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

The main role of clouds in DevOps is providing spontaneity in Infrastructure as a service and platform as a service

This means when we are starting a project we need to setup Infrastructure(OS, Network, Datacentres, Software installations , configuring network) to all these it’s take lot of time and effort but with these clouds we can bring up all this infra with in minutes there are many advantages

* Get start work on projects fast
* We can use fully managed services those are provided by cloud
* We can scale in or out very quickly
* We can pay what we have used
* Automation
* Security
* Flexibility
* Backup and disaster recovery very easily and highly available

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

* First, I will check is there needed to implement DevOps in that project based on IT and business goals
* Next, we will plan how to proceed and discussion with IT departments.
* We need to encourage collaboration between departments (Development, Testing, Operations, Security administrators and people involved in project. It will improve to take better decisions then it fetches better output and ideas.
* Follow the Agile methodology – we need to adapt customer demands and changes -> to turn this we need to change culture which needs team effort, better communication and commitment to customer satisfaction.
* Start with small release then scale up – it will improve confidence and trust in all stakeholders who are involved with early success.
* Make automation (repeatedly using things) as much as possible and whenever you can.
* Take right decisions in selecting tools make sure they are compatible with what we are using.
* Reviewing performance of teams and an individual.
* Select good tools for project management which will ensure Realtime visibility into the project.
* Follow continuous integration and delivery and monitoring – which can detect defects quickly and provides feedback on releases so that we can rectify bugs at early stages.

1. Mention some of the core benefits of DevOps.

* End to end responsibility
* Focus on customer satisfaction
* Collaborates, cooperates and unites your teams for faster products delivery
* Simplifies development focus
* Introduces automation into the project life cycle

1. What are the different phases in DevOps?

* Plan
* Code
* Build
* Test
* Release
* Deploy
* Operate
* monitor

1. Explain the concept of branching in Git.

Git Branching concept is like a tree. Here trunk is master branch (it always been there), then branches are subbranches they will come and fall. This means a branch in Git is a way to keep developing and coding a new feature or modification to the software and still not affecting the main part of the project (master branch). For every organisation have their own branching strategy Master->Staging->QA->Development under those branches we can create subbranches like feature1, feature2 etc.

* Branches give you the freedom to independently work on different modules (*not necessarily though*) and merge the modules when you finish developing them
* We can remove unwanted code or feature easily no need to stress.
* We can roll back easily
* Branches in Git help the team, which are in different parts of the world, work independently on independent features that would ultimately combine to produce a great project.
* We can track all history of the project

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

When two persons working on same file and changed the things in same lines of code in two different ways; In such case, Git cannot automatically determine what is correct. – Conflicts only affect the developer conducting the merge, the rest of the team is unaware of the conflict. Git will mark the file as being conflicted and halt the merging process. It is then the developers' responsibility to resolve the conflict.

Error message**: Merge Conflict <Filename>, merge failed**

We can solve this in two ways

* Manually we can open the file and delete >>>>, ===== and <<<<< symbols and decide what is correct code to keep yours or others then commit it and merge it
* Next, we can use tools $ git merge –abort

Executing git merge with the --abort option will exit from the merge process and return the branch to the state before the merge began.

$ git reset

Git reset can be used during a merge conflict to reset conflicted files to a known good state.

Security

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

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. Main goal of this type of attacks to overwhelm them with more traffic than the server or network can accommodate.

We can detect this type of attacks by slow accessing files, internet connection, problem accessing websites and number of spam mails.

* I will configure firewalls and routers as they will reject bogus traffic and I will make them UpToDate.
* I will secure IoT devices by installing trusted security software’s.
* Developing a Denial of service response plan
* Maintain redundant network architecture so one server attacked other can handle the network traffic.
* Overprovision bandwidth.
* When I identify this type of attacks first, I will notify to internet service provider and determine is there any possibility re-route the traffic.
* Maintaining hybrid network environment.

1. What are the benefits of having Policy management?

* It provides awareness in workers what is expected of them
* It demonstrates your good faith by treating workers fairly and equally.
* Methods to deal with misunderstandings and complaints
* It creates awareness in workers organisation culture
* Provides confidence and reduce bias in decision making

1. How HTTPS is different from HTTP?

HTTPS is the HTTP with encryption. HTTPS uses SSL(TSL) certificates to encrypt HTTP requests and responses.

With HTTP:

If we send request by Google.com (attacker can see same)

With HTTPS:

Attacker sees (some bunch seemingly random characters)

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

I haven’t got much chance work in networking side,

* Denial of service
* Connection hijacking

1. Explain OAuth?

OAuth is an open-standard authorisation protocol that describes how unrelated servers and services allow safely to authenticate access to their services without sharing initial login credentials. It uses authorisation tokens to prove an identity between services. It helps to interaction between one application to another on your behalf without compromising security.

1. What types of firewalls are there?

* Software firewalls
* Application level gateways
* Packet-filtering firewalls
* Circuit-level gateways
* Hardware firewalls
* Stateful Inspection firewall