Mini guida Keycloak

Keycloak è un software open-source di gestione dell'autenticazione che si basa su OAuth2 e che punta a rendere il più semplice possibile questo tipo di operazione.

Dipendenze

Le dipendenze utilizzate che sono state inserite all'interno del file *pom.xml* di spring boot sono state le seguenti:

```
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-oauth2-client</artifactId>
</dependency>
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-security</artifactId>
</dependency>
<dependency>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-oauth2-resource-server</artifactId>
   <version>2.7.5</version>
</dependency>
```

Inoltre è necessario anche inserire delle configurazioni all'interno del file *.yaml*

```
spring:
 security:
   oauth2:
     client:
       registration:
         keycloak:
           scope:
             - openid
           authorization-grant-type: authorization_code
           client-id: Gateway
       provider:
         keycloak:
           user-name-attribute: preferred_username
           issuer-uri: http://localhost:7070/realms/Gateway
     resourceserver:
       jwt:
         issuer-uri: http://localhost:7070/realms/Gateway
 main:
   allow-bean-definition-overriding: true
   web-application-type: reactive
```

Come è possibile notare all'interno di questo file è presente l'uri con il quale è possibile accedere al portale di *keycloak* per impostare il sistema di autenticazione a piacimento.

Impostare keycloak

Il primo passaggio consiste nel creare un container docker per l'uso di keycloak:

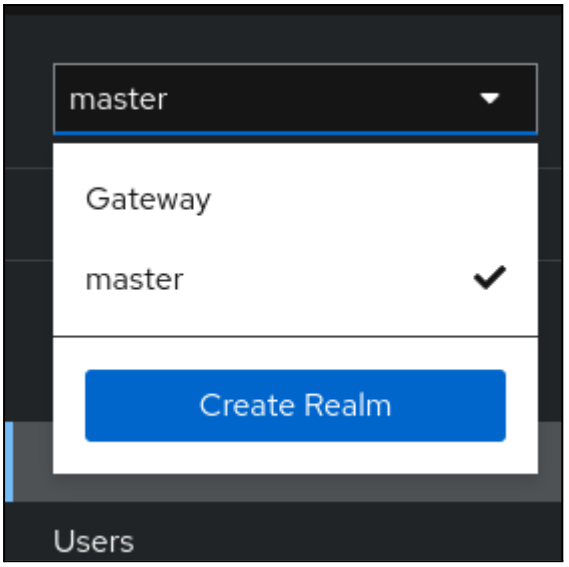
```
docker run -p 7070:8080 -e
KEYCLOAK_ADMIN=admin -e
KEYCLOAK_ADMIN_PASSWORD=admin
quay.io/keycloak/keycloak:20.0.1 start-dev
```

E' possibile notare come attraverso questi comandi si è già predisposto un utente di nome "admin" che ci consentirà di accedere per effettuare le operazioni che vedremo in seguito.

Andando all'indirizzo *http://localhost:7070/*, sarà possibile accedere alla voce *administration console* che ci condurrà in una schermata di login, nella quale una volta effettuato l'accesso sarà possibile effettuare tutte le impostazioni necessarie per il corretto funzionamento di keycloak.

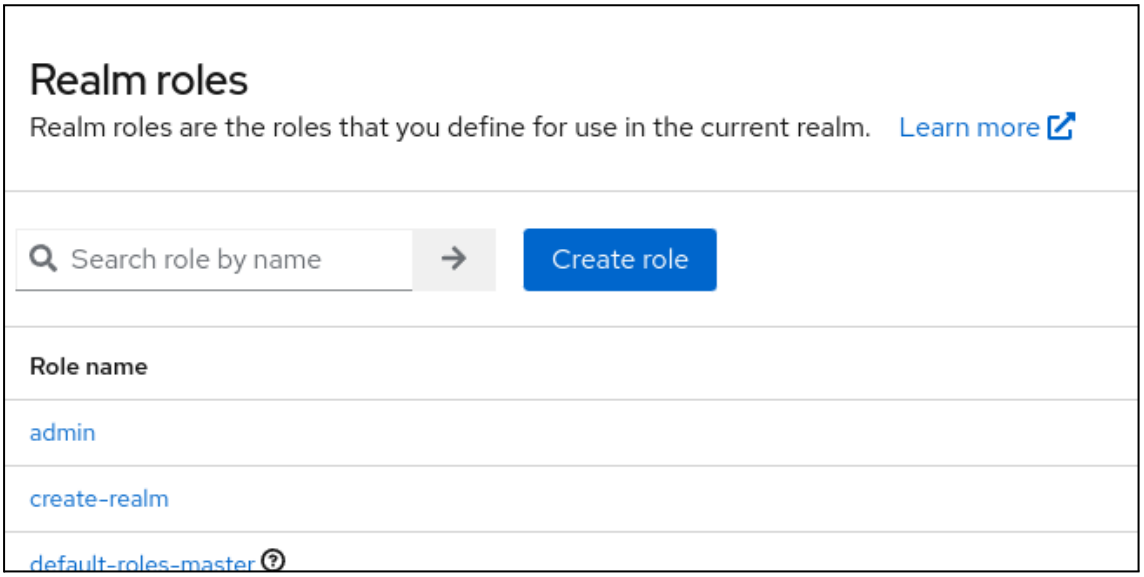
Come prima operazione è necessario definire dei *reami* (o *realms* in inglese) che è un concetto di keycloak che si riferisce a un oggetto che gestisce una serie di utenti assieme alle loro credenziali, ruoli e gruppi di appartenenza: infatti ogni utente appartiene, e può appartenere, ad un unico *reame* e quando esso farà l'autenticazione, lo farà automaticamente anche al reame, oltre che al servizio che vuole usare

Per creare un nuovo reame basta aprire il menu a tendina presente in alto a sinistra



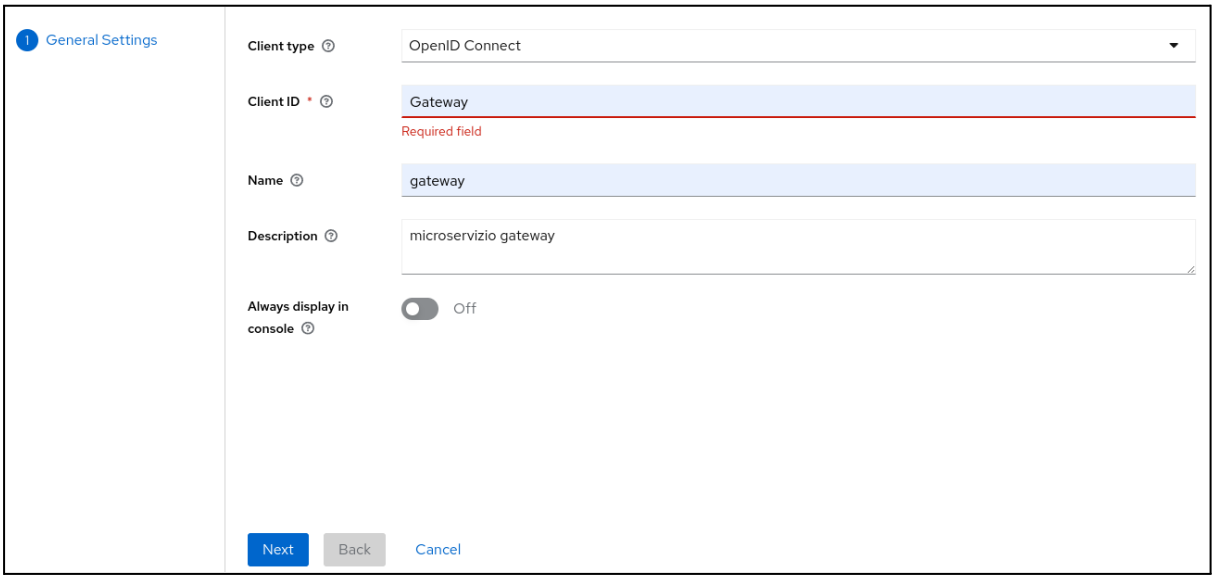
E cliccare sul bottone *create realm*: a questo punto basterà definire un nome e salvare il tutto. Adesso il reame sarà selezionabile dal menu a tendina visto precedentemente.

Chiaramente sarà utile anche definire dei ruoli e quindi per crearne uno nuovo basta accedere alla sezione del menu *realm roles* e cliccare sul bottone *create role* che è possibile vedere qui sotto.



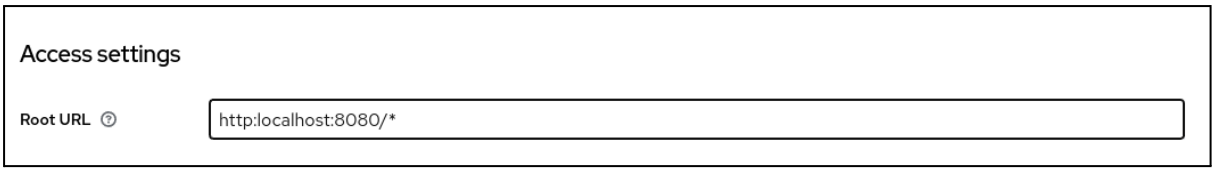
A questo punto verranno richiesti il nome del ruolo e una descrizione, e basterà cliccare su *save* per definire un nuovo *ruolo*.

Dopodiché è necessario definire un client, cioè un servizio o applicazione che necessita l'autenticazione di un utente. In questo esempio vedremo come creare un client associato al gateway di un microservizio. Per fare ciò basta selezionare la voce *clients* e successivamente, nella pagina che verrà visualizzata *create client,* e apparirà il seguente form

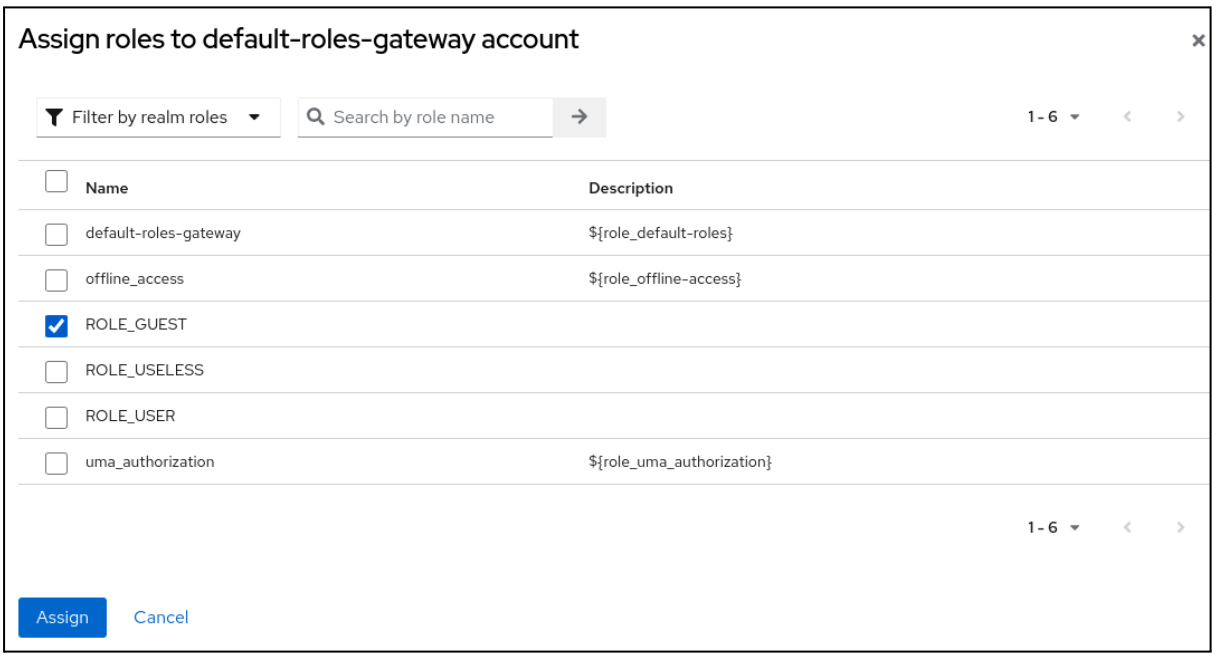


A questo punto basta compilare i vari campi, passare alla sezione successiva dove sarà possibile definire impostazioni più avanzate che non sono di diretto interesse per questo

caso d'uso, e a questo punto creare il *client.*
Una volta creato il client bisogna definire a che url è associato, per fare ciò basta cliccare sul client appena create tra la lista dei client, recarsi alla voce *access settings* e definire il cosiddetto url root come segue:



Potrebbe essere utile anche assegnare un ruolo di default quando si crea un nuovo utente, per fare ciò basta recarsi nella sezione *realm settings,* passare alla scheda *user registration,* cliccare sul bottone *assign role* e apparirà un form di questo tipo:



Qui basta spuntare i ruoli di nostro interesse e premendo su *assign* effettueremo l'assegnazione dei ruoli di default.