Certified Tech Developer
The Ultimate Degree

Especialización en Back End II

Trabajo Integrador - Ejercicio 2

- Ejercitación individual
- Nivel de complejidad: medio 🔥🔥

Enunciado

Continuamos trabajando en el sistema de películas online, en esta etapa vamos a seleccionar una estrategia de autorización para proteger los diferentes microservicios del sistema.

Luego del relevamiento inicial se descubrieron 4 tipos de usuarios que consumen la diferentes APIs, estos son :

- Clientes (Usuarios que utilizaran el sistema con el fin de ver las películas).
- Administradores (Usuarios que gestionan las películas, típicamente las operaciones CRUD).
- Proveedores de facturas (Un sistema externo que se encarga de crear las facturas de los usuarios y guardarlas en la base de datos del sistema, para que luego los usuarios puedan descargarlas).
- Sistemas internos (Llamadas de un microservicio a otro dentro del mismo sistema).

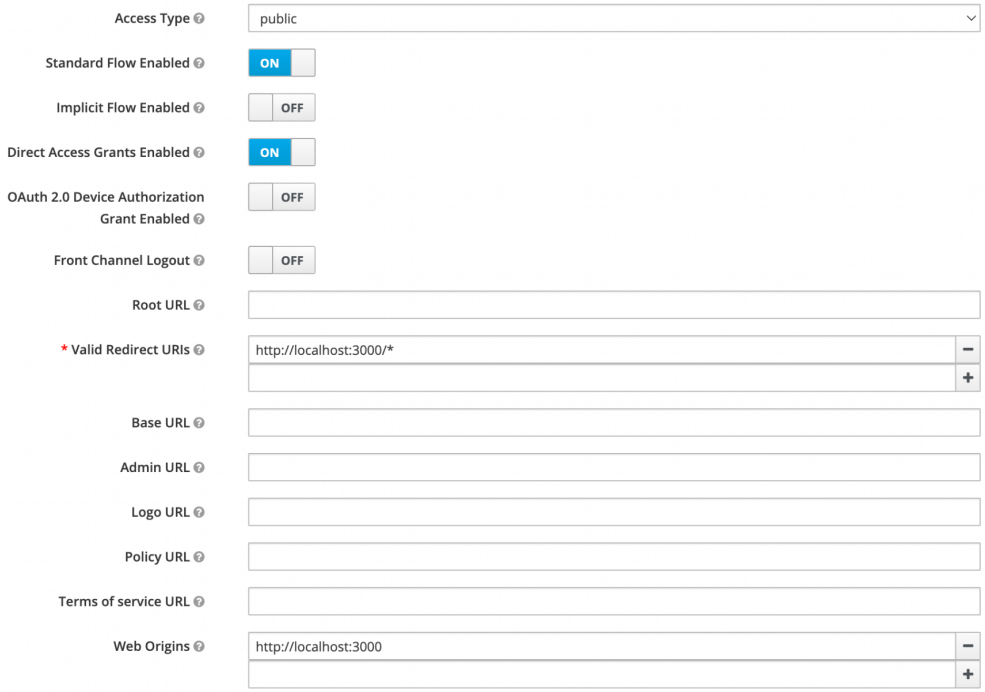
Teniendo en cuenta estos 4 escenarios en los que se requerirá validar al usuario según sea su tipo de acceso, se pensaron las siguientes estrategias :

1. Para los Clientes, Administradores y Proveedores de facturas se utilizara **GBAC** es decir group based access control. Crearemos 3 grupos
    A. client
    B. admin
    C. provider

2. Para las llamadas entre microservicios utilizaremos **scopes**. Inicialmente crearemos un scope genérico para todas las llamadas entre microservicios llamado **SCOPE_internal**

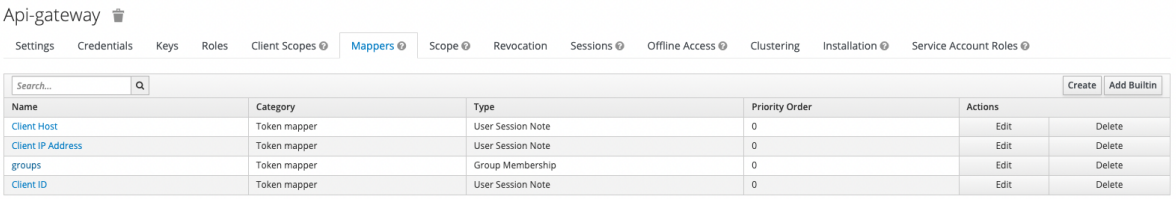
Teniendo en cuenta lo planteado anteriormente, se nos pide crear en Keycloak, dentro del reino DigitalMedia:

1. Crear un cliente llamado “**microservicios**”
    a. Configurar el tipo de acceso como confidencial.
    b. Poner en **ON** la opción “Service Accounts Enabled”
    c. Crear los grupos client, admin, provider.
    d. Configurar el tiempo de inactividad de la sesión en 5 minutos
2. Crear un scope en el tab “Client Scopes” llamado “**internal**”
3. Crear un cliente llamado “internal”
    a. Configurar el tipo de acceso como público.
    b. Definir la URIs válidas de redirect como: http://localhost:3000/*
    c. Definir en la opción “Web Origins” : http://localhost:3000



4. Crear un cliente llamado ”api-gateway”
    a. Configurar el tipo de acceso como confidencial.
    b. Poner en **ON** la opción “Service Accounts Enabled”

5. Asociar a cada uno de los clientes creados un mapper de tipo “group membership” llamado groups:



6. Crear tres usuarios y sus passwords para agregarle a cada uno un grupo diferente:
    a. client
    b. admin
    c. provider