DevOps Shack

Setting Up SonarQube On Ubuntu Machine Through Linux Commands

To install SonarQube on Ubuntu 22.04, you can follow this detailed guide step by step. Here's a summary of the process, including the installation and configuration of SonarQube, PostgreSQL, and Nginx, as well as setting up security measures like firewall rules and SSL.

Prerequisites

- A fresh Ubuntu 22.04 server with sudo privileges.
- At least 2GB RAM, 1 CPU core, and 30GB free space.
- Java 11 or 17 installed (Java 17 is used in this guide).

Step 1: Update the System

Ensure your system is up-to-date:

```
sudo apt update
```

```
sudo apt upgrade -y
```

Step 2: Install Java

SonarQube requires Java 11 or 17. Install OpenJDK 17:

```
sudo apt install openjdk-17-jdk -y
```

Verify the installation:

```
java -version
```

Step 3: Install PostgreSQL

SonarQube uses PostgreSQL as its database. Install and configure PostgreSQL 15:

1. Install dependencies:

```
sudo apt install curl ca-certificates
```

```
sudo install -d /usr/share/postgresql-common/pgdg
```

```
sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc --fail
https://www.postgresql.org/media/keys/ACCC4CF8.asc
```

2. Add PostgreSQL repository:

```
sudo sh -c 'echo "deb [signed-by=/usr/share/postgresql-common/pgdg/apt.postgresql.org.asc] https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main" > /etc/apt/sources.list.d/pgdg.list'
```

3. Install PostgreSQL 15:

```
sudo apt update

sudo apt install postgresql-15 -y
```

4. Configure PostgreSQL:

```
sudo -i -u postgres

createuser sonar

createdb sonar -O sonar

psql

ALTER USER sonar WITH ENCRYPTED PASSWORD 'your_password';

\q

exit
```

Step 4: Install SonarQube

1. Download SonarQube:

```
wget https://binaries.sonarsource.com/Distribution/sonarqube/sonarqube-10.5.1.90531.zip
```

2. Extract and move SonarQube:

```
unzip sonarqube-10.5.1.90531.zip

sudo mv sonarqube-10.5.1.90531 /opt/sonarqube
```

3. Create a SonarQube user and change ownership:

```
sudo adduser --system --no-create-home --group --disabled-login sonarqube

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

4. Configure SonarQube:

Edit the SonarQube configuration file:

```
sudo vi /opt/sonarqube/conf/sonar.properties
```

Uncomment and set the following properties:

```
sonar.jdbc.username=sonar

sonar.jdbc.password=your_password

sonar.jdbc.url=jdbc:postgresql://localhost/sonar
```

Step 5: Create a Systemd Service File

1. Create the service file for SonarQube:

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

Add the following content:

```
[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
```

2. Reload the systemd daemon and start SonarQube:

```
sudo systemctl daemon-reload
sudo systemctl start sonarqube
sudo systemctl enable sonarqube
```

Step 6: Configure System Limits

1. Check and increase file descriptors limit:

```
ulimit -n
```

```
sudo vi /etc/security/limits.conf
```

Add:

```
sonarqube   -   nofile   65536
sonarqube   -   nproc    4096
```

2. Set virtual memory limits:

```
sudo sysctl -w vm.max_map_count=262144
```

```
sudo vi /etc/sysctl.conf
```

Add:

```
vm.max_map_count=262144
```

Apply changes:

```
sudo sysctl -p
```

Step 7: Install and Configure Nginx

1. Install Nginx:

```
sudo apt install nginx -y
```

```
sudo mkdir -p /var/www/html/.well-known/acme-challenge/
echo "test" | sudo tee /var/www/html/.well-known/acme-challenge/test-file
```

2. Create Nginx configuration for SonarQube:

```
sudo vi /etc/nginx/sites-available/adityatesting.in
```

Add:

```
server {
   listen 80;
  server_name adityatesting.in www.adityatesting.in;

   # Handle the Let's Encrypt ACME Challenge
   location /.well-known/acme-challenge/ {
      root /var/www/html;
      try_files $uri =404;
   }

   # Proxy pass all other requests to SonarQube
   location / {
      proxy_pass http://127.0.0.1:9000;  # Your SonarQube application
      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 $scheme;
        proxy_redirect off;
    }
}
```

Enable the new configuration:

```
sudo ln -s /etc/nginx/sites-available/adityatesting.in /etc/nginx/sites-enabled/

sudo nginx -t

sudo systemctl restart nginx
```

Step 8: Configure HTTPS

```
sudo apt install certbot python3-certbot-nginx -y
sudo certbot --nginx -d adityatesting.in

sudo nginx -t
sudo systemctl reload nginx
sudo certbot --nginx -d adityatesting.in -d www.adityatesting.in
```