

Configuraciones iniciales de Keycloak

Rodrigo Batista - Parcial Backend II

1. Ejecutar Keycloak con Docker

```
docker run -p 8080:8080 -e KEYCLOAK_ADMIN=admin -e KEYCLOAK_ADMIN_PASSWORD=admin  
quay.io/keycloak/keycloak:22.0.1 start-dev
```

2. Crear un nuevo reino importando el archivo realm-export.json

Create realm

A realm manages a set of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users that they control.

Resource file

Drag a file here or browse to upload Browse... Clear

```
1 {  
2   "id": "5c7895b8-3a62-4d0d-a897-e1393d455775",  
3   "realm": "dh_bills",  
4   "notBefore": 0,  
5   "defaultSignatureAlgorithm": "RS256",  
6   "revokeRefreshToken": false,  
7   "refreshTokenMaxReuse": 0.
```

Upload a JSON file

Realm name *

dh_bills

Enabled

☒ On

Create

Cancel

3. Ingresar al cliente "bills-client" y regenerar el Client secret.

Clients > Client details

bills-client

OpenID Connect

☒ Enabled ⓘ Action ▾

Clients are applications and services that can request authentication of a user.

Settings

Keys

Credentials

Roles

Client scopes

Service accounts roles

Sessions

Advanced

Client Authenticator ⓘ

Client Id and Secret ▾

Save

Client secret

..... ⓘ ⓘ

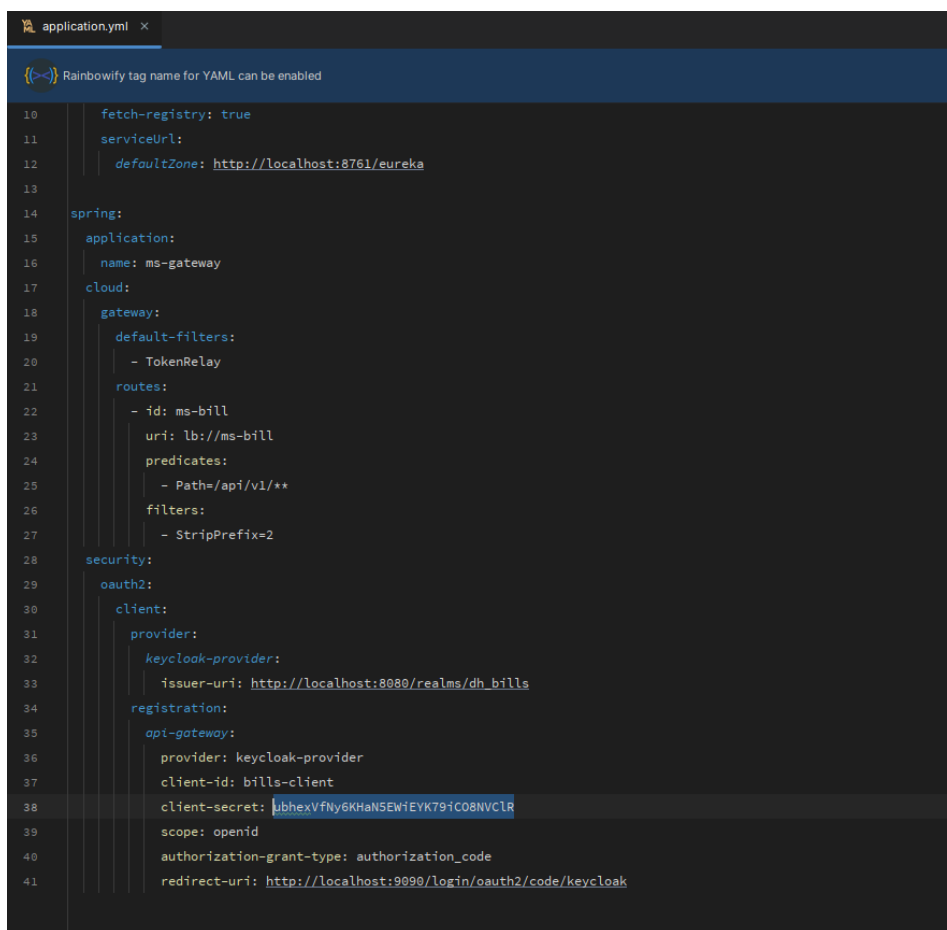
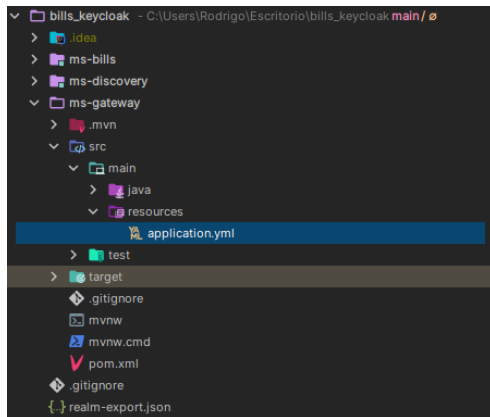
Regenerate

Registration access token ⓘ

..... ⓘ

Regenerate

Este nuevo “client-secret” generado debe ser colocado en el application.yml correspondiente al microservicios del gateway.



4. Crear dos usuarios en el reino creado: user_authorized, user_not_authorized

Users

Users are the users in the current realm. [Learn more](#)

User list

Default search

Search user

→

Add user

Delete user

1-2

<

>

<input type="checkbox"/>	Username	Email	Last name	First name	Status	
<input type="checkbox"/>	user_authorized	✖ --	--	--	--	⋮
<input type="checkbox"/>	user_not_authorized	✖ --	--	--	--	⋮

1-2

<

>

5. Asignar una contraseña a cada uno de los usuarios creados.

Users > User details

user_authorized

Enabled

Action

Details

Attributes

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

+

Set password for user_authorized

✕

Password *

Password confirmation *

Temporary ⓘ

Off

Save

Cancel

6. Asignar el rol de user (rol a nivel de reino), solo al usuario “user_authorized”

Users > User details

user_authorized

Enabled

Action

Details

Attributes

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

Search by name

→

Hide inherited roles

Assign role

Unassign

1-2

<

>

<input type="checkbox"/>	Name	Inherited	Description
<input type="checkbox"/>	user	False	--
<input type="checkbox"/>	default-roles-dh_bills	False	\${role_default-roles}

1-2

<

>

El usuario “user_not_authorized” debe quedar sin el rol user asignado.

Users > User details

user_not_authorized

Enabled

Action

Details

Attributes

Credentials

Role mapping

Groups

Consents

Identity provider links

Sessions

Search by name

→

Hide inherited roles

Assign role

Unassign

1-1

<

>

<input type="checkbox"/>	Name	Inherited	Description
<input type="checkbox"/>	default-roles-dh_bills	False	\${role_default-roles}

1-1

<

>