ESTÁNDAR SONARQUBE

Versión 1.0

Arquitectura y Estándares TI

09/09/2022

Tabla de contenido

1. Versiones

Descripción	Versión	Autor	Fecha
Publicación de documento original	1.0.0	Ruddy Claros	09/09/2022

2. Definiciones

Concepto	Definición
Vulnerabilidad	Debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.
Bug	Errores de código; pueden ser por un error en la lógica del programador, puede ser por la incompatibilidad de una librería o un error de la propia plataforma de desarrollo

3. Objetivo

El documento establece el procedimiento a realizarse para implementar un análisis del código fuente con la herramienta SonarQube dentro de los proyectos en Azure DevOps.

Brinda atribuciones a las Reuniones de Revisión de Arquitectura TI y al equipo de Seguridad de la Información para establecer los proyectos que deben implementar este análisis dentro de las soluciones desarrolladas en el Banco de Crédito S.A.

4. Consideraciones Iniciales

Los proyectos que deben implementar el análisis con la herramienta SonarQube serán designados en Reuniones de Revisión de Arquitectura TI y/o por análisis y evaluación del equipo de Seguridad de la Información.

El equipo de Seguridad de la Información evalúa los resultados del análisis y tiene la potestad de aprobar o rechazar el pase a producción.

El análisis con SonarQube debe realizarse obligatoriamente en la rama main/master y con esta rama se debe realizar el despliegue hacia certificación y producción.

5. Solicitud Token

Mediante correo dirigido al equipo de Seguridad de la Información se debe remitir el nombre del proyecto en el siguiente formato:

NEMÓNICO APLICATIVO_COMPONENTE_SONARQUBE

BIZTALK_SERVICIOS_API_CORE_SONARQUBE

El equipo de Seguridad de la Información responderá remitiendo lo siguiente:

Credenciales de acceso a la consola de SonarQube (únicas para cada equipo):

- ✓ Usuario: UsrArqEstSQ
- ✓ Contraseña: ArqEst7:saTrGR;D

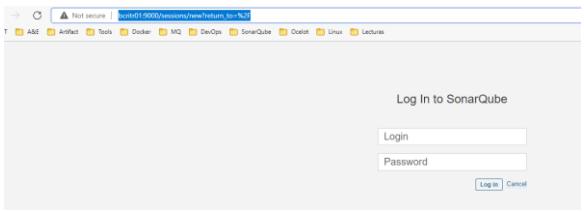
Tokens por Proyecto

- ✓ Project Key: uajWretwYbvcxvpkM1JyasdasdZKzudJU
- ✓ Token: squ_bbdcafwqewef9e5asdasdbc4d5aa2eb505

6. Acceso a la consola de SonarQube

Con las credenciales otorgadas por el equipo de Seguridad de la Información, accedemos en la siguiente ruta:

http://bcritr01:9000/sessions/new?return_to=%2F

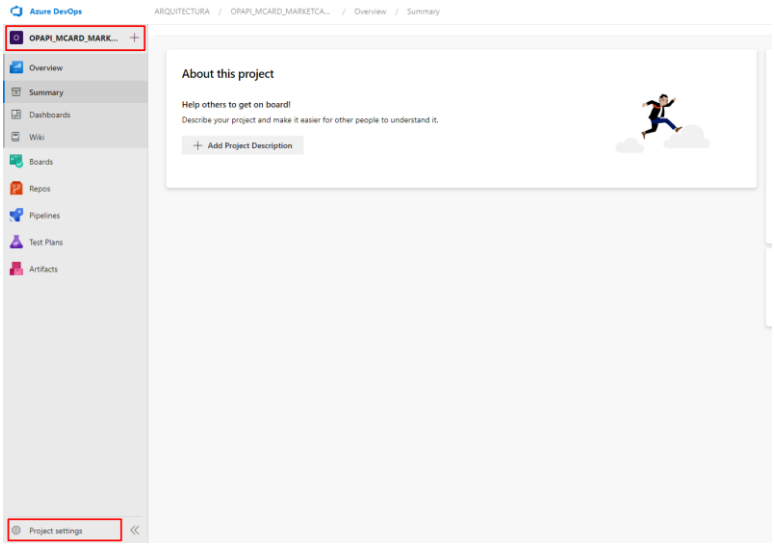


7. Configuración en DevOps

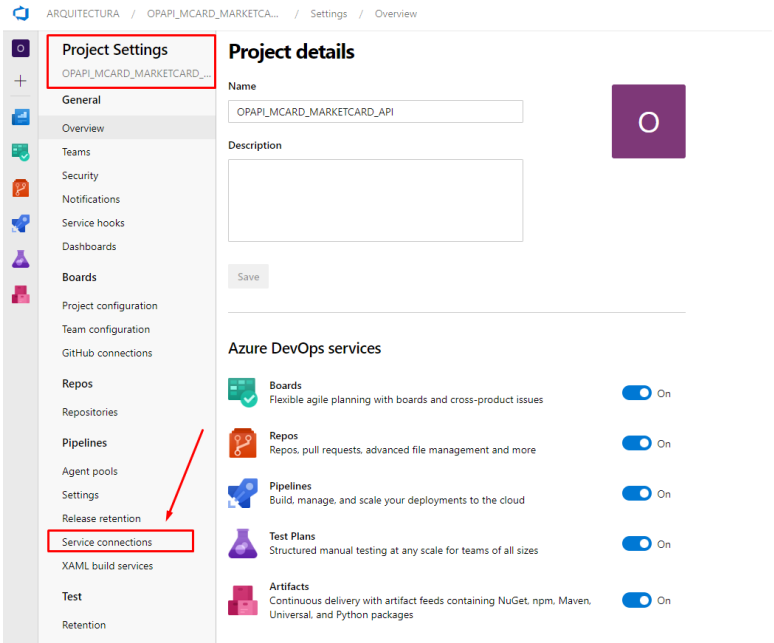
Conexión al Servicio de SonarQube

A continuación, se ejemplifica la conexión a SonarQube desde Azure DevOps.

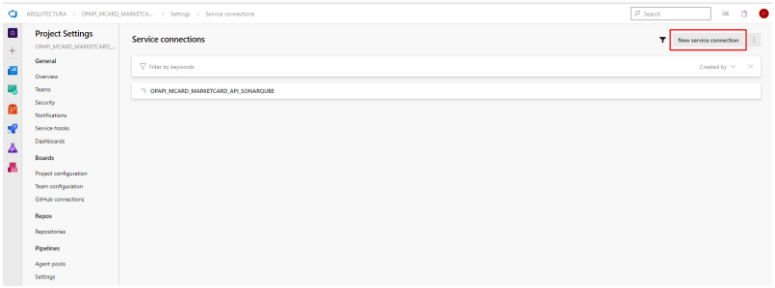
Nos posicionamos en el proyecto donde requerimos implementar el análisis con SonarQube y seleccionamos *"Project Settings"*.



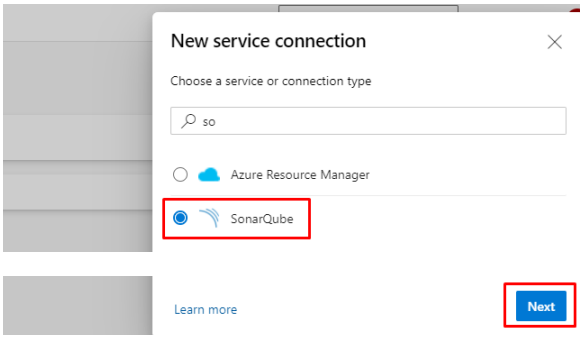
Seguidamente, seleccionamos *"Service connections"*.



Seleccionamos *"New service connection"*



Seleccionamos *"SonarQube"* y damos click en *"Next"*.



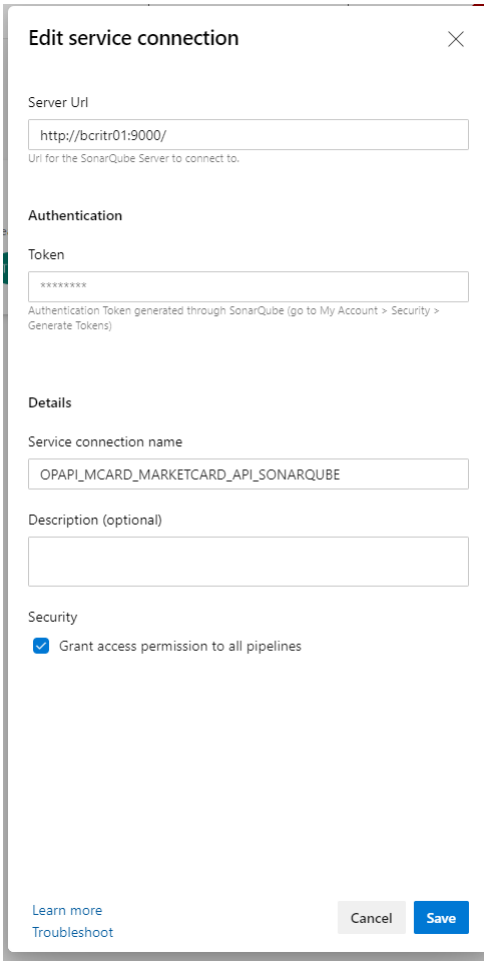
En la siguiente pantalla ingresamos los siguientes datos y presionamos "Save":

Server Url: http://bcritr01:9000/

Token: Ingresar Token proporcionado.

Service connection name: Ingresar nombre del Proyecto.

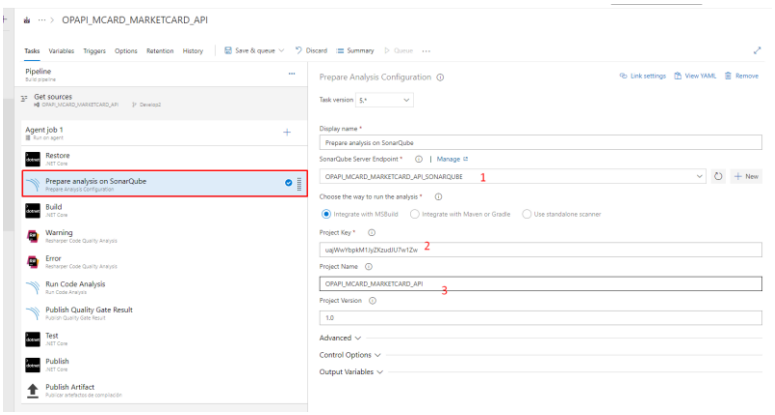
Security: Otorgar permisos altos de acceso para todos los pipelines.



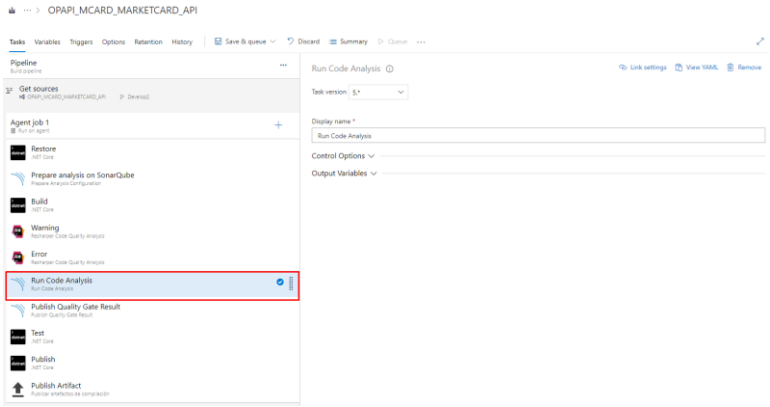
Configuración de Tasks en el Pipeline

En el Pipeline de compilación del proyecto deben configurarse los siguientes tasks:

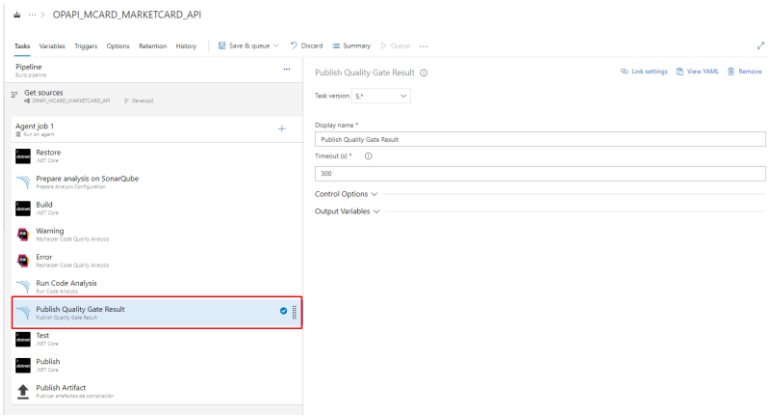
- ✓ **Prepare analysis on SonarQube**
  1. Ingresamos el nombre de la conexión al servicio de SonarQube.
  2. Ingresamos el Project Key, proporcionado por Seguridad de la Información.
  3. Ingresamos el nombre del proyecto



- ✓ **Run Code Analysis**

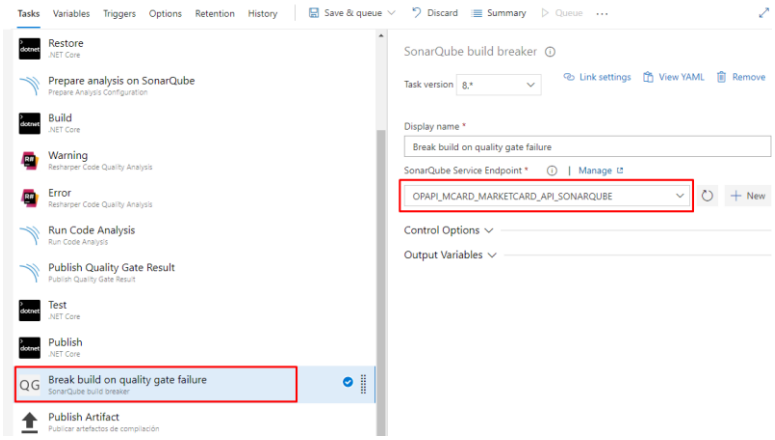


- ✓ **Publish Quality Gate Result**



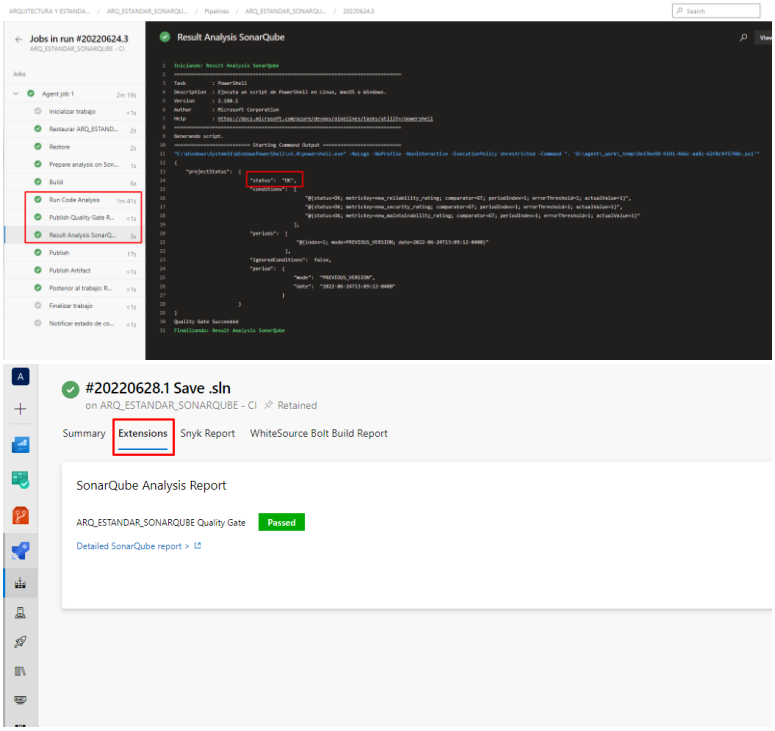
✓ **SonarQube Build Breaker**

1. Se establece el nombre de la conexión al servicio.



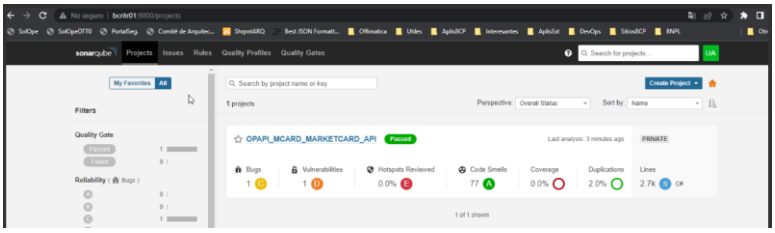
Reporte SonarQube

✓ **Análisis sin vulnerabilidades**



✓ **Análisis con vulnerabilidades**

En el análisis realizado se logró detectar una vulnerabilidad dentro de la solución, esto se expone en la consola de SonarQube a la que podemos acceder con las credenciales remitidas por el equipo de Seguridad de la Información.



8. Acciones a Tomar

Mandatoriamente todas las vulnerabilidades, bugs, entre otros; hallados en el análisis deben ser solucionados para continuar con el pase a producción.

9. Repositorio de ejemplo

A fin de coadyuvar y ejemplificar esta implementación, se proporciona el siguiente proyecto en Azure DevOps accesible desde la siguiente ruta:

https://btbdow00/tfs/ARQUITECTURA%20Y%20ESTANDARES/ARQ_ESTANDAR_SONARQUBE/_build

10. Observaciones

En caso de tener alguna observación o agregar alguna consideración, enviarlo a los siguientes correos:

Bolivia - Arquitectura y Estándares TI	BolArqEstaTI@bancred.com.bo
Jose Angel Zurita Plata	JZurita@bcp.com.bo
Braian Espejo Peralta	BEspejo@bcp.com.bo
Diego Tarquino Tapia	DTarquino@bcp.com.bo