🔑

Spring Cloud Security + JWT

인증 서버와 Gateway 역할 분리

- JWT token 발행 → 인증 서버
- JWT parsing&validation → Gateway

인증 서버

- access & refresh token 발행
- logout blacklist 관리
- refresh token db 관리

Gateway

- 첫 token 발행 request를 받으면 인증 서버로 전달해 access & refresh token 받아 client로 전달
- client로부터 refresh token을 받으면 인증 서버에서 확인하고
  - 유효하면 새로운 access token을 발급받은 뒤 client에 전달
  - 유효하지 않으면 로그인 redirect

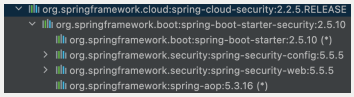
Spring Cloud security

✅ `@EnableWebSecurity` VS `@EnableWebFluxSecurity`

- `@EnableWebSecurity`

```
// jwt token 필터를 id,pw 인증 필터 전에 추가
.addFilterBefore(new JwtAuthenticationFilter(jwtTokenProvider), UsernamePasswordAuthenticationFilter.class);
```

- `@EnableWebFluxSecurity`




```
@EnableWebFluxSecurity
public class SecurityConfig {
    @Bean
    public SecurityWebFilterChain springSecurityFilterChain(ServerHttpSecurity http) {
        http
                .authorizeExchange()
                .anyExchange().authenticated()
                .and()
                .httpBasic().and().formLogin();
        return http.build();
    }
}
```

  - SecurityWebFilterChain을 Bean으로 등록해 ServerHttpSecurity 객체를 커스터마이징

✅ JWT token Flow

회원가입

1. access & refresh token 발급, SecurityContext 에 저장, redis 에 Token(username, refreshToken) 저장

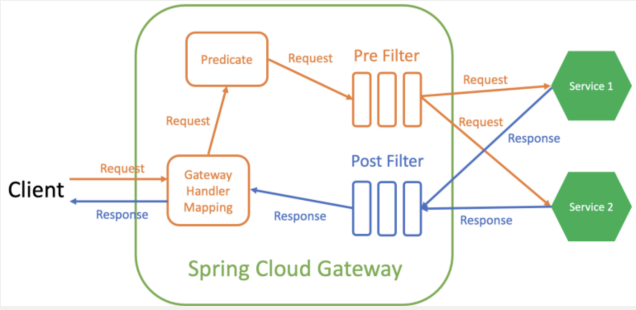
로그인

1. 로그인 진행
2. 로그인 성공 시 Access Token 및 Refresh 토큰 발행
3. Request Header의 Authentication Bear로 Access Token 전달
4. API Gateway에서 JWT 인증
    - Access Token validation 체크
    - Access Token 유효기간 체크
    - Role 체크
5. 해당 리소스에 접근

Access Token 갱신

1. client로부터 **refresh token**을 받으면 gateway에서 확인
    - 유효하면 새로운 access token을 발급받은 뒤 client에 전달
    - 유효하지 않으면 로그인 redirect

✅ **Gateway 인증 처리**



1. **로그인, 회원가입 요청은 module-api로 넘겨주기**
   a. module-api에서 access token과 refresh token 발급
      - access token: 30 minute, refresh token: 1 week
        - access token의 payload에 subject로 username을 담아 사용
        - refresh token은 redis에 key: email, value: Token(username, refreshToken) 형태로 저장

---

2. **그 이외 요청(/users/**, /managers/**)의 인증은 gw 담당**
   a. request header “Authorization” 체크
   b. access token 유효성 체크
      - access Token validation
      - access token 기한
      - role (해당 요청이 필요로 하는 권한이 요청을 보낸 유저에게 있는지)
3. **token 재발급 요청도 gw 담당**
   - https://wildeveloperetrain.tistory.com/59
   - Client가 refresh token과 만료된 access token을 갖고 재발급 요청 시,
     1. 만료된 token에서 username을 얻고
     2. redis에 username key값 확인
     3. refresh token 유효기간 & 변조 유무 확인
        - 통과 못하면 로그인 redirect