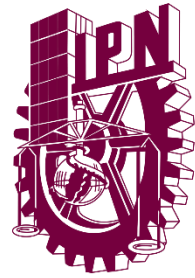




**Instituto Politécnico
Nacional**



Unidad Profesional Interdisciplinaria en Ingeniería y
Tecnologías Avanzadas

Seguridad de Redes

Profesor. Polanco Montelongo Francisco Antonio

Alumno: Hernández Guzmán Bryan Alexis

Grupo: 3TV4

Práctica: Sonarqube

INTRODUCCION

SonarQube es una plataforma de código abierto para la inspección continua de la calidad del código a través de diferentes herramientas de análisis estático de código fuente. Proporciona métricas que ayudan a mejorar la calidad del código de un programa permitiendo a los equipos de desarrollo hacer seguimiento y detectar errores y vulnerabilidades de seguridad para mantener el código limpio.

Es una herramienta esencial para la fase de testing y auditoría de código dentro del ciclo de desarrollo de una aplicación y se considera perfecta para guiar a los equipos de desarrollo durante las revisiones de código. Soporta una etapa de inspección continua.

SonarQube está escrito en Java, pero puede analizar y administrar código 29 lenguajes de programación importantes, incluidos c / c ++, PL / SQL, Cobol, etc., a través de conjuntos de reglas incorporados que pueden ser ampliados con varios complementos.

Esta herramienta al centrarse en el nuevo código ayuda a la detección de muchos problemas, facilitando su solución de manera rápida en cuanto aparece por lo que permite mantener el código limpio, sencillo y fácil de leer.

Los desarrolladores se apoyan en esta plataforma para lograr la integración e implementación continuas del código, que no solo funciona para detectar los problemas, sino también, para rastrear, controlar y verificar la calidad continua del código.

Características

- Admite los lenguajes de programación más populares como Java, C / C ++, Objective-C, C #, PHP, Flex, Groovy, JavaScript, Python, PL / SQL, COBOL, etc.
- Realiza revisiones automáticas con análisis de código estático detectando problemas que afectan la calidad del código.
- Facilita informes ofreciendo información objetiva de la calidad actual de los proyectos utilizando métricas y gráficos de prueba de calidad avanzados. Esto incluye datos sobre código duplicado, estándares de codificación, pruebas unitarias, cobertura de código, complejidad del código, errores potenciales, comentarios, diseño y arquitectura.

- Se integra con toda la cadena de herramientas de DevOps ayudando al flujo de trabajo productivo, incluidos los sistemas de compilación, los motores de CI, utilizando webhooks y su RestAPI integral.
- Es ampliable con el uso de complementos.

Beneficios de SonarQube

1. Alerta de manera automática a los desarrolladores de los errores de código para corregirlos previamente a la implementación en producción.
2. No sólo muestra los errores, también las reglas de codificación, la cobertura de las pruebas, las duplicaciones, la complejidad y la arquitectura, plasmando todos estos datos en paneles de control detallados.
3. Ayuda al equipo a mejorar en sus habilidades como programadores al facilitar un seguimiento de los problemas de calidad.
4. Permite la creación de paneles y filtros personalizables para centrarse en áreas clave y entregar productos de calidad a tiempo.
5. Favorece la productividad al reducir la complejidad del código acortando tiempos y costes adicionales al evitar cambiar el código constantemente.

Desarrollo:

Primeramente se usara este comando:

```
sudo apt install default-jdk
```

Yo tuve problemas con los repositorios sin embargo con el puro comando de sudo, me funcionó

```
sudo apt install postgresql
```

Después de que instalamos el postgresql, verificamos que este corriendo:

```
sudo systemctl is-enabled postgresql  
sudo systemctl status postgresql
```

Luego de que este verificado, procederemos a logearnos:

```
sudo -u postgres psql
```

Escribiremos las siguientes líneas de comando:

```
CREATE USER sonarqube WITH PASSWORD 'Password';  
CREATE DATABASE sonarqube OWNER sonarqube;  
GRANT ALL PRIVILEGES ON DATABASE sonarqube TO sonarqube;
```

Procederemos a hacer algunos ajustes de la aplicación con el siguiente comando:

```
sudo useradd -b /opt/sonarqube -s /bin/bash sonarqube
```

Abriremos el editor para agregar un par de líneas con:

```
sudo nano /etc/sysctl.conf
```

y agregaremos:

```
vm.max_map_count=524288  
fs.file-max=131072
```

Agregaremos el siguiente comando para efectuar los cambios hechos:

```
sudo sysctl --system
```

procederemos a hacer más configuraciones:

```
sudo nano /etc/security/limits.d/99-sonarqube.conf
```

agregando las siguientes líneas de texto:

```
sonarqube - nofile 131072  
sonarqube - nproc 8192
```

Procedremos a descargar sonarqube:

```
sudo apt install unzip software-properties-common wget  
wget https://binaries.sonarsource.com/Distribution/sonarqube/  
sonarqube-9.6.1.59531.zip
```

```
unzip sonarqube-9.6.1.59531.zip
```

Movemos el siguiente directorio:

```
mv sonarqube-9.6.1.59531 /opt/sonarqube  
sudo chown -R sonarqube:sonarqube /opt/sonarqube
```

Procedemos a configurar Sonarqube:

```
nano /opt/sonarqube/conf/sonar.properties
```

Agregamos los siguientes detalles en el editor:

```
sonar.jdbc.username=sonarqube  
sonar.jdbc.password=Password  
  
sonar.jdbc.url=jdbc:postgresql://localhost:5432/sonarqube  
sonar.search.javaOpts=-Xmx512m -Xms512m -XX:MaxDirectMemorySize=25  
6m -XX:+HeapDumpOnOutOfMemoryError  
sonar.web.host=127.0.0.1  
sonar.web.port=9000  
sonar.web.javaAdditionalOpts=-server  
  
sonar.log.level=INFO  
sonar.path.logs=logs
```

Para proceder con el siguiente comando:

```
sudo nano /etc/systemd/system/sonarqube.service
```

```
[Unit]  
Description=SonarQube service  
After=syslog.target network.target  
  
[Service]  
Type=forking  
ExecStart=/opt/sonarqube/bin/linux-x86-64/sonar.sh start  
ExecStop=/opt/sonarqube/bin/linux-x86-64/sonar.sh stop  
User=sonarqube  
Group=sonarqube
```

```
Restart=always
LimitNOFILE=65536
LimitNPROC=4096
```

```
[Install]
WantedBy=multi-user.target
```

Y agregar en el editor de texto

Activamos con los siguientes comandos:

```
sudo systemctl start sonarqube.service
sudo systemctl enable sonarqube.service
```

Para correrlos necesitamos:

```
sudo apt install nginx
```

Habilitamos:

```
sudo systemctl is-enabled nginx
sudo systemctl status nginx
```

Dentro del siguiente archivo se harán las siguientes configuraciones:

```
sudo nano /etc/nginx/sites-available/sonarqube.conf
```

```
server {

    listen 80;
    server_name sonar.hwdomain.io;
    access_log /var/log/nginx/sonar.access.log;
    error_log /var/log/nginx/sonar.error.log;
    proxy_buffers 16 64k;
    proxy_buffer_size 128k;

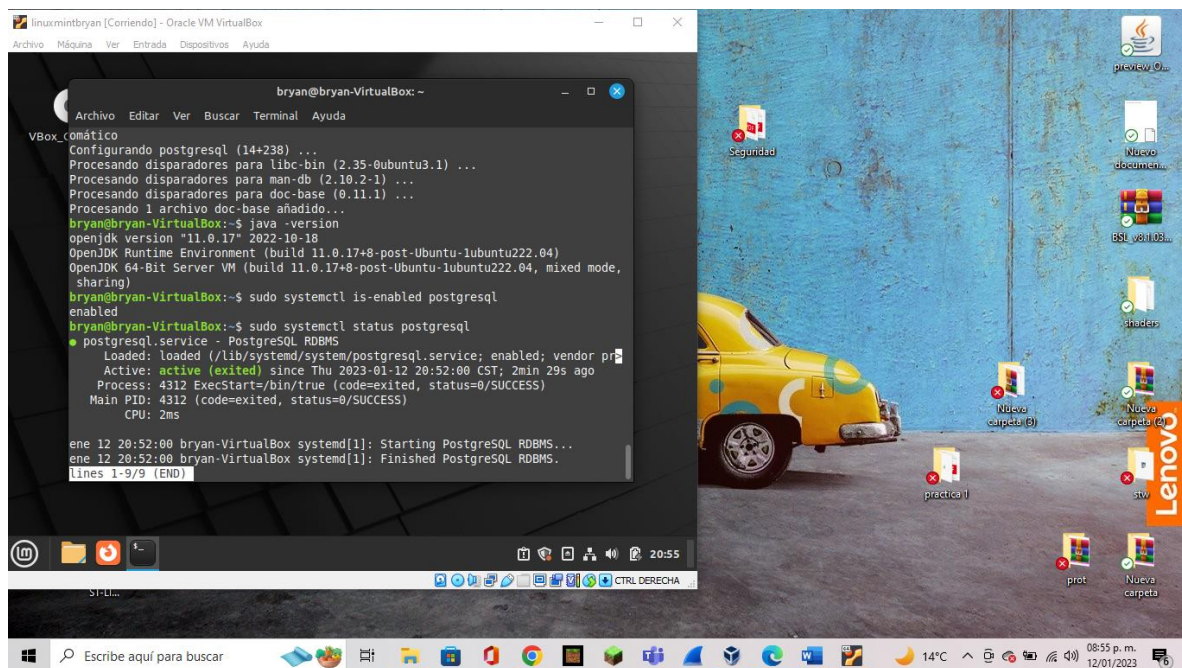
    location / {
        proxy_pass http://127.0.0.1:9000;
        proxy_next_upstream error timeout invalid_header http_500
http_502 http_503 http_504;
```

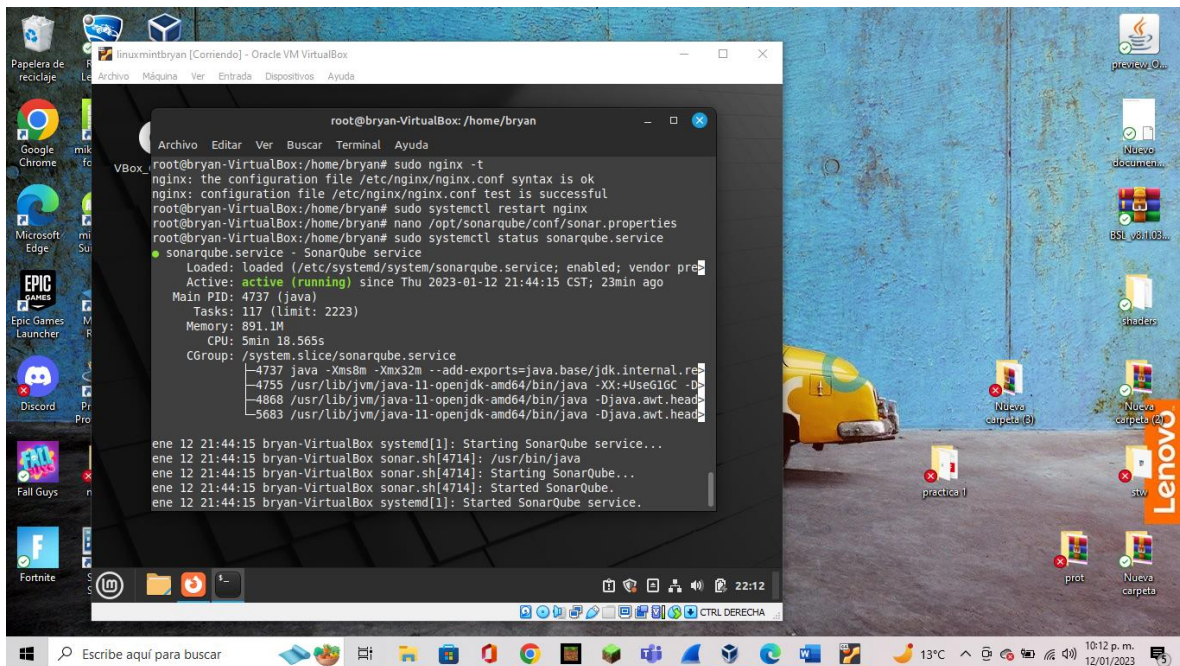
```
proxy_redirect off;
proxy_set_header Host $host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;

    proxy_set_header X-Forwarded-Proto http;
}
```

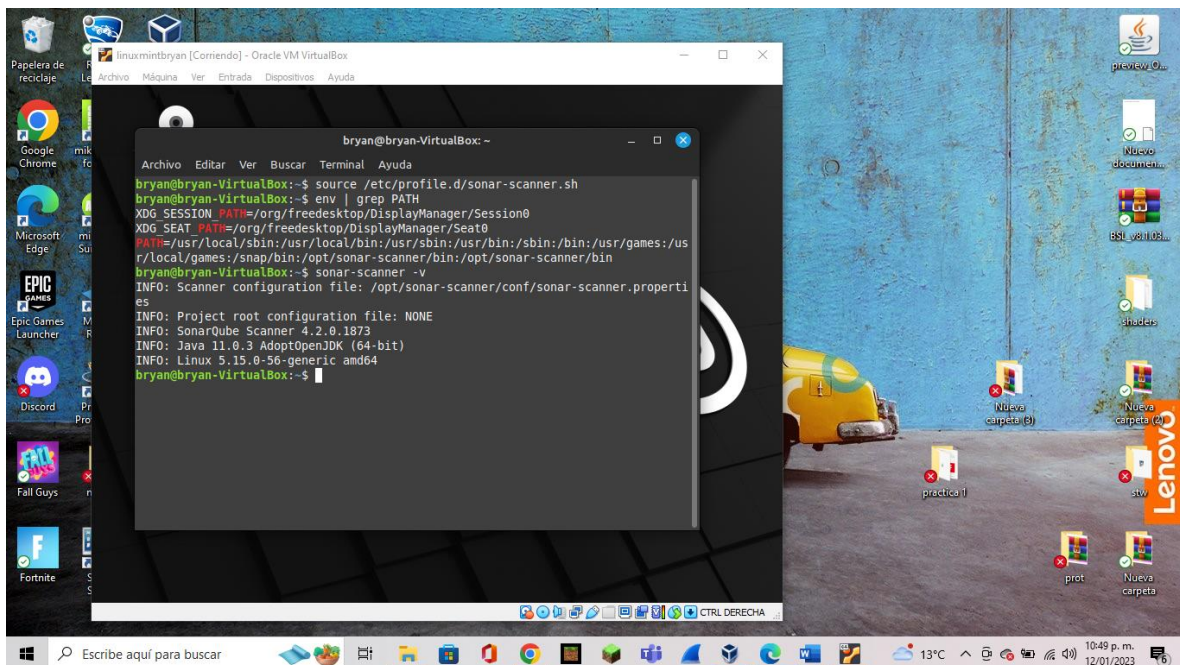
Salvamos y reiniciamos:

```
sudo systemctl restart nginx
```



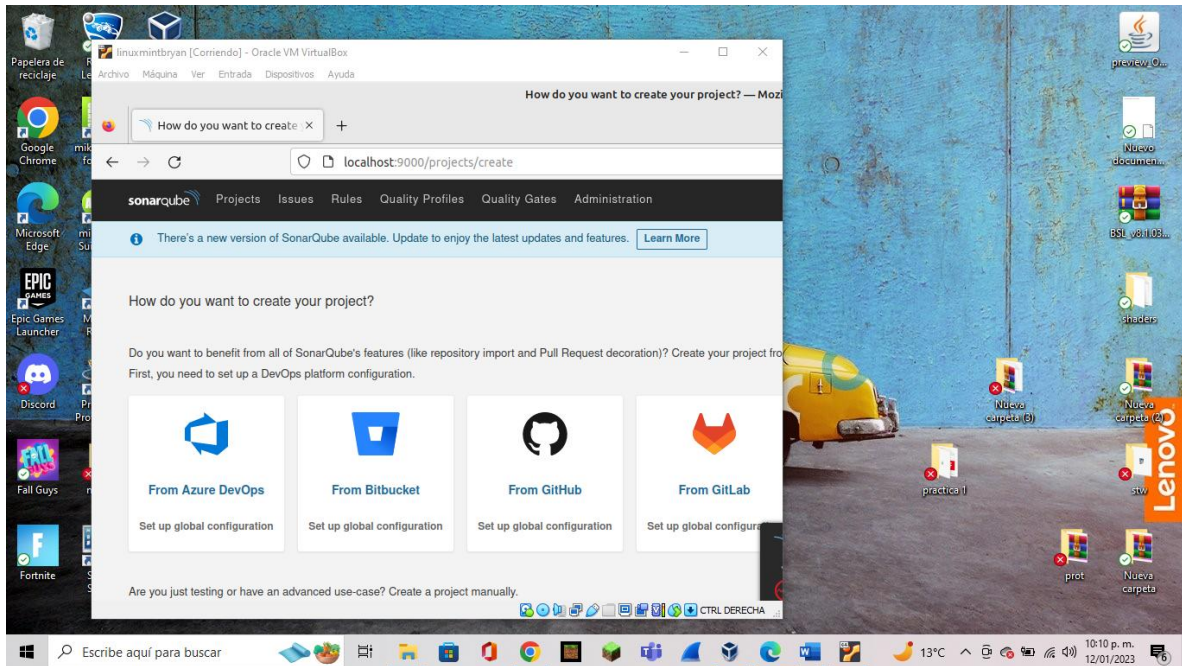


Para poder acceder se tiene que entrar en el bucar con Localhost:9000 que fue el puerto que le asignamos, se hace accede escribiendo admin en el usuario y el password y después te pedirá cambiar las contraseña y ahí se cambia por la que uno lo requiera



Aquí terminamos de instalar el escáner para proceder a entrar a la página.

La página nos pedirá que nos loguemos con admin de usuario y contraseña admin para cambiarla posteriormente



Crearemos un nuevo proyecto a analizar, le pondremos zabbix

Nos generara un token que posteriormente nos va a servir:

Browser tabs: (58) WhatsApp, Tutorial - Inst, How to Instal, P7 - Google, Horarios de c, Ingeniería Te, trayectoria id, sonar.hwdom, +

URL: techexpert.tips/es/sonarqube-es/sonarqube-instalacion-del-escaner-en-ubuntu-linux/?fbclid=IwAR229-SR3NKyx39EWeSKpfzTE2hvYvh_XqzuT2ZeZE-7y-JHng...

TechExpert TIPS

Home - TechExpert Tutorials Libro - Proyecto de Red con Switch HP Youtube Channels About Español

Set Up

Establezca una clave de proyecto y un nombre para mostrar.

Analyze your project

We initialized your project on SonarQube, now it's up to you to launch analyses!

1 Provide a token

Generate a token

token-zabbix

The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point of time in your [user account](#).

Escriba una cadena para el nombre del token de proyecto y haga clic en el botón Generar.

En nuestro ejemplo, introdujimos el nombre de token Zabbix.

El token se utiliza para identificarle cuando se realiza un análisis.

Si se ha visto comprometido, puede revocarlo en cualquier momento de su cuenta de usuario.

En nuestro ejemplo, el token generado fue zabbix: 47c300fa4d7b9e8a3e7c953e77c250477f3617e5

BAHIA PRINCIPE HOTELS & RESORTS

Cancelación Gratuita

Grand Bahia Principe Cuba

This website uses cookies and third party services.

Windows taskbar: Escribe aquí para buscar, 13°C, 11:01 p.m., 12/01/2023

zabbix ☆ master +

Overview Issues Security Hotspots Measures Code Activity

1 Provide a token

token-zabbix: **sqp_7fdeb044f6c1501a689dbfe47954debbfc642234**

The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point in time in your [user account](#).

Se aplicarán las siguientes opciones:

Overview Issues Security Hotspots Measures Code Activity

2 Run analysis on your project

What option best describes your build?

Maven Gradle .NET Other (for JS, TS, Go, Python, PHP, ...)

What is your OS?

Linux Windows macOS

Para ejecutar el escáner se hará de esto, con las características que ya se le dieron al programa sonar-scanner \

-Dsonar.projectKey=zabbix \

-Dsonar.sources=. \

-Dsonar.host.url=http://localhost:9000 \

-Dsonar.login= sqp_7fdeb044f6c1501a689dbfe47954debbfc642234

```

Archivo  Editor  Ver  Buscar  Terminal  Ayuda
INFO: Sensor VB.NET Analysis Log [vbnet]
INFO: Sensor VB.NET Analysis Log [vbnet] (done) | time=333ms
INFO: Sensor VB.NET Properties [vbnet]
INFO: Sensor VB.NET Properties [vbnet] (done) | time=6ms
INFO: ----- Run sensors on project
INFO: Sensor Analysis Warnings import [csharp]
INFO: Sensor Analysis Warnings import [csharp] (done) | time=14ms
INFO: Sensor Zero Coverage Sensor
INFO: Sensor Zero Coverage Sensor (done) | time=98ms
INFO: SCM Publisher No SCM system was detected. You can use the 'sonar.scm.provider' property to e
xplicitly specify it.
INFO: CPD Executor Calculating CPD for 0 files
INFO: CPD Executor CPD calculation finished (done) | time=0ms
INFO: Analysis report generated in 1042ms, dir size=115.7 kB
INFO: Analysis report compressed in 262ms, zip size=13.8 kB
INFO: Analysis report uploaded in 283ms
INFO: ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=zabbix
INFO: Note that you will be able to access the updated dashboard once the server has processed the
submitted analysis report
INFO: More about the report processing at http://localhost:9000/api/ce/task?id=AYWpmFFGy8EWzY9gnI2
r
INFO: Analysis total time: 48.375 s
INFO: -----
INFO: EXECUTION SUCCESS
INFO: -----
INFO: Total time: 57.077s
INFO: Final Memory: 15M/69M

```

Se observa el proceso de revisión del proyecto:

The screenshot displays the SonarQube web interface. On the left, there are filters for 'Quality Gate' (Passed: 1, Failed: 0) and 'Reliability' (A rating: 1, B rating: 0, C rating: 0, D rating: 0, E rating: 0). The main area shows a search bar, a list of 1 project, and a detailed view for 'zabbix' which is 'Passed'. The last analysis was on January 12, 2023 at 11:26 PM. A message states 'The main branch of this project is empty.' The footer indicates 'SonarQube™ technology is powered by SonarSource Community Edition - Version 9.6.1 (build 59531) - LGPL v3 - Community - D'.

Conclusión:

Esta práctica lo difícil fue la instalación, muchos comandos que en su mayoría no aplicaba para nuestra distribución, al final se consiguió visualizar el apartado del sonarqube como una pagina web y un ambiente gráfico, el analizar proyecto para ver vulnerabilidades es de suma importancia, ya que puede evitar problemas antes de ejecutarlos, no necesariamente que contengan virus pero si algún bug que pueda perjudicar dicho proyecto, muy útil a la hora de revisar proyectos propios