

Resumen workflow GitHub generado

Proyecto: tfg-cicd-aws-2526

Plataforma CI: GitHub Actions

Ramas CI: main, develop

PR activado: sí

Proyecto con Node: sí

Requisitos del proyecto para este workflow:

- Proyecto Java con Maven Wrapper (./mvnw).
- Fichero pom.xml (el workflow llama a -f pom.xml).
- Si el código está en otra ruta, tengo que adaptar las rutas -f pom.xml en el YAML.
- Si no tengo mvnw, puedo cambiar ./mvnw por mvn en los pasos de Maven.
- Si uso Node, necesito package.json con scripts de test/lint si quiero aprovecharlos.

Sonar: sí

Quality gate estricto: no

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

sonar.projectKey: davidtome97_tfg-cicd-aws-2526

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_URL (ejemplo de valor: 123456789012.dkr.ecr.eu-west-1.amazonaws.c
- Repositorio ECR: ECR_REPOSITORY (ejemplo de valor: tfg-cicd-aws-2526)
- Host/IP EC2: EC2_HOST (ejemplo de valor: ec2-11-22-33-44.eu-west-1.compute.amazonaws.com)
- Usuario EC2: EC2_USUARIO (ejemplo de valor: ubuntu)

Base de datos: sí (solo informativo)

Recuerdo que tengo que crear los secrets en GitHub → Settings → Secrets and variables → Actions.

¿De dónde saco estos valores?

Token de SonarCloud (SONAR_TOKEN):

1. Entro en SonarCloud con mi usuario.
2. Arriba a la derecha → My Account → Security.
3. Creo un token nuevo (scope: analysis).
4. Copio el token y lo guardo (solo se muestra una vez).
5. Creo el secret SONAR_TOKEN en GitHub con ese valor.

Credenciales de AWS (Access key / Secret key):

1. Entro en AWS Console → IAM → Users.
2. Selecciono un usuario con permisos para ECR/EC2.
3. Pestaña 'Security credentials' → Create access key.
4. Copio 'Access key ID' y 'Secret access key'.
5. Creo 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_URL: copiar desde AWS ECR (Copy URI, parte del registry).
- ECR_REPOSITORY: nombre del repo de ECR (sin la URL completa).
- EC2_HOST: IP pública / DNS de la instancia EC2.
- EC2_USUARIO: ej. ubuntu / ec2-user.

Cómo crear secrets en GitHub:

1. Abro mi repositorio en GitHub.
2. Voy a Settings → Secrets and variables → Actions.
3. Pulso 'New repository secret'.
4. Escribo el NOMBRE EXACTO del secret que aparece en este PDF.
5. Pego el valor correspondiente.
6. Repito el proceso para cada secret necesario.