جـامعة الحسن الثـاني بالدار البيضاء
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵍ ⵃⴰⵙⵏ ⵍⵙⵙⴰⵏⵉ ⵖⵙ ⵣ ⵜⵜⴰⵇⵎⴰⵟⵜ
UNIVERSITÉ HASSAN II DE CASABLANCA

Rapport
Examen Final

Lehcene MOHAMED
LEMINE

Sous la direction de monsieur

Dr. YOUSSFI Mohamed

ENSET
ECOLE NORMALE SUPÉRIEURE DE L'ENSEIGNEMENT
TECHNIQUE DE MOHAMMEDIA
UNIVERSITÉ HASSAN II DE CASABLANCA

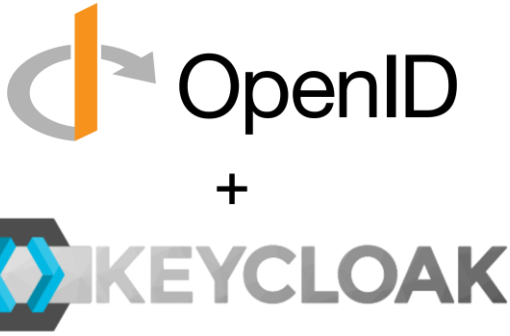
Année universitaire : 2023 – 2024

Master de Recherche SDIA

1-Introduction

Ce rapport décrit la conception et la mise en œuvre d'une application de gestion de ressources et de réservations basée sur les microservices. L'application est sécurisée avec Keycloak.

Les Technologies et les outils utilisés



2-Contexte général du projet

On souhaite créer une application basée sur une architecture micro-service qui permet de gérer des réservations concernant des ressources. Chaque réservation concerne une seule ressource. Une ressource est définie par son id, son nom, son type (MATERIEL_INF0, MATERIEL_AUDIO_VUSUEL). Une réservation est définie par son id, son nom, son contexte, sa date, sa durée. Chaque réservation est effectuée par une personne. Une personne est définie par son id, son nom, son email et sa fonction. L'application doit permettre de gérer les ressources et les réservations. Pour faire plus simple, cette application se composera de deux micro-services fonctionnels:

• Un Micro-service qui permet de gérer des « Resources-Service ».

• Un Micro-service qui permet de gérer les réservations effectuées par des personnes.

Les micro-services technique à mettre en place sont :

• Le service Gateway basé sur Spring cloud Gateway

• Le service Discovery base sur Eureka Server ou Consul Discovery (au choix)

• Le service de configuration basé sur Spring cloud config ou Consul Config (au choix)

Pour l'application, nous avons besoin de développer une frontend web, basé sur Angular Framework.

La sécurité de l'application est basée sur Oauth2 et OIDC avec Keycloak comme Provider

Pour les micro-services, il faut générer la documentation des web services Restfull en utilisant la spécification

OpenAPIDoc (Swagger). Prévoir aussi des circuit breakers basés sur Resilience4J comme solution de fault

tolerence

Travail de mandé :

Rendre un rapport PDF et le code source des projets au format zip, répondant aux questions suivantes

1. Établir une architecture technique du projet

2. Créer un Projet Maven incluant les micro-services suivants : resources-service, reservation-service,

gateway-service, discovery-service, config-service et angular-front-app

3. Développer et tester les micro-services discovery-service et gateway-service et config-service

4. Développer et tester le micro-service resources-service (Entities, DAO, service, DTO, Mapper,

RestController)

5. Développer et tester le micro-service reservation-service (Entities, DAO, service, DTO, Mapper,

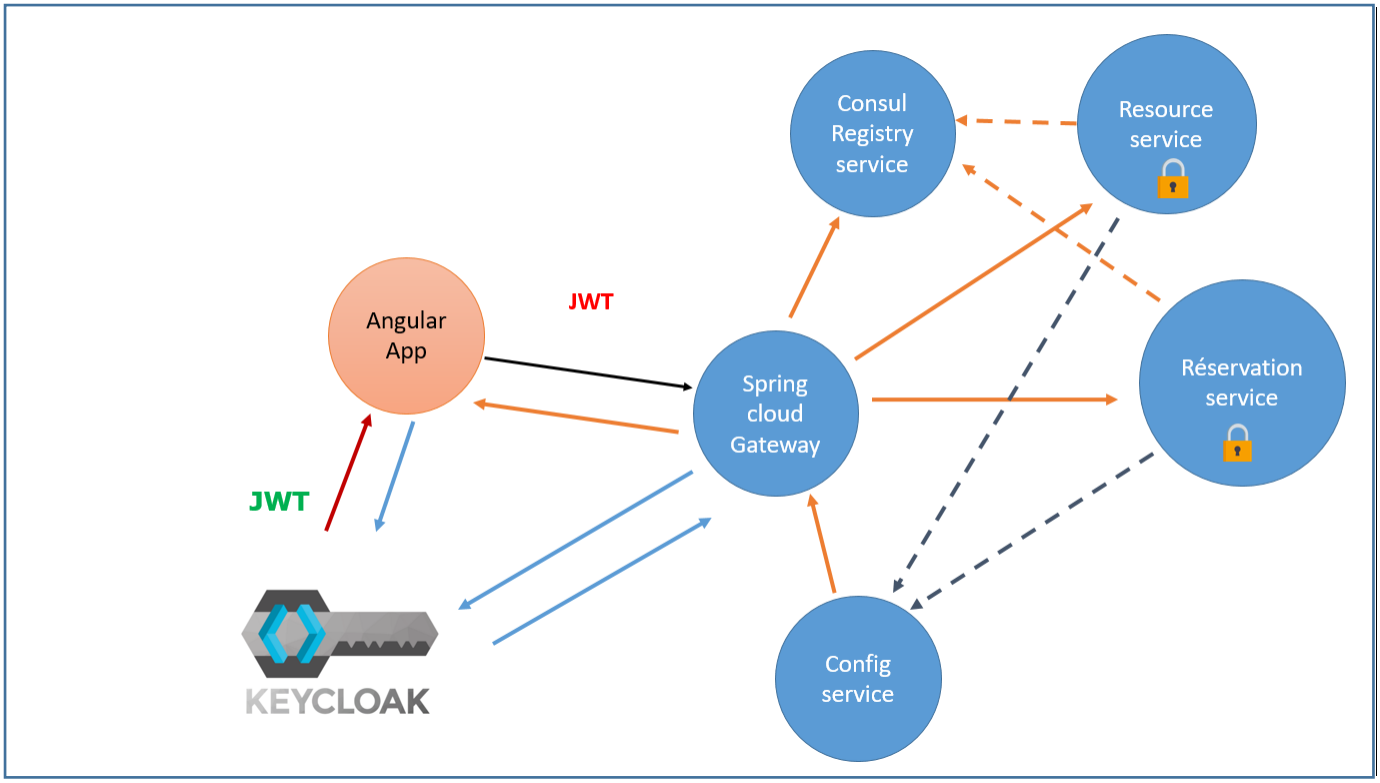
RestController, Client Rest Open Feign)

6. Développer un simple frontend web pour l'application

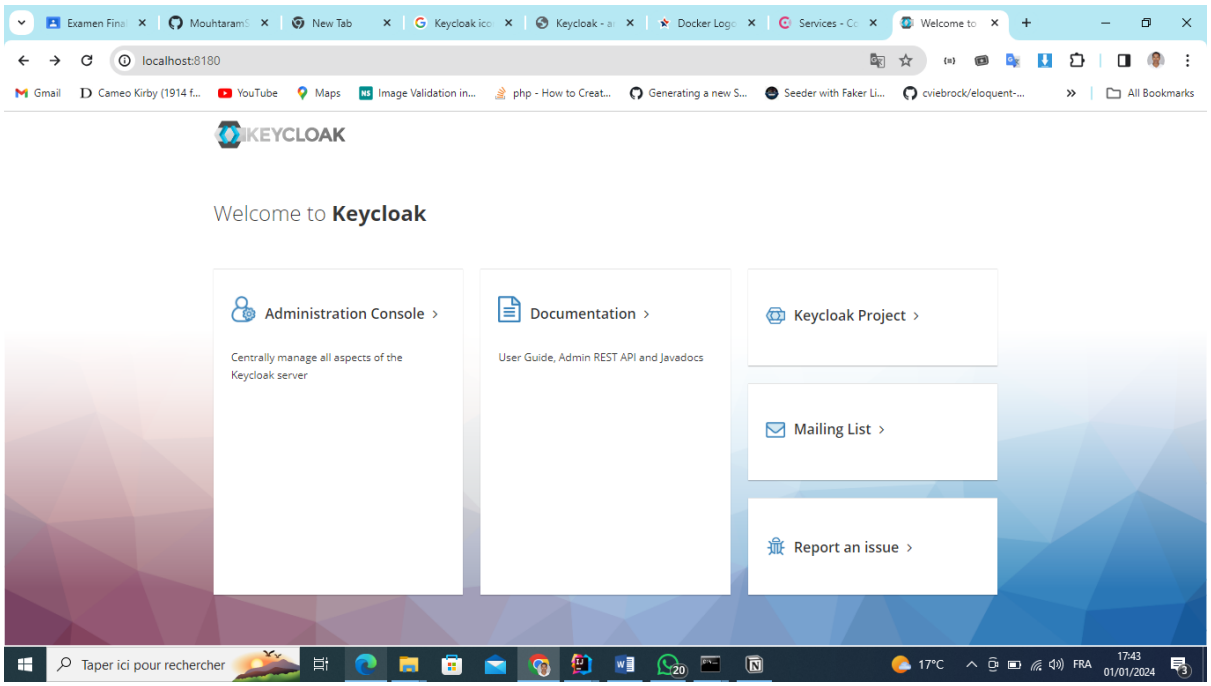
7. Sécuriser l'application avec une authentification Keycloak

8. Déployer l'application avec Docker et Docker compose

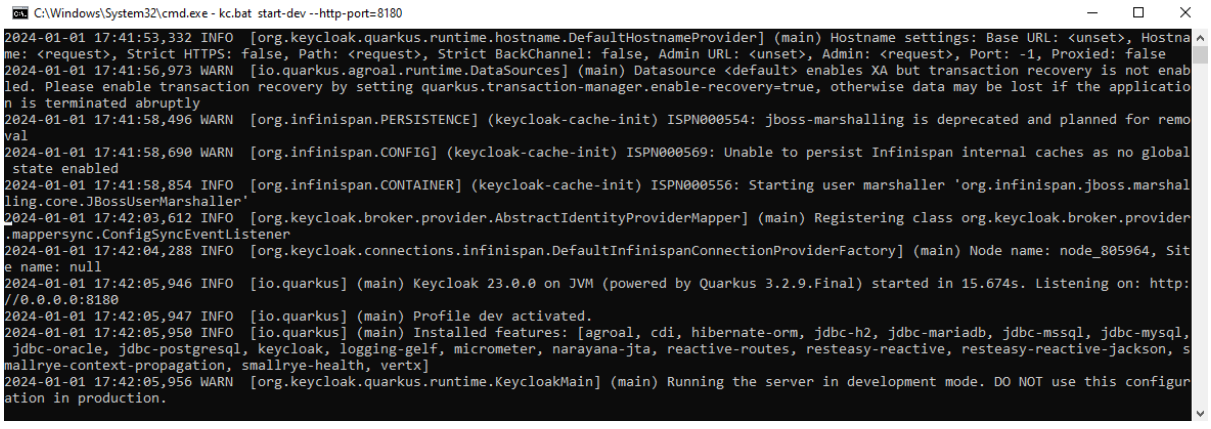
3-Architecture



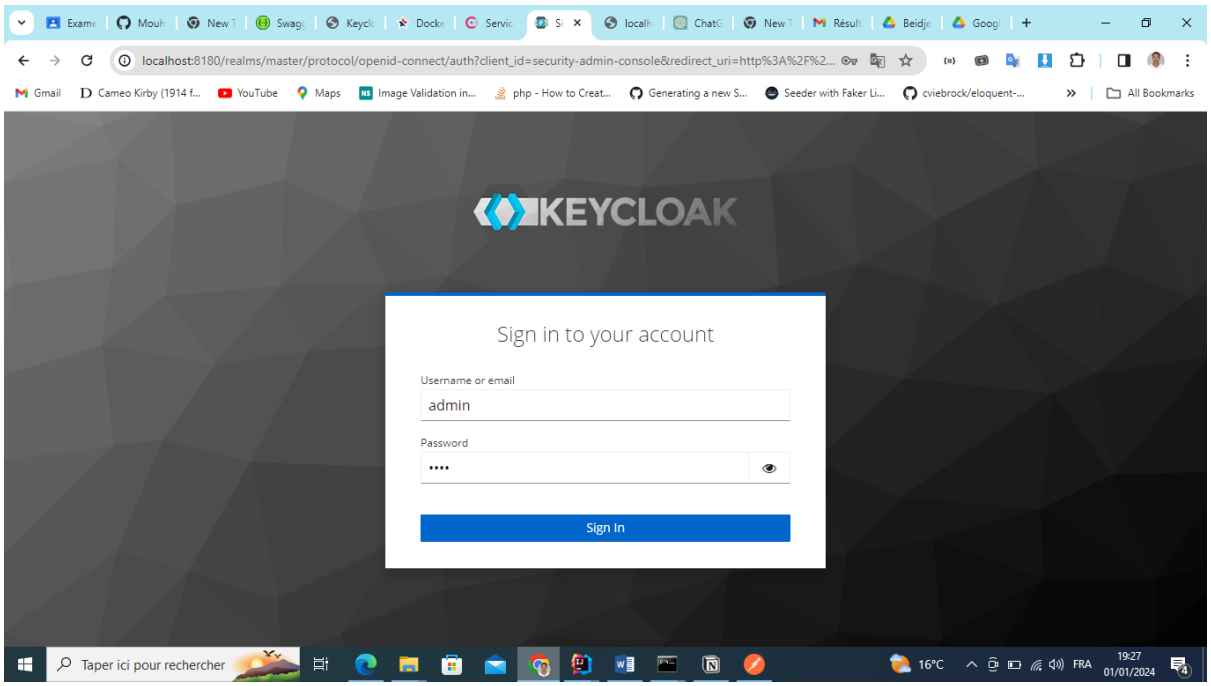
4-Keycloak



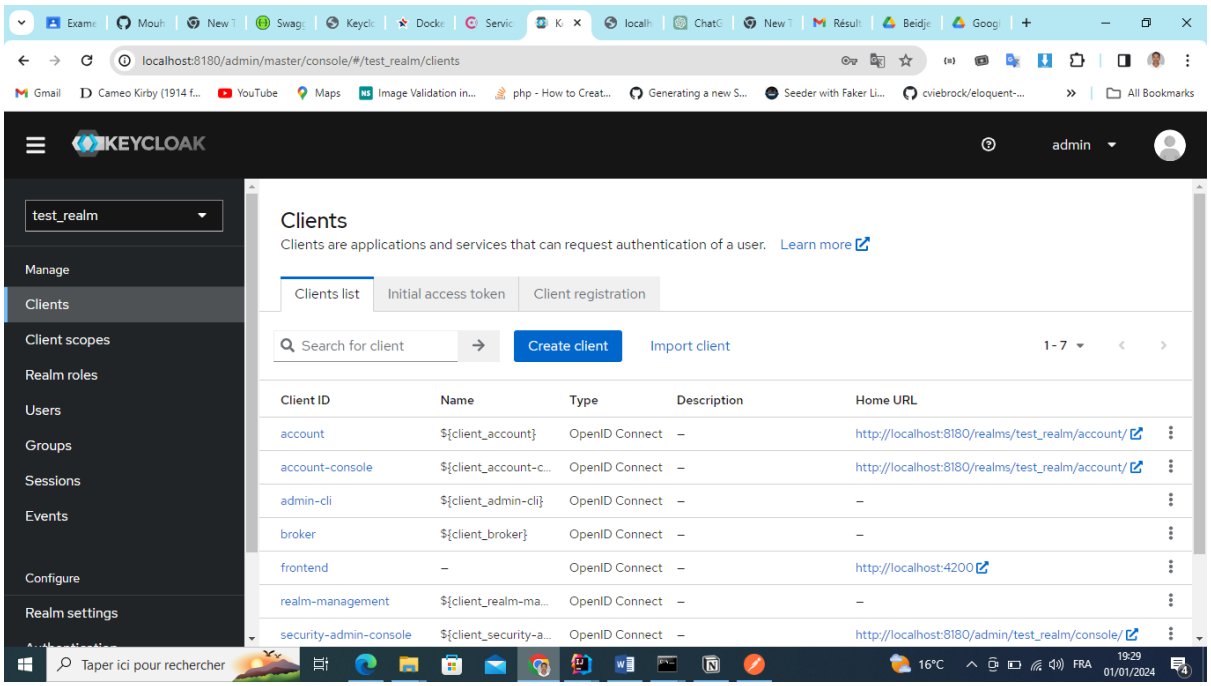
⇨ Interface de KEYCLOAK



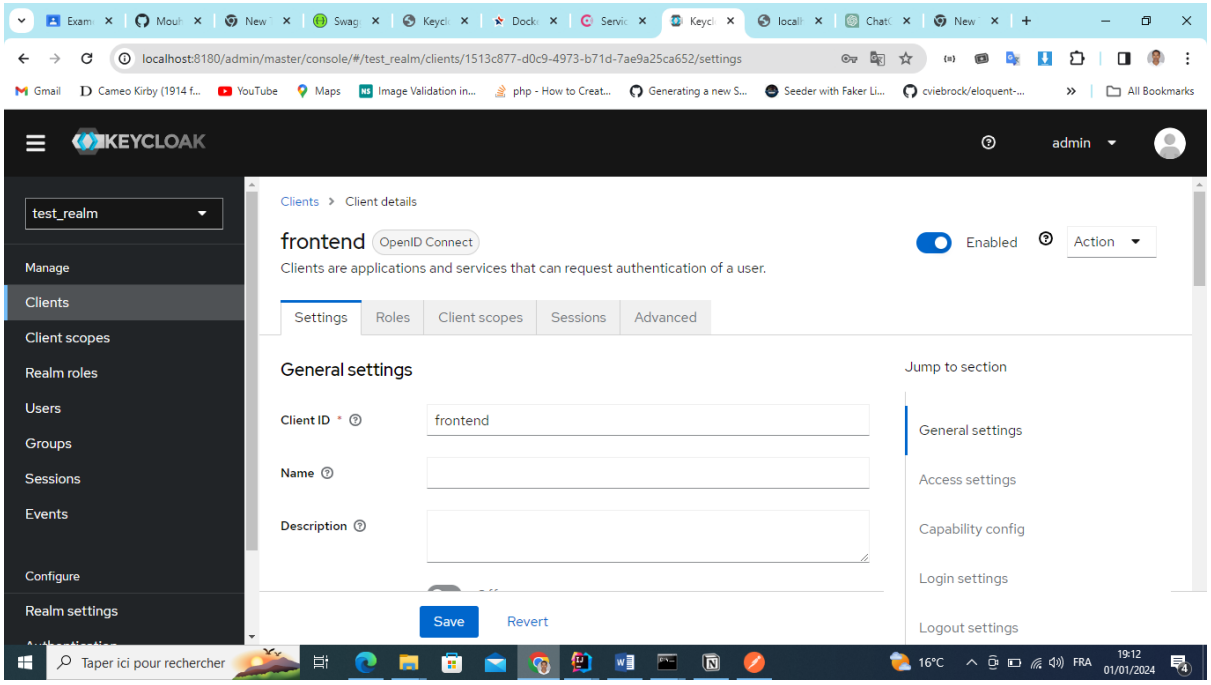
⇨ Voici je démarre KEYCLOAK avec ligne de commande sur port 8180

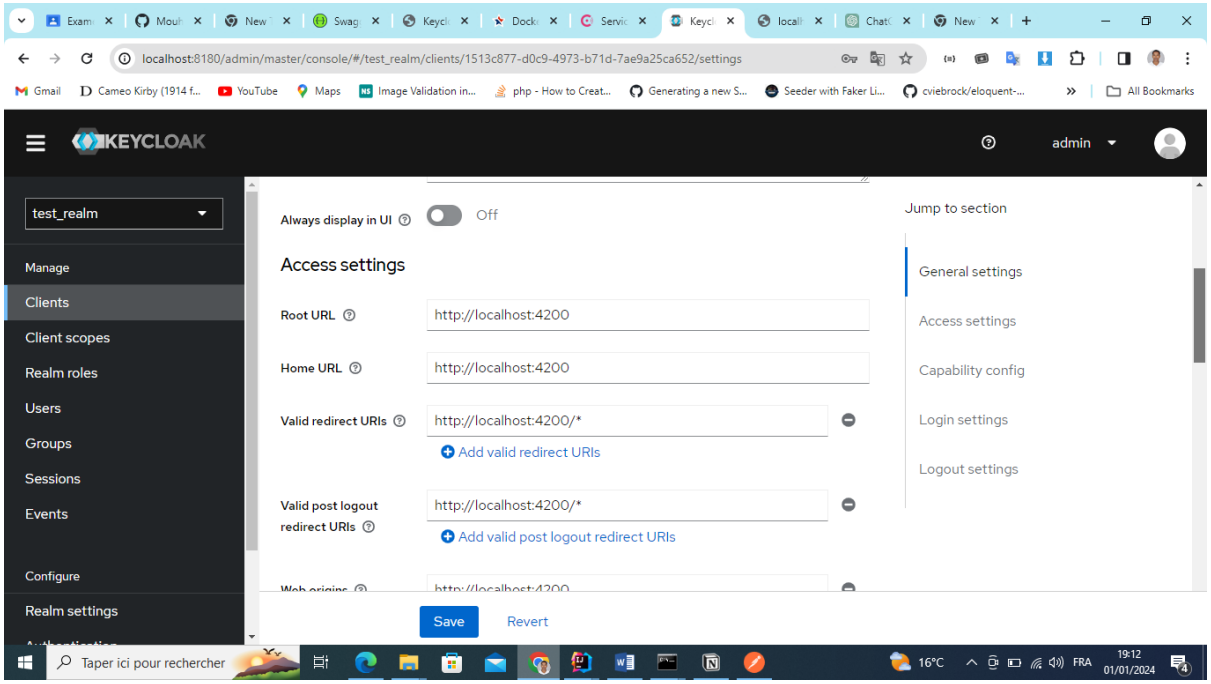


⇨ Connexion avec userName : admin & password : admin

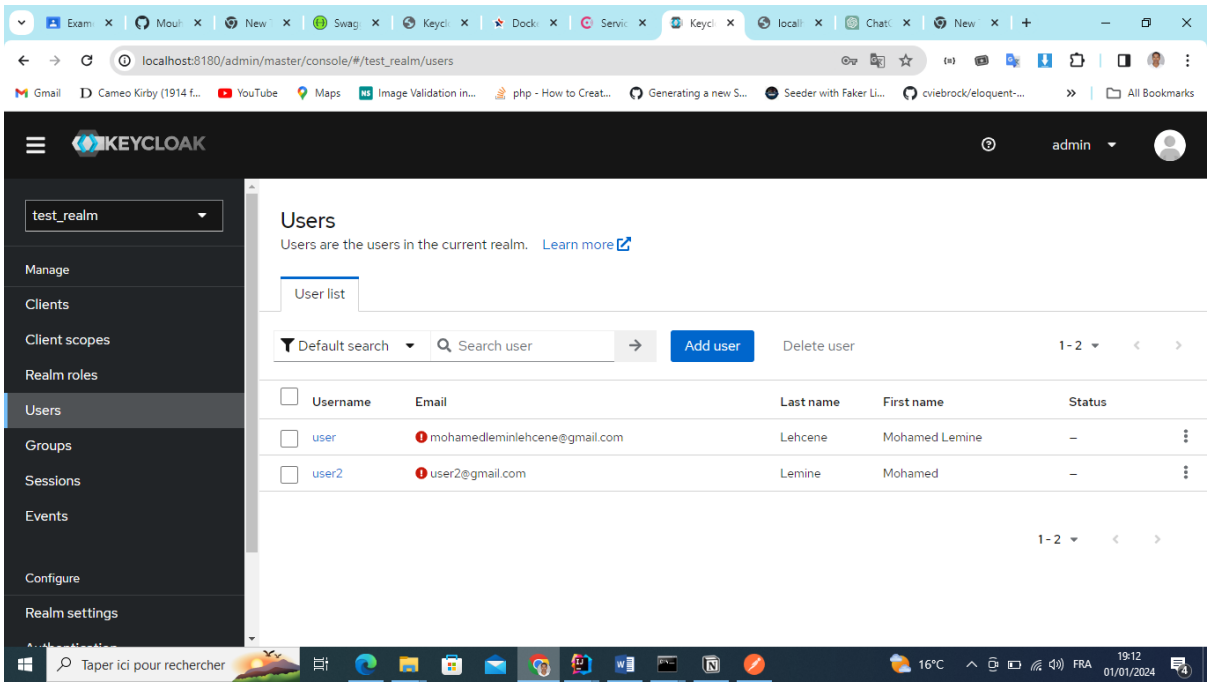


⇨ Authentification est réussie

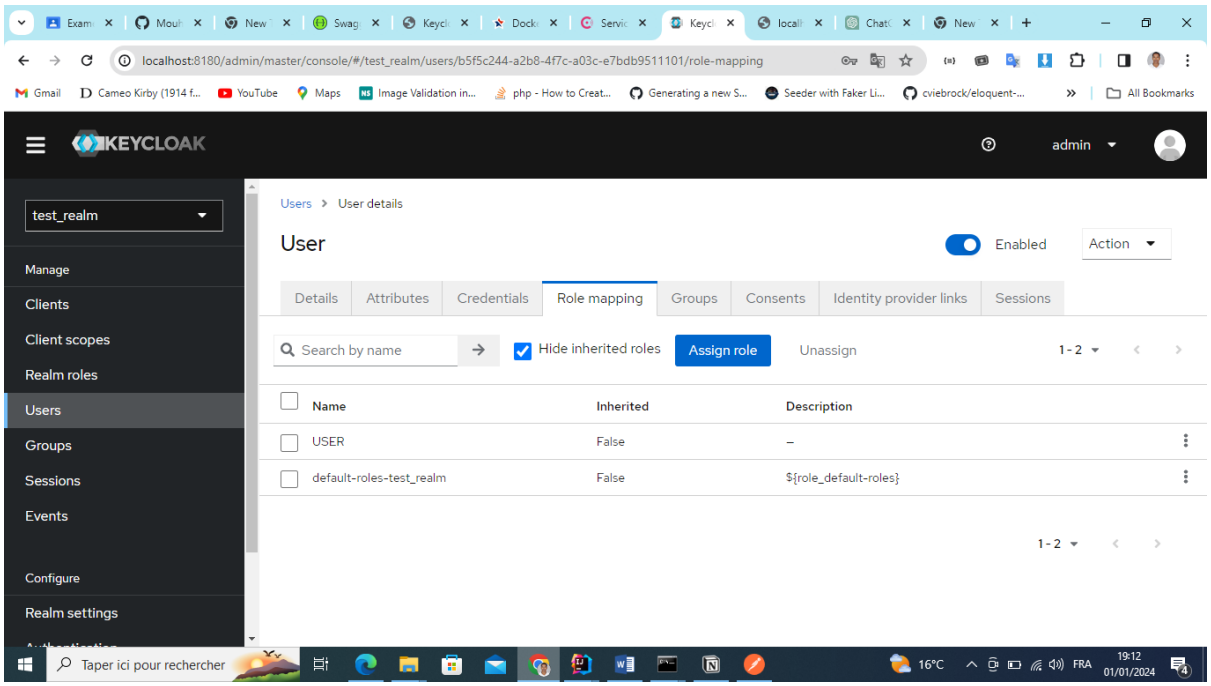




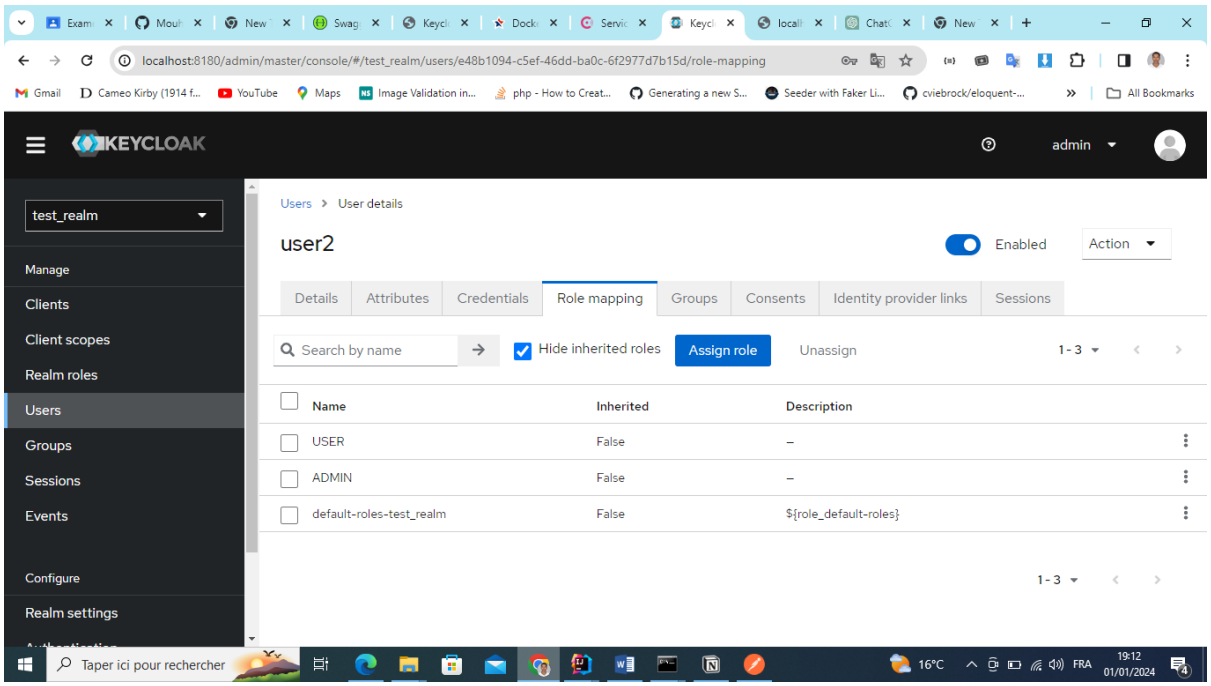
⇨ Voici je crée un client : frontend pour ANGULAR



⇨ Voici liste des utilisateurs

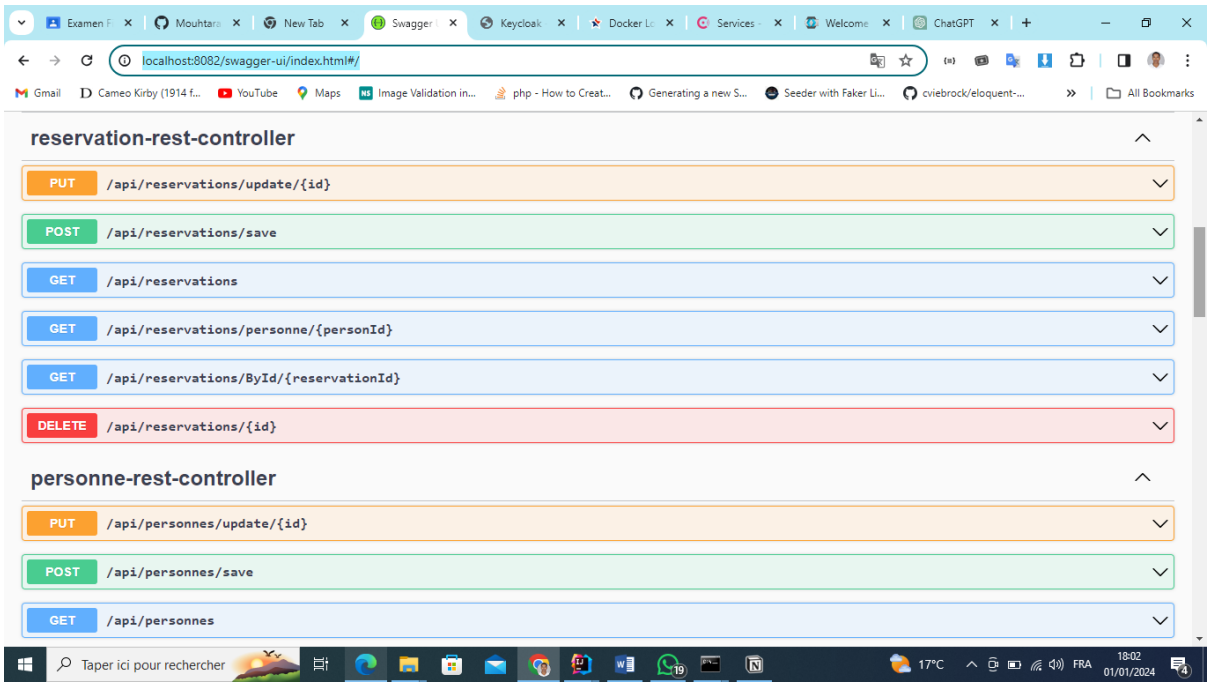


⇨ Utlisateur user avec role USER

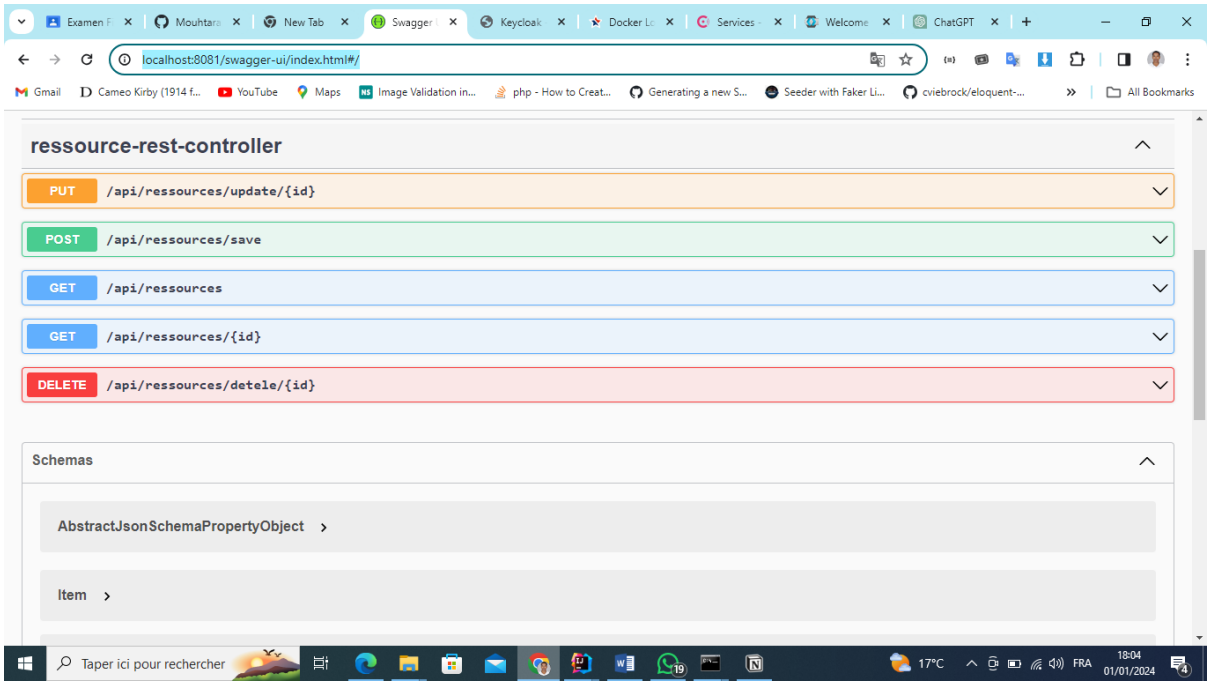


⇨ Utilisateur user2 avec roles : USER & ADMIN

5-SWAGGER

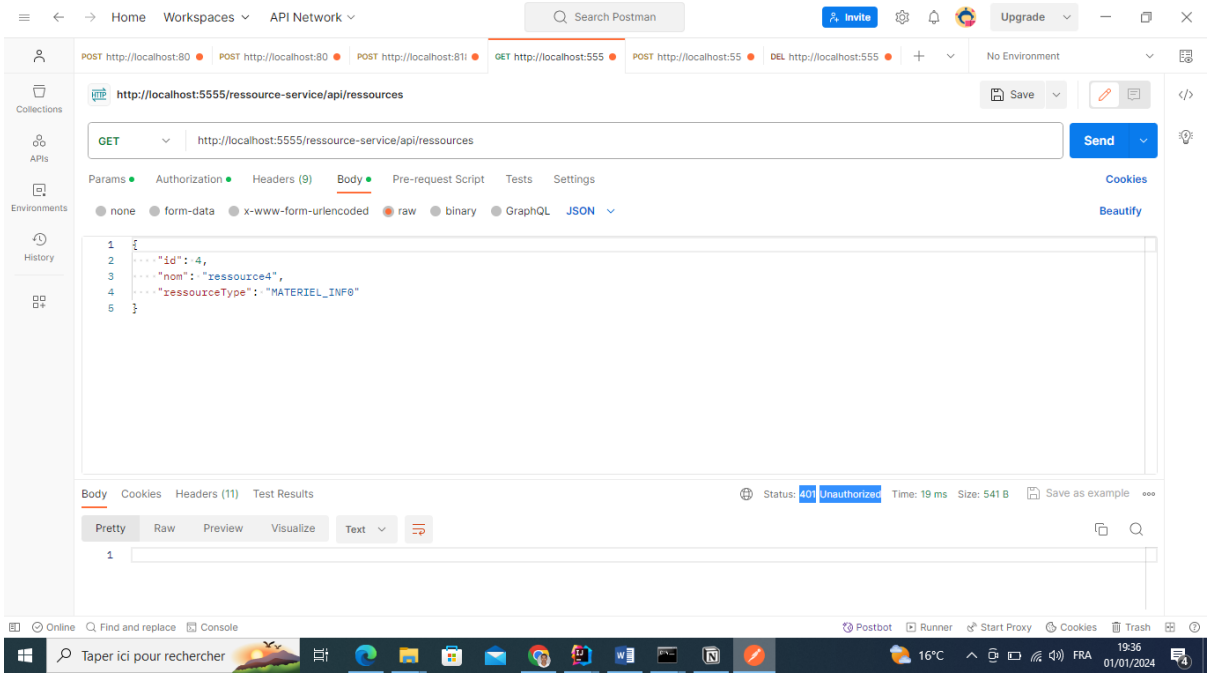


⇨ Voic je consulte interafce swagger pour micro service reservation sur port : 8082

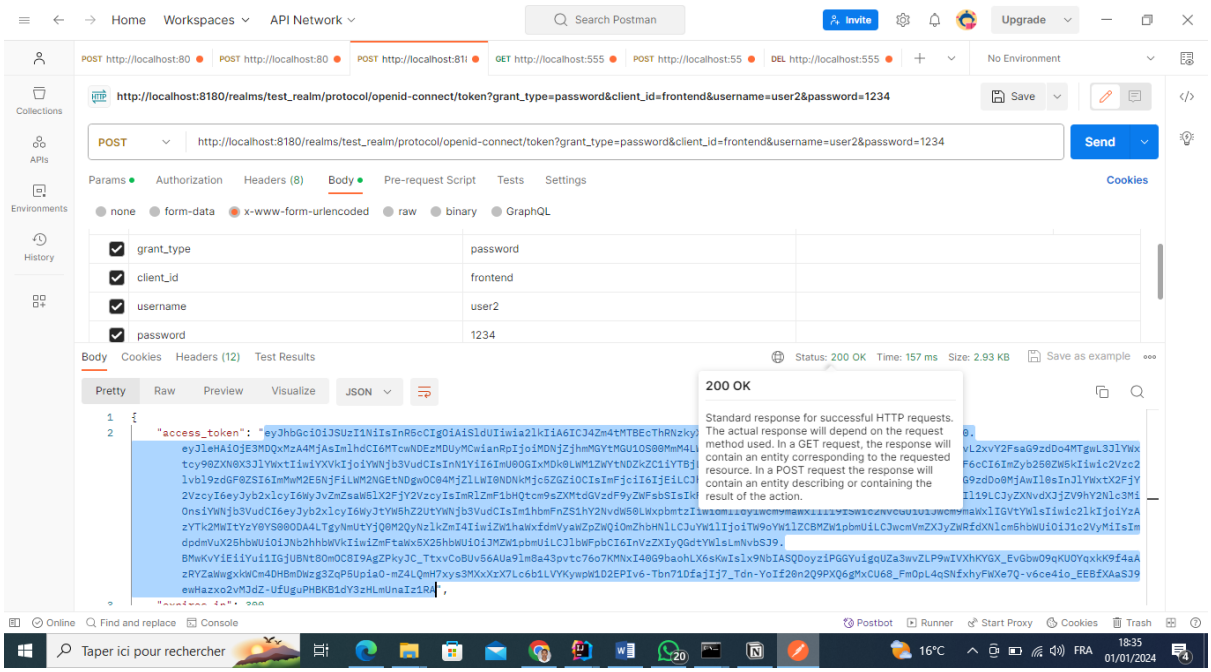


⇨ Voici j'ai consulté interface swagger pour micro service
⇨ ressource sur port : 8081

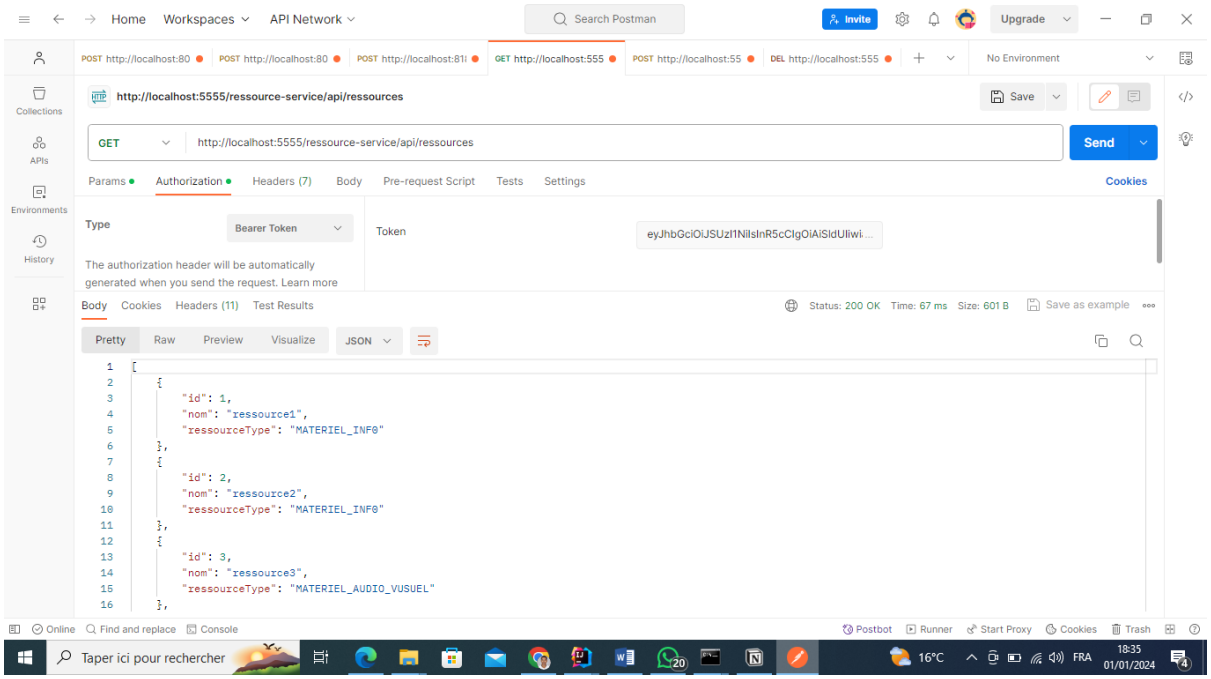
6-POSTMAN



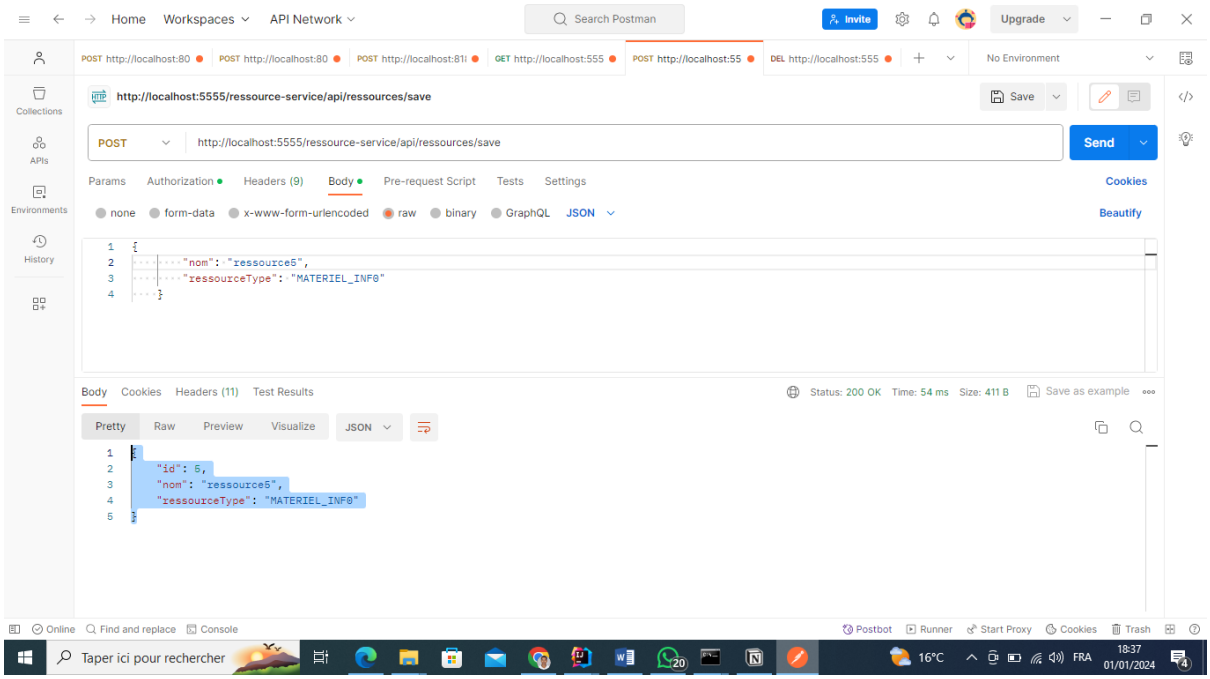
⇨ http://localhost:5555/ressource-service/api/ressources : pour afficher liste des ressources mais il m'envoie comme résultat 401 Unauthorized car je besoin d'authentifier et encore envoyer JWT TOKEN



⇨ Voici je fais une authentification avec POSTMAN sur KEYLCOAK pour obtenir JWT TOKEN

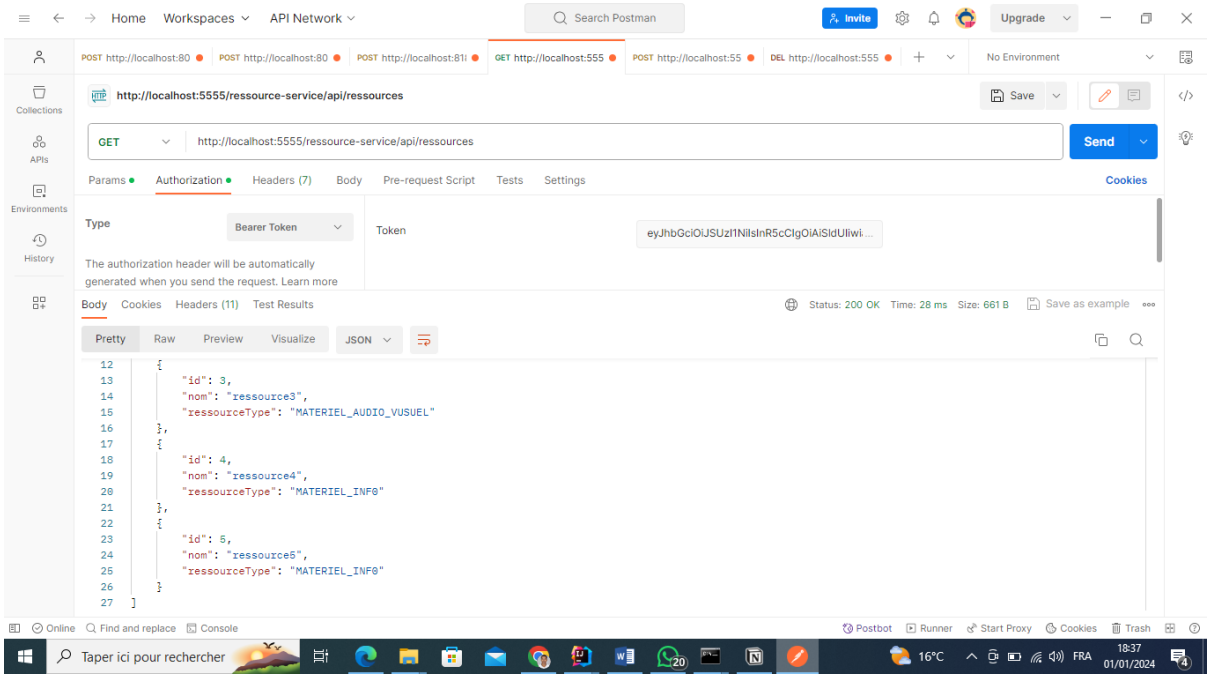


⇨ Voici-je affiche liste des ressources car j'envoie JWT TOKEN que j'obtiens par KEYCLOAK



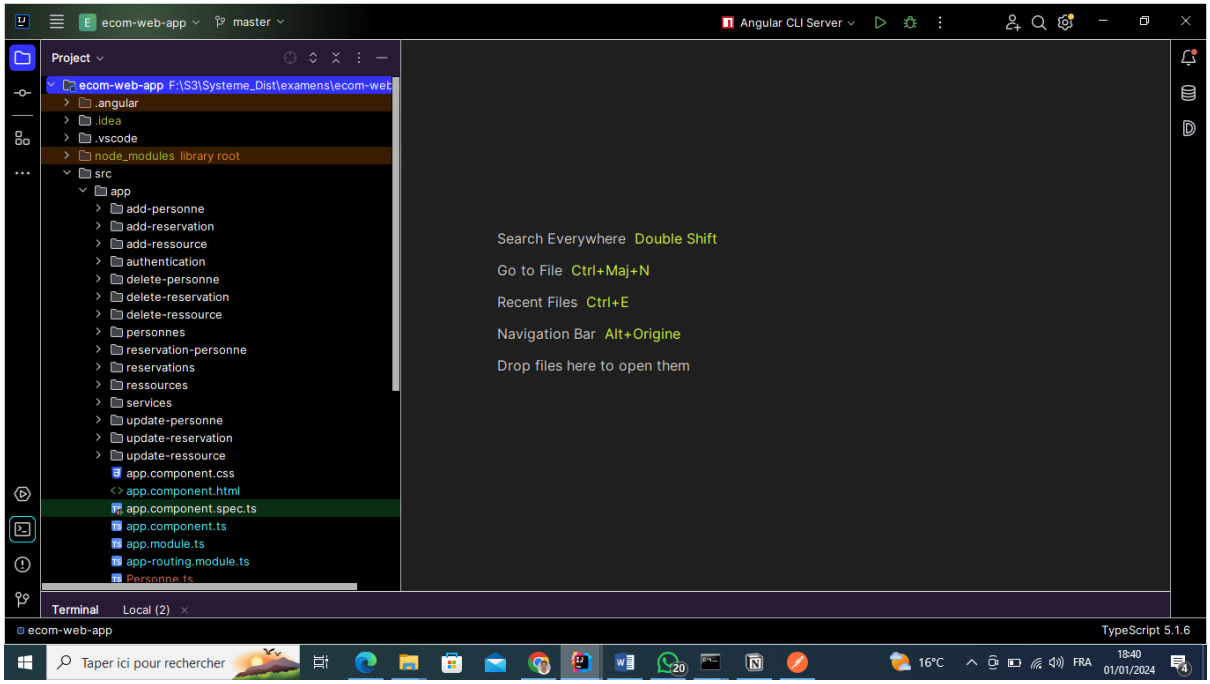
⇨

http://localhost:5555/ressource-service/api/ressources/save
pour une nouvelle ressource et encore j'envoie JWT TOKEN



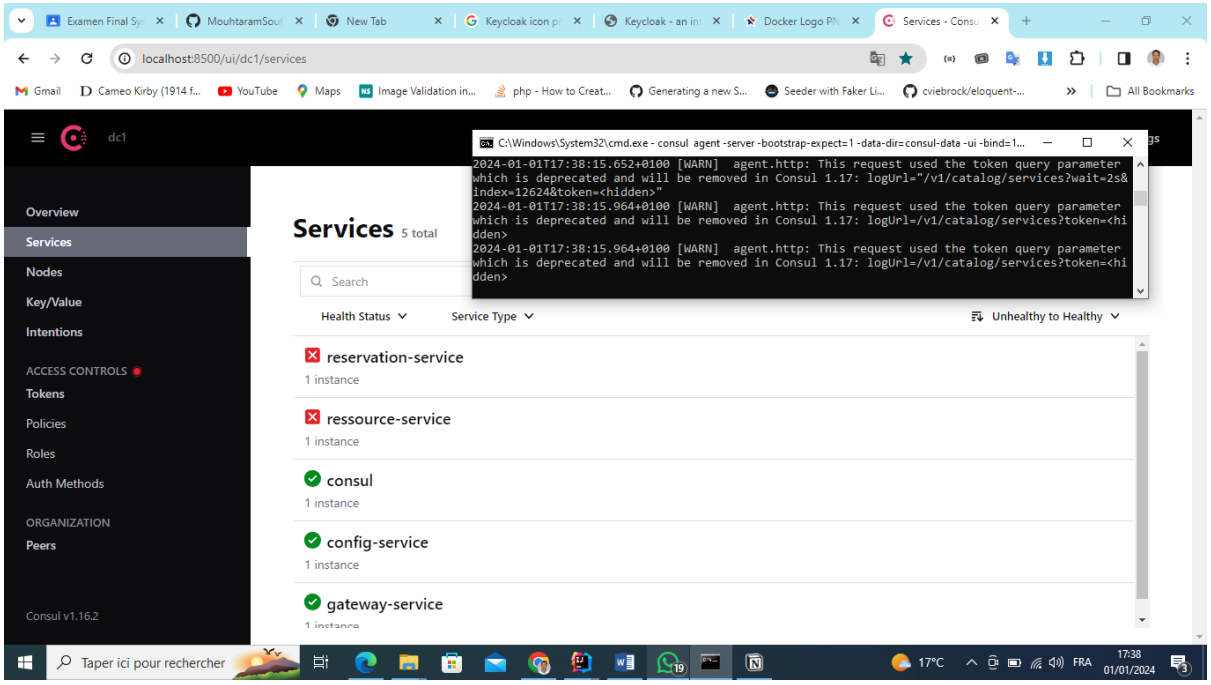
⇨ Voici l'ajoute du nouvelle ressource est réussi

7-Structure du projet ANGULAR



8-CONSUL DISCOVERY

Interface CONSUL qui contient l’ensemble des micros services qui enregistre sur eux



9-SECURITE DES MICROSERVICES

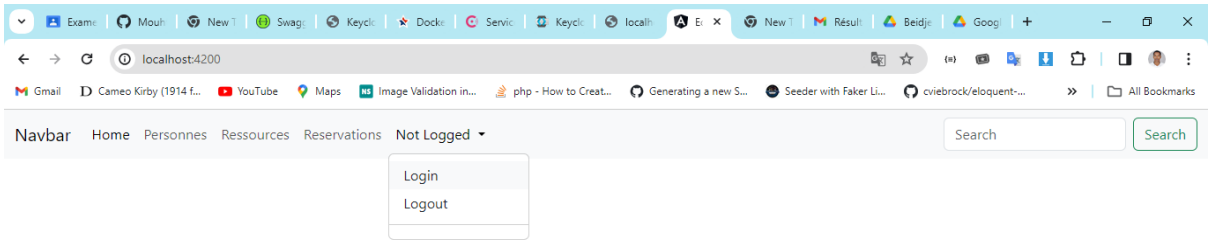
Classe JwtAuthConverter:

```
@Component
public class JwtAuthConverter implements Converter<Jwt,
AbstractAuthenticationToken> {
    private final JwtGrantedAuthoritiesConverter
jwtGrantedAuthoritiesConverter=new JwtGrantedAuthoritiesConverter();


    @Override
    public AbstractAuthenticationToken convert(Jwt jwt) {
        Collection<GrantedAuthority> authorities = Stream.concat(
                jwtGrantedAuthoritiesConverter.convert(jwt).stream(),
                extractResourceRoles(jwt).stream()
        ).collect(Collectors.toSet());
        return new JwtAuthenticationToken(jwt,
authorities,jwt.getClaim("preferred_username"));
    }

    private Collection<GrantedAuthority> extractResourceRoles(Jwt jwt) {
        Map<String , Object> realmAccess;
        Collection<String> roles;
        if(jwt.getClaim("realm_access")==null){
            return Set.of();
        }
        realmAccess = jwt.getClaim("realm_access");
        roles = (Collection<String>) realmAccess.get("roles");
        return roles.stream().map(role->new
SimpleGrantedAuthority(role)).collect(Collectors.toSet());
    }

}
```

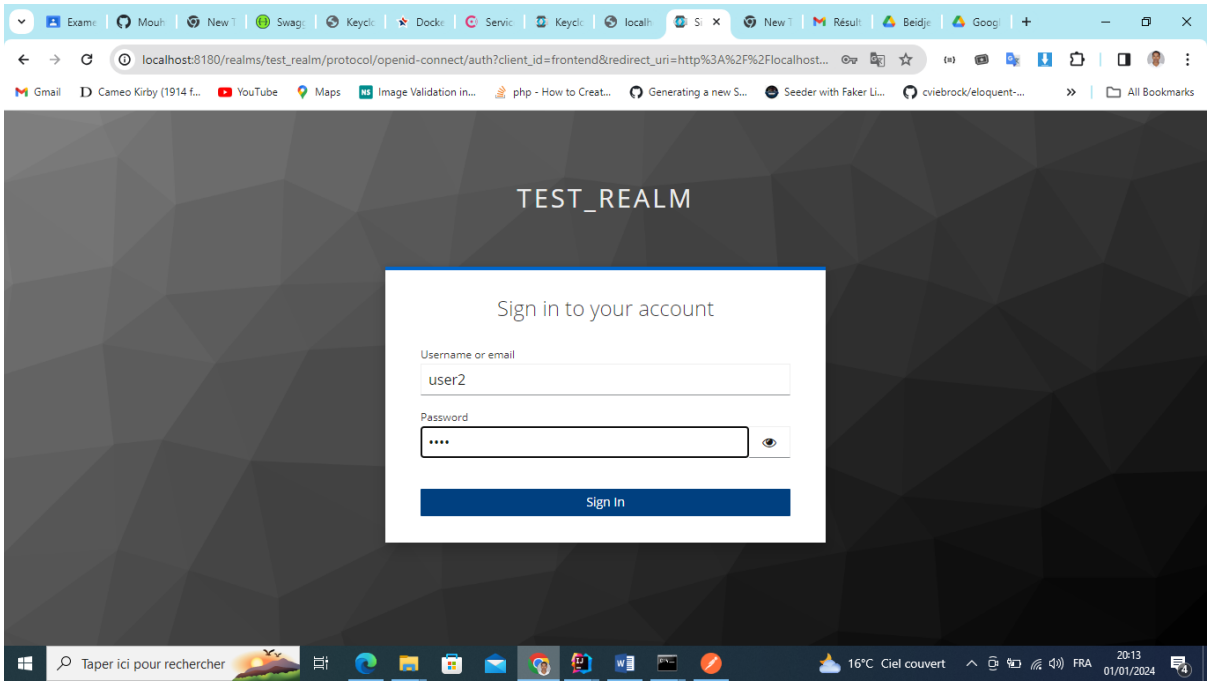
Classe SecurityConfig

```
@Configuration
@EnableWebSecurity
@EnableMethodSecurity(prePostEnabled = true)
public class SecurityConfig {

    private JwtAuthConverter jwtAuthConverter;

    public SecurityConfig(JwtAuthConverter jwtAuthConverter) {
        this.jwtAuthConverter = jwtAuthConverter;
    }

    @Bean
    public SecurityFilterChain securityFilterChain(HttpSecurity http)
throws Exception {
        return http
                .csrf(csrf->csrf.disable())
                .authorizeHttpRequests(ar -> ar.requestMatchers(
                        "/v3/api-docs/**",
                        "/swagger-ui/**",
                        "/swagger-ui.html",
                        "health/**",
                        "/h2-console/**").permitAll())
                .authorizeHttpRequests(ar->ar.anyRequest().authenticated())
                .oauth2ResourceServer(o2->o2.jwt(jwt-
>jwt.jwtAuthenticationConverter(jwtAuthConverter)))
                .headers(h->h.frameOptions(fo->fo.disable()))
                .csrf(csrf->csrf.ignoringRequestMatchers("/h2-console/**"))
                .build();
    }

    @Bean
    CorsConfigurationSource corsConfigurationSource() {
        CorsConfiguration configuration = new CorsConfiguration();
        configuration.setAllowedOrigins(Arrays.asList("*"));
        configuration.setAllowedMethods(Arrays.asList("*"));
        configuration.setAllowedHeaders(Arrays.asList("*"));
        UrlBasedCorsConfigurationSource source = new
UrlBasedCorsConfigurationSource();
        source.registerCorsConfiguration("/**", configuration);
        return source;
    }
}
```

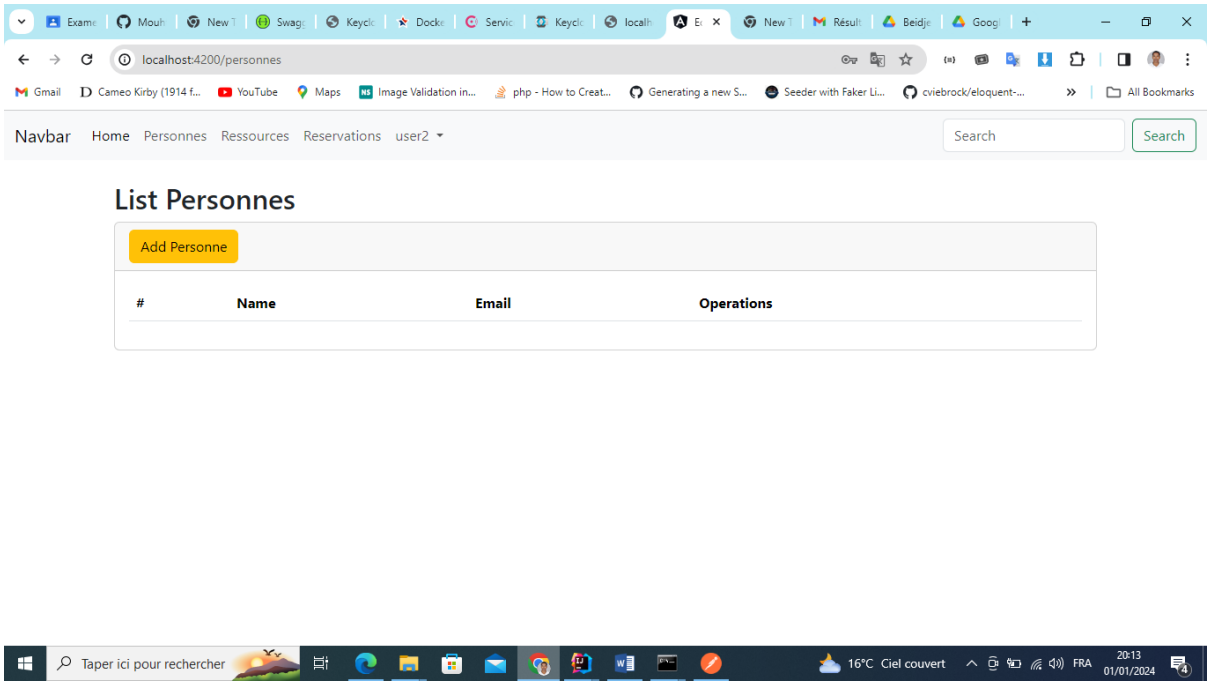
10- ANGULAR



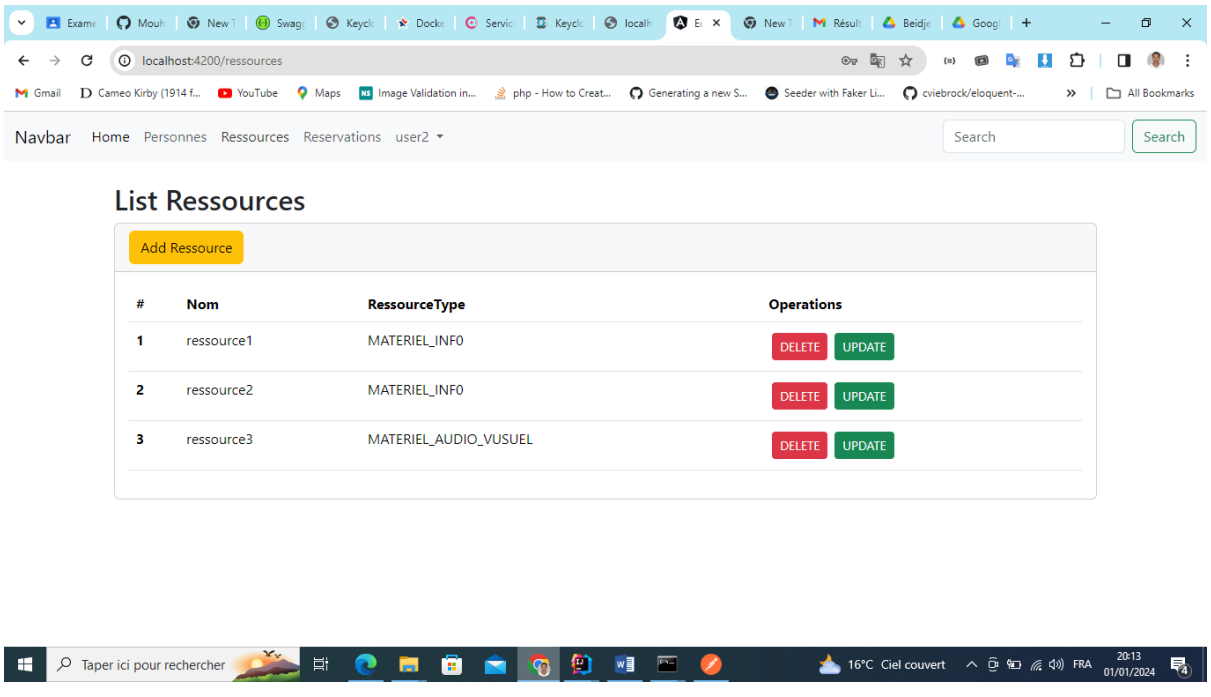
⇨ Page home de mon application : http://localhost:4200/



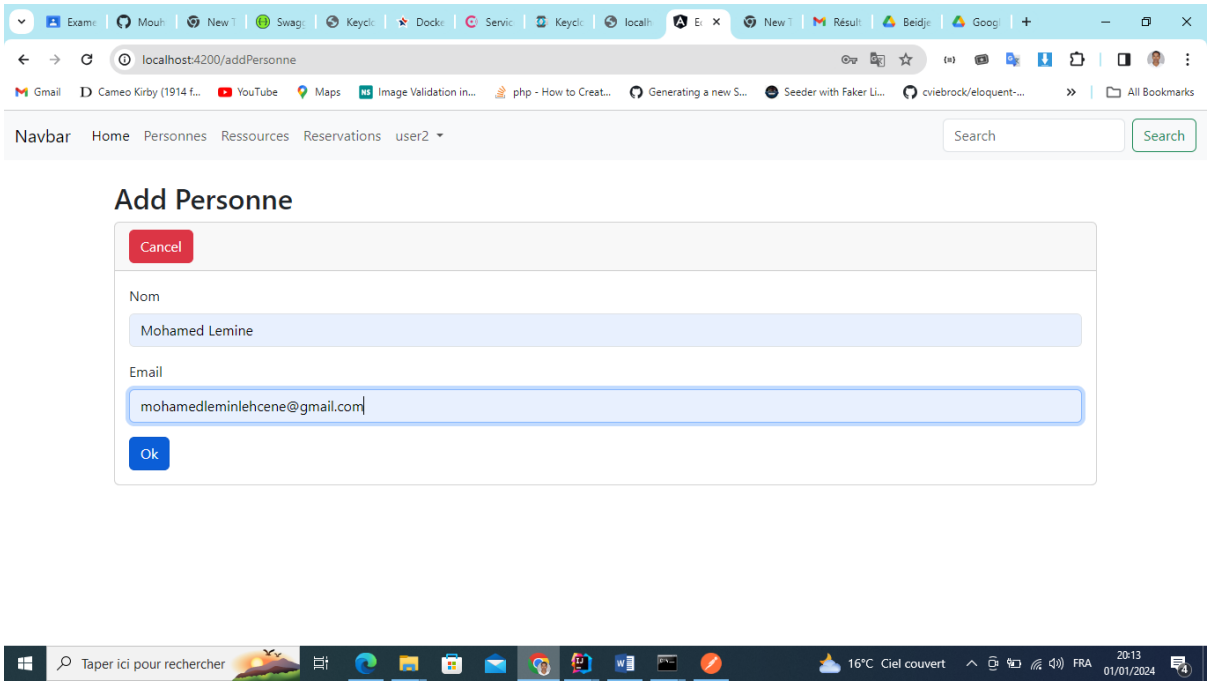
⇨ Voici lors ce que j’’ai clique sur personnes il ma rédigée vers login qui propose par keycloak cette root est protége par guards qui demande authentification



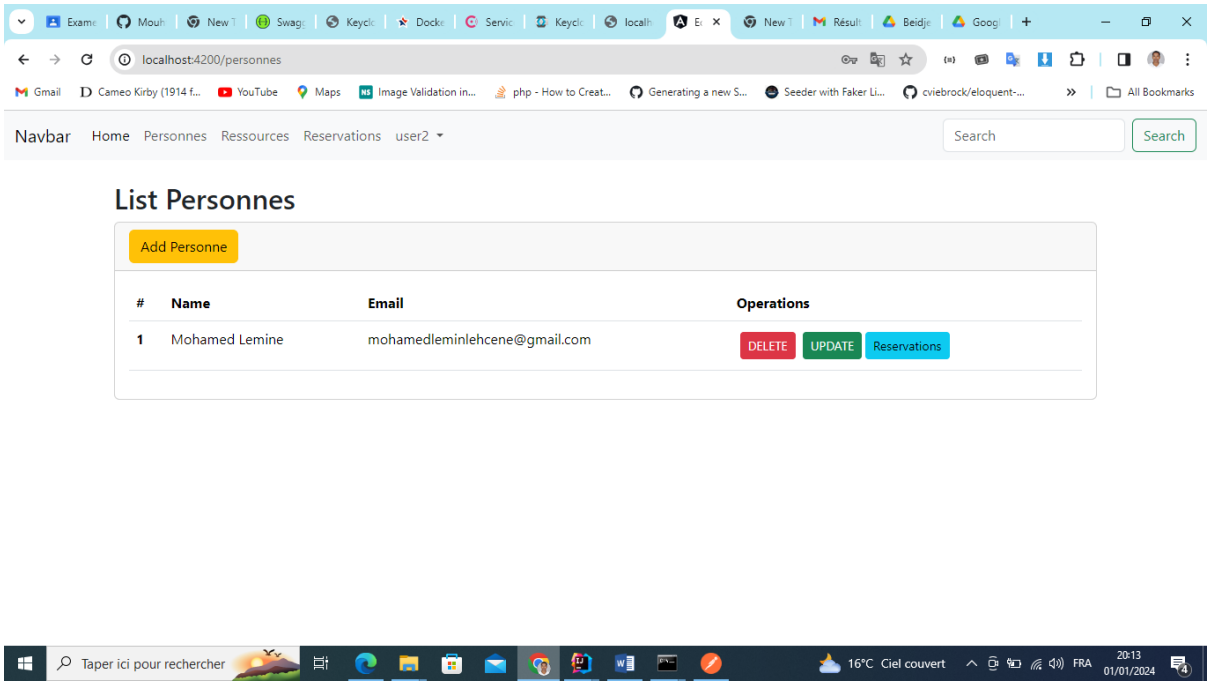
⇨ Voici liste des personnes après l'authentification avec uer2 qui a mot de passe : 1234 qui est à ce moment ne contient aucun personne



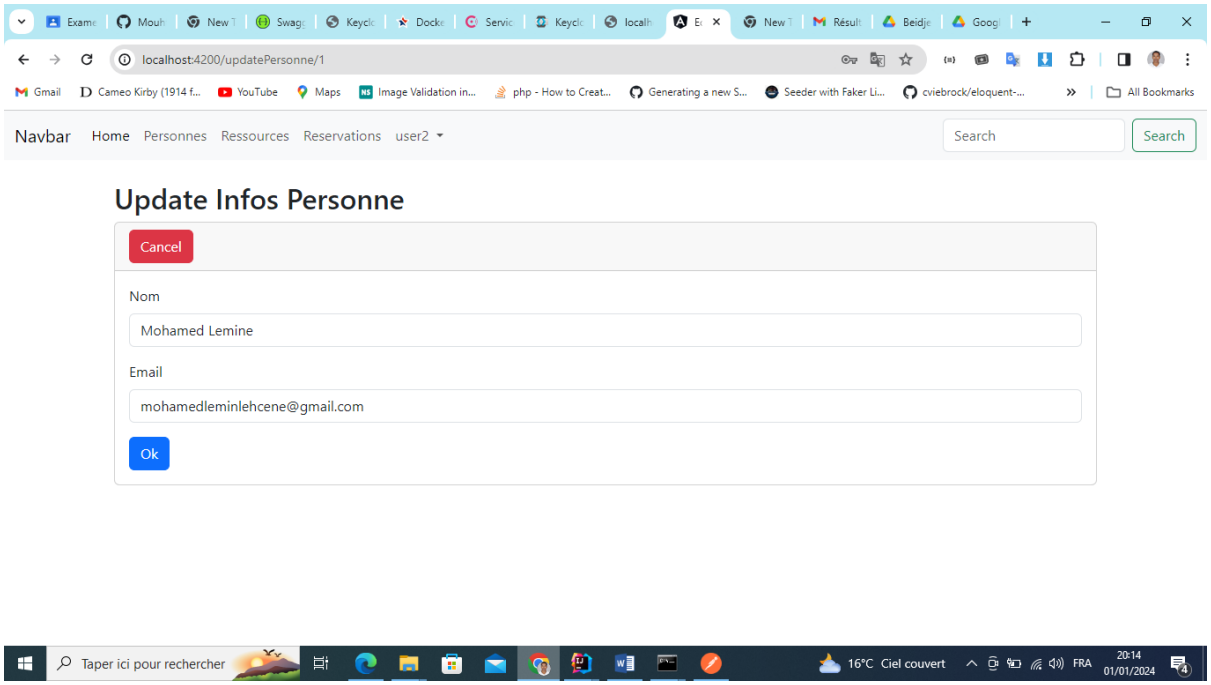
⇨ Voici liste des ressources



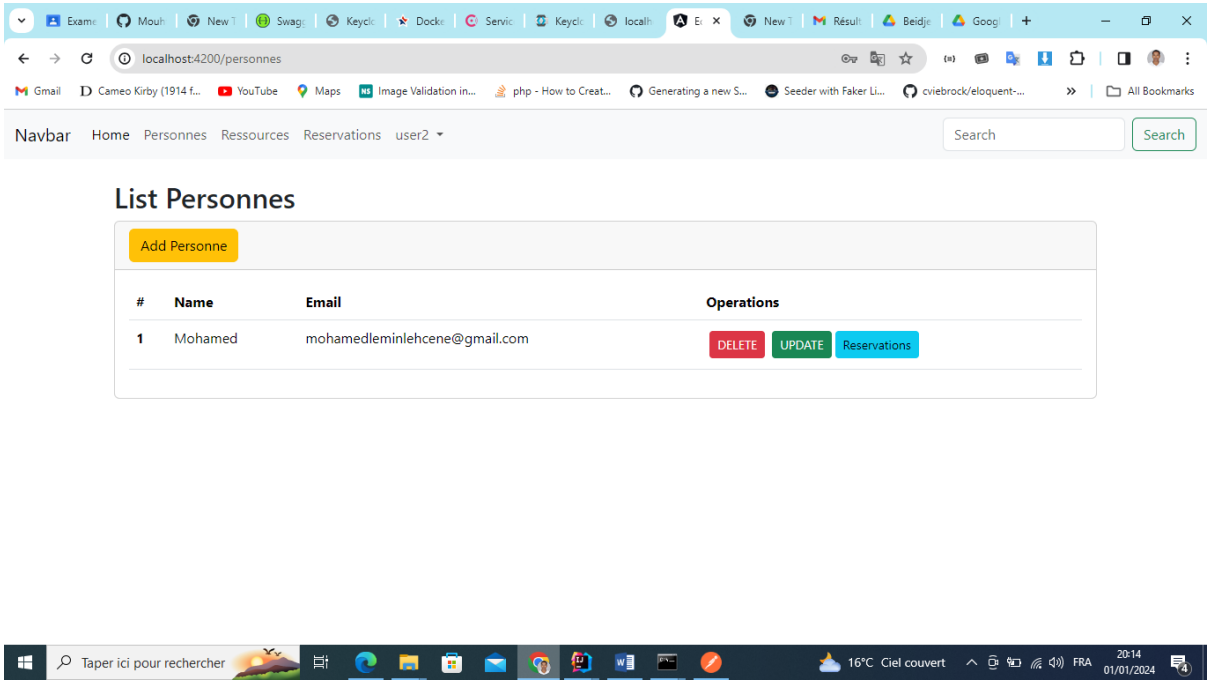
⇨ Pour ajouter nouvelle personne



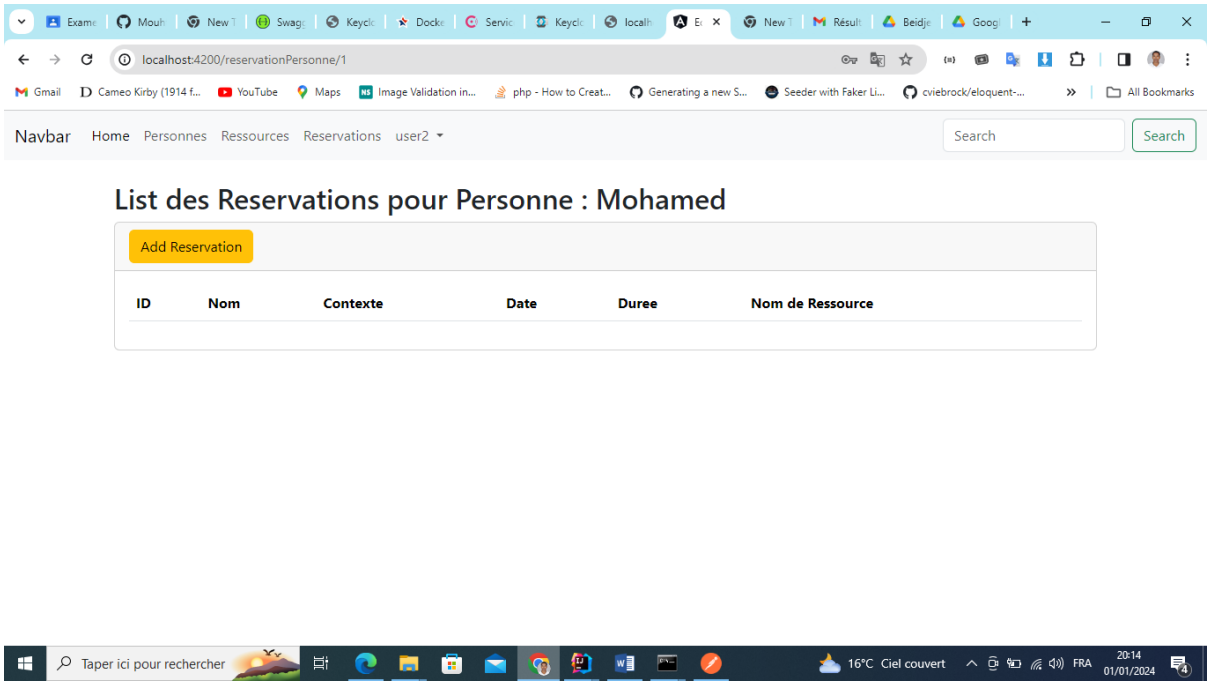
⇨ Voici ajoutassions du nouvelle personne est réussie



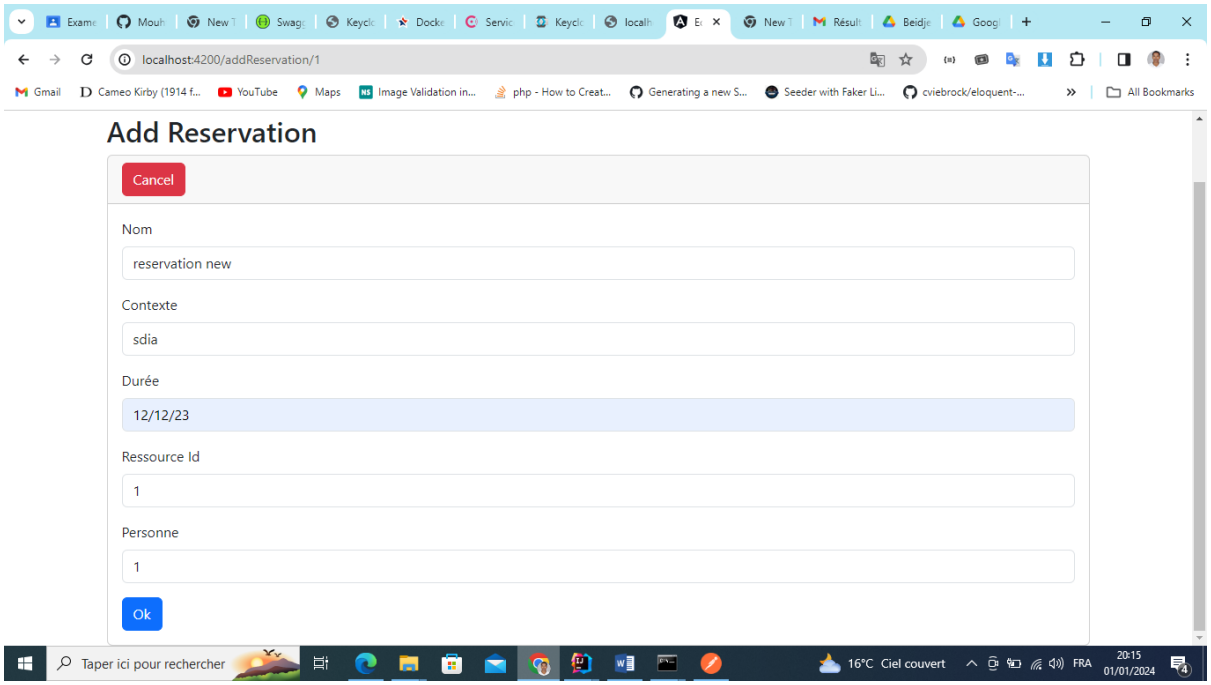
⇨ Pour modifier l'information de personne par son ID : 1



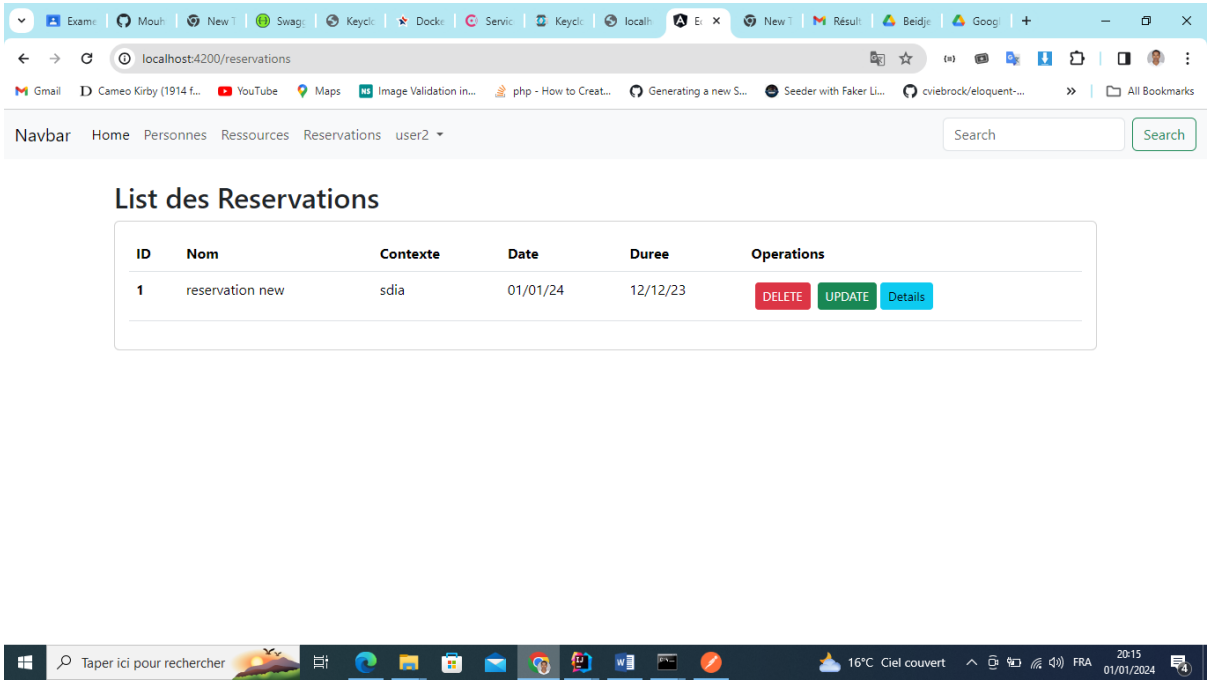
⇨ Voici modification de l'information de personne de son ID égal 1 est réussie



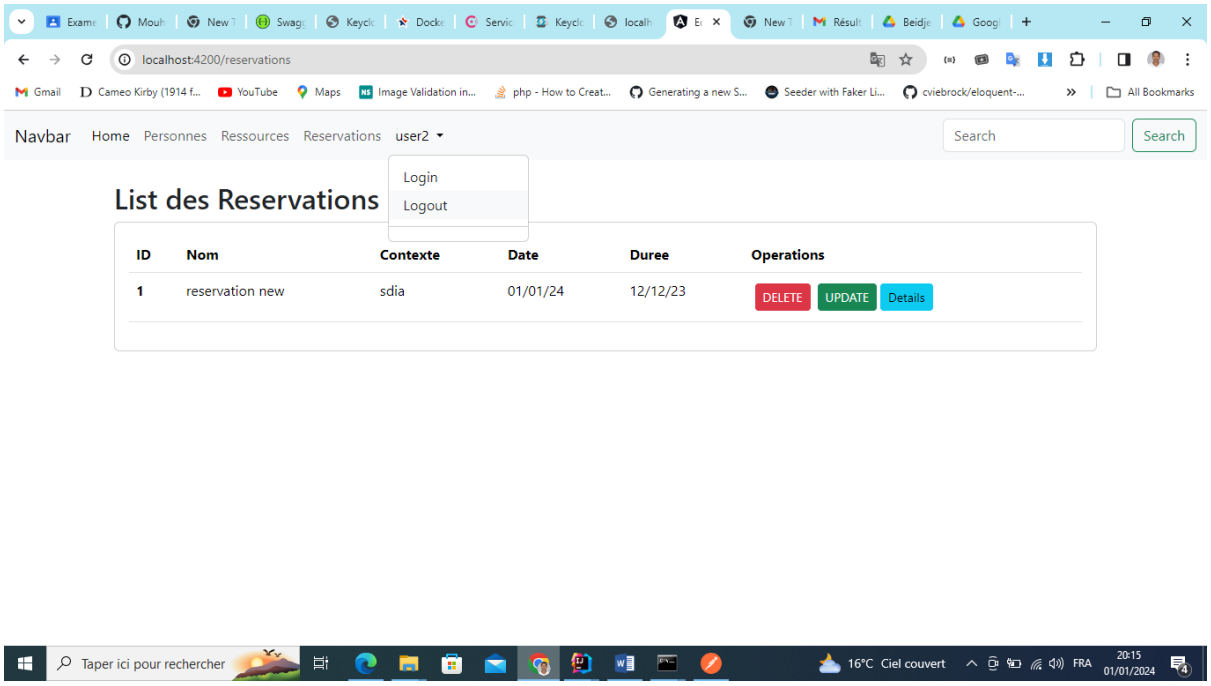
⇨ Liste des réservations pour personne qui a ID : 1



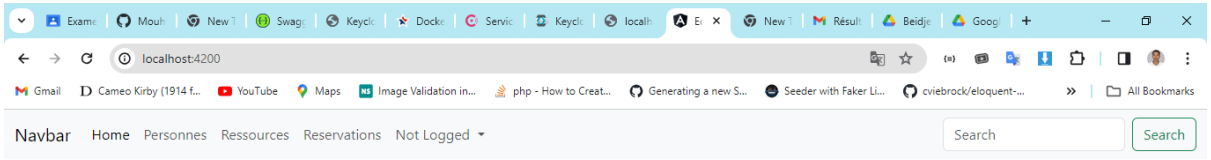
⇨ Pour faire une réservation pour personne qui a ID : 1



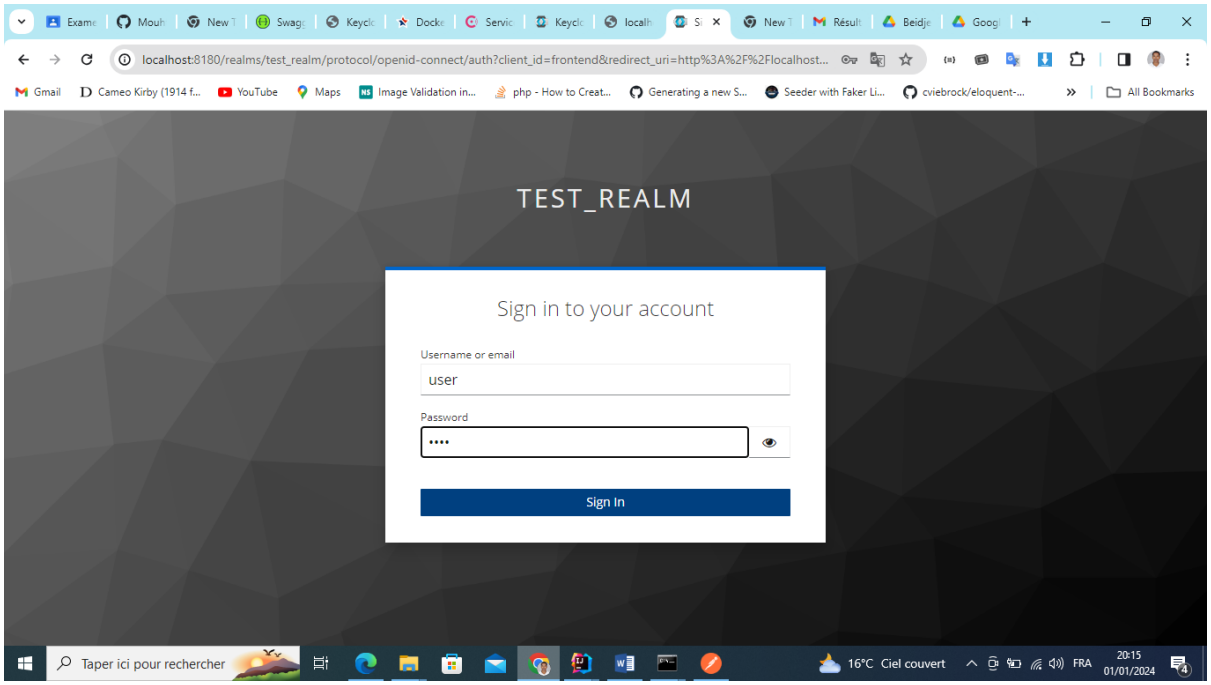
⇨ Voici la réservation est réussie



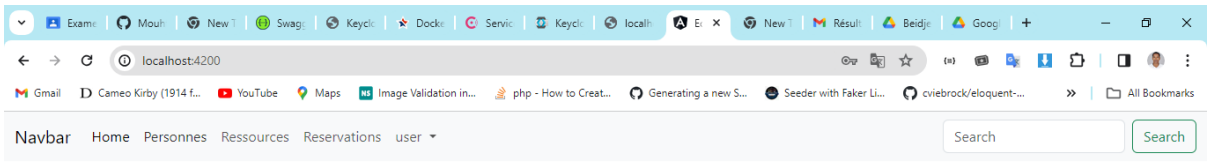
⇨ Pour faire LOGOUT lors ce qu'on clique sur bouton Logout



⇨ Voici LOGOUT est réussie



⇨ Authentification avec utilisateur username : user & password : 1234



⇨ Voici lors ce que j'ai authentifié avec utilisateur de username user ne peut pas d'accédé au liste des personnes car je protégé par rôle ADMIN

MERCI DE VOTRE ATTENTION