

Resumen workflow GitHub generado

Proyecto: tfg-cicd-aws-2526

Plataforma CI: GitHub Actions

Ramas CI: main, develop

PR activado: sí

Requisitos del proyecto para este workflow:

- Proyecto Java con Maven Wrapper (./mvnw).
- Fichero app/pom.xml (el workflow llama a -f app/pom.xml).
- Si tu código está en otra ruta, adapta las rutas -f app/pom.xml en el YAML.
- Si no tienes mvnw, puedes cambiar ./mvnw por mvn en los pasos de Maven.

Sonar: sí

Quality gate estricto: no

Host Sonar: <https://sonarcloud.io>

sonar.projectKey: davidtome97_tfg-parent

sonar.organization: davidtome97

Secrets necesarios para SonarCloud:

- SONAR_HOST_URL (ej: <https://sonarcloud.io>)
- SONAR_TOKEN (token personal de SonarCloud para análisis)

AWS (deploy): sí

Modo deploy: tag (release)

Secrets AWS utilizados en el workflow:

- Access Key ID: AWS_ACCESS_KEY_ID (ejemplo de valor: AKIAIOSFODNN7EXAMPLE)
- Secret Access Key: AWS_SECRET_ACCESS_KEY (ejemplo de valor: wJalrXUtnFEMI/K7MDENG)
- Región AWS: AWS_REGION (ejemplo de valor: eu-west-1)
- Registry ECR: AWS_ECR_REGISTRY (ejemplo de valor: 123456789012.dkr.ecr.eu-west-1.amazonaws.com)
- Repositorio ECR: AWS_ECR_REPOSITORY (ejemplo de valor: tfg-cicd-aws-2526)
- Host/IP EC2: AWS_EC2_HOST (ejemplo de valor: ec2-11-22-33-44.eu-west-1.compute.amazonaws.com)
- Usuario EC2: AWS_EC2_USER (ejemplo de valor: ubuntu)

Base de datos: sí (solo informativo)

Recuerda crear los secrets en GitHub → Settings → Secrets and variables → Actions.

¿De dónde saco estos valores?

Token de SonarCloud (SONAR_TOKEN):

1. Entra en SonarCloud con tu usuario.
2. Arriba a la derecha → My Account → Security.
3. Crea un token nuevo (scope: analysis).
4. Copia el token y guárdalo (solo se muestra una vez).
5. Crea el secret SONAR_TOKEN en GitHub con ese valor.

Credenciales de AWS (Access key / Secret key):

1. Entra en AWS Console → IAM → Users.
2. Selecciona un usuario con permisos para ECR/EC2.

3. Pestaña 'Security credentials' → Create access key.
4. Copia 'Access key ID' y 'Secret access key'.
5. Crea los secrets AWS_ACCESS_KEY_ID y AWS_SECRET_ACCESS_KEY en GitHub.

Otros valores AWS necesarios:

- AWS_REGION: ej. eu-west-1
- AWS_ECR_REGISTRY: copiar desde AWS ECR (Copy URI, parte del registry).
- AWS_ECR_REPOSITORY: nombre del repo de ECR (sin la URL completa).
- AWS_EC2_HOST: IP pública / DNS de la instancia EC2.
- AWS_EC2_USER: ej. ubuntu / ec2-user.

Cómo crear secrets en GitHub:

1. Abre tu repositorio en GitHub.
2. Ve a Settings → Secrets and variables → Actions.
3. Pulsa 'New repository secret'.
4. Escribe el NOMBRE EXACTO del secret que aparece en este PDF.
5. Pega el valor correspondiente.
6. Repite el proceso para cada secret necesario.