



ESPECIALIDAD: JAVA



NIVEL: AVANZADO



MODALIDAD: ONLINE



**Curso:**

# ARQUITECTURA DE MICROSERVICIOS I

(Spring Boot, Spring Cloud, Docker, Design, Patterns, Buildings, Deployments)



**Jean Ramal**  
Instructor

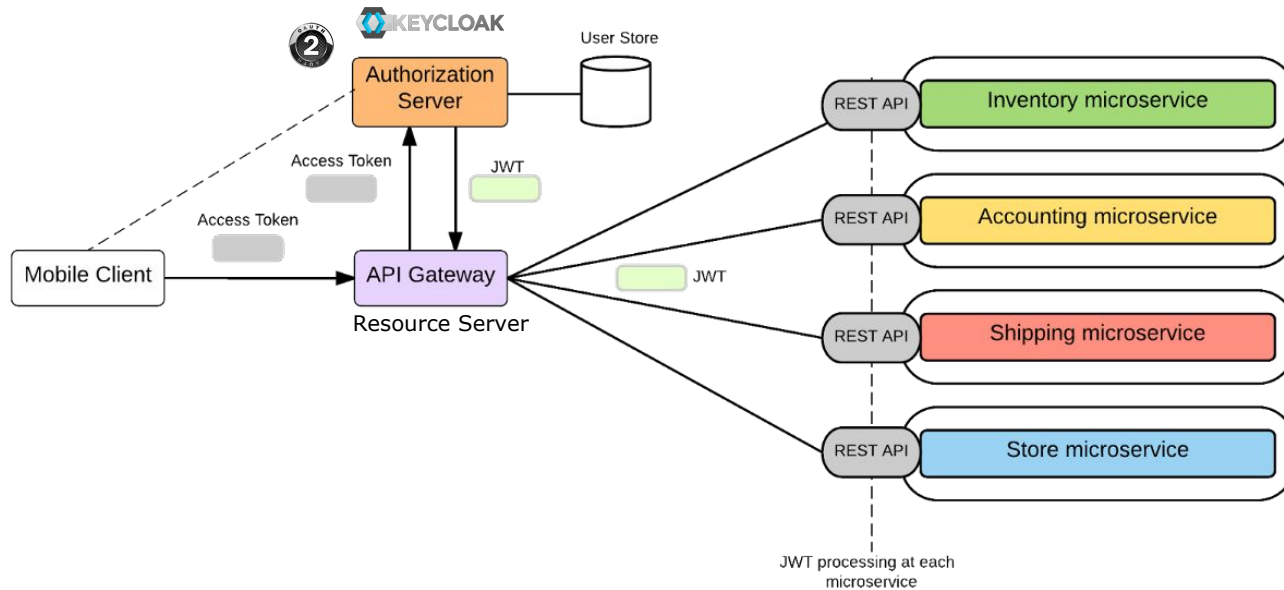
# Agenda - Sesión 04

## **Implementación de la arquitectura de Microservicios**

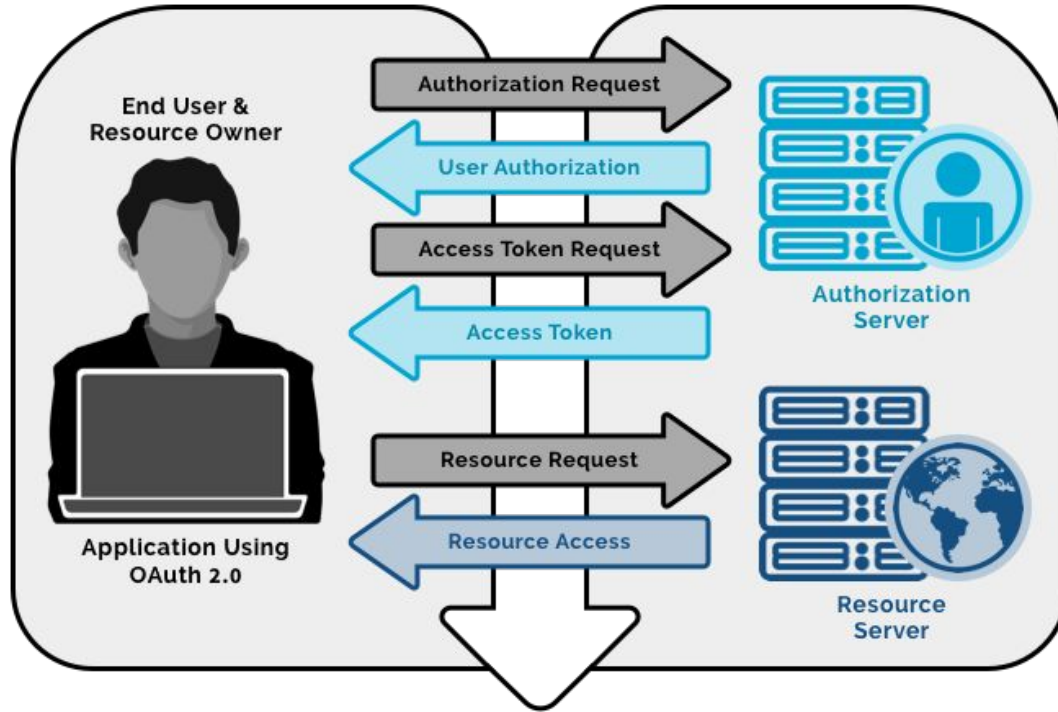
- Patrones a implementar: Authorization Server, Service per Container.
- Spring Security, Spring Authorization Server, Deployments en Docker
- Implementar los patrones.

# Authorization Server

- Identificación de forma segura
- Autenticación y autorización
- Implementación en Spring con **Spring Security Spring Authorization Server**.



# Authorization Server



# Keycloak

Keycloak es un gestor de identidad y acceso.

Agrega autenticación a las aplicaciones y asegura servicios con mínimo esfuerzo.

No necesita lidiar con almacenamiento o autenticación de usuarios.

- Single-Sign On
- Identity brokering and Social Login
- User Federation
- Admin Console
- Account Management Console
- Standard Protocols
- Authorization Services



# OAuth 2

OAuth 2.0 es el protocolo estándar de la industria para la autorización. OAuth 2.0 se centra en la simplicidad del desarrollador al tiempo que proporciona flujos de autorización específicos para aplicaciones web, aplicaciones de escritorio, teléfonos móviles y dispositivos de sala de estar.



# Json Web Token (JWT)

Estándar para la generación de tokens de acceso que permiten el intercambio de identificación y privilegios entre 2 partes.

- Estructura:

Token

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c
```

HEADER: ALGORITHM & TOKEN TYPE

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```

PAYLOAD: DATA

```
{  
  "sub": "1234567890",  
  "name": "John Doe",  
  "iat": 1516239022  
}
```

VERIFY SIGNATURE

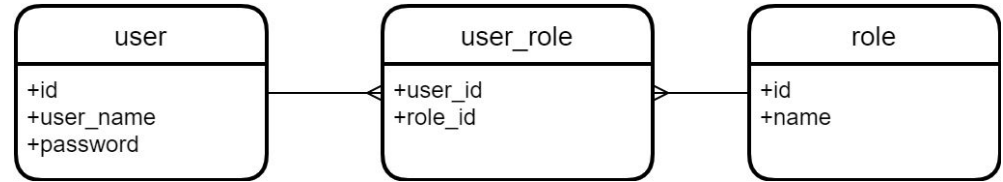
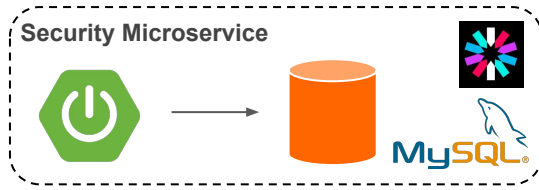
```
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  your-256-bit-secret  
) ☐ secret base64 encoded
```

# Json Web Token (JWT)

- Campos del PAYLOAD:

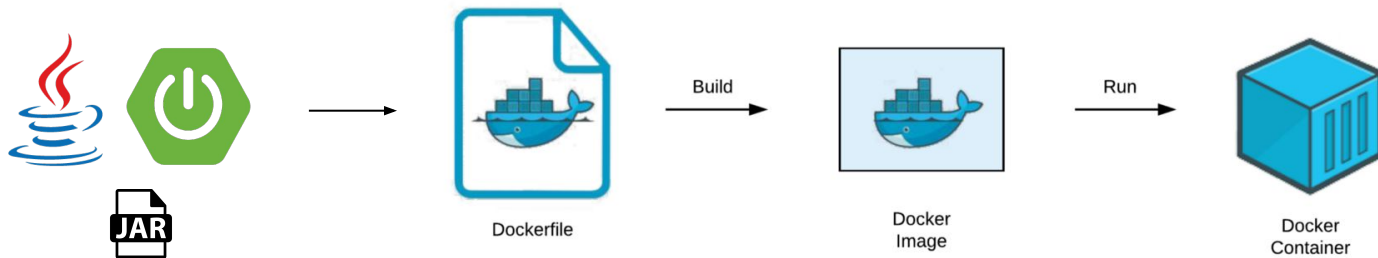
| Código | Nombre          | Descripción                                                                                                                                                                                                                                                                                                           |
|--------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| iss    | Issuer          | Identifica el proveedor de identidad que emitió el JWT                                                                                                                                                                                                                                                                |
| sub    | Subject         | Identifica el objeto o usuario en nombre del cual fue emitido el JWT                                                                                                                                                                                                                                                  |
| aud    | Audience        | Identifica la audiencia o receptores para lo que el JWT fue emitido. Cada servicio que recibe un JWT para su validación tiene que controlar la audiencia a la que el JWT está destinado. Si el proveedor del servicio no se encuentra presente en el campo <code>aud</code> , entonces el JWT tiene que ser rechazado |
| exp    | Expiration time | Identifica la marca temporal luego de la cual el JWT <b>no tiene</b> que ser aceptado.                                                                                                                                                                                                                                |
| nbf    | Not before      | Identifica la marca temporal en que el JWT comienza a ser válido. EL JWT <b>no tiene</b> que ser aceptado si el token es utilizando antes de este tiempo.                                                                                                                                                             |
| iat    | Issued at       | Identifica la marca temporal en qué el JWT fue emitido.                                                                                                                                                                                                                                                               |
| jti    | JWT ID          | Identificador único del token incluso entre diferentes proveedores de servicio.                                                                                                                                                                                                                                       |

# Microservicios de Seguridad



# Service per Container

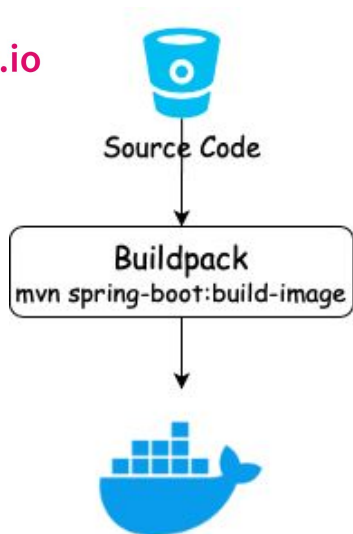
- Despliegue y escalamiento de manera independiente.
- Servicios aislados entre sí.
- Creación e implementación rápidamente.
- Establecer y restringir recursos de forma independiente.
- Los servicios se pueden escribir en distintos lenguajes, frameworks y versiones de los mismos.
- Implementación con Docker.



# Service per Container

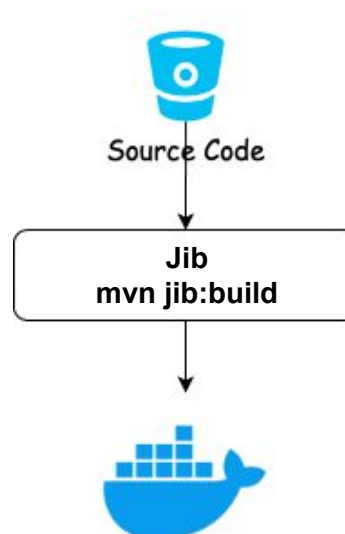


Buildpacks.io



Docker (OCI) Image

Source to Image



Docker (OCI) Image

Source to Image

# Recursos de Arquitectura de Microservicios

<https://microservices.io/patterns/security/access-token.html>

<https://docs.microsoft.com/es-es/azure/architecture/patterns/valet-key>

<https://www.keycloak.org/>

<https://oauth.net/2/>

<https://jwt.io/>

<https://spring.io/projects/spring-authorization-server>

# ¡GRACIAS!

**Correo:** jean.ramal@gmail.com

**Wa:** 51994641153

**Link:** <https://www.linkedin.com/in/jeanramal/>