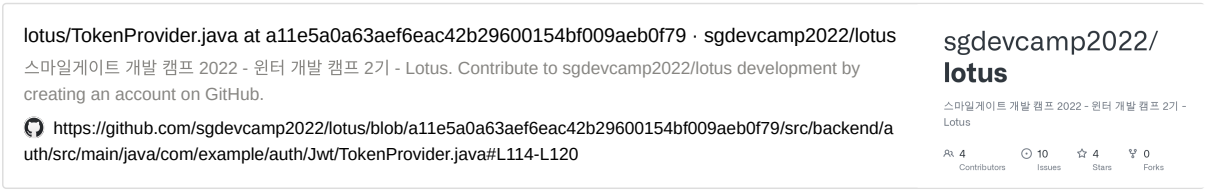
상우

인증서버

Access Token을 발급하는 코드



고민: SNS 이메일 중복

구현하는 SNS로그인이 네이버, 카카오, 구글이 있는데

카카오와 네이버에서 문제가 있었습니다.

저 같은 경우는 naver계정의 아이디와 카카오 계정의 아이디가 같습니다 ex) 네이버도 abcd@naver.com 카카오도 abcd@naver.com

여기서부터 많이 꼬이기 시작했는데 우선 sns로그인의 중복아이디 검사를 없앴고,

db에 Provider라는 컬럼을 추가해 sns 유형을 구분하고자 했습니다.

그런데 문제는 원래 토큰에 이메일에 대한 정보만 넣어서 보내주었는데

카카오때문에 구분이 안되는 바람에 이메일 말고 유저테이블의 pk값을 담아서 보내주었습니다

그러다보니 토큰에서 유저정보를 가져오는 것도 원래 email로 가져왔는데

user_id(pk)로 바꿔오는걸로 코드를 전부 고치게 되었는데 이 과정이 비효율적이었던 것 같습니다

기존에는 현재 로그인된 계정정보를 가져올때 spring security contextholder에서

UserDetails라는 객체에서 email을 가져와 email로 db에서 조회하는 방식이었는데,

지금은 access token을 받아서 access token에 담긴 user pk값을 가지고 db에서 조회하는 방식을 사용하여 시큐리티의 getcontext는 사용하지 않는 상태입니다.

시큐리티의 장점을 잘 활용하지 못하는가 고민이 듭니다

그래서 궁금한거는 sns가 다른데 이메일이 똑같은 저의 상황이 특별한 케이스인건지?

토큰에 db에 pk의 값을 넣어도 되는건지?

다른 sns지만 이메일이 같은 경우 구분을 어떻게 하는건지? 궁금합니다.

이메일을 pk로 정하면 안되는 이유

→ 이메일 바꿀 수도 있다, 정지가 된다, 이메일 계정 자체를 잃어버릴 수 있다

토큰에 pk를 넣어도되는가?

→ 보안에 위협이 되진 않다고 생각하지만, db를 짐작할 수 있다

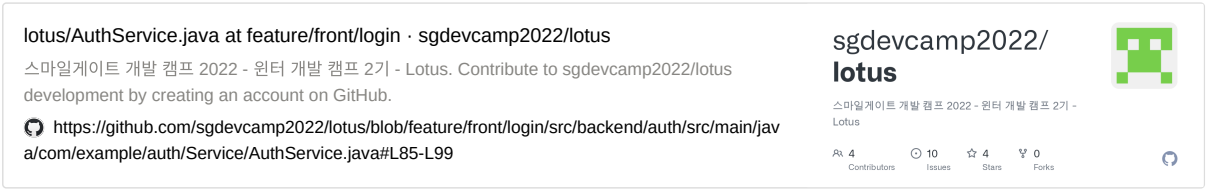
oauth 로그인에서 oauthid를 얻을 수 있다.

이런식으로 랜덤으로 생성된 문자열을 토큰에 넣어도 될 것 같다

provider를 구현하는 것은 좋다

sns 연동을 하면 밑에 표시를 해야할 수도 있다

로그인/로그아웃 로직



로그아웃기능은 accesstoken의 blacklist를 만들어서 하고있는데

대부분의 블로그에서 accesstoken을 redis에 저장할때

해당 유저의 refreshtoken을 삭제해줍니다
그러면 로그아웃->로그인 할때마다 항상 refreshtoken이 발급되는데
이 부분이 이해가 안됩니다
원래 refreshtoken은 accesstoken을 재발급할때 사용하는걸로 최초로그인시만 발급하고

안 발급 해주는걸로 생각을했는데

그러면 refreshtoken을 쓰는건 로그아웃안하고 창을 닫거나 혹은 로그아웃안하고 계속사용하다

액세스토큰이 만료될때만 쓰는건가요?
궁금한 부분은 로그아웃을 하면 refresh token 왜 삭제해야하는지 잘 모르겠습니다.

→ 로그아웃을 하면 refresh token이 버려진 정보이기때문에

남겨둘 이유가 없다

RedisHash의 @Indexed고민

---

lotus/RefreshToken.java at feature/front/login · sgdevcamp2022/lotus

스마일게이트 개발 캠프 2022 - 윈터 개발 캠프 2기 - Lotus. Contribute to sgdevcamp2022/lotus development by creating an account on GitHub.

https://github.com/sgdevcamp2022/lotus/blob/feature/front/login/src/backend/auth/src/main/java/com/example/auth/Entity/RefreshToken.java#L14-L34

redis에 refreshtoken을 저장할때 기존에는

@Indexed를 userId로만 설정했었습니다.
로그인할때 accesstoken으로부터 userId를 가져와
redis에 userID로 refreshtoken으로 조회해서 존재하면 refreshtoken을 재발급해주지않고,

존재하지 않으면 refreshtoken을 새로발급해주기 위해 userId에 Indexed를 사용했습니다

access token으로부터 userId정보를 가져와 redis에서 찾을 수 있었기 때문입니다.

그러나 accesstoken 재발급을 구현할때

accesstoken과 refreshtoken을 받는데, accesstoken은 만료됐기때문에

accesstoken으로부터 userId를 가져올 수 없다는걸 알게 되었고,

사용자로부터 받은 refreshtoken을 조회할 수 있는 방법이 없는 상황이 되었습니다.

고민하다가 refreshToken String값에도 @Indexed속성을 추가했는데,

@Indexed를 사용하면 redis에 저장되는 값이 하나 더 늘어나는 것을 알게되었습니다.

redis가 인메모리방식 db라 데이터가 많이쌓이면 효율적이지 않을 것 같은데
이렇게 사용해도 되는건지 궁금합니다

→redis에 필요한 정보만 담는 것은 중요하긴한데

이 자체로는 큰 데이터를 차지할 것 같지 않다

결국 jpa에서 활용하기때문에 고려하지 않아도 될 것 같습니다.

redis에 refreshtoken을 저장하는 것 자체가 비용을 포기하고 성능을 선택한 것이다.

인증서버&친구서버

lotus/UserController.java at feature/front/login · sgdevcamp2022/lotus

스마일게이트 개발 캠프 2022 - 윈터 개발 캠프 2기 - Lotus. Contribute to sgdevcamp2022/lotus development by creating an account on GitHub.

https://github.com/sgdevcamp2022/lotus/blob/feature/front/login/src/backend/auth/src/main/java/com/example/auth/Controller/UserController.java#L47-L60

유저테이블에서 회원가입을하면

친구서버에서 해당 pk에 맞는 친구테이블에 행이 하나 생기게 하고싶었습니다.

mysql에는 on delete나 on update는 있지만, on create기능은 없어서

처음엔 trigger를 설정해서 적용했는데요,

로컬에서 ec2환경으로 배포를 변경하면서

권한 문제가 발생해 현재는
인증서버에 친구테이블의 entity를 가지고,
회원가입하면 친구목록 행이 생기게 하고있습니다.
msa구조에서 한 서버가 다른 서버의 entity를 가지는 것이 msa에 위반되는 것 같은데요,
현업에서는 어떤 방식으로 이러한 기능을 구현하는지 궁금합니다.

Q. 인증서버에서 친구 api를 호출하는 방식을 고려해보았나?
A. 처음에 하려다가 편하게하려고 적용을안했다

→ 이런문제가 생기는 이유: 호출을하면 성능떨어지고 번거롭다
서버를 잘게 나누지말라는 이유가 이것 때문이다
가능하면 두 개의 서버를 합쳤어도 괜찮았을 것 같다
나누기 전에 나눌만한 이유가 보이지 않으면 나누지 않는 것이 Computer science의 1법칙이다
Optimizing은 나중에 하는 것을 추천드린다
