**Backend การตรวจสอบสิทธิ์**

ใช้การตรวจสอบสิทธิ์การเข้าใช้งานด้วย JSON Web Token (JWT) โดย Session Creation Policy จะเป็นแบบ stateless

ไลบรารี่ที่ใช้งาน คือ maven: com.auth0 / java-jwt / 3.18.1

[auth0/java-jwt: Java implementation of JSON Web Token (JWT) (github.com)](https://github.com/auth0/java-jwt)

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

ซึ่ง JWT ที่สร้างจะเก็บ

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. principal คือสิ่งไว้ระบุตัวตนผู้ใช้ โดยเก็บเป็น User Id ที่ไม่สามารถเปลี่ยนแปลงได้
2. role คือสิทธิ์ว่าผู้ใช้สามารถเข้าถึง Endpoint ได้ในระดับไหน
3. iss คือการบอกว่า JWT นี้ถูกสร้างมาจาก cfanBackend
4. exp คือวันหมดอายุของ JWT ซึ่งได้กำหนดไว้เป็น 24 ชม.

**ขั้นตอนการสร้าง JWT**

1. ตรวจสอบสิทธิ์การใช้งานของผู้ใช้ที่เข้าสู่ระบบ

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. สร้าง JWT จากข้อมูลของ User ที่ผ่านการยืนยันแล้ว

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. ส่งคืนข้อมูล JWT ที่สร้าง

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

**ขั้นตอนการตรวจสอบสิทธิ์การเข้าถึง**

1. ตรวจสอบว่า request ที่เข้ามามี Header “Authorization” และเริ่มต้นด้วย

“Bearer ” หรือไม่

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. ตรวจสอบว่า JWT ที่เข้ามาไม่ได้อยู่ใน jwtblacklist ซึ่งเก็บข้อมูลของ JWT ที่ได้ logout

ไปแล้ว

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. Verify JWT โดยจะตรวจสอบว่า JWT ถูกต้อง ไม่ได้ถูกแก้ไขและยังไม่หมดอายุ

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. นำข้อมูลที่ได้จาก JWT มาเก็บไว้ใน Context โดยเก็บ role เป็น authorities

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. User ที่มี authorities ถูกต้องจะสามารถเข้า Endpoint ได้ตามที่กำหนดไว้

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. ในทุก ๆ Endpoint ของ /user จะมีการดึงข้อมูล User จาก Id ใน Context มาตรวจสอบ

อีกครั้ง

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

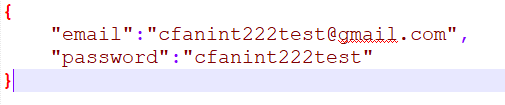
1. หากเป็น /Admin ก็จะมีการตรวจสอบว่า User มี Status Admin หรือไม่อีกครั้ง

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

**กรณีตัวอย่างการใช้งาน**

1. การเข้าสู่ระบบ



รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. การเรียกข้อมูล User คนนั้น ๆ

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

กรณีไม่ได้ส่ง Header

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. การออกจากระบบ

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

กรณี JWT ที่ส่งมาถูกใช้ออกจากระบบไปแล้ว

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

1. เมื่อ User จะเข้า Endpoint ที่ไม่มีสิทธิ์

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ

รูปภาพประกอบด้วย ข้อความ

คำอธิบายที่สร้างโดยอัตโนมัติ