Athawa Prabhu
D15A43

# Advance Devops Assignment 2

04/05

Q.1) Create a REST API with serverless framework.

Ans Creating REST API with serverless framework is an effecient way to deploy serverless applications that can scall automatically without managing servers.

(i) Serverless Framework: A powerful tool that simplifies the deployment of serverless application across various cloud providers such as AWS, Azure and Google Cloud.

(ii) Serverless Architecture: This design model Allows developers to build applications without worrying about underlying infrastructure, enabling focus on code and buisness logic

(iii) REST API: Representational State Transfer is architectural style for designing network applications.

Steps for creating REST API for serverless framework:

1) Install serverless framework:
You stard by installing Serverless framework CLI globally using Node Package Manager (npm). This allows you to manage serverless applications directly from youre terminal

2) Create a Node.js serverless project:
A directory is created for your project, where you intiatize serverless service (project). This service will have all youre lambda functions,

configurations and cloud resources. Using the command 'serverless create', you set up a template for AWS Node.js microservices that will eventually deploy to AWS Lambda.

Project Structure:
The project scaffold creates essential files like handler.js (which contains code for lambda functions) and serverless.yml.

4) Create a REST API resource
In the serverless.yml file you define function that handles HTTP POST requests.

5) Deploy the service:
With the 'sls deploy' command, serverless framework packages your applications, uploads necessary resources to AWS and set up the infrastructure.

6) Testing the API:
Once deployed you can test REST API using tools like curl or Postman by making POST requests to generated API.

7) Storing data in Dynamo DB
To store ~~sum~~ submitted Candidate data, you integrate AWS Dynamo DB as database

8) Adding more functionalities
Adding functionalities like 'List all candidates. Get candidates

9) AWS IAM Permissions
You need to ensure that serverless framework is given right permissions to interact with AWS resources like dynamo DB.

10) Monitoring and Maintenance
After deployment serverless framework provides service information

Q.2) Case Study for Sonar Qube:
Creating your own profile in Sonarqube for testing project quality. Use screenshot to anbalyze your Github code.
Install sonarlint in your Java Intellij Ide and analyze Java code
Analyze python project with sonarqube.
Analyze node js project with sonarqube
→ Sonar Qube is an open source platform used inspection of code quality. It detects bugs, code smells and security vulnerabilities

1) Profile creation in Sonar Qube:
Quality profiles in Sonar Qube are essential configurations that define rules applied during code analysis. Each project has a

quality profile for every supported language with default being 'Sonarway' profile comes builtin for all languages. Custom profiles can be created by copying or extending existing ones. Copying creates an independent profile, while extending inherits rules from parent profile and reflects future changes automatically. You can activate or deactivate rules, prioritizes certain rules and configure parameters to tailor profile to specific projects. Permissions to manage quality profile are restricted to users with administrative privileges. Sonar Qube allows for the comparison of two profiles to check for difference in activated rules and users can track changes via event log. Quality profiles can also be imported from other instances via backup and restore. To ensure profiles include new rules it's important to check against updated built in profiles or use SonarQube rules page (which contains code for Lambda function and Serverless.yml.

2) Using SonarCloud to Analyze Github code:
Sonarcloud is cloud based counterpart of Sonar Qube that integrates directly with Github, Azure and GitHab repositories. To get started with Sonarcloud via GitHab sign up via Sonarcloud product page and connect to the Github organisation or personal account. Once con-

but it requires third party tool like Coverage.py to generate coverage part. To enable coverage adjust your blind process so that coverage tool runs before sonar scanner and ensures report file is saved in defined path.
For setup you can use Py Test and coverage.py to configure and run test. In your text include configurations for Pytest and coverage to generate coverage report in XML format. The build process can be automated using Github Actions, which install dependencies runs, tests and invoke SonarQube scanner. Ensure report in XML format and place where scanner can have access to it.

5) Analyzing Node.js Projects with SonarQube:
For Node.js project SonarQube can analyze Javascript and Typescript code. Similar to the Python setup, you can configure SonarQube to analyze node.js projects by installing appropriate plugin and using Sonar Scanner against industry standard rules and best practices, flagging issues related to security vulnerabilities bugs and performance optimization.

8.3) At a large organization, you centralized operations team may get many repetitive infrastructure requests. You can use Terraform to build a self-serve infrastructure model that lets product teams manage their own infrastructure indepen

nected SonarCloud mirrors your Github setup with each project corresponding to Github repository. After setting up the organisation choose subscription plan (free for public repository). Next import repositories into your SonarCloud organisation where each Github repo become a SonarCloud Project. Define 'new code' to focus on recent changes and choose between automatic analysis and cloud based analysis. Automatic analysis happens directly in SonarCloud. While CI-based analysis integrates with your build process once analysis is complete results can be viewed in both sonarcloud and Github including security importissue.

3) Sonarlint in Java IDE

Sonarlint is an IDE that performs on the fly code analysis as you write code. It helps developers detect bugs, security vulnerabilities and code smells directly in the development environment such as Intellij Idea or Eclipse. To set it up, install the SonarLint plugin, configure the connection with SonarQube or SonarCloud and select the project profile to analyze Java code. This approach ensures immediate feedback on code quality, promoting clean and maintainable code from beginning.

1) Analyzing Python projects with SonarQube:

SonarQube supports python coverage & reporting

dently. You can create and use Terraform modules
Q3) that codify the standards for deploying and managing services in your organisation.

Ans Implementing a self serve infrastructure model using terraform can significantly streamline operations with large organisation's. Here's structured approach to achieve this.

1) Centralized operations

- Address repetitive infrastructure request from product teams by using terraform.

2) Create terraform modules

- Develop reusable modules that define standards for deploying and managing infrastructure.

3) Empower product team:-
- Set up self-service portal where team can initiate requests using predefined modules enabling them to manage the infrastructure independently.

4) Integrate terraform cloud
- Connect terraform cloud with ticket system like service to automate requests.