

Sonarqube – Introdução



DevOps  
Mão na  
Massa

# O que é e para que serve?

---

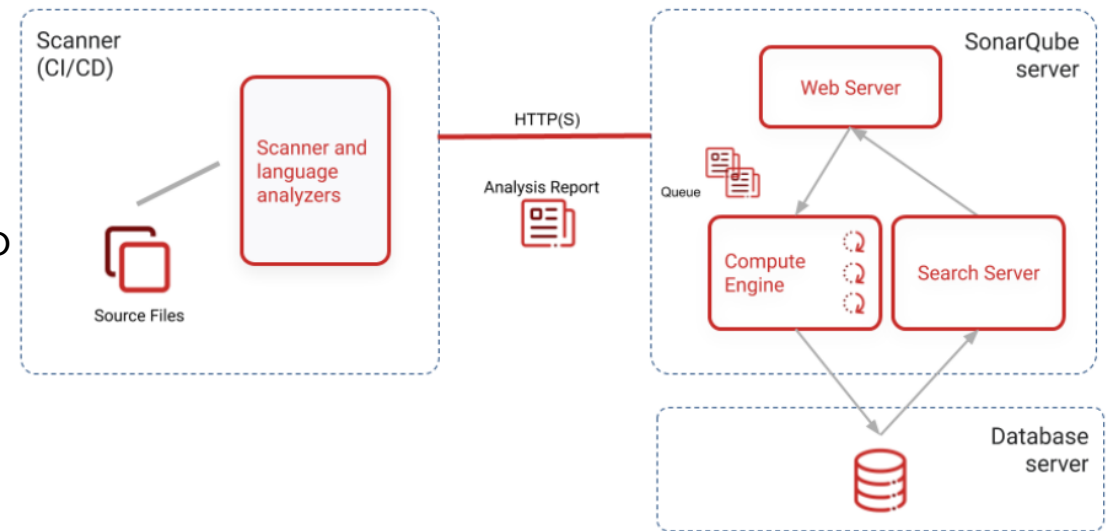
- Ferramenta open source escrita em Java
- Análise estática de código - verifica qualidade e segurança da aplicação
- Dashboards e reports desenvolvidos para o time de desenvolvimento
- Suporte a múltiplas linguagens como Java, Python, .Net, Javascript, etc.
- Fácil integração aos pipelines de CI/CD, automação da análise de código durante os commits
- Reduzir o risco de efetuar o deploy de uma aplicação com vulnerabilidades, possíveis bugs ou código complexo com problemas de manutenção



# Arquitetura

---

- Servidor banco de dados
- App web - dashboards e relatórios
- Compute engine: processamento da análise do código
- Search Server - ELK



<https://docs.sonarqube.org/latest/setup/install-server/>

# Sonarqube- mão na massa - Instalação

---

## 1. Vagrantfile

```
Vagrant.configure("2") do |config|
  config.vm.box = "centos/7"
  config.vm.hostname = "sonarqube"
  config.vm.network "forwarded_port", guest: 9000, host: 9000, host_ip: "127.0.0.1"
  config.vm.provision "shell", path: "provision.sh"
  config.vm.provider "virtualbox" do |v|
    v.memory = 1024
  end
end
```

## 2. provision.sh - Instalação do sonarqube e sonar-scanner

```
#!/usr/bin/bash
useradd sonar
yum install wget unzip java-11-openjdk-devel -y
wget https://binaries.sonarsource.com/Distribution/sonarqube/sonarqube-9.1.0.47736.zip
unzip sonarqube-9.1.0.47736.zip -d /opt/
mv /opt/sonarqube-9.1.0.47736 /opt/sonarqube
chown -R sonar:sonar /opt/sonarqube
# instalacao sonar scanner
wget https://binaries.sonarsource.com/Distribution/sonar-scanner-cli/sonar-scanner-cli-4.6.2.2472-linux.zip
sudo unzip sonar-scanner-cli-4.6.2.2472-linux.zip -d /opt/sonar-scanner
chown -R sonar:sonar /opt/sonar-scanner
```

## 3. Acesso a console:

<http://localhost:9000>



# Sonarqube – Configurar Primeiro projeto

## Configuração inicial

1. Senha inicial – admin / admin
2. Reset da senha default

### Update your password

This account should not use the default password.

Enter a new password

All fields marked with \* are required

Old Password \*

New Password \*

Confirm Password \*

Update

## 3. Criar projeto manual

Are you just testing or have an advanced use-case? Create a project manually.



Manually

## 4. Criar projeto redis-app

### Create a project

All fields marked with \* are required

Project display name \*



Up to 255 characters. Some scanners might override the value you provide.

Project key \*



The project key is a unique identifier for your project. It may contain up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '\_' (underscore), '.' (period) and ':' (colon), with at least one non-digit.


Set Up

# Sonarqube – Configurar Primeiro projeto

---

## 5. Analisar localmente

Are you just testing or have an advanced use-case? Analyze your project locally.



Locally

## 6. Nomear token

### 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

Generate

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

## 7. Copiar token

#### 1 Provide a token

redis-app-token: **ca82b69f0d5ab9ad6dd78eef3fbd00fcf9e326cb** 

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

Continue

# Sonarqube – Executar sonar scanner

---

## **Copiar aplicação redis-app para o server**

1. vagrant upload redis-app

## **Executar sonar-scanner:**

2. sonar-scanner -Dsonar.projectKey=redis-app -Dsonar.sources=. \\  
-Dsonar.host.url=http://localhost:9000 \\  
-Dsonar.login=ca82b69f0d5ab9ad6dd78eef3fbd00fcf9e326cb

```
INFO: CPD Executor Calculating CPD for 0 files
INFO: CPD Executor CPD calculation finished (done) | time=1ms
INFO: Load project repositories
INFO: Load project repositories (done) | time=341ms
INFO: Analysis report generated in 595ms, dir size=102.3 kB
INFO: Analysis report compressed in 29ms, zip size=13.1 kB
INFO: Analysis report uploaded in 522ms
INFO: ANALYSIS SUCCESSFUL, you can browse http://localhost:9000/dashboard?id=redis-app
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=AXx07d-eF-fPDoAaqkBB
INFO: Analysis total time: 29.941 s
INFO: -----
INFO: EXECUTION SUCCESS
INFO: -----
INFO: Total time: 37.953s
INFO: Final Memory: 8M/47M
INFO: -----
```

# Sonarqube – Gerar um bug

**Copiar linha de código para inicializar key no redis duas vezes:**

```
//Set initial visits  
client.set('visits', 0);  
  
//Set initial visits  
client.set('visits', 0);
```

**Executar o sonar-scanner novamente**

The screenshot displays the SonarQube web interface for a project named 'redis-app' on the 'master' branch. The top navigation bar includes links for Overview, Issues, Security Hotspots, Measures, Code, and Activity. A notification banner at the top right states 'Last analysis had 2 warnings' on October 12, 2021, at 11:39 AM. The main content area is divided into two sections: 'QUALITY GATE STATUS' and 'MEASURES'.

**QUALITY GATE STATUS**

- Failed** (3 conditions failed)
- On New Code**
  - Reliability Rating on New Code is worse than A (C)
  - Maintainability Rating on New Code is worse than A (C)
  - Security Hotspots Reviewed on New Code is less than 100% (0.0%)

**MEASURES**

- New Code** (Since October 12, 2021, Started 20 minutes ago)
- Overall Code**
- 1** New Bugs (Reliability: C)
- 0** New Vulnerabilities (Security: A)
- 1** New Security Hotspots (0.0% Reviewed, Security Review: E)
- 5min** Added Debt (1 New Code Smells, Maintainability: C)
- 0.0%** Coverage on 1 New Lines to cover
- 0.0%** Duplications on 3 New Lines



# Sonarqube – Corrigir bug – falha de segurança

BUG:

```
10
11 //Set initial visits
12 1 client.set('visits', 0);
13
14 ... //Set initial visits
15 client.set('visits', 0);
16
```

Verify this is the index that was intended; "visits" was already set on line 12. Why is this an issue? 15 minutes ago ▾ L15 1 🔗

🔧 Bug ▾ 🚨 Major ▾ 🔵 Open ▾ ⚪ Not assigned ▾ 5min effort Comment

October 12, 2021, 11:42 AM

Falha de segurança:

**Make sure disclosing the fingerprinting of this web technology is safe here.** [Add Comment](#) [Open in IDE](#) [Get Permalink](#)

Disclosing fingerprints from web application technologies is security-sensitive [javascript:S5689](#)

Category	Others	<b>Status: To review</b>
Review priority	<b>LOW</b>	This Security Hotspot needs to be reviewed to assess whether the code poses a risk.
Assignee	Not assigned <a href="#">🔗</a>	<a href="#">Change status ▾</a>

[/index.js](#) [🔗](#)

```
1  const express = require('express')
2  const redis = require('redis')
3
4  const app = express()
5  //const client = redis.createClient()
6  const client = redis.createClient({
7    host: 'redis-server',
8    port: 6379
9  })
```