

@Bean

public PasswordEncoder passwordEncoder() {

return new BCryptPasswordEncoder();

}

@Override

protected void configure(AuthenticationManagerBuilder auth) throws Exception {

auth.userDetailsService(userDetailsService).passwordEncoder(passwordEncoder());

}

}

Essa configuração assume que você tem um filtro JWT (JwtRequestFilter) que intercepta as requisições e autentica os usuários baseados no token JWT enviado no cabeçalho Authorization. A classe JwtAuthenticationEntryPoint é usada para gerenciar exceções relacionadas à autenticação, como o envio de uma resposta 401 Unauthorized quando o token é inválido ou ausente.

**Conclusão:**

Com esses ajustes, você agora tem um controlador de usuários que permite o registro, login, atualização, exclusão e recuperação de perfil, com segurança baseada em JWT. Além disso, é importante configurar corretamente o Spring Security para garantir que os endpoints sejam protegidos adequadamente.

Para completar o sistema de gerenciamento de usuários, vamos criar um **DTO (Data Transfer Object)** para o usuário. O **UserDTO** servirá para transferir dados entre o cliente e o servidor sem expor diretamente a entidade do banco de dados. Geralmente, ele é utilizado para **encapsular** dados da API de forma mais segura e permitir a validação de dados de entrada.

Abaixo, vou criar o DTO com validação e um modelo básico de como os dados do usuário são transferidos:

**UserDTO.java**

java

Copiar código

package com.exemplo.usermanagement.dto;

import javax.validation.constraints.Email;

import javax.validation.constraints.NotBlank;

import javax.validation.constraints.Size;

public class UserDTO {

@NotBlank(message = "Username is required")

@Size(min = 3, max = 20, message = "Username must be between 3 and 20 characters")

private String username;

@NotBlank(message = "Password is required")

@Size(min = 6, message = "Password must be at least 6 characters long")

private String password;

@NotBlank(message = "Email is required")

@Email(message = "Email should be valid")

private String email;

// Papel do usuário (ADMIN, USER)

@NotBlank(message = "Role is required")

private String role;

// Getters e Setters

public String getUsername() {

return username;

}

public void setUsername(String username) {

this.username = username;

}

public String getPassword() {

return password;

}

public void setPassword(String password) {

this.password = password;

}

public String getEmail() {

return email;

}

public void setEmail(String email) {

this.email = email;

}

public String getRole() {

return role;

}

public void setRole(String role) {

this.role = role;

}

// Métodos adicionais, se necessário

}

**Explicação do DTO:**

1. **Validações**:
   * **@NotBlank**: Garante que o campo não pode ser vazio ou nulo.
   * **@Size**: Define um tamanho mínimo ou máximo para o campo, como no caso do username (mínimo de 3 e máximo de 20 caracteres).
   * **@Email**: Valida se o e-mail fornecido está no formato correto.
2. **Campos**:
   * **username**: O nome de usuário do usuário.
   * **password**: A senha do usuário (que deve ser hashada antes de ser armazenada).
   * **email**: O e-mail único do usuário.
   * **role**: O papel do usuário (pode ser ADMIN ou USER).

**Utilização do DTO no UserController**

No controlador UserController, já configuramos a utilização do UserDTO para receber os dados de entrada nos endpoints de **registro de usuário** e **login**.

Exemplo de uso no método de **registro de usuário**:

java

Copiar código

@PostMapping("/register")

public ResponseEntity<?> register(@Valid @RequestBody UserDTO userDTO) {

User newUser = userService.registerUser(userDTO);

return new ResponseEntity<>(newUser, HttpStatus.CREATED);

}

**Conclusão**

Agora, com o **UserDTO** configurado, temos um **Data Transfer Object** seguro e validado para manipulação dos dados de entrada na aplicação. Ele ajuda a manter a separação de responsabilidades e a proteger dados sensíveis, como a senha do usuário, evitando que a entidade do banco de dados seja diretamente exposta na API.

Esse DTO pode ser utilizado em todos os pontos de entrada da aplicação onde os dados do usuário precisam ser manipulados, garantindo que apenas dados válidos sejam processados.

Com base nas informações fornecidas, podemos criar a **modelagem da tabela** users no banco de dados, além de refletir essa estrutura em uma **entidade JPA** para usar com o Spring Boot.

**Estrutura da Tabela no Banco de Dados**

**Tabela**: users

| **Campo** | **Tipo** | **Descrição** |
| --- | --- | --- |
| id | UUID | Identificador único (UUID). |
| username | String | Nome de usuário (único). |
| email | String | E-mail único. |
| password | String | Senha hashada. |
| role | String | Papel do usuário (ADMIN, USER). |
| created\_at | Timestamp | Data de criação do usuário. |
| updated\_at | Timestamp | Data de última atualização do usuário. |

**Definindo a Entidade User em Java (JPA)**

Agora, vamos criar a **entidade JPA** para refletir essa tabela no banco de dados. Essa entidade usará o **UUID** como identificador, conforme especificado.

**User.java (Entidade JPA)**

java

Copiar código

package com.exemplo.usermanagement.model;

import javax.persistence.\*;

import java.time.LocalDateTime;

import java.util.UUID;

@Entity

@Table(name = "users")

public class User {

@Id

@GeneratedValue(strategy = GenerationType.AUTO)

private UUID id;

@Column(unique = true, nullable = false)

private String username;

@Column(unique = true, nullable = false)

private String email;

@Column(nullable = false)

private String password;

@Column(nullable = false)

private String role;

@Column(name = "created\_at", updatable = false)

private LocalDateTime createdAt;

@Column(name = "updated\_at")

private LocalDateTime updatedAt;

@PrePersist

public void onCreate() {

createdAt = LocalDateTime.now();

}

@PreUpdate

public void onUpdate() {

updatedAt = LocalDateTime.now();

}

// Getters e Setters

public UUID getId() {

return id;

}

public void setId(UUID id) {

this.id = id;

}

public String getUsername() {

return username;

}

public void setUsername(String username) {

this.username = username;

}

public String getEmail() {

return email;

}

public void setEmail(String email) {

this.email = email;

}

public String getPassword() {

return password;

}

public void setPassword(String password) {

this.password = password;

}

public String getRole() {

return role;

}

public void setRole(String role) {

this.role = role;

}

public LocalDateTime getCreatedAt() {

return createdAt;

}

public void setCreatedAt(LocalDateTime createdAt) {

this.createdAt = createdAt;

}

public LocalDateTime getUpdatedAt() {

return updatedAt;

}

public void setUpdatedAt(LocalDateTime updatedAt) {

this.updatedAt = updatedAt;

}

}

**Explicação:**

1. **UUID para o id**: O identificador único do usuário é do tipo UUID, conforme sua especificação.
2. **Campos username, email, password, role**: Esses campos estão mapeados para as respectivas colunas na tabela users. O username e email são únicos, e o password armazena a senha hashada.
3. **createdAt e updatedAt**: Usamos LocalDateTime para armazenar as datas de criação e atualização. O método @PrePersist é usado para definir automaticamente o createdAt antes de persistir o objeto. O método @PreUpdate é usado para atualizar o updatedAt sempre que o objeto for alterado.
4. **@Entity**: A classe é anotada com @Entity, indicando que é uma entidade JPA.
5. **@Table(name = "users")**: Especifica o nome da tabela no banco de dados.

**Repositório JPA**

Agora, vamos criar o repositório JPA para manipulação dos dados da tabela users.

**UserRepository.java**

java

Copiar código

package com.exemplo.usermanagement.repository;

import com.exemplo.usermanagement.model.User;

import org.springframework.data.jpa.repository.JpaRepository;

import java.util.Optional;

import java.util.UUID;

public interface UserRepository extends JpaRepository<User, UUID> {

// Buscar um usuário pelo nome de usuário

Optional<User> findByUsername(String username);

// Buscar um usuário pelo email

Optional<User> findByEmail(String email);

// Verificar se o nome de usuário existe

boolean existsByUsername(String username);

// Verificar se o email existe

boolean existsByEmail(String email);

}

**Explicação:**

* **findByUsername**: Método para buscar um usuário pelo nome de usuário.
* **findByEmail**: Método para buscar um usuário pelo email.
* **existsByUsername e existsByEmail**: Métodos para verificar se um usuário com o nome de usuário ou email já existe no banco de dados.

**Conclusão**

Com a modelagem da tabela users, a entidade User e o repositório UserRepository configurados, o sistema agora pode realizar operações de criação, leitura, atualização e exclusão (CRUD) de usuários com base nessa estrutura de banco de dados.

Você pode expandir ou adaptar esse código para incluir mais funcionalidades de acordo com a necessidade do seu sistema, como validações adicionais ou campos extras.

A camada de **Service** no Spring Boot é responsável pela lógica de negócios da aplicação. Ela atua entre o **Controller** e o **Repository**, manipulando os dados de maneira mais abstrata, sem expor diretamente a implementação dos dados. No caso do sistema de gerenciamento de usuários, a camada de serviço irá lidar com o registro, login, recuperação, atualização e exclusão de usuários.

A seguir, vou criar o serviço UserService para o gerenciamento de usuários. Ele irá usar o repositório UserRepository para persistência dos dados no banco de dados.

**UserService.java**

java

Copiar código

package com.exemplo.usermanagement.service;

import com.exemplo.usermanagement.dto.UserDTO;

import com.exemplo.usermanagement.model.User;

import com.exemplo.usermanagement.repository.UserRepository;

import com.exemplo.usermanagement.security.JwtTokenUtil;

import org.springframework.beans.factory.annotation.Autowired;

import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;

import org.springframework.stereotype.Service;

import java.util.List;

import java.util.Optional;

@Service

public class UserService {

@Autowired

private UserRepository userRepository;

@Autowired

private JwtTokenUtil jwtTokenUtil;

@Autowired

private BCryptPasswordEncoder passwordEncoder;

// Registrar um novo usuário

public User registerUser(UserDTO userDTO) {

// Verifica se o nome de usuário ou e-mail já existem no banco de dados

if (userRepository.existsByUsername(userDTO.getUsername())) {

throw new RuntimeException("Username is already taken");

}

if (userRepository.existsByEmail(userDTO.getEmail())) {

throw new RuntimeException("Email is already taken");

}

// Criação de um novo usuário

User newUser = new User();

newUser.setUsername(userDTO.getUsername());

newUser.setEmail(userDTO.getEmail());

newUser.setPassword(passwordEncoder.encode(userDTO.getPassword())); // Senha criptografada

newUser.setRole(userDTO.getRole());

return userRepository.save(newUser);

}

// Login de um usuário - gera um token JWT

public String loginUser(UserDTO userDTO) {

User user = userRepository.findByUsername(userDTO.getUsername())

.orElseThrow(() -> new RuntimeException("User not found"));

// Verifica se a senha fornecida é válida

if (!passwordEncoder.matches(userDTO.getPassword(), user.getPassword())) {

throw new RuntimeException("Invalid password");

}

// Gerar o token JWT

return jwtTokenUtil.generateToken(userDTO.getUsername());

}

// Recuperar um usuário pelo nome de usuário

public User getUserByUsername(String username) {

return userRepository.findByUsername(username)

.orElseThrow(() -> new RuntimeException("User not found"));

}

// Atualizar um usuário

public User updateUser(String id, UserDTO userDTO) {

User user = userRepository.findById(id)

.orElseThrow(() -> new RuntimeException("User not found"));

user.setUsername(userDTO.getUsername());

user.setEmail(userDTO.getEmail());

user.setPassword(passwordEncoder.encode(userDTO.getPassword())); // Senha criptografada

user.setRole(userDTO.getRole());

return userRepository.save(user);

}

// Deletar um usuário

public void deleteUser(String id) {

User user = userRepository.findById(id)

.orElseThrow(() -> new RuntimeException("User not found"));

userRepository.delete(user);

}

// Listar todos os usuários (admin)

public List<User> getAllUsers() {

return userRepository.findAll();

}

}

**Explicação do UserService:**

1. **Injeção de dependências**:
   * **UserRepository**: O repositório para acesso ao banco de dados e manipulação de dados de usuários.
   * **JwtTokenUtil**: Utilitário para gerar tokens JWT.
   * **BCryptPasswordEncoder**: Usado para criptografar e comparar senhas.
2. **Métodos**:
   * **registerUser(UserDTO userDTO)**: Cria um novo usuário. Verifica se o nome de usuário ou o e-mail já existem no banco e, caso contrário, salva o novo usuário com a senha criptografada.
   * **loginUser(UserDTO userDTO)**: Autentica um usuário e gera um token JWT para acesso à API.
   * **getUserByUsername(String username)**: Recupera um usuário com base no nome de usuário.
   * **updateUser(String id, UserDTO userDTO)**: Atualiza os dados de um usuário. A senha é criptografada novamente.
   * **deleteUser(String id)**: Deleta um usuário do banco de dados.
   * **getAllUsers()**: Lista todos os usuários (somente acessível a administradores).

**Como isso se integra ao seu sistema:**

1. **Controller**: O UserController chama esses métodos para manipular as requisições dos usuários.
2. **Repository**: O UserRepository é responsável pela persistência de dados no banco.
3. **Segurança**: O JwtTokenUtil é usado no serviço para gerar e validar tokens JWT, garantindo que os usuários possam autenticar-se e acessar suas informações de forma segura.

**Testes**

Além disso, o UserService pode ser testado com uma camada de testes automatizados, utilizando o **Spring Boot Test** para garantir que a lógica de negócios esteja funcionando corretamente.

**Conclusão**

Agora, com o UserService, temos a camada de serviço que centraliza toda a lógica de negócios para gerenciamento de usuários, permitindo registro, login, atualização e exclusão de usuários, tudo de forma segura e organizada.

A camada de segurança é essencial para proteger a aplicação contra acessos não autorizados e ataques. Em um sistema Spring Boot, a segurança é implementada usando o Spring Security. No caso deste projeto, configuraremos autenticação baseada em JWT (JSON Web Tokens).

**Estrutura da Segurança**

1. **JwtTokenUtil**: Classe para gerar e validar tokens JWT.
2. **SecurityConfig**: Configuração do Spring Security.
3. **JwtAuthenticationFilter**: Filtro para interceptar requisições e verificar o token JWT.
4. **Autenticação baseada em AuthenticationManager**.

**1. JwtTokenUtil.java**

Esta classe é usada para gerar e validar os tokens JWT.

java

Copiar código

package com.exemplo.usermanagement.security;

import io.jsonwebtoken.\*;

import org.springframework.beans.factory.annotation.Value;

import org.springframework.security.core.Authentication;

import org.springframework.stereotype.Component;

import java.util.Date;

@Component

public class JwtTokenUtil {

@Value("${jwt.secret}")

private String jwtSecret;

@Value("${jwt.expiration}")

private long jwtExpirationMs;

// Gera um token JWT

public String generateToken(Authentication authentication) {

String username = authentication.getName();

return Jwts.builder()

.setSubject(username)

.setIssuedAt(new Date())

.setExpiration(new Date((new Date()).getTime() + jwtExpirationMs))

.signWith(SignatureAlgorithm.HS512, jwtSecret)

.compact();

}

// Recupera o nome de usuário do token JWT

public String getUsernameFromToken(String token) {

return Jwts.parser().setSigningKey(jwtSecret).parseClaimsJws(token).getBody().getSubject();

}

// Valida o token JWT

public boolean validateToken(String token) {

try {

Jwts.parser().setSigningKey(jwtSecret).parseClaimsJws(token);

return true;

} catch (ExpiredJwtException e) {

System.out.println("JWT Token expired");

} catch (MalformedJwtException e) {

System.out.println("Invalid JWT Token");

} catch (SignatureException e) {

System.out.println("Invalid JWT Signature");

} catch (IllegalArgumentException e) {

System.out.println("JWT Claims string is empty");

}

return false;

}

}

**2. SecurityConfig.java**

Configuração principal do Spring Security.

java

Copiar código

package com.exemplo.usermanagement.security;

import org.springframework.context.annotation.Bean;

import org.springframework.context.annotation.Configuration;

import org.springframework.security.authentication.AuthenticationManager;

import org.springframework.security.config.annotation.authentication.builders.AuthenticationManagerBuilder;

import org.springframework.security.config.annotation.web.builders.HttpSecurity;

import org.springframework.security.config.annotation.web.configuration.EnableWebSecurity;

import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;

import org.springframework.security.crypto.password.PasswordEncoder;

import org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter;

@Configuration

@EnableWebSecurity

public class SecurityConfig extends org.springframework.security.config.annotation.web.configuration.WebSecurityConfigurerAdapter {

private final JwtAuthenticationFilter jwtAuthenticationFilter;

public SecurityConfig(JwtAuthenticationFilter jwtAuthenticationFilter) {

this.jwtAuthenticationFilter = jwtAuthenticationFilter;

}

@Bean

@Override

public AuthenticationManager authenticationManagerBean() throws Exception {

return super.authenticationManagerBean();

}

@Bean

public PasswordEncoder passwordEncoder() {

return new BCryptPasswordEncoder();

}

@Override

protected void configure(HttpSecurity http) throws Exception {

http.csrf().disable()

.authorizeRequests()

.antMatchers("/api/v1/users/register", "/api/v1/users/login").permitAll()

.anyRequest().authenticated()

.and()

.addFilterBefore(jwtAuthenticationFilter, UsernamePasswordAuthenticationFilter.class);

}

}

**3. JwtAuthenticationFilter.java**

Filtro para interceptar requisições e validar o token JWT.

java

Copiar código

package com.exemplo.usermanagement.security;

import org.springframework.beans.factory.annotation.Autowired;

import org.springframework.security.core.context.SecurityContextHolder;

import org.springframework.security.core.userdetails.UserDetails;

import org.springframework.security.core.userdetails.UserDetailsService;

import org.springframework.security.web.authentication.WebAuthenticationDetailsSource;

import org.springframework.stereotype.Component;

import org.springframework.web.filter.OncePerRequestFilter;

import javax.servlet.FilterChain;

import javax.servlet.ServletException;

import javax.servlet.http.HttpServletRequest;

import javax.servlet.http.HttpServletResponse;

import java.io.IOException;

@Component

public class JwtAuthenticationFilter extends OncePerRequestFilter {

@Autowired

private JwtTokenUtil jwtTokenUtil;

@Autowired

private UserDetailsService userDetailsService;

@Override

protected void doFilterInternal(HttpServletRequest request, HttpServletResponse response, FilterChain filterChain)

throws ServletException, IOException {

String token = jwtTokenUtil.getTokenFromRequest(request);

if (token != null && jwtTokenUtil.validateToken(token)) {

String username = jwtTokenUtil.getUsernameFromToken(token);

UserDetails userDetails = userDetailsService.loadUserByUsername(username);

if (userDetails != null) {

UsernamePasswordAuthenticationToken authentication = new UsernamePasswordAuthenticationToken(

userDetails, null, userDetails.getAuthorities());

authentication.setDetails(new WebAuthenticationDetailsSource().buildDetails(request));

SecurityContextHolder.getContext().setAuthentication(authentication);

}

}

filterChain.doFilter(request, response);

}

}

**4. Configurações no application.properties**

Adicione as configurações de JWT no arquivo application.properties:

properties

Copiar código

jwt.secret=your\_secret\_key

jwt.expiration=86400000 # 24 horas em milissegundos

**5. Customização de UserDetailsService**

Implemente o UserDetailsService para carregar usuários do banco:

java

Copiar código

package com.exemplo.usermanagement.security;

import com.exemplo.usermanagement.model.User;

import com.exemplo.usermanagement.repository.UserRepository;

import org.springframework.beans.factory.annotation.Autowired;

import org.springframework.security.core.userdetails.UserDetails;

import org.springframework.security.core.userdetails.UsernameNotFoundException;

import org.springframework.stereotype.Service;

@Service

public class CustomUserDetailsService implements UserDetailsService {

@Autowired

private UserRepository userRepository;

@Override

public UserDetails loadUserByUsername(String username) throws UsernameNotFoundException {

User user = userRepository.findByUsername(username)

.orElseThrow(() -> new UsernameNotFoundException("User not found with username: " + username));

return org.springframework.security.core.userdetails.User.builder()

.username(user.getUsername())

.password(user.getPassword())

.roles(user.getRole())

.build();

}

}

**Resultado**

1. **Rotas públicas**:
   * POST /api/v1/users/register: Registro de novos usuários.
   * POST /api/v1/users/login: Login e geração de token JWT.
2. **Rotas protegidas**:
   * Requisições a outros endpoints exigem um token JWT válido no cabeçalho Authorization: Bearer <TOKEN>.
3. **Segurança**:
   * Todas as senhas são hashadas.
   * Tokens JWT garantem autenticação sem estado.

4o

**Dito por si:**

onde fica e pra que serve? UserDetailsService

**Dito pelo ChatGPT:**

ChatGPT

**Onde fica o UserDetailsService?**

O UserDetailsService é uma interface fornecida pelo Spring Security e geralmente implementada por uma classe customizada na sua aplicação. Ele está localizado no pacote:

java

Copiar código

org.springframework.security.core.userdetails.UserDetailsService

Você pode criar sua própria implementação para carregar os detalhes do usuário a partir de uma fonte de dados personalizada, como um banco de dados.

**Pra que serve o UserDetailsService?**

O UserDetailsService é usado para:

1. **Carregar informações do usuário**: Ele carrega um objeto de usuário (UserDetails) com base em um identificador, como o nome de usuário (username).
2. **Autenticação**: É utilizado pelo Spring Security para autenticar os usuários durante o login. O serviço busca o usuário pelo nome de usuário fornecido, e o Spring compara as credenciais (nome e senha) para autenticação.
3. **Integração com o Spring Security**: Ele permite que o Spring Security interaja com a fonte de dados do usuário, abstraindo os detalhes do armazenamento (banco de dados, memória, etc.).

**Exemplo de implementação personalizada do UserDetailsService**

Aqui está um exemplo prático de como você pode usar o UserDetailsService para carregar usuários de um banco de dados:

**1. Implementação Customizada**

java

Copiar código

package com.exemplo.usermanagement.security;

import com.exemplo.usermanagement.model.User;

import com.exemplo.usermanagement.repository.UserRepository;

import org.springframework.beans.factory.annotation.Autowired;

import org.springframework.security.core.userdetails.UserDetails;

import org.springframework.security.core.userdetails.UserDetailsService;

import org.springframework.security.core.userdetails.UsernameNotFoundException;

import org.springframework.stereotype.Service;

@Service

public class CustomUserDetailsService implements UserDetailsService {

@Autowired

private UserRepository userRepository;

@Override

public UserDetails loadUserByUsername(String username) throws UsernameNotFoundException {

// Busca o usuário no banco de dados

User user = userRepository.findByUsername(username)

.orElseThrow(() -> new UsernameNotFoundException("User not found with username: " + username));

// Converte o usuário para um objeto UserDetails

return org.springframework.security.core.userdetails.User.builder()

.username(user.getUsername())

.password(user.getPassword()) // A senha deve estar hashada

.roles(user.getRole()) // Define os papéis do usuário

.build();

}

}

**2. Configuração no Spring Security**

No arquivo de configuração de segurança (SecurityConfig), você registra o CustomUserDetailsService:

java

Copiar código

package com.exemplo.usermanagement.security;

import org.springframework.context.annotation.Bean;

import org.springframework.context.annotation.Configuration;

import org.springframework.security.authentication.AuthenticationManager;

import org.springframework.security.config.annotation.authentication.builders.AuthenticationManagerBuilder;

import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;

import org.springframework.security.crypto.password.PasswordEncoder;

@Configuration

public class SecurityConfig {

private final CustomUserDetailsService customUserDetailsService;

public SecurityConfig(CustomUserDetailsService customUserDetailsService) {

this.customUserDetailsService = customUserDetailsService;

}

@Bean

public PasswordEncoder passwordEncoder() {

return new BCryptPasswordEncoder();

}

@Bean

public AuthenticationManager authenticationManager(AuthenticationManagerBuilder auth) throws Exception {

return auth

.userDetailsService(customUserDetailsService)

.passwordEncoder(passwordEncoder())

.and()

.build();

}

}

**Fluxo de funcionamento**

1. O usuário envia uma solicitação de login com o username e password.
2. O Spring Security chama o método loadUserByUsername da sua implementação de UserDetailsService.
3. O método busca os dados do usuário no banco de dados (ou outra fonte) e retorna um objeto UserDetails.
4. O Spring Security valida as credenciais fornecidas pelo usuário contra os dados retornados pelo UserDetails.
5. Se as credenciais forem válidas, o usuário é autenticado.

**Por que usar o UserDetailsService?**

* Ele abstrai a lógica de autenticação, permitindo integrar o Spring Security com diferentes fontes de dados.
* Facilita a implementação de segurança personalizada.
* Proporciona suporte a diferentes métodos de autenticação (banco de dados, memória, etc.).

**Benefício adicional**

Se no futuro você precisar alterar a forma como os dados dos usuários são carregados (por exemplo, de um banco relacional para um serviço externo), basta modificar o UserDetailsService sem impactar o restante da aplicação.