# Technical challenges for DevOps Engineer position

> Please create a Git Repository for this challenge and commit all answers to it. Please keep this organised and commit with clear messages. Once complete, notify us and we will provide you with an email to add to the repository so we can review.

## Basics

> General

1. What is the role of AWS/Azure/GCP in DevOps?

2. How will you approach a project that needs to implement DevOps?

**Project need CI/CD pipeline implement below pointes.**

**1.Organizing a DevOps initiative**

**2.Building the DevOps strategy**

**3.Containerizing**

**4.Integrating infrastructure automation with CI/CD tools**

**5.Increasing the amount of test automation and aligning QA with development**

**6.Ensuring total application performance monitoring**

3. Mention some of the core benefits of DevOps.

**1.devops delivering faster.**

**2.Agile practices and different delivery models along with DevOps is used.**

**3.devops developers create automated security testing/assessment solutions.**

**4.The organization's reputation is at stake when critical vulnerabilities are found in shipped solution(s) and customer**

**sensitive data is compromised due to lack of security testing focus**

**5.Operations has traditionally been responsible for maintaining the data center or infrastructure**

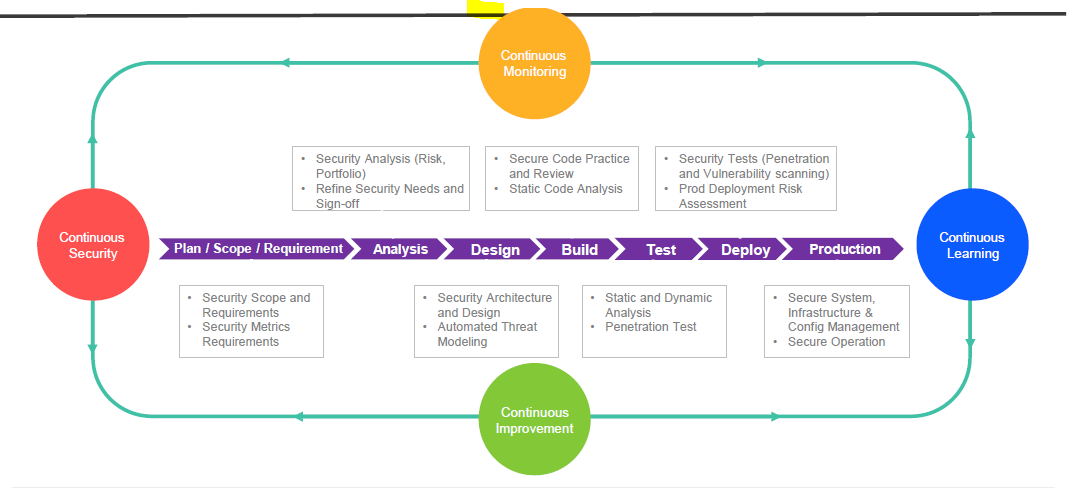
**6.DevSecOps is a combination of Development, Security and Operations for bringing quality and security from the start**

**that help organizations improve time to market and release software faster**

**7.A malicious software deployed by an attacker to infect individuals computer or an entire digital network is a**

**malware It exploits target system vulnerabilities that can be hijacked, such as bugs in legitimate software (browser or web application plugin)**

4. What are the different phases in DevOps?



5. Explain the concept of branching in Git.

**Branching used in developers to Master branch, Hot fixing & bug fixing code base and isolated their work, Git to easily merge versioning checking.**

6. What is a merge conflict in Git, and how can it be resolved?

**Developer A and Developer B. Both of them pull the same code file from the remote repository and try to make various amendments in that file it come conflict git repo.**

> Security

1. What is DDoS attack? How do you deal with it?

**“Rugged” can also be used to describe the software applications produced by rugged organizations. These applications are not only well-protected against attacks, but are also able to analyze themselves, report on their own security status, detect attacks in progress, and respond appropriately.**

**Rugged DevOps can’t defend against L3/L4 attacks, it could help mitigate L7 attacks, Gates notes. Since L7 attacks are so common, a Rugged DevOps approach that fixes many.**

2. What are the benefits of having Policy management?

3. How HTTPS is different from HTTP?

**HTTPS :- http encryption normal and it's used TLS (SSl)**

**HTTP :- Requesting to Accessing and Reponses.**

4. What TCP and UDP vulnerabilities are you familiar with?

**it's work 65% of vulnerabilities it found in Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports are linked to SSH (22/TCP).**

**UDP :-Unreliable transport on top of IP**

**TCP :- Connection-oriented, preserves order (sender / receiver)**

5. Explain OAuth

6. What types of firewalls are there?

**The Cloud Controls Matrix**

**The Cloud Security Alliance ( has consolidated most security compliance methods into a single resource called**

**the Cloud Controls Matrix ( which defines the control ID used to uniquely identify vulnerabilities**

**The Open Web Application Security Project (OWASP)**

**The OWASP is an online community project that provides free articles, methodologies, documentation, tools, and**

**technologies for web application security**

**OWASP is an international organization, and the OWASP Foundation supports OWASP efforts around the world**

**Federal Information Processing Standards (FIPS)**

**The FIPS are security standards developed by the U S federal government for use in non-military government**

**computer systems FIPS defines minimum security requirements for the use of cryptographic modules**

•

The FIPS publication Security Requirements for Cryptographic Modules explains which cryptographic modules are

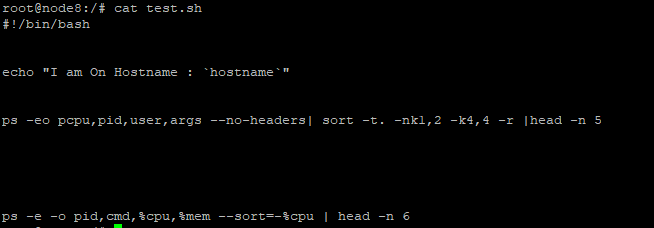
considered safe, legacy or weak

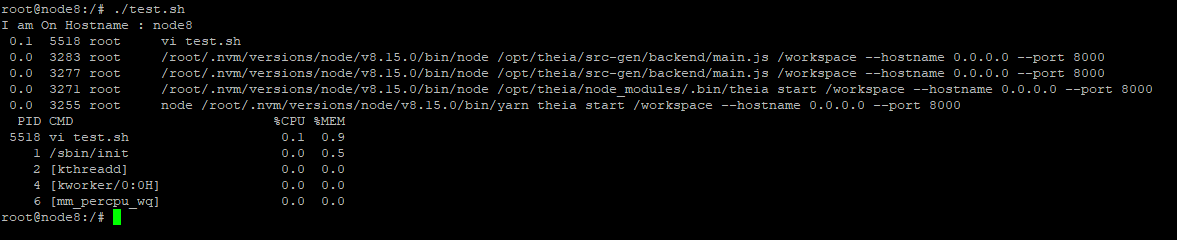
> Technical challenge

\*\*Please also produce a Design Document for this challenge\*\*

**1. Write a simple program in any language you want that outputs "I'm on %HOSTNAME%" (HOSTNAME should be the actual host name on which the app is running) and deploy it to Github**

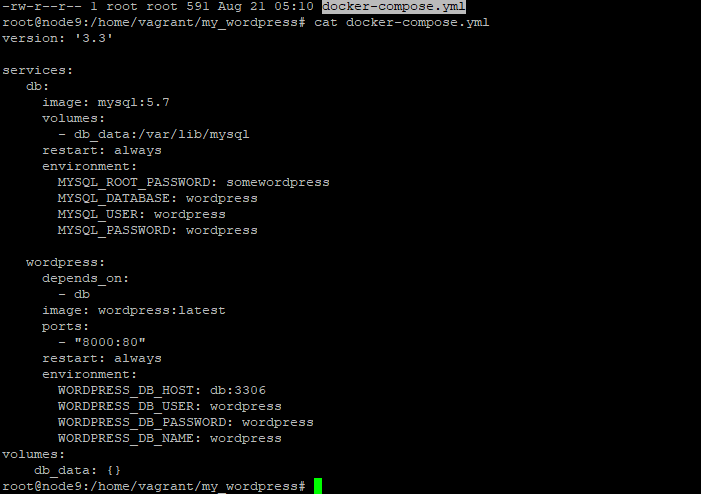
Output:-

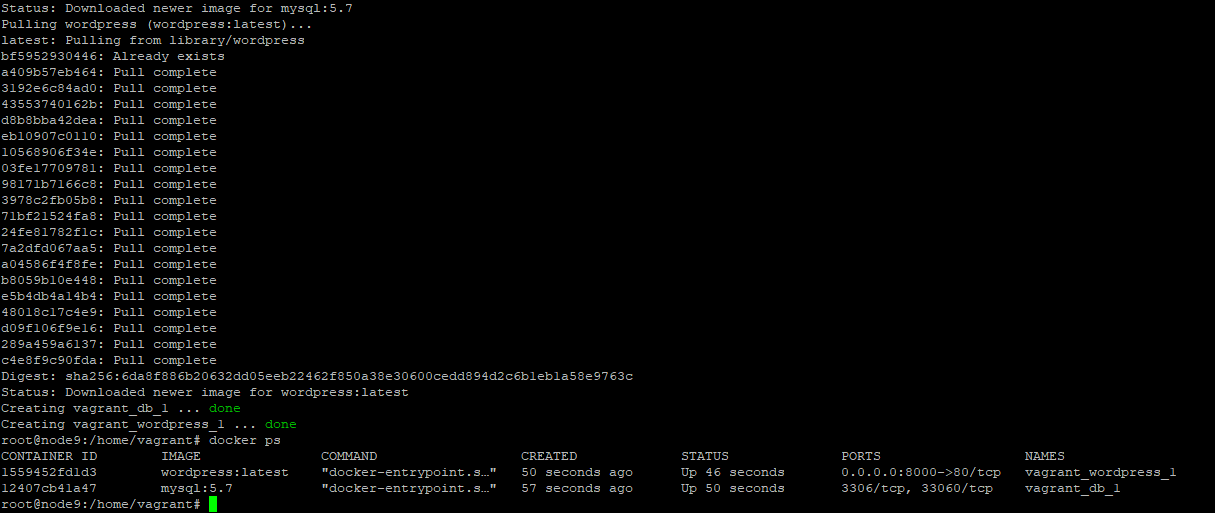
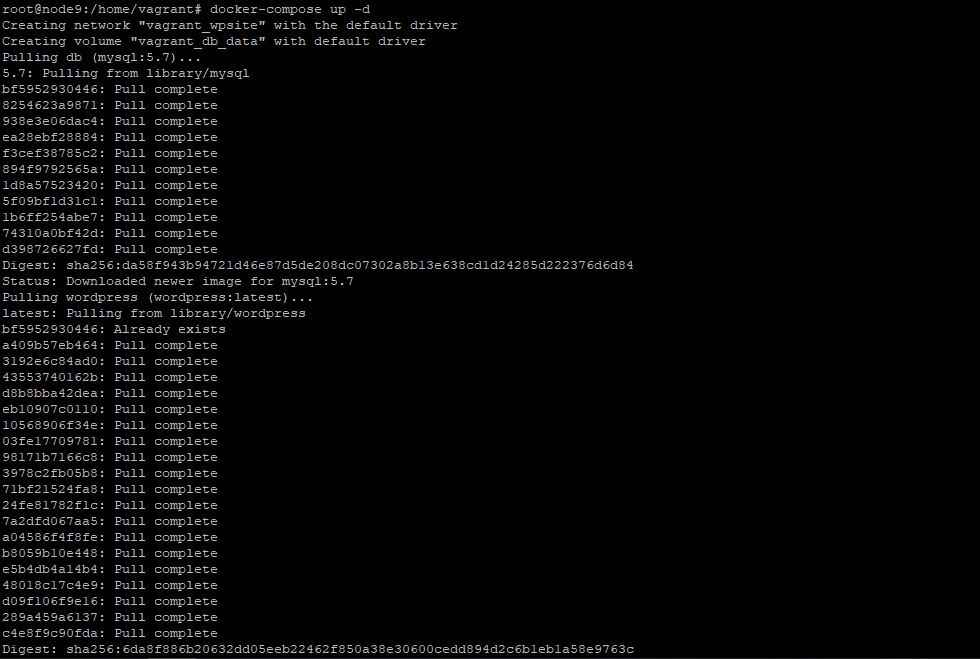


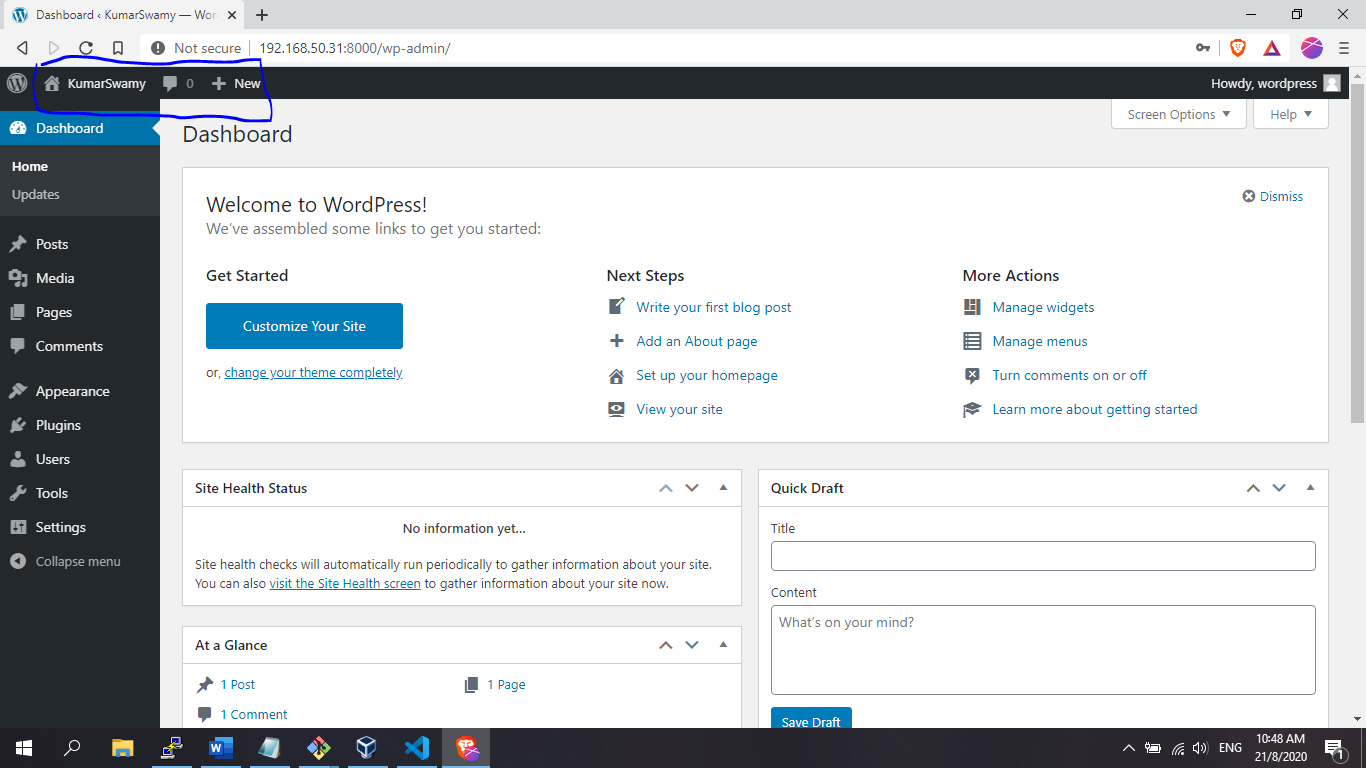


2. Write a Dockerfile which will run your app

Please find Docker file running below Appl







3. Create Github Actions Pipeline to Build the Docker image and push to AWS ECR

Step 1. Aws ECR

2. create repository –any giving name

3. aws ecr create-repository –repository-name dockerimagea\_PSS\_Team - –region us-east-1

4. aws ecr describe-repositories --region us-east-1

5. create Dockerfile ( it’s very simple one below)

FROM alpine

MAINTAINER “kumarswamy”

CMD [“echo”, “Hello, Welcome to Docker!”]

Docker build -t my-friest-repo .

# $(aws ecr get-login –no-include-email –region us-east-1

# Docker tag e7f723f4dc86 586945237890.dkr.ecr.eu-central-1.amazonaws.com/my-first-repo:latest

# Docker push 586945237890.dkr.ecr.eu-central-1.amazonaws.com/my-first-repo:latest

4. Extend the Actions Pipeline to deploy the app to AWS EKS

5. Setup KubeCtl on AWS EKS

EKS cluster setup :

EKS cluster

Iam roles

Security groups

Vpc

Worker node: -

Lanuch configuration

Autoscaling group

Iam roles

Security group

Connect to EKS:

/kube/config

configMap

kubectl

Heptio auth

> Additional features

\*\*Not\*\* required but would be great additional questions to answer

1. Add to your plan how you would handle User Authentication

2. How would you approach Microservice deployments using Azure?

3. How would you deploy API's in Azure and how would you ensure they are secure?